Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v2.0

Modern WAN architectures require additional network capabilities to support current higher bandwidth and mission-critical applications. Requirements for deploying voice over IP (VoIP) and video conferencing include high availability, IP multicast, and quality of service (QoS). Today, most enterprises rely on private WAN connections such as Frame Relay, ATM, or leased-line services to connect their businesses. When deploying a traditional Frame Relay or ATM-based private WAN, however, network operations must implement point-to-point or hub-and-spoke architectures that make provisioning and management of moves, adds, or changes on the network complex. Also, the operational expense for a private WAN can sometimes be higher than IP-based WAN technologies. The goal is to have reliable connectivity that is secure, can be easily updated, and can scale to meet evolving business needs.

To address these needs, Cisco provides validated, extensible network architectures that are underpinned by a comprehensive line of services aggregation routers. The portfolio of WAN solutions enables an enterprise to rapidly introduce new business applications and services from the branch office, through the campus, to the data center, while reducing operating costs and network complexity.

This design guide extends the portfolio of WAN solutions to provide a highly available, secure network design to the WAN edge. Providing the WAN architecture with security from outside attacks as well as protecting the traffic entering or exiting the WAN network is the focus of this design guide. This design guide defines the comprehensive functional components required to secure the infrastructure and data paths for an enterprise WAN edge.

Cisco Enterprise Systems Engineering (ESE) is dedicated to producing high-quality tested design guides that are intended to help deploy the system of solutions more confidently and safely. This design guide is part of an ongoing series that addresses enterprise WAN solutions using the latest advanced services technologies from Cisco and based on best practice design principles that have been tested in an enterprise systems environment.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Introduction

This design guide evaluates the securing of an enterprise WAN edge network as it pertains to the Cisco enterprise WAN and MAN architectures. These architectures are defined in detail at the following URL: http://www.cisco.com/go/wanandman

The following four architectures were established to provide reliable connectivity to your global enterprise while reducing operational expenses, becoming more resilient, and enabling some of the latest network services:

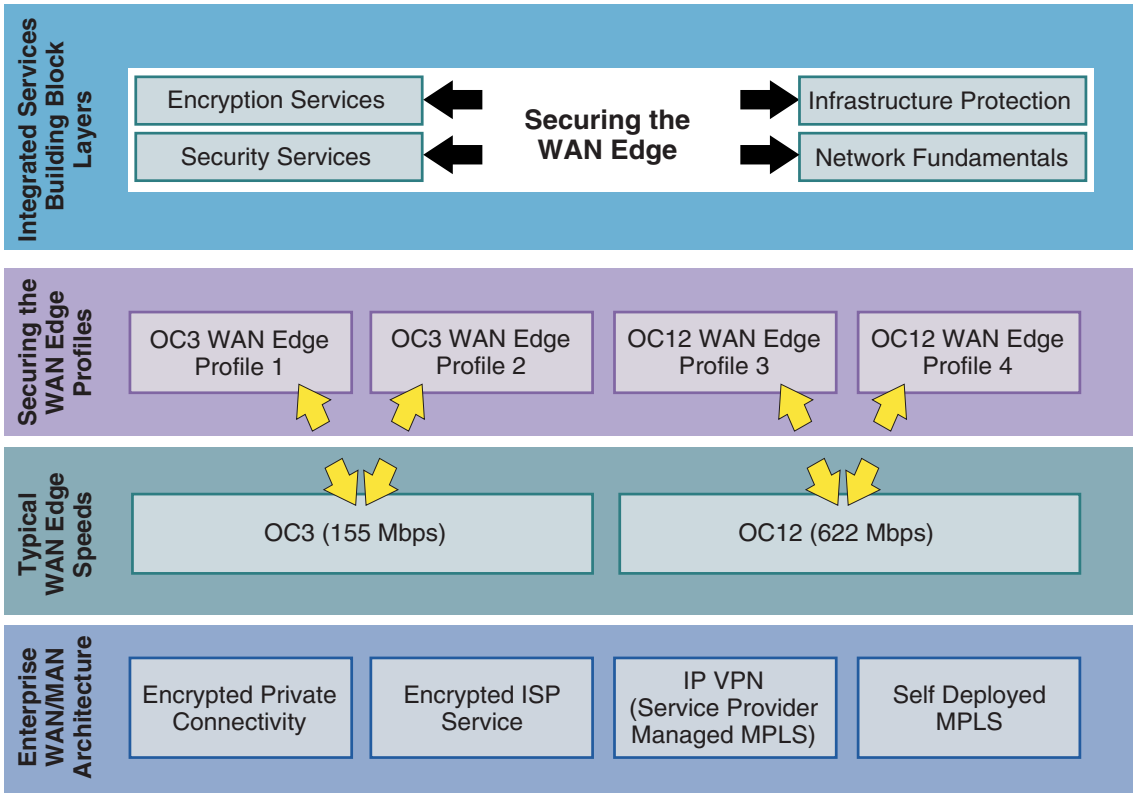
- Encrypted private connectivity—Takes advantage of existing traditional private WAN and MAN connections
- Encrypted ISP service—Takes advantage of the ubiquity of public and private IP networks to provide secure connectivity
- IP VPN (service provider-managed MPLS)—Delivers Layer 2 and Layer 3 VPNs
- Self-deployed MPLS—Provides any-to-any connectivity

These four architectures offer several secure alternatives to traditional private WAN connectivity that help increase network scalability and flexibility.

This design guide focuses only on the enterprise WAN edge network. The enterprise WAN edge is defined as the set of networking devices that aggregate traffic from enterprise branch offices, and pass that traffic to the enterprise campus or data center. Regardless of which enterprise WAN/MAN architecture is chosen, it is crucial to guarantee the devices and traffic residing at the WAN edge. This design guide examines two typical WAN edge speeds, OC3 (155 Mbps) and OC12 (622 Mbps), and

establishes profiles for each WAN speed. These profiles are not intended to be the *only* recommended design architectures for the WAN edge. They are meant to show examples based on the majority of enterprise WAN edge architectures available today. Each profile provides guidelines for securing the WAN edge including infrastructure protection mechanisms, network fundamentals such as routing and high availability, and, finally, the security services needed to protect against threats to the WAN edge. The framework for this document is shown in Figure 1.

Figure 1 Enterprise WAN Edge Network Framework



This design guide begins with an overview followed by design recommendations. In addition, configuration examples are presented. Each service is described in detail and then shown in each of the various profiles to provide complete guidance on how to tackle securing a WAN edge network. You must have a basic understanding of all the following to successfully implement the concepts shown in this document:

- IPsec VPNs
- Firewalling (using either PIX, ASA, or FWSM)
- Access control lists
- QoS and traffic policing
- Dynamic routing protocols
- Basic understanding of denial of service (DoS) attacks and how they operate

Target Audience

This design guide is targeted for Cisco systems engineers and customer support engineers to provide guidelines and best practices for customer deployments.

A version of this design guide suitable for customer use is available at the following URL: http://www.cisco.com/go/wanandman

Scope of Work

This version of the design guide addresses the following applications of the secure NGWAN edge solution:

- Infrastructure protection mechanisms
  - Device hardening
  - Infrastructure access control list (iACL)
  - CPU overload protections such as Control Plane Policing (CoPP) and Call Admission Control (CAC)
  - DoS mitigation mechanisms such as scavenger class QoS and Unicast Reverse Path Forwarding (uRPF)
- Encryption service mechanisms
  - VPN topologies using IPsec as the tunneling method (some include tunnel interfaces) and the effect on dynamic routing protocols.
- Security service mechanisms
  - Firewalling—Using ASA Firewall Appliance or Firewall Service Module (FWSM)
  - Super-logging (also known as remote syslogging)—All relevant NGWAN edge devices remote syslogging to a syslog daemon to a common hardened server in the private (protected) network for audit availability
  - AAA server integration
  - PKI server integration
- A converged data/voice network
  - Data and VoIP converged traffic requirements
  - QoS features are enabled
- Recommendations and limitations for Cisco product performance and scalability considerations within resilient designs

Out of Scope for this Document

Cisco devices incorporate a wide variety of security services and mechanisms designed to protect the network infrastructure and attached host. This version of this document does not cover the following security-related features at this time:

- Intrusion Protection System (IPS) or Intrusion Detection System (IDS)
- Network Admission Control (NAC) or Clean Access technologies
- Managed DDoS Protection

- Network Virtualization (formally known as Network Segmentation)
- Cisco Application Control Engine (ACE)—Application inspection and load balancer
- Blackhole routing using BGP and uRPF

Design Overview

This section provides a high-level overview of concepts to secure an enterprise WAN edge. Design and Implementation, page 24 provides more detail on the design considerations, while Scalability Considerations, page 77 presents primary considerations to be considered before deploying the design for scalability.

A network engineer and a security engineer are usually at odds when it comes to network security. They generally have conflicting goals. The network engineer is trying to connect users with services at the highest possible speed with as little intervention into the actual traffic as possible, while the security engineer is trying to secure the network from both network intrusions (restricting access to services) as well as providing protection to the network itself from DoS-type attacks that rob the infrastructure of valuable uptime. All network security can be summarized is a trade-off of simplicity and efficiency for a level of security and protection. The high-level goal of the security engineer is to achieve these layers of security at the lowest cost to the infrastructure (bandwidth, CPU utilization, and packet delay) as possible.

When choosing which security services and infrastructure protections are right for a customer, it is strongly recommended that customers perform a risk versus cost analysis. This leads to a monetary baseline that a service disruption (down or degraded time) would incur. A “dollar per minute unavailable” value helps in choosing the proper amount of layers and mechanisms that are appropriate for the customer. The customer should compute the amount of monies lost, computed as lost development time, possible PR fallout, legal fees, lost revenue (transactions), and so on, if a network intrusion occurred that yielded proprietary data being made public or consumed by the competition. These values of monies lost help the customer and the Cisco sales engineer decide which of the possible security features are required, explain to management the cost justifications of buying security gear, and assist in the staffing requirements for security enabling the enterprise WAN edge.

Under normal operating conditions, the legitimate end user network traffic consumes some, if not most, of the network resources (bandwidth, CPU utilization, forwarding capacity, and so on) as packets of the end user pass through the network devices. In the event of a DoS attack, a packet, or series of packets, are sent in the attempt to consume those network resources and keep the network from processing the legitimate traffic; thus, denying the legitimate user traffic the services it requires. The goals of infrastructure protection are to limit intrusions, prevent data/service theft, and to minimize the likelihood of success and mitigate the damage caused by DoS attacks. Infrastructure protection includes device hardening to secure the network devices from unauthorized access by non-solution administrators over various communication protocols, as well as mechanisms to control the use of CPU and memory resources.

This document describes some infrastructure protection features embedded in Cisco IOS and some Cisco firewalls, and also the integration of some key security services namely IPsec VPNs and firewalls. This document provides design guidance on enabling and integrating these protections and services on a single network device. It is not intended to be an exhaustive technical review of all nuances of the features, but rather how to implement them in a layered approach to provide a cohesive security solution for the NG WAN edge.

Some alternate barrier (firewall) locations and the ramification to security, performance, and connectivity are discussed in detail in Appendix A—Other Possible Topologies, page 177.

The security features described in this document are by no means an exhaustive integration of all possible security features, but rather the start of a reasonable security framework using the "security in layers" approach to implementing security. The strength of many security layers is stronger than the sum of those security components separately. Most security professionals agree that no one security mechanism is adequate alone. A layered approach of several distinct features is the preferred approach to most security challenges, and provides a more robust solution to the wide range of threats.

Assumptions

The design approach presented in this design guide makes several starting assumptions:

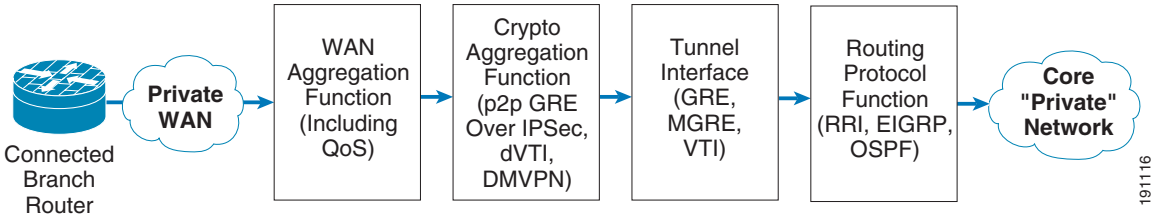
- This document suggests the combination of a minimum set of security-related features to achieve a baseline of security and protection for the devices from unauthorized access, network protection, access control, accounting and syslogging, and some protection from DoS attacks. More possible security features may be enabled and incorporated at a future time. (See Design Components, page 8 for a list of the security features that will be integrated.)
- The design supports a typical converged traffic profile. See Scalability Considerations, page 77 for more detail on the traffic profile used during testing
- High availability is of critical importance; therefore, the recommendations in this design guide reflect the benefits of built-in redundancy and failover with fast convergence. The goal of this high availability is to allow continued operation in the event of a single failure. This is discussed further later in this section and also in Design and Implementation, page 24.
- Cisco products should be maintained at reasonable CPU utilization levels. This is discussed in more detail in Scalability Considerations, page 77, including recommendations for enterprise WAN edge headend devices, and software revisions.
- Although costs were certainly considered, the design recommendations assume that the customer will deploy current security technologies, including hardware-accelerated encryption and a layered security approach.
- The enterprise WAN edge is a transit network that aggregates the connections from the enterprise branch offices LANs via a private or public service provider network. The enterprise WAN edge does not directly connect end users in the campus or branches; rather, it provides connectivity for the enterprise branch LANs to connect to the enterprise core network and its resources.
- The secure enterprise WAN edge devices should *not* also be used as the Internet gateway for the enterprise core network, mainly because of performance reasons. This limitation is more for voice quality, the ability to guarantee bandwidth to branch connectivity, and for redundancy reasons; then for security-related reasons. It is possible to draw a third interface off of the inner barrier firewall (the outside interface on the firewalls was left unused in this document for this reason) to the Internet gateway edge to a separate WAN router and WAN connection if desired.
- Cisco IOS includes a firewall feature. At the NGWAN edge, a dedicated firewall appliance is used instead because it provides the highest scalability. Cisco recommends the use of the Cisco IOS Firewall feature set in some branch and teleworker deployments, because of a much lower number of users and connection rates than at an enterprise WAN edge headend location.
- Voice over IP (VoIP) and video are assumed to be requirements in the network. Detailed design considerations for handling VoIP and other latency-sensitive traffic is not explicitly addressed in this design guide, but may be found in Voice and Video Enabled IPsec VPN (V3PN), which is available at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf

- This design is targeted for deployment by enterprise-owned WAN edge. However, the concepts and conclusions are valid regardless of the ownership of the edge tunneling equipment, and are therefore valuable for service provider-managed WAN edges as well.

Design Components

The four architectures defined for Enterprise WAN and MAN networks provide an alternative solution to private WAN technologies such as Frame Relay and ATM-based networks. The design guides written around these architectures focused on support for network growth, availability, operational expenses, voice and video support, and level of complexity. Each of the architectures can be summarized into the seven basic components shown in Figure 2.

Figure 2 Enterprise WAN and MAN High-Level Architecture Basic Components



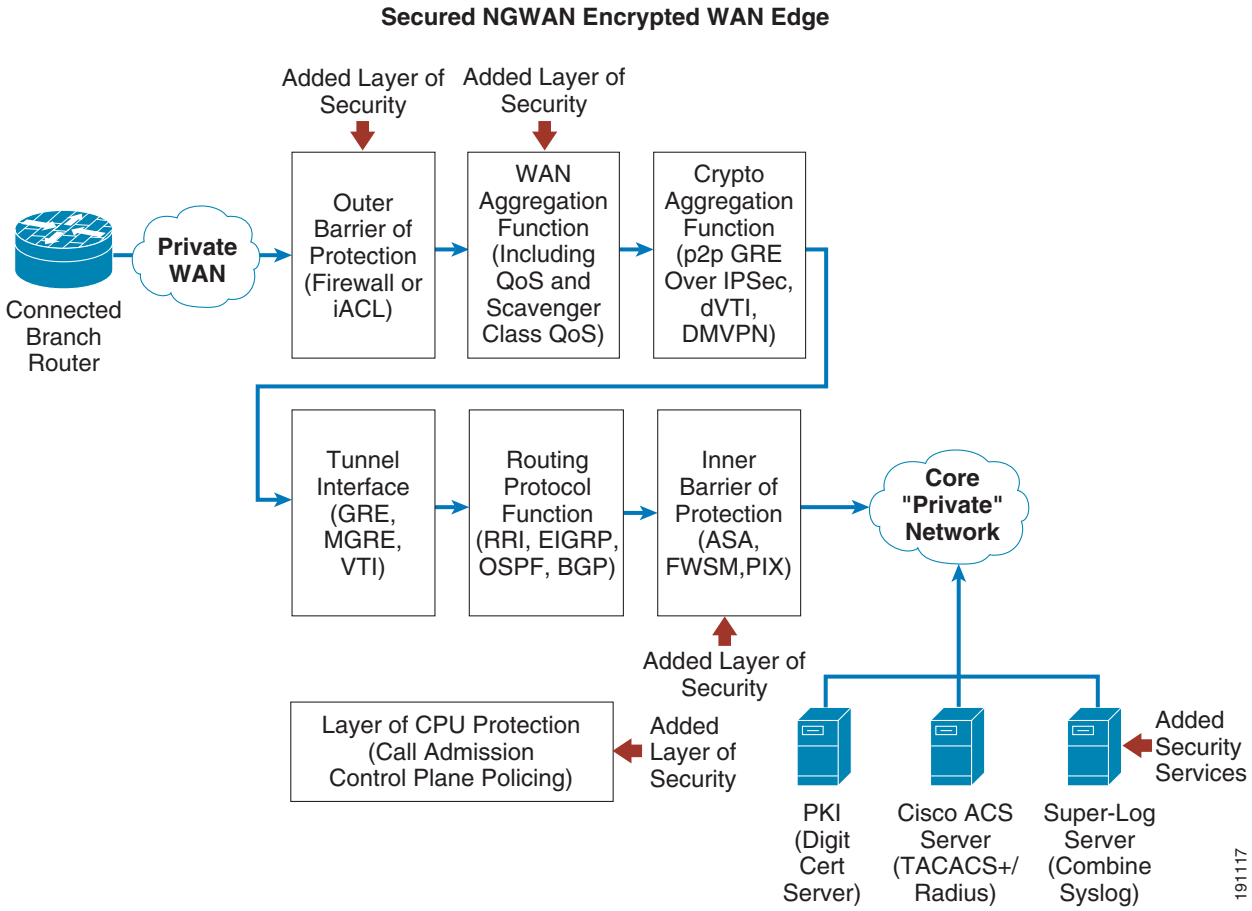
These components are the following:

- Connected branch router component—These are the devices that connect to the WAN edge for connectivity to the core “private” network.
- Private WAN cloud component—This is the WAN transport that connects the branch routers to the WAN edge network. IP-based WAN technologies are used in the enterprise WAN and MAN architectures.
- WAN aggregation functionality component—This functionality in an enterprise WAN edge network terminates all the connections from the branch routers through the private WAN.
- Crypto aggregation functionality component—If an IPsec-based encryption technology is used between the branch and WAN edge, this component encrypts and decrypts these connections. IPsec only, point-to-point generic route encapsulation (p2p GRE), dynamic multipoint VPN (DMVPN), and virtual tunnel interface (VTI) tunnels become encrypted or decrypted within this component
- Tunnel interface component—GRE, multipoint GRE (mGRE), or VTI interfaces are originated and terminated within this component.
- Routing protocol functionality component—This component provides the mechanisms to connect the branch routers to the core “private” network.
- Core “private” network component—This component can be referred to as the enterprise campus or data center. In essence, this component is where all enterprise servers and the application host reside.

These seven components are the basic components needed for all the enterprise WAN and MAN architectures. Not all four architectures use every one of the seven components, but an overview of all seven is shown for completeness. Also, the WAN aggregation, crypto aggregation, tunnel interface, and routing protocol functionality components can reside in a single chassis or multiple chassis, depending on the WAN and MAN architecture chosen.

In Figure 2, no mention is made of how to secure the actual devices within the WAN edge, how to block malicious traffic from entering the WAN edge, or how to guarantee the appropriate users or branch routers are allowed into the WAN edge network. This design guide focuses on providing guidance in these areas. The component overview of the enterprise WAN and MAN architectures are supplemented with additional components to secure the WAN edge. The concept of securing the NGWAN edge is to add additional layers of security and security functions to the existing encrypted VPN topology that may exist in a WAN edge. These security features add an inner and outer layer of access control as well as basic infrastructure protections of those systems. Figure 3 shows the location of these added components.

Figure 3 Securing the WAN Edge High-Level Architecture Additional Components



These added security components are the following:

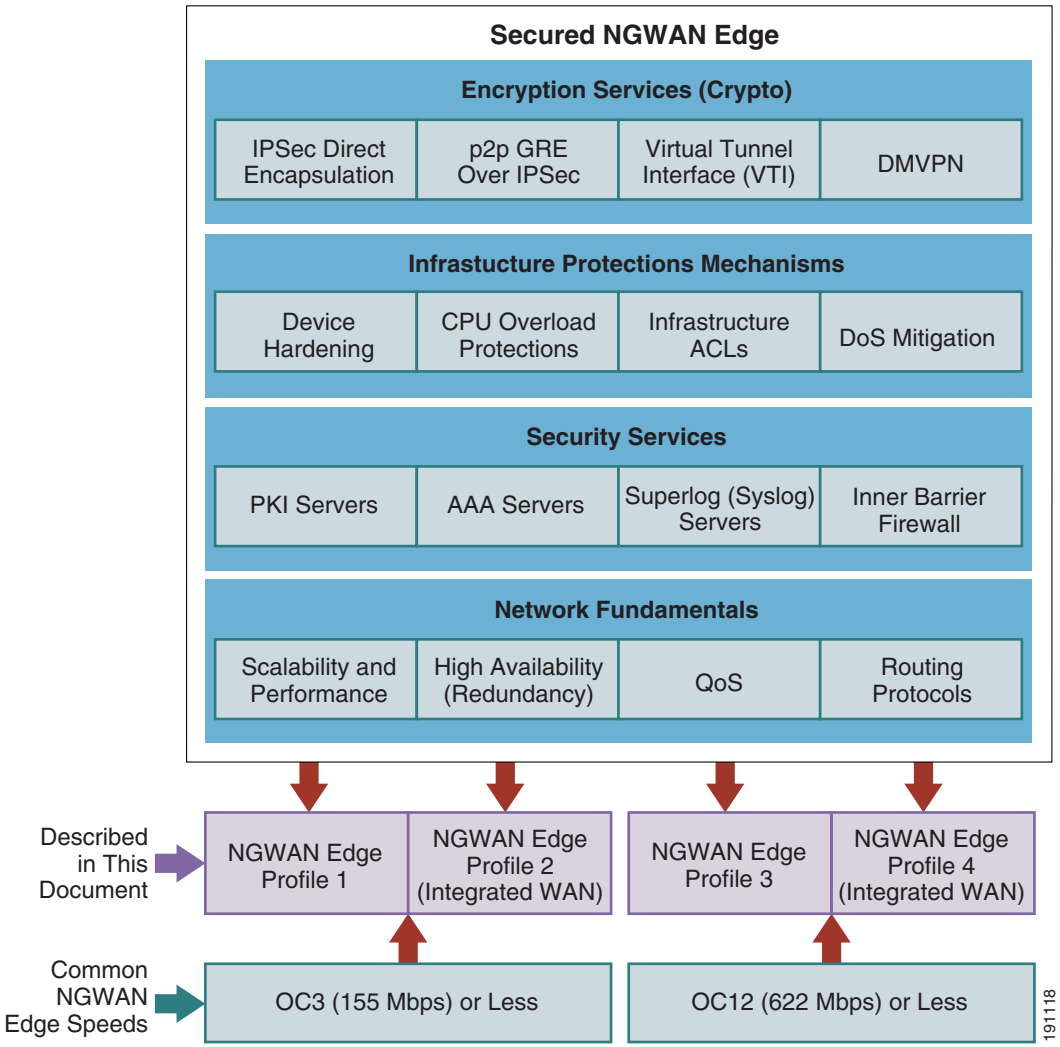
- Outer barrier of protection
- WAN aggregation functionality to include scavenger class QoS
- Inner barrier of protection
- Additional security-related servers (PKI, Cisco ACS, and super-log [syslog])
- Various layers of CPU protection

Each of these additional components is discussed in detail throughout this document. Figure 3 can be regarded as the high-level architecture overview to secure the enterprise WAN edge. This document takes this high-level architecture overview and creates a set of profiles for each of the two typical WAN speeds:

OC3 (155 Mbps) and OC12 (622 Mbps). Two profiles are created for OC3 and two for OC12 WAN speeds. This profile approach shows each of the above components in an integrated as well as separate device network architecture based on the current platform set available from Cisco for these two WAN speeds. Each profile contains the various layers of security available in the additional components shown in Figure 3.

The organization of this document is summarized in Figure 4.

Figure 4 Securing the WAN Edge Documentation Framework



In addition to the additional security components, network fundamentals such as scalability and performance, high availability, QoS, and routing protocols are discussed.

WAN Speed Profiles

There are two typical WAN speeds for a WAN Edge network: OC3 (155 Mbps) and OC12 (622 Mbps). The choice of these two network speeds determines the platform set from Cisco chosen. In addition, this design guide creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network regardless of which enterprise WAN and MAN architecture is

selected. The profiles for each WAN speed investigate integrated versus dedicated chassis for each functionality component as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the functions described in this document reside on a single or very few chassis. Other customers prefer the granularity and scalability of these same functions separated across multiple chassis. Both solutions have their advantages and disadvantages. From these profiles, guidance and configuration examples are given for securing the WAN edge mechanisms, as discussed in Figure 4. These mechanisms are encryption services (crypto), infrastructure protection services, security services, and network fundamentals.

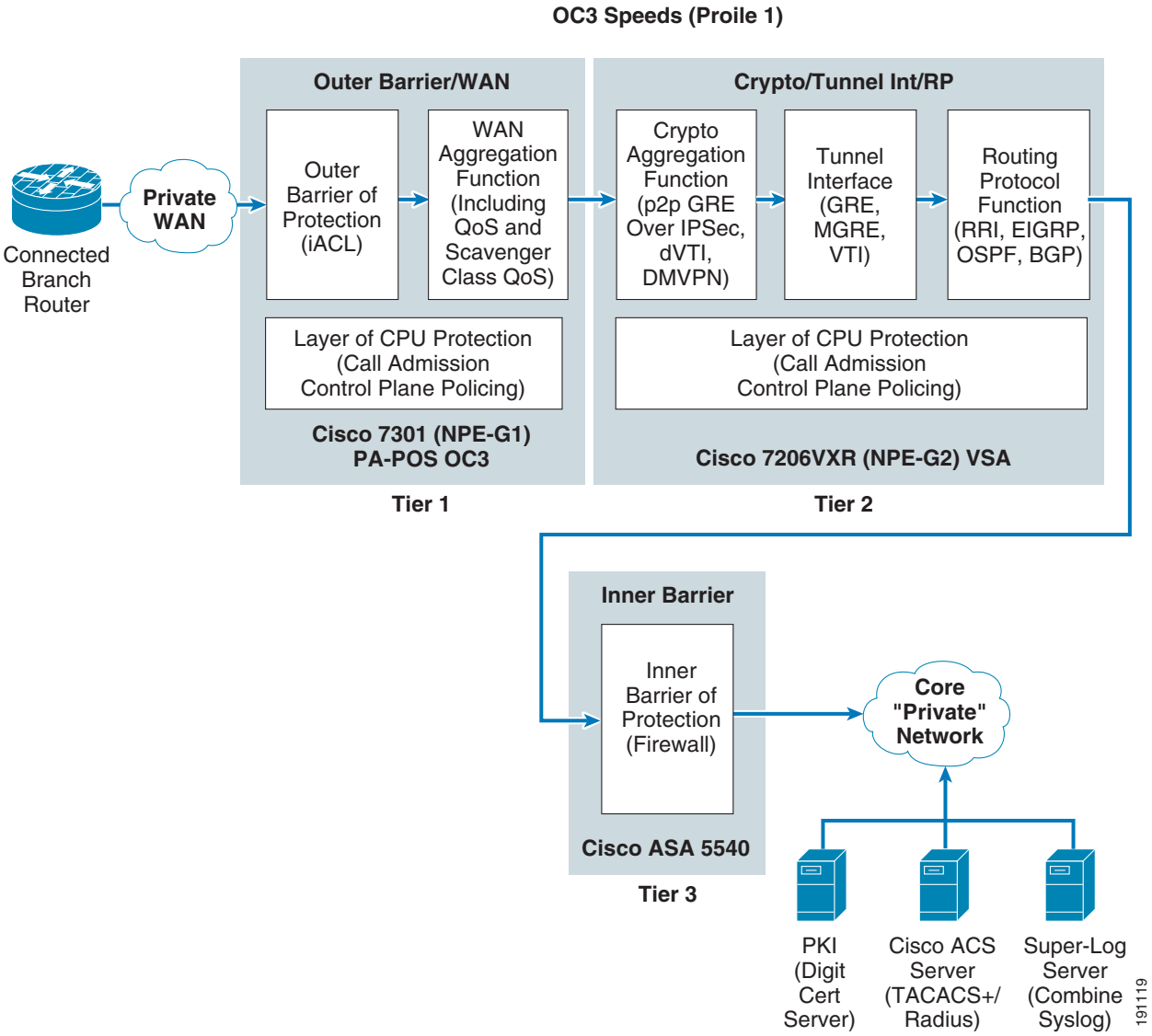
OC3 Profiles

Based on the high-level architecture for an enterprise WAN edge network, two profiles were chosen for a WAN edge requiring an OC3 connection from the private WAN cloud. The first profile shows a dedicated chassis solution and the second profile shows an integrated solution. The platforms chosen are also discussed in the following sections.

OC3 Profile 1—Three-Tier Solution

Figure 5 shows how the seven basic network components of high-level WAN edge architecture are organized to provide a dedicated chassis, separated by function solution.

Figure 5 Profile 1 OC3 Architecture (Three-Tier Solution)



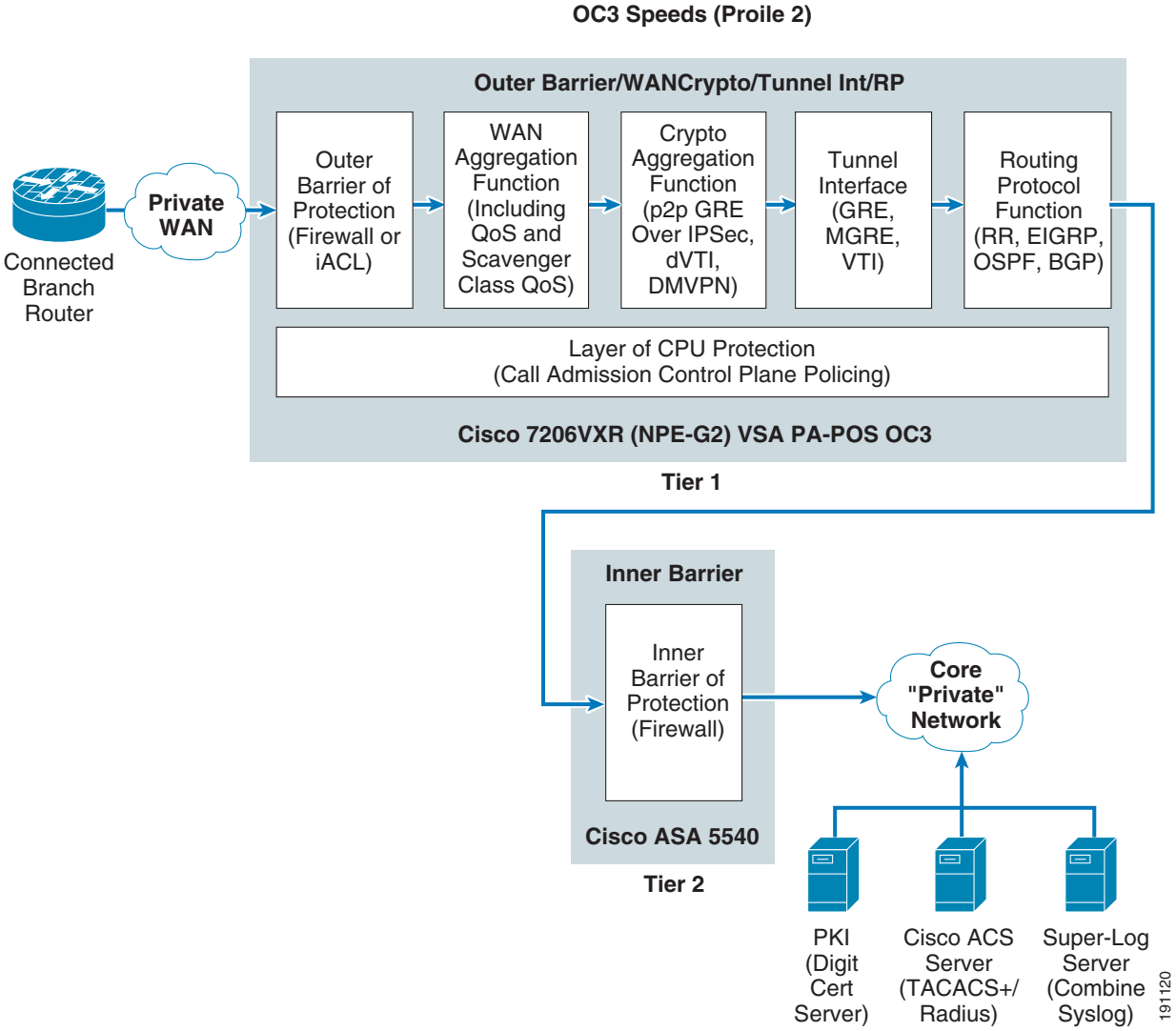
To meet the OC3 WAN speed requirement, the following Cisco platforms were chosen to fulfill each network component:

- Outer barrier/WAN component—A Cisco 7301 with a PA-POS OC3 was tested as the dedicated WAN router.
- Crypto/tunnel interface/routing protocol component—A Cisco 7200 VXR (NPE- G2) with a VSA Hardware Encryption Accelerator module was tested.
- Inner barrier component—A Cisco ASA 5540 was tested as the inner barrier firewall.

OC3 Profile 2—Two-Tier Solution

Figure 6 shows how the seven basic network components of high-level WAN edge architecture are organized to provide an integrated functionality solution.

Figure 6 Profile 2 OC3 Architecture (Two-Tier Solution)



To meet the OC3 WAN speed requirement, the following Cisco platforms were chosen to fulfill each network component:

- Outer barrier/WAN/crypto/tunnel interface/routing protocol component—a Cisco 7200 VXR (NPE-G2) with a VSA hardware accelerator module was tested as both the integrated WAN router with outer barrier and crypto aggregation.
- Inner barrier component—An ASA 5540 was tested as the inner barrier firewall.

Comparison of the OC3 Profiles

Table 1 shows the advantages and disadvantages of the two OC3 profiles created.

Table 1 Comparison of the OC3 Profiles—Advantages and Disadvantages

	Profile 1 (OC3)–3 Tier	Profile 2 (OC3)–2 Tier
Advantages	Each major function (WAN aggregation, crypto aggregation, and inner barrier firewall) are on dedicated systems. This approach is more scalable and gives more options for a multi-threaded redundancy plan. It also is easier to incrementally add systems to the architecture as users or traffic volume increases. Implementing WAN and crypto aggregation functions on separate routers provides each function with independent CPU resources. This adds flexibility and redundancy options. Each chassis can run a different code version. This can be very important where you need a different version of code to pick up a bug fix or to add features in the future, without impacting the other functions of the solution.	Fewer systems to purchase and maintain.
Disadvantages	More systems to purchase and maintain	Less scaling options, harder to incrementally grow the platform as traffic or users increase. The various features of both the crypto aggregation system and the WAN router (with QoS and the outer barrier) are all implemented on a single router. Should the CPU requirements reach peak levels for both crypto and WAN aggregation simultaneously, performance, and stability may be adversely affected. A combined crypto/WAN device is much harder to migrate to an IP multicast design, because packet fan-out affects CPU load, and input/output buffers are harder to selectively control.

Both profile 1 and 2 share a dedicated inner barrier firewall of a Cisco ASA 5540 (as an inner barrier firewall).

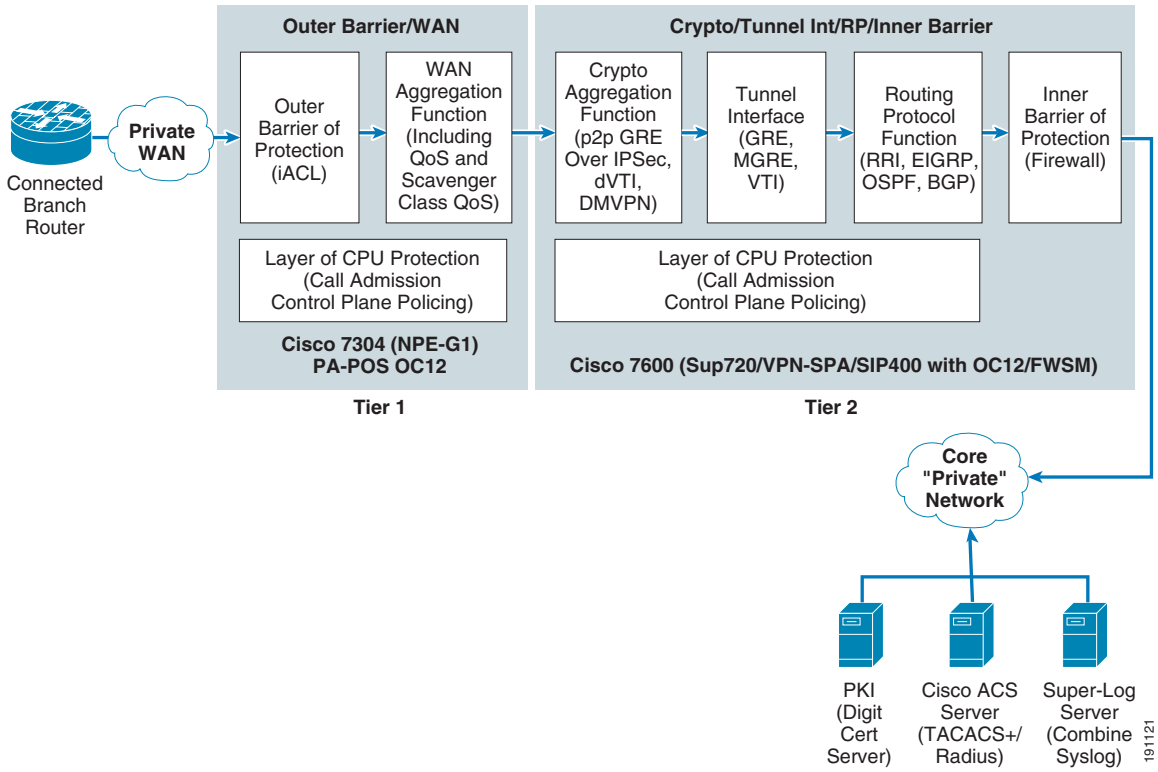
OC12 Profiles

Based on the high-level architecture for an enterprise WAN edge network, two profiles were chosen for a WAN edge requiring an OC12 connection from the private WAN cloud. The third profile shows a dedicated chassis solution and the fourth profile shows an integrated solution at OC12 speeds. The platforms chosen are also discussed in the following sections.

OC12 Profile 3—Two-Tier Solution

Figure 7 shows how the seven basic network components of high-level WAN edge architecture are organized to provide a dedicated chassis, two-tier solution.

Figure 7 Profile 3 OC12 Architecture (Two-Tier Solution)



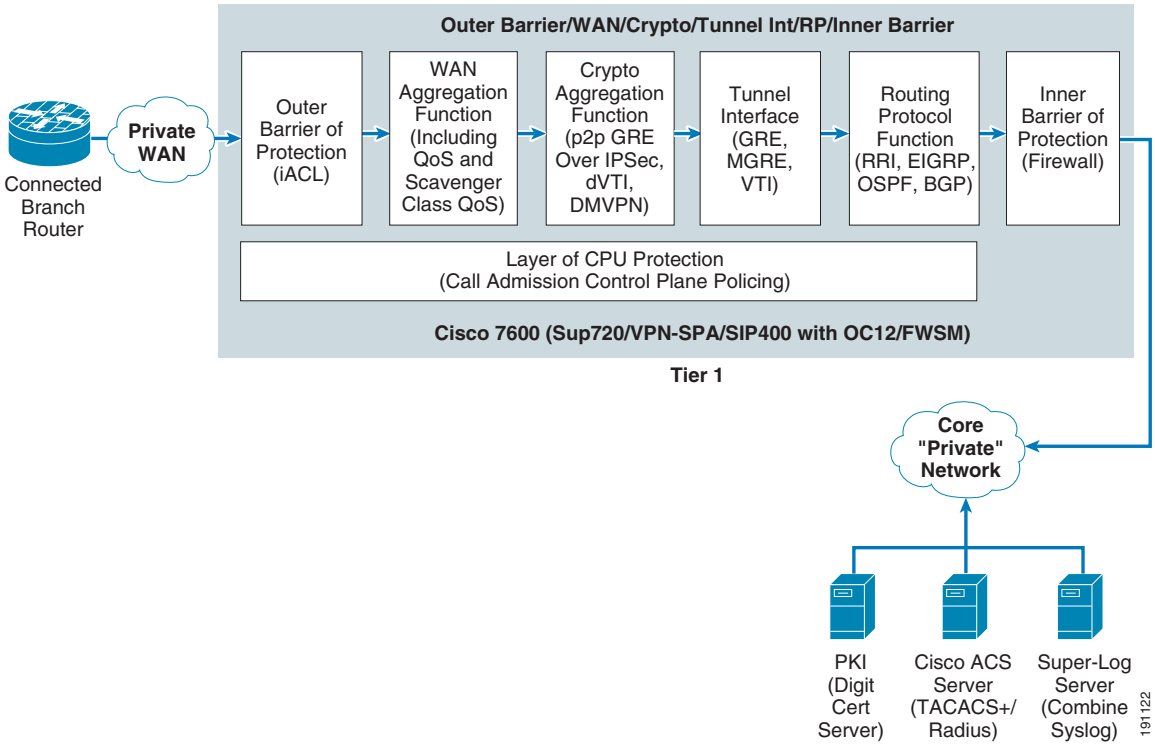
To meet the OC12 WAN speed requirement, the following Cisco platforms were chosen to fulfill each network component:

- Outer barrier /WAN component—A Cisco 7304 (NPE-G1 processor) with a SPA OC12 WAN card was tested as the dedicated WAN aggregation router with outer barrier functionality.
- Crypto/tunnel interface/routing protocol/inner barrier component—A Cisco 7600 (with a Sup-720/PFC3 processor) with a VPN-SPA hardware crypto accelerator module and an FWSM as the inner barrier firewall. The FWSM, although it occupies a physical slot in the 7600 chassis, has a dedicated CPU independent from the main MSFC in the 7600 chassis.

OC12 Profile 4—Integrated Functionality Solution (One-Tier Solution)

Figure 8 shows how the seven basic network components of high-level WAN edge architecture are organized to provide an integrated functionality solution.

Figure 8 Profile 4 OC12 Architecture (One-Tier Solution)



To meet the OC12 WAN speed requirement, the following Cisco platforms were chosen to fulfill each network component:

- Outer barrier/WAN/crypto/tunnel interface/routing protocol/inner barrier component—A Cisco 7600 (with a SUP-720/PFC3 processor), a SIP-400 with a SPA OC-12 module to provide WAN termination, and a VPN-SPA Hardware Crypto Accelerator Module, an FWSM as the inner barrier firewall. This profile implements all functions in one physical chassis. The Cisco FWSM, although it occupies a physical slot in the 7600 chassis, has a dedicated CPU independent from the main MSFC in the 7600 chassis. Note that this architecture brings the functionality of the WAN router into the Cisco 7600 platform (including the outer barrier and QoS functions).

Comparison of the OC12 Profiles

Table 2 shows the advantages and disadvantages of the two OC12 profiles created.

Table 2 Comparison of the OC12 Profiles—Advantages and Disadvantages

	Profile 3 (OC12)—2 Tier	Profile 4 (OC12)—1 Tier (Fully Integrated)
Advantages	A dedicated WAN aggregation router adds more flexibility and allows more redundancy options. The CPU of the WAN router runs the outer barrier (iACL and its logging, as well as QoS for the WAN circuit) offloading it from the crypto aggregation system. It is easier to add more WAN capability as users and traffic increases. Each chassis can run a different code version. This can be very important when you need a different version of code to pick up a bug fix or to add features in the future, without impacting the other functions of the solution.	Fewer systems to support and maintain. Simplified management. Both FWSM and VPN-SPA modules are the highest throughput of all Cisco product lines. Fewer redundancy options if WAN, crypto, and inner barrier firewall all reside on same chassis, so if the whole chassis fails, all are failed.
Disadvantages	More systems to purchase and maintain.	More features on central MSFC CPU—This may have unforeseen performance and scalability ramifications. It is harder and more expensive to incrementally add systems to the architecture as users or traffic, while you can add cards (VPN-SPAs or WAN interfaces) the gating factor can still be the central MSFC processor A combined crypto/WAN device is much harder to migrate to an IP multicast design, because packet fan-out affects CPU load, and input/output buffers are harder to selectively control.

Both profile 3 and 4 share a FWSM, as the inner barrier firewall. Although integrated in the 7600 chassis, the FWSM has its own independent CPU and network processors.

Securing the NG WAN Edge

The key security components of this architecture are organized in this document into three categories: infrastructure protection services, security services, and encryption services (crypto).

Encryption Services

The crypto aggregation component provides its functionality within the WAN edge. The crypto aggregation component creates a secure and encrypted communication channel between the branch sites and the core private network, as well as from "branch-to-hub-to-other branch" connections. The encryption services involve the four IPsec-based WAN architectures and are discussed in great detail in the design guides located at the following URL: http://www.cisco.com/go/wanandman:

- IPsec Direct Encapsulation VPN Design Guide
- Point-to-Point GRE over IPsec Design Guide
- Dynamic Multipoint VPN (DMVPN) Design Guide
- Virtual Tunnel Interface (VTI) Design Guide

Design and Implementation, page 24 discusses these four VPN topologies as they apply to the WAN speed profiles created. Infrastructure protection services and security services are discussed in the next two sections.

Infrastructure Protection Services

Infrastructure protection services provide proactive measures to protect devices, in this case Cisco IOS software-based routers, switches, and appliances, from direct and indirect attacks. Infrastructure protection services assist in maintaining network transport continuity and availability. Regardless of which enterprise WAN and MAN architecture or WAN edge speed profile chosen, infrastructure protection services apply to all the network components in the WAN edge. To protect these devices, the following methods are used:

- Device hardening—A myriad of device hardening options exist in Cisco products. This feature set is recommended as a starting point to achieve a minimal security baseline. For links to both the Cisco IOS essentials (now a Cisco Press book) and the NSA documents that can be used for further information on device hardening, see the following URL: http://www.thewaystation.com/techref/choke.shtml

  This document uses built-in facilities such as the following:

  - A well-created banner page (motd) to state that the access is restricted to only authorized personnel.
  - Authentication, authorization, accounting (AAA) with TACACS+ for device account administration, command authorization, and CLI command accounting.
  - Using SSH versus Telnet for remote administration of the device; this provides encryption to the shell session to prevent snooping of the commands or passwords of administrators.
  - Access control of SNMP, SSH, and other protocols used to monitor the devices.
  - Disabling of known potentially hazardous services and interface features (that is, directed broadcast, IP redirect, IP proxy-ARP, CDP, and so on) and any global daemons/services (that is, small services, HTTP, and so on) not specifically required in the architecture.
  - Neighbor authentication and hashed communication for dynamic routing protocols.
- CPU overload protections—Protecting router CPU utilization is crucial to guaranteeing service delivery of traffic. Ensuring that the router CPU is available for routing updates and voice calls provides a level of infrastructure protection. As described in this document, the following two features are used to help protect the NGWAN edge gear from CPU over utilization.
  - Control Plane Policing (CoPP)—A QoS policy using traffic policers that identifies and limits the amount of traffic that is destined to the CPU of this chassis and rate limits by class of traffic. This helps limit the impact to the CPU or bandwidth utilization of the targeted system by a DoS attack.
  - Call Admission Control (CAC)—A process that monitors CPU and memory utilization on the router and limits new connections to this chassis if the CPU is above a configured threshold.
- Infrastructure ACLs—These ACLs are required to keep out unwanted traffic from the physical links from the private WAN cloud.
  - Outer barrier [infrastructure ACLs (iACLs)]—This functionality is used as the outer barrier of protection that creates the front line of defense from attacks, starting from the service provider or SP-connected network, but allows the encrypted traffic (cipher text) packets to pass through to reach the crypto peer on the crypto aggregation system. Firewalls may also be used to achieve this functionality.

- DoS mitigation—This functionality encompasses the mechanisms to detect, mitigate, and protect devices against violations and unauthorized events.
  - Unicast Reverse Path Forwarding (uRPF)—This feature is used for preventing source address spoofing. It is a "looking backward" ability that allows the router to check whether the IP packet received at a router interface arrived on the best return path (return route) to the source address of the packet.
  - Scavenger class QoS—A protection mechanism whereby traffic arriving at a rate higher than the normal rate for the application is considered to be a potential threat and marked with a DSCP value of CS1. Typically, this marking is done by a branch or campus switch. A QoS policy can create a scavenger class for the CS1 traffic, allocating bandwidth even less than best effort for it. This prevents traffic anomalies that can impair network performance.

More detailed descriptions and configurations of all these infrastructure protection mechanisms are provided in Infrastructure Protection Mechanisms, page 27.

Security Services

Security services provide the added functionality within the WAN edge network to control that the appropriate users can access the network device, the appropriate certificates are given, and that a protected and archived audit trail of security events exists. The following security services methods were used:

- PKI Digital Certificate Server (CA server)—Used for IKE authentication for crypto IPsec tunnels.
- AAA server—Used to control AAA functions on network devices and to provide a repository for account information, authorization command set, and accounting for login and commands issued on network devices.
- Super-logging (remote syslogging)—Used as a remote master syslog service, so that all devices in the WAN edge create log entries in a local buffer and to the "super-log server", which is a dedicated syslog server in the protected network core.
- Inner barrier (firewall)—Used as the inner barrier of protection, it provides an inspection engine and "rule set" that can view the clear text (unencrypted) communication from the branch to the enterprise core and controls that access with its rule-based firewall. This may also do advanced firewalling features such as user authentication, web URL filtering, and so on.

A more detailed description and configuration of all the previous listed security services are shown in Security Service Integration, page 51.

Network Fundamentals

Network fundamentals refer to the basic services that are required for network connectivity. These services include high availability, IP routing, and QoS. Unique to the WAN edge is the scalability and performance network fundamental. Given that the WAN edge aggregates numerous branch sites and forwards that traffic to the core "private" network, selecting a platform that can meet the branch aggregation requirements and still be able to forward traffic is fundamental to a WAN edge network. Network Fundamentals, page 72 discusses this network fundamental in greater detail.

High Availability

Implementing designs that incorporate high availability require the solution administrator to identify the components that may likely fail, to provide redundancy during the failure, and then to simulate a failure and recovery to test the plan. This section shows the high-level architecture of a single site,

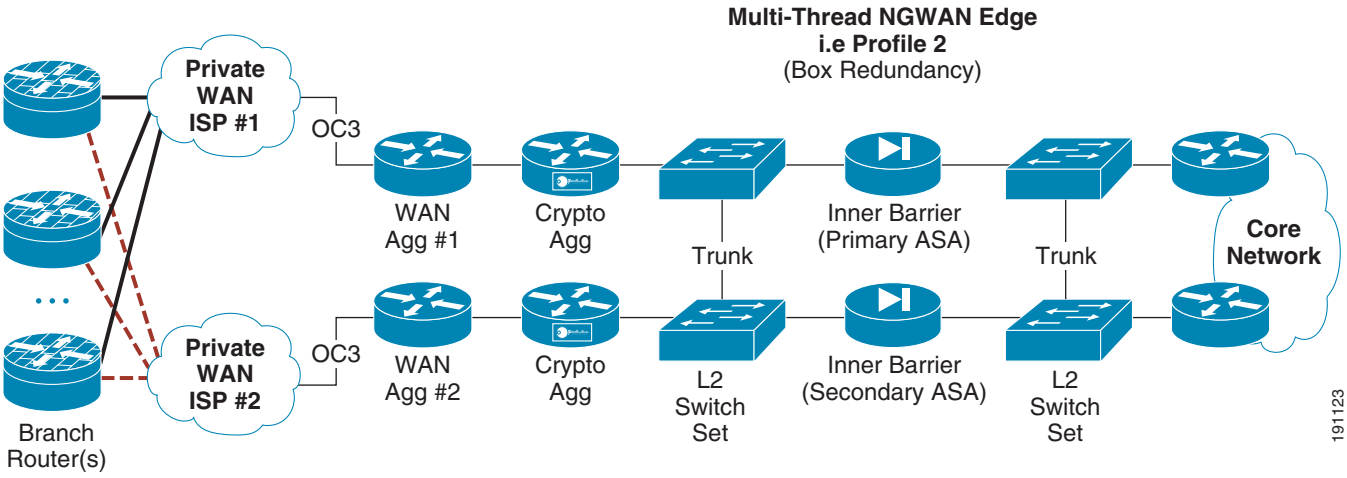
multi-threaded architecture (box-level redundancy), and discusses the architecture of a multi-site redundant architecture (geographical site redundancy). See High Availability (Redundancy), page 68 for detailed network designs and implementation information.

Redundant Multi-Threaded in a Single-Site Location

The core concept in this redundancy model is to supply device and circuit redundancy at each major function of the topology within a single site. The number of chasses chosen to implement the solution has a major impact on how much redundancy is possible.

Figure 9 shows an example of this multi-threaded system in a single-site location.

Figure 9 Multi-Threaded System in a Single Location (Profile 1)



There are trunk links between the core and the inner firewall, and also between the inner firewall and the crypto aggregation devices. This allows cross failover of one set of functions (that is, WAN and crypto or inner firewall) without failover of the whole thread.

Table 3 lists the advantages and disadvantages of a multi-threaded single-site deployment.

Table 3 Multi-Threaded Single-Site Deployment—Advantages and Disadvantages

	Effect of Number of Chasses in WAN Edge on Intra-Site Redundancy	
Various Chassis Deployment Profiles	**Pro**	**Con**
Profile 1 OC3—Separated WAN routers (with independent WAN circuits), separated crypto aggregation (crypto agg) routers, separated inner barrier firewalls, L2 switch set(s).	Each subsystem (WAN and crypto agg, or inner firewall) can failover independently of each other. This gives a very redundant and easily expandable topology. Each major component can use a different failover mechanism (that is, crypto agg may use the RP at a failover detection mechanism while the inner firewall may be a stateful firewall set)	Because each of the major functions is separated physically, an L2 switching layer is required between each set of devices.

Table 3 Multi-Threaded Single-Site Deployment—Advantages and Disadvantages (continued)

Profile 2 OC3—Integrated WAN interfaces (with independent WAN circuits) and crypto agg routers, separated inner barrier firewalls, L2 switch set(s).		Because the WAN interface and the crypto agg functions are integrated in the Cisco 7200VXR chassis, if a WAN interface or circuit fails, all traffic to that system needs to be failed over to its backup system.
Profile 3 OC12—Separated WAN routers (with independent WAN circuits), integrated crypto agg and FWSM inner barrier firewall	No additional L2 switching layer is required because the Cisco 7600s have switching capabilities themselves. If a WAN failover occurs for a device or circuit loss, the corresponding crypto agg function is also down, but the inner barrier firewall on that chassis is unaffected.	The firewall is integrated in the 7600 chassis (on FWSM). If a whole 7600 chassis is lost, inner firewall failover occurs.
Profile 4 OC12—Integrated WAN interfaces (with independent WAN circuits), crypto agg, and FWSM inner barrier firewall	No additional L2 switching layer is required because the Cisco 7600s have switching capabilities themselves.	Because the WAN interface and the crypto aggregation functions are integrated in the Cisco 7600 chassis, if a WAN interface or circuit fails, all traffic to that system needs to be failed over to its backup system. Also, because the firewall is integrated in the chassis (on the FWSM), if a chassis failure of a 7600 chassis occurs, inner firewall failover occurs.

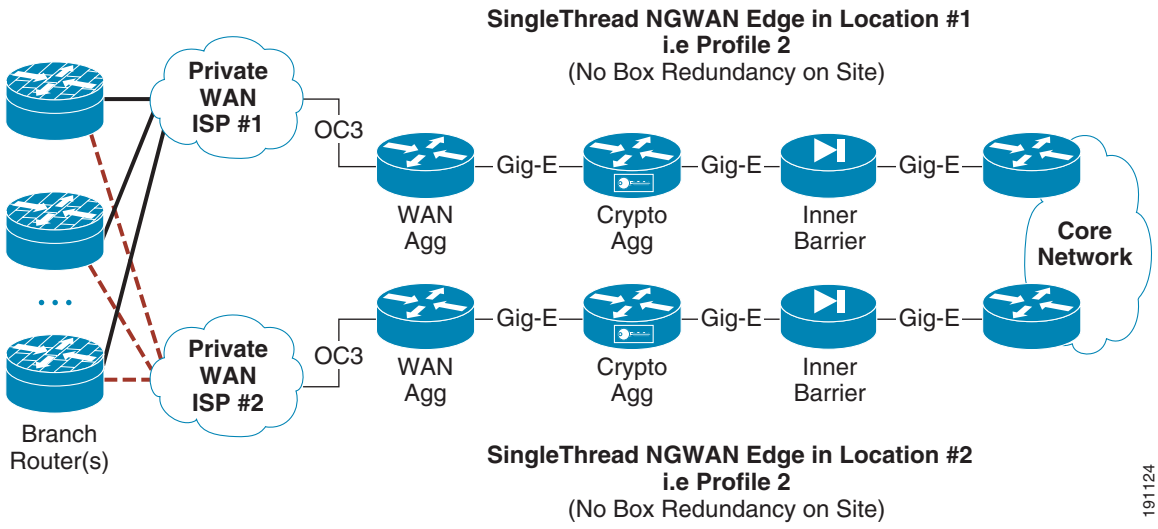
If L2 switches are required for redundancy, they may be implemented as unique sets of switches at each spot in the NGWAN edge topology. Alternatively, the L2 switches may simply be different VLANs off the same two shared switches. This choice depends on the company requirements for keeping various levels of traffic separated or not on a L2 device. Opinions on this practice vary among security professionals. If you are concerned that the L2 switches could be compromised giving access into a more protected location in the network topology, multiple independent sets of switches are recommended. See Redundant Multi-Threaded in a Single Site Location, page 68 for details on topology and implementation.

Multiple Single-Threaded Site Locations of NGWAN Edge

A single threaded solution has one path through the set of systems (a thread). By creating two or more site locations for each single thread, geographical redundancy is achieved. This NGWAN edge topology provides very good redundancy while still maintaining cost efficiency.

The example shown in Figure 10 does not provide for redundancy within a location but provides redundancy across two or more locations.

Figure 10 Multiple Single-Threaded Site Locations Redundancy (Profile 1)



In a multiple single-threaded site locations NGWAN edge redundancy model, some basic considerations need to be designed into the network for the redundancy to operate correctly. See Multiple Single-Threaded Site Locations of NGWAN Edge, page 70 for details on topology and implementation.

Quality of Service

QoS (with the exception of scavenger class QoS) is implemented to achieve some guarantees on certain application performance across the network, such as VoIP traffic. For implementation details, see QoS for WAN Aggregation Routers, page 72.

Routing Protocols

Routing protocols (and possibly the redistribution of them) are extremely important to redundancy and the time to detect and respond to a failure event. This is described in detail in Routing Protocol Implementation, page 74.

For implementation details of these items, also see Network Fundamentals, page 72.

Best Practices and Known Limitations

The following sections contain a summary of the best practices and limitations for the design. More detailed information is provided in Design and Implementation, page 24.

Best Practices Summary

The following lists at a high-level the best practices recommendations for infrastructure protection and security service integration on the WAN edge systems:

- Use a super-log server (remote syslog) as a dedicated server in the protected internal network as the double log point of all NGWAN edge devices. This provides a good system for record keeping of security/system level events.

- Use a PKI server (digital certificate server) located on the protected internal network to issue digital certificates to the crypto peers, which use the certificates for IKE authentication of the ISAKMP tunnels (VPN topology).
- Use an AAA server (that is, Cisco Secure ACS server) as a AAA repository on the protected internal network for AAA functional on all NGWAN edge devices.
- Use the "qos pre-classify" feature in Cisco IOS on any Cisco router that has crypto and QoS on the same chassis (not available on Cisco 7600).
- Always use the "enable secret" instead of the "enable password" option in all Cisco IOS routers.

Known Limitations Summary

The following summarizes the known limitations for infrastructure protection and security service integration on the WAN edge systems:

- "Branch-to-hub-to-branch" encrypted traffic (even in a hub-and-spoke topology) goes to the crypto aggregation system but not to the inner barrier firewall; it therefore cannot be inspected via that inner barrier (firewall) in this network architecture.
- uRPF restrictions on Sup720/PFC3 on 7600; when configuring Unicast RPF check, follow these guidelines and restrictions:
  - If you configure uRPF check to filter with an ACL, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the MSFC for the uRPF check. Packets permitted by the ACL are forwarded in hardware without a uRPF check (CSCdz35099).
  - Because the packets in a DoS attack typically match the deny ACL and are sent to the MSFC for the uRPF check, they can overload the MSFC.
  - The PFC provides hardware support for traffic that does not match the uRPF check ACL, but that does match an input security ACL.
  - The PFC does not provide hardware support uRPF check for policy-based routing (PBR) traffic. (CSCea53554).
- The uRPF feature was not available in the Cisco 7301 or Cisco 7304 images tested and was not enabled on those platforms.
- If using Cisco 7600 systems for crypto aggregation, the dynamic or static virtual tunnel interface (dVTI or VTI) crypto topology is not supported as of the tested image (12.2-18.SXF2) image. This feature should be available in 2008.
- If using a Cisco 7600 system for crypto aggregation and integrated WAN (with QoS), the "qos pre-classify" feature is not available on that platform at this time. WAN interface QoS policy maps must operate by DSCP/BHP markings only.
- If using a Cisco 7200VXR, Cisco 7301, or Cisco 7304 routers for the outer barrier, there is no equivalent to the Cisco 7600 series feature for Optimized Access List (OAL), so rate limiting the syslog output is critical.

Additional detailed information on these recommendations is discussed in the sections that follow.

Design and Implementation

Which security products and features to include in the “securing” of the NGWAN edge, where those services should reside, and how to properly configure them, is the primary focus of this section.

Each function in this design may have network traffic that is used for itself (control plane) or for a higher level traffic. It is important to understand how the components of this architecture communicate with their counterparts at the branch location, and where each component of the NGWAN edge is meant to terminate.

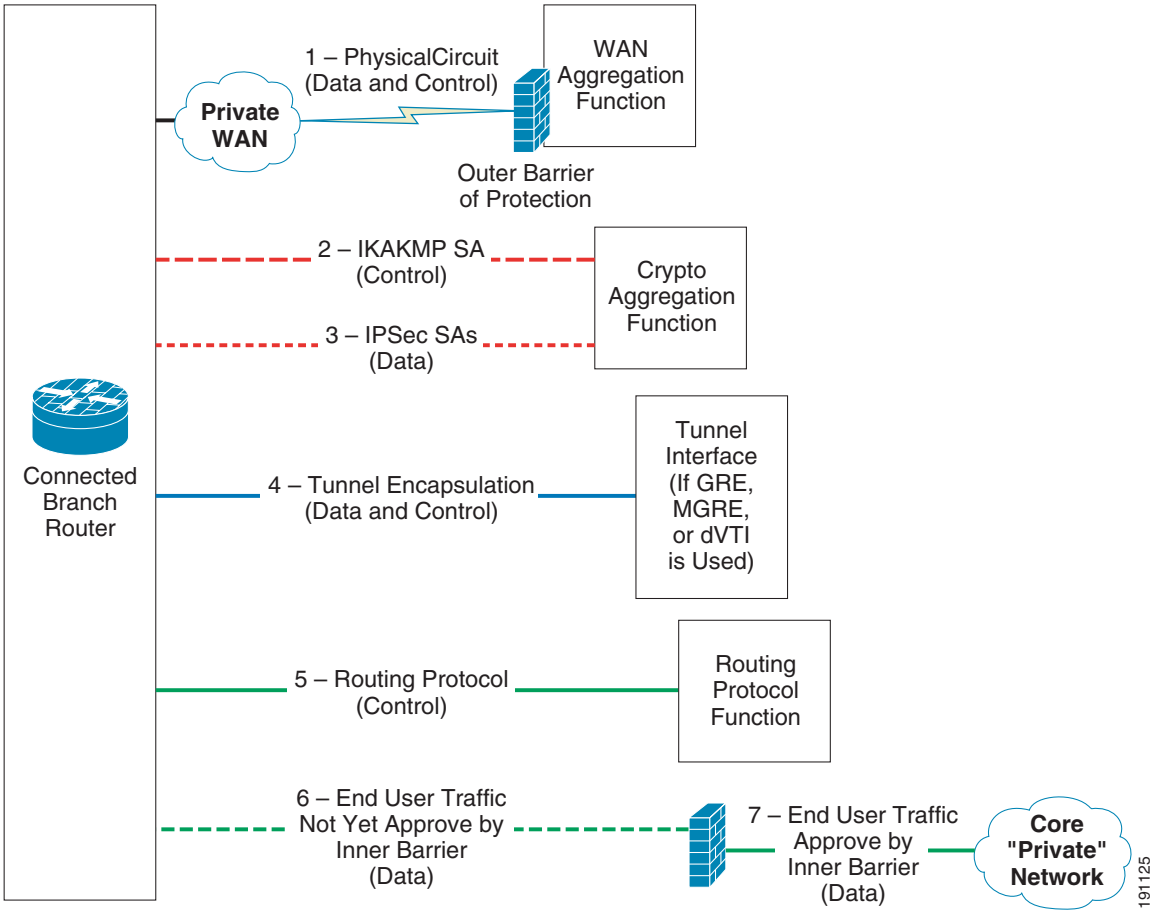
The following describes the concept of different classes of traffic and the devices on which they terminate:

- WAN (access layer)—Terminates at WAN aggregation device
- Crypto (ISAKMP) control traffic—Terminates at crypto aggregation device
- Crypto (IPsec) data traffic—Terminates at Crypto aggregation device.
- Tunnel interface—Terminates at the main processor (or subordinate card) in the crypto aggregation device.
- Routing protocol control traffic—Terminates at crypto aggregation device
- Clear text (unencrypted) end user data has two general classes:
  - End user traffic transiting the encrypted network but not yet approved through the rule set of the inner barrier (firewall)
  - End user traffic transiting the encrypted network that is approved through the rule set of the inner barrier (firewall)

In a multi-function system such as the NGWAN edge, several types of traffic go through the system at any given time. The vast majority of the packets per second (pps) and bits per second (bps) of the traffic transiting the NGWAN edge is end-user data. A smaller proportion of the traffic is considered control plane traffic. An example of control plane traffic is the routing protocol used inside the IPsec VPN tunnel (VPN IGP) to the branches. The solution administrator may choose to use any IGP (that is, EIGRP or OSPF) as the routing protocol. This traffic is critical to the stability of the network but is not generated by the end users. It is generated and terminated by the network gear itself. Other examples of control plane traffic are ISAKMP connections for IPsec, and even the solution administrator of the system connecting to them for remote administration or device monitoring.

Figure 11 shows a comparison of control plane and data plane traffic in the NGWAN edge architecture.

Figure 11 Control Plane versus Data Plane Traffic in NGWAN Edge Architectures



Each type of connection is described in more detail as follows:

1. Private WAN circuit to service provider network “private WAN”. (Only approved traffic such as encrypted traffic is permitted in through the outer barrier). This is a physical circuit and carries both control and data plane traffic. The outer barrier (in this case, an iACL) helps protect this circuit and crypto peer reachable in #2 and #3 below from DoS or intrusions.
2. The ISAKMP tunnel between the crypto aggregation device and the encrypting branch router is a control plane used for IKE authentication, transform set negotiation, and for session key transport of the IPsec SAs.
3. IPsec tunnel (set of IPsec SAs) between the crypto aggregation device and encrypting branch router carries end-user payload and is part of the data plane. (The IPsec SAs may also carry higher level control plane traffic in the data plane of the IPsec tunnel).
4. Tunnel interface encapsulation carries both control and data plane packet inside the tunnel. The control plane traffic may be routing hellos or GRE keepalives, and the data plane is end-user data or other higher layers control plane traffic (see #5 below).
5. The routing protocol communication is between routing peers and is strictly control plane traffic. The VPN IGP travels inside the encapsulating tunnel in #4.
   a. An RP (such as EIGRP or OSPF) is used as the VPN IGP

   b. An RP (such as OSFP or RIP) is used as the RP between the inner barrier (firewall and the crypto agg system) and also between the inner barrier and the enterprise core routers.

6. End-user traffic goes through the encapsulating tunnel in #4 gets decapsulated, and then carries to the inner barrier firewall (it has not been approved yet to pass through that firewall). This traffic is data plane traffic but not yet approved to access the core network.
7. End-user traffic goes through the encapsulating tunnel in #4 gets decapsulated, and then carries to the inner barrier firewall and has been approved in the inner barrier firewall rules to be permitted into the core network.

Design Considerations

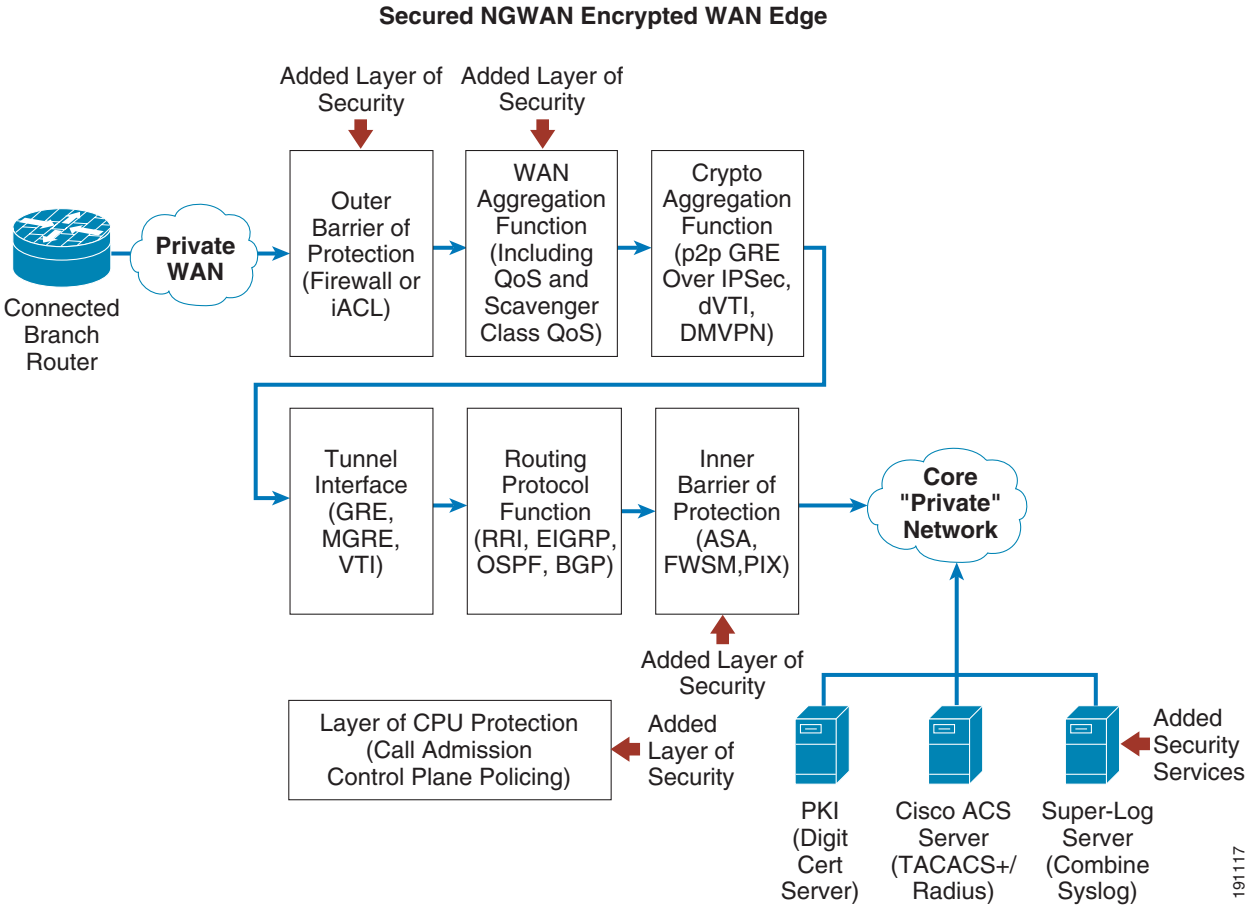
This section gives provides configuration summaries and more detail descriptions of the various security and other mechanisms being enabled on the NGWAN edge gear. The goal of this section is to expand on the concepts in Design Overview, page 6 and provide the detail needed for the solution administrator to understand and implement each feature. This section is not a technical “deep dive” into each subject described but rather how to integrate all the various features into a comprehensive “security in layers” solution and show the difference in devices and configuration.

Most of the configuration examples in this section are based off of an “integrated WAN router” model as represented in profile 2 (OC3) or profile 4 (OC12). Full configurations for all profiles are shown in Test Bed Configuration Files, page 80.

Security Concepts—Implementation and Configuration

The key components of this infrastructure protection and security service integration are indicated by red arrows, as shown in Figure 12.

Figure 12 Implementing Security Services and Infrastructure Protections



Infrastructure Protection Mechanisms

The goals of infrastructure protection are to lessen the likelihood or amount of damage done to critical systems by a deliberate or collateral intrusion attempt or DoS-type attack on that respective system, and to prevent unauthorized access to private data or service theft of the NGWAN edge systems. The NGWAN edges are located in a campus or data center of the enterprise. The NGWAN edge solution aggregates hundreds or thousands of branch devices giving connectivity to the enterprise core network; as such, it becomes a likely target of interest to an attacker.

Device Hardening

Hardening the access options of the NGWAN edge devices and removing potentially dangerous features and services is a requirement to the securing of the NGWAN edge. A basic common sense approach to device hardening is shown in the following section.

Create a Banner

For links to both the Cisco IOS essentials (now a Cisco Press book) and the NSA document, see the following URL: http://www.thewaystation.com/techref/choke.shtml. The banner is more for establishing legal ownership and the ability to prosecute an intruder. It is similar to a “no trespassing” sign in the physical world.

Create a banner for any shell connection attempts, so that the system is clearly marked as private. Cisco recommends that you consult your legal department or group for the exact language required by your company or organization in such a banner. It is recommended not to divulge any unnecessary information in the banner (that is, device name or network administration information).

Commands for creating a banner (motd):

- Cisco IOS router

```
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
! *Note the ^C should be a character not used
! in the banner itself when entered, once
! enter the router will convert it to a ^C in
! the configuration - this is normal.
```

- Cisco ASA/FWSM

```
!
banner motd Warning this is a private system
banner motd Unauthorized access is prohibited.
banner motd Violators will be prosecuted.
banner motd .
!
! *Note each line of the banner can have it's own command
! in the config there is no "end of block" type character
! like in IOS.
```

Use AAA on all Devices

AAA with TACACS+ can provide an easy-to-manage source for device account administration, authorization command sets, and a repository for accounting information. These AAA commands are used in conjunction with a Cisco Secure Access Control Server (ACS) or other TACACS+ server. The following are benefits of using AAA commands with an ACS server:

- Authentication (who you are)—Account UserID and password are stored in ACS (for easy management and grouping abilities)
- Authorization (what you are allowed to do)—A downloadable authorization command set are served from ACS to the devices after a successful login (allows simplified control and easy grouping of administrative commands for devices).
- Accounting (record of what you did, on which device, and when it occurred)—The ACS server accounting screens have a command-by-command record of all commands issue on each device, which include device IP, timestamp, and exact command issued.
- Failed attempts at authentication to the devices are kept as a record in the ACS server; the ACS server may institute a "number of attempts" lockout policy if desired.
- All communications from the device (NAS) to the AAA server (via TACACS+) uses a hash algorithm so it is not sent in clear text. This can be considered TACACS+ authentication, and in Cisco Secure ACS (the AAA server), you can limit the IP source of the network access servers (NAS). In this case, those are the network devices themselves.
- If you have multiple solution administrators of this NGWAN edge solution, the accounting feature can be a very good tool to keep a record of which solution administrator did what, when, and where, and can be extremely helpful in troubleshooting outages.

Commands for Authentication, Authorization, Accounting (CLI AAA via TACACS+)

In this example, the AAA server (Cisco Secure ACS) is at 10.59.138.11 and uses a secret key between the device (NAS) and the AAA server.

- Cisco IOS router

```
!
! Enable service password-encryption:
service password-encryption
!
! Create a local database login
! for backup if ACS is down:
username cisco123 privilege 15 password 7 104D000A061843595F
! Enable aaa new-model mode for AAA
aaa new-model
!
! Configuring location of the TACACS+ Server and parameters:
tacacs-server host 10.59.138.11 key 7 070C285F4D06
!
tacacs-server timeout 10
tacacs-server directed-request
!
! AAA Authentication commands: (request authentication via
! tacacs+ for both login and for enable level:
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
! AAA authorization (with command set send down from tacacs+):
aaa accounting exec default start-stop group tacacs+
!
! AAA accounting to TACACS+ for start-stop records (for
! session time and also any commands entered in privilege
! level 0, 1, and 15 :
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa session-id common
!
! *Note – In the aaa accounting commands you need to create on
! for each privilege level you wish to go to accounting.
! This behavior configures differently then in ASA/FWSM code.
```

- Cisco ASA/FWSM

```
!
! Create a local database login
! for backup if ACS is down:
username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
! Configuring location of the TACACS+ Server and parameters:
aaa-server tacacs-group protocol tacacs+
aaa-server tacacs-group host 10.59.138.11
 key cisco
aaa-server TACACS+ protocol tacacs+
!
! AAA Authentication commands: (request authentication via
! tacacs+ for both login and for enable level:
aaa authentication enable console tacacs-group LOCAL
aaa authentication ssh console tacacs-group LOCAL
aaa authentication telnet console tacacs-group LOCAL
! if you are on an ASA Security Appliance you will need this additional command
!  which is not necessary on a FWSM:
aaa authentication serial console tacacs-group LOCAL
!
! AAA authorization (with command set PIX SHELL send down from tacacs+):
```

```
aaa authorization command tacacs-group LOCAL
! AAA accounting to TACACS+ for start-stop records (for session time
! in either telnet or ssh and also any commands entered for privilege
! level 1 thru 15
aaa accounting telnet console tacacs-group
aaa accounting ssh console tacacs-group
aaa accounting command tacacs-group
!
! *Note - the "aaa accounting command" is for that level and up
! this example was 1 and up - which is default
! This behavior is configures differently then in Cisco IOS
```

For more information, see the following URLs:

- http://www.cisco.com/en/US/partner/products/ps6120/products_command_reference_chapter09186a00805fb9bd.html
- http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_guide_chapter09186a008054d863.html#wp1042026

AAA configuration and behavior is slightly different in Cisco IOS, Cisco ASA 5540, and Cisco FWSM. In general, the use of AAA is the same on all platforms: to provide a userID/password login for "privilege level 1", and to enable password login for "enable or configure" (privilege level 15) commands.

In Cisco IOS devices, the configuration of this document uses the "default" group. This uses a userID/password for the "privilege level 1" login, and depending on the account setup in the AAA (Cisco Secure ACS) server, may also require a separate "enable" level login (privilege level 15). This is true whether the solution administrator connects via SSH or via the physical console port. Both use the default of AAA. As a backup if the AAA server is unavailable, there is a "local account" configured in the device, but this is used *only* if the AAA server is unreachable from that specific device.

In a Cisco ASA security appliance, the commands are slightly different, there is no default, and the solution administrator must configure the AAA authentication command per communication protocol in which the AAA is to be applied. The commands differ in syntax from traditional IOS AAA commands; the term *console* really means *command-line interface* (CLI). The physical port of the console is actually named *serial* in the configuration, and AAA must be applied to this separately. If a solution administrator connects to the Cisco ASA via SSH or via the serial (physical console) port, AAA behavior is determined by that specific command in the configuration. The default behavior, if no AAA policy is applied to the serial, is to use the login "enable_1" for the account ID, although this is not recommended. Only the active ASA in a failover pair has the OSPF routing table that gives a dynamic network route to the AAA server if more that one hop away; thus, *only* the active system has access to the AAA server, super-log syslog server, and so on. Any static routes are valid on the "standby" but not any dynamically learned routes via a dynamic routing protocol (that is, OSPF in this document). This means that a serial (physical console) connection on the standby unit must use the local user account in the configuration to get either "privilege level 1 or 15" access via the physical console port.

In a Cisco FWSM, the commands are mostly similar to the Cisco ASA Security Appliance, but there is no physical serial console on the module. The solution administrator can connect via SSH or by connecting via a special command issued on the 7600 chassis where the module is installed. That command is **session slot 4 processor 1**, where the FWSM is installed in slot 4 of the chassis. This creates a *reverse telnet* from the 7600 chassis to the FWSM for administration. The FWSM always accepts this reverse telnet from the 7600, even when the Telnet protocol has been disabled and the AAA rules apply. Much like on the ASA appliances, only the active has routes via a dynamic routing protocol, so if the AAA server is more than one hop away (and no static route exists to it), you need to use the login of the local account in the configuration on the standby unit.

Restrict Shell Access to SSH instead of Telnet

Use SSH instead of Telnet for remote administration of devices in the NGWAN edge. This provides an encryption shell and adds encrypted privacy to the administrative shell session of the solution administrator to prevent snooping by unwanted parties.

When an solution administrator uses Telnet or r-shell (rsh) to access a device, the UserID and password for that shell session are sent over the network in clear text, as well as any commands they may enter or the responses to those commands. By allowing *only* SSH, the shell session of the solution administrator is encrypted and uses keyed endpoint authentication to keep the session private and not easily viewable. The solution administrator needs to carefully choose Cisco IOS images for their routers that support SSH (usually indicated in the image description or as a 3DES image).

Commands for only using SSH (no telnet or other protocols) for an administrative shell are as follows:

- Cisco IOS router

```
!
! set the routers hostname and domain
hostname wpoc1-r1
ip domain name ese.cisco.com
!
! Create a key for SSH:
cry key generate rsa general-keys modulus 1024
!
! set at SSH version 2 and parameters
ip ssh time-out 30
ip ssh source-interface gi0/1
ip ssh authentication-retries 3
ip ssh logging events
! ***SSH logging not available in cisco 7600 image tested.
ip ssh version 2
!
!  This allow ONLY ssh (not telnet) as an inbound
!  management shell
line vty 0 15
 transport input ssh
 …
!
```

- Cisco ASA/FWSM

```
!
! set the firewall's hostname and domain
hostname wpoc2-asa1
domain-name ese.cisco.com
!
! Create a key for SSH:
cry key generate rsa modulus 1024
!
! *Note – see section below to set range of valid client IP's
! before it will operate – This is required.
```

Using ACLs to Restrict Access

An important step in hardening the devices is to use access control of any protocols that are permitted to the devices for administrative or monitoring purposes (that is, SNMP, SSH, and other protocols used to monitor the devices). A basic shell setting such as a timeout value (not infinite) is also strongly recommended.

In the ASA/FWSM, take special care when allowing SNMP on the inner barrier firewall. Cisco strongly recommends that if you wish to poll the ASA/FWSM, use the configuration similar to what is shown in the configurations below. This allows polling from a particular host, but does not configure an SNMP

trap to be sent to that host. A busy firewall such as the ASA or FWSM located in the NGWAN edge with a high level of syslogging (that is, syslog level 6 or 7) can output a tremendous amount of syslog/SNMP traps, so it can easily overwhelm a normal network management system with SNMP traps. Cisco does not recommend using SNMP trap for the firewall to a network management system. If you choose to do this, trap only lower level events.

The SNMP shown in the example below is SNMPv3, and is using the authentication and encryption options of v3. Some network management stations may require a lower version of SNMP or may not support the authentication option shown here. The solution administrator should contact the network management team and see what SNMP support level is possible in the network NMS tools before implementation. For example, Cisco Works (CW), Cisco LNS, Cisco Resource Manager Essentials (RME) for the most part do not support *authpriv*, but do support most other common NMS systems (such as HP OpenView).

SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensuring that a packet has not been tampered with in transit
- Authentication—Determining that the message is from a valid source
- Encryption—Scrambling the contents of a packet prevents it from being learned by an unauthorized source
- Access control of the IP source allowed to do polling

Note This example was not using a trap host, therefore none is configured.

The following are commands for access control of device administration protocols (access control of SSH is in the following section):

- Cisco IOS router

```
!
! Define a standard ACL of which subnets or hosts are ALLOW
! access to VTY and/or SNMP
!
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
!
!
! Applies ACL 10 to control access to the VTY ports and also
! set the timeout for a shell to 3 minutes
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 …
!
! if you allow or wish to use SNMP to these devices you should
! at a minimum tie the ACL for access control for Reading
! and possible encrypt, authentication, and hash communication if supported by
! the NMS station (SNMPv3)
!
snmp-server group NMS v3 priv
snmp-server user nmsstation NMS v3 auth md5 remoteNMS priv 3des NMSpassword access 10
! *** Note the line entered above will not show in running config,
!    do a "show snmp user" to confirm
!
```

- Cisco ASA/FWSM (note that SNMP v3 is not available in the ASA or FWSM at this time, so this example uses v2c instead).

```
!
! Access control for SSH for ASA:
! Enter a line for each subnets you wish to allow SSH access
ssh 10.0.0.0 255.0.0.0 dmz1
ssh 10.0.0.0 255.0.0.0 inside
ssh scopy enable
!
! This set the timeout period for an existing SSH shell to 3 minutes
ssh timeout 3
!
! Repeat line below for any existing telnet permitted subnets.
no telnet <network> <mask> <interface>
telnet timeout 1
!
! Also set a console timeout:
console timeout 3
!
! if SNMP is used to poll Firewall then set the host(s) allowed to poll:
! repeat for any stations that will be permitted to poll
snmp-server host inside 10.10.0.4 poll community NMScommunity version 2c
snmp-server location inner-barrier
snmp-server contact admin@company.com
snmp-server community NMScommunity
! Disable trapping
no snmp-server enable traps snmp authentication linkup linkdown coldstart
no snmp-server enable traps all
!
```

For more information on SNMPv3, its parameters and other options, see the following URLs:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.html
- http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1830/products_feature_guide09186a00800878fa.html

Disable all Known Hazardous or Unused Features

Disable all known potentially hazardous and unused features, such as directed broadcasts, IP redirect, IP proxy-ARP, CDP, small services, and the built-in global HTTP/HTTPS daemons in Cisco IOS.

The ASA and FWSM have a secure web-based graphical user interface (GUI) for administration of the system named Adaptive Security Device Manager (ASDM). Enabling this GUI requires that the ASA/FWSM run an extra image (separate from the image the chassis runs) on that system in the flash disk. For proper operation, the image for the ASDM GUI and the image that runs on the chassis need to be downloaded and installed together in lock step. The following configurations show how to enable and access-control which IP addresses can access that GUI. The use of this GUI is completely optional, and can be downloaded from the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/asa

Most Cisco IOS routers also have a secure web-based GUI interface for administration named Secure Device Manager (SDM). It is shown as disabled in the configurations below, which is done by disabling the HTTP and HTTPS daemons.

Cisco recommends that on all Cisco IOS systems, **enable secret** be used instead of **enable password**, and also enabling **service password-encryption** to hash other passwords in the configuration when possible.

Following are commands for the disabling of known hazardous or unneeded features:

- Cisco IOS router

```
!
```

```
! Enable Service password encryption
service password-encryption
!
! Disable CDP globally and other un-required features
! *Note – some of these are already off by default
! and just being shown for completeness:
no cdp run
no service udp-small-servers
no service tcp-small-servers
!
! The SDM GUI uses the web server(s) in the IOS router
!  by disabling them the SDM GUI is disabled.
no ip http
no ip https
!
! On ALL active Layer 3 interfaces (up-up) - turn off default interface behaviors that
can be misused. You do not need to do this on L2 interface (like a port that is a
"switchport mode":
interface <xxxxx>
  no ip proxy-arp
  no ip redirect
  no ip directed-broadcast
  no cdp enable
!
```

- Cisco ASA/FWSM

```
!
! These features are not enabled on a ASA/FWSM – no action required
!
! *** if you wish to use ASA User Auth (Uauth) or the ASA
!  Secure Device Manager (ASDM) you will need to enable
!  the http services like the following:
http server enable
http 10.0.0.0 255.0.0.0 dmz1
http 10.0.0.0 255.0.0.0 inside
!
```

Restrict Dynamic Routing Protocols

By default, routing updates on either a Cisco IOS router or Cisco ASA/FWSM are sent unauthenticated and un-hashed (sent in clear text). A malicious attacker who knows the routing protocol process number can become a routing peer and then send or receive routing information with the routing devices. This can lead to false routes being injected into the NGWAN edge routing information and may lead to network disruption or enabling an intruder to gain more access to the network than the solution administrator intended.

To overcome this, for *all* routing protocols used (this document uses EIGRP and OSPF), configure a key and enable the hashing option in that dynamic routing protocol.

The following commands are used for authentication and hashing of the routing protocol (OSPF). EIGRP is used in this document inside the mGRE tunnels (VPN IGP) from the branch routers to the NGWAN crypto aggregation system. It is then redistributed into OSPF from the crypto aggregation routers to the inner barrier (firewall) and into the private core network.

- Cisco IOS router (other OSPF-related items are also shown in this example; for example, redistribution EIGRP into O)

```
!
! Create an ACL for the what is permitted to be redistributed
ip access-list extended route-redist-ACL
 permit ip 10.2.0.0 0.0.255.255 any
```

```
!
! Create a route-map for the redistributed
! This example prefers Crypto Agg 1 over crypto Agg 2
! for all connected branches. You may wish a split of active
! branches (see appropriate VPN design guide for details).
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15388160
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12828160
 set metric 20
!

! Securing (Authenticating RP - OSPF)
router ospf 100
 router-id 10.9.2.3
 log-adjacency-changes
 ! area 1 statement below sets that MD5 hashing is required
 ! in area OSPF area 1:
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface POS5/0
 passive-interface Tunnel1
 network 10.2.0.0 0.0.255.255 area 1
 network 10.7.2.0 0.0.0.255 area 1
 network 10.8.2.0 0.0.0.255 area 1
 network 10.9.2.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.1.0 0.0.0.255 area 1
!
! on neighboring interfaces set that authentication and MD5
! hashing are required:
interface GigabitEthernet0/1
 description to-ASA
  …
 ip ospf authentication message-digest
 ip ospf authentication-key 7 00071A150754
  …
!
```

- Cisco ASA/FWSM

```
! Securing (Authenticating RP - OSPF)
!
router ospf 100
 network 10.0.0.0 255.0.0.0 area 1
 ! area 1 statement below sets that MD5 hashing is required
 ! in area OSPF area 1:
 area 1 authentication message-digest
 router-id 10.9.2.1
 log-adj-changes
!
!
! on neighboring interfaces set that authentication and MD5
! hashing are required:
interface GigabitEthernet0/0
 description DMZ1
 nameif dmz1
 security-level 50
 …
 ospf authentication-key cisco
```

```
 ospf authentication message-digest
!
! on neighboring interfaces set that authentication and MD5
! hashing are required:
interface GigabitEthernet0/1
 description inside
 nameif inside
 security-level 100
 ip address 10.12.1.1 255.255.255.0 standby 10.12.1.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
```

The following commands are used for authentication and hashing of the routing protocol (EIGRP).

Note EIGRP is used in this document inside the mGRE tunnels (VPN IGP) from the branch routers to the NGWAN crypto aggregation system. It is then redistributed into OSPF from the crypto aggregation routers to the inner barrier (firewall) and into the private core network.

- Cisco IOS NGWAN router

```
!
! Create a key-chain for use by EIGRP for authentication
key chain 1
 key 1
  key-string cisco
!
! This is the basic eigrp configuration
!  use the passive-interface on any interface that you do
!  not wish to listen for RP updates.
router eigrp 1
 passive-interface FastEthernet0/0
 passive-interface GigabitEthernet0/1
 passive-interface POS5/0
 network 10.0.0.0
 no auto-summary
!
! Require the key and md5 hashing of EIGRP messages
! this would also be done on tun1 on appropriate system
interface tun0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
  …
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 6
  …
 no ip split-horizon eigrp 1
 ip hold-time eigrp 1 35
 …
!
```

- Cisco IOS branch router

```
!
! Create a key-chain for use by EIGRP for authentication
key chain 1
 key 1
  key-string cisco
!
! This is the basic eigrp configuration
!  use the passive-interface on any interface that you do
!  not wish to listen for RP updates.
router eigrp 1
```

```
 network 10.0.0.0
 no auto-summary
!
! Require the key and md5 hashing of EIGRP messages
interface tun0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 …
!
! Require the key and md5 hashing of EIGRP messages
interface tun1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 …
!
```

Outer Barrier—Infrastructure ACLs (iACLs) and Logging

An infrastructure ACL (iACL) is used as the outer barrier (the first line of defense) from the WAN interface connected to the service provider (SP) cloud. The primary function of the iACL is to allow the cipher traffic (encrypted VPN tunnel traffic) from the branch router and possibly some other basic services (such as NTP or a routing protocol to the SP if desired), and deny all non-permitted traffic with some logging of packets that are denied. This iACL is used primarily to attempt to stop unauthorized access, DoS attacks, or DDoS attacks that originate from the SP or a network connected to the SP, as well as preventing intrusions and data/service theft. This network location usually cannot inspect the end user data packets because they are already encapsulated and encrypted at this location in the solution, so making decisions based on those end user packets/flows is also not possible. Most of the advanced firewalling options are also not possible in the network location of this device. A solution administrator could alternately use a full "stateful inspection firewall" (such as a Cisco FWSM or Cisco ASA) in this network location, but it would not be very well used in this spot in the network and most dedicated firewall products do not support WAN type interfaces directly at this time.

The logging of denied attempts is a critical function for the security audit trail. The solution administrator needs to have a reasonable amount of logs entries to do the following:

- Tell whether an attack took place at a previous time when the system was not being actively monitored
- Have a record of the attempted intrusion or attack to use as evidence to a legal entity
- Have a record of the attempted intrusion or attack to use with the SP to help block at an earlier spot in the SP network

The question arises as to whether to log denied attempts. The answer is to definitely log but within the limits of the system. Use the logging options but with special features and rate limiting in place and tuned to the respective system so as to not overwhelm the host CPU on that system. It is also a common security practice to log to the internal buffer log of the device for troubleshooting and real-time viewing, while concurrently logging off-system to a protected dedicated remote syslog server (this is also known as super-logging or remote syslogging).

The iACL behaves and logs slightly differently on the Cisco 7200VXR and Cisco 7300 Series routers and on the Cisco 7600 Series routers, as described in the following subsections.

iACL and Logging on the Cisco 7200VXR Platform

On the Cisco 7200VXR platform, the switching path of the device, whether a separate dedicated WAN router or as an integrated part of the crypto aggregation system, the "log" statements in the access list can cause the system to go to process switch mode for the logging of an access list line hit. A prolonged

high CPU utilization can cause the network to become unstable and unavailable. To mitigate this problem, it is strongly recommended that you use the available logging and rate limiting commands available in Cisco IOS to help contain the amount of logging per second the device with the iACL does.

The following is a configuration for iACL and logging on the Cisco 7200VXR platform. This example is from Profile 2 (crypto and WAN interface on a Cisco 7200VXR). This sets up some logging options, creates an iACL, and applies it to an outside (POS) interface:

```
!
!
! Set logging host and level
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
! Set logging host and level
logging buffered 32768 informational
logging 10.10.0.2

! *Note the command below is ONLY use with a Cisco 7200 VXR or 7301 or 7304
!  systems and is not required with a Cisco 7600 with OAL enabled.
logging rate-limit 1 except notifications
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
 permit icmp any host 192.0.2.1 echo
 permit icmp any host 192.0.2.1 packet-too-big
 permit icmp any host 192.0.2.1 unreachable
 permit icmp any host 192.0.2.1 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
!
interface POS5/0
 description OC3-to-wan-rtr
 ip address 192.0.2.1 255.255.255.252
 ip access-group InfraProt in
 …
!
```

iACL and Logging on the Cisco 7304 and the 7301 Platforms

On the Cisco 7304 or Cisco 7301 platforms, the switching path of the device, whether on a separate dedicated WAN router or on a chassis that also runs crypto, the log statements in the access list can cause the system to go to process switch mode for the logging of an access list line hit. A prolonged high CPU utilization can cause the network to become unstable and unavailable. To mitigate this problem, it is strongly recommended that you use the available logging and rate limiting commands available in Cisco IOS to help contain the amount of logging per second done by the device with the iACL.

Following is a configuration example for iACL and logging on the Cisco 7304 or Cisco 7301 platform. This sets up some logging options, creates an iACL, and applies it to an outside (POS) interface:

```
!
! Set logging host and level
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
! Set logging host and level
logging buffered 32768 informational
logging 192.0.2.17
!
! *Note the command below is ONLY use with a Cisco 7200 VXR or 7301 or 7304
!  systems and is not required with a Cisco 7600 with OAL enabled.
logging rate-limit 1 except notifications
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 remark This line is not required on WAN rtr - permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq 4500
 permit esp any host 192.0.2.17
 permit icmp any host 192.0.2.17 echo
 permit icmp any host 192.0.2.17 packet-too-big
 permit icmp any host 192.0.2.17 unreachable
 permit icmp any host 192.0.2.17 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
!
!
interface POS5/0/0
 description OC12-TO-WAN-RTR
 ip address 192.0.2.25 255.255.255.252
 ip access-group InfraProt in
```

```
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
!
```

iACL and Logging on the Cisco 7600 Platform

The Cisco 7600 platform (with a Sup720 [PFC3]) has a special feature called Optimized Access List (OAL) that is not available in the other Cisco router series. OAL should be used to optimize the logging function and to offload the processing of the iACL and the respective logging to the PFC3 card. This allows this platform to perform a much more detailed level of logging of denies while still preserving the CPU rate of the MSFC (used for other critical functions such as dynamic routing, IKE, ISAKMP, and so on).

For more details on the OAL feature in the Cisco 7600 Series, see *Understanding Cisco IOS ACL Support* at the following URL:
http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a00801609f6.html

Note The Cisco 7600 is running a 12.2 image, and "double processes" the iACL; once on the cipher text packet and then again on the clear text packet. The line in the iACL that permits the encapsulating mGRE tunnel (which is sourced and destined to and from a WAN IP address) permits that traffic on the second pass. If you are using an IPsec direct encapsulation VPN topology, rather than the DMVPN hub-and-spoke topology used in this document, you need to permit the RFC 1918 numbers that reside at the branch locations to be allowed ingress to the iACL on the second pass (clear text).

The line in the iACL that permits ESP protocol never has any counters in a **show access-list InfraProt** command. This is because the VPN-SPA gets the ESP traffic "bridged down" to the hardware accelerator before the ACL can be incremented. The PFC3 on the Supervisor720 (Sup720) encapsulates or decapsulates the mGRE in hardware (because of unique source and no tunnel-key), but the line for that in the iACL is not incremented. This is considered normal behavior and does not affect operations. These iACL lines are still shown in the iACL for completeness and parity to the other profiles.

Following is the configuration for iACL and OAL logging on the Cisco 7600 platform. This sets up some logging options, creates an iACL, and applies it to an outside (vlan100) interface.

```
!
!
! Set logging host and level
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
! Set logging host and level
logging buffered 32768 informational
logging 10.10.0.2
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
```

```
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
 permit icmp any host 192.0.2.17 echo
 permit icmp any host 192.0.2.17 packet-too-big
 permit icmp any host 192.0.2.17 unreachable
 permit icmp any host 192.0.2.17 time-exceeded
remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
!
! Apply it inbound on the other L3 interface.
!
interface Vlan100
 description VLAN OUTside VPNSPA target
 ip address 192.0.2.17 255.255.255.252
 ip access-group InfraProt in
 ip verify unicast source reachable-via rx allow-default
 no ip redirects
 no ip proxy-arp
 ! It is strongly recommend to enable the Optimized Access List (OAL) feature on the PFC3
card for the
 ! Cisco 7600 platform. You enable it on the interface doing the logging as such:
 logging ip access-list cache in
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 5/0
!
```

Control Plane Policing

At the highest level, Control Plane Policing (CoPP) uses QoS traffic policers to restrict the amount of traffic that is destined to the system on which it is configured. The goal of this feature is to keep a high-level of requests or packets of valid permitted traffic from causing the CPU of the system to spike up and become unstable. Often DoS and DDoS attacks make use of a high volume of normal traffic in an attempt to run a system out of resources and become unavailable.

A basic example of this is if the solution administrator has SSH enabled on the device for device administration, and an attacker sends a flurry of SSH requests in an attempt to eat up CPU and cause the device to be so busy so it does not respond to a critical task (such as routing hellos), and makes the network unstable.

More information on CoPP is available at the following URLs:

- http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_white_paper0900aecd802ca5d6.shtml

- http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a00804559b7.html

CoPP must be “tuned” to the chassis on which it runs and checked periodically for changes in traffic by the solution administrator. The speed of the router processor, the type of traffic that is permitted and rate limited in the policy map, and the switching path in which it occurs (that is, process, CEF, FAST, and so on) can all have an impact on how efficiently CoPP operates on that particular platform. Although this tuning may be difficult, the value of CoPP to prevent an abnormal amount of authorized traffic is a powerful infrastructure protection and worth the investment of time to configure and tune.

The following configuration of CoPP on Cisco 7200VXR (NPE-G2) is an example of some basic CPU and traffic rate policing to this chassis. This example is from Profile 2.

```
!
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.5 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.5
!
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
!
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
!
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.2.0 0.0.0.255 host 10.9.2.4
 permit ospf 10.8.2.0 0.0.0.255 host 10.8.2.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
 permit eigrp 10.0.0.0 0.255.255.255 host 10.8.2.1
!
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
!
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
!
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
```

```
 match access-group name coppacl-vpn
class-map match-all coppclass-igp
 match access-group name coppacl-igp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
!
policy-map copp-policy
 class coppclass-igp
 class coppclass-filemanagement
 class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
 class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
 class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class coppclass-vpn
 class class-default
police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
!
!
control-plane
 service-policy input copp-policy
!
```

The following configuration of CoPP on the Cisco 7600 is an example of some basic CPU and traffic rate policing to this chassis. This example is from Profile 4.

```
!
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.17 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.17
!
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
!
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
!
ip access-list extended coppacl-igp
 remark IGP traffic class
```

```
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.4.0 0.0.0.255 host 10.9.4.3
 permit ospf 10.7.4.0 0.0.0.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
!
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
!
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
!
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
!
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
  match access-group name coppacl-vpn
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
!
policy-map copp-policy
  class coppclass-bgp
   police cir 4000000 bc 400000 be 400000 conform-action transmit exceed-action drop
  class coppclass-igp
   police cir 300000 bc 3000 be 3000 conform-action transmit exceed-action drop
class coppclass-filemanagement
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class coppclass-management
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
  class coppclass-monitoring
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-critical-app
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-vpn
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class class-default
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
!
!
control-plane
```

```
!
service-policy input copp-policy
!
!
```

The following configuration of CoPP on Cisco 7301 WAN router is an example of some basic CPU and traffic rate policing to this chassis. This is an example from Profile 1.

Note Note that the VPN and IGP classes are not in use on this separate WAN router and have been removed from the configuration.

```
!
!
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.9 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.9
!
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
!
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
!
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
!
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
!
policy-map copp-policy
 description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
 class coppclass-filemanagement
 class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
```

```
    exceed-action drop
 class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
 class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
!
!
control-plane
 service-policy input copp-policy
!
!
```

The following configuration of CoPP on Cisco 7304 WAN router is an example of some basic CPU and traffic rate policing to this chassis. This example is from Profile 3.

Note Note that the VPN and IGP classes are not in use on this separate WAN router and have been removed from the configuration.

```
!
!
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.127 host 192.0.2.25 eq bgp
 permit tcp 192.0.2.0 0.0.0.127 eq bgp host 192.0.2.25
!
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
!
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
!
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
!
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
```

```
 permit icmp any any echo
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
!
policy-map copp-policy
 description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
  class coppclass-filemanagement
  class coppclass-bgp
   police cir 80000 bc 8000 be 8000
     conform-action transmit
     exceed-action drop
  class coppclass-management
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
  class coppclass-monitoring
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class coppclass-critical-app
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class class-default
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
!
control-plane
 service-policy input copp-policy
!
```

Further documentation of the CoPP feature on Cisco IOS-based routers is at the following URLs:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml
- http://www.cisco.com/en/US/partner/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080435872.html

Call Admission Control (CAC) for IKE

This feature helps keep the number of concurrent IKE requests from overwhelming the CPU of the NGWAN crypto aggregation system. This is likely to occur in the event of the system recovering after a box failure (that is, boot or reboot). All the branches (which may be in the thousands) attempt to connect to the crypto aggregation system at once, which can result in a race condition that makes the network stabilization take longer than desired. To help restrict the speed at which “new” IPsec peers and routing peers are established, this feature prefers the current connections over new connections. This keeps the IPsec and routing peers that have been established up while slowly adding more each time slice. Without this feature enabled, you may find a situation where three IPsec and routing peers are

established, and then two go down while the next few are being processed. This results in IPsec and routing flapping that causes high CPU and network instability. Fortunately, the **call-admission limit %** command corrects this situation.

CAC polls a global resource monitor, so that IKE knows when the router is running short of CPU cycles or memory buffers. You can configure a resource limit, from 1 to 100, that represents a percentage of system resources. When that level of CPU utilization is reached, the IKE process drops the SA requests (and does not accept new requests). Cisco recommends a value such as 70 percent of CPU.

The configuration of CAC on Cisco IOS platforms is as follows:

```
!
call admission limit 70
!
```

Further documentation of the CAC for IKE feature is available at the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a0080229125.html#wp1058297

Note There is a second version of this feature that uses the number of SAs to limit the total number of SAs that a system can have concurrently. This is not appropriate for an NGWAN crypto aggregation headend system.

Unicast Reverse Path Forwarding

As a basic measure to protect against spoofing-based attacks, the Unicast Reverse Path Forwarding (uRPF) check should be performed. The uRPF feature discards packets that lack a consistent source IP address, such as spoofed IP source addresses created by malicious users to intercept valuable data. This feature uses Cisco Express Forwarding (CEF) tables to verify that the source addresses and the interfaces on which packets were received are consistent with the forwarding tables on the supervisor engine. If the packet is received from reverse path routes, the packet is forwarded. If there is no reverse path route on the interface on which the packet was received, the packet fails the uRPF check and is discarded silently.

uRPF can be deployed throughout the campus network at hardware-based performance rates.

An optional ACL can be tied into the **ip verify** command (**ip verify unicast reverse-path <list>**) to provide a finer grain control over what is discarded if desired.

Note The default route 0.0.0.0/0 cannot be used to perform a uRPF check. For example, if a packet with source address 10.10.10.1 comes on the Serial 0 interface and the only route matching 10.10.10.1 is the default route 0.0.0.0/0 pointing out Serial 0 on the router, the uRPF check fails and it drops that packet. Thus, if the WAN (untrusted) network is a private network (Frame Relay, ATM, MPLS), a routing protocol should be used within that SP cloud. If the WAN network is the Internet with two different ISPs, you most likely use a routing protocol (that is, BPG) from the WAN routers to the ISPs anyway. If no routing protocol is used, no static routes toward the WAN cloud should be the 0.0.0.0/0 route.

The following configuration of uRPF on Cisco IOS and firewall platforms is an example of using uRPF check in the CEF table for packets arriving on the interface to see whether a reverse path route exists to that interface for that source IP of a received packet.

- Cisco IOS NGWAN router. This helps prevent spoofing from the SP cloud:

```
! On a Cisco 7200VXR or Cisco 7301 or Cisco 7304:
! This following command placed on the WAN interface
!  toward the SP cloud
```

```
interface POS5/0
 …
 ip verify unicast reverse-path
 …
!

! on a Cisco 7600 platform
! This following command placed on the VLAN interface
!  that is crypto connected to the WAN interface
!  toward the SP cloud
interface VLAN100
 …
 ip verify unicast source reachable-via rx allow-default
 …
!
```

- Cisco ASA or FWSM. This helps prevent spoofing from the users in the branches that traveled down through the VPN.

```
!
! This following command placed on the outside interface
!  toward the crypto Agg and wan router (global command)
ip verify reverse-path interface dmz1
!
```

Further documentation of uRPF features is available at the following URLs:

- On Cisco 7200VXR platform—
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00804b046b.html
- On Cisco 7301 and Cisco 7304 platform—This feature is unavailable in IOS images tested.
- On Cisco 7600 platform—
http://www.cisco.com/en/US/partner/products/hw/routers/ps368/products_configuration_guide_chapter09186a0080160ec9.html#wp1031429
- On ASA or FWSM platform—
http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_guide_chapter09186a008054ecb8.html#wp1042625
- And also—
http://www.cisco.com/en/US/partner/products/ps6120/products_command_reference_chapter09186a00805fb9f7.html#wp1668353

Aside from being an efficient anti-spoofing solution, uRPF can also be used effectively in combination with static routes pointing to Null0 adjacencies to drop traffic from specific hosts or networks. Null0 Forwarding Information Base (FIB) adjacencies can in turn be distributed automatically with internal BGP (iBGP) to quickly drop packets from infected hosts (also known as remotely triggered blackhole filtering). This is not described in this document, but more information on remotely triggered blackhole filtering is available at the following URL:
http://www.cisco.com/warp/public/732/Tech/security/docs/blackhole.pdf

Scavenger Class QoS

The Scavenger Class QoS strategy is to identify known worms and attacks and drop those packets at a point very close to the end user (usually the switch port at which they are connected). Other traffic patterns from that end user that are considered “unusual” or is “normal traffic but at an unusually high rate” may be marked as scavenger class–CS1 in the DSCP field and allow to pass through the switch. If a device in the branch, NGWAN edge, or campus has a choke point where congestion occurs, the first thing the QoS policy drops is this “anomalous traffic” that is marked CS1.

Because no end user devices are directly plugged into the NGWAN edge gear, it shapes into a *very* small amount of bandwidth any traffic that the campus or branch switches have marked this way, but these systems do not mark the traffic themselves.

Further documentation of the Scavenger Class QoS feature is at the following URL: http://www.cisco.com/univercd/cc/td/doc/solution/esm/qossrnd.pdf

The configuration of a scavenger class is part of the bigger QoS policy that is applied to the WAN circuit. See the following configuration for an example of this class as part of a V3PN-style QoS policy map (CBWFQ-LLQ).

The following configuration of Scavenger Class QoS on a Cisco VXR Platform is an example of creating a general V3PN QoS map and adds in the Scavenger Class QoS class.

```
!
!
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map OC-WAN-wSCAVENGER
 class CALL-SETUP
  bandwidth percent 5
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority percent 33
 class TRANSACTIONAL-DATA
  bandwidth percent 30
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
!
!
interface POS5/0
 description OC3-to-wan-rtr
 …
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
```

The following configuration of Scavenger Class QoS on a Cisco 7600 platform is an example of a general V3PN QoS map and adds in the Scavenger Class QoS class.

```
!
! Because of the use of SIP-400 card carrier and a SPA POS OC-12 card some minor
! configuration difference are require to achieve the same affect:
!
class-map match-any VOICE
```

```
  match ip dscp ef
  match ip precedence 5
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
! The difference between the OC12 QoS map here and the OC3 one on the VXR is that the
! VOICE class can NOT use
! a priority percent or priority bandwidth statement on a SIP-400. So therefore a policer
! in the strict priority queue must be used.
!
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000 conform-action transmit exceed-action drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
interface POS3/1/0
 description OC12-TO-WAN-RTR
  …
 crypto connect vlan 100
 service-policy output OC12-WAN-wSCAVENGER
!
```

Security Service Integration

Inner Barrier—Stateful Inspection Firewall

The inner barrier, usually a fully functional stateful inspection firewall product (Cisco FWSM or a Cisco ASA system) is tasked with access control of the end user traffic that is from branch to campus or campus to branch. This location can use the basic features in a typical Cisco firewall such as NAT functionally, access control, and application inspection. The solution administrator may also use more advanced firewall techniques such as URL filtering, user authentication, and others. The location in the topology of this device can inspect end user traffic that is in clear text (not encrypted) and allows for more fine grain checks and controls on that traffic. The primary function of the inner barrier firewall is traffic (access) control, but also supplies some DoS protection from attacks originating from within the tunnel either to or from a connected branch.

A stateful inspection firewall is used as the inner barrier (the last line of defense) that can inspect the branch clear text traffic (traffic that has already been decrypted) that is destined to the campus network or Internet.

Because this firewall is able to inspect the end user traffic, this firewall can perform access control from branches to the campus core or to the Internet, as well as more advanced firewall features such as user authentication, URL filtering/logging, and so on. The inner barrier firewall may also be used as the Internet gateway edge device in a given location. This fits well if the branch routers do *not* do "split tunneling". Split tunneling is where a branch router sends traffic that is destined to the Internet directly to the Internet and not through the VPN tunnel. If the branch routers are *not* doing split tunneling, all traffic goes to the crypto aggregation device. Traffic destined to either the campus or Internet then goes to the inner firewall. Branch-to-branch encrypted traffic (even in a hub-and-spoke topology) goes to the crypto aggregation system but not to the firewall. This is a limitation of the solution.

This document uses either Cisco ASA Firewall or the Cisco FWSM with a basic firewall rule set and no NAT translations of subnets that are in the enterprise core (inside) to the branch side (DMZ1).

The following is a configuration of ASA 5540 with active primary ASA and partial configuration of interfaces, NAT, rule set and inspections:

```
! Interfaces:
!
interface GigabitEthernet0/0
 description DMZ1
 nameif dmz1
 security-level 50
 ip address 10.9.2.1 255.255.255.0 standby 10.9.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 description inside
 nameif inside
 security-level 100
 ip address 10.12.1.1 255.255.255.0 standby 10.12.1.2
 ospf authentication-key cisco
 ospf authentication message-digest
!

! Nat Rules: to keep internal networks on the same IP subnets (not NATing)
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.1.0 10.12.1.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0


! Rule base:
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
!
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.2.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.7.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended deny ip any any log
access-group dmz1_access_in in interface dmz1
access-group inside_access_in in interface inside
!
! Dynamic inspections:
!
class-map inspection_default
```

```
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect dns maximum-length 512
  inspect netbios
  inspect sunrpc
  inspect tftp
  inspect xdmcp
!
service-policy global_policy global

!
```

The following is a configuration of the FWSM, with active primary FWSM (and partial configuration of interfaces, NAT, rule set and inspections) *and* also the 7600 commands to trunk down VLANs to FWSM:

```
! COMMANDS on 7600 to trunk vlan down to FWSM
firewall module 4 vlan-group 1
firewall vlan-group 1  88,94,104


! ON FWSM:
! Interfaces:
!
interface Vlan94
 nameif dmz1
 security-level 50
 ip address 10.9.4.1 255.255.255.0 standby 10.9.4.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface Vlan104
 nameif inside
 security-level 100
 ip address 10.12.2.1 255.255.255.0 standby 10.12.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!

! Nat Rules: to keep internal networks on the same IP subnets (not NATing)
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.2.0 10.12.2.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0


! Rule base:
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
!
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.4.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.4.0 255.255.255.0 10.0.0.0 255.0.0.0
```

```
access-list dmz1_access_in extended permit ip 10.7.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended deny ip any any log
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
!
! Dynamic inspections:
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect skinny
  inspect smtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
```

Super-Logging (Remote SYSLOG Server)

The goal of this mechanism is to provide one unified syslog of all the systems that compose the NGWAN edge (whether Cisco IOS routers, ASA/FSWM, or other devices capable of syslog output) and optionally even the branch routers. A “super-log” is very useful in a multi-system architecture because all the NGWAN edge devices syslog to a single super-log server. The super-log should be backed up regularly, as a recording keeping mechanism of all relevant devices. As the solution administrator, you need to have some records of what, when, and how often an incident occurred to engage the authorities in the event of an attack or intrusion. You may also be required to collect these logs for prosecutors, legal, or governmental entities. The type of operating system and syslog product on the super-log syslog server is a matter of the preference of the solution administrator: various UNIXs, Windows-based (with syslog application), or others are all potential choices. It is not as important as the availability and ability to do some basic log file rotation and archiving.

The Cisco Monitoring Analysis Reporting System (MARS) is also a possible candidate to be the super-log. Cisco MARS can do event correlation to reduce the amount of labor involved in log review, and bring intelligence to the logs as well as alarming and even NetFlow options.

Note FWSM version 3.1.1 used in this document is not currently supported in the Cisco MARS product, but is scheduled in the near future.

A super-log that is stored in the protected network using files, rather than a wrapping buffer, is a good security mechanism by itself. It is a common practice of attackers to attempt an intrusion and then to initiate many DoS attacks to fill the logging buffer of network gear to wrap the intrusion attempt out of the buffer log. A well-configured and secure super-log is off the attacked system and is not susceptible to this type of attack.

Note Some security devices such as PIX, ASA, and FWSM have an option for TCP-guaranteed logging. This option allows only end user traffic if the firewall can log that transaction. This is *not* recommended for most enterprise customers because it can cause service disruptions if the syslog server is unavailable. If the enterprise security policy requires this feature, it should be implemented with care and a full understanding of the risks to service availability.

A best effort (usually UDP-based) syslog super-log of all devices is recommended in most profiles and does not become a point of failure in the security architecture (as TCP-guaranteed logging may cause). In a security appliance (such as PIX, ASA, or FWSM), the solution manager must take care to log only to the syslog level that is required. A firewall set at a high-level of logging can generate a tremendous amount of logging information (this is also true of SNMP traps). In the following example, the ASA/FWSM is logged at "syslog level 6 (informational) into the internal buffer" but only at "syslog level 5 (notifications)" to the super-log. This represents a customer who does not require URL or connection level logging that occurs at syslog level 6. This is not a one size fits all parameter, and the enterprise needs to see what level is enough for it. There are also rate limiting options in the firewall appliances, but if a correct level is chosen, the need to rate limit it is greatly reduced.

The following commands are for configuring the remote syslog to a super-log server. This assumes that each device has NTP configured and running.

- Cisco IOS router

```
! Set network time protocol (NTP) to sync to a clock
clock timezone est -5
clock summer-time edt recurring
ntp server 10.10.0.1 source GigabitEthernet0/1
!
! Set logging host and level
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
!
! Set logging host and level
logging buffered 32768 informational
logging 10.10.0.2

! *Note the command below is ONLY use with a Cisco 7200 VXR
!  system and is not require with a Cisco 7600 with OAL
! enabled.
logging rate-limit 1 except notifications
!
```

- Cisco ASA/FWSM

Note The FWSM v3.1.1 does not currently support NTP.

```
! Set network time protocol (NTP) to sync to a clock
clock timezone est -5
clock summer-time edt recurring
ntp server 10.10.0.1 source inside prefer
!
! Set logging host and level
logging enable
logging timestamp
logging standby
logging buffered informational
logging trap notifications
!
```

```
! The following line is only required if the ASDM GUI is enabled.
logging asdm informational
logging host inside 10.10.0.2
!
```

AAA Server Integration—Access Control Server (via TACACS+)

A TACACS+ server was implemented for control of AAA from the network devices in the NGWAN edge topology. This document describes a Cisco Secure ACS server (v3.3) located in the private (protected) network to be a repository for administration accounts (UserID/Password) and also to provide downloadable command sets to both the Cisco IOS and ASA/FWSM systems, and lastly to provide an accounting server for record of all logins and commands issued on the respective network gear.

For more information on the configuration of a Cisco Secure ACS server, see the Cisco Secure ACS documentation at the following URLs:

- http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/index.html
- http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/tsd_products_support_series_home.html

PKI Digital Certificates

This document describes a Cisco IOS Certificate Authority (CA) server running a Cisco IOS router that is located in the private (protected) core network and issues certificates to the NGWAN edge crypto aggregation devices as well as the branches that connects to them. There are some security and scalability benefits of using X.509 certificates rather than the other options for IKE authentication (wildcard pre-shared keys, per-peer pre-shared keys, or IKE aggressive mode). Digital Certificates offer a highly secure but still very scalable and manageable solution for IKE authentication.

The Certificate Authority issues a certificate to each device and signs it with the public signing certificate of the CA. That device certificate is valid only on that system that contains the private key and only for the time determined when it was issued. The CA has facilities such as a Certificated Revocation List (CRL) for revoking a particular certificate without affecting the other certificates that it has issued.

Table 4 shows a comparison of PKI Digital Certificates with other IKE authentication methods.

Table 4 Comparison of PKI Digital Certificates with Other IKE Authentication Methods

On Crypto Aggregation System:		
	Limitations of other IKE authentication mechanisms	**Comparison of X.509 Digital Certificates to other IKE authentication mechanisms**

Table 4 Comparison of PKI Digital Certificates with Other IKE Authentication Methods (continued)

Wild card preshared	A single all-network "0.0.0.0/0" preshared key on the crypto aggregation system configuration. If any crypto peer in the architecture is compromised, that shared key must be manually changed on the crypto aggregation systems and *all* branches. (No easy revocation method). Also, there are no built in expiry times for this key.	Each Digital Certificate is device-specific and only valid for the time period described in the certificate. Each certificate can be revoked using a CRL (or OSCP) independently of the rest of the crypto topology. There is a fixed amount of configuration lines for Digital Certificates present in the crypto aggregation devices configuration. But this information is not secret and cannot be used by an intruder without the private key (which is not stored in the running or startup configuration but rather in protected NVRAM). Certificates always have a valid period (start and stop date) for which they are valid; this keeps them current, and approved devices can re-enroll before their current certificates expire.

Table 4 Comparison of PKI Digital Certificates with Other IKE Authentication Methods (continued)

Per-peer preshared	A specific preshared per peer address, pre-configured in the crypto aggregation configuration. If branches are dynamically addressed, this is *not* a valid option because branch IPs cannot be coded in advance in the crypto aggregation configuration, because they change periodically. If a particular branch is compromised, only that particular shared secret needs to be changed on the crypto headend. This is an improvement over a wildcard pre-shared. The disadvantage is hundred or thousands of lines of keys would be stored in the crypto aggregation system configuration, making manageability more difficult. Also, there are no built-in expiry times for these keys.	A per-peer preshared has to be removed on a compromised branch and also from the crypto agg system. Although a certificate for a compromised branch only needs to revoke that offending branch, there are no changes to the crypto headend at all. There is a fixed amount of configuration lines for Digital Certificates present in the crypto aggregation devices configuration. But this information is not secret and cannot be used by an intruder without the private key (which is not stored in the running or startup configuration but rather in protected NVRAM). Certificates always have a valid period (start and stop date) for which they are valid. This keeps them current, and approved devices can re-enroll before their current certificates expire.
IKE aggressive mode	IKE aggressive mode adds a device authentication (usually via a RADIUS server) in addition to a key to add a layer of control per peer. This extra authentication can be a UserID/Password stored in an ACS server and accessed via RADIUS from the crypto aggregation system. This requires a bit more configuration on the crypto aggregation devices. An advantage of this mechanism is that it does allow one branch to be disallowed by simply disabling that UserID to which the branch used to connect (similar in end result to a certificate revocation). The disadvantages are that the UserID/Password information adds more management. IKE aggressive mode sends that UserID\Password information hashed but in clear text, not in the ISAKMP encrypted channel. This is less secure than other mechanisms. Although most RADIUS servers (including Cisco Secure ACS) have an option to force password changes based on time, a network device would be unable to do this change. If an administrator changes the password for an account, they would have to manually edit the configuration of the branch using it.	Digital Certificate authentication is done completely in the ISAKMP (encrypted) tunnel and is protected by that Security Association. Each certificated can be revoked using a CRL (or OSCP) independently of the rest of the crypto topology Certificates always have a valid period (start and stop date) for which they are valid. This keeps them current, and approved devices can re-enroll before their current certificates expire.

The next section provides the configuration of both crypto VPN and digital certificates on the crypto aggregation systems.

Implementation and basic management of a PKI infrastructure is described in Digital Certificates/PKI for IPsec VPNs at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/cdccont_0900aecd804102a1.pdf

Encryption Services (VPN Topology)

The choice of which VPN topology is used is the largest and most important decision in this process. It has major ramifications to the configuration, routing protocol, performance, and scalability. The VPN topologies have been already described in detail in their respective design guides.

The crypto aggregation function usually includes the actual crypto aggregation as well as tunnel interfaces and the VPN IGP routing protocol (used "in" the VPN tunnel). This may be on a single chassis or have multiple chasses for scalability.

The high-level aspects of each of the NGWAN VPN design topologies are listed in Table 5.

Table 5 High-Level Comparison of VPN Topologies

VPN Topology	Tunnel Interfaces?	Routing Protocol in VPN
IPsec Direct Encapsulation	None	None (uses RRI and DPD), which may be redistributed into an internal core routing protocol at the headend crypto aggregation system
P2P GRE over IPsec	GRE tunnel interface(s)	Uses a routing protocol (EIGRP or OSPF) inside the GRE tunnels through to the branches
DMVPN (hub-and-spoke)	• Multipoint GRE (mGRE) tunnel interfaces on headend • GRE tunnel interfaces at branch	Uses a routing protocol (EIGRP or OSPF) inside the mGRE tunnels through to the branches, and also uses NHRP protocol at the headend
Virtual Tunnel Interface (VTI)	• Tunnel interfaces and virtual templates on headend • Tunnels are point-to-point (virtual access interfaces) generated off the headend template.	Uses a routing protocol (EIGRP or OSPF) inside the tunnel through to the branches

For an overview, see the *IPsec VPN Design Overview* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns130/c649/ccmigration_09186a0080685ce6.pdf.

This helps you choose which VPN solution is right for your deployment.

See also the following NGWAN VPN topology design chapters:

- IPsec Direct Encapsulation Design Chapter—
  http://www.cisco.com/univercd/cc/td/doc/solution/direncap.pdf
- p2p GRE over IPsec Design Chapter—
  http://www.cisco.com/univercd/cc/td/doc/solution/p2pgre_x.pdf
- Dynamic Multipoint VPN (DMVPN) Design Chapter—
  http://www.cisco.com/univercd/cc/td/doc/solution/dmvpn_x.pdf
- Virtual Tunnel Interface (VTI) Design Chapter—
  http://www.cisco.com/univercd/cc/td/doc/solution/contnet/vti_dgex.pdf

It is important that the solution administrator choose Cisco IOS images for the crypto aggregation systems that support the encryption level (3DES or AES) that they desire to use, and it is *always* recommended to use a hardware crypto accelerator.

This document uses a DMVPN (dual hub–dual cloud) hub-and-spoke as the basis for documentation purposes, although any of the various VPN topologies listed above can also be a viable choice. The use of PKI X.509 Digital Certificates was also used as a strong and scalable authentication for IKE on the crypto IPsec VPN tunnels. See PKI Digital Certificates, page 56 for details on implementing digital certificates.

The following are commands for configuration of DMVPN on Cisco 7200VXR crypto aggregation systems. This document uses a DMVPN hub-and-spoke topology (dual hub-dual cloud) as the crypto topology from the crypto aggregation system to the branch routers.

- Cisco 7200VXR aggregation system; this side is using tunnel protect mode on the mGRE interface:

```
!
ip host wpoc3-r1 10.10.0.3
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 05
  3082026B 308201D4 A0030201 02020105 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363036 30393135 34313537 5A170D30 38303630 38313534 3135375A
  30273125 30230609 2A864886 F70D0109 02161677 706F6331 2D72312E 6573652E
  63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 8100E983 7A05FE61 6456E526 45F91462 98B5B452 56B01B19 380DB530
  693116DE AFA693CF 6101413B 5FB3A141 3F2E18CA 9FCCBA8E 6DE638C6 61BF524C
  288FAC70 E96495CF 70C4B6FE 6D04C49E 88246645 F0C05552 079FEAD0 2A00E932
  D1AB056A E377E441 DC66998F 15F6EAA5 EF7F7F59 3BA4F53A 97BBA338 F5F8EC3F
  A4B1CD6A 30D70203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 1433F99C A898E52D 26D2B97C A26D05FC 1EF109C3 45301D06
  03551D0E 04160414 5998F583 47BEC171 BB297786 1BA75A95 5EBE5135 300D0609
  2A864886 F70D0101 04050003 818100D1 5D87FF1F D3C5FD0B 3B39FAF2 D1DBDB3C
  75651151 CF9AABAE 1B45E8B4 CBC104B6 62AD6489 42267761 25F0D039 70107A3B
  F60F5F36 5A79FBF6 4BC0DBB5 7073EB93 9553C6EE EBB04A6D 4148DDA6 C08D2668
  7964997E 6815DB9A CD4AB633 E567F861 83ACC246 283114B6 B00FE406 884984A1
  0EF96354 2162AD9C E7AAB15C 840EE7
  quit
certificate ca 01
  308202D7 30820240 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363033 31343231 33323136 5A170D31 30303331 33323133 3231365A
  307F311C 301A0609 2A864886 F70D0109 01160D20 6573652D 76706E2D 7465616D
  310C300A 06035504 08130320 4E433111 300F0603 55040713 08205261 6C656967
  68311B30 19060355 040A1312 20436973 636F2053 79737465 6D732049 6E63310D
  300B0603 55040B13 04204553 45311230 10060355 04031309 2077706F 63332D72
  3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100EB32
  6078EF84 40A19FB3 05775BA2 E7BFFE87 17AF2FEE 3E5C9387 0D9FAB35 A4186073
  45CA8B41 DE7C1FB4 B99D0093 69AD253C E7829575 6956D485 B78B18E2 A10D9EC4
  04CEE4A5 9AFEF3FB E10E9A61 2A224B7E 50D6E7DA 3B7501E7 D49E8F73 9DD90CFC
```

```
  89050020 BBFB63C1 82A092D0 C36D322C 46AD2132 11D5E531 0E55C0E9 66E70203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1433F99C A898E52D 26D2B97C
  A26D05FC 1EF109C3 45301D06 03551D0E 04160414 33F99CA8 98E52D26 D2B97CA2
  6D05FC1E F109C345 300D0609 2A864886 F70D0101 04050003 81810080 FC245598
  CA42E74B 960901C7 E1E11205 5EDBF3D8 38767D96 C4307F85 0C905FCF 0BC687C0
  C88302D0 32EBBACA 6124BEAE 43C6A984 0E1D733B F404A684 793E1526 C25637A1
  99A3E97B C92C5E41 DAB0DCDD 324631B0
  87266EC9 21FEC360 13FC20C3 9B18CFE4
  75F7A788 E0855654 49880300 95BB46D7 F37A63F0 FFB7855F FCD3F6
  quit
!

!
! In the crypto isakmp policy RSA mode is the default
! (PKI Digital Certificates is the default)
crypto isakmp policy 10
 encr 3des
 group 2
!
! Configure a DPD keepalive - ALWAYS…
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.2.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 qos pre-classify
 tunnel source POS5/0
 tunnel mode gre multipoint
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
 !
 !
 ! Used in this document as static route to branches, could also
 !  use a routing protocol over the wan or with the wan ISP(i.e. bgp)
 ip route 192.0.2.0 255.255.255.128 192.0.2.2
 !
```

- Connected Cisco IOS branch router; this side is using tunnel protect mode on the mGRE interface:

```
!
ip host wpoc3-r1 10.10.0.3
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
```

```
 revocation-check none
 source interface FastEthernet0/0
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 09
  30820227 30820190 A0030201 02020109 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363036 30393135 35303332 5A170D30 38303630 38313535 3033325A
  30273125 30230609 2A864886 F70D0109 02161677 706F6331 2D72382E 6573652E
  63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101 0500034B 00304802
  4100BEC6 4CC7E6E0 9FAFDEC6 F91C6D67 82FF943C 3ABD1CEB 675E6A94 222A2D56
  28522A22 8DDC598C 81110895 A5956402 F6A38C93 B8B94957 8870A341 FEC0F645
  54F30203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304
  18301680 1433F99C A898E52D 26D2B97C A26D05FC 1EF109C3 45301D06 03551D0E
  04160414 7977C6FA E05E3352 D25A374D 8C22F369 7DE93ADF 300D0609 2A864886
  F70D0101 04050003 8181006A 96338109 7B07667E D7AF2148 60FEA48E 2DE5BFBB
  CCD48148 BB157A44 D3035BFE D2AD5F93 B710F490 42B196F4 B27BB9FC A2586708
  690A60C4 4C33F207 ACBF5622 93EB4821 5D4F2C73 BDDDAE63 E36641F8 A46963B3
  1051D25F 813E1A67 25523974 7E425EA1 BA28AEE0 0CF2F32E 2C0F7DAE 3D40CCD0
  C986668D F7518168 2AD904
  quit
 certificate ca 01
  308202D7 30820240 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363033 31343231 33323136 5A170D31 30303331 33323133 3231365A
  307F311C 301A0609 2A864886 F70D0109 01160D20 6573652D 76706E2D 7465616D
  310C300A 06035504 08130320 4E433111 300F0603 55040713 08205261 6C656967
  68311B30 19060355 040A1312 20436973 636F2053 79737465 6D732049 6E63310D
  300B0603 55040B13 04204553 45311230 10060355 04031309 2077706F 63332D72
  3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100EB32
  6078EF84 40A19FB3 05775BA2 E7BFFE87 17AF2FEE 3E5C9387 0D9FAB35 A4186073
  45CA8B41 DE7C1FB4 B99D0093 69AD253C E7829575 6956D485 B78B18E2 A10D9EC4
  04CEE4A5 9AFEF3FB E10E9A61 2A224B7E 50D6E7DA 3B7501E7 D49E8F73 9DD90CFC
  89050020 BBFB63C1 82A092D0 C36D322C 46AD2132 11D5E531 0E55C0E9 66E70203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1433F99C A898E52D 26D2B97C
  A26D05FC 1EF109C3 45301D06 03551D0E 04160414 33F99CA8 98E52D26 D2B97CA2
  6D05FC1E F109C345 300D0609 2A864886 F70D0101 04050003 81810080 FC245598
  CA42E74B 960901C7 E1E11205 5EDBF3D8 38767D96 C4307F85 0C905FCF 0BC687C0
  C88302D0 32EBBACA 6124BEAE 43C6A984 0E1D733B F404A684 793E1526 C25637A1
  99A3E97B C92C5E41 DAB0DCDD 324631B0 87266EC9 21FEC360 13FC20C3 9B18CFE4
  75F7A788 E0855654 49880300 95BB46D7 F37A63F0 FFB7855F FCD3F6
  quit
!
!
! In the crypto isakmp policy RSA mode is the default
! (PKI Digital Certificates is the default)
crypto isakmp policy 10
 encr 3des
 group 2
!
! Configure a DPD keepalive - ALWAYS…
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
```

```
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
interface Tunnel0
description Tunnel0 - to wpoc1-r1
 bandwidth 1000000
 ip address 10.7.2.10 255.255.255.0
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast 192.0.2.1
 ip nhrp map 10.7.2.1 192.0.2.1
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 ip nhrp nhs 10.7.2.1
 qos pre-classify
 tunnel source FastEthernet0/1
 tunnel destination 192.0.2.1
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface Tunnel1
  description Tunnel1 - to wpoc1-r2 - secondary by routing
 bandwidth 1000000
 ip address 10.8.2.10 255.255.255.0
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast 192.0.2.5
 ip nhrp map 10.8.2.1 192.0.2.5
 ip nhrp network-id 105640
 ip nhrp holdtime 300
 ip nhrp nhs 10.8.2.1
 delay 60000
 qos pre-classify
 tunnel source FastEthernet0/1
 tunnel destination 192.0.2.5
 tunnel key 105601
 tunnel protection ipsec profile vpn-dmvpn
!
! To prevent recursive routing.
ip route 192.0.2.0 255.255.255.128 192.0.2.33
!
```

The following are commands for the configuration of DMVPN Cisco 7600 crypto aggregation systems. This document uses a DMVPN hub-and-spoke topology (dual hub-dual cloud) as the crypto topology from the crypto aggregation system to the branch routers. This example *does not* use mGRE tunnel keys.

- Cisco 7600 crypto aggregation system; this side is using a dynamic crypto map and an mGRE interface:

```
!
ip host wpoc3-r1 10.10.0.3
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
```

```
crypto pki certificate chain ese-ios-ca
 certificate 07
  3082026F 308201D8 A0030201 02020107 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363036 30393135 34353032 5A170D30 38303630 38313534 3530325A
  302B3129 30270609 2A864886 F70D0109 02161A77 706F6332 2D373630 302D312E
  6573652E 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100A44C 107A83AA BF098999 36A44AD3 6176969F 1DC9E4DD
  A697792F 76BD0F5A 2CBEA916 E04CE204 152F2700 AA81F9E4 FA331478 E15CE849
  8BC893DB 66551600 65A61571 53F0D9F0 E97DF70B E7882453 51D6F761 D65D08C5
  13B15324 68AC10C2 5365C4E8 A11DD2A0 25BACAB8 561B0089 EDD11871 5231A888
  5DB16E81 6E91FA14 D9CD0203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 1433F99C A898E52D 26D2B97C A26D05FC 1EF109C3
  45301D06 03551D0E 04160414 09EC731E 1569A4CD AE073048 B0F3065E ED1E57D5
  300D0609 2A864886 F70D0101 04050003 8181008E 22252713 C828BACD 1285CA7D
  1CDF8FC7 1D0D1AC5 BBE4E30C E3A402A8 51FA6A2A AE895688 E7375441 7E2427AC
  F05A2200 4F6E385E F2D6037A DEC25544 856F07B0 3A608631 A41A01CE 6C99E398
  D962ED59 4612EA03 C300A9E4 D3856EB1 6791C562 A9DE5931 2E4C51C2 DE8D7AE3
  E38764BE BDA4D8A8 82BC5963 B725622B B894F0
  quit
 certificate ca 01
  308202D7 30820240 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363033 31343231 33323136 5A170D31 30303331 33323133 3231365A
  307F311C 301A0609 2A864886 F70D0109 01160D20 6573652D 76706E2D 7465616D
  310C300A 06035504 08130320 4E433111 300F0603 55040713 08205261 6C656967
  68311B30 19060355 040A1312 20436973 636F2053 79737465 6D732049 6E63310D
  300B0603 55040B13 04204553 45311230 10060355 04031309 2077706F 63332D72
  3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100EB32
  6078EF84 40A19FB3 05775BA2 E7BFFE87 17AF2FEE 3E5C9387 0D9FAB35 A4186073
  45CA8B41 DE7C1FB4 B99D0093 69AD253C E7829575 6956D485 B78B18E2 A10D9EC4
  04CEE4A5 9AFEF3FB E10E9A61 2A224B7E 50D6E7DA 3B7501E7 D49E8F73 9DD90CFC
  89050020 BBFB63C1 82A092D0 C36D322C 46AD2132 11D5E531 0E55C0E9 66E70203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1433F99C A898E52D 26D2B97C
  A26D05FC 1EF109C3 45301D06 03551D0E 04160414 33F99CA8 98E52D26 D2B97CA2
  6D05FC1E F109C345 300D0609 2A864886 F70D0101 04050003 81810080 FC245598
  CA42E74B 960901C7 E1E11205 5EDBF3D8 38767D96 C4307F85 0C905FCF 0BC687C0
  C88302D0 32EBBACA 6124BEAE 43C6A984 0E1D733B F404A684 793E1526 C25637A1
  99A3E97B C92C5E41 DAB0DCDD 324631B0 87266EC9 21FEC360 13FC20C3 9B18CFE4
  75F7A788 E0855654 49880300 95BB46D7 F37A63F0 FFB7855F FCD3F6
  quit
!
!
! In the crypto isakmp policy RSA mode is the default
! (PKI Digital Certificates is the default)
crypto isakmp policy 10
 encr 3des
 group 2
!
! Configure a DPD keepalive - ALWAYS…
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
```

```
!
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!

!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.4.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
ip nhrp map multicast dynamic
 ip nhrp network-id 105700
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 load-interval 30
 tunnel source Vlan100
 tunnel mode gre multipoint
!

!
!
interface Vlan100
 description VLAN OUTside VPNSPA target
 ip address 192.0.2.17 255.255.255.252
  …
 crypto map dynamic-map
 crypto engine subslot 5/0
!
!
interface POS3/1/0
 description OC12-TO-WAN-RTR
 …
 crypto connect vlan 100
 …
!
! Used to be a static route to WAN for branches- you may choose to
!   use a dynamic routing protocol to the WAN or ISP WAN (i.e. bgp)
ip route 192.0.2.0 255.255.255.128 192.0.2.18
!
! Because this crypto Agg device uses the VPN-SPA crypto HW
! accelerator it has these "internal" interfaces, they are
! automatically configured and no use intervention is require ! ! on them:
!
interface GigabitEthernet5/0/1
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
```

```
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/0/2
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
```

- Cisco IOS branch router; this side is using tunnel protect mode on the mGRE interface:

```
!
ip host wpoc3-r1 10.10.0.3
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check none
 source interface GigabitEthernet0/0
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 0F
  3082026B 308201D4 A0030201 0202010F 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363036 30393136 35393534 5A170D30 38303630 38313635 3935345A
  30273125 30230609 2A864886 F70D0109 02161677 706F6331 2D72392E 6573652E
  63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003 818D0030
  81890281 8100C3D8 DBCCF741 BAE42543 49CB82CC 72840D5F 6E47971A 6B1725AA
  18ECB988 31CA2BC2 A0452B2F E9227086 F9C4C762 A0EFB835 3806089C 216B6B8E
  903D9730 7432315F 13575446 EE880BD8 65EA38DC B37822FE 7FAD5FA2 3D5010E1
  DB147E3A 5F2B4529 FBFB33DA 6DF14CC2 CE41CC83 0FB8E7E1 6F7DA6C2 C54E263C
  F20F30E9 9AA50203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 1433F99C A898E52D 26D2B97C A26D05FC 1EF109C3 45301D06
  03551D0E 04160414 3B30BDAE 49256B4F F8407F63 74EB572D 77CCDDB0 300D0609
  2A864886 F70D0101 04050003 818100AA C371C324 1052C315 ECB9DDE8 574EA7B6
  3F2B5D65 A3C0A8AB C0D1B03D 6F08A528 D126E368 4B717EAF 223983D3 53519ECE
  E8C04E28 2787CD6D 92FC8CAC 8B762C9C D172CE21 B8BA5484 EF63C8DC F6C595CE
  AA79C656 3ED664A7 F6CD7E8C 583C2658 C584243D 8E4A1404 6499B242 DDD4EC57
  BDD215F4 2933CA26 5869B14D 25A8C2
  quit
 certificate ca 01
  308202D7 30820240 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  7F311C30 1A06092A 864886F7 0D010901 160D2065 73652D76 706E2D74 65616D31
  0C300A06 03550408 1303204E 43311130 0F060355 04071308 2052616C 65696768
  311B3019 06035504 0A131220 43697363 6F205379 7374656D 7320496E 63310D30
  0B060355 040B1304 20455345 31123010 06035504 03130920 77706F63 332D7231
  301E170D 30363033 31343231 33323136 5A170D31 30303331 33323133 3231365A
  307F311C 301A0609 2A864886 F70D0109 01160D20 6573652D 76706E2D 7465616D
  310C300A 06035504 08130320 4E433111 300F0603 55040713 08205261 6C656967
  68311B30 19060355 040A1312 20436973 636F2053 79737465 6D732049 6E63310D
  300B0603 55040B13 04204553 45311230 10060355 04031309 2077706F 63332D72
  3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100EB32
```

```
  6078EF84 40A19FB3 05775BA2 E7BFFE87 17AF2FEE 3E5C9387 0D9FAB35 A4186073
  45CA8B41 DE7C1FB4 B99D0093 69AD253C E7829575 6956D485 B78B18E2 A10D9EC4
  04CEE4A5 9AFEF3FB E10E9A61 2A224B7E 50D6E7DA 3B7501E7 D49E8F73 9DD90CFC
  89050020 BBFB63C1 82A092D0 C36D322C 46AD2132 11D5E531 0E55C0E9 66E70203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1433F99C A898E52D 26D2B97C
  A26D05FC 1EF109C3 45301D06 03551D0E 04160414 33F99CA8 98E52D26 D2B97CA2
  6D05FC1E F109C345 300D0609 2A864886 F70D0101 04050003 81810080 FC245598
  CA42E74B 960901C7 E1E11205 5EDBF3D8 38767D96 C4307F85 0C905FCF 0BC687C0
  C88302D0 32EBBACA 6124BEAE 43C6A984 0E1D733B F404A684 793E1526 C25637A1
  99A3E97B C92C5E41 DAB0DCDD 324631B0 87266EC9 21FEC360 13FC20C3 9B18CFE4
  75F7A788 E0855654 49880300 95BB46D7 F37A63F0 FFB7855F FCD3F6
  quit
!
! In the crypto isakmp policy RSA mode is the default
! (PKI Digital Certificates is the default)
crypto isakmp policy 10
 encr 3des
 group 2
!
! Configure a DPD keepalive - ALWAYS…
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
crypto map static-map local-address GigabitEthernet0/1
!
!
interface Tunnel0
description Tunnel0 - to wpoc2-7600-1
 bandwidth 1000000
 ip address 10.7.4.11 255.255.255.0
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast 192.0.2.17
 ip nhrp map 10.7.4.1 192.0.2.17
 ip nhrp network-id 105700
 ip nhrp holdtime 300
 ip nhrp nhs 10.7.4.1
 load-interval 30
 qos pre-classify
 tunnel source GigabitEthernet0/1
 tunnel destination 192.0.2.17
 tunnel protection ipsec profile vpn-dmvpn
!
interface Tunnel1
description Tunnel1 - to wpoc2-7600-2 Secondary by routing
 bandwidth 1000000
 ip address 10.8.4.11 255.255.255.0
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast 192.0.2.21
 ip nhrp map 10.8.4.1 192.0.2.21
 ip nhrp network-id 105701
 ip nhrp holdtime 300
```

```
 ip nhrp nhs 10.8.4.1
 load-interval 30
 delay 60000
 qos pre-classify
 tunnel source GigabitEthernet0/1
 tunnel destination 192.0.2.21
 tunnel protection ipsec profile vpn-dmvpn
!
!
! To prevent recursive routing.
ip route 192.0.2.0 255.255.255.128 192.0.2.65
!
```

High Availability (Redundancy)

Network performance in the event of a failure is a primary concern during the planning of a secure NGWAN edge deployment. This section provides some recommendations for a highly available secured NGWAN edge.

The full configuration samples in Test Bed Configuration Files, page 80 are of the four profiles in a multi-threaded architecture. By simply removing the redundancy options (that is, failover in the firewall and other basic setups), the single threaded configurations are clearly shown.

Redundant Multi-Threaded in a Single Site Location

In this topology, a dynamic routing protocol (an IGP) is used from the crypto aggregation system through the VPN down to the branches (a VPN IGP), and then an RP such as OSPF is used between the crypto aggregation system and the inner barrier (firewall) and also between the inner barrier and the enterprise core. This is necessary so that the inner firewall knows exactly which crypto aggregation system to a particular branch is the "preferred" path. Keep in mind that each branch would have a VPN tunnel to both crypto aggregation systems, and that one would be the preferred path. The solution administrator has the choice to make one crypto aggregation preferred to all branches, or perform an administrative load balance (by use of the delay or cost commands in the RP) to prefer some branches to one crypto aggregation system and some to the other. This topology supports either.

An important note on routing is that branch subnets should *not* be summarized to the crypto aggregation systems, inner firewall, or enterprise core network. Each branch subnet should show up as preferred on one of the crypto aggregation devices and less preferred on the other. This is even more important in the multi-site topology described in the next section.

This document shows the use of EIGRP as the VPN IGP, and then uses redistribution into OSPF "area 1" for communication to the inner barrier firewall and into the enterprise core RP.

Note Note that if OSPF is used, Cisco strongly recommends that it not be "area 0"; this is a WAN connection and should not be in the core area of OSPF. Although both routers and ASA/FWSM systems can be area border routers (ABRs), Cisco recommends that the ABR be on a core router for stability reasons.

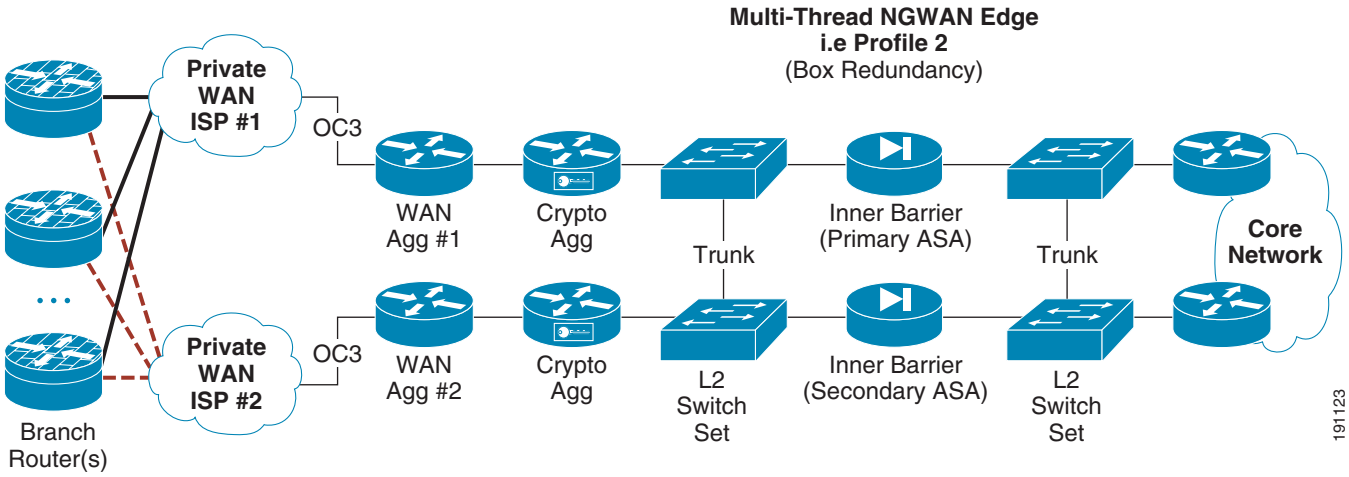
This topology has many layers of failover:

- Failover of a branch is determined by the RP used in the VPN IGP. This detects a failure in the VPN or in the WAN circuit (either headend or branches).
- Failover of the inner barrier firewall(s) is an active-standby stateful failover set and is independent of the VPN IGP of the crypto aggregation system.

The following figures show multi-threaded network topologies for Profiles 2 and 4 (with box level redundancy) located at a single site.

In Figure 13, the choice was made to not have a failover layer between the WAN agg and the crypto agg layers in the topology. This choice was to make subnetting and failover behavior similar to the other profiles. Because the WAN IP subnetting is assumed to be private address space (RFC 1918), it is also possible to have an L2 switch layer between the WAN and crypto agg systems if desired.

Figure 13 Multi-Threaded Single Site OC3 Solution

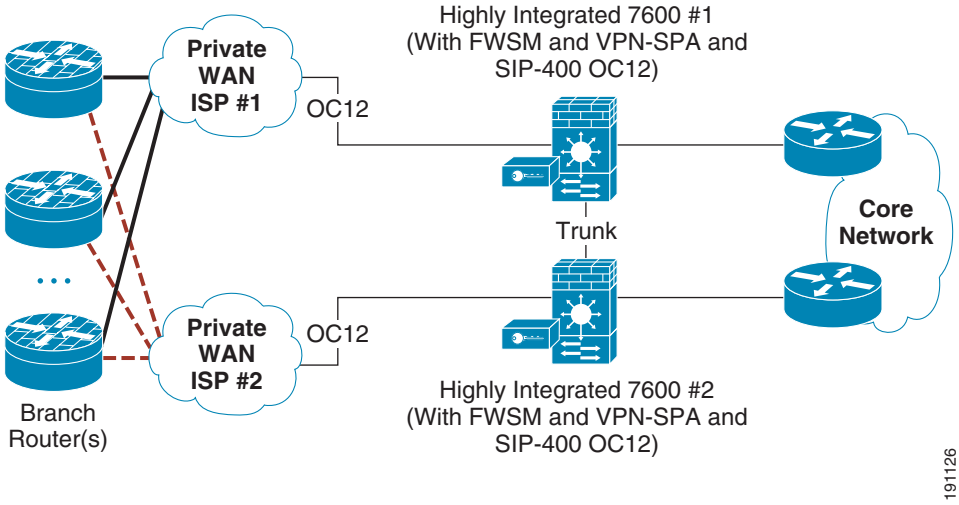


If L2 switches are required for redundancy, they may be implemented as unique sets of switches at each spot in the NGWAN edge topology. Alternatively, the L2 may simply be different VLANs off the same two shared switches. This choice depends on the company requirements for keeping different levels of traffic separated or not on a L2 device. Views on this practice vary among security professionals. The company security policy may require that the switch pair not carry multiple VLANs from different security zones. The primary concern is that if a switch is compromised, access to a more protected location in the network topology (VLAN) can be exposed. A solution to this concern is to implement the switch pairs as unique pairs at each location in the network, which requires more network gear.

Only in a multi-threaded site do you need a secured set of switches (that is, a Cisco Catalyst 3560G). An example of configurations for a secured and redundant pair of switches for various profiles that use one pair of switches for multiple VLANs are shown in Test Bed Configuration Files, page 80.

Figure 14 shows a multi-threaded single site OC12 solution.

Figure 14 Multi-Threaded Single Site OC12 Solution



On a Cisco ASA/FWSM, if the firewall is doing dynamic routing with the crypto agg and the core router (OSPF or RIP) and is in an ACTIVE-STANDBY pair for redundancy, *only* the active unit is a routing neighbor that has the dynamically learned routes from that RP. The standby unit has only connected and static routes in its routing table. This may prevent facilities such as AAA from properly working because the standby does not likely have a route to the AAA server, and may also prevent communication inband to the standby unit (see CSCeb23798).

The full configuration samples are supplied in Test Bed Configuration Files, page 80 for the four secure NGWAN edge profiles in this multi-threaded single site topology as the most complex and difficult to implement.

Multiple Single-Threaded Site Locations of NGWAN Edge

The basics of this redundancy model are a single thread in a site, and multiple sites to provide geographical redundancy between locations. The single-threaded version in a given site is shown in Figure 15 and Figure 16 in single-threaded flow (no box redundancy) for both the topologies previously discussed in Profile 2 and Profile 4.

Figure 15 Single-Threaded OC3 Solution

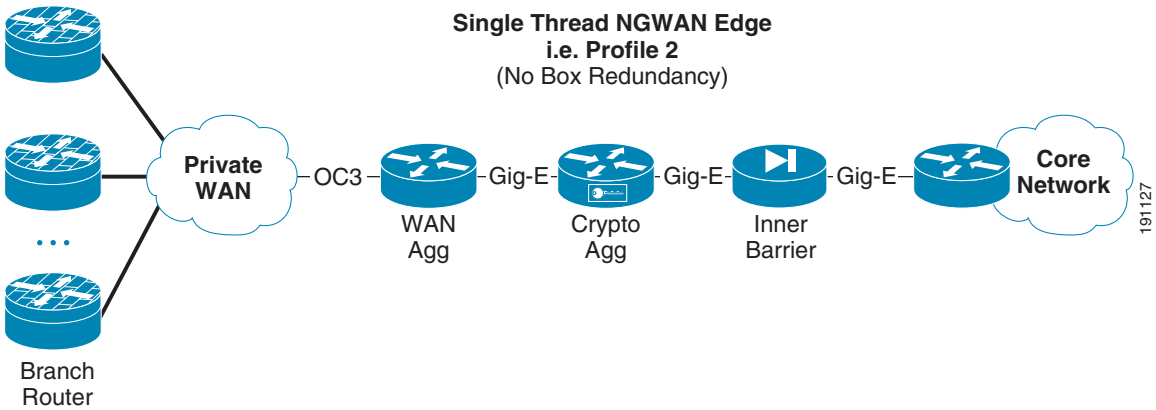
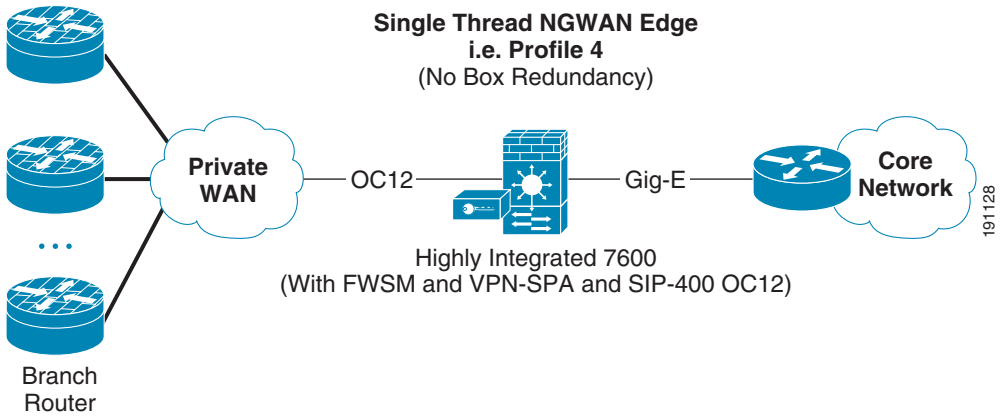


Figure 16 Single-Threaded OC12 Solution



In both Figure 15 and Figure 16, a single thread of devices is implemented and provide no box level redundancy in that site.

If multi-site redundancy is required, two occurrences of either single-threaded or multi-threaded can be implemented in two or more separate physical locations. The core network dynamic routing protocol is used to choose a particular site for the active connection and the other for backup purposes (chosen by prefer RP preferences). It is important that routes to and from the core are symmetrical and that both the call and response traverse the same path (through the same NGWAN edge location) because the inner barrier is a stateful inspection machine. Asymmetric routing between locations results in a high amount of packet or connection loss and packet re-ordering, and should be avoided. Also of critical importance is that each branch LAN subnet be distinct and *not* summarized with other branches in the RP. This allows the core RP to failover one particular branch without affecting all branches in a summary.

The likely failure point is usually the WAN circuits themselves. With this in mind, a single-threaded system in two distinct sites is usually enough redundancy for most customers, but if both box level and site level is required, two or more multi-threaded sites are possible but more costly in equipment and complexity. (See Figure 17 and Figure 18.)

Figure 17 Multi-Site Single-Threaded OC3 Solution

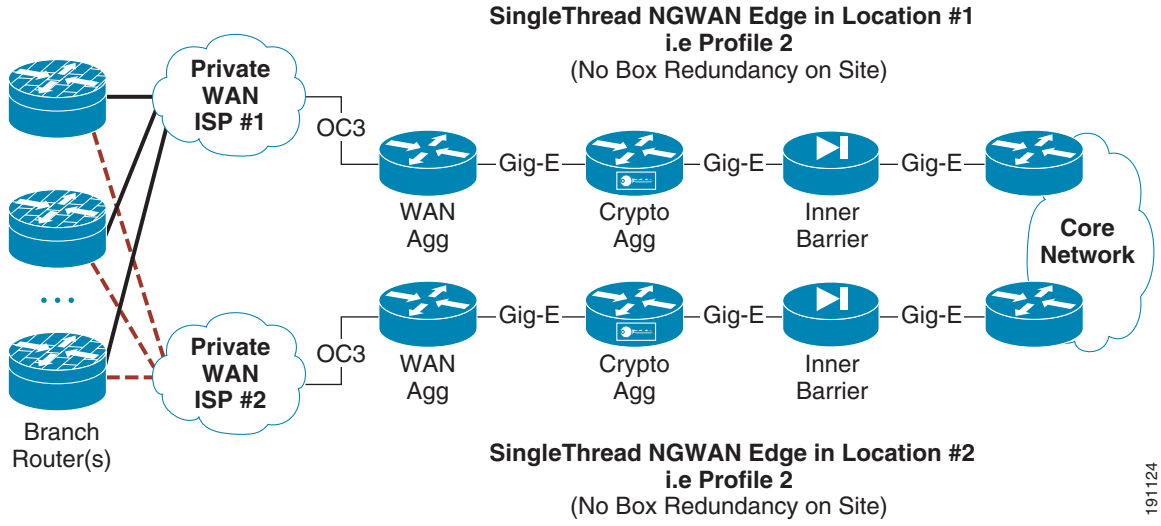
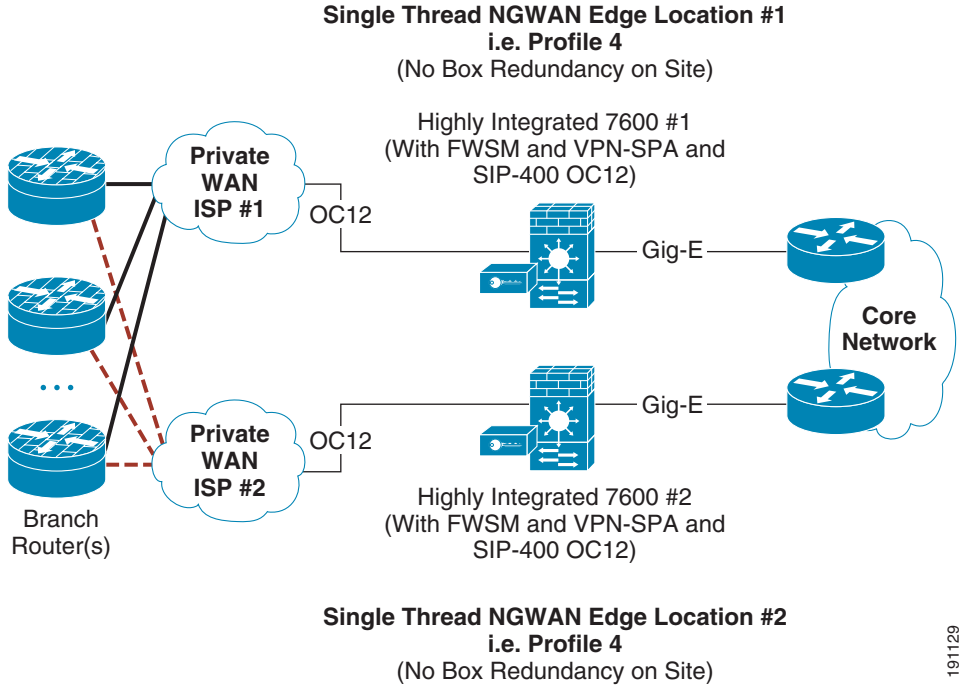


Figure 18 Multi-Site Single-Threaded OC12 Solution



Failure is detected and converged by the routing protocol between a branch router via the VPN IGP and the crypto aggregation devices; this is described in more detail in Routing Protocol Implementation, page 74. This is imported to the proper function of the site failover mechanism.

Network Fundamentals

This section addresses two fundamental concepts that are not specific to infrastructure protection but must be addressed because they are key components to the proper network function. These concepts are QoS and a dynamic routing protocol.

QoS for WAN Aggregation Routers

The profiles in this document use one or more OC3 or OC12 links to a WAN service provider network. The WAN service provider can be an Internet Service Provider (ISP), an MPLS VPN service provider, or a traditional private network (based on HDLC, PPP, Frame Relay, or ATM). It is assumed that the service provider connects the branch routers at some lesser bandwidth; for example, T1 or T3.

It is assumed that the service provider implements a QoS service policy that is coordinated with the requirements of the enterprise customer. The service provider is expected to enable QoS on the WAN links to the branch offices as well as on the OC3 or OC12 links to the campus headend. The enterprise customer also enables QoS on the branch routers and at the WAN aggregation routers at the campus.

Cisco Powered Network (CPN) certified service providers have next-generation networks that enable QoS between the service provider and enterprise network. Enterprises can select service providers using either the Internet or an MPLS core to transport voice, video, and data over the enterprise VPN. To locate these service providers, see the Cisco Powered Network—Find Recommended Service Providers URL at the following URL: http://www.cisco.com/pcgi-bin/cpn/cpn_pub_bassrch.pl and select “IP VPN Multiservice” in the dialog box.

The configuration example in this section includes a configuration that is consistent with a V3PN implementation with the addition of a scavenger class to provide isolation of traffic anomalies.

For more information on enterprise QoS and V3PN, see the specific design guide at the following URL: http://www.cisco.com/go/srnd.

The following configuration example illustrates the addition of scavenger class to a V3PN QoS service policy.

- Configuration of QoS on a Cisco 7200VXR platform; this uses the general V3PN QoS map for V3PN-style converged traffic:

```
!
!
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map OC-WAN-wSCAVENGER
 class CALL-SETUP
  bandwidth percent 5
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority percent 33
 class TRANSACTIONAL-DATA
  bandwidth percent 30
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
!
interface tun0
 …
 qos pre-classify
 …
!
interface POS5/0
 description OC3-to-wan-rtr
 …
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
```

- Configuration of Scavenger Class QoS on a Cisco 7600 platform; this uses the general V3PN QoS map for V3PN style converged traffic. QoS pre-class is not available on this platform.

```
!
! Because of the use of SIP-400 card carrier and an POS OC-12 card, some minor
! configuration differences are required to achieve the same effect:
```

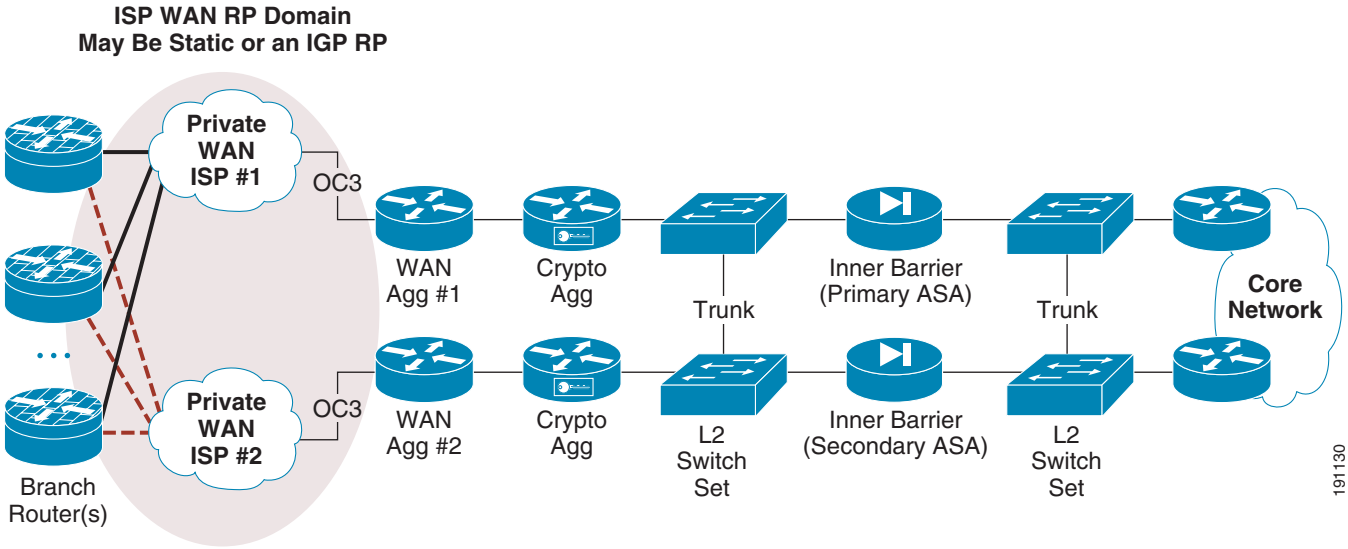
```
!
class-map match-any VOICE
  match ip dscp ef
  match ip precedence 5
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
! The difference between the OC12 QoS map here and the OC3 one on the VXR is that the
! VOICE class can NOT use
! a priority percent or priority bandwidth statement on a SIP-400. So therefore a
! policer in the strict priority queue must be used.
!
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000 conform-action transmit exceed-action
drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
interface POS3/1/0
 description OC12-TO-WAN-RTR
  …
 crypto connect vlan 100
 service-policy output OC12-WAN-wSCAVENGER
!
```

Routing Protocol Implementation

This section addresses the routing protocol implementation at the NGWAN edge, VPN aggregation routers, and within the enterprise network core.

The routing protocol configuration between the WAN service provider and the campus WAN aggregation routers is a static route for the examples in this document. Typically in an actual deployment, static routes or BGP are used in both the ISP and MPLS service provider environments. (See Figure 19.)

Figure 19 RP used to the ISP



The routing protocol implemented within the VPN tunnels (VPN IGP) is EIGRP. EIGRP, being a distance vector protocol, is an excellent choice for hub-and-spoke topologies that are common with IPsec VPNs. The advantages of EIGRP over a link-state protocol such as OSPF include the following:

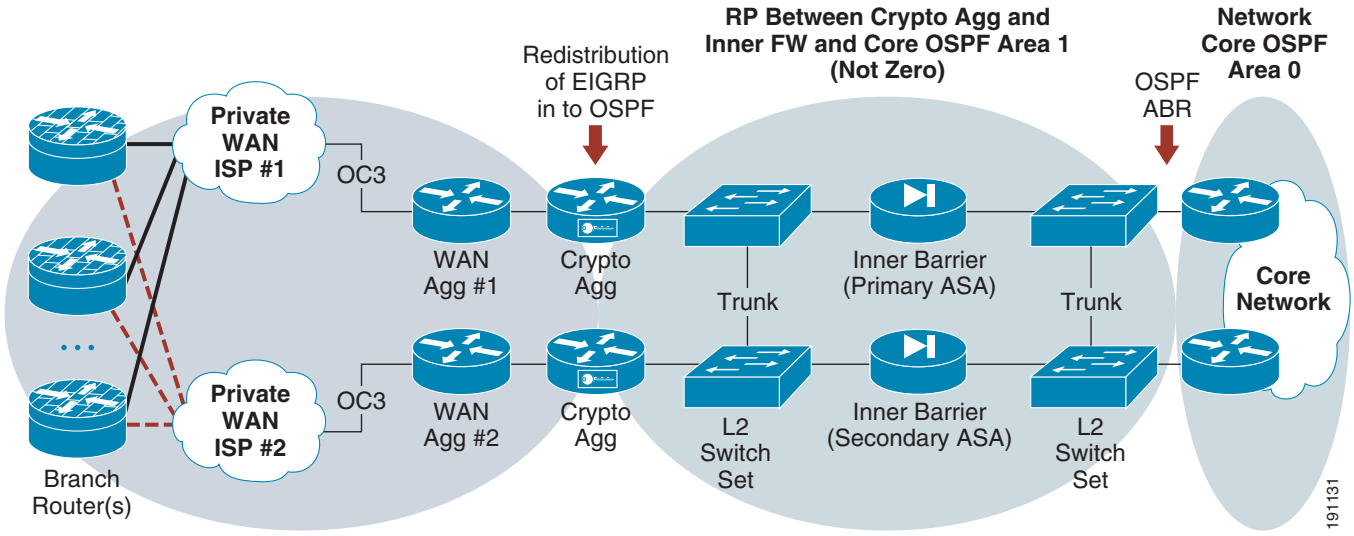
- EIGRP can summarize on a per-interface basis
- No need to flood topology database; there are no AREAS in EIGRP
- EIGRP stub eliminates queries to spokes
- No periodic database synchronization
- EIGRP sends very few updates when configured as STUB and advertising a default (0/0) or summary route to the spokes

To demonstrate how an enterprise customer might implement EIGRP on the crypto aggregation router with OSPF in the core network, EIGRP is redistributed into OSPF. The crypto aggregation router is an OSPF autonomous system border router (ASBR) as it redistributes from EIGRP to OSPF Area 1.

The crypto aggregation, inner barrier firewall, and the enterprise network core are all in OSPF area 1. (See Figure 20.)

It is assumed in the campus network that at least two OSPF ABRs advertise a summary advertisement (area range) into OSPF Area 0. This prevents network instability from being advertised into Area 0.

Figure 20 RPs used for the VPN IGP and from the Crypto Aggregation to the Core

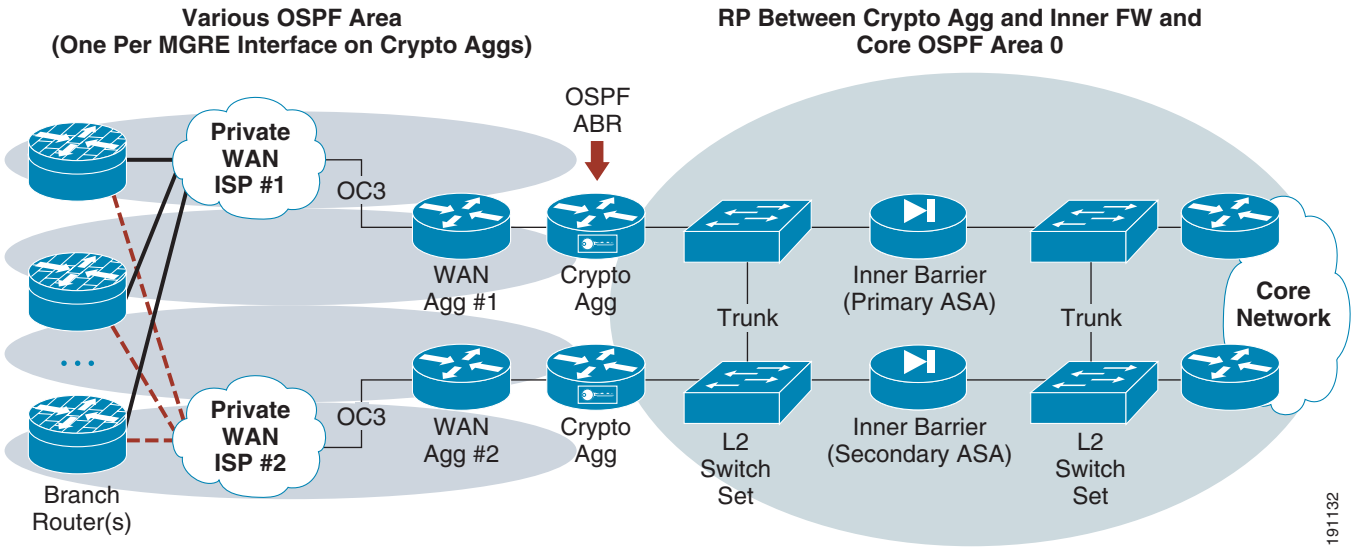


Note that the ASA firewall appliance and the FWSM do not support EIGRP. However, they do support OSPF, so a design that implements OSPF at this spot in the topology is warranted.

To implement site redundancy, the OSPF ABR routers must share a link within Area 1 between these two routers. This allows both ABRs to advertise a summary network but to forward packets to the other ABR over the shared Area 1 link. In the event a single VPN tunnel is down to a branch, the surviving path is through the alternate ABR router. This eliminates black holes because of summarization.

An alternative configuration is to use OSPF entirely and to eliminate EIGRP on the crypto aggregation routers. The major disadvantage to this is the crypto aggregation routers now become OSPF ABRs and are responsible for the summarization into Area 0. Also, the inner barrier firewalls must be in OSPF Area 0. Having firewall devices that are subject to CPU processing spikes because of malicious network traffic as OSPF Area 0 routers represents an exposure to the network core. Figure 21 shows this topology.

Figure 21 OSPF as only RP



Although it is possible to implement, OSPF as the sole RP is not a recommended topology because of the added complexity of areas and the interaction on the inner barrier firewalls.

Scalability Considerations

This section presents the steps required to properly size the NGWAN edge devices to provide a scalable secured NGWAN edge.

Each profile shown in this document is capable of supporting the speed for which it was created or less, and has been tested for this performance in the Cisco lab.

For example:

- Profile 1 and Profile 2 are Cisco 7200VXR-based solutions that support an e-mix of traffic to the OC3 link capacity or less.
- Profile 3 and Profile 4 are Cisco 7600-based solutions that support an e-mix of traffic to the OC12 link capacity or less.

Note Supporting a line rate (such as OC3 or OC12) is defined in this document to be when either ingress or egress capacity is at the point of line congestion. This includes cases where normal QoS policies are engaged. The results predict real-world performance, not necessary the ideal case.

Performance and Scalability Considerations

General scalability considerations are provided to assist you with design requirements. The following are listed in order of importance to the performance and scalability of the NGWAN edge solution.

Packets Per Second

Although bandwidth throughput capacity must be considered, even more important is the packet rate for the connection speeds being terminated or aggregated.

In general, routers and encryption engines have upper boundaries for processing a given number of packets per second (pps). Size of packets used for testing and throughput evaluations can under- or overstate true performance. For example, if a router with a VPN module can handle 20 kpps, 100-byte packets lead to 16 Mbps throughput, while 1300-byte packets at the same packet rate lead to 224 Mbps.

Because of such a wide variance in throughput, pps is a better parameter than bps to determine the forwarding potential of the router. Scalability of the NGWAN edge system is the aggregate forwarding potential of all branches that terminate a tunnel to that headend. Therefore, the aggregate pps from all branches impacts the pps load of that headend.

The traffic mix at the NGWAN edge has an impact on the pps rate, and therefore the performance and scalability of the NGWAN edge. In lab testing, a mix of normal data, transactional data, voice, and sometimes video was used. Most importantly in this traffic mix, approximately one-third of the network bandwidth is used for RTP traffic (active voice calls). This means a much higher pps rate for the same bps rate when compared to the traditional Internet mix (IMIX) traffic profile because RTP tends to reduce the average packet size.

For more information on V3PN traffic mix, see *Voice and Video Enabled IPsec VPN (V3PN) Design Chapter* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf

Hardware Crypto Acceleration is Required

The use of a hardware crypto accelerator is a requirement to gain voice quality over a VPN topology. Cisco strongly recommends that you implement hardware accelerators at both the crypto aggregation systems and also all connecting branches. The ISR branch routers have built-in crypto accelerators as a default on the motherboards, or can alternately use add-on cards for crypto hardware acceleration.

If hardware acceleration is not implemented at the crypto aggregation systems, it adversely affects both performance (voice quality) and scalability (number of pps/bps or number of branches) compared to what is shown in this document.

VPN Topology and Routing Protocol Design

The VPN topology and corresponding dynamic routing protocol design has a major impact on the number of branches that a crypto headend can aggregate. A point-to-point GRE interface can only support one routing neighbor per interface. Often the routing protocol design limitation affects the number of routing neighbors that a multi-point tunnel (mGRE) interface used in DMVPN can support. This is even more important when OSPF is chosen as the VPN IGP routing protocol, because the number of neighbors in an area must be considered. For specifics on the various VPN topologies, see the respective design guide for the scalability of that particular VPN topology before implementing in a secure NGWAN edge architecture.

WAN Throughput

The WAN interface bandwidth capacity may become the limiting factor in most of the secure NGWAN edge profiles shown in this document.

To clarify, end user network data traffic is not usually symmetric in the amount and size of packets upstream and downstream from the NGWAN edge. This is typical with data applications. Consider a branch user with a web browser surfing an intranet web server. The user makes a small HTTP get request to the web server in the core network, but the server responds with an HTML page and graphics. The result is a traffic imbalance between the single packet transmitted and the many large packets received. It is considered normal for the headend WAN interface transmit limit to fill before the receive limit, because most data is stored in the enterprise network data center and the branches are just accessing it. VoIP does not follow this asymmetric size behavior, and does cause an even amount of traffic both upstream and downstream for a given RTP stream because voice is a full duplex application. Even on mute, a phone generates the same load as one transmitting audio.

Therefore, if either the transmit or receive limit of the WAN interface is approached and the normal QoS policies are engaged and dropping traffic, the pipe should be considered full. It is not expected to fill the link completely in both directions, because real-world traffic does not actually act in that manner.

Level and Type of Logging of Security Mechanisms

With any facilities that do syslogging (such as logging ACL denies), depending on the level and type of logging, it may yield an extensive amount of data output to the internal syslog buffer or to a remote syslog server. It can cause the platform to spend too many system resources on logging and not enough on forwarding packets. Also, this logging may cause some devices to leave the Cisco Express

Forwarding path and go to process mode, on denies that are logged in the iACL, which may further degrade performance. Packets that are destined to be dropped by an ACL (with a log statement on that deny) are not switched but are dropped. The creation of the log entries on the deny statement at an extremely high rate is a potential issue if not rate-limited.

Use logging rate limiting to help mitigate this problem on the Cisco 7200VXR platform and OAL on the Cisco 7600 platforms. However, if the NGWAN edge is under extremely heavy DoS attack, even rate limiting or off loading may not be enough to guarantee normal performance.

No systems can fully guarantee non-degraded performance under any type or number of DoS attacks, so Cisco strongly recommends that the solution administrator create a service-level agreement (SLA) with the customer base in such a way so as to not guarantee perfect performance under attack. However, you should still take the steps described in this document to help lessen the amount of damage and likelihood of DoS attacks in the event they occur.

IPsec Encryption Throughput

The throughput capacity of the IPsec encryption engine in each platform must be considered for scalable designs because each packet that is encrypted must traverse through the encryption engine.

Therefore, encryption throughput must consider the bi-directional speed of the WAN link for the maximum amount of encrypted data to be expected. Examples are shown in the Table 6.

Table 6 Headend Connection Speeds

Connection Type	Wan Speed Uni-directional (in Mbps)	Encrypted Bi-directional Throughput Required (in Mbps)
OC3	155	310
OC12	622	1244

Software Releases Evaluated

Table 7 lists the software releases that were used in the performance and functionality testing.

Table 7 Software Releases Evaluated

Cisco Product Family	SW Release
Cisco 7600	Cisco IOS 12.2(18)SXF2 *s72033-advipservicesk9_wan-mz.122-18.SXF2* *c7600-fpd-pkg.122-18.SXF2.pkg*
Cisco 7200VXR	Cisco IOS 12.4(4)XD3 *c7200p-adventerprisek9-mz.124-4.XD3.bin* *c7200-fpd-pkg.124-4.XD3.pkg*
Cisco ASA	PIXOS 7.1.1 *asa711-k8.bin* *asdm511.bin*
Cisco Firewall Service Module	FWSM 3.1.1 *c6svc-fwm-k9.3-1-1.bin*

Table 7 Software Releases Evaluated (continued)

Cisco 7301	Cisco IOS 12.3(14)T7 *c7301-jk9s-mz.123-14.T7.bin*
Cisco 7304	Cisco IOS 12.2(28)SB2 *c7300-a3jk91s-mz.122-28.SB2.bin* *c7304-fpd-pkg.122-28.SB2.pkg*
Cisco Catalyst 3560	Cisco IOS 122-25.SEE *c3560-advipservicesk9-mz.122-25.SEE*

Before selecting Cisco IOS software, perform the appropriate research on CCO, and if you have technical questions, consult with Cisco Customer Advocacy (TAC).

Note If you wish to use SSH for "secure CLI device administration", it is important to make sure the SSH is supported in the images you choose.

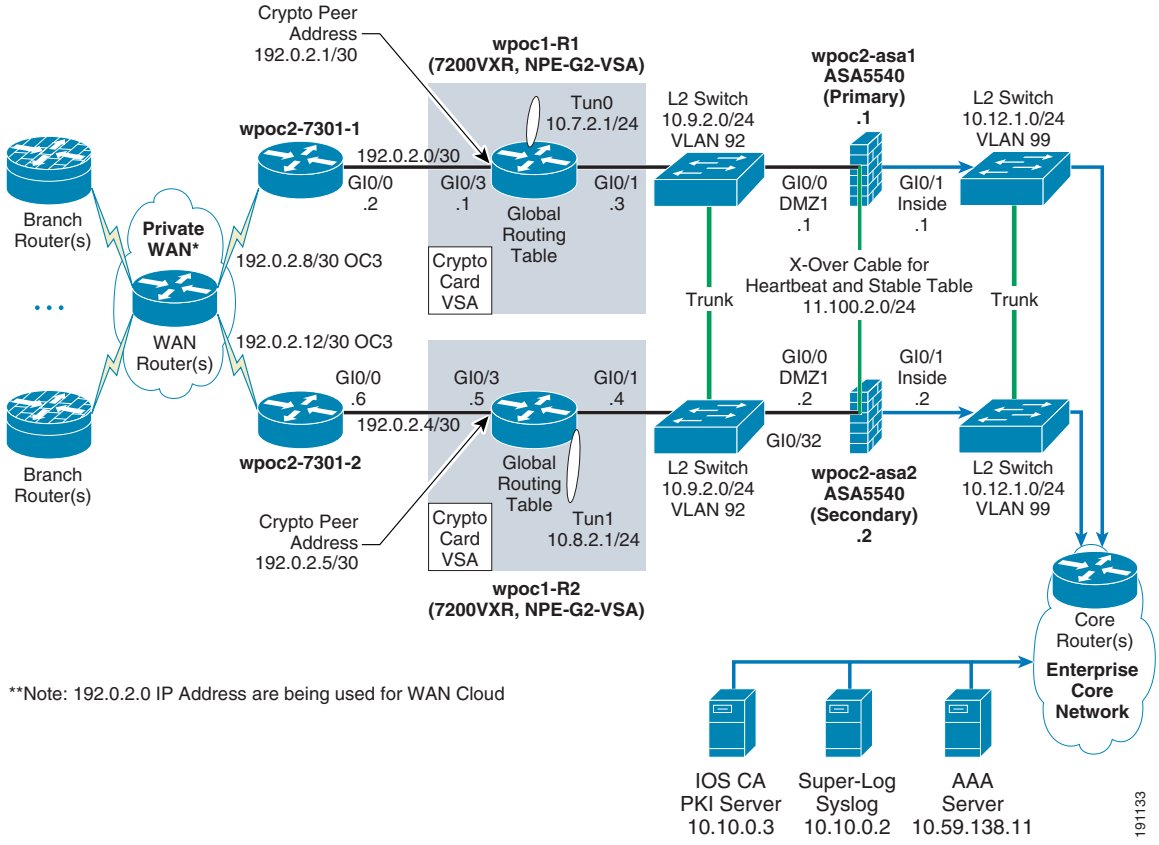
Test Bed Configuration Files

The configurations for the NGWAN edge gear are listed below in the following sections. Note that these configurations have been extracted from real configurations used in Cisco testing. They are provided as a reference only.

Profile 1 Configurations

These configurations uses L2 switches (see L2 Switch Configurations for all Profiles, page 169). Figure 22 shows a network diagram of the Profile 1 network configuration.

Figure 22 Profile 1 (OC3) Multi-Thread in One Site (Three-Tier Solution)



**Note: 192.0.2.0 IP Address are being used for WAN Cloud

Profile 1 and Profile 2 are very similar but have some configuration and performance differences. The basic difference between Profile 1 and Profile 2 is whether the WAN function is integrated in the crypto aggregation system or as a separate dedicated WAN router.

Profile 1 uses a dedicated WAN router, so therefore the following is true:

- The crypto aggregation router and the WAN router are GigE connected.
- The crypto aggregation router does not do QoS or Scavenger Class QoS, but rather the WAN router does instead.
- The crypto aggregation router needs to NAT the syslog server and TACACS server ports to ports on the crypto peer address to make sure that only the LAN side of the WAN router can access those ports (using a new ACL named *Protect-syslog-AAA* on the GigE interface to the WAN router).
- The crypto aggregation router is the NTP clock source for the WAN router.
- The mGRE tunnel interface on the crypto aggregation system is sourced from the outside LAN interface (gi0/3 in the example).
- The crypto aggregation router needs to add a network statement for OSPF area 1 for the Gi0/3 LAN on the respective connected crypto aggregation system. This is so that the WAN router interface IP address has a network path back from the AAA and syslog servers in the core.
- The WAN router uses the outer barrier and the iACL (the example uses the ACL named *InfraProt*)
- The WAN router performs the QoS and Scavenger Class QoS.

- The WAN router accesses the super-log syslog server via the NAT-ed port on the crypto aggregation router.
- The WAN router accesses the AAA server via the NAT-ed port on the crypto aggregation router.
- The WAN router CoPP policy does not need to include VPN or IGP classes because those particular items do not terminate on the WAN router.
- The inner barrier firewall (ASA 5540) must add some rules to the ACL to allow the LAN IP of the WAN router to access the internal AAA server and internal syslog super-log server in the core.

Profile 1—Full Configuration for Cisco 7200VXR Crypto Aggregation Routers

Crypto Agg (Headend #1)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc1-r1
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$EvUN$ppamSuhtGoiqPk.N/DNeW/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/1
ip ssh version 2
!
```

```
!
!
key chain 1
 key 1
  key-string 7 05080F1C2243
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 16 nvram:wpoc3-r1#3116.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
controller ISA 0/1
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
 match access-group name coppacl-vpn
class-map match-all coppclass-igp
 match access-group name coppacl-igp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
!
!
policy-map copp-policy
  class coppclass-igp
  class coppclass-filemanagement
  class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
  class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
  class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
```

```
    conform-action transmit
    exceed-action drop
  class coppclass-vpn
  class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
!
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
!
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.2.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 qos pre-classify
 tunnel source GigabitEthernet0/3
 tunnel mode gre multipoint
 tunnel key 105600
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description to-ASA
 ip address 10.9.2.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
 ip ospf authentication message-digest
 ip ospf authentication-key 7 104D000A0618
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
```

```
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/3
 description to-wan-rtr
 ip address 192.0.2.1 255.255.255.252
 ip access-group Protect-syslog-AAA in
 ip verify unicast reverse-path
 no ip redirects
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS5/0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
!
router eigrp 1
 passive-interface GigabitEthernet0/1
 passive-interface GigabitEthernet0/3
 passive-interface POS5/0
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.2.3
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface POS5/0
 passive-interface Tunnel0
 network 10.2.0.0 0.0.255.255 area 1
 network 10.7.2.0 0.0.0.255 area 1
 network 10.8.2.0 0.0.0.255 area 1
 network 10.9.2.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.1.0 0.0.0.255 area 1
```

```
 network 192.0.2.0 0.0.0.3 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.2
no ip http server
no ip http secure-server
!
!
ip nat inside source static tcp 10.59.138.11 49 interface GigabitEthernet0/3 49
ip nat inside source static udp 10.10.0.2 514 interface GigabitEthernet0/3 514
!
ip access-list extended Protect-syslog-AAA
 remark ------------------------------------------------------
 remark ONLY allow the wan router to access the nat-ed ports for tacacs or syslog and ntp
 permit udp host 192.0.2.2 host 192.0.2.1 eq syslog
 permit tcp host 192.0.2.2 host 192.0.2.1 eq tacacs
 permit udp host 192.0.2.2 host 192.0.2.1 eq ntp
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
 permit icmp any host 192.0.2.1 echo
 permit icmp any host 192.0.2.1 packet-too-big
 permit icmp any host 192.0.2.1 unreachable
 permit icmp any host 192.0.2.1 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.1 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.1
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.2.0 0.0.0.255 host 10.9.2.3
 permit ospf 10.7.2.0 0.0.0.255 host 10.7.2.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
 permit eigrp 10.0.0.0 0.255.255.255 host 10.7.2.1
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
```

```
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
ip access-list extended route-redist-ACL
 permit ip 10.2.0.0 0.0.255.255 any
 deny   ip any any
!
logging alarm informational
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15362816
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
!
!
tacacs-server host 10.59.138.11 key 7 070C285F4D06
tacacs-server timeout 10
tacacs-server directed-request
!
control-plane
 service-policy input copp-policy
!
call admission limit 70
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
ntp clock-period 17180803
```

```
ntp server 10.10.0.1 source GigabitEthernet0/1 prefer
!
end
!
```

Crypto Agg (Headend #2)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc1-r2
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$uat5$SCrYLACqx.vS4Wx9ffei21
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/1
ip ssh logging events
ip ssh version 2
!
!
!
key chain 1
 key 1
  key-string 7 060506324F41
!
!
!
```

```
!
!
!
!
!
!
!
!
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 17 nvram:wpoc3-r1#3117.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
controller ISA 0/1
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
 match access-group name coppacl-vpn
class-map match-all coppclass-igp
 match access-group name coppacl-igp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
!
!
policy-map copp-policy
  class coppclass-igp
  class coppclass-filemanagement
  class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
  class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
  class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
!
!
```

```
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
!
!
!
!
interface Tunnel1
 description Tunnel1
 bandwidth 1000000
 ip address 10.8.2.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 delay 60000
 qos pre-classify
 tunnel source GigabitEthernet0/3
 tunnel mode gre multipoint
 tunnel key 105601
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description to-ASA
 ip address 10.9.2.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
 ip ospf authentication message-digest
 ip ospf authentication-key 7 00071A150754
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
```

```
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/3
 description to-wan-rtr
 ip address 192.0.2.5 255.255.255.252
 ip access-group Protect-syslog-AAA in
 ip verify unicast reverse-path
 no ip redirects
 no ip proxy-arp
 ip nat outside
 ip virtual-reassembly
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS5/0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
!
router eigrp 1
 passive-interface GigabitEthernet0/1
 passive-interface GigabitEthernet0/3
 passive-interface POS5/0
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.2.4
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface POS5/0
 passive-interface Tunnel1
 network 10.2.0.0 0.0.255.255 area 1
 network 10.7.2.0 0.0.0.255 area 1
 network 10.8.2.0 0.0.0.255 area 1
 network 10.9.2.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.1.0 0.0.0.255 area 1
 network 192.0.2.4 0.0.0.3 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.6
no ip http server
no ip http secure-server
!
!
```

```
ip nat inside source static udp 10.10.0.2 514 interface GigabitEthernet0/3 514
ip nat inside source static tcp 10.59.138.11 49 interface GigabitEthernet0/3 49
!
ip access-list extended Protect-syslog-AAA
 remark ------------------------------------------------------
 remark ONLY allow the wan router to access the nat-ed ports for tacacs or syslog and ntp
 permit udp host 192.0.2.6 host 192.0.2.5 eq syslog
 permit tcp host 192.0.2.6 host 192.0.2.5 eq tacacs
 permit udp host 192.0.2.6 host 192.0.2.5 eq ntp
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
 permit icmp any host 192.0.2.5 echo
 permit icmp any host 192.0.2.5 packet-too-big
 permit icmp any host 192.0.2.5 unreachable
 permit icmp any host 192.0.2.5 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.5 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.5
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.2.0 0.0.0.255 host 10.9.2.4
 permit ospf 10.8.2.0 0.0.0.255 host 10.8.2.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
 permit eigrp 10.0.0.0 0.255.255.255 host 10.8.2.1
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
ip access-list extended route-redist-ACL
 permit ip 10.2.0.0 0.0.255.255 any
 deny   ip any any
```

```
!
logging alarm informational
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15362816
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
!
!
tacacs-server host 10.59.138.11 key 7 121A0C041104
tacacs-server timeout 10
tacacs-server directed-request
!
control-plane
 service-policy input copp-policy
!
call admission limit 70
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
ntp clock-period 17180767
ntp server 10.10.0.1 source GigabitEthernet0/1
!
end
!
```

Profile 1—Full Configuration for Cisco 7301 WAN Routers

WAN Agg 7301 (Headend #1)

```
!

version 12.3
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc2-7301-1
!
boot-start-marker
boot system disk0:c7301-jk9s-mz.123-14.T7.bin
boot-end-marker
!
no logging queue-limit
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$8J4i$/5vYsag2yIcqv6W6QyxJO.
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
no ip dhcp use vrf connected
!
!
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/0
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
 match access-group name coppacl-bgp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all coppclass-management
 match access-group name coppacl-management
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map copp-policy
description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
 class coppclass-filemanagement
 class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
 class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
 class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
policy-map OC-WAN-wSCAVENGER
 class CALL-SETUP
  bandwidth percent 5
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority percent 33
 class TRANSACTIONAL-DATA
```

```
  bandwidth percent 30
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
!
!
no crypto isakmp ccm
!
!
!
!
interface GigabitEthernet0/0
 description to-wpoc1-r1
 ip address 192.0.2.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip tcp adjust-mss 1400
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/1
 no ip address
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS1/0
 description to-WAN-wpoc1-r0
 ip address 192.0.2.9 255.255.255.252
 ip access-group InfraProt in
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.10
!
no ip http server
no ip http secure-server
```

```
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 remark this line is no longer needed -> permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
 permit icmp any host 192.0.2.1 echo
 permit icmp any host 192.0.2.1 packet-too-big
 permit icmp any host 192.0.2.1 unreachable
 permit icmp any host 192.0.2.1 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.127 host 192.0.2.9 eq bgp
 permit tcp 192.0.2.0 0.0.0.127 eq bgp host 192.0.2.9
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
logging 192.0.2.1
access-list 10 permit 10.0.0.0 0.255.255.255
```

```
access-list 10 permit 192.0.2.0 0.0.0.3
access-list 10 permit 192.0.2.4 0.0.0.3
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
!
tacacs-server host 192.0.2.1
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 00071A150754
!
!
control-plane
 service-policy input copp-policy
!
call admission limit 70
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 password 7 13061E010803
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 00071A150754
 logging synchronous
 transport input ssh
!
ntp clock-period 17179962
ntp server 192.0.2.1 source GigabitEthernet0/0 prefer
!
end
!
```

WAN Agg 7301 (Headend #2)

```
!
version 12.3
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc2-7301-2
!
boot-start-marker
```

```
boot system disk0:c7301-jk9s-mz.123-14.T7.bin
boot-end-marker
!
no logging queue-limit
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$lIU9$7jh9IVpsotS7hqAeJBqm81
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
clock calendar-valid
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
no ip dhcp use vrf connected
!
!
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/0
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-any VOICE
 match ip dscp ef
```

```
 match ip precedence 5
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-all coppclass-management
 match access-group name coppacl-management
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map copp-policy
description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
 class coppclass-filemanagement
 class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
 class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
 class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
 class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
policy-map OC-WAN-wSCAVENGER
 class CALL-SETUP
  bandwidth percent 5
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority percent 33
 class TRANSACTIONAL-DATA
  bandwidth percent 30
 class SCAVENGER
  bandwidth percent 1
 class class-default
  bandwidth percent 25
  random-detect
!
!
no crypto isakmp ccm
!
!
!
!
interface GigabitEthernet0/0
```

```
 description to-wpoc1-r2
 ip address 192.0.2.6 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/1
 no ip address
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS1/0
 description to-WAN-wpoc1-r0
 ip address 192.0.2.13 255.255.255.252
 ip access-group InfraProt in
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.14
!
no ip http server
no ip http secure-server
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
```

```
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 remark this line is no longer needed -> permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
 permit icmp any host 192.0.2.5 echo
 permit icmp any host 192.0.2.5 packet-too-big
 permit icmp any host 192.0.2.5 unreachable
 permit icmp any host 192.0.2.5 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.127 host 192.0.2.13 eq bgp
 permit tcp 192.0.2.0 0.0.0.127 eq bgp host 192.0.2.13
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
logging 192.0.2.5
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 permit 192.0.2.0 0.0.0.3
access-list 10 permit 192.0.2.4 0.0.0.3
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
!
tacacs-server host 192.0.2.5
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 110A1016141D
!
!
control-plane
 service-policy input copp-policy
```

```
!
call admission limit 70
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 password 7 045802150C2E
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 121A0C041104
 logging synchronous
 transport input ssh
!
ntp clock-period 17179908
ntp server 192.0.2.5 source GigabitEthernet0/0 prefer
!
end
!
```

Profile 1—Configuration for Cisco ASA 5540s

Inner Barrier Firewall #1 (Active in Stateful Failover Pair)

```
!
!
hostname wpoc2-asa1
domain-name ese.cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface GigabitEthernet0/0
 description DMZ1
 nameif dmz1
 security-level 50
 ip address 10.9.2.1 255.255.255.0 standby 10.9.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 description inside
 nameif inside
 security-level 100
 ip address 10.12.1.1 255.255.255.0 standby 10.12.1.2
```

```
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/2
 description OUTSIDE
 shutdown
 nameif outside
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!
passwd 9jNfZuG3TC5tCVH0 encrypted
banner motd Warning this is a private system.
banner motd Unauthorized access is prohibited.
banner motd Violators will be prosecuted.
banner motd .
boot system disk0:/asa711-k8.bin
ftp mode passive
clock timezone est -5
clock summer-time edt recurring
dns server-group DefaultDNS
 domain-name ese.cisco.com
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
access-list dmz1_access_in extended permit tcp host 192.0.2.4 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.4 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.2.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.7.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit tcp host 192.0.2.2 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.2 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit tcp host 192.0.2.6 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.6 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended deny ip any any log
pager lines 24
logging enable
logging timestamp
logging standby
logging buffered informational
logging trap notifications
logging asdm informational
logging host inside 10.10.0.2
mtu dmz1 1500
mtu inside 1500
mtu outside 1500
mtu management 1500
ip verify reverse-path interface dmz1
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover key *****
failover replication http
failover link failover GigabitEthernet0/3
```

```
failover interface ip failover 11.100.2.1 255.255.255.0 standby 11.100.2.2
asdm image disk0:/asdm511.bin
no asdm history enable
arp timeout 14400
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.1.0 10.12.1.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0
access-group dmz1_access_in in interface dmz1
access-group inside_access_in in interface inside
!
router ospf 100
 network 10.0.0.0 255.0.0.0 area 1
 area 1 authentication message-digest
 router-id 10.9.2.1
 log-adj-changes
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server tacacs-group protocol tacacs+
aaa-server tacacs-group host 10.59.138.11
 key cisco
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
aaa authentication enable console tacacs-group LOCAL
aaa authentication ssh console tacacs-group LOCAL
aaa authentication telnet console tacacs-group LOCAL
aaa authentication serial console tacacs-group LOCAL
aaa authorization command tacacs-group LOCAL
aaa accounting command tacacs-group
aaa accounting ssh console tacacs-group
aaa accounting telnet console tacacs-group
http server enable
http 10.0.0.0 255.0.0.0 dmz1
http 10.0.0.0 255.0.0.0 inside
snmp-server host inside 10.10.0.4 poll community NMScommunity version 2c
snmp-server location inner-barrier
snmp-server contact admin@company.com
snmp-server community NMScommunity
telnet timeout 1
ssh scopy enable
ssh 10.0.0.0 255.0.0.0 dmz1
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 3
console timeout 3
dhcpd lease 3600
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect skinny
  inspect esmtp
  inspect sqlnet
```

```
  inspect sip
  inspect dns maximum-length 512
  inspect netbios
  inspect sunrpc
  inspect tftp
  inspect xdmcp
!
service-policy global_policy global
ntp server 10.10.0.1 source inside prefer
Cryptochecksum:81d4f1027607d4f760235b64e9d1ff5f
: end
!
```

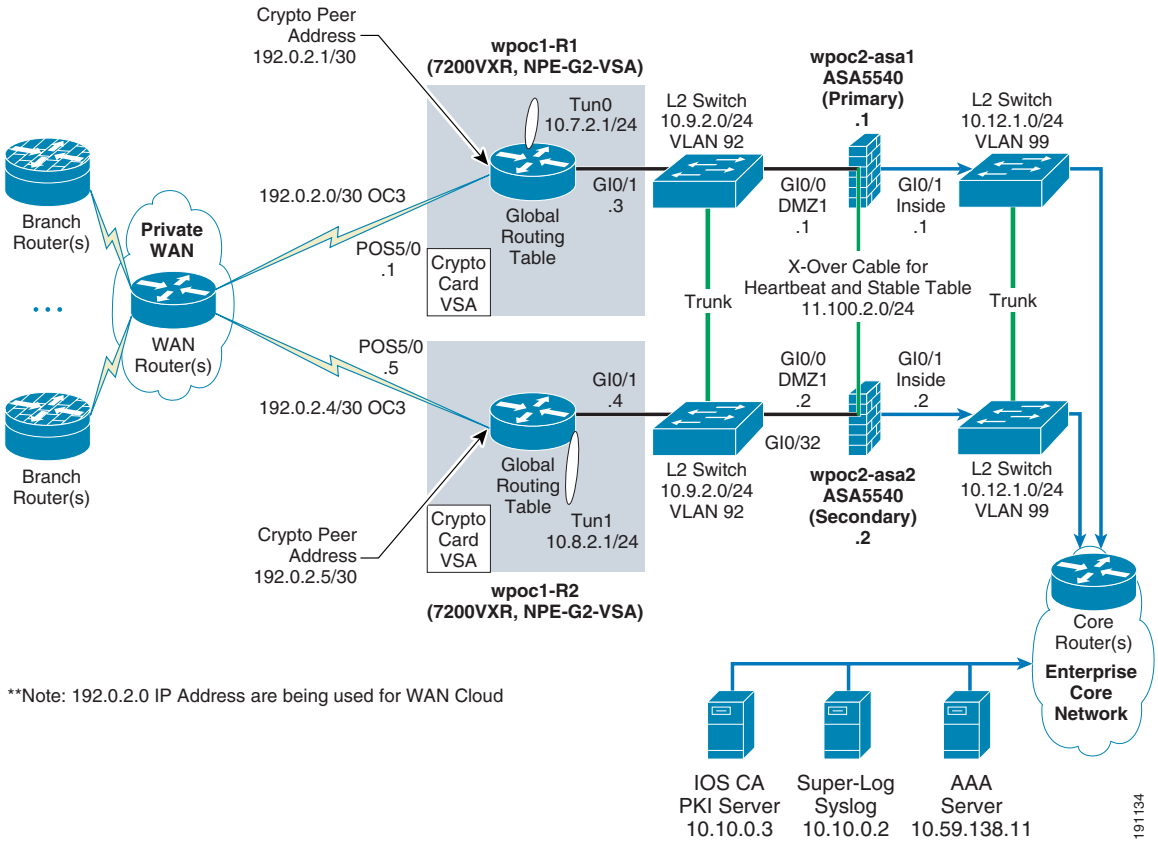
Inner Barrier Firewall #2 (Standby in Stateful failover pair)

```
!
! Config is same as Active above (except for the following):
failover lan unit secondary
!
```

Profile 2 Configurations

These configurations use L2 switches (see L2 Switch Configurations for all Profiles, page 169). Figure 23 shows a network diagram of the Profile 2 network configuration.

Figure 23 Profile 2 (OC3) Multi-Thread in One Site (Two-Tier Solution)



**Note: 192.0.2.0 IP Address are being used for WAN Cloud

Profile 2—Full Configuration for Cisco 7200VXR Integrated–Crypto Aggregation and WAN Systems

Crypto Agg and WAN Router (Headend #1)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc1-r1
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$EvUN$ppamSuhtGoiqPk.N/DNeW/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/1
ip ssh logging events
ip ssh version 2
!
!
!
key chain 1
 key 1
  key-string 7 05080F1C2243
!
!
!
!
!
!
```

```
!
!
!
!
!
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 16 nvram:wpoc3-r1#3116.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
controller ISA 0/1
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
 match access-group name coppacl-vpn
class-map match-all coppclass-igp
 match access-group name coppacl-igp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map copp-policy
  class coppclass-igp
  class coppclass-filemanagement
  class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
  class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
  class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
```

```
    conform-action transmit
    exceed-action drop
  class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class coppclass-vpn
  class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
policy-map OC-WAN-wSCAVENGER
  class CALL-SETUP
  bandwidth percent 5
  class INTERNETWORK-CONTROL
  bandwidth percent 5
  class VOICE
  priority percent 33
  class TRANSACTIONAL-DATA
  bandwidth percent 30
  class SCAVENGER
  bandwidth percent 1
  class class-default
  bandwidth percent 25
  random-detect
!
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
!
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.2.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 qos pre-classify
 tunnel source POS5/0
 tunnel mode gre multipoint
 tunnel key 105600
```

```
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description to-ASA
 ip address 10.9.2.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 104D000A0618
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/3
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS5/0
 description OC3-to-wan-rtr
 ip address 192.0.2.1 255.255.255.252
 ip access-group InfraProt in
 ip verify unicast reverse-path
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
router eigrp 1
 passive-interface GigabitEthernet0/1
 passive-interface POS5/0
 network 10.0.0.0
 no auto-summary
!
```

```
router ospf 100
 router-id 10.9.2.3
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface POS5/0
 passive-interface Tunnel0
 network 10.2.0.0 0.0.255.255 area 1
 network 10.7.2.0 0.0.0.255 area 1
 network 10.8.2.0 0.0.0.255 area 1
 network 10.9.2.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.1.0 0.0.0.255 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.2
no ip http server
no ip http secure-server
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
 permit icmp any host 192.0.2.1 echo
 permit icmp any host 192.0.2.1 packet-too-big
 permit icmp any host 192.0.2.1 unreachable
 permit icmp any host 192.0.2.1 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.1 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.1
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
```

```
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.2.0 0.0.0.255 host 10.9.2.3
 permit ospf 10.7.2.0 0.0.0.255 host 10.7.2.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
 permit eigrp 10.0.0.0 0.255.255.255 host 10.7.2.1
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.1
 permit udp any host 192.0.2.1 eq isakmp
 permit udp any host 192.0.2.1 eq non500-isakmp
 permit esp any host 192.0.2.1
ip access-list extended route-redist-ACL
 permit ip 10.2.0.0 0.0.255.255 any
 deny   ip any any
!
logging alarm informational
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15362816
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
!
!
tacacs-server host 10.59.138.11 key 7 070C285F4D06
tacacs-server timeout 10
tacacs-server directed-request
!
control-plane
 service-policy input copp-policy
!
call admission limit 70
!
!
!
!
```

```
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
ntp clock-period 17180669
ntp server 10.10.0.1 source GigabitEthernet0/1 prefer
!
end
!
```

Crypto Agg and WAN Router (Headend #2)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc1-r2
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
no logging console
enable secret 5 $1$uat5$SCrYLACqx.vS4Wx9ffei21
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
```

```
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/1
ip ssh logging events
ip ssh version 2
!
!
!
key chain 1
 key 1
  key-string 7 060506324F41
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 17 nvram:wpoc3-r1#3117.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
controller ISA 0/1
!
class-map match-all coppclass-critical-app
 match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
 match access-group name coppacl-vpn
class-map match-all coppclass-igp
 match access-group name coppacl-igp
class-map match-all coppclass-bgp
 match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
 match access-group name coppacl-monitoring
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-all coppclass-filemanagement
 match access-group name coppacl-filemanagement
class-map match-all coppclass-management
 match access-group name coppacl-management
```

```
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
 match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
 match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
 match ip dscp af21
 match ip precedence 2
!
!
policy-map copp-policy
  class coppclass-igp
  class coppclass-filemanagement
  class coppclass-bgp
  police cir 80000 bc 8000 be 8000
    conform-action transmit
    exceed-action drop
  class coppclass-management
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
  class coppclass-monitoring
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class coppclass-critical-app
  police cir 500000 bc 5000 be 5000
    conform-action transmit
    exceed-action drop
  class class-default
  police cir 10000000 bc 100000 be 100000
    conform-action transmit
    exceed-action drop
policy-map OC-WAN-wSCAVENGER
  class CALL-SETUP
  bandwidth percent 5
  class INTERNETWORK-CONTROL
  bandwidth percent 5
  class VOICE
  priority percent 33
  class TRANSACTIONAL-DATA
  bandwidth percent 30
  class SCAVENGER
  bandwidth percent 1
  class class-default
  bandwidth percent 25
  random-detect
!
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
```

```
!
!
!
!
!
!
interface Tunnel1
 description Tunnel1
 bandwidth 1000000
 ip address 10.8.2.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 delay 60000
 qos pre-classify
 tunnel source POS5/0
 tunnel mode gre multipoint
 tunnel key 105601
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/1
 description to-ASA
 ip address 10.9.2.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 00071A150754
 load-interval 30
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description to-wan-rtr
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet0/3
 no ip address
```

```
 no ip redirects
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS5/0
 description OC3-to-wan-rtr
 ip address 192.0.2.5 255.255.255.252
 ip access-group InfraProt in
 ip verify unicast reverse-path
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 max-reserved-bandwidth 100
 service-policy output OC-WAN-wSCAVENGER
!
router eigrp 1
 passive-interface GigabitEthernet0/1
 passive-interface POS5/0
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.2.4
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface POS5/0
 passive-interface Tunnel1
 network 10.2.0.0 0.0.255.255 area 1
 network 10.7.2.0 0.0.0.255 area 1
 network 10.8.2.0 0.0.0.255 area 1
 network 10.9.2.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.1.0 0.0.0.255 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.6
no ip http server
no ip http secure-server
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
```

```
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
 permit icmp any host 192.0.2.5 echo
 permit icmp any host 192.0.2.5 packet-too-big
 permit icmp any host 192.0.2.5 unreachable
 permit icmp any host 192.0.2.5 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.5 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.5
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.2.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.2.0 0.0.0.255 host 10.9.2.4
 permit ospf 10.8.2.0 0.0.0.255 host 10.8.2.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
 permit eigrp 10.0.0.0 0.255.255.255 host 10.8.2.1
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.5
 permit udp any host 192.0.2.5 eq isakmp
 permit udp any host 192.0.2.5 eq non500-isakmp
 permit esp any host 192.0.2.5
ip access-list extended route-redist-ACL
 permit ip 10.2.0.0 0.0.255.255 any
 deny   ip any any
!
logging alarm informational
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
```

```
access-list 10 deny   any log
snmp-server group NMS v3 priv
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15362816
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
!
!
tacacs-server host 10.59.138.11 key 7 121A0C041104
tacacs-server timeout 10
tacacs-server directed-request
!
control-plane
 service-policy input copp-policy
!
call admission limit 70
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
ntp clock-period 17180756
ntp server 10.10.0.1 source GigabitEthernet0/1
!
end
!
```

Profile 2—Full Configuration for Cisco ASA 5540

Inner Barrier Firewall #1 (ACTIVE in Stateful Failover Pair)

```
!
hostname wpoc2-asa1
domain-name ese.cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface GigabitEthernet0/0
 description DMZ1
 nameif dmz1
 security-level 50
 ip address 10.9.2.1 255.255.255.0 standby 10.9.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 description inside
 nameif inside
 security-level 100
 ip address 10.12.1.1 255.255.255.0 standby 10.12.1.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/2
 description OUTSIDE
 shutdown
 nameif outside
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 description LAN/STATE Failover Interface
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!
passwd 9jNfZuG3TC5tCVH0 encrypted
banner motd Warning this is a private system.
banner motd Unauthorized access is prohibited.
banner motd Violators will be prosecuted.
banner motd .
boot system disk0:/asa711-k8.bin
ftp mode passive
clock timezone est -5
clock summer-time edt recurring
dns server-group DefaultDNS
 domain-name ese.cisco.com
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
access-list dmz1_access_in extended permit tcp host 192.0.2.4 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.4 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.2.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.2.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.7.2.0 255.255.255.0 10.0.0.0 255.0.0.0
```

```
access-list dmz1_access_in extended permit tcp host 192.0.2.2 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.2 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit tcp host 192.0.2.6 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.6 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended deny ip any any log
pager lines 24
logging enable
logging timestamp
logging standby
logging buffered informational
logging trap notifications
logging asdm informational
logging host inside 10.10.0.2
mtu dmz1 1500
mtu inside 1500
mtu outside 1500
mtu management 1500
ip verify reverse-path interface dmz1
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover key *****
failover replication http
failover link failover GigabitEthernet0/3
failover interface ip failover 11.100.2.1 255.255.255.0 standby 11.100.2.2
asdm image disk0:/asdm511.bin
no asdm history enable
arp timeout 14400
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.1.0 10.12.1.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0
access-group dmz1_access_in in interface dmz1
access-group inside_access_in in interface inside
!
router ospf 100
 network 10.0.0.0 255.0.0.0 area 1
 area 1 authentication message-digest
 router-id 10.9.2.1
 log-adj-changes
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server tacacs-group protocol tacacs+
aaa-server tacacs-group host 10.59.138.11
 key cisco
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
aaa authentication enable console tacacs-group LOCAL
aaa authentication ssh console tacacs-group LOCAL
aaa authentication telnet console tacacs-group LOCAL
aaa authentication serial console tacacs-group LOCAL
aaa authorization command tacacs-group LOCAL
aaa accounting command tacacs-group
aaa accounting ssh console tacacs-group
aaa accounting telnet console tacacs-group
http server enable
http 10.0.0.0 255.0.0.0 dmz1
http 10.0.0.0 255.0.0.0 inside
snmp-server host inside 10.10.0.4 poll community NMScommunity version 2c
```

```
snmp-server location inner-barrier
snmp-server contact admin@company.com
snmp-server community NMScommunity
telnet timeout 1
ssh scopy enable
ssh 10.0.0.0 255.0.0.0 dmz1
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 3
console timeout 3
dhcpd lease 3600
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect dns maximum-length 512
  inspect netbios
  inspect sunrpc
  inspect tftp
  inspect xdmcp
!
service-policy global_policy global
ntp server 10.10.0.1 source inside prefer
Cryptochecksum:81d4f1027607d4f760235b64e9d1ff5f
: end
!
```

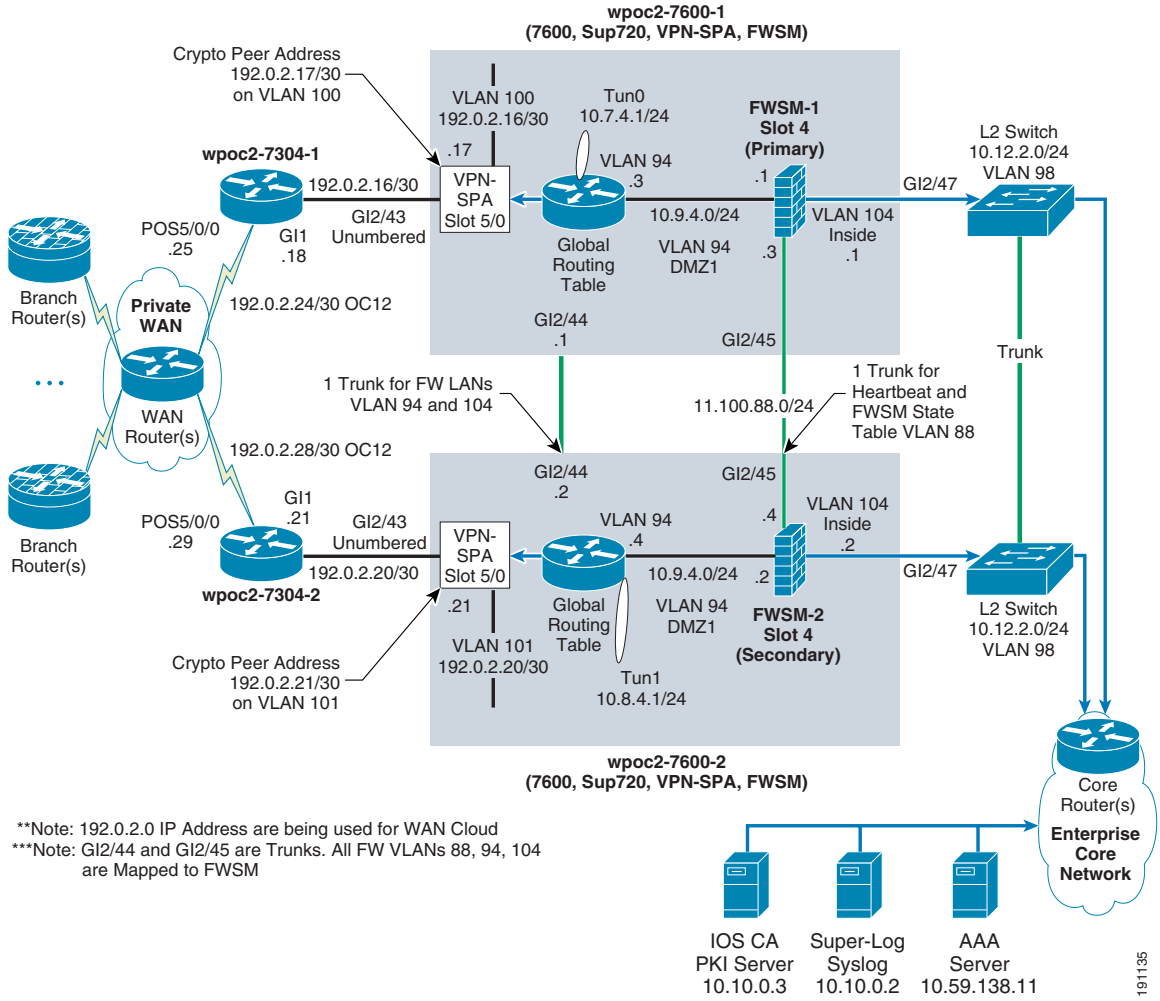
Inner Barrier Firewall #2 (Standby in Stateful Failover Pair)

```
!
! Config is same as Active above (except for the following):
failover lan unit secondary
!
```

Profile 3 Configurations

These configurations use L2 switches between the firewall and core (see L2 Switch Configurations for all Profiles, page 169). Figure 24 shows a network diagram of the Profile 3 network configuration.

Figure 24 Profile 3 (OC12) Multi-Thread in One Site (Two-Tier Solution)



Profile 3 uses a dedicated WAN router, so therefore:

- The crypto aggregation router and the WAN router are GigE connected.
- The crypto aggregation router does not perform QoS or Scavenger Class QoS, but rather the WAN router does.
- The crypto aggregation router needs to NAT the syslog server and TACACS server ports to ports on the crypto peer address to make sure only the LAN side of the WAN router can access those ports (using a new ACL named *Protect-syslog-AAA* on the GigE interface to the WAN router).
- The crypto aggregation router is the NTP clock source for the WAN router.
- The crypto aggregation router needs to add a network statement for OSPF area 1 for the outside VLAN LAN (that is, vlan100 or vlan101) on the respective connected crypto aggregation system. This is so that the WAN router interface IP address has a network path back from the AAA and syslog servers in the core.
- The WAN router is the "outer barrier" and uses the iACL (the example used an ACL named *InfraProt*)
- The WAN router accesses the super-log syslog server via the NAT-ed port on the crypto aggregation router.

- The WAN router accesses the AAA server via the NAT-ed port on the crypto aggregation router.
- The WAN router CoPP policy does not need to include VPN or IGP classes because these particular items do not terminate on the WAN router.
- The inner barrier firewall (FWSM) must add some rules to the ACL to allow the LAN IP of the WAN router to access the internal AAA server and internal super-log syslog server in the core.

Profile 3—Full Configuration for Cisco 7600 Crypto Aggregation System

Crypto Agg 7600 (Headend #1)

```
!
upgrade fpd auto
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service counters max age 10
!
hostname wpoc2-7600-1
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging buffered 32768 informational
enable secret 5 $1$HhD2$yGoJwBLlIz/ha2WqwMZyt1
!
username cisco123 privilege 15 password 7 104D000A061843595F
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
firewall module 4 vlan-group 1
firewall vlan-group 1  88,94,104
ip subnet-zero
!
!
!
ip ssh time-out 30
ip ssh source-interface Vlan94
ip ssh version 2
no ip domain-lookup
ip domain-name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls rate-limit unicast acl vacl-log
no mls acl tcam share-global
mls cef error action freeze
!
key chain 1
 key 1
  key-string 7 094F471A1A0A
```

```
call admission limit 70
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 07 nvram:wpoc3-r1#3107.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
  match access-group name coppacl-vpn
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
```

```
  match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
!
!
policy-map copp-policy
  class coppclass-bgp
   police cir 4000000 bc 400000 be 400000 conform-action transmit exceed-action drop
  class coppclass-igp
   police cir 300000 bc 3000 be 3000 conform-action transmit exceed-action drop
  class coppclass-filemanagement
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class coppclass-management
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
  class coppclass-monitoring
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-critical-app
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-vpn
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class class-default
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.4.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105700
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 load-interval 30
 tunnel source Vlan100
 tunnel mode gre multipoint
!
interface GigabitEthernet2/1
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet2/42
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
```

```
!
interface GigabitEthernet2/43
 description to-WAN-rtr-7304-1
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 speed 1000
 duplex full
 no cdp enable
 crypto connect vlan 100
!
interface GigabitEthernet2/44
 description TRUNK-TO-7600-2-FW-Statetable-heartbeat
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 88
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/45
 description TRUNK-TO-7600-2-vlan-94-104-99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 94,104
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/46
 description TO-3500-Vlan99-Inet
 switchport
 switchport access vlan 99
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/47
 description TO-Campus-Core
 switchport
 switchport access vlan 104
 switchport mode access
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/48
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface POS3/1/0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 clock source internal
```

```
 no cdp enable
!
interface GigabitEthernet5/0/1
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/0/2
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 no cdp enable
!
interface GigabitEthernet6/2
 description NOT-USED
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan94
 description TO-FWSM-1
 ip address 10.9.4.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip ospf authentication message-digest
 ip ospf authentication-key 7 0822455D0A16
 load-interval 30
!
interface Vlan100
 description VLAN OUTside VPNSPA target
 ip address 192.0.2.17 255.255.255.252
 ip access-group Protect-syslog-AAA in
 ip verify unicast source reachable-via rx allow-default
 no ip redirects
 no ip proxy-arp
```

```
 ip nat outside
 logging ip access-list cache in
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 5/0
!
router eigrp 1
 passive-interface Vlan94
 passive-interface GigabitEthernet2/43
 passive-interface GigabitEthernet2/47
 passive-interface GigabitEthernet2/48
 passive-interface POS3/1/0
 passive-interface GigabitEthernet6/2
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.4.3
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface Vlan100
 passive-interface Tunnel0
 network 10.4.0.0 0.0.255.255 area 1
 network 10.7.4.0 0.0.0.255 area 1
 network 10.8.4.0 0.0.0.255 area 1
 network 10.9.4.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.2.0 0.0.0.255 area 1
 network 192.0.2.16 0.0.0.3 area 1
!
ip nat inside source static udp 10.10.0.2 514 interface Vlan100 514
ip nat inside source static tcp 10.59.138.11 49 interface Vlan100 49
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.18
!
no ip http server
!
ip access-list extended Protect-syslog-AAA
 remark ------------------------------------------------------
 remark ONLY allow the wan router to access the nat-ed ports for tacacs or syslog and ntp
 permit udp host 192.0.2.18 host 192.0.2.17 eq syslog
 permit tcp host 192.0.2.18 host 192.0.2.17 eq tacacs
 permit udp host 192.0.2.18 host 192.0.2.17 eq ntp
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
 permit icmp any host 192.0.2.17 echo
 permit icmp any host 192.0.2.17 packet-too-big
 permit icmp any host 192.0.2.17 unreachable
 permit icmp any host 192.0.2.17 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.17 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.17
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
```

```
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.4.0 0.0.0.255 host 10.9.4.3
 permit ospf 10.7.4.0 0.0.0.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
ip access-list extended route-redist-ACL
 permit ip 10.4.0.0 0.0.255.255 any
 deny   ip any any
!
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15388160
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
snmp-server group NMS v3 priv
tftp-server disk0:c6svc-fwm-k9.3-1-1.bin
tacacs-server host 10.59.138.11 key 7 14141B180F0B
tacacs-server timeout 10
tacacs-server directed-request
!
radius-server source-ports 1645-1646
!
control-plane
!
service-policy input copp-policy
!
```

```
!
dial-peer cor custom
!
!
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
!
ntp clock-period 17179960
ntp server 10.10.0.1 source Vlan94 prefer
no cns aaa enable
end
!
```

Crypto Agg 7600 (Headend #2)

```
!
upgrade fpd auto
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service counters max age 10
!
hostname wpoc2-7600-2
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging buffered 32768 informational
enable secret 5 $1$YwBj$Q6OhaI0a.5bjHsUWItfvb1
!
username cisco123 privilege 15 password 7 104D000A061843595F
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
firewall module 4 vlan-group 1
firewall vlan-group 1  88,94,104
ip subnet-zero
!
!
```

```
!
ip ssh time-out 30
ip ssh source-interface Vlan94
ip ssh version 2
no ip domain-lookup
ip domain-name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls rate-limit unicast acl vacl-log
no mls acl tcam share-global
mls cef error action freeze
!
key chain 1
 key 1
  key-string 7 110A1016141D
call admission limit 70
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 08 nvram:wpoc3-r1#3108.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
```

```
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
  match access-group name coppacl-vpn
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
!
!
policy-map copp-policy
  class coppclass-bgp
   police cir 4000000 bc 400000 be 400000 conform-action transmit exceed-action drop
  class coppclass-igp
   police cir 300000 bc 3000 be 3000 conform-action transmit exceed-action drop
  class coppclass-filemanagement
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class coppclass-management
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
  class coppclass-monitoring
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-critical-app
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-vpn
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class class-default
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
!
!
!
interface Tunnel1
 description Tunnel1
 bandwidth 1000000
 ip address 10.8.4.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105701
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 load-interval 30
 delay 60000
 tunnel source Vlan101
```

```
 tunnel mode gre multipoint
!
interface GigabitEthernet2/1
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet2/42
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet2/43
 description to-WAN-rtr-7304-2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 speed 1000
 duplex full
 no cdp enable
 crypto connect vlan 101
!
interface GigabitEthernet2/44
 description TRUNK-TO-7600-1-FW-Statetable-heartbeat
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 88
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/45
 description TRUNK-TO-7600-1-vlan-94-104-99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 94,104
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/46
 description TO-3500-Vlan99-Inet
 switchport
 switchport access vlan 99
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/47
 description TO-Campus-Core
 switchport
 switchport access vlan 104
 switchport mode access
```

```
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/48
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface POS3/1/0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 clock source internal
 no cdp enable
!
interface GigabitEthernet5/0/1
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,101,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/0/2
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 no cdp enable
!
interface GigabitEthernet6/2
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
```

```
 no ip proxy-arp
 shutdown
!
interface Vlan94
 description TO-FWSM-2
 ip address 10.9.4.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip ospf authentication message-digest
 ip ospf authentication-key 7 1511021F0725
 load-interval 30
!
interface Vlan101
 description VLAN OUTside VPNSPA target
 ip address 192.0.2.21 255.255.255.252
 ip access-group Protect-syslog-AAA in
 ip verify unicast source reachable-via rx allow-default
 no ip redirects
 no ip proxy-arp
 ip nat outside
 logging ip access-list cache in
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 5/0
!
router eigrp 1
 passive-interface Vlan94
 passive-interface GigabitEthernet2/43
 passive-interface GigabitEthernet2/47
 passive-interface GigabitEthernet2/48
 passive-interface POS3/1/0
 passive-interface GigabitEthernet6/2
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.4.4
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface Vlan101
 passive-interface Tunnel1
 network 10.4.0.0 0.0.255.255 area 1
 network 10.7.4.0 0.0.0.255 area 1
 network 10.8.4.0 0.0.0.255 area 1
 network 10.9.4.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.2.0 0.0.0.255 area 1
 network 192.0.2.20 0.0.0.3 area 1
!
ip nat inside source static udp 10.10.0.2 514 interface Vlan101 514
ip nat inside source static tcp 10.59.138.11 49 interface Vlan101 49
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.22
!
no ip http server
!
ip access-list extended Protect-syslog-AAA
 remark ------------------------------------------------------
 remark ONLY allow the wan router to access the nat-ed ports for tacacs or syslog and ntp
 permit udp host 192.0.2.22 host 192.0.2.21 eq syslog
 permit tcp host 192.0.2.22 host 192.0.2.21 eq tacacs
```

```
 permit udp host 192.0.2.22 host 192.0.2.21 eq ntp
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.21
 permit udp any host 192.0.2.21 eq isakmp
 permit udp any host 192.0.2.21 eq non500-isakmp
 permit esp any host 192.0.2.21
 permit icmp any host 192.0.2.21 echo
 permit icmp any host 192.0.2.21 packet-too-big
 permit icmp any host 192.0.2.21 unreachable
 permit icmp any host 192.0.2.21 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.21 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.21
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.4.0 0.0.0.255 host 10.9.4.4
 permit ospf 10.8.4.0 0.0.0.255 host 10.8.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 10.8.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.21
 permit udp any host 192.0.2.21 eq isakmp
 permit udp any host 192.0.2.21 eq non500-isakmp
 permit esp any host 192.0.2.21
ip access-list extended route-redist-ACL
 permit ip 10.4.0.0 0.0.255.255 any
 deny   ip any any
!
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
```

```
 match metric 15388160
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12828160 12802816
 set metric 20
!
snmp-server group NMS v3 priv
tftp-server disk0:c6svc-fwm-k9.3-1-1.bin
tacacs-server host 10.59.138.11 key 7 104D000A0618
tacacs-server timeout 10
tacacs-server directed-request
!
radius-server source-ports 1645-1646
!
control-plane
!
service-policy input copp-policy
!
!
dial-peer cor custom
!
!
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
!
monitor event-trace timestamps
ntp clock-period 17180015
ntp server 10.10.0.1 source Vlan94 prefer
no cns aaa enable
end
!
```

Profile 3—Full Configuration for Cisco 7304 WAN Router

WAN Router 7304 (Headend #1)

```
!
upgrade fpd auto
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
```

```
!
hostname wpoc2-7304-1
!
boot-start-marker
boot system disk0:c7300-a3jk91s-mz.122-28.SB2.bin
boot-end-marker
!
logging snmp-authfail
logging buffered 32768 informational
logging rate-limit 1 except notifications
enable secret 5 $1$0E8M$4ZYsm7x72UShi8Z/WQmsu/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
!
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name ese.cisco.com
no ip dhcp use vrf connected
!
!
ip ssh time-out 30
ip ssh source-interface GigabitEthernet1
ip ssh logging events
ip ssh version 2
!
!
!
redundancy
 mode sso
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-any VOICE
  match ip dscp ef
  match ip precedence 5
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-all coppclass-management
  match access-group name coppacl-management
```

```
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
!
policy-map copp-policy
 description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
  class coppclass-filemanagement
  class coppclass-bgp
   police cir 80000 bc 8000 be 8000
     conform-action transmit
     exceed-action drop
  class coppclass-management
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
  class coppclass-monitoring
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class coppclass-critical-app
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class class-default
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000    conform-action transmit     exceed-action
drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
!
interface GigabitEthernet0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
```

```
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet1
 description to-cryagg1-wpoc2-7600-1
 ip address 192.0.2.18 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface POS5/0/0
 description OC12-TO-WAN-RTR
 ip address 192.0.2.25 255.255.255.252
 ip access-group InfraProt in
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 service-policy output OC12-WAN-wSCAVENGER
!
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.26
!
no ip http server
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
```

```
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 remark This line is not required on WAN rtr - permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq 4500
 permit esp any host 192.0.2.17
 permit icmp any host 192.0.2.17 echo
 permit icmp any host 192.0.2.17 packet-too-big
 permit icmp any host 192.0.2.17 unreachable
 permit icmp any host 192.0.2.17 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.127 host 192.0.2.25 eq bgp
 permit tcp 192.0.2.0 0.0.0.127 eq bgp host 192.0.2.25
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
!
!
!
!
!
!
!
!
logging 192.0.2.17
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 permit 192.0.2.16 0.0.0.3
access-list 10 permit 192.0.2.20 0.0.0.3
access-list 10 deny   any log
no cdp run
!
snmp-server engineID local 800000090300000E834DF700
snmp-server group NMS v3 priv
tacacs-server host 192.0.2.17
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 01100F175804
!
!
```

```
control-plane
 service-policy input copp-policy
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 104D000A0618
 logging synchronous
 transport input ssh
!
ntp clock-period 17179960
ntp server 192.0.2.17 source GigabitEthernet1 prefer
!
end
!
```

WAN Router 7304 (Headend #2)

```
!
upgrade fpd auto
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc2-7304-2
!
boot-start-marker
boot system disk0:c7300-a3jk91s-mz.122-28.SB2.bin
boot-end-marker
!
logging snmp-authfail
logging buffered 32768 informational
logging rate-limit 1 except notifications
enable secret 5 $1$.K2R$a8VSaKFWTc/rs8AsPt.Jb0
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
!
```

```
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name ese.cisco.com
no ip dhcp use vrf connected
!
!
ip ssh time-out 30
ip ssh source-interface GigabitEthernet1
ip ssh logging events
ip ssh version 2
!
!
!
redundancy
 mode sso
username cisco123 privilege 15 password 7 104D000A061843595F
!
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-any VOICE
  match ip dscp ef
  match ip precedence 5
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-all coppclass-management
  match access-group name coppacl-management
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
!
policy-map copp-policy
 description NOTE that the IGP and VPN classes are removed on WAN rtr CoPP config
  class coppclass-filemanagement
  class coppclass-bgp
   police cir 80000 bc 8000 be 8000
     conform-action transmit
     exceed-action drop
  class coppclass-management
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
  class coppclass-monitoring
```

```
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class coppclass-critical-app
   police cir 500000 bc 5000 be 5000
     conform-action transmit
     exceed-action drop
  class class-default
   police cir 10000000 bc 100000 be 100000
     conform-action transmit
     exceed-action drop
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000    conform-action transmit     exceed-action
drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
!
interface GigabitEthernet0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet1
 description to-cryagg2-wpoc2-7600-2
 ip address 192.0.2.22 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 no negotiation auto
 no cdp enable
!
interface GigabitEthernet2
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 duplex auto
 speed auto
 media-type rj45
```

```
 no negotiation auto
 no cdp enable
!
interface POS5/0/0
 description OC12-TO-WAN-RTR
 ip address 192.0.2.29 255.255.255.252
 ip access-group InfraProt in
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 service-policy output OC12-WAN-wSCAVENGER
!
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.30
!
no ip http server
!
!
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 remark This line is not required on WAN rtr - permit gre any host 192.0.2.21
 permit udp any host 192.0.2.21 eq isakmp
 permit udp any host 192.0.2.21 eq 4500
 permit esp any host 192.0.2.21
 permit icmp any host 192.0.2.21 echo
 permit icmp any host 192.0.2.21 packet-too-big
 permit icmp any host 192.0.2.21 unreachable
 permit icmp any host 192.0.2.21 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class - this class for BGP to ISP if desired.
 permit tcp 192.0.2.0 0.0.0.127 host 192.0.2.29 eq bgp
 permit tcp 192.0.2.0 0.0.0.127 eq bgp host 192.0.2.29
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
```

```
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
!
!
!
!
!
!
!
!
logging 192.0.2.21
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 permit 192.0.2.16 0.0.0.3
access-list 10 permit 192.0.2.20 0.0.0.3
access-list 10 deny   any log
no cdp run
!
snmp-server engineID local 800000090300000E834DF800
snmp-server group NMS v3 priv
tacacs-server host 192.0.2.21
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 110A1016141D
!
!
control-plane
 service-policy input copp-policy
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 104D000A0618
 logging synchronous
 transport input ssh
!
ntp clock-period 17179988
```

```
ntp server 192.0.2.21 source GigabitEthernet1 prefer
!
end
!
```

Profile 3—Configuration for Cisco Firewall Service Modules

Inner Barrier Firewall #1 (Active in Stateful Failover Pair)

```
!
hostname FWSM-1
domain-name ese.cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan88
 description LAN/STATE Failover Interface
!
interface Vlan94
 nameif dmz1
 security-level 50
 ip address 10.9.4.1 255.255.255.0 standby 10.9.4.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface Vlan104
 nameif inside
 security-level 100
 ip address 10.12.2.1 255.255.255.0 standby 10.12.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
passwd 2KFQnbNIdI.2KYOU encrypted
banner motd Warning this is a private system.
banner motd Unauthorized access is prohibited.
banner motd Violators will be prosecuted.
banner motd .
ftp mode passive
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.4.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.7.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit tcp host 192.0.2.18 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.18 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit tcp host 192.0.2.22 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.22 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended deny ip any any log
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
pager lines 24
logging enable
logging timestamp
logging standby
logging buffered informational
logging trap notifications
logging asdm informational
logging host inside 10.10.0.2
mtu dmz1 1500
mtu inside 1500
ip verify reverse-path interface dmz1
failover
```

```
failover lan unit primary
failover lan interface failover Vlan88
failover link failover Vlan88
failover interface ip failover 11.100.88.1 255.255.255.0 standby 11.100.88.2
monitor-interface dmz1
monitor-interface inside
icmp permit any dmz1
icmp permit any inside
no asdm history enable
arp timeout 14400
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.2.0 10.12.2.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0
access-group dmz1_access_in in interface dmz1
access-group inside_access_in in interface inside
!
router ospf 100
 network 10.0.0.0 255.0.0.0 area 1
 area 1 authentication message-digest
 router-id 10.9.4.1
 log-adj-changes
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server tacacs-group protocol tacacs+
aaa-server tacacs-group host 10.59.138.11
 key cisco
username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
aaa authentication enable console tacacs-group LOCAL
aaa authentication ssh console tacacs-group LOCAL
aaa authentication telnet console tacacs-group LOCAL
aaa authorization command tacacs-group LOCAL
aaa accounting command tacacs-group
aaa accounting telnet console tacacs-group
aaa accounting ssh console tacacs-group
http server enable
http 10.0.0.0 255.0.0.0 dmz1
http 10.0.0.0 255.0.0.0 inside
snmp-server host inside 10.10.0.4 poll community NMScommunity version 2c
snmp-server location inner-barrier
snmp-server contact admin@company.com
snmp-server community NMScommunity
snmp-server enable traps snmp authentication linkup linkdown coldstart
sysopt nodnsalias inbound
sysopt nodnsalias outbound
telnet timeout 1
ssh scopy enable
ssh 10.0.0.0 255.0.0.0 dmz1
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 60
console timeout 60
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
```

```
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect skinny
  inspect smtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a9696595e039a119e8a5f9b94cea7283
: end
!
```

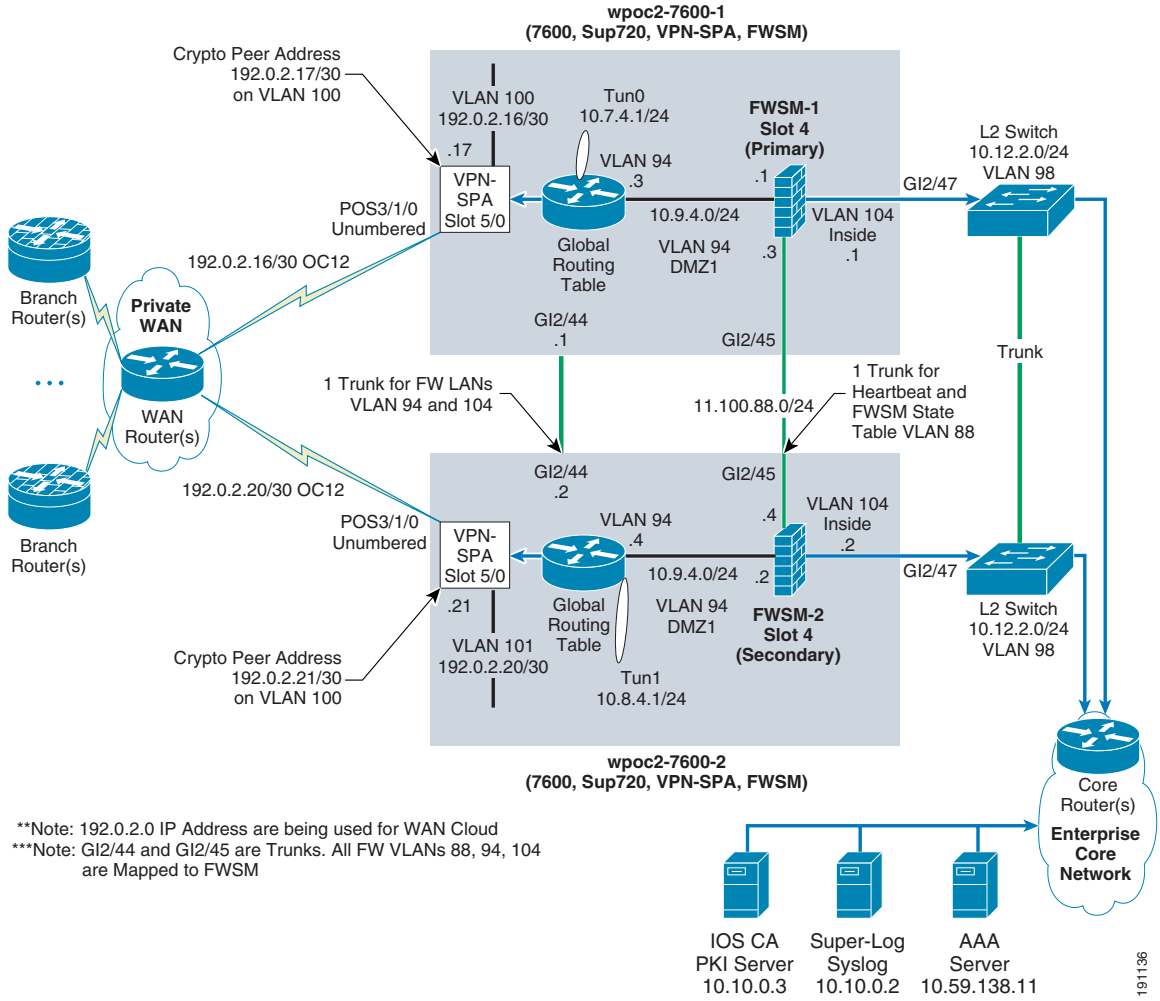
Inner Barrier Firewall #2 (Standby in Stateful Failover Pair)

```
!
! Config is same as Active above (except for the following):
failover lan unit secondary
!
```

Profile 4 Configurations

These configurations use L2 switches between the firewall and core (see L2 Switch Configurations for all Profiles, page 169). Figure 25 shows a network diagram of the Profile 4 network configuration.

Figure 25 Profile 4 (OC12) Multi-Thread in One Site (One-Tier Solution)



Profile 4—Full Configuration for Cisco 7600 Crypto Aggregation and WAN System

Crypto Agg and WAN Router (Headend #1)

```
!
upgrade fpd auto
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service counters max age 10
!
hostname wpoc2-7600-1
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging buffered 32768 informational
no logging console
enable secret 5 $1$HhD2$yGoJwBLlIz/ha2WqwMZyt1
!
username cisco123 privilege 15 password 7 104D000A061843595F
```

```
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
firewall module 4 vlan-group 1
firewall vlan-group 1  88,94,104
ip subnet-zero
!
!
!
ip ssh time-out 30
ip ssh source-interface Vlan94
ip ssh version 2
no ip domain-lookup
ip domain-name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls rate-limit unicast acl vacl-log
no mls acl tcam share-global
mls cef error action freeze
!
key chain 1
 key 1
  key-string 7 094F471A1A0A
call admission limit 70
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 07 nvram:wpoc3-r1#3107.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
```

```
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
  match access-group name coppacl-vpn
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-any VOICE
  match ip dscp ef
  match ip precedence 5
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
!
policy-map copp-policy
  class coppclass-bgp
   police cir 4000000 bc 400000 be 400000 conform-action transmit exceed-action drop
  class coppclass-igp
   police cir 300000 bc 3000 be 3000 conform-action transmit exceed-action drop
  class coppclass-filemanagement
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
```

```
  class coppclass-management
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
  class coppclass-monitoring
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-critical-app
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-vpn
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class class-default
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000 conform-action transmit exceed-action drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 1000000
 ip address 10.7.4.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105700
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 load-interval 30
 tunnel source Vlan100
 tunnel mode gre multipoint
!
interface GigabitEthernet2/1
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet2/43
 no ip address
 no ip redirects
 no ip proxy-arp
```

```
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet2/44
 description TRUNK-TO-7600-2-FW-Statetable-heartbeat
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 88
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/45
 description TRUNK-TO-7600-2-vlan-94-104-99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 94,104
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/46
 description TO-3500-Vlan99-Inet
 switchport
 switchport access vlan 99
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/47
 description TO-Campus-Core
 switchport
 switchport access vlan 104
 switchport mode access
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/48
 description NOT-USED
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface POS3/1/0
 description OC12-TO-WAN-RTR
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 crypto connect vlan 100
 service-policy output OC12-WAN-wSCAVENGER
!
interface GigabitEthernet5/0/1
 description VPN-SPA
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/0/2
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 no cdp enable
!
interface GigabitEthernet6/2
 description NOT-USED
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan94
 description TO-FWSM-1
 ip address 10.9.4.3 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 0822455D0A16
 load-interval 30
!
interface Vlan100
 description description VLAN OUTside VPNSPA target
 ip address 192.0.2.17 255.255.255.252
 ip access-group InfraProt in
 ip verify unicast source reachable-via rx allow-default
 no ip redirects
 no ip proxy-arp
 logging ip access-list cache in
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 5/0
!
```

```
router eigrp 1
 passive-interface Vlan94
 passive-interface GigabitEthernet2/47
 passive-interface GigabitEthernet2/48
 passive-interface POS3/1/0
 passive-interface GigabitEthernet6/2
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.4.3
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface Vlan100
 passive-interface Tunnel0
 network 10.4.0.0 0.0.255.255 area 1
 network 10.7.4.0 0.0.0.255 area 1
 network 10.8.4.0 0.0.0.255 area 1
 network 10.9.4.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.2.0 0.0.0.255 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.18
!
no ip http server
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
 permit icmp any host 192.0.2.17 echo
 permit icmp any host 192.0.2.17 packet-too-big
 permit icmp any host 192.0.2.17 unreachable
 permit icmp any host 192.0.2.17 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.17 eq bgp
```

```
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.17
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
 remark IGP traffic class
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.4.0 0.0.0.255 host 10.9.4.3
 permit ospf 10.7.4.0 0.0.0.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 10.7.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.17
 permit udp any host 192.0.2.17 eq isakmp
 permit udp any host 192.0.2.17 eq non500-isakmp
 permit esp any host 192.0.2.17
ip access-list extended route-redist-ACL
 permit ip 10.4.0.0 0.0.255.255 any
 deny   ip any any
!
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15388160
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12802816
 set metric 20
!
snmp-server group NMS v3 priv
tftp-server disk0:c6svc-fwm-k9.3-1-1.bin
tacacs-server host 10.59.138.11 key 7 14141B180F0B
tacacs-server timeout 10
tacacs-server directed-request
!
radius-server source-ports 1645-1646
!
control-plane
```

```
!
service-policy input copp-policy
!
!
dial-peer cor custom
!
!
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
!
ntp clock-period 17179966
ntp server 10.10.0.1 source Vlan94 prefer
no cns aaa enable
end
!
```

Crypto Agg and WAN Router (Headend #2)

```
!
upgrade fpd auto
version 12.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service counters max age 10
!
hostname wpoc2-7600-2
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF2.bin
logging buffered 32768 informational
no logging console
enable secret 5 $1$YwBj$Q6OhaI0a.5bjHsUWItfvb1
!
username cisco123 privilege 15 password 7 104D000A061843595F
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
```

```
firewall module 4 vlan-group 1
firewall vlan-group 1  88,94,104
ip subnet-zero
!
!
!
ip ssh time-out 30
ip ssh source-interface Vlan94
ip ssh version 2
no ip domain-lookup
ip domain-name ese.cisco.com
ip host wpoc3-r1 10.10.0.3
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls rate-limit unicast acl vacl-log
no mls acl tcam share-global
mls cef error action freeze
!
key chain 1
 key 1
  key-string 7 110A1016141D
call admission limit 70
!
crypto pki trustpoint ese-ios-ca
 enrollment url http://wpoc3-r1:80
 revocation-check crl
 auto-enroll 70
!
!
crypto pki certificate chain ese-ios-ca
 certificate 08 nvram:wpoc3-r1#3108.cer
 certificate ca 01 nvram:wpoc3-r1#3101CA.cer
!
!
crypto isakmp policy 10
 encr 3des
 group 2
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
!
crypto ipsec profile vpn-dmvpn
 set transform-set vpn-test
!
!
crypto dynamic-map dmap 10
 set transform-set vpn-test
 reverse-route
!
!
crypto map dynamic-map 10 ipsec-isakmp dynamic dmap
!
!
!
!
!
!
!
redundancy
 mode sso
 main-cpu
```

```
  auto-sync running-config
  auto-sync standard
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
fabric buffer-reserve queue
port-channel per-module load-balance
!
vlan internal allocation policy ascending
!
class-map match-all coppclass-critical-app
  match access-group name coppacl-critical-app
class-map match-all coppclass-vpn
  match access-group name coppacl-vpn
class-map match-all coppclass-igp
  match access-group name coppacl-igp
class-map match-all coppclass-bgp
  match access-group name coppacl-bgp
class-map match-all coppclass-monitoring
  match access-group name coppacl-monitoring
class-map match-any VOICE
  match ip dscp ef
  match ip precedence 5
class-map match-all coppclass-filemanagement
  match access-group name coppacl-filemanagement
class-map match-all coppclass-management
  match access-group name coppacl-management
class-map match-all SCAVENGER
  match ip dscp cs1
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match ip precedence 6
class-map match-any TRANSACTIONAL-DATA
  match ip dscp af21
  match ip precedence 2
!
!
policy-map copp-policy
  class coppclass-bgp
   police cir 4000000 bc 400000 be 400000 conform-action transmit exceed-action drop
  class coppclass-igp
   police cir 300000 bc 3000 be 3000 conform-action transmit exceed-action drop
  class coppclass-filemanagement
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class coppclass-management
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
  class coppclass-monitoring
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-critical-app
   police cir 900000 bc 9000 be 9000 conform-action transmit exceed-action drop
  class coppclass-vpn
   police cir 6000000 bc 60000 be 60000 conform-action transmit exceed-action drop
  class class-default
   police cir 500000 bc 5000 be 5000 conform-action transmit exceed-action drop
policy-map OC12-WAN-wSCAVENGER
 description VOICE-class is 33% of OC-12(622M) aka 205,000,000
```

```
  class VOICE
    priority
   police cir 205000000 bc 2050000 be 2050000 conform-action transmit exceed-action drop
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class CALL-SETUP
    bandwidth percent 5
  class TRANSACTIONAL-DATA
    bandwidth percent 30
  class SCAVENGER
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    random-detect
!
!
!
interface Tunnel1
 description Tunnel1
 bandwidth 1000000
 ip address 10.8.4.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip hold-time eigrp 1 35
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 1
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105701
 ip nhrp holdtime 300
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0 5
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0 250
 load-interval 30
 delay 60000
 tunnel source Vlan101
 tunnel mode gre multipoint
!
interface GigabitEthernet2/1
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet2/43
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet2/44
 description TRUNK-TO-7600-1-FW-Statetable-heartbeat
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 88
 switchport mode trunk
 no ip address
 load-interval 30
```

```
 no cdp enable
!
interface GigabitEthernet2/45
 description TRUNK-TO-7600-1-vlan-94-104-99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 94,104
 switchport mode trunk
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/46
 description TO-3500-Vlan99-Inet
 switchport
 switchport access vlan 99
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/47
 description TO-Campus-Core
 switchport
 switchport access vlan 104
 switchport mode access
 no ip address
 load-interval 30
 no cdp enable
!
interface GigabitEthernet2/48
 description NOT-USED
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
interface POS3/1/0
 description OC12-TO-WAN-RTR
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 clock source internal
 no cdp enable
 crypto connect vlan 101
 service-policy output OC12-WAN-wSCAVENGER
!
interface GigabitEthernet5/0/1
 description VPN-SPA
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,101,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/0/2
 description VPN-SPA
 switchport
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/1
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 no cdp enable
!
interface GigabitEthernet6/2
 description NOT-USED.
 no ip address
 no ip redirects
 no ip proxy-arp
 shutdown
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
 no ip proxy-arp
 shutdown
!
interface Vlan94
 description TO-FWSM-2
 ip address 10.9.4.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 1511021F0725
 load-interval 30
!
interface Vlan101
 description VLAN OUTside VPNSPA target
 ip address 192.0.2.21 255.255.255.252
 ip access-group InfraProt in
 ip verify unicast source reachable-via rx allow-default
 no ip redirects
 no ip proxy-arp
 logging ip access-list cache in
 load-interval 30
 no mop enabled
 crypto map dynamic-map
 crypto engine subslot 5/0
!
router eigrp 1
 passive-interface Vlan94
 passive-interface GigabitEthernet2/47
 passive-interface GigabitEthernet2/48
 passive-interface POS3/1/0
 passive-interface GigabitEthernet6/2
 network 10.0.0.0
 no auto-summary
!
router ospf 100
 router-id 10.9.4.4
```

```
 log-adjacency-changes
 area 1 authentication message-digest
 redistribute eigrp 1 subnets route-map route-redist
 passive-interface Vlan101
 passive-interface Tunnel1
 network 10.4.0.0 0.0.255.255 area 1
 network 10.7.4.0 0.0.0.255 area 1
 network 10.8.4.0 0.0.0.255 area 1
 network 10.9.4.0 0.0.0.255 area 1
 network 10.10.0.0 0.0.255.255 area 1
 network 10.12.2.0 0.0.0.255 area 1
!
ip classless
ip route 192.0.2.0 255.255.255.128 192.0.2.22
!
no ip http server
!
ip access-list extended InfraProt
 remark ------------------------------------------------------
 remark usual anti-frag rules
 deny   tcp any any log fragments
 deny   udp any any log fragments
 deny   icmp any any log fragments
 remark ------------------------------------------------------
 remark usual anti-spoofing rules - most not possible on 12.2 code...
 deny   ip host 0.0.0.0 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 remark Usually the subnet 192.0.2.0/24 is not internet routable and
 remark is usually blocked - but in this document we are using part 192.0.2.0/25
 remark as the subnet for the addressing of the WAN cloud IP addressing so part
 remark of it will be omitted from the deny below.
 deny   ip 192.0.2.128 0.0.0.127 any log
 deny   ip 224.0.0.0 31.255.255.255 any log
 deny   ip host 255.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark ------------------------------------------------------
 remark permit GRE and isakmp/esp and inbound icmp echo to outside-int
 permit gre any host 192.0.2.21
 permit udp any host 192.0.2.21 eq isakmp
 permit udp any host 192.0.2.21 eq non500-isakmp
 permit esp any host 192.0.2.21
 permit icmp any host 192.0.2.21 echo
 permit icmp any host 192.0.2.21 packet-too-big
 permit icmp any host 192.0.2.21 unreachable
 permit icmp any host 192.0.2.21 time-exceeded
 remark ------------------------------------------------------
 remark default deny all log..
 deny   ip any any log
ip access-list extended coppacl-bgp
 remark BGP traffic class
 permit tcp 192.0.2.0 0.0.0.128 host 192.0.2.21 eq bgp
 permit tcp 192.0.2.0 0.0.0.128 eq bgp host 192.0.2.21
ip access-list extended coppacl-critical-app
 remark CoPP critical apps traffic class
 permit ip any host 224.0.0.2
ip access-list extended coppacl-filemanagement
 remark CoPP File transfer traffic class
 permit tcp any eq ftp any gt 1023 established
 permit tcp any eq ftp-data any gt 1023
 permit tcp any gt 1023 any gt 1023 established
 permit udp any gt 1023 any gt 1023
ip access-list extended coppacl-igp
```

```
 remark IGP traffic class
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.5
 permit ospf 10.9.4.0 0.0.0.255 host 224.0.0.6
 permit ospf 10.9.4.0 0.0.0.255 host 10.9.4.4
 permit ospf 10.8.4.0 0.0.0.255 host 10.8.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 10.8.4.1
 permit eigrp 10.0.0.0 0.255.255.255 host 224.0.0.10
ip access-list extended coppacl-management
 remark CoPP management traffic class
 permit tcp any eq tacacs any established
 permit tcp any any eq 22
 permit tcp any any eq telnet
 permit udp any any eq snmp
 permit udp any any eq ntp
ip access-list extended coppacl-monitoring
 remark CoPP monitoring traffic class
 permit icmp any any ttl-exceeded
 permit icmp any any port-unreachable
 permit icmp any any echo-reply
 permit icmp any any echo
ip access-list extended coppacl-vpn
 permit gre any host 192.0.2.21
 permit udp any host 192.0.2.21 eq isakmp
 permit udp any host 192.0.2.21 eq non500-isakmp
 permit esp any host 192.0.2.21
ip access-list extended route-redist-ACL
 permit ip 10.4.0.0 0.0.255.255 any
 deny   ip any any
!
logging 10.10.0.2
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
!
route-map route-redist permit 10
 match ip address route-redist-ACL
 match metric 15388160
 set metric 30
!
route-map route-redist permit 20
 match ip address route-redist-ACL
 match metric 12828160 12802816
 set metric 20
!
snmp-server group NMS v3 priv
tftp-server disk0:c6svc-fwm-k9.3-1-1.bin
tacacs-server host 10.59.138.11 key 7 104D000A0618
tacacs-server timeout 10
tacacs-server directed-request
!
radius-server source-ports 1645-1646
!
control-plane
!
service-policy input copp-policy
!
!
dial-peer cor custom
!
!
!
banner motd ^C
Warning this is a private system.
Unauthorized access is prohibited.
```

```
Violators will be prosecuted.
.
^C
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 logging synchronous
 transport input ssh
!
!
ntp clock-period 17180017
ntp server 10.10.0.1 source Vlan94 prefer
no cns aaa enable
end
!
```

Profile 4—Full Configuration for Cisco Firewall Service Module

Inner Barrier Firewall #1 (Active in Stateful Failover Pair)

```
!
FWSM Version 3.1(1)
!
hostname FWSM-1
domain-name ese.cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan88
 description LAN/STATE Failover Interface
!
interface Vlan94
 nameif dmz1
 security-level 50
 ip address 10.9.4.1 255.255.255.0 standby 10.9.4.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
interface Vlan104
 nameif inside
 security-level 100
 ip address 10.12.2.1 255.255.255.0 standby 10.12.2.2
 ospf authentication-key cisco
 ospf authentication message-digest
!
passwd 2KFQnbNIdI.2KYOU encrypted
banner motd Warning this is a private system.
banner motd Unauthorized access is prohibited.
banner motd Violators will be prosecuted.
banner motd .
ftp mode passive
access-list dmz1_access_in extended permit icmp any any log
access-list dmz1_access_in extended permit ip 10.4.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.9.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.8.4.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list dmz1_access_in extended permit ip 10.7.4.0 255.255.255.0 10.0.0.0 255.0.0.0
```

```
access-list dmz1_access_in extended permit tcp host 192.0.2.18 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.18 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended permit tcp host 192.0.2.22 host 10.59.138.11 eq tacacs
access-list dmz1_access_in extended permit udp host 192.0.2.22 host 10.10.0.2 eq syslog
access-list dmz1_access_in extended deny ip any any log
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
pager lines 24
logging enable
logging timestamp
logging standby
logging buffered informational
logging trap notifications
logging asdm informational
logging host inside 10.10.0.2
mtu dmz1 1500
mtu inside 1500
ip verify reverse-path interface dmz1
failover
failover lan unit primary
failover lan interface failover Vlan88
failover link failover Vlan88
failover interface ip failover 11.100.88.1 255.255.255.0 standby 11.100.88.2
monitor-interface dmz1
monitor-interface inside
icmp permit any dmz1
icmp permit any inside
no asdm history enable
arp timeout 14400
nat-control
static (inside,dmz1) 10.10.0.0 10.10.0.0 netmask 255.255.0.0
static (inside,dmz1) 10.12.2.0 10.12.2.0 netmask 255.255.255.0
static (inside,dmz1) 10.59.138.0 10.59.138.0 netmask 255.255.254.0
access-group dmz1_access_in in interface dmz1
access-group inside_access_in in interface inside
!
router ospf 100
 network 10.0.0.0 255.0.0.0 area 1
 area 1 authentication message-digest
 router-id 10.9.4.1
 log-adj-changes
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server tacacs-group protocol tacacs+
aaa-server tacacs-group host 10.59.138.11
 key cisco
username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
aaa authentication enable console tacacs-group LOCAL
aaa authentication ssh console tacacs-group LOCAL
aaa authentication telnet console tacacs-group LOCAL
aaa authorization command tacacs-group LOCAL
aaa accounting command tacacs-group
aaa accounting telnet console tacacs-group
aaa accounting ssh console tacacs-group
http server enable
http 10.0.0.0 255.0.0.0 dmz1
http 10.0.0.0 255.0.0.0 inside
snmp-server host inside 10.10.0.4 poll community NMScommunity version 2c
```

```
snmp-server location inner-barrier
snmp-server contact admin@company.com
snmp-server community NMScommunity
snmp-server enable traps snmp authentication linkup linkdown coldstart
sysopt nodnsalias inbound
sysopt nodnsalias outbound
telnet timeout 1
ssh scopy enable
ssh 10.0.0.0 255.0.0.0 dmz1
ssh 10.0.0.0 255.0.0.0 inside
ssh timeout 60
console timeout 60
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect skinny
  inspect smtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a9696595e039a119e8a5f9b94cea7283
: end
!
```

Inner Barrier Firewall #2 (Standby in Stateful Failover Pair)

```
!
! Same as Active except:
failover lan unit secondary
!
```

L2 Switch Configurations for all Profiles

All Profiles—Full Configuration for Cisco Catalyst 3560 Switch (Used Mainly as L2 Switch)

Switch #1

```
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
```

```
service password-encryption
!
hostname wpoc2-3500-1
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
enable secret 5 $1$EvUN$ppamSuhtGoiqPk.N/DNeW/
!
username cisco123 password 7 13061E010803557878
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
vtp domain l2switches
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name ese.cisco.com
!
ip ssh time-out 30
ip ssh source-interface GigabitEthernet0/1
ip ssh logging events
ip ssh version 2
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 92,98-99
!
!
interface GigabitEthernet0/1
 description to-wpoc2-7600-1-FWSMp
 switchport access vlan 98
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/2
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/3
 no switchport
 no ip address
 load-interval 30
```

```
 shutdown
 no cdp enable
!
interface GigabitEthernet0/4
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/5
 description to wpoc2-7304-3-g2
 switchport access vlan 98
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/6
 description to wpoc2-7304-3-g1
 switchport access vlan 99
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/7
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/14
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/15
 description to wpoc2-asa1p-inside
 switchport access vlan 99
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/16
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/31
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/32
```

```
 description to wpoc2-asa1p-dmz1
 switchport access vlan 92
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/33
 description to wpoc1-r1-gi0/1
 switchport access vlan 92
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/34
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/46
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/47
 description trunk-between-L2-switches
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 92,98,99
 switchport mode trunk
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/48
 no switchport
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/52
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan99
 description campus-side-int
 ip address 10.12.1.4 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 110A1016141D
!
router ospf 100
 log-adjacency-changes
```

```
 area 1 authentication message-digest
 network 10.0.0.0 0.255.255.255 area 1
!
ip classless
no ip http server
no ip http secure-server
!
!
logging 10.10.0.2
access-list 10 remark ONLY allow the net10 to admin this system.
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
snmp-server group NMS v3 priv
tacacs-server host 10.59.138.11
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 094F471A1A0A
radius-server source-ports 1645-1646
!
control-plane
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 104D000A0618
 logging synchronous
 transport input ssh
line vty 5 15
 access-class 10 in
 exec-timeout 3 0
 password 7 13061E010803
 logging synchronous
 transport input ssh
!
ntp clock-period 36028957
ntp server 10.10.0.1 source Vlan99
end
!
```

Switch #2

```
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname wpoc2-3500-2
!
logging buffered 32768 informational
logging rate-limit 1 except notifications
enable secret 5 $1$EvUN$ppamSuhtGoiqPk.N/DNeW/
!
username cisco123 password 7 13061E010803557878
aaa new-model
aaa authentication login default group tacacs+ local enable
aaa authentication enable default group tacacs+ enable
```

```
aaa authorization exec default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
!
aaa session-id common
clock timezone est -5
clock summer-time edt recurring
vtp domain l2switches
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name ese.cisco.com
!
ip ssh time-out 30
ip ssh source-interface Vlan94
ip ssh logging events
ip ssh version 2
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 92,98-99
!
!
interface GigabitEthernet0/1
 description to-wpoc2-7600-2-FWSMs
 switchport access vlan 98
 switchport mode access
 load-interval 30
 speed 1000
 duplex full
 no cdp enable
!
interface GigabitEthernet0/2
 no switchport
 no ip address
 load-interval 30
 shutdown
 speed 1000
 duplex full
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/14
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/15
 description to wpoc2-asa2s-inside
 switchport access vlan 99
 switchport mode access
```

```
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/16
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/31
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/32
 description to wpoc2-asa2s-dmz1
 switchport access vlan 92
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/33
 description to wpoc1-r2-gi0/1
 switchport access vlan 92
 switchport mode access
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/34
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/46
 no switchport
 no ip address
 load-interval 30
 shutdown
 no cdp enable
!
interface GigabitEthernet0/47
 description trunk-between-L2-switches
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 92,98,99
 switchport mode trunk
 load-interval 30
 no cdp enable
!
interface GigabitEthernet0/48
 no switchport
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 shutdown
```

```
 no cdp enable
!
! … <snipped shutdown interfaces for brevity> …
!
interface GigabitEthernet0/52
 load-interval 30
 shutdown
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan94
 no ip address
!
interface Vlan99
 description campus-side-int
 ip address 10.12.1.5 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip ospf authentication message-digest
 ip ospf authentication-key 7 110A1016141D
!
router ospf 100
 log-adjacency-changes
 area 1 authentication message-digest
 network 10.0.0.0 0.255.255.255 area 1
!
ip classless
no ip http server
no ip http secure-server
!
!
logging 10.10.0.2
access-list 10 remark ONLY allow the net10 to admin this system.
access-list 10 permit 10.0.0.0 0.255.255.255
access-list 10 deny   any log
no cdp run
snmp-server group NMS v3 priv
tacacs-server host 10.59.138.11
tacacs-server timeout 10
tacacs-server directed-request
tacacs-server key 7 01100F175804
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
 exec-timeout 3 0
 logging synchronous
 stopbits 1
line vty 0 4
 access-class 10 in
 exec-timeout 3 0
 password 7 104D000A0618
 logging synchronous
 transport input ssh
line vty 5 15
 access-class 10 in
 exec-timeout 3 0
 password 7 13061E010803
 logging synchronous
```

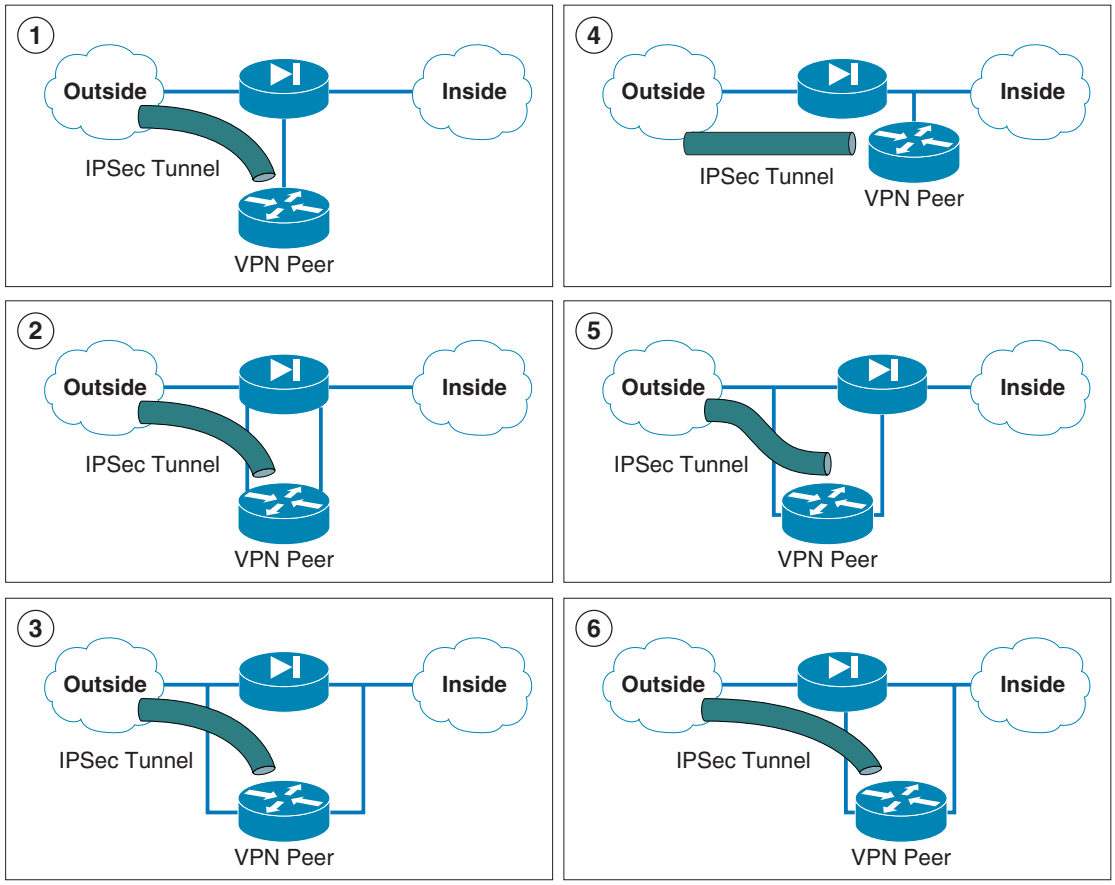
```
 transport input ssh
!
ntp clock-period 36028883
ntp server 10.10.0.1 source Vlan99 prefer
end
!
```

Appendix A—Other Possible Topologies

This section describes other possible topologies of the crypto aggregation system in relation to the location firewall placement in the NGWAN edge architecture.

Figure 26 shows other possible locations of the firewall relative to the crypto aggregation systems.

Figure 26 Other VPN/Firewall Topologies



Various other topologies are determined by the location of the firewall and crypto aggregation system. Six common examples are shown in figure above. Cisco Enterprise Solutions Engineering (ESE) does not generally recommend any of these topologies. Some of the reasons are listed in Table 8 desribing the ramifications for security, performance, and connectivity.

Table 8 Comparison of Six Other Firewall Placements in Relation to the Crypto Aggregation System

	Security Ramifications (Required—outer and inner barrier firewall)	Performance Ramifications (Required—a DMVPN hub-and-spoke VPN topology)	Connectivity Ramifications (Required—a Cisco VXR and an ASA Firewall Appliance)
1) Single armed crypto aggregation in a separate DMZ of the firewall	Both the encrypted and decrypted traffic reside in a single DMZ subnet together. Two sets of rules are required on the firewall one from the outside to the DMZ (for cipher text packets) and one from the DMZ to the inside (for clear text packets). This allows independent inspection of both the cipher and clear text packets, as does the inner and outer barrier in the recommended design.	Firewall load is doubled because packets are processed as both cipher text (encrypted) and clear text (unencrypted) for both uni-directional VoIP flows. Possible overwhelming of CPU of firewall because of VoIP traffic at high speeds. Each VoIP phone call usually caused 100 pps (50 pps each direction), but it must cross the firewall twice: therefore, the load of 200 pps per VoIP call is imposed on the firewall.	A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection. Also the bandwidth of the single-arm crypto agg system is used for both cipher and clear text packets; this may be a limitation depending on bandwidth and configurations. It is required to use **ip route-cache same interface** commands on the crypto agg device because it is single-armed (single-homed). Packets are both inbound and then outbound on the same interface of the router.
2) Each arm of the crypto aggregation in a separate DMZ of the same firewall	No security issue. Two sets of rules would be required on the firewall: one from the outside to the DMZ1 (for cipher text packets), and one from the DMZ2 to the inside (for clear text packets). This does allow independent inspection of both the cipher and clear text packets, as does the inner and outer barrier in the recommended design.	Firewall load is doubled because packets are processed as both cipher text (encrypted) and clear text (unencrypted) for both uni-directional VoIP flows. Possible overwhelming of CPU of firewall because of VoIP traffic Each VoIP phone call usually caused 100 pps (50 pps each direction), but it must cross the firewall twice: therefore, the load of 200 pps per VoIP call is imposed on the firewall.	A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection.
3) Crypto agg system and firewall system are providing parallel paths	The firewall is absolutely bypassed, so it does not provide any security to the crypto aggregation system (pre or post crypto). This means no branch-to-core traffic is inspected, branch users are not authenticated, and URL filtering does not take place.	No performance issue	A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection. This also may complicate the routing protocol configuration because there are two viable paths.

Table 8 Comparison of Six Other Firewall Placements in Relation to the Crypto Aggregation System (continued)

4) Single armed crypto agg located on the private network inside of firewall	The firewall can see only packets that are cipher text (encrypted), so no real firewall application inspection can take place, except to just let the VPN tunnel in to the crypto agg system. Also no firewall inspection on packets post decryption (clear text) can occur because no firewall is between crypto aggregation inside and the core network.	No performance issue	May complicate routing protocol configuration because there are two viable paths. A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection.
5) Outside arm of the crypto agg in a parallel path with outside of firewall, and the inside arm of the crypto aggregation system is in a separate DMZ of the firewall	There is no protection for the outside crypto peer. However, this design provides control for the unencrypted traffic coming from the tunnel.	No performance issue	A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection.
6) Inside arm of the crypto agg in a parallel path with the firewall, and the outside arm of the crypto agg system is in a separate DMZ of the firewall	The firewall can see only packets that are cipher text (encrypted), so no real firewall application inspection can take place, except to just let the VPN tunnel into the crypto agg system. Also, no firewall inspection on packets post decryption (clear text) can occur because no firewall is between crypto aggregation inside and the core network.	No performance issue	May complicate routing protocol configuration. A separate WAN router would be required if a WAN circuit (FR, ATM, POS, and so on) is used as the SP connection.

References and Reading

Documents

- IPsec VPN WAN Design Overview—http://www.cisco.com/application/pdf/en/us/guest/netsol/ns130/c649/ccmigration_09186a0080685ce6.pdf
- IPsec Direct Encapsulation Design Guide—http://www.cisco.com/univercd/cc/td/doc/solution/direncap.pdf

- Point-to-Point GRE over IPsec Design Guide—
http://www.cisco.com/univercd/cc/td/doc/solution/p2pgre_x.pdf
- Dynamic Multipoint VPN (DMVPN) Design Guide—
http://www.cisco.com/univercd/cc/td/doc/solution/dmvpn_x.pdf
- Virtual Tunnel Interface (VTI) Design Guide—
http://www.cisco.com/univercd/cc/td/doc/solution/contnet/vti_dgex.pdf
- Voice and Video Enabled IPsec VPN (V3PN) Design Guide—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- Multicast over IPsec VPN Design Guide—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/cdccont_0900aecd80402f07.pdf
- V3PN: Redundancy and Load Balancing Design Guide—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/cdccont_0900aecd8048e105.pdf
- Digital Certificates/PKI for IPsec VPNs—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns656/c649/cdccont_0900aecd804102a1.pdf
- Enterprise QoS SRND—
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf
- Catalyst 6500 Series Switches Denial of Service (DoS) Protection:—
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080435872.html
- Control Plane Policing White Paper—
http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html
- Virtual LAN Security Best Practices—
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml
- SAFE: Best Practices for Securing Routing Protocols—
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008020b51d.shtml
- Infrastructure Protection on Cisco Catalyst 6500 and 4500 Series Switches—<<URL pending>>

Request For Comment (RFC) Papers

- Security Architecture for the Internet Protocol—RFC2401
- IP Authentication Header—RFC2402
- The Use of HMAC-MD5-96 within ESP and AH—RFC2403
- The Use of HMAC-SHA-1-96 within ESP and AH—RFC2404
- The ESP DES-CBC Cipher Algorithm With Explicit IV—RFC2405
- IP Encapsulating Security Payload (ESP)—RFC2406
- The Internet IP Security Domain of Interpretation for ISAKMP—RFC2407

- Internet and Key Management Protocol (ISAKMP)—RFC2408
- The Internet Key Exchange (IKE)—RFC2409
- The NULL Encryption Algorithm and Its Use With IPsec—RFC2410
- IP Security Document Roadmap—RFC2411
- The OAKLEY Key Determination Protocol—RFC2412

Acronyms

Term	Definition
3DES	Triple Data Encryption Standard
ACE	Access Control Entry (one line of an ACL)
ACL	Access Control List
ACS	Access Control Server
AES	Advanced Encryption Standard
AH	Authentication Header
ASA	Cisco Adaptive Security Appliance
ATM	Asynchronous Transfer Mode
CA	Certificate Authority
CAC	Call Admission Control
CAR	Committed Access Rate
CBWFQ	Class Based Weighted Fair Queuing
CEF	Cisco Express Forwarding
CoPP	Control Plane Policing
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
DDOS	Distributed Denial of Service
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multipoint Virtual Private Network
DMZ	De-Militarized Zone
DNS	Domain Name Service
DOS	Denial of Service
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Protocol

FIFO	First In First Out
FQDN	Fully Qualified Domain Name
FR	Frame Relay
FRTS	Frame Relay Traffic Shaping
FTP	File Transfer Protocol
FWSM	Firewall Service Module (for Cisco 7600 Platform)
GRE	Generic Route Encapsulation
iACL	Infrastructure Access Control List
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPmc	IP Multicast
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
Layer 2	OSI reference model Link Layer
Layer 3	OSI reference model Network Layer
Layer 4	OSI reference model Transport Layer
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
MAN	Metropolitan Area Network
mGRE	Multipoint Generic Route Encapsulation
MLPPP	Multi-link Point-to-point Protocol
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NetFlow	Cisco IOS component, collects, and exports traffic statistics
NGWAN	Next Generation Wide Area network
NHRP	Next Hop Resolution Protocol
NHS	Next-Hop Server
OAL	Optimized Access List (feature for Cisco 7600 platform)
OSPF	Open Shortest Path First
p2p GRE	Point to Point Generic Route Encapsulation
PAM	Port Application Mapping
PAT	Port Address Translation
PBR	Policy Based Routing
PE	Premises Equipment

PFC	Policy Feature Card
PIX	Cisco Pix Firewall Series
PKI	Public Key Infrastructure
POS	Packet Over Sonnet
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User System
RRI	Reverse Route Injection
RTP	Real-Time Protocol
SA	Security Association
SAA	Service Assurance Agent
SHA-1	Secure Hash Algorithm One
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SP	Service Provider (same as ISP)
SPA	Shared Port Adapter
SSH	Secure Shell
SSO	Stateful Switch Over
SSP	State Synchronization Protocol
Super-log	Master Remote Syslog Server
Syslog	System logging (originally from Unix environment)
TACACS+	Terminal Access Control – Access Control Server plus
TCP	Transmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
uRPF	Unicast Reverse Path Forwarding
V^3PN	Voice and Video Enabled IPsec VPN
VAM2+	VPN Hardware Acceleration Module (for Cisco VXR platform)
VoIP	Voice over IP
VPN	Virtual Private Network
VPN-SPA	VPN Hardware Acceleration Module (for Cisco 7600 platform)
VSA	VPN Hardware Acceleration Module (for Cisco 7200VXR platform)
VTI	Virtual Tunnel Interface
WAN	Wide Area Network
WRED	Weighted Random Early Detection
X.509	X.509 formatted Digital Certificate