



Cisco SAFE for Medium Enterprise Networks

Executive Summary

As medium enterprises embrace new communication and collaboration tools, transitioning to more Internet-based, media-rich applications, a whole new set of network security challenges arise. Internet-based organized crime and espionage, identity and data theft, botnet infections, and insider attacks are common threats affecting all types of businesses. Particularly attractive to mid-sized businesses, mobile user access technologies and cloud-based services deliver great flexibility and cost-savings, but not without posing new challenges. Understanding the nature and diversity of all threats affecting medium enterprises, and how they may evolve over time, is the first step towards a successful security strategy. Although medium enterprises tend to have fewer locations and employees to protect, tighter budgets and limited resources require medium enterprises to take an innovative and cost-effective approach to security. Additionally, the security strategy should be one that helps the medium enterprise achieve and maintain compliance with the mandated standards and regulations.

This document explains how the proven design and implementation principles of the Cisco SAFE Reference Architecture help secure the medium enterprise by building a solid and reliable network infrastructure that is resilient to both well-known and new forms of attacks. Cisco SAFE provides detailed design and implementation guidelines for organizations looking to build highly secure and reliable networks. Cisco SAFE leverages Cisco's many years of design and deployment experience, and is an architecture that was thoroughly tested and validated as part of the Cisco Validated Design (CVD) program. This document discusses the Cisco SAFE best practices and guidelines that ensure the confidentiality, integrity, and availability of data and system resources supporting the key business functions. Design recommendations presented are based on an understanding of the current and future needs of, and in consideration of the technical and financial constraints often faced by, medium enterprises.

The objective of this guide is to present the Cisco SAFE best practices, designs, and configurations applicable to the medium enterprise, and it aims to provide network and security engineers with the necessary information to help them succeed in designing, implementing, and operating secure network infrastructures based on Cisco products and technologies. Although the target audience is technical in nature, business decision makers, senior IT leaders, and systems architects can benefit from understanding the design driving principles and fundamental security concepts.



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

© 2010 Cisco Systems, Inc. All rights reserved.

Cisco SAFE Security Reference Architecture

The Cisco SAFE Reference Architecture consists of design blueprints based on the Cisco Validated Designs (CVDs) and proven security best practices that provide the design guidelines for building secure and reliable network infrastructures. The Cisco SAFE design blueprints implement defense-in-depth by strategically positioning Cisco products and capabilities across the network, and by leveraging cross-platform network intelligence and collaboration. Multiple layers of security controls are implemented throughout the network, but under a common strategy and administration. Cisco SAFE uses modular designs that accelerate deployment and that facilitate the implementation of new solutions and technologies as business needs evolve. This modularity extends the useful life of existing equipment, protecting capital investments. At the same time, the designs incorporate a set of tools to facilitate day-to-day operations, reducing overall operational expenditures.

The Cisco SAFE uses the Cisco Security Control Framework (SCF), a common framework that drives the selection of products and features that maximize visibility and control, the two most fundamental aspects driving security. Also used by Cisco's Continuous Improvement Lifecycle services, the framework facilitates the integration of Cisco's rich portfolio of security services designed to support the entire solution lifecycle.

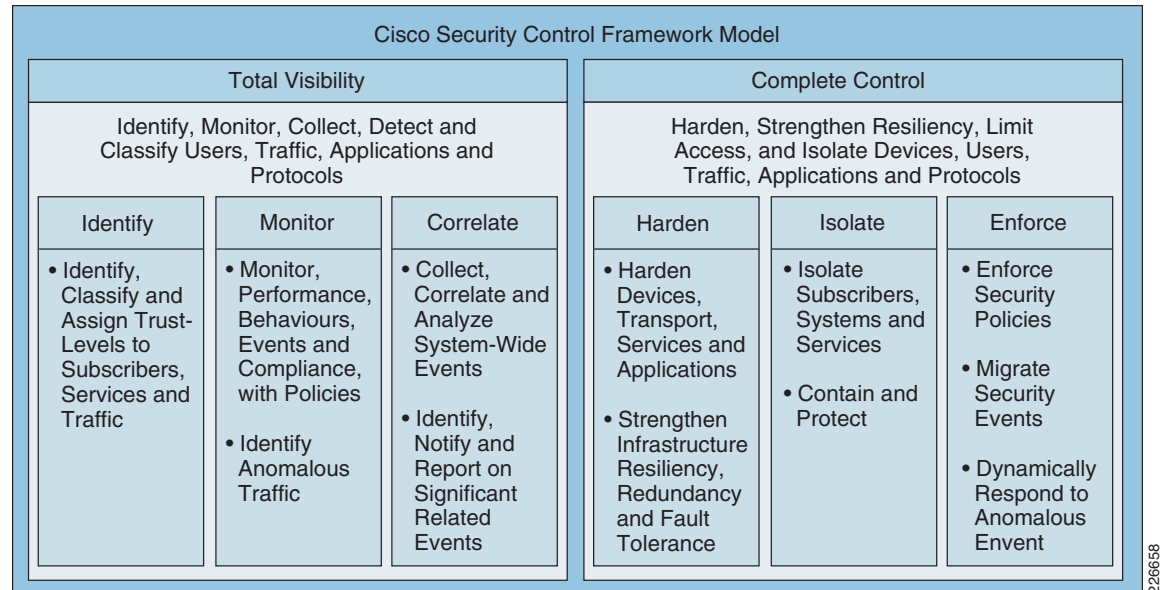
Cisco Security Control Framework (SCF)

The Cisco SCF is a security framework aimed at ensuring network and service availability and business continuity. Because security threats are an ever-moving target, the SCF is designed to address current threat vectors, as well as track new and evolving threats, through the use of best common practices and comprehensive solutions. Cisco SAFE uses SCF to create network designs that ensure network and service availability and business continuity. Cisco SCF drives the selection of the security products and capabilities, and guides their deployment throughout the network where they best enhance visibility and control.

SCF assumes the existence of security policies developed as a result of threat and risk assessments, and in alignment with business goals and objectives. The security policies and guidelines are expected to define the acceptable and secure use of each service, device, and system in the environment. The security policies should also determine the processes and procedures needed to achieve the business goals and objectives. The collection of processes and procedures define security operations. It is crucial to business success that security policies, guidelines, and operations do not prevent but rather empower the organization to achieve its goals and objectives.

The success of the security policies ultimately depends on the degree they enhance visibility and control. Simply put, security can be defined as a function of visibility and control. Without any visibility, there is no control; and without any control, there is no security. Therefore, SCF's main focus is on enhancing visibility and control. In the context of SAFE, SCF drives the selection and deployment of platforms and capabilities to achieve a desirable degree of visibility and control.

SCF defines six security actions that help enforce the security policies and improve visibility and control, as shown in [Figure 1](#). Visibility is enhanced through the actions of identify, monitor, and correlate. Control is improved through the actions of harden, isolate, and enforce.

Figure 1 Cisco Security Control Framework

The SAFE designs are derived from the application of SCF to each place in an enterprise network, such as the data center, campus, and branch offices. The result is the identification of technologies and best common practices that best satisfy each of the six key actions for visibility and control. In this way, SAFE designs incorporate a variety of technologies and capabilities throughout the network to gain visibility into network activity, enforce network policy, and address anomalous traffic. As a result, network infrastructure elements such as routers and switches are used as pervasive, proactive policy-monitoring and enforcement agents.

Cisco SAFE Architecture Principles

The Cisco SAFE design blueprints were created according to the following architecture principles:

- Defense in depth—Multi-layer security is embedded throughout the entire infrastructure, endpoints, and applications.
- Global and local intelligence and collaboration—Cloud-based threat information, reputation-based intelligence, and local event and posture information are shared across safeguards for greater visibility and control under a common strategy.
- Service availability and resiliency—Multi-level redundancy and device hardening are included.
- Modularity and flexibility—Functional modular designs for maximum flexibility and adaptability are provided.
- Operational efficiency—Tools and procedures are provided to verify the effectiveness and proper operation of safeguards.
- Regulatory compliance—A rich set of security practices and functions commonly required by regulations and standards are delivered.

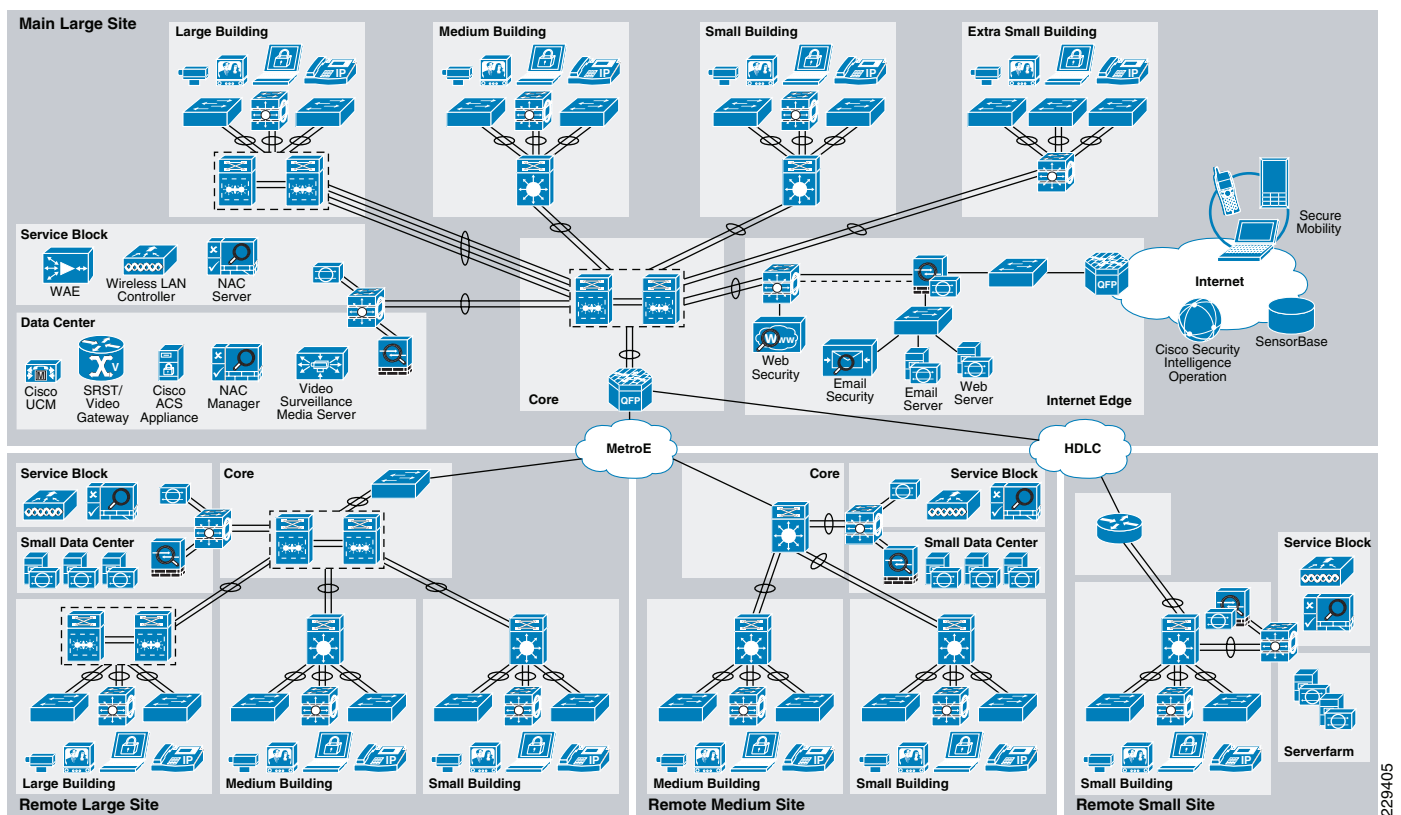
For more information on the Cisco SAFE Reference Architecture, see: <http://www.cisco.com/go/safe>.

Underlying Network Design

The Cisco SAFE security best practices, designs, and configurations presented in this document were integrated and validated using the network design for medium enterprises as documented in the Medium Enterprise Design Profile. The Medium Enterprise Design Profile is a Cisco Validated Design (CVD) network architecture that enables medium enterprises to deliver all the services required for an enhanced business environment. The Medium Enterprise Design Profile includes a routing and switching LAN foundation and integrates services such as WAN connectivity, security, unified communications, and mobility.

The Medium Enterprise Design Profile is based on a validated network architecture designed around both business operations and technical considerations. Because cost is a common limiting factor to medium enterprise network designs, the architecture topologies and platforms were carefully selected to increase productivity while reducing overall costs. The Medium Enterprise Design Profile accommodates a main site and one or more remote sites of various sizes, interconnected over a metro Ethernet or managed WAN service. Each of these sites may contain one or more buildings of varying sizes, as shown in Figure 2.

Figure 2 *Secure Enterprise Design*



At the heart of the architecture is a robust routing and switching network. Operating on top of this network are all the services used within the enterprise environment, such as safety and security systems, voice communications, business databases, ordering systems, payroll, accounting and customer relationship management (CRM) applications, and so on. The core of these services are deployed and managed at the main site, allowing the enterprise to reduce the need for separate services to be operated and maintained at various remote locations. These centralized systems and applications are served by a data center at the main site.

The network design used for the Medium Enterprise Design Profile is based around the desire to represent as many medium enterprise environments as possible. To accomplish this, a modular design is used, represented by sites and buildings of varying sizes. The sites are made up of one or more buildings of varying sizes where buildings are sized with the determining factor being the number of users or connections in that building as well as physical size. Additionally, it is expected that at least half of the network connections will be wireless.

The main headquarters site and large remote site designs are meant to represent significantly sized sites containing the largest user populations. The design for the main headquarters site can accommodate up to six buildings of varying sizes ranging from large to extra small. Each building within the main site connects back to the resilient core located in the main building of that site via multiple 10 GB Ethernet links. The core also typically connects to a data center and service block within the main building. The large remote site connects to the main headquarters site via a 1 GB Metro Ethernet link. The main HQ site and large remote site are almost identical, with the exception that the main site is connected to outside entities such as the Internet using the Internet edge components, and also has all other sites within the enterprise connecting to it.

The medium remote site design is targeted at enterprise sites that have approximately three buildings ranging in size from medium to small. Each building within the medium site connects to the core located in one of the buildings at that site via multiple 10 GB links, and the core also connects to a small data center (or serverfarm) and service block. The medium site is connected to the main HQ site via a 100 MB Metro Ethernet link. This link to the main site provides connectivity to the other sites as well as external networks such as the Internet.

The small remote site design represents a site with just one building. In this case, the core and distribution layers are collapsed into one. The small site is connected to the main site via a fractional DS3 with a 20 MB bandwidth rating. The link to the main site provides connectivity to the other sites as well as external networks such as the Internet.

There are four building profiles: large, medium, small, and extra small. All buildings have access switches that connect users. The buildings also have distribution switches that connect the access switches together as well as connect the building itself to the core network. The core switches should reside in a centrally located building.

The large building is designed for 1600 Ethernet access ports ranging in bandwidth from 100 MB to 1 GB. The ports are distributed over four floors, each floor having 400 access ports. There are 80 wireless access points using the IEEE 802.11 ABGN standards with 20 access points per floor. Additionally, there are six outdoor mesh access points to cover the outdoor skirt of the building.

The medium building was designed for 800 Ethernet access ports ranging in bandwidth from 100 MB to 1 GB. The ports are distributed over two floors, each floor having 400 access ports. There are 40 wireless access points using the IEEE 802.11 ABGN standards with 20 access points per floor. Additionally, there are four outdoor mesh access points to cover the outdoor skirt of the building.

The small building is designed for 200 Ethernet access ports ranging in bandwidth from 100 MB to 1 GB. The ports are all located on one floor. There are ten wireless access points using the IEEE 802.11 ABGN standards, and two outdoor mesh access points to cover the outdoor skirt of the building.

The extra small building is designed for 48 100 MB Ethernet access ports. The ports are all located on one floor. There are three wireless access points using the IEEE 802.11 ABGN standards, and one outdoor mesh access point to cover the outdoor skirt of the building.

For information on the details of the LAN, WAN, and Mobility design within the Medium Enterprise Design Profile, see:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/MEDP.html.

Medium Enterprise Network Security Design

The medium enterprise design presented in this document implements security following the guidelines of the Cisco SAFE Security Reference Architecture. The architecture is designed with built-in security to protect the infrastructure and to provide a secure online environment for businesses. A series of network security technologies and products are strategically deployed throughout the network to protect employees and company assets, to guarantee confidentiality of sensitive data, and to ensure the availability and integrity of systems and data. Safeguards were carefully chosen to mitigate well-known attacks as well as emerging threats. Understanding the diverse nature of threats and how they may evolve over time is the first step towards a successful enterprise security strategy.

The following are some of the common threats to enterprise environments:

- Service disruption—Disruption to the infrastructure, applications, and other business resources caused by botnets, worms, malware, adware, spyware, viruses, denial-of-service (DoS) attacks, and Layer 2 attacks
- Network abuse—Use of non-approved applications by employees, peer-to-peer file sharing and instant messaging abuse, and access to non-business-related content
- Unauthorized access—Intrusions, unauthorized users, escalation of privileges, IP spoofing, and unauthorized access to restricted resources
- Data loss—Loss or leakage of private data from servers and endpoints while in transit or as a result of spyware, malware, key-loggers, viruses, and so on
- Identity theft and fraud—Theft of personal identity or fraud on servers and end users through phishing and E-mail spam

As shown in [Figure 2](#), applying the Cisco SAFE principles to the medium enterprise network design requires using a defense-in-depth approach where multiple layers of security protection are integrated into the architecture. The various security products and technologies are combined to provide enhanced visibility and control.

The medium enterprise network security design focuses on the following key security elements:

- Network Foundation Protection
- Device hardening, control plane, and management plane protection throughout the entire infrastructure
- Ensuring the availability, resiliency, and integrity of the network infrastructure
- Internet perimeter protection
 - Ensuring safe connectivity to the Internet
 - Protecting internal resources and users from botnets, malware, viruses, and other malicious software
 - Protecting employees from harmful content
 - Enforcing E-mail and Web browsing policies to prevent identity theft and fraud
 - Blocking command and control traffic from infected internal bots to external hosts
- Data center protection
 - Ensuring the availability and integrity of centralized applications and systems
 - Protecting the confidentiality and privacy of proprietary and sensitive data
- Network access security and control
 - Securing the access edges

- Enforcing authentication and role-based access for users residing at the main site and remote sites
- Ensuring that systems are up-to-date and in compliance with the enterprise’s network security policies
- Secure mobility
 - Providing secure, persistent connectivity to all mobile employees on laptops, smartphones, and other mobile platforms; enforcing encryption, authentication, and role-based access to all mobile users
 - Delivering consistent protection to all mobile employees from viruses, malware, botnets, and other malicious software
 - Ensuring a persistent enforcement of enterprise network security policies to all users; making sure systems comply with corporate policies and have up-to-date security

Together, these key security areas create a defense-in-depth solution for protecting medium enterprises from common security threats such as service disruption, network abuse, unauthorized access, data loss, and identity theft and fraud. Design guidelines and best practices for key areas of the medium enterprise network security design are detailed in the following sections.

**Note**

Network management is out of the scope of this document. For best practices in implementing network management, see “Chapter 9, Management” of the *Cisco SAFE Reference Guide* at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap9.html

Network Foundation Protection

Medium enterprise networks are built with routers, switches, and other infrastructure network devices that keep the applications and services running. These infrastructure devices must be properly hardened and secured to maintain continued operation and access to these services.

To ensure the availability of the medium enterprise network infrastructure, the security design leverages the Network Foundation Protection best practices for the following areas:

- Infrastructure device access
 - Restrict management device access to authorized parties and via only authorized ports and protocols.
 - Enforce authentication, authorization, and accounting (AAA) with Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) to authenticate access, authorize actions, and log all administrative access.
 - Display legal notification banners.
 - Ensure confidentiality by using secure protocols such as Secure Shell (SSH) and HTTPS.
 - Enforce idle and session timeouts.
 - Disable unused access lines.
- Routing infrastructure
 - Restrict routing protocol membership by enabling Message-Digest 5 (MD5) neighbor authentication and disabling default interface membership.
 - Enforce route filters to ensure that only legitimate networks are advertised, and networks that are not supposed to be propagated are never advertised.

- Log status changes of neighbor sessions to identify connectivity problems and denial-of-service (DoS) attempts on routers.
- Device resiliency and survivability
 - Disable unnecessary services.
 - Implement control plane policing (CoPP).
 - Enable traffic storm control.
 - Implement topological, system, and module redundancy for the resiliency and survivability of routers and switches and to ensure network availability.
 - Keep local device statistics.
- Network telemetry
 - Enable Network Time Protocol (NTP) time synchronization.
 - Collect system status and event information with Simple Network Management Protocol (SNMP), Syslog, and TACACS+/RADIUS accounting.
 - Monitor CPU and memory usage on critical systems.
 - Enable NetFlow to monitor traffic patterns and flows.
- Network policy enforcement
 - Implement access edge filtering.
 - Enforce IP spoofing protection with access control lists (ACLs), Unicast Reverse Path Forwarding (uRPF), and IP Source Guard.
- Switching infrastructure
 - Implement a hierarchical design, segmenting the LAN into multiple IP subnets or virtual LANs (VLANs) to reduce the size of broadcast domains.
 - Protect the Spanning Tree Protocol (STP) domain with BPDU Guard and STP Root Guard.
 - Use Per-VLAN Spanning Tree (PVST) to reduce the scope of possible damage.
 - Disable VLAN dynamic trunk negotiation on user ports.
 - Disable unused ports and put them into an unused VLAN.
 - Implement Cisco Catalyst Infrastructure Security Features (CISF) including Port Security, Dynamic ARP Inspection, DHCP snooping, and IP Source Guard.
 - Use a dedicated VLAN ID for all trunk ports.
 - Explicitly configure trunking on infrastructure ports.
 - Use all tagged mode for the native VLAN on trunks and drop untagged frames.
- Network management
 - Ensure the secure management of all devices and hosts within the enterprise network infrastructure.
 - Authenticate, authorize, and keep records of all administrative access.
 - If possible, implement a separate out-of-band (OOB) management network (hardware- or VLAN-based) to manage systems local to the main site.
 - Secure the OOB management access by enforcing access controls, using dedicated management interfaces or virtual routing and forwarding (VRF) tables.

- Provide secure in-band management access for systems residing at the remote sites by deploying firewalls and ACLs to enforce access controls, using Network Address Translation (NAT) to hide management addresses, and using secure protocols such as SSH and HTTPS.
- Ensure time synchronization by using NTP.
- Secure management servers and endpoints with endpoint protection software and operating system (OS) hardening best practices.

For more detailed information on the NFP best practices including configuration examples, see “Chapter 2, Network Foundation Protection” in the *Cisco SAFE Reference Guide* at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap2.html.

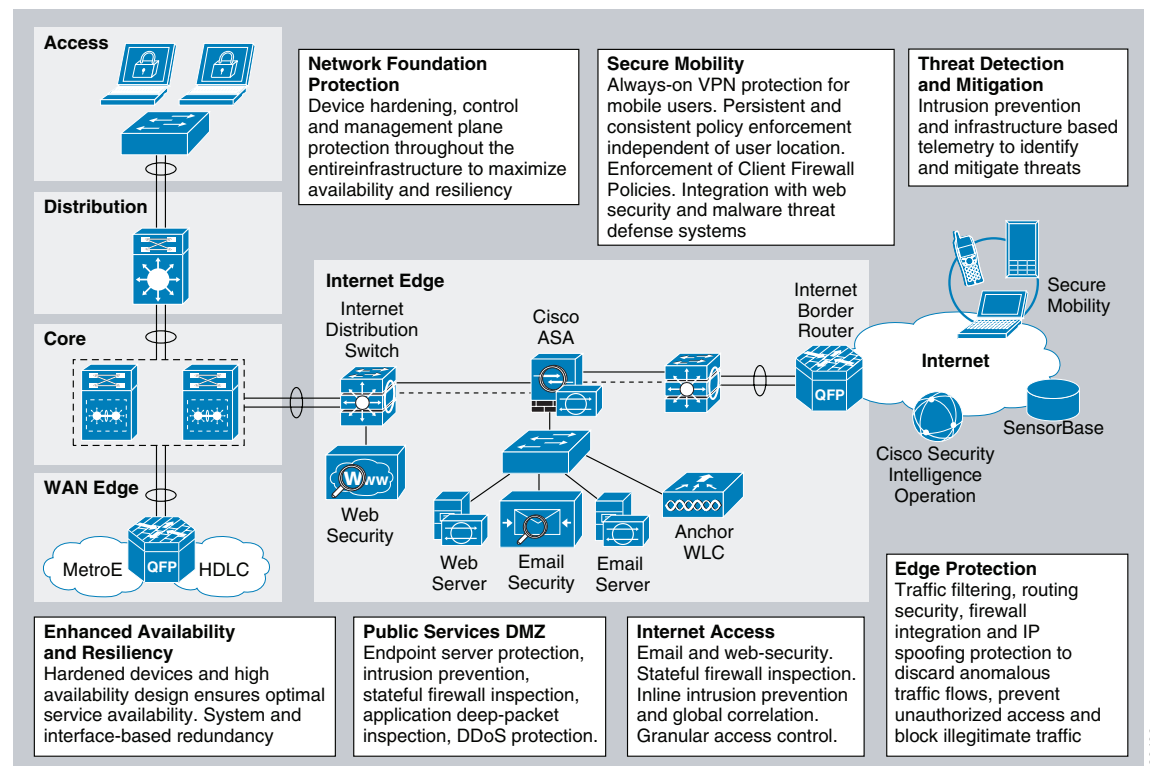
Internet Perimeter Protection

The medium enterprise network design assumes a centralized connection to the Internet at the headquarters or main site. This connection serves users at the main site as well as all remote sites or offices. Common services typically provided by this connection include the following:

- E-mail and Internet Web browsing for employees
- Hosting of a company’s Web portal accessible to clients and partners over the Internet
- Secure remote access to the enterprise network for mobile users and remote workers
- Other services may also be provided using the same infrastructure

The part of the network infrastructure that provides connectivity to the Internet is defined as the Internet perimeter, as shown in [Figure 3](#).

Figure 3 Internet Perimeter



229406

The Internet perimeter provides safe and secure centralized access to the Internet for employees and guest users residing at all locations. It also provides access to public services such as the company's Web portal and public services without compromising the confidentiality, integrity, and availability of the resources and data of the enterprise. To provide secure access, the Internet perimeter should incorporate the following security functions:

- **Internet border router**—The Internet border router is the gateway responsible for routing traffic between the enterprise and the Internet. It may be administered by the company's IT staff or may be managed by the Internet service provider. This router provides the first line of protection against external threats and should be hardened according to the NFP best practices.
- **Internet firewall**—A Cisco Adaptive Security Appliance (ASA) provides stateful access control and deep packet inspection to protect enterprise resources and data from unauthorized access and disclosure. In addition, the Cisco ASA Botnet Traffic Filter feature can be enabled to defend the enterprise against botnet threats. Once enabled, the Botnet Traffic Filter feature monitors network ports for rogue activity and detects and blocks traffic from infected internal endpoints, sending command and control traffic back to a host on the Internet. The ASA is configured to control or prevent incoming access from the Internet, to protect the enterprise Web portal and other Internet public services, and to control user traffic bound towards the Internet. The security appliance may also provide secure remote access to employees with the Cisco AnyConnect Secure Mobility client.
- **Intrusion prevention**—An Advanced Inspection and Prevention Security Service Module (AIP SSM) on the Cisco ASA or a separate IPS appliance can be implemented for enhanced threat detection and mitigation. The IPS module or appliance is responsible for identifying and blocking anomalous traffic and malicious packets recognized as well-known attacks. IPS can be deployed in either inline or promiscuous mode. The module or appliance may be configured to participate in Cisco IPS Global Correlation, allowing the IPS to gain visibility on global threats as they emerge in the Internet and to quickly react to contain them. IPS may also be configured to help block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on.
- **Public services demilitarized zone (DMZ)**—The company's external Internet Web portal, mail server, and other public facing servers and services are placed on a DMZ for security and control purposes. The DMZ acts as a middle stage between the Internet and enterprise private resources, preventing external users from directly accessing any internal servers and data. The Internet firewall is responsible for restricting incoming access to the public services in the DMZ, and controls outbound access from DMZ resources to the Internet. Systems residing within the DMZ should be hardened with endpoint protection software and OS hardening best practices.
- **E-mail security**—A Cisco IronPort C Series E-Mail Security Appliance (ESA) is deployed in the DMZ to inspect incoming and outgoing E-mails and eliminate threats such as E-mail spam, viruses, and worms. The ESA appliance also offers E-mail encryption to ensure the confidentiality of messages, and data loss prevention (DLP) to detect the inappropriate transport of sensitive information.
- **Web security**—A Cisco IronPort S Series Web Security Appliance (WSA) is deployed at the distribution switches to inspect HTTP and HTTPS traffic bound to the Internet. The WSA enforces URL filtering policies to block access to websites containing non-business-related content or that are known sources of spyware, adware, botnets, or other types of malware. The WSA may also be configured to block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on.
- **Guest access wireless LAN controller**—The Cisco Unified Wireless LAN Guest Access option offers a flexible, easy-to-implement method for deploying wireless guest access via Ethernet over IP (RFC3378). Ethernet over IP (EoIP) tunneling is used between two wireless LAN controller (WLC) endpoints in the centralized network design. A WLC is located in the Internet perimeter DMZ, where it is referred to as an *anchor controller*. The anchor controller is responsible for terminating EoIP tunnels originating from centralized campus WLCs located in the services block,

and interfacing the traffic from these controllers to a firewall or border router. Traffic to and from this guest access WLAN is tunneled to the DMZ transparently, with no visibility by, or interaction with, other traffic in the enterprise internal network. For more information on the wireless guest access solution, see the *Medium Enterprise Design Profile Mobility Design* document at: http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

The following subsections describe the design guidelines for implementing the above security functions.

Internet Border Router Security Guidelines

The Internet border router provides connectivity to the Internet through one or more Internet service providers. The router acts as the first line of defense against unauthorized access, distributed DoS (DDoS), and other external threats. ACLs, uRPF, and other filtering mechanisms should be implemented for anti-spoofing and to block invalid packets. NetFlow, Syslog, and SNMP should be used to gain visibility on traffic flows, network activity, and system status. In addition, the Internet border router should be hardened and secured following the best practices explained in [Network Foundation Protection](#). This includes restricting and controlling administrative access, protecting the management and control planes, and securing the dynamic exchange of routing information.

[Internet Border Router Edge ACL Deployment](#) provides a sample configuration of an Internet Edge ACL. For more information on how to secure and configure the Internet border router, see “Chapter 6, Enterprise Internet Edge” in the *Cisco SAFE Reference Guide* at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap6.html.

Internet Firewall Guidelines

A Cisco ASA firewall should be deployed at the Internet perimeter to protect the enterprise internal resources and data from external threats, and is responsible for the following:

- Preventing incoming access from the Internet
- Protecting public resources deployed in the DMZ by restricting incoming access to the public services and by limiting outbound access from DMZ resources out to the Internet
- Controlling user Internet-bound traffic
- Monitoring network ports for rogue activity and preventing infected internal endpoints from communicating with botnet masters or command and control hosts on the Internet

The Cisco ASA should be configured to enforce access policies, keep track of connection status, and inspect packet payloads. Examples of the needed access policies include the following:

- Deny or control any connection attempts originating from the Internet to internal resources and subnets.
- Allow outbound Internet access for users residing at any of the enterprise locations and for the protocols permitted by the organization’s policies; that is, HTTP and HTTPS.
- Allow outbound SSL access to the Internet for devices requiring administrative updates such as SensorBase, IPS signature updates, and so on.
- Allow user access to DMZ services such as the company’s web portal, E-mail, and domain name resolution (HTTP, HTTPS, SMTP, point-of-presence [POP], Internet Message Access Protocol [IMAP], Domain Name Service [DNS]).
- Restrict inbound Internet access to the DMZ for the necessary protocols and servers (HTTP to web server, SMTP to Mail Transfer Agent, DNS to DNS servers, and so on).

- Restrict connections initiated from the DMZ to only necessary protocols and sources (DNS from DNS server, SMTP from mail server, and HTTP/SSL from Cisco IronPort ESA).
- Enable stateful inspection for the outbound protocols being used to ensure returning traffic is dynamically allowed by the firewall.
- Prevent access to the anchor WLC deployed in the DMZ for guest access except for tunneled traffic coming from the centralized campus WLCs (UDP port 16666 and IP protocol ID 97) and traffic needed to manage it (SNMP, TFTP, HTTP, HTTPS, SSH).
- Implement NAT and Port Address Translation (PAT) to shield the internal address space from the Internet.

**Note**

Whenever available, a dedicated management interface should be used. However, in cases where the firewall is managed in-band, identify the protocols and ports required before configuring the firewall ACLs.

When deploying the Internet firewall, it is important to understand the traffic and policy requirements when selecting a firewall. An appropriately sized Cisco ASA model should be chosen so that it does not become a bottleneck. The Cisco ASA should also be hardened following the NFP best practices as described in [Network Foundation Protection](#). This includes restricting and controlling administrative access, securing dynamic exchange of routing information with MD5 authentication, and enabling firewall network telemetry with SNMP, Syslog, and NetFlow.

In the medium enterprise design, high availability is achieved by using redundant physical interfaces. This represents the most cost-effective solution for high-availability. As an alternative, a pair of firewall appliances can be deployed in stateful failover using separate boxes at a higher cost.

Cisco ASA Botnet Traffic Filter

The Cisco ASA Botnet Traffic Filter feature can be enabled to monitor network ports for rogue activity and to prevent infected internal endpoints from sending command and control traffic back to an external host on the Internet. The Botnet Traffic Filter on the ASA provides reputation-based control for an IP address or domain name, similar to the control that Cisco IronPort SensorBase provides for E-mail and web servers.

The Cisco Botnet Traffic Filter is integrated into all Cisco ASA appliances, and inspects traffic traversing the appliance to detect rogue traffic in the network. When internal clients are infected with malware and attempt to phone home to an external host on the Internet, the Botnet Traffic Filter alerts the system administrator of this through the regular logging process and can be automatically blocked. This is an effective way to combat botnets and other malware that share the same phone-home communications pattern.

The Botnet Traffic Filter monitors all ports and performs a real-time lookup in its database of known botnet IP addresses and domain names. Based on this investigation, the Botnet Traffic Filter determines whether a connection attempt is benign and should be allowed, or is a risk and should be blocked.

The Cisco ASA Botnet Traffic Filter has three main components:

- Dynamic and administrator blacklist data—The Botnet Traffic Filter uses a database of malicious domain names and IP addresses that is provided by Cisco Security Intelligence Operations. This database is maintained by Cisco Security Intelligence Operations and is downloaded dynamically from an update server on the SensorBase network. Administrators can also configure their own local blacklists and whitelists.

- Traffic classification and reporting—Botnet Traffic Filter traffic classification is configured through the **dynamic-filter** command on the ASA. The dynamic filter compares the source and destination addresses of traffic against the IP addresses that have been discovered for the various lists available (dynamic black, local white, local black), and logs and reports the hits against these lists accordingly.
- DNS snooping—To map IP addresses to domain names that are contained in the dynamic database or local lists, the Botnet Traffic Filter uses DNS snooping in conjunction with DNS inspection. Dynamic Filter DNS snooping looks at User Datagram Protocol (UDP) DNS replies and builds a DNS reverse cache (DNSRC), which maps the IP addresses in those replies to the domain names they match. DNS snooping is configured via the Modular Policy Framework (MPF) policies

The Botnet Traffic Filter uses two databases for known addresses. Both databases can be used together, or the dynamic database can be disabled and the static database can be used alone. When using the dynamic database, the Botnet Traffic Filter receives periodic updates from the Cisco update server on the Cisco IronPort SensorBase network. This database lists thousands of known bad domain names and IP addresses.

**Note**

The SensorBase network is an extensive network that monitors global E-mail and web traffic for anomalies, viruses, malware, and other abnormal behavior. The network is composed of the Cisco IronPort appliances, Cisco ASA, and Cisco IPS appliances and modules installed in more than 100,000 organizations worldwide, providing a large and diverse sample of Internet traffic patterns.

The Cisco ASA uses this dynamic database as follows:

- When the domain name in a DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to the DNS reverse lookup cache.
- When the infected host starts a connection to the IP address of the malware site, the Cisco ASA sends a syslog message reporting the suspicious activity and optionally drops the traffic if the Cisco ASA is configured to do so.
- In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs or drops any traffic to that IP address without having to inspect DNS requests.

The database files are stored in running memory rather than Flash memory. The database can be deleted by disabling and purging the database through the configuration.

**Note**

To use the database, be sure to configure a domain name server for the Cisco ASA so that it can access the URL of the update server. To use the domain names in the dynamic database, DNS packet inspection with Botnet Traffic Filter snooping needs to be enabled; the Cisco ASA looks inside the DNS packets for the domain name and associated IP address.

In addition to the dynamic database, a static database can be used by manually entering domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist. Static blacklist entries are always designated with a Very High threat level. Domain names or IP addresses can also be entered in a whitelist.

When a domain name is added to the static database, the Cisco ASA waits one minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the DNS host cache. This action is a background process, and does not affect your ability to continue configuring the ASA. Cisco also recommends that DNS packet inspection be enabled with Botnet Traffic Filter snooping. When enabled, the Cisco ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The Cisco ASA DNS server is unavailable.
- A connection is initiated during the one minute waiting period before the Cisco ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the Cisco ASA looks inside the DNS packets for the domain name and associated IP address, and adds the name and IP address to the DNS reverse lookup cache.

If Botnet Traffic Filter snooping is not enabled, and one of the above circumstances occurs, that traffic is not monitored by the Botnet Traffic Filter.



Note

It is important to realize that a comprehensive security deployment should include Cisco Intrusion Prevention Systems (IPS) with its reputation-based Global Correlation service and IPS signatures in conjunction with the security services provided by the Cisco ASA security appliance such as Botnet Traffic Filter.

For more information on the Cisco ASA Botnet Traffic Filter feature, see:

http://www.cisco.com/en/US/prod/vpndevc/ps6032/ps6094/ps6120/botnet_index.html.

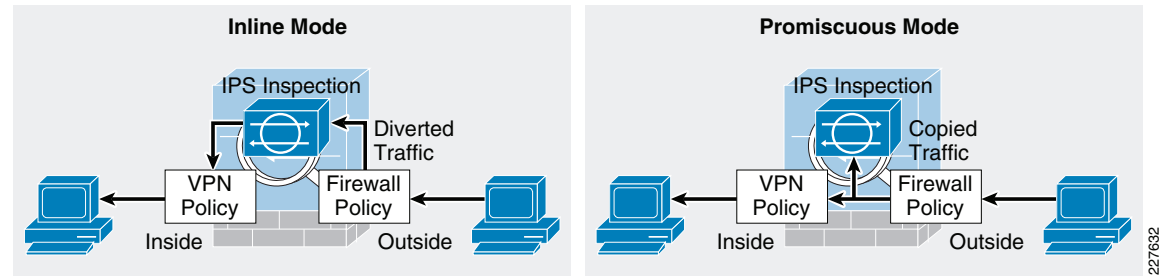
Intrusion Prevention Guidelines

IPS is responsible for identifying and blocking anomalous traffic and packets recognized as well-known attacks. An AIP SSM IPS module on the Cisco ASA Internet firewall or a separate IPS appliance can be implemented in the Internet perimeter for enhanced threat detection and mitigation. IPS may also be configured to help block certain Internet applications such as AOL Messenger, BitTorrent, Skype, and so on.

Integrating IPS on a Cisco ASA appliance using an AIP SSM provides a cost-effective solution for medium enterprise networks. The AIP SSM is supported on Cisco ASA 5510 and higher platforms. The AIP SSM runs advanced IPS software providing proactive, full-featured intrusion prevention services to stop malicious traffic before it can affect the enterprise network.

The AIP SSM may be deployed in inline or promiscuous mode:

- **Inline mode**—The AIP SSM is placed directly in the traffic flow (see the left side of [Figure 4](#)). Traffic identified for IPS inspection cannot continue through the Cisco ASA without first passing through and being inspected by the AIP SSM. This mode is the most secure because every packet that has been identified for inspection is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput if not designed or sized appropriately.
- **Promiscuous mode**—A duplicate stream of traffic is sent to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, in promiscuous mode the AIP SSM can block traffic only by instructing the ASA to shun the traffic or by resetting a connection on the ASA. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the ASA before the AIP SSM can shun it. The right side of [Figure 4](#) shows the AIP SSM in promiscuous mode.

Figure 4 *IPS Inline and Promiscuous Mode*

The recommended IPS deployment mode depends on the goals and policies of the enterprise. IPS inline mode is more secure because of its ability to stop malicious traffic in real-time; however, it may impact traffic throughput if not properly designed or sized. Conversely, IPS promiscuous mode has less impact on traffic throughput but is less secure because there may be a delay in reacting to the malicious traffic.

Although the AIP SSM runs as a separate application within the Cisco ASA, it is integrated into the traffic flow. The AIP SSM contains no external interfaces itself, except for the management interface on the SSM itself. When traffic is identified for IPS inspection on the Cisco ASA, traffic flows through the ASA and the AIP SSM in the following sequence:

1. Traffic enters the ASA.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane.
4. The AIP SSM applies its security policy to the traffic and takes appropriate actions.
5. (Inline mode only) Valid traffic is sent back to the ASA over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. Remote access VPN policies are applied (if configured).
7. Traffic exits the ASA.

The AIP SSM card may be configured to fail open or close when the module becomes unavailable. When configured to fail open, the ASA allows all traffic through, uninspected, if the AIP SSM becomes unavailable. Conversely, when configured to fail close, the ASA blocks all traffic in case of an AIP SSM failure.

Cisco IPS Global Correlation

The AIP SSM module on the Cisco ASA (or IPS appliance) may also participate in Cisco Global Correlation for further threat visibility and control. Once enabled, the participating IPS sensor receives threat updates from the Cisco SensorBase network at regular intervals. The Cisco SensorBase network contains detailed information about known threats on the Internet, including serial attackers, botnet harvesters, malware outbreaks, and dark nets. IPS incorporates the global threat data into its system to detect and prevent malicious activity even earlier allowing IPS to filter out the worst attackers before they have a chance to attack critical assets.

IPS Global Correlation is an important improvement in the basic functions of IPS because it enables it to understand the world in which it operates—an understanding of who the attacker is and whether the attacker has a record of bad behavior. With Global Correlation, the sensor does not have to rely on just the data in the packet or connection to make a decision about the intent of the activity and determine whether the activity is malicious. Now, the sensor can look at a ping sweep and know that the source of the ping sweep does not have a negative reputation, but later can look at another ping sweep and see that

the source is a known malicious site with a history of web attacks, and the sensor can block access to and from that site. Global Correlation provides users greater confidence in the actions the sensor takes because these actions are applied to attackers that have shown a predisposition for malicious behavior.

Global Correlation provides a process through which security data is collected for IP addresses and a reputation score is developed for each IP address globally by Cisco. Cisco IPS 7.0 uses this reputation data in the following two ways:

- **Reputation filters**—Used to block a subset of IP networks that are owned wholly by malicious groups or were unused and have been hijacked. This first line of defense helps prevent malicious contact ranging from spam to intelligence gathering in preparation for directed attacks. Reputation filters also prevent attempts by botnets to phone home if the botnet controller machine resides in one of these networks.
- **Global Correlation inspection**—Uses reputation scores for normal IP addresses to increase the percentage of attacks that the sensor can block. First, the sensor must detect some sort of malicious activity and fire an event as a result. When an event is triggered, that event is processed to determine whether the attacker's IP address has a negative reputation and to what degree. If the event is sourced from an attacker with a negative reputation, the sensor adds risk to the event, raising its risk rating and making it more likely that the sensor will deny the event. This enables the sensor to deny packets and attackers based on the fact that the event has a negative reputation in addition to a high risk rating calculated on the sensor.

When Global Correlation is configured, the IPS works in the following manner:

1. When a packet enters the sensor, the first check is against the preprocessor, which performs Layer 2 packet normalization and atomic signature checks. Here the packet header is processed to help ensure that the packet is an IP packet, that the header is not incorrectly formed, and that the packet does not match any atomic signatures.
2. Next, the packet is sent through the Cisco IPS reputation filters. Packets that match are discarded immediately, assuming that the reputation filters are enabled and not in Audit mode. Packets that do not match go to the inspection engines, starting with the Layer 3 and 4 normalization engine, then all the signature engines, and then anomaly detection.
3. If any events are triggered, alerts are sent to the Global Correlation inspection processor, where the source IP address for any alert is checked for negative reputation, and the risk rating is modified and actions are added as appropriate.
4. Finally, any actions assigned to alerts are processed and acted upon, including event action overrides to add new actions and event action filters to remove actions

Reputation Filters

Cisco IPS reputation filters use a list of hundreds of networks that can be safely blocked because they are not owned by any legitimate source. The reputation of the networks on this list can be considered to be -10. This list includes only IP networks consisting entirely of stolen, “zombie” address blocks and address blocks controlled entirely by malicious organizations. Individual IP addresses are never found on this list. Because there is no way that a legitimate IP address can go from a positive or neutral reputation and then, because of malicious activity, earn a place on the Cisco IPS reputation filter list, users can confidently block all activity to and from networks on this list.

The primary purpose of the IPS reputation filters is to provide protection from direct scanning, botnet harvesting, spamming, and DDoS attacks originating from these malicious address blocks and from connections being attempted back to these networks from systems already infected. Packets that match the IPS reputation filters, are dropped before signature inspection.

**Note**

There is currently no capability to view the networks on this list, but the networks that are being blocked get logged by the sensor in the Statistics section of Cisco IPS Manager Express (IME).

The only user configuration required for reputation filters is enabling or disabling them and specifying whether Global Correlation is set to Audit mode (a global configuration setting for the entire sensor). In Audit mode, the sensor reports potential deny actions because of reputation filters instead of actually denying the activity.

Global Correlation Inspection

The primary activity of an IPS sensor is the detection of malicious behavior. After the packet goes through the IPS reputation filter process, the signature inspection occurs. This involves inspection of packets flowing through the sensor by the various engines looking for the various types of malicious behavior. Alerts that are created are passed to the Global Correlation inspection process for reputation lookups.

When an event occurs, the Global Correlation inspection process performs a local lookup of the source (attacker) IP address of the event in its reputation database. This lookup process returns a value ranging from -1 to -10 ; the more negative the value, the more negative the reputation of the source IP address. This reputation score is calculated for Cisco IPS sensors using the data in Cisco SensorBase and is sent to the sensor as a reputation update. If an IP address returns no value for reputation, it is considered to be neutral. Cisco IPS, unlike E-mail and web security reputation applications, has no concept of positive reputation. When an event is checked for reputation, this checking occurs entirely on the sensor using data downloaded previously from Cisco SensorBase. Unlike other devices, the sensor does not send a live request for information about an IP address that it has just seen. It looks in the data that it has, and if it finds the address, it uses that data; otherwise, the sensor assumes that the address has a neutral reputation.

Global Correlation inspection has three modes of primary operation: permissive, standard (default), and aggressive; you can also select Off:

- Permissive mode tells the sensor to adjust the risk rating of an event, but not to assign separate reputation-only actions to the event.
- Standard mode tells the sensor to adjust the risk rating and to add a Deny Packet action due to reputation if the risk rating is greater than or equal to 86. It also adds a Deny Attacker action due to reputation if the risk rating is greater than or equal to 100.
- Aggressive mode also adjusts the risk rating due to reputation, adds a Deny Packet action due to reputation if the risk rating is greater than or equal to 83, and adds a Deny Attacker action due to reputation if the risk rating is greater than or equal to 95.
- Selecting Off in the Global Correlation Inspection window prevents the sensor from using updates from Cisco SensorBase to adjust reputation.

If Global Correlation inspection is enabled and an event is generated by an attacker with a negative reputation, the risk rating for the event is elevated by a certain amount that is determined by a statistical formula. The amount by which the risk rating is raised depends on the original risk rating of the event and the reputation of the attacker.

Network Participation and Correlation Updates

The IPS sensor pulls reputation information for addresses on the global Internet from Cisco SensorBase. When the sensor is configured initially, a DNS server needs to be configured for the sensor to use to connect to Cisco SensorBase; or an HTTP or HTTPS proxy (that has DNS configured) needs to be configured. After the sensor has this information, the sensor makes an outbound connection to check for the latest updates from Cisco SensorBase. It initiates an HTTPS request to Cisco SensorBase update

servers and downloads a manifest that contains the latest versions of the files related to Global Correlation. The sensor checks Cisco SensorBase every five minutes for updates. If changes are needed, the sensor performs a DNS lookup of the server name returned in the initial request. This lookup returns the location of the server nearest to the sensor. The sensor then initiates an HTTP connection that actually transfers the data. The size of a full update is about 2 MB; incremental updates average about 100 KB. If a sensor loses connection to Cisco SensorBase, Global Correlation information begins to time out within days, and sensor health changes accordingly.

The other component of Global Correlation is network participation. This feature sends data from events that the sensor fires back to Cisco SensorBase to adjust the reputation of IP addresses; this information is then packaged in future reputation data downloads from Cisco SensorBase. The sensor passes this information back to Cisco SensorBase according to the sensor configuration. The possible configuration options are Off, Partial, and Full.

- With the Off (default) setting, the sensor does not send back any data. The sensor still receives reputation data, and this setting does not affect its use of that data except that the reputations of addresses attacking the network being protected are not influenced by their generation on the sensor.
- With the Partial setting, the sensor sends back alert information. This information consists of protocol attributes such as the TCP maximum segment size and TCP options string, the signature ID and risk rating of the event, the attacker IP address and port, and Cisco IPS performance and deployment mode information.
- The Full setting adds victim IP address and port information to the information reported with the Partial setting.



Note

No actual packet content information is sent to Cisco. In addition, events having RFC 1918 addresses, because they are not unique, are not considered interesting; therefore, all events reported to Cisco SensorBase have any such IP address information stripped from the reported data.

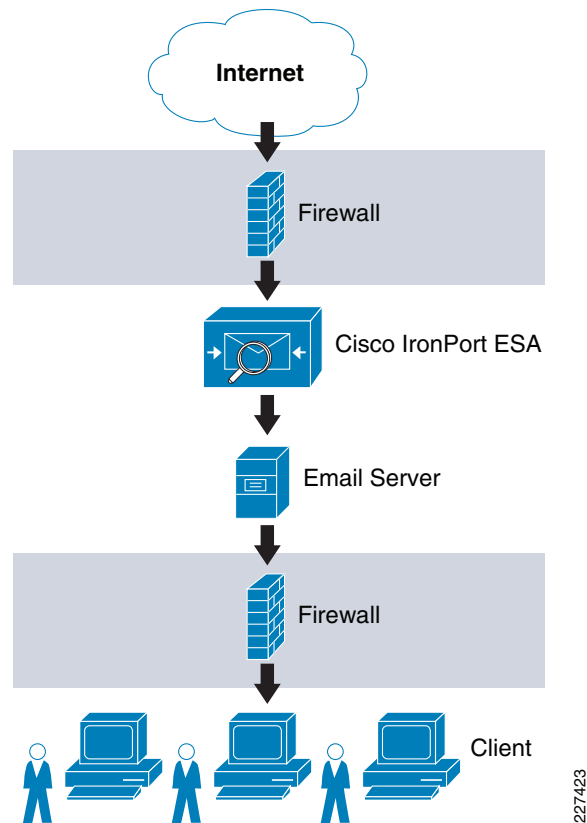
The mechanism used to update Cisco SensorBase with new attack information is straightforward. The sensor takes event information, parses out the important pieces of data, and buffers this data for transmission back to Cisco SensorBase. It sends this data in the form of an HTTPS connection that it initiates on average every ten minutes. The average size of an update is 2 to 4 KB, with weekly averages of about 0.5 to 1 MB. Some higher-volume sensors have average update sizes of about 50 KB, with weekly totals in the 45 MB range. Sensors with very high alert volumes can have average update sizes of about 850 KB, with weekly totals of up to 900 MB; these sensors, however, are at the extreme end of the range.

For more information on IPS Global Correlation including configuration information, see:

http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_collaboration.html

E-Mail Security Guidelines

The medium enterprise design implements a Cisco IronPort C Series E-Mail Security Appliance (ESA) in the DMZ to inspect E-mails and prevent threats such as E-mail spam, viruses, and worms. The ESA acts as a firewall and threat monitoring system for SMTP traffic (TCP port 25). Logically, the ESA acts as a Mail Transfer Agent (MTA) within the E-mail delivery chain, as shown in [Figure 5](#).

Figure 5 **Logical E-Mail Delivery Chain**

227423

**Note**

Figure 5 shows a logical implementation of a DMZ hosting the E-mail server and ESA appliance. This can be implemented physically by either using a single firewall or two firewalls in a “sandwich” configuration.

When the Cisco ESA receives the E-mails, they are evaluated using a reputation score mechanism based on the SensorBase network, which is an extensive network that monitors global E-mail and web traffic for anomalies, viruses, malware, and other abnormal behavior. The SensorBase network consists of Cisco IronPort appliances, Cisco ASA, and IPS appliances installed in more than 100,000 organizations worldwide. This provides a large and diverse sample of Internet traffic patterns. By leveraging the information in the SensorBase network, messages originating from domain names or servers known to be the source of spam or malware, and therefore with a low reputation score, are automatically dropped or quarantined by preconfigured reputation filters.

In addition, an enterprise may optionally choose to implement some of the other functions offered by the Cisco ESA appliance, including anti-virus protection with virus outbreak filters and embedded anti-virus engines (Sophos and McAfee); encryption to ensure the confidentiality of messages; and data loss prevention (DLP) for E-mail to detect the inappropriate transport of sensitive information.

**Note**

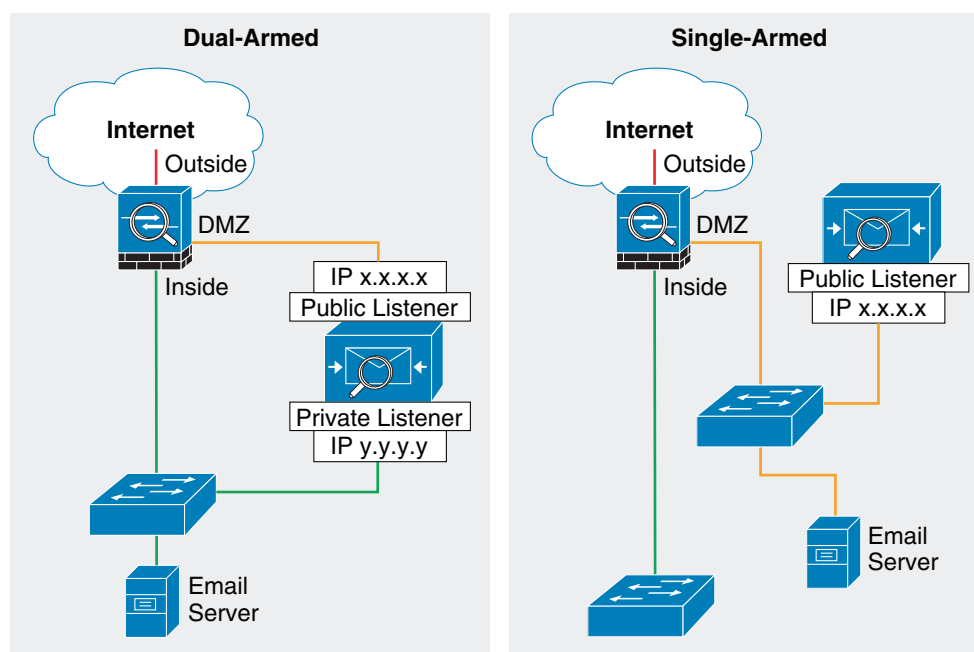
Alternatively, Cisco offers managed hosted and hybrid hosted E-mail security services. These services are provided through a dedicated E-mail infrastructure hosted in a network of Cisco data centers. For more information, see <http://www.cisco.com/go/designzone>.

There are two options for deploying the ESA appliance, depending on the number of interfaces used:

- **Dual-armed configuration**—Two physical interfaces are used to serve as a public mail listener and a private mail listener where each interface is configured with a separate logical IP address. The public listener receives E-mail from the Internet and directs messages to the internal mail servers. The private listener receives E-mail from the internal servers and directs messages to the Internet. The public listener interface would connect to the DMZ and the private listener interface can connect to the inside of the firewall closer to the mail server.
- **One-armed configuration**—A single interface is configured on the ESA with a single IP address and used for both incoming and outgoing E-mail. A public mail listener is configured to receive and relay E-mail on that interface. The best practice is to connect the ESA interface to the DMZ where the E-mail server resides.

Figure 6 shows both configurations.

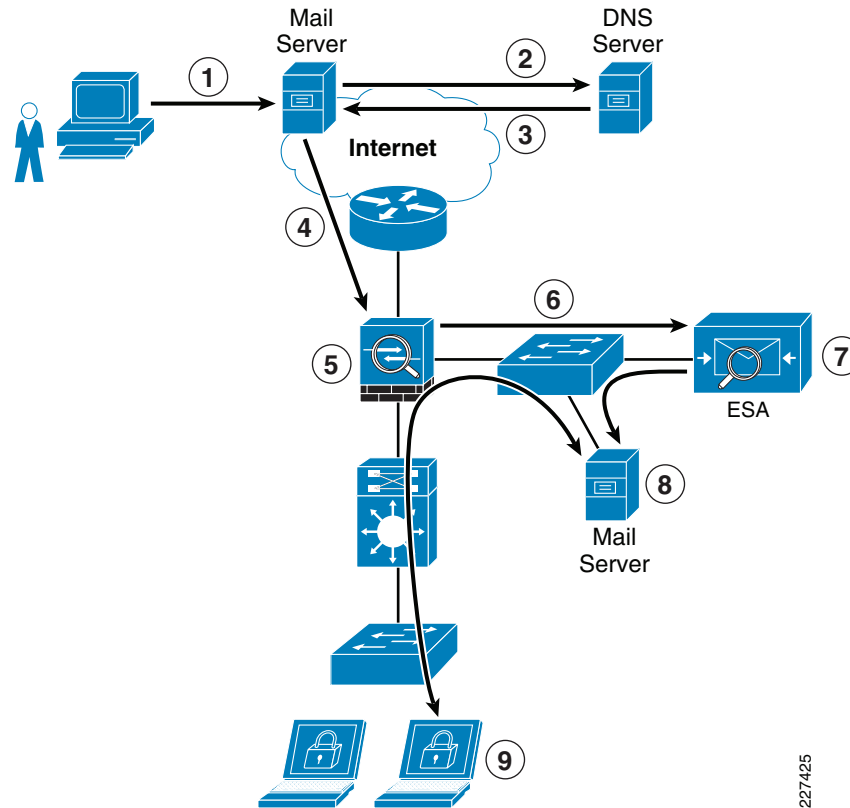
Figure 6 Common Cisco ESA Deployments



For simplicity, the medium enterprise security design implements the Cisco ESA with a single interface in a single-armed configuration. This also leaves the other data interfaces available for redundancy.

Figure 7 shows the logical location of the Cisco ESA within the E-mail flow chain and the typical data flow for inbound E-mail traffic.

Figure 7 Typical Data Flow for Inbound E-Mail Traffic



The following steps explain what is taking place in [Figure 7](#):

1. Sender sends an E-mail to xyz@domain X.
2. What's the IP address of domain X?
3. It is a.b.c.d (public IP address of ESA).
4. E-mail server sends message to a.b.c.d using SMTP.
5. Firewall permits incoming SMTP connection to the ESA, and translates its public IP address.
6. ESA performs a DNS query on sender domain and checks the received IP address in its reputation database, and drops, quarantines E-mail based on policy.
7. ESA forwards E-mail to preconfigured inbound E-mail server.
8. E-mail server stores E-mail for retrieval by receiver.
9. Receiver retrieves E-mail from server using POP or IMAP.

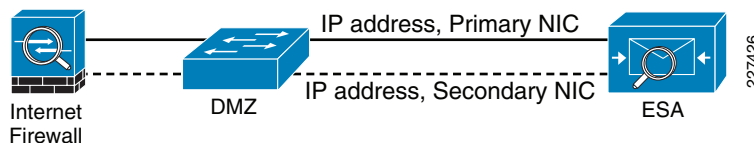
The Cisco IronPort ESA appliance functions as an SMTP gateway, also known as a mail exchange (MX). The following outlines some of the key deployment guidelines for the ESA within the medium enterprise design:

- The Cisco ESA appliance needs to be accessible via the public Internet, and is the first hop in the E-mail infrastructure. If another MTA sits at your network's perimeter and handles all external connections, the ESA is not able to determine the sender's IP address. The IP address of the sender is needed to identify and distinguish the senders in the Mail Flow Monitor to query the SensorBase Reputation Service for the SensorBase Reputation Service Score (SBRs) of the sender. Therefore, a separate MTA should not be deployed at the network perimeter to handle the external connections.

- The ESA needs to be registered in DNS for features such as IronPort Anti-Spam, Virus Outbreak Filters, McAfee Antivirus, and Sophos Antivirus. A DNS “A” record should be created to map the appliance hostname to its public IP address, and an MX record that maps the public domain to the appliance hostname. A priority is specified for the MX record to advertise the ESA appliance as the primary MTA for the domain.
- A static IP address translation entry on the Internet firewall should be defined to map the public IP address of the ESA to its private internal address if NAT is configured on the Internet firewall.
- All the local domains for which the ESA appliance accepts mail needs to be added to the Recipient Access Table (RAT). Inbound E-mail destined to domains not listed in the RAT are rejected. External E-mail servers connect directly to the ESA appliance to transmit E-mail for the local domains, and the ESA appliance relays the mail to the appropriate groupware servers (for example, Exchange, GroupWise, Domino) via SMTP routes.
- For each private listener, the host access table (HAT) must be configured to indicate the hosts that are allowed to send E-mails. The ESA appliance accepts outbound E-mail based on the settings of the HAT table. Configuration includes the definition of sender groups associating groups or users, and on which mail policies can be applied. Policies include the following:
 - Mail flow policies—A way of expressing a group of HAT parameters; access rule, followed by rate limit parameters and custom SMTP codes and responses
 - Reputation filtering—Allows the classification of E-mail senders, and restricting E-mail access based on sender trustworthiness as determined by the IronPort SensorBase Reputation Service.
- Define SMTP routes to direct E-mail to the appropriate internal mail servers.
- If an OOB management network is available, a separate interface for administration should be used.

Because a failure on the ESA appliance may cause a service outage, a redundant design is recommended. One way to implement redundancy is to use IronPort NIC pairing, as shown in [Figure 8](#).

Figure 8 Cisco IronPort ESA NIC Pairing



IronPort NIC pairing provides redundancy at the network interface card level by teaming two of the Ethernet interfaces in the ESA appliance. If the primary interface fails, the IP address and MAC address are moved to the secondary interface. IronPort NIC pairing is the most cost-effective solution because it does not require the deployment of multiple ESA appliances and other hardware. However, it does not provide redundancy in case of chassis failure.

Alternative redundant designs include the following:

- Multiple MTAs—Adding a second ESA appliance or MTA and using a secondary MX record with an equal cost to load balance between the MTAs.
- Load balancer—Using a load balancer such as the Cisco Application Control Engine (ACE) to load balance traffic across multiple ESA appliances.

To accommodate traffic to and from the IronPort ESA provisioned in the DMZ, the Internet firewall needs to be configured to allow this communication. Protocols and ports to be allowed vary depending on the services configured on the ESA.

The following are some of the common services required to be allowed through the Internet firewall:

- Outbound SMTP (TCP/25) from ESA to any Internet destination

- Inbound SMTP (TCP/25) to ESA from any Internet destination
- Outbound HTTP (TCP/80) from ESA to downloads.ironport.com and updates.ironport.com
- Outbound SSL (TCP/443) from ESA to updates-static.ironport.com and phonehome.senderbase.org
- Inbound and outbound DNS (TCP and UDP port 53)
- Inbound IMAP (TCP/143), POP (TCP/110), SMTP (TCP/25) to E-mail server from any internal client

Also, if the ESA is managed in-band, the appropriate firewall rules need to be configured to allow traffic such as SSH, NTP, and SYSLOG to/from the ESA.

For more information on how to configure the ESA, see:

- *Cisco SAFE Reference Guide*: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html
- *Cisco IronPort ESA User Guide*: <http://www.ironport.com/support>

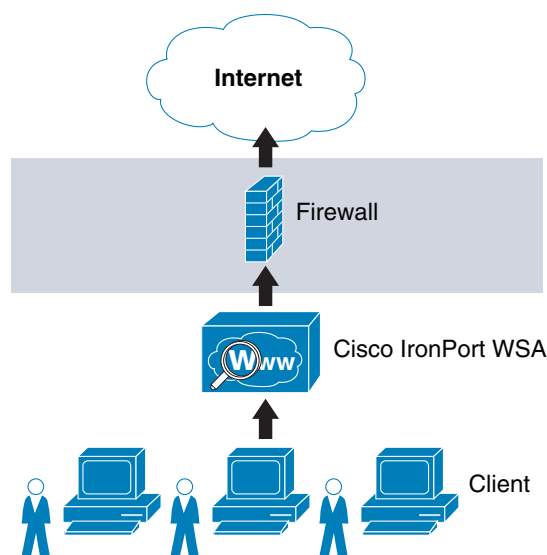
Web Security Guidelines

The medium enterprise network design implements a Cisco IronPort S Series Web Security Appliance (WSA) to block HTTP and HTTPS access to sites on the Internet with non-business-related content and to protect the enterprise network from Web-based malware and spyware.

The Cisco IronPort WSA relies on two independent services to protect the network:

- **Web proxy**—Provides URL filtering, Web reputation filters, and optionally anti-malware services. The URL filtering capability defines the handling of each Web transaction based on the URL category of the HTTP requests. Leveraging the SensorBase network, the Web reputation filters analyze the Web server behavior and characteristics to identify suspicious activity and protect against URL-based malware. The anti-malware service leverages anti-malware scanning engines such as Webroot and McAfee to monitor for malware activity.
- **Layer 4 traffic monitoring (L4TM)**—Monitors all Layer 4 traffic for rogue activity, and to detect infected clients.

The medium enterprise design assumes a centralized Internet connection implemented at the main site. The WSA should be implemented at the distribution layer in the Internet perimeter network. This allows for the inspection and enforcement of Web access policies to all users located at any of the enterprise sites. Logically, the WSA sits in the path between Web users and the Internet, as shown in [Figure 9](#).

Figure 9 Cisco IronPort WSA

There are two deployment modes for enabling the Cisco IronPort WSA Web Proxy service:

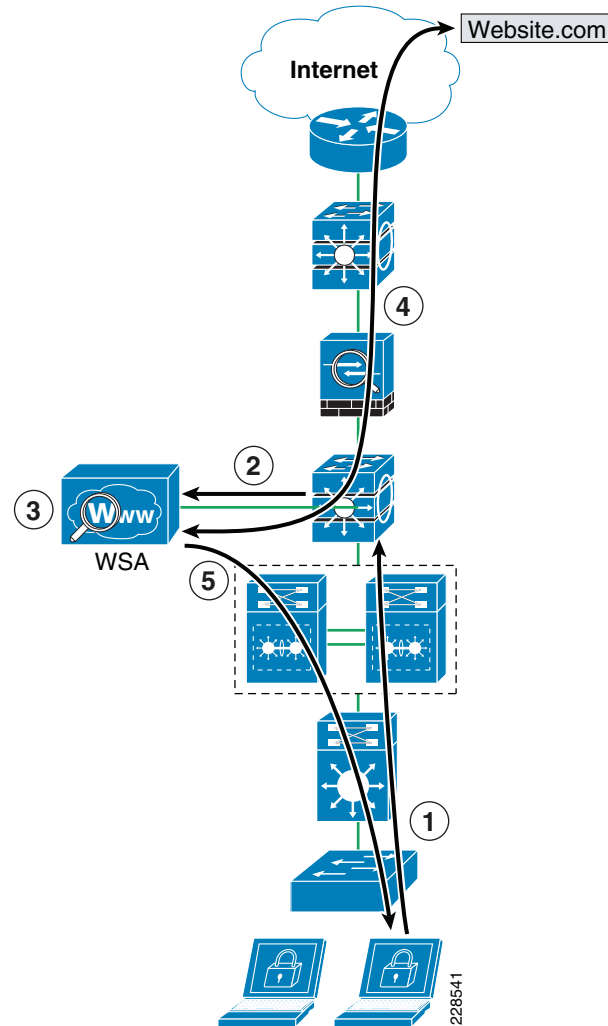
- **Explicit forward proxy**—Client applications, such as Web browsers, are aware of the Web proxy and must be configured to point to the WSA as its proxy. The Web browsers can be configured either manually or by using proxy auto configuration (PAC) files. Manual configuration does not allow for redundancy, while the use of PAC files allows the definition of multiple WSAs for redundancy and load balancing. If supported by the browser, the Web Proxy Auto-discovery Protocol (WPAD) can be used to automate the deployment of PAC files. WPAD allows the browser to determine the location of the PAC file using DHCP and DNS lookups.
- **Transparent proxy**—Client applications are unaware of the Web proxy and do not have to be configured to connect to the proxy. This mode requires the implementation of a Web Cache Communications Protocol (WCCP)-enabled device or a Layer 4 load balancer to intercept and redirect traffic to the WSA before going to the Internet. Both WCCP and Layer 4 load balancer options provide for redundancy and load balancing.

Explicit forward proxy mode requires the enterprise to have control over the configuration of the endpoints, which may not be always possible. For example, the enterprise may allow the use of personal laptops, smart phones, or other devices outside the company's administration. Conversely, transparent proxy mode provides transparent integration of WSA without requiring any configuration control over the endpoints. In addition, transparent proxy also eliminates the possibility of users reconfiguring their Web browsers to bypass the WSA appliance without the knowledge of the administrators. For these reasons, the medium enterprise design implements transparent proxy mode with WCCP. In the medium enterprise design, the Cisco Catalyst 3750 Stackwise distribution switches deployed in the Internet perimeter can be leveraged as the WCCP server while the WSA acts as a WCCP traffic processing entity.

The Cisco Catalyst 3750 switches uses WCCP version 2, which has a built-in failover and load balancing mechanism. Per the WCCPv2 specifications, multiple appliances (up to 32 entities) can be configured as part of the same service group. HTTP and HTTPS traffic is load balanced across the active WSA appliances based on source and destination IP addresses. The WCCP server (Cisco Catalyst 3750 switch) monitors the availability of each appliance in the group and can identify the appliance failures in 30 seconds. After failure, the traffic is redirected across the remaining active appliances. In the case where no appliances are active, WCCP takes the entire service group offline and subsequent requests bypass redirection. In addition, WCCPv2 supports MD5 authentication for the communication between the WCCP server and the WSA appliances.

Figure 10 shows how WCCP redirection works in conjunction with the Cisco Catalyst 3750 StackWise distribution switches.

Figure 10 **WCCP Redirection**



As shown in Figure 10, the following steps take place:

1. The client browser requests a connection to `http://website.com`.
2. The Cisco Catalyst 3750 Internet perimeter distribution switch intercepts and redirects HTTP/HTTPS requests to WSA via Layer 2 redirection.
3. If the content is not present in the local cache, WSA performs a DNS query on the destination site and checks the received IP address against URL and reputation rules, and allows/denies the request accordingly.
4. If allowed, WSA fetches the content from the destination website.
5. The content is inspected and then delivered to the requesting client.

In the event that the entire service group fails, WCCP automatically bypasses redirection, allowing users to browse the Internet without the Web controls. If it is desired to handle a group failure by blocking all traffic, an inbound ACL may be configured on the Cisco ASA inside interface to permit only

HTTP/HTTPS traffic originated from the WSA appliance itself, and to block any direct requests from clients. The ACL may also have to be configured to permit HTTP/HTTPS access from IPS and other systems requiring direct access to the Internet without going through the WSA proxy.

WCCPv2 supports Generic Route Encapsulation (GRE) and Layer 2-based redirection. The Cisco Catalyst 6500 and 3750 switches support Layer 2-based redirection, and the redirection is supported in hardware. Therefore, the WSA must be directly connected to the switch running WCCP. In addition, WCCP is supported only on the ingress of an interface. For these reasons, WSA should connect directly to the Internet perimeter distribution switch using a VLAN that is different than the VLAN from where the client traffic is coming.

**Note**

The Cisco Catalyst 4500 does not provide the ability to create WCCP traffic redirect exception lists, which is an important component of the design. If a Cisco Catalyst 4500 is implemented as the distribution layer switch, another device, such as the Cisco ASA, should be used as the WCCP server.

The following describes some of the design considerations and caveats for implementing a Cisco IronPort WSA with WCCP on a Cisco Catalyst 3750 switch:

- The WSA must be Layer 2-adjacent to the Cisco Catalyst 3750 switch.
- The WSA and switches in the same service group must be in the same subnet directly connected to the switch that has WCCP enabled.
- Configure the switch interfaces that are facing the downstream Web clients, the WSA(s), and the Web servers as Layer 3 interfaces (routed ports or switch virtual interfaces [SVIs]).
- Use inbound redirection only.
- WCCP is not compatible with VRF-Lite. WCCP does not have visibility into traffic that is being used by the virtual routing tables with VRFs.
- WCCP and policy-based routing (PBR) on the same switch interface are not supported.
- WCCP GRE forwarding method for packet redirection is not supported.
- Use MD5 authentication to protect the communication between the Cisco Catalyst 3750 switches and the WSA(s).
- Use redirect-lists to specifically control what hosts/subnets should be redirected.
- Cisco Catalyst 3750 switches support switching in hardware only at Layer 2; therefore, no counters increment when the command **show ip wccp** is issued on the switch.
- In an existing proxy environment, deploy the WSA downstream from the existing proxy servers (closer to the clients).
- If an OOB management network is available, use a separate interface for WSA administration.

For more information on WCCP in relation to the Cisco Catalyst 3750 switch, see:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_46_se/configuration/guide/swwccp.html.

**Note**

WCCP, firewall, and other stateful features typically require traffic symmetry where traffic in both directions should flow through the same stateful device. Care should be taken when implementing active-active firewall pairs because they may introduce asymmetric paths.

The WSA appliance may also be configured to control or block peer-to-peer file sharing and instant messaging applications such as AOL Messenger, BitTorrent, Skype, Kazaa, and so on. Depending on the port used for transport, the WSA handles these applications as follows:

- Port 80—Applications that use HTTP tunneling on port 80 can be handled by enforcing access policies within the Web proxy configuration. Applications access can be controlled based on applications, URL categories, and objects. Applications are matched based on their user agent pattern, and the use of regular expressions. URLs can be blocked based on specific categories, such as predefined chat and peer-to-peer categories, or custom categories defined by the administrator. Peer-to-peer access can also be filtered based on object and Multipurpose Internet Mail Extensions (MIME) types.
- Ports other than 80—Applications using ports other than 80 can be handled with the L4TM feature. L4TM can block access to specific applications by preventing access to the server or IP address blocks to which the client application must connect.

In the medium enterprise design, the Internet perimeter firewall can be configured to allow only Web traffic (HTTP and HTTPS) outbound to the Internet from only the WSA. This prevents users from bypassing the WSA to browse the Internet.


Note

Peer-to-peer file sharing and Internet instant messaging applications can also be blocked using Cisco IPS appliances and modules and the Cisco ASA firewall (using modular policy framework).

The WSA L4TM service is deployed independently from the Web proxy functionality. L4TM monitors network traffic for rogue activity and for any attempts to bypass port 80. It works by listening to all UDP and TCP traffic and by matching domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic. The L4TM internal database is continuously updated with periodic updates from the Cisco IronPort update server (<https://update-manifests.ironport.com>).

For more information on how to configure the L4TM feature on Cisco IronPort WSA, see:

- *Cisco SAFE Reference Guide*: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html.
- *IronPort WSA User Guide*: <http://www.ironport.com/support>.

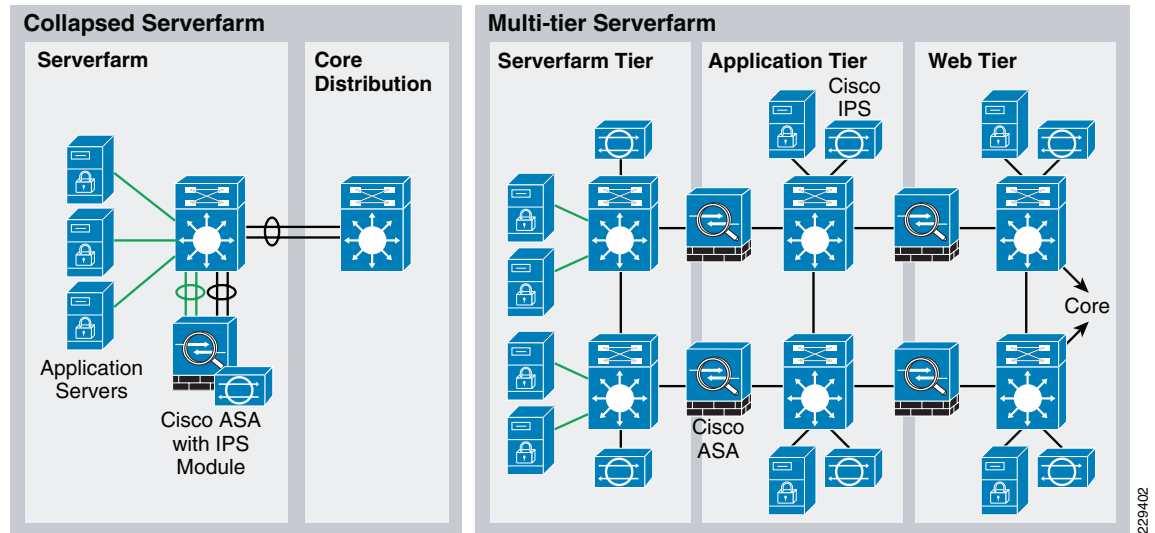
Data Center Protection

Medium enterprise networks typically include a data center at the main site that hosts the systems that serve business applications and store the data accessible to internal users. The infrastructure supporting them may include application servers, the storage media, routers, switches, load balancers, off-loaders, application acceleration devices and other systems. In addition, they may also host foundational services as part of the enterprise network such as identity and security services, unified communication services, mobility services, video services, partner applications, and other services.

Depending on the need and the size of the enterprise network, a single data center may be deployed at the main site. If needed, smaller data centers or serverfarms may also be deployed in remote sites.

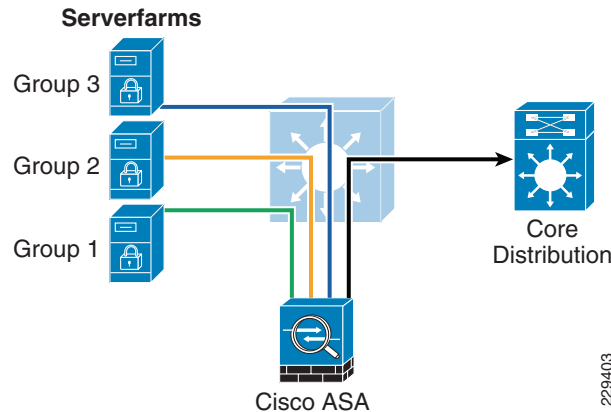
The data center may be constructed following various design models. [Figure 11](#) illustrates a collapsed and multi-tier design. In the collapsed design, all services are hosted in a shared physical serverfarm, and high availability is achieved by using redundant processors and interfaces. Enterprises may also implement a more scalable multi-tier design data center with chassis redundancy.

Figure 11 Collapsed and Multi-tier Data Center Designs



Independent from the design model adopted by the enterprise, the following are the primary security guidelines for the data center design:

- **Network Foundation Protection**—All infrastructure equipment should be protected following the Network Foundation Protection best practices described earlier in this document. This includes restricting and controlling administrative access, protecting the management and control planes, and securing the switching and routing planes.
- **Firewall**—A stateful firewall may be deployed to limit access to only the necessary applications and services, and for the intended users. The firewall should be configured to control and inspect both traffic entering and leaving the serverfarm segments. The firewall may also be leveraged to ensure the appropriate segregation between application layers or groups. In addition, the firewall's deep packet inspection may be used to mitigate DoS attacks and enforce protocol compliance.
- **Intrusion prevention**—An IPS module on the Cisco ASA or a separate IPS appliance may be implemented for enhanced threat detection and mitigation. The IPS is responsible for identifying and blocking anomalous traffic and packets recognized as well-known attacks. The Cisco IPS may be configured either in inline or promiscuous mode. When deployed in inline mode, the Cisco IPS is placed in the traffic path and is capable of stopping malicious traffic before it reaches the intended target.
- **Service isolation**—Services and applications serving different groups of users or under different security requirements should be properly isolated. Isolation helps prevent data leakage and contain possible compromises from spreading across different serverfarm groups. Logical isolation may be achieved by separating applications and services in different VLANs and by assigning them into different firewall interfaces (physical or logical). This is illustrated in [Figure 12](#).

Figure 12 Service Isolation

- Switch security—Private VLANs, port security, storm control, and other switch security features may be leveraged to mitigate spoofing, man-in-the-middle, DoS, and other network-based attacks directed to the data center applications and the switching infrastructure.
- Endpoint protection—Servers residing at the various layers should be protected with host-based IPS or other endpoint security software.

SSL termination and inspection, Web Application Firewall (WAF), Application Control Engine (ACE), and other solutions may be leveraged to complement the guidelines described above. For a more detailed discussion of data center security, see “Chapter 4, Intranet Data Center” of the *Cisco SAFE Reference Guide* at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap4.html.

Network Access Security and Control Guidelines

One of the most vulnerable points of a network is at the access edge. The access layer is where end users connect to the network. In the past, network administrators have largely relied on physical security to protect this part of the network. Unauthorized users were not allowed to enter secure buildings where they could plug into the network. Today, with the proliferation of wireless networks, increased use of laptops and smart mobile devices, enterprises cannot simply rely on physical controls to prevent these unauthorized devices from plugging into ports of the access switches. Contractors and consultants regularly have access to secure areas, and there is nothing preventing them from plugging into a wall jack in a cubicle or conference room to gain access to the enterprise network. When connected to the network, everyone has access to all resources on the network.

Protection needs to be embedded into the network infrastructure, leveraging the native security features available in switches and routers. In addition, the network infrastructure should also provide dynamic identity or role-based access controls for all devices attempting to gain access. Implementing role-based access controls for users and devices help reduce the potential loss of sensitive information by enabling administrators to verify a user or device identity, privilege level, and security policy compliance before granting access to the network. Security policy compliance can consist of requiring anti-virus software, OS updates, or patches. Unauthorized or noncompliant devices can be placed in a quarantine area where remediation can occur before network access.

The medium enterprise design provides access security and control by leveraging the following technologies:

- Cisco Catalyst Integrated Security Features (CISF)—Wired users
- Cisco Unified Wireless Network (CUWN) Integrated Security Features—Wireless users

- Cisco Identity-Based Network Services (IBNS)—Wired and wireless users
- Cisco Network Admission Control (NAC) Appliance—Wired and wireless users

Cisco Catalyst Integrated Security Features

Cisco CISF is a set of native security features available on Cisco Catalyst switches designed to protect the access layer infrastructure and users from spoofing, man-in-the-middle (MITM), DoS, and other network-based attacks. CISF should be considered part of the security baseline of any network and should be deployed on all ports on the access switches within the enterprise network architecture.

CISF includes the following features:

- Port Security—Mitigates MAC flooding and other Layer 2 CAM overflow attacks by restricting the MAC addresses that are allowed to send traffic on a particular port. After Port Security is enabled on a port, only packets with a permitted source MAC address are allowed to pass through the port. A permitted MAC address is referred to as a secure MAC address.
- DHCP Snooping—Inspects and filters DHCP messages on a port to ensure DHCP server messages come only from a trusted interface. Additionally, it builds and maintains a DHCP snooping binding table that contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information corresponding to the local untrusted interfaces of a switch. This binding table is used by the other CISF features.
- Dynamic ARP inspection (DAI)—Validates that the source MAC and IP address in an ARP packet received on an untrusted interface matches the source MAC and IP address registered on that interface (using the DHCP snooping binding table) to prevent ARP spoofing and MITM attacks.
- IP Source Guard—Restricts IP traffic on a port based on DHCP or static IP address MAC bindings to prevent IP spoofing attacks. IP address bindings are validated using information in the DHCP Snooping binding table.
- Storm Control—Prevents broadcast and multicast storms by monitoring packets passing from an interface to the switching bus and determines whether the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the one-second time interval and compares the measurement with a predefined suppression-level threshold. When the suppression-level threshold is reached, the port blocks traffic until the traffic falls below the threshold level.

Cisco Unified Wireless Network (CUWN) Integrated Security Features

The Cisco Unified Wireless Network adds to the 802.11 security standards by providing additional security features. Some of these are the WLAN equivalent of CISF features such as Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP) protection, peer-to-peer blocking, and ACL and firewall features. Additionally, other more WLAN specific features are provided, including Enhanced WLAN security options, wireless intrusion detection system (IDS), client exclusion, rogue AP detection, management frame protection, dynamic radio frequency management, and network IDS integration.

The Cisco Unified Wireless Network solutions are discussed in the Wireless and Network Security Integration Solution Design Guide at:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_sec_wireless.html.

Cisco Identity-Based Network Services (IBNS)

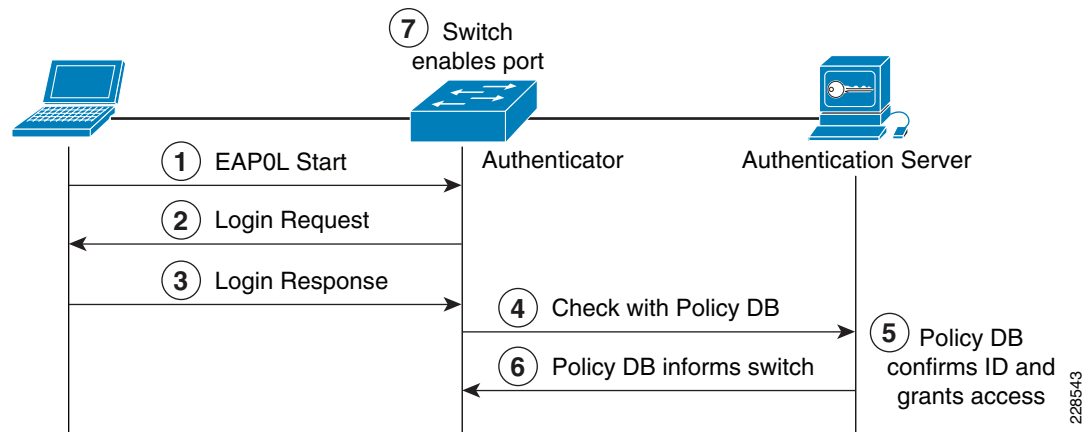
The Cisco IBNS solution is a set of Cisco IOS software services that provide secure user and host access to enterprise networks powered by Cisco Catalyst switches and wireless LANs. Cisco IBNS provides standards-based network access control at the access layer by using the 802.1X protocol to secure the physical ports where end users connect. 802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device. 802.1X is a well-known way to secure wireless network access and is also capable of securing wired network access.

IEEE 802.1X Protocol

The IEEE 802.1X protocol allows Cisco Catalyst switches to offer network access control at the port level. Every port on the switch is individually enabled or disabled based on the identity of the user or device connecting to it. When 802.1X is first enabled on a port, the switch automatically drops all traffic received on the port except the request to start 802.1X authentication. After the 802.1X authentication successfully completes, the switch starts accepting other kinds of traffic on the port.

The high-level message exchange shown in [Figure 13](#) illustrates how port-based access control works within an identity-based system.

Figure 13 Port-Based Access Control



The following steps describe the port-based access control flow as shown in [Figure 13](#):

1. A client, such as a laptop with an 802.1X supplicant, connects to an IEEE 802.1X-enabled network and sends a start message to the LAN switch (the authenticator).
2. When the start message is received, the LAN switch sends a login request to the client.
3. The client replies with a login response.
4. The switch forwards the response to the policy database (authentication server).
5. The authentication server authenticates the user.
6. After the user identity is confirmed, the policy database authorizes network access for the user and informs the LAN switch.
7. The LAN switch then enables the port connected to the client.

The user or device credentials are processed by an AAA server. The AAA server is able to reference user or device profile information either internally, using the integrated user database, or externally using database sources such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), Novell Directory, or Oracle databases. This enables the IBNS solution to be integrated into existing user management structures and schemes, which simplifies overall deployment.

802.1X and EAP

When authenticating users for network access, the client must provide user and/or device identification using strong authentication technologies. IEEE 802.1X does not dictate how this is achieved. Instead, the 802.1X protocol defines an encapsulation for the transport of the Extensible Authentication Protocol (EAP) from the client to the switch. The 802.1X encapsulation is sometimes referred to as EAP over LAN (EAPoL). The switch in turn relays the EAP information to the authentication server using the RADIUS protocol (EAP over RADIUS).

EAP is defined by RFC 3748. EAP is a framework and not a specific authentication method. It provides a way for the client and the authentication server to negotiate an authentication method that they both support. There are many EAP methods, but the ones used more frequently for 802.1X wired authentication include EAP-TLS, EAP-PEAP, and EAP-FAST.

Impacts of 802.1X on the Network

When 802.1X is enabled on a port, the default security posture is to drop all traffic except 802.1X EAPoL packets. This is a fundamental change from the traditional model, where traffic is allowed from the moment a port is enabled and a device is plugged into the port. Ports that were traditionally open are now closed by default. This is one of the key elements of the strong security and network access control provided by 802.1X. However, this change in the default network access model can have a profound impact on network devices and applications. Understanding and accommodating for this change in access behavior facilitates a smooth deployment of 802.1X network access control.

Non-802.1X-Enabled Devices

802.1X must be enabled on both the host device and on the switch to which it connects. If a device without an 802.1X supplicant attempts to connect to a port that is enabled for 802.1X, it is subjected to the default security posture. The default security posture says that 802.1X authentication must succeed before access to the network is granted. Therefore, by default, non-802.1X-capable devices cannot get access to an 802.1X-protected network.

Although an increasing number of devices support 802.1X, there will always be devices that require network connectivity but do not and/or cannot support 802.1X. Examples of such devices include network printers, badge readers, legacy servers, and Preboot Execution Environment (PXE) boot machines. Some provisions must be made for these devices.

The Cisco IBNS solution provides two features to accommodate non-802.1X devices: MAC Authentication Bypass (MAB) and Guest VLAN. These features provide fallback mechanisms when there is no 802.1X supplicant. After 802.1X times out on a port, the port can move to an open state if MAB succeeds or if a Guest VLAN is configured. Application of either or both of these features is required for a successful 802.1X deployment.



Note

Network-specific testing is required to determine the optimal values for the 802.1X timers to accommodate the various non-802.1X-capable devices on your network.

802.1X in Medium Enterprise Networks

As mentioned in the previous sections, 802.1X authentication requires a supplicant on the host device. This typically has been a challenge in enterprise environments that have a wide range of devices and limited or no management of many of these devices. In many enterprise environments, this is still the case, which makes a company-wide 802.1X deployment very challenging. However, there may be pockets of an enterprise network where 802.1X may be a good choice.

For example, 802.1X-protected ports may be a good choice for the network ports in the company's headquarters or main site, because these locations are more likely to have managed PCs.

Other locations in the enterprise network still need protection, but user network access may be better served by a NAC Appliance Solution (discussed in the next section). For networks requiring role-based access control using posture assessments to ensure security compliance, Cisco NAC Appliance should be considered. In addition, network access ports in open areas such as lobbies and meeting rooms may use 802.1X or Cisco NAC Appliance to protect these ports.

When considering an 802.1X deployment, there are four main 802.1X authentication options to consider:

- Basic 802.1X authentication—An 802.1X-controlled port with an 802.1X client directly connected
- IP phone ports—An IP phone and an 802.1X-controlled port with an 802.1X client connected to the phone
- MAC Auth By-Pass—Using the MAC address of the client to provide authentication and bypass the 802.1X authentication process; printer and legacy device support are typical applications
- Web Auth—Allowing a user to authenticate by entering username and passwords in a Web page; legacy device support and guest access are typical deployment applications

For more information on the Cisco IBNS 802.1X network access solution, see: <http://www.cisco.com/go/ibns>.

Cisco NAC Appliance

Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With Cisco NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines before network access. The NAC Appliance identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network security policies, and can repair any vulnerability before permitting access to the network.

When deployed, Cisco NAC Appliance provides the following benefits:

- Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
- Evaluates whether machines are compliant with security policies. Security policies can include requiring specific anti-virus or anti-spyware software, OS updates, or patches. Cisco NAC Appliance supports policies that vary by user type, device types, or operating system.
- Enforces security policies by blocking, isolating, and repairing non-compliant machines.

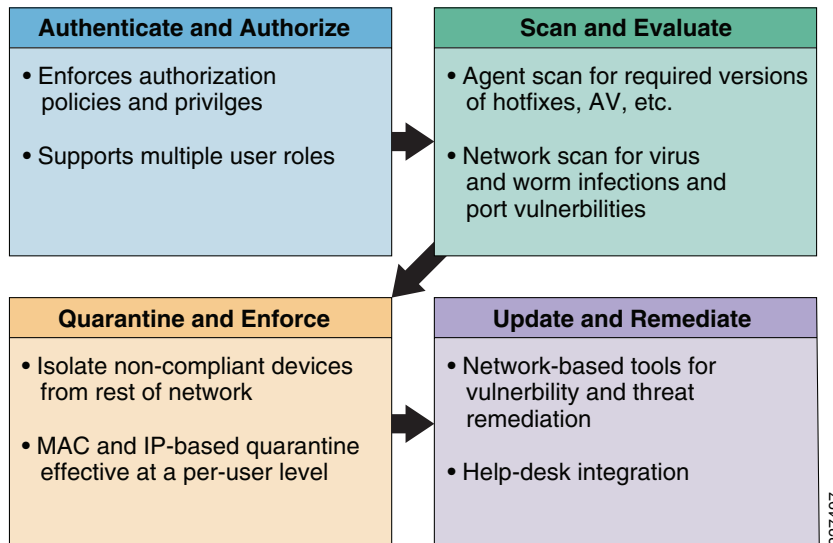
Non-compliant machines are redirected to a quarantine network, where remediation occurs at the discretion of the administrator

The NAC solution provides the following four functions, as shown in [Figure 14](#):

- Authenticates and authorizes

- Scans and evaluates
- Quarantines and enforces
- Updates and remediates

Figure 14 *Four Functions of the NAC Solution*

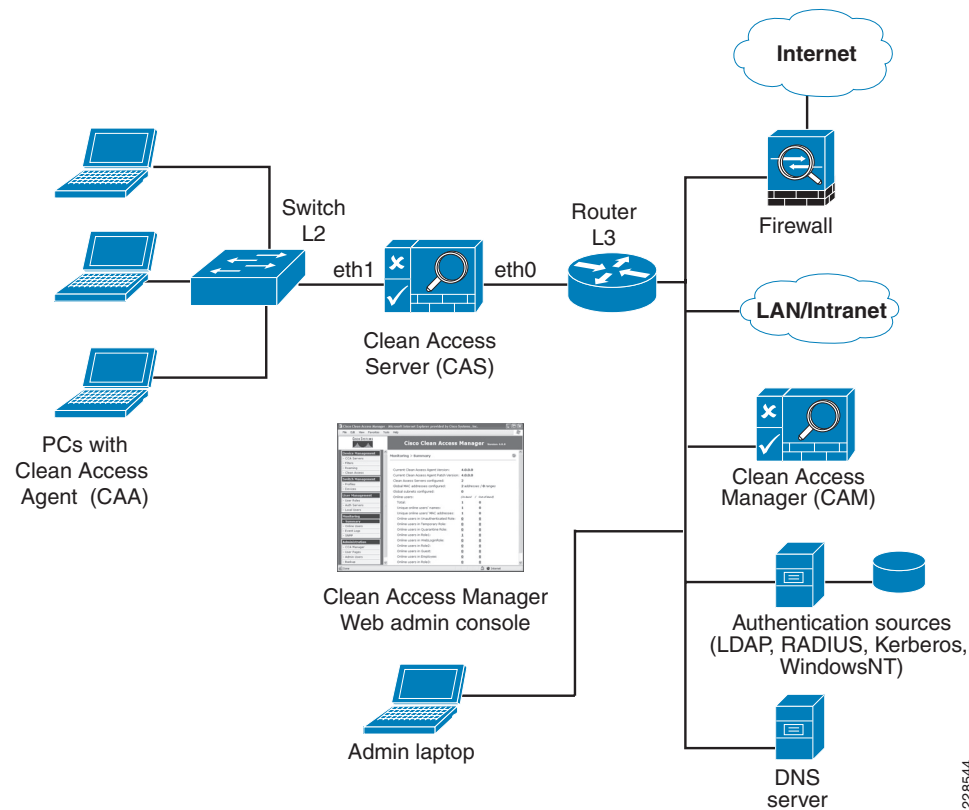


For more details of the Cisco NAC Appliance Solution, see: <http://www.cisco.com/go/nacappliance>.

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric, integrated solution administered from the Cisco Clean Access Manager (CAM) Web console and enforced through the Cisco Clean Access Server (CAS) and (optionally) the Clean Access Agent (CAA) or NAC Web Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and anti-virus software, and quarantines vulnerable or infected clients for remediation before clients access the network.

Figure 15 shows Cisco NAC Appliance components.

Figure 15 NAC Appliance Components**Cisco Clean Access Manager**

The Cisco CAM is the administration server for NAC Appliance deployments. The secure Web console of the CAM is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if using a SuperCAM). For OOB deployments, the Web administration console controls the switches and VLAN assignment of user ports through the use of SNMP. In the medium enterprise network design, the CAM is located in the data center at the main site.

Cisco Clean Access Server (CAS)

The Cisco CAS is the enforcement server between the untrusted network and the trusted network. The CAS enforces the policies defined by the CAM Web administration console. Policies can include network access privileges, authentication requirements, bandwidth restrictions, and system requirements. The CAS can be installed as either a standalone appliance (such as the Cisco NAC-3300 Series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis. The CAS can be deployed in in-band (always inline with user traffic) or OOB (inline with user traffic only during authentication and posture assessment).

Additionally, the CAS can be deployed in Layer 2 mode (users are Layer 2-adjacent to the CAS) or Layer 3 mode (users are multiple Layer 3 hops away from the CAS). Multiple CASs of varying size/capacity can be deployed to fit the needs of various network segments. For example, Cisco NAC-3300 Series appliances can be installed in a main site core to handle thousands of users, and one or more Cisco NAC network modules can be simultaneously installed in ISR platforms to accommodate smaller groups of users in a satellite office.

In the medium enterprise network design, the CAS would be located at the main site and the remote sites, and deployed in Layer 2 OOB (for wireless clients) and Layer 3 OOB (for wired clients) modes for authentication and posture assessments.

Cisco Clean Access Agent (CAA)

The Cisco CAA is an optional read-only agent that resides on Windows clients. It checks applications, files, services, or registry keys to ensure that clients meet the specified network and software requirements before gaining access to the network.

**Note**

There is no client firewall restriction with CAA posture assessment. The agent can check the client registry, services, and applications even if a personal firewall is installed and running.

If NAC is implemented as part of the medium enterprise network security design, it is recommended that the CAA be used.

Cisco NAC Web Agent

The Cisco NAC Web Agent provides temporal posture assessment for client machines. Using a Web browser, users launch the Cisco Web Agent executable file, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet. When the user terminates the Web Agent session, the Web Agent logs the user off the network and their user ID disappears from the online users list.

In the medium enterprise security design, the NAC Web Agent can be used for unmanaged clients.

Clean Access Policy Updates

Regular updates of prepackaged policies/rules can be used to check the up-to-date status of operating systems, anti-virus (AV), anti-spyware (AS), and other client software. Built-in support is provided for 24 AV and 17 AS vendors.

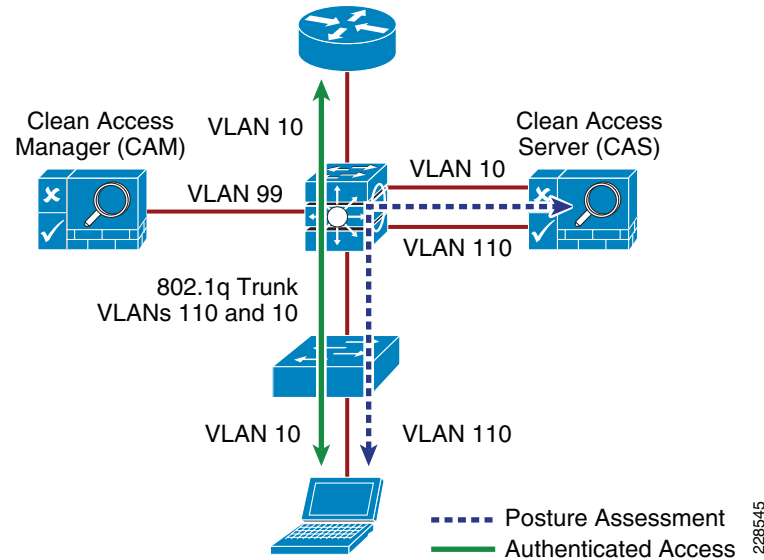
NAC Appliance Modes and Positioning

The NAC Appliance can be deployed in multiple deployment options and placed at various locations in the network. The modes of operation can be generally defined as follows:

- Out-of-band (OOB) virtual gateway
- OOB real IP gateway
- In-band (IB) virtual gateway
- IB real IP gateway

OOB Modes

OOB deployments require user traffic to traverse through the NAC Appliance only during authentication, posture assessment, and remediation (see [Figure 16](#)). When a user is authenticated and passes all policy checks, their traffic is switched normally through the network and bypasses the NAC Appliance.

Figure 16 **Layer 2 OOB Topology**

To deploy the NAC Appliance in OOB mode, the client device must be directly connected to the network via a Cisco Catalyst switch port. After the user is authenticated and passes posture assessment, the CAM instructs the switch to map the user port from an unauthenticated VLAN (which switches or routes user traffic to the CAS) to an authenticated (authorized) VLAN that offers full access privileges. For example, as shown in [Figure 16](#), the client PC is connected through VLAN 110 to the NAC CAS for the authentication and posture assessment, and is moved to VLAN 10 after it successfully completes the authentication/authorization and scan/evaluation phases of the NAC Appliance solution.

In-Band Modes

When the NAC Appliance is deployed in-band, all user traffic, both unauthenticated and authenticated, passes through the NAC Appliance. The CAS may be positioned logically or physically between the end users and the networks being protected. [Figure 17](#) shows a logical in-band topology example and [Figure 18](#) shows a physical in-band topology example.

Figure 17 In-Band Virtual Gateway Topology

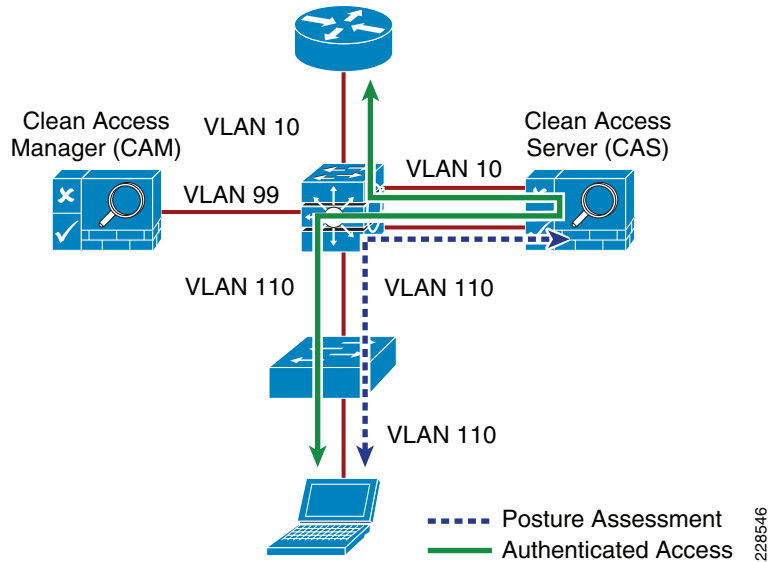
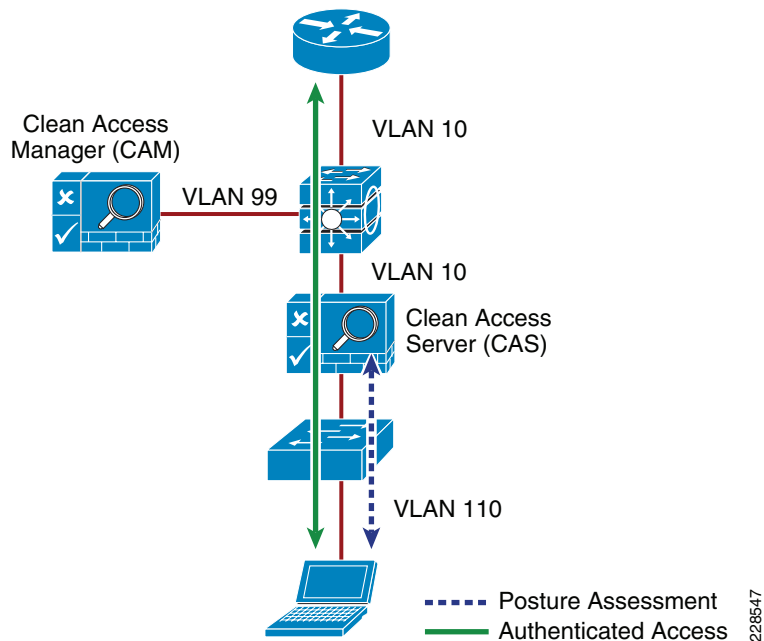


Figure 18 Physical In-Band Topology



In-Band Virtual Gateway

When the NAC Appliance is configured as a virtual gateway, it acts as a bridge between the end users and the default gateway (router or switch) for the client subnet being managed. The following two bridging options are supported by the NAC server:

- **Transparent**—For a given client VLAN, the NAC server bridges traffic from its untrusted interface to its trusted interface. The NAC server is aware of “upper layer” protocols and is able to permit those protocols that are necessary for a client to connect to the network, authenticate, and undergo posture assessment and remediation. By default, it blocks all traffic except for Bridge Protocol Data

Unit (BPDU) frames (spanning tree), and those protocols explicitly permitted in the “unauthorized” role, such as DNS and DHCP. This option is viable when the NAC server is positioned physically in-band between the end users and the upstream network(s) being protected, as shown in [Figure 18](#).

- **VLAN mapping**—This is similar in behavior to the transparent option except that rather than bridging the same VLAN from the untrusted side to the trusted side of the NAC server, two separate VLANs are used. For example, client VLAN 110 is defined for the untrusted interface of the NAC server. There is no routed interface or SVI associated with VLAN 110. VLAN 10 is configured between the trusted interface of the NAC server and the next-hop router interface (or SVI) for the client subnet. A mapping rule is made in the NAC server that forwards packets arriving on VLAN 110 and forwards them out VLAN 10 by swapping VLAN tag information. The process is reversed for packets returning to the client. Also, in this mode, BPDUs are not passed from the untrusted-side VLANs to their trusted-side counterparts.

The VLAN mapping option is typically used when the NAC server is positioned logically in-band between clients and the network(s) being protected, as shown in [Figure 17](#). This is the bridging option that should be used if the NAC Appliance is deployed in virtual gateway mode.

In-Band Real IP Gateway

When the NAC server is configured as a “real” IP gateway, it behaves like a router and routes packets between its interfaces. In this scenario, one or more client VLAN/subnets reside behind the untrusted interface. The NAC server acts as a default gateway for all clients residing on those networks. Conversely, a single VLAN/subnet is defined on the trusted interface, which represents the path to the protected upstream network(s). After successful client authentication and posture assessment, the NAC server by default routes traffic from the untrusted networks to the trusted interface, where it is then forwarded based on the routing topology of the network.

The NAC server is not currently able to support dynamic routing protocols. Therefore, static routes must be configured within the trusted side of the Layer 3 network for each client subnet terminating on or residing behind the untrusted interface. These static routes should reference the IP address of the NAC server trusted interface as its next hop.

If one or more Layer 3 hops exist between the untrusted NAC interface and the end-client subnets, static routes must be configured in the NAC server. In addition, a static default route is required within the downstream Layer 3 network (referencing the IP address of the untrusted NAC server interface) to facilitate default routing behavior from the client networks to the NAC server.

Depending on the topology, multiple options exist to facilitate routing clients to and from the NAC server, including ACLs, static routes, PBR, VRF-Lite, Multiprotocol Label Switching (MPLS) VPN, and other segmentation techniques. These options are discussed in later sections.

In-Band Versus Out-of-Band

[Table 1](#) summarizes various characteristics of the two deployment types.

Table 1 *In-Band versus Out-of-Band Characteristics*

In-Band Deployment Characteristics	Out-of-Band Deployment Characteristics
The CAS is always inline with user traffic (both before and after authentication, posture assessment, and remediation). Enforcement is achieved through being inline with traffic.	The CAS is inline with the user traffic only during the process of authentication, posture assessment, and remediation. After that, user traffic does not go to the CAS. Enforcement is achieved through the use of SNMP to control switches and VLAN assignments to end-user ports.
The CAS can be used to securely control authenticated and unauthenticated user traffic policies (based on port, protocol, subnet), bandwidth policies, and so on.	The CAS can control user traffic during the authentication, posture assessment, and remediation phases but cannot do so post remediation because traffic is OOB.

Table 1 *In-Band versus Out-of-Band Characteristics*

Does not provide switch port level control.	Provides port-level control by assigning ports to specific VLANs as necessary using SNMP.
In-band deployment is supported for wired and wireless clients.	OOB deployments support wired and wireless clients. Wireless OOB requires a specific network topology. ¹
Cisco NAC in-Band deployment with supported Cisco switches is compatible with 802.1X.	Cisco does not recommend using 802.1X in an OOB deployment, because conflicts will likely exist between Cisco NAC Appliance OOB and 802.1X in setting the VLAN on the switch interfaces/ports.

1. OOB NAC deployments for wireless require the NAC server to be deployed in Layer 2 OOB virtual gateway (bridge) mode, and the NAC server must be placed Layer 2-adjacent to the wireless LAN controller (WLC).

Out-of-Band Requirements

OOB implementation of Cisco NAC Appliance requires the access switches and WLCs to be supported by the NAC Appliance software for the NAC Manager to make the necessary changes to the switch ports and WLCs during the authentication, assessment, and remediation process. If access switches are to be used that are not supported, the NAC Solution must be deployed in in-band mode.

To obtain the latest list of supported devices, see the latest version of the *Cisco NAC Appliance-Clean Access Manager Installation and Administration Guide* at:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/47cam-book.html.

Layer 2 and Layer 3 Out-of-Band

The proposed deployment option for the medium enterprise network security design is an OOB design. This provides the highest possible performance and scalability for traffic that has completed the authentication, posture assessment, and remediation stages of NAC. For wireless clients, a Layer 2 OOB solution should be deployed and for wired users, a Layer 2 OOB or Layer 3 OOB solution can be deployed, depending on the topology of your network.

NAC Deployment in the Medium Enterprise Network

Within the medium enterprise design, a Cisco NAC Appliance solution is deployed at each of the site types; main or headquarters site, remote large site, remote medium site, and remote small site. A centralized CAM is deployed at the main site and is deployed within the data center at that site. A CAS is deployed at each of the sites (main and remote sites) and is connected within the service block connecting to the core switches at each of the sites.

The medium enterprise network security design accommodates host network connectivity using wired and wireless technologies. As such, the NAC Appliance solution must provide a solution for both connectivity options. For wireless clients, a Layer 2 OOB NAC solution is deployed, and for wired clients, a Layer 2 OOB or a Layer 3 OOB NAC solution may be deployed.

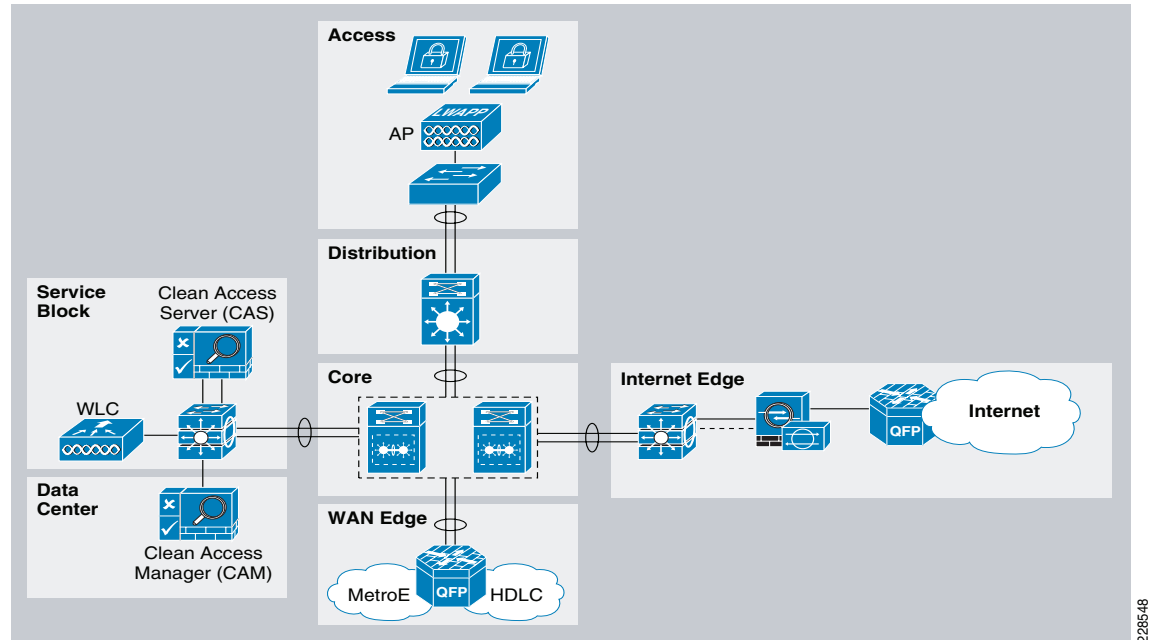
NAC Deployment for Wireless Clients

To provide network access control for wireless clients within the medium enterprise network, the recommended design is the virtual gateway (bridge mode) and central OOB deployment solution. In this design, the NAC server must be placed Layer 2-adjacent to the WLC. In the medium enterprise network, the WLCs are centrally deployed at each site and are implemented in the service block off the core switches, as detailed in the *Medium Enterprise Design Profile Mobility Design* document at:

http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

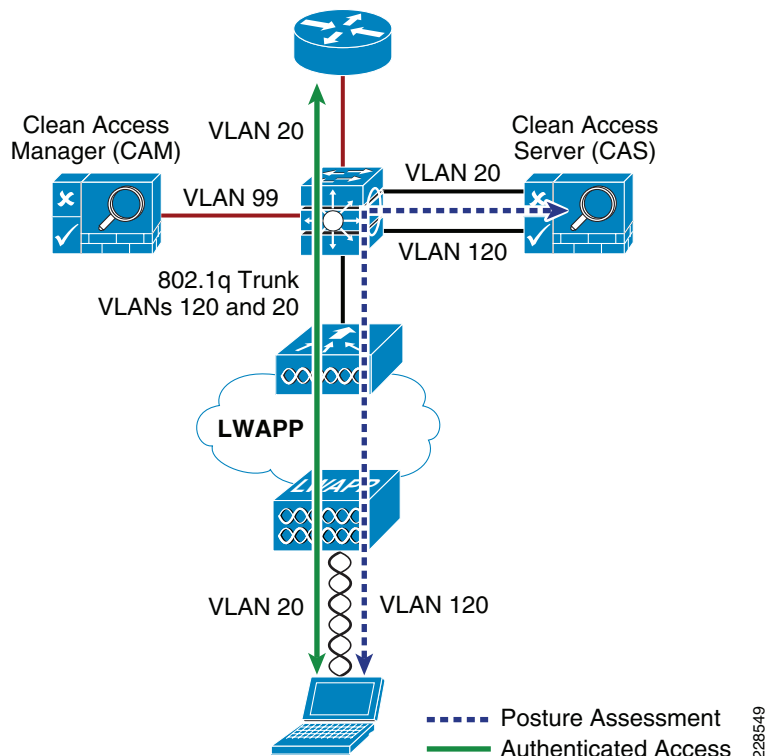
Therefore, the NAC server must also be implemented in the service block. The NAC Manager is implemented in the data center block, as shown in [Figure 19](#).

Figure 19 NAC OOB Deployment for Wireless Clients



The WLC connects to the service block switch using a trunk port carrying the unauthenticated quarantine VLAN and authenticated access VLAN (VLAN 20 and 120). On the switch, the quarantine VLAN is trunked to the untrusted interface on the NAC server (CAS), and the access VLAN is trunked directly to the Layer 3 switch interface. Traffic that reaches the quarantine VLAN on the CAS is mapped to the access VLAN based on a static mapping configuration within the CAS.

When a wireless client associates to the WLC, it initially maps the WLAN/SSID to the quarantine VLAN interface and the client traffic flows in the quarantine VLAN (VLAN 120), which is trunked to the CAS untrusted interface. When NAC authentication, posture assessment, and remediation stages are complete and the user is certified, the NAC Manager sends an SNMP set message to the WLC that updates the VLAN ID from the quarantine VLAN to the access VLAN. After this occurs, the traffic then bypasses the NAC server and goes directly to the network. (See [Figure 20](#).)

Figure 20 **Wireless NAC OOB Traffic Flow**

When implementing the NAC OOB wireless solution, it is recommended to enable RADIUS single sign-on (SSO), which is an option that does not require user intervention and is relatively easy to implement. This option makes use of the VPN SSO capability of the NAC solution, coupled with the Clean Access Agent software that runs on the client PC. VPN SSO uses RADIUS accounting records to notify the NAC Appliance about authenticated remote access users that connect to the network. In the same way, this feature can be used in conjunction with the WLAN controller to automatically inform the NAC server about authenticated wireless clients that connect to the network.

The most transparent method to facilitate wireless user authentication is to enable VPN SSO authentication on the NAC server and configure the WLCs to forward RADIUS accounting to the NAC server. In the event that accounting records need to be forwarded to a RADIUS server upstream in the network, the NAC server can be configured to forward the accounting packet to the RADIUS server.

**Note**

If VPN SSO authentication is enabled without the Clean Access Agent installed on the client PC, users are still automatically authenticated. However, they are not automatically connected through the NAC Appliance until their Web browser is opened and a connection attempt is made. In this case, when users open their Web browser, they are momentarily redirected (without a logon prompt) within the agentless phase. When the SSO process is complete, they are connected to their originally requested URL.

For more information on deploying NAC OOB for wireless environments, see the *NAC Out-Of-Band (OOB) Wireless Configuration Example* at:
http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml.

NAC Deployment for Wired Clients

For wired clients, the medium enterprise security design also uses a central OOB NAC deployment with a NAC server implemented at each of the sites deployed in the service block off the core switch. Depending on the type of network topology deployed, a Layer 3 OOB or Layer 2 OOB solution can be deployed. If the Layer 2 OOB solution is used, the same NAC server can be leveraged for both wired and wireless clients. However, if the Layer 3 OOB solution is deployed, separate NAC servers must be deployed for wired and wireless users.

Layer 3 Out-of-Band Deployment

Layer 3 (L3) OOB is best suited for routed access designs and has rapidly become one of the most popular deployment methodologies for NAC. By deploying NAC in an L3 OOB methodology, a single NAC Appliance can scale to accommodate more users. This deployment also allows NAC Appliances to be centrally located rather than distributed across the site or organization. Thus, L3 OOB deployments are much more cost-effective, both from a capital and operational expense standpoint.

For the main, large, and medium remote site locations, an L3 OOB NAC deployment is recommended, given the 3-tier hierarchical design. In the L3 OOB NAC solution, when a user connects to the access switch before being certified by the NAC server, the user is placed in the authentication VLAN (also called “dirty” VLAN). The user should not have access to any part of the network from the authentication VLAN except for the NAC server and the remediation servers in the quarantine segment. After users are certified by the NAC server, they are placed in the authenticated access VLAN, where their traffic is switched normally through the network and bypasses the NAC server.

The following are three widely deployed techniques for redirecting client traffic from the dirty VLAN to the NAC server for authentication, posture assessment, and remediation purposes:

- Access control lists—Use ACLs on the edge access switches to allow traffic from the unauthenticated VLAN only to the NAC server untrusted interface and specific infrastructure resources needed to get on the network for authentication purposes such as DHCP, DNS, and remediation servers. All other traffic from the dirty VLAN must be blocked.
- VRFs/GRE/MPLS—Use VRFs to route unauthenticated traffic to the CAS. Traffic policies configured on the NAC server (CAS) are used for enforcement on the dirty network. This approach has two sub-approaches. In the first approach, VRFs are pervasive throughout the infrastructure, in which case all Layer 3 devices participate in the tag switching. The second approach uses VRF-Lite and GRE tunnels to tunnel the VRFs through the Layer 3 devices that do not understand tag switching. The benefit to the second approach is that minimal configuration changes are required to your core infrastructure. For more information on this approach, see: http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a3a8a7.shtml.
- Policy-based routing—Use PBR to redirect all traffic in the dirty VLAN to the NAC server. PBR needs to be configured on every Layer 3 hop between the dirty VLAN and the NAC server to ensure that traffic is appropriately redirected.

The most common approach used for isolating the dirty VLAN traffic is to use ACLs. The ACLs on the Layer 3 edge access switches act as the enforcement point to ensure segregation between the “clean” and “dirty” networks. When clients first attach to the network, they are placed in a quarantine or dirty VLAN on the access switches. ACLs should be applied on the SVIs for the dirty VLAN. This ACL should block all access from the dirty VLAN going to the internal networks and allow traffic only to the untrusted interface on the NAC server, the needed remediation servers, and a few infrastructure devices needed for network access such as the DNS, DHCP, and Active Directory servers.

The clients need to communicate with the NAC server untrusted interface for the certification process. The ACLs on the access switches act as the enforcement point for path isolation for the dirty VLAN traffic. Methods for getting the dirty VLAN traffic to the untrusted interface vary, depending on whether the NAC Client Agent is used.

When the NAC agent is used, the NAC Agent communicates with the NAC server untrusted interface to initiate the login process. The NAC Agent tries to discover the NAC server based on the known discovery host value. The discovery host value in the NAC Agent points to the untrusted interface of the NAC server. In the medium enterprise network security design, the NAC Agent can be used for managed PCs.

Web login may also be required for devices that are not managed. With the ACL isolation technique, the NAC server untrusted interface is not directly in the path of the data traffic; therefore, the user is not automatically redirected to the login page when first opening the browser. The following two options can enable the end host to get the login page:

- Option 1—Have a guest login URL known to the users (for example, *guest.nac.local*). In this case, the guest must open a browser and manually enter this URL, which redirects them to the login page.
- Option 2—Create a dummy DNS server for the unauthenticated user subnet. This dummy DNS server resolves every URL to the untrusted interface of the NAC server. When guests open a browser, regardless of which URL they are trying to reach, they are redirected to the login page. When users are then moved to the respective Role/VLAN, they get a new DNS address assignment when performing IP release/renew on a successful login.

Layer 2 Out-of-Band Deployment

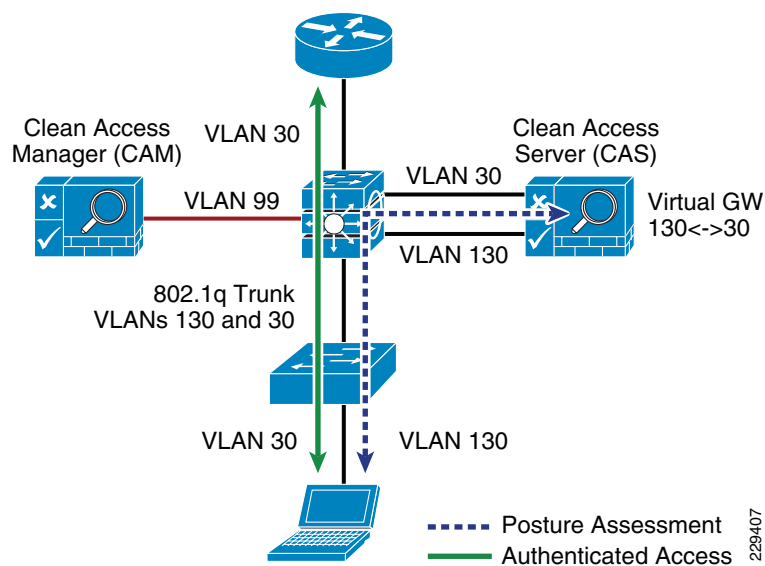
For the small remote sites, a two-tier, collapsed core/distribution LAN design is recommended, as explained in the *Medium Enterprise Design Profile LAN Design* document at:

http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

In a collapsed core/distribution design, the CAS should be deployed in the services block connected to the core/distribution switch. In this simple topology, a Layer 2 Out-of-Band (L2 OOB) NAC deployment can be used.

In the L2 OOB NAC design for the small remote site, the unauthenticated and authenticated VLANs on the access switch (VLANs 30 and 130) are extended to the core/distribution switch using a trunk connection, as shown in Figure 21.

Figure 21 Layer 2 OOB Topology



When a client device initially connects to the access switch before authentication, it is placed in the unauthenticated VLAN (VLAN 130), which connects the client directly to the untrusted interface of the CAS. The CAS maps VLAN 130 to the VLAN 30 trusted interface, allowing the client to obtain an IP

address that belongs on VLAN 30. After the client is authenticated and passes the posture assessment, the access switch is instructed, via SNMP from the CAM, to change the client VLAN to the authenticated VLAN (VLAN 30), where the traffic now bypasses the CAS to access the rest of the network. Although the client has changed Layer 2 VLANs, its Layer 3 network connections are unchanged.

NAC Availability Considerations

Both the CAS and CAM are highly involved in client network access. Consideration must be given to the impact on clients if either a CAS or CAM fails or needs to be taken out of service for a period of time.

The CAS is inline with client devices during the authentication, authorization, and posture assessment phases of NAC, and if NAC is deployed in in-band mode, it is inline even after authentication and certification. A CAS outage for inline clients prevents access for all clients. However, if NAC is deployed in OOB mode, a CAS outage does not affect already connected clients but does prevent network access for new clients.

In situations where availability of a CAS is critical, a high availability (HA) CAS solution can be implemented where a pair of CAS servers are installed using a primary CAS, and a secondary in hot standby. For more information, see the *Cisco NAC Appliance-Clean Access Server Installation and Configuration Guide* at:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cas/461cas-book.html.

The CAM is also a critical part of the authentication, authorization, and posture assessment phases of NAC. Although it does not pass client traffic, the impact of its availability needs to be considered in the network design as well. Like the CAS, the CAM has an HA solution that provides for a primary server and a hot standby secondary server. In addition, each CAS may be configured with a fallback option that defines how it manages client traffic in a situation where the CAM is unavailable.

The use of the CAM and CAS HA features depends on the requirements of the enterprise. However, CAS fallback should always be configured to ensure that critical network services are available, even during a network outage.

Secure Mobility

Today's workers use laptops, smartphones, and other smart mobile devices to access information and applications at anytime and from anywhere there is an Internet connection. Although embracing a mobile workforce clearly boosts productivity and makes the medium enterprise more competitive, a number of challenges arise from the use of mobile technologies. Workers often use the same devices to access both business and personal information. Devices used outside the enterprise onsite controls may potentially introduce viruses, worms, spyware and other type of malware as mobile workers connect back to the corporate network. Confidential and proprietary information may also be lost or stolen while mobile users connect outside the company premises. In addition, the great variety in hardware types, operating systems, and applications represents a clear challenge to the enforcement of security controls and policies.

To continue to foster innovation, enable productivity, and meet the needs of the mobile workforce, companies must adapt to the changing trends in mobility. A viable solution is one that enables access for mobile workers while ensuring that the corporate data, assets, and network remain secure. Additionally, users want the flexibility of choosing how, when, and where to access both personal and professional information to be productive without being inconvenienced by security checks.

The medium enterprise network security design provides persistent and secure mobile access by implementing the Cisco AnyConnect Secure Mobility solution. This solution delivers secure, persistent connectivity to all mobile employees independently from the type of mobile device used. The Cisco AnyConnect Secure Mobility solution also ensures a consistent enforcement of the network security policies to all users, no matter when, where and how they connect to the network.

The Cisco AnyConnect Secure Mobility is a collection of features across multiple Cisco products that extends control and security into borderless networks. The products that work together to provide AnyConnect Secure Mobility are as follows:

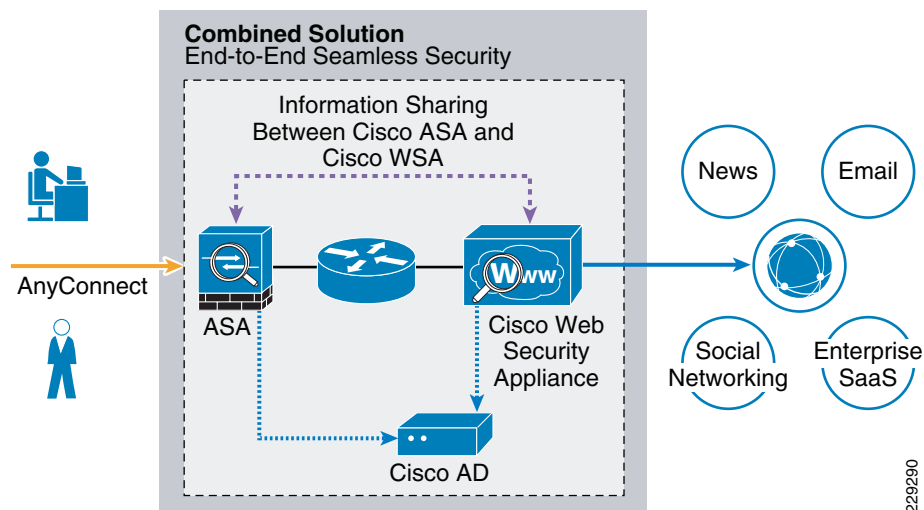
- Cisco IronPort Web Security appliance (WSA)
- Cisco ASA 5500 Series Adaptive Security Appliance (ASA)
- Cisco AnyConnect client

Cisco AnyConnect Secure Mobility addresses the challenges of a mobile workforce by offering the following features:

- Secure, persistent connectivity—Cisco AnyConnect (with the Cisco ASA at the headend) provides the remote access connectivity portion of AnyConnect Secure Mobility. The connection is secure because both the user and device must be authenticated and validated before being provided access to the network. The connection is persistent because Cisco AnyConnect is typically configured to be always-on even when roaming between networks. Although Cisco AnyConnect is always-on, it is also flexible enough to apply different policies based on location, allowing users access to the Internet in a “captive portal” situation, when users must accept terms of agreement before accessing the Internet.
- Persistent security and policy enforcement—The Web Security appliance applies context-aware policies, including enforcing acceptable use policies and protection from malware for all users, including mobile (remote) users. The WSA also accepts user authentication information from the AnyConnect client, providing an automatic authentication step for the user to access Web content.

Figure 22 illustrates the relationship between the various elements of the Cisco AnyConnect Secure Mobility solution.

Figure 22 *Cisco AnyConnect Secure Mobility Solution*



Remote and mobile users use the Cisco AnyConnect Secure VPN client to establish VPN sessions with the Cisco ASA appliance. The Cisco ASA sends Web traffic to the WSA appliance along with information identifying the user by IP address and user name. The WSA scans the traffic, enforces acceptable use policies, and protects the user from security threats. The Cisco ASA returns all traffic deemed safe and acceptable to the user.

All Internet traffic scanning is done by the WSA, not the client on the mobile device. This improves overall performance by not burdening the mobile device, some of which have limited processing power. In addition, by scanning Internet traffic on the network, the enterprise can more easily and quickly update security updates and acceptable use policies because the enterprise does not have to wait days, weeks, or even months to push the updates to the client. The WSA tracks the requests it receives and applies policies configured for remote users to traffic received from remote users.

For complete details about the Cisco AnyConnect Secure Mobility solution, see the documentation at: <http://www.cisco.com/en/US/netsol/ns1049/index.html>.

Threats Mitigated

The success of the security tools and measures in place ultimately depends on the degree they enhance visibility and control. Simply put, security can be defined as a function of visibility and control. Without any visibility, it is difficult to enforce any control, and without any control it is hard to achieve an adequate level of security. Therefore, the security tools selected in the enterprise network design were carefully chosen not only to mitigate certain threats but also to increase the overall visibility and control.

Table 2 summarizes how the security tools and measures used in the medium enterprise security design help mitigate certain threats, and how they contribute to increasing visibility and control. Note that the table is provided for illustration purposes and it is not intended to include all possible security tools, and threats.

Table 2 **Security Measures of the Medium Enterprise Security Design**

	Service Disruption	Harmful Content	Network Abuse	Unauthorized Access	Data Loss	Visibility	Control
Network Foundation Protection	X			X	X	X	X
Stateful Firewall	X		X	X		X	X
IPS	X	X	X	X		X	X
Security Mobility	X	X	X	X	X	X	X
Web Security		X	X	X	X	X	X
E-mail Security		X	X		X	X	X
Access Security and Control			X	X		X	X

Medium Enterprise Network Security Deployment Guidelines

The previous sections of this document provides design guidelines and considerations for deploying security within a medium enterprise network environment. The sections that follow provide deployment and configuration examples and guidelines for deploying some of these features. Security features and devices covered include the following:

- Internet border router edge ACL deployment
- Internet firewall deployment
- IPS Global Correlation deployment
- Web security deployment
- Cisco Catalyst Integrated Security Features deployment
- NAC deployment for wired and wireless clients

Internet Border Router Edge ACL Deployment

Whether the Internet border router is managed by the enterprise or the ISP, it must be hardened following the best practices discussed in [Network Foundation Protection](#). This includes restricting and controlling administrative access, protecting the management and control planes, and securing the dynamic exchange of routing information. In addition, the Internet border router may be leveraged as the first layer of protection against outside threats. To that end, edge ACLs, uRPF, and other filtering mechanisms may be implemented for anti-spoofing and to block invalid packets.

The following configuration snippets illustrate the structure of an edge ACL applied to the upstream interface of the Internet border router. The ACL is designed to block invalid packets and to protect the infrastructure IP addresses from the Internet. The configuration assumes the enterprise is assigned the 198.133.219.0/24 address block for its public-facing services, and that the upstream link is configured in the 64.104.10.0/24 subnet.

Module 1—Implement Anti-spoofing Denies

These ACLs deny fragments, RFC 1918 space, invalid source addresses, and spoofs of the internal address space.

- Deny fragments.


```
access-list 110 deny tcp any 198.133.219.0 0.0.0.255 fragments
access-list 110 deny udp any 198.133.219.0 0.0.0.255 fragments
access-list 110 deny icmp any 198.133.219.0 0.0.0.255 fragments
```
- Deny special-use address sources. (See RFC 3330 for additional special-use addresses.)


```
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
```
- Filter RFC 1918 space.


```
access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 172.16.0.0 0.15.255.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
```
- Deny packets spoofing the enterprise public addresses

```
access-list 110 deny ip 198.133.219.0 0.0.0.255 any
```

Module 2—Implement Explicit Permits

Permit only applications/protocols whose destination address is part of the infrastructure IP block. The source of the traffic should be known and authorized.

- Permit external BGP to peer 64.104.10.113

```
access-list 110 permit tcp host 64.104.10.114 host 64.104.10.113 eq bgp
access-list 110 permit tcp host 64.104.10.114 eq bgp host 64.104.10.113
```

Module 3—Implement Explicit Deny to Protect Infrastructure

```
access-list 110 deny ip 64.104.10.0 0.0.0.255 any
```

Module 4—Implement Explicit Permit for Traffic to the Enterprise's Public Subnet

```
access-list 110 permit ip any 198.133.219.0 0.0.0.255
```



Note

The 64.104.0.0/16 and 198.133.219.0/24 address blocks used in the examples in this document are reserved for the exclusive use of Cisco Systems, Inc.

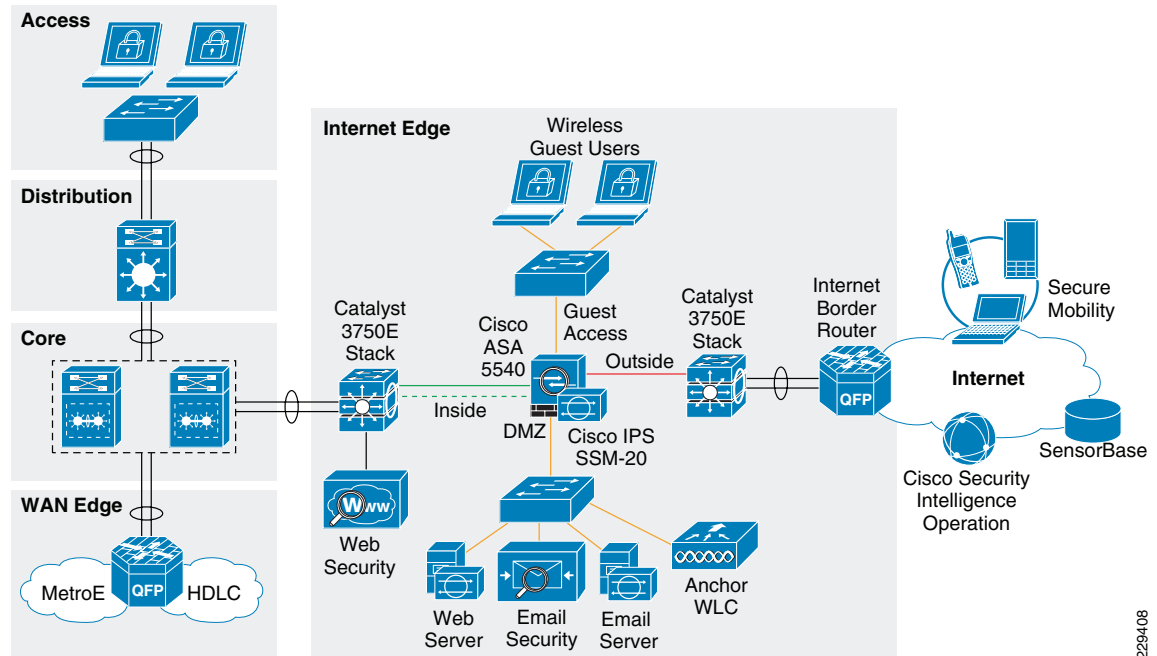
For more information and configuration examples on how to secure the Internet border router using the other Network Foundation Protection features, see “Chapter 6, Enterprise Internet Edge” in the *Cisco SAFE Reference Guide* at:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap6.html.

Internet Firewall Deployment

The Internet firewall is responsible for protecting the enterprise's internal resources and data from external threats, securing the public services provided by the DMZ, and to control user's traffic to the Internet. The medium enterprise network security uses a Cisco ASA appliance for the Internet firewall, as shown in [Figure 23](#).

Figure 23 Internet Edge Firewall



Firewall Hardening and Monitoring

The Cisco ASA should be hardened in a similar fashion as the infrastructure routers and switches. According to the Cisco SAFE security best practices, the following is a summary of the measures to be taken:

- Implement dedicated management interfaces to the OOB management network.
- Present legal notification for all access attempts.
- Use HTTPS and SSH for device access. Limit access to known IP addresses used for administrative access.
- Configure AAA for role-based access control and logging. Use a local fallback account in case the AAA server is unreachable.
- Use NTP to synchronize the time.
- Use Syslog or SNMP to keep track of system status, traffic statistics, and device access information. Authenticate routing neighbors and log neighbor changes.
- Implement firewall access policies (explained in [Firewall Access Policies](#)).

The Cisco ASA 5510 and higher appliance models come with a dedicated management interface that should be used whenever possible. Using a dedicated management interface keeps the management plane of the firewall isolated from threats originating from the data plane. The management interface should connect to the OOB management network, if one is available.

The following is an example of the configuration of a dedicated management interface:

```
interface Management0/0
 nameif management
 security-level 100
 ip address 172.26.136.170 255.255.254.0
 management-only
```

**Note**

Any physical interface or logical sub-interface can be configured as a management-only interface using the **management-only** command.

It is recommended that a legal notification banner is presented on all interactive sessions to ensure that users are notified of the security policy being enforced and to which they are subject. The notification banner should be written in consultation with your legal advisors.

The following example displays the banner after the user logs in:

```
banner motd UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
banner motd You must have explicit, authorized permission to access or configure this
device.
banner motd Unauthorized attempts and actions to access or use this system may result in
civil and/or criminal penalties.
banner motd All activities performed on this device are logged and monitored.
```

Management access to the firewall should be restricted to SSH and HTTPS. SSH is needed for CLI access and HTTPS is needed for the firewall GUI-based management tools such as CSM and ASDM. Additionally, this access should be permitted only for users authorized to access the firewalls for management purposes.

The following Cisco ASA configuration fragment illustrates the configuration needed to generate a 768 RSA key pair and enable SSH and HTTPS access for devices located in the management subnet:

```
! Generate RSA key pair with a key modulus of 768 bits
crypto key generate rsa modulus 768
! Save the RSA keys to persistent flash memory
write memory
! enable HTTPS
http server enable
! restrict HTTPS access to the firewall to permitted management stations
http <CSM/ASDM-IP-address> 255.255.255.255 management
! restrict SSH access to the firewall to well-known administrative systems
ssh <admin-host-IP-address-subnet> 255.255.255.0 management
! Configure a timeout value for SSH access to 5 minutes
ssh timeout 5
```

Administrative users accessing the firewalls for management must be authenticated, authorized, and access should be logged using AAA. The following Cisco ASA configuration fragment illustrates the AAA configurations needed to authenticate, authorize, and log user access to the firewall:

```
aaa-server tacacs-servers protocol tacacs+
 reactivation-mode timed
aaa-server tacacs-servers host <ACS-Server>
 key <secure-key>
aaa authentication ssh console tacacs-servers LOCAL
aaa authentication serial console tacacs-servers LOCAL
aaa authentication enable console tacacs-servers LOCAL
aaa authentication http console tacacs-servers LOCAL
aaa authorization command tacacs-servers LOCAL
aaa accounting ssh console tacacs-servers
aaa accounting serial console tacacs-servers
aaa accounting command tacacs-servers
aaa accounting enable console tacacs-servers
aaa authorization exec authentication-server
! define local username and password for local authentication fallback
username admin password <secure-password> encrypted privilege 15
```

As with the other infrastructure devices in the network, it is important to synchronize the time on the firewall protecting the management module using NTP.

The following configuration fragment illustrates the NTP configuration needed on a Cisco ASA to enable NTP to an NTP server located in the management network:

```
ntp authentication-key 10 md5 *
ntp authenticate
ntp trusted-key 10
ntp server <NTP-Server-address> source management
```

Syslog and SNMP can be used to keep track of system status, device access, and session activity. NetFlow Security Event Logging (NSEL), now supported on all Cisco ASA models, may also be used for the monitoring and reporting of session activity. The following configuration fragment illustrates the configuration of Syslog.

```
logging trap informational
logging host management <Syslog-Server-address>
logging enable
```

The routing protocol running between the Internet firewall and the distribution switch should be secured. The following Cisco ASA configuration fragment illustrates the use of EIGRP MD5 authentication to authenticate the peering session between the inside firewall interface and the Internet edge distribution switch:

```
interface Redundant1
description connection to CR12-3750s-IE distribution switch
nameif inside
security-level 100
ip address 10.125.32.18 255.255.255.240
authentication key eigrp 100 <removed> key-id 1
authentication mode eigrp 100 md5
```

Network Address Translation

NAT is required because enterprises typically get a limited number of public IP addresses. In addition, NAT helps shield the company's internal address space from reconnaissance and other malicious activity. The following illustrates the NAT configuration:

```
! Static translation for servers residing at DMZ
static (dmz,outside) 198.133.219.35 10.125.32.35 netmask 255.255.255.255
static (dmz,outside) 198.133.219.36 10.125.32.36 netmask 255.255.255.255
static (dmz,outside) 198.133.219.40 10.125.32.40 netmask 255.255.255.255
static (dmz,outside) 198.133.219.41 10.125.32.41 netmask 255.255.255.255
!
! Dynamic Port Address Translation (PAT) for inside hosts and wireless guest access
! clients going to the Internet
global (outside) 10 interface
nat (inside) 10 10.0.0.0 255.0.0.0
nat (guestaccess) 10 10.125.32.64 255.255.255.240
!
! Static translation for inside hosts going to the DMZ and vice-versa.
! The inside IP addresses are visible to the DMZ.
static (inside,dmz) 10.0.0.0 10.0.0.0 netmask 255.0.0.0
!
```

Firewall Access Policies

The Internet firewall should be configured with access policies to do the following:

- Protect the enterprise's internal resources and data from external threats by preventing incoming access from the Internet

- Protect public resources served by the DMZ by restricting incoming access to the public services and by limiting outbound access from DMZ resources out to the Internet
- Control user's Internet-bound traffic
- Prevent wireless guest access users from accessing internal resources

Enforcing such policies require configuration of the appropriate interface security levels and the deployment of ACLs to control what traffic is allowed or prevented from transiting between interfaces. By default, the Cisco ASA appliance allows traffic from higher to lower security level interfaces (that is, from inside to outside). However, depending on the sensitivity of an enterprise environment, the security administration are recommended to override the default rules with more stringent rules indicating exactly what ports and protocols are permitted.

In this configuration example, the inside, DMZ, guestaccess, and outside interfaces were configured with the security levels of 100, 50, 10, and 0 respectively. With this, by default any traffic originating from the inside to the DMZ, guestaccess, and outside, from the DMZ to the guestaccess and outside interface, and from the guestaccess to the outside is allowed freely. At the same time, any traffic originating from the outside to the DMZ, guestaccess, and inside, and from the DMZ to the guestaccess and inside interfaces is blocked. Although this may satisfy the basic access control requirements of the organization, it is always a good idea to reinforce the policies by enforcing granular ACLs.

Note also that, as the Cisco ASA inspects traffic, it is able to recognize packets belonging to already established sessions. The stateful inspection engine of the firewall dynamically allows the returning traffic associated with those sessions. Therefore, the firewall ACLs should be constructed to match traffic in the direction in which it is being initiated. In the following sample configurations, ACLs are applied in the ingress direction.

The following are guidelines and configuration examples for the ACLs controlling access and traffic flows:

- Ingress inside

Allow users residing at all enterprise sites to access the Internet for the allowed ports and protocols. Depending on the policy of the enterprise, this may only allow HTTP and HTTPS access or may be less restrictive to allow additional protocols and ports. The following example only allows HTTP and HTTPS access to the Internet:

```
access-list outbound extended permit tcp 10.0.0.0 255.0.0.0 any eq www
access-list outbound extended permit tcp 10.0.0.0 255.0.0.0 any eq https
```

Allow users access to DMZ services such as the company's Web portal, E-mail, and domain name resolution. This could include HTTP, HTTPS, SMTP, POP, IMAP, and DNS protocols. Permit tunneled control and user traffic from internal WLCs to Anchor WLC in DMZ for wireless guest access (UDP 16666, UDP 16667, IP Protocol 97). Permit management traffic from the management segment to the Anchor WLC in DMZ (SNMP, SSH, and HTTPS). Allow WSA access to the IronPort SensorBase network (HTTPS) for updates. Note that the previous entries in the ACL already permit HTTP and HTTPS traffic.

```
! Allow DNS queries to DNS server located in DMZ
access-list outbound extended permit udp 10.0.0.0 255.0.0.0 host 10.125.32.35 eq
domain

! Allow SMTP, POP3 and IMAP access to DMZ mail server
access-list outbound extended permit tcp 10.0.0.0 255.0.0.0 host 10.125.32.40 eq smtp
access-list outbound extended permit tcp 10.0.0.0 255.0.0.0 host 10.125.32.40 eq pop3
access-list outbound extended permit tcp 10.0.0.0 255.0.0.0 host 10.125.32.40 eq imap4

! Allow access to the Anchor WLC on the DMZ from the internal WLCs for wireless Guest
access
access-list outbound extended permit udp host 10.125.30.2 host 10.125.32.34 eq 16666
access-list outbound extended permit udp host 10.125.30.3 host 10.125.32.34 eq 16666
access-list outbound extended permit udp host 10.124.2.66 host 10.125.32.34 eq 16666
```

```

access-list outbound extended permit udp host 10.125.30.2 host 10.125.32.34 eq 16667
access-list outbound extended permit udp host 10.125.30.3 host 10.125.32.34 eq 16667
access-list outbound extended permit udp host 10.124.2.66 host 10.125.32.34 eq 16667
access-list outbound extended permit 97 host 10.125.30.2 host 10.125.32.34
access-list outbound extended permit 97 host 10.125.30.3 host 10.125.32.34
access-list outbound extended permit 97 host 10.124.2.66 host 10.125.32.34
! Allow management access to the Anchor WLC on the DMZ
access-list outbound extended permit udp 10.125.31.0 255.255.255.0 host 10.125.32.34
eq snmp
access-list outbound extended permit udp 10.125.31.0 255.255.255.0 host 10.125.32.34
eq snmptrap
access-list outbound extended permit tcp 10.125.31.0 255.255.255.0 host 10.125.32.34
eq ssh
!
! Apply ACL to inside interface
access-group outbound in interface inside

```

- Ingress DMZ

Restrict connections initiated from DMZ only to the necessary protocols and sources. This typically includes DNS queries and zone transfer from DNS server, SMTP from E-mail server, HTTP/SSL access from the Cisco IronPort ESA for updates, SensorBase, and so on.

```

! Allow DNS queries and zone transfer from DNS server
access-list dmz-acl extended permit udp host 10.125.32.35 any eq domain
access-list dmz-acl extended permit tcp host 10.125.32.35 any eq domain
!
! Allow SMTP from Cisco IronPort ESA
access-list dmz-acl extended permit tcp host 10.125.32.36 any eq smtp
!
! Allow update and SensorBase access to Cisco IronPort ESA
access-list dmz-acl extended permit tcp host 10.125.32.36 any eq www
access-list dmz-acl extended permit tcp host 10.125.32.36 any eq https
!
! Apply ACL to DMZ interface
access-group dmz-acl in interface dmz

```

- Ingress outside

Inbound traffic from the Internet should be restricted to the public services provided at the DMZ such as SMTP, Web, and DNS. Any connection attempts to internal resources and subnets from the Internet should be blocked. ACLs should be constructed using the servers' global IP addresses.

```

! Allow DNS queries and zone transfer to DNS server
access-list inbound extended permit udp any host 198.133.219.35 eq domain
access-list inbound extended permit tcp any host 198.133.219.35 eq domain
!
! Allow SMTP to Cisco IronPort ESA
access-list inbound extended permit tcp any host 198.133.219.36 eq smtp
!
! Allow HTTP/HTTPS access to the company's public web portal
access-list inbound extended permit tcp any host 198.133.219.41 eq www
access-list inbound extended permit tcp any host 198.133.219.41 eq https
!
! Apply ACL to outside interface
access-group inbound in interface outside

```

- Ingress guest access

Wireless guest access users should be restricted to only having access to the Internet. Access to the internal enterprise network should not be allowed. Because the security level of the guest access interface is lower than the internal and DMZ interfaces, traffic coming from the guest access interface going to the internal and DMZ segments is automatically blocked. In addition, because the

security level for the guest access interface is also higher than the outside interface, traffic is permitted to the Internet. If the guest wireless clients need to access the DMZ servers, an ACL needs to be configured and applied to allow this access. However, if desired to reinforce this policy, granular ACLs may also be applied to the guest access interface.

```
! Deny access to internal networks
access-list guestaccess-acl extended deny ip any 10.0.0.0 255.0.0.0
access-list guestaccess-acl extended deny ip any 192.168.0.0 255.255.0.0
access-list guestaccess-acl extended deny ip any 172.16.0.0 255.240.0.0
! Permit all other access to the Internet, Internet2 and NLR network
access-list guestaccess-acl extended permit ip any any
!
! Apply ACL to guest-access interface
access-group guestaccess-acl in interface guestaccess
```

Firewall Redundancy

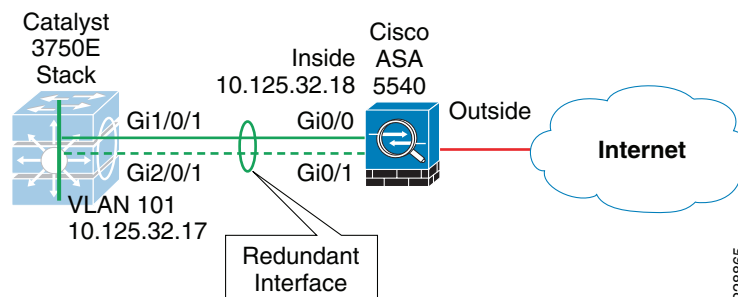
The Internet perimeter of the medium enterprise network uses a single Cisco ASA appliance configured with redundant interfaces. The use of redundant interfaces makes the design resilient to link-level failures, representing an affordable option for high availability. In cases where chassis redundancy is desirable, the enterprise may consider deploying a pair of Cisco ASA appliances configured for stateful failover. Both active/active and active/standby failover modes are supported. Although stateful failover protects against chassis failures, it requires the deployment of two identical Cisco ASA appliances and the adjustment of the topologies around the firewalls, so its deployment should be carefully planned.

This section explains the use of redundant interfaces. For information on how to configure stateful failover using multiple platforms, see the *Cisco ASA 5500 Series Adaptive Security Appliances Configuration Guides* at:

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html.

A Cisco ASA redundant interface is a logical interface that pairs two physical interfaces, called *active* and *standby* interfaces. Under normal operation, the active interface is the only one passing traffic. The active interface uses the IP address defined at the redundant interface, and the MAC address of the first physical interface associated with the redundant interface. When the active interface fails, the standby interface becomes active and starts passing traffic. The same IP address and MAC address are maintained so that traffic is not disrupted. Figure 24 illustrates the concept of redundant interface

Figure 24 Cisco ASA Redundant Interface



The configuration of a redundant interface requires the configuration of the physical interface parameters and the logical redundant interface. Physical parameters such as media type, duplex, and speed are still configured within the physical interface. IP address, interface name, routing protocols, security level are configured as part of the logical redundant interface. The following configuration example corresponds to Figure 24.

```

! Physical interface and Ethernet parameters
interface GigabitEthernet0/0
  description Connection to CR12-3750s-IE port Gig1/0/1
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/1
  description backup connection to CR12-3750s-IE port Gig2/0/1
  no nameif
  no security-level
  no ip address
!
! Define logical redundant interface and associate with physical interfaces.
! Configures IP and logical interface parameters.

interface Redundant1
  description connected to CR12-3750s-IE
  member-interface GigabitEthernet0/0
  member-interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 10.125.32.18 255.255.255.240
  authentication key eigrp 100 ***** key-id 1
  authentication mode eigrp 100 md5
!

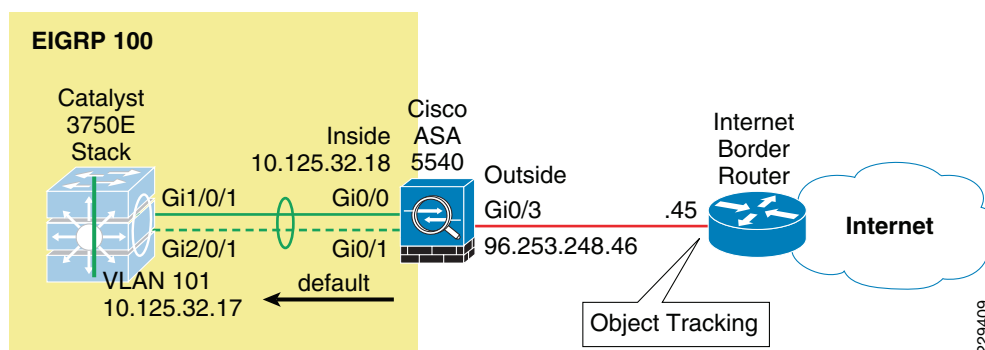
```

Routing

Within the medium enterprise network, an interior gateway protocol, EIGRP, is used for dynamic routing. The Internet firewall may participate in routing by learning the internal routes within the enterprise network and by injecting a default route pointing to the Internet. The default route should be removed dynamically if the Internet connection becomes unavailable.

Within the medium enterprise network, the Cisco ASA appliance is configured with a static default route pointing to the Internet gateway. Object tracking is configured to dynamically remove the default route when the Internet connection becomes unavailable. The default route is redistributed into EIGRP, and from there propagated into the rest of the internal network, as shown in [Figure 25](#).

Figure 25 Cisco ASA Static Route



It is highly recommended to use object tracking so that the default route is removed when the Internet connection becomes unavailable. Without object tracking, the default route is removed only if the outside interface of the appliance goes down. Therefore, there is a possibility that the default route may remain in the routing table even if the Internet border router becomes unavailable. To avoid this problem, the static default route can be configured with object tracking. This is accomplished by associating the

default route with a monitoring target. The Cisco ASA appliance monitors the target using ICMP echo requests. If an echo reply is not received within a specified time period, the object is considered down and the associated default route is removed from the routing table.

The monitoring target needs to be carefully selected. Pick one that can receive and respond to ICMP echo requests sent by the Cisco ASA. It is better to use a persistent network object. In the configuration example below, the Cisco ASA monitors the IP address of the next hop gateway, which helps identifying if the Internet gateway goes down, but it will not help if the connection is lost upstream. If available, you may want to monitor a persistent network object located somewhere in the ISP network. Static route tracking can also be configured for default routes obtained through DHCP or PPPoE.

In the following configuration snippet, the IP address of the next hop gateway (96.253.248.45) is used as the monitoring target. The static default route is then redistributed into EIGRP.

```
router eigrp 100
 network 10.125.32.0 255.255.255.0
 passive-interface default
 no passive-interface dmz
 no passive-interface inside
 redistribute static metric 1000000 2000 255 1 1500
!
route outside 0.0.0.0 0.0.0.0 96.253.248.45 1 track 10
!
sla monitor 1
 type echo protocol ipIcmpEcho 96.253.248.45 interface outside
sla monitor schedule 1 life forever start-time now
!
track 10 rtr 1 reachability
```


Note

The frequency and timeout parameters of object tracking can be adjusted to detect topological changes faster.

Another option for dynamically controlling the injection and removal of a default route in the enterprise routing table is to use OSPF where the Cisco ASA appliance learns the default route from the Internet border router using OSPF. The default route is then redistributed into EIGRP, and from there propagated into the rest of the internal network. Injecting a default route with OSPF requires the configuration of an OSPF process between the Cisco ASA and the Internet border router. If the Internet border router is managed by the ISP, the configuration requires coordination with the service provider. This scenario also requires the default route to be propagated over OSPF. The actual default route may originate from the Internet border router itself or somewhere in the ISP network.

Botnet Traffic Filter

The medium enterprise network security design uses the ASA Botnet Traffic Filter on the Internet firewall to detect malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or other proprietary data) when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses (the blacklist), and then logs or blocks any suspicious activity.

Configuring the Botnet Traffic Filter requires the following steps:

1. Configuring the DNS server
2. Enabling the use of the dynamic database
3. Enabling DNS snooping
4. Enabling traffic classification and actions for the Botnet Traffic Filter

5. Verifying and monitoring the Botnet Traffic Filter operation

The following sections provide configuration examples for each of these steps.

Configuring DNS Server

The Botnet Traffic Filter requires a DNS server to access Cisco's dynamic database update server and to resolve entries in the static database. The following configuration illustrates this configuration:

```
! Enable DNS requests to a DNS Server out the outside interface
dns domain-lookup outside
! Specify the DNS Server Group and the DNS Servers
dns server-group DefaultDNS
  name-server 68.238.112.12
  name-server 68.238.96.12
  domain-name cisco.com
```

Enabling Use of the Dynamic Database

The Botnet Traffic Filter can receive periodic updates for the dynamic database from the Cisco update server. This database lists thousands of known bad domain names and IP addresses. The following configuration enables database updates, and also enables use of the downloaded dynamic database by the adaptive security appliance.

```
! enable downloading of the dynamic database from the Cisco Update server
dynamic-filter updater-client enable
! enable use of the dynamic database
dynamic-filter use-database
```

Enabling DNS Snooping

DNS Snooping enables inspection of DNS packets and enables Botnet Traffic Filter Snooping, which compares the domain name with those in the dynamic or static databases and adds the name and IP address to the DNS reverse lookup cache. This cache is then used by the Botnet Traffic Filter when connections are made to the suspicious address.

It is recommended that DNS Snooping be enabled only on interfaces where external DNS requests are going. Enabling DNS Snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the ASA. For example, if the DNS server is on the outside interface, you should enable DNS inspection with snooping for all UDP DNS traffic on the outside interface.

The following configuration example illustrates enabling DNS Snooping on the outside interface:

```
! create a class map to identify the traffic you want to inspect DNS
class-map dynamic-filter-snoop-class
  match port udp eq domain
! create a policy map to enable DNS inspection with Botnet Traffic Filtering snooping
! for the class map
policy-map dynamic-filter-snoop-policy
  class dynamic-filter-snoop-class
    inspect dns preset_dns_map dynamic-filter-snoop
! activate the policy map on the outside interface
service-policy dynamic-filter-snoop-policy interface outside
```

Enabling Traffic Classification and Actions for the Botnet Traffic Filter

The Botnet Traffic Filter compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a Syslog message and/or drops any matching traffic. When an address matches,

the Cisco ASA sends a Syslog message and can optionally be configured to drop the connection. You can enable Botnet Traffic Filter on a subset of traffic or for all traffic by enabling an access list to classify traffic.

The following configuration example enables the Botnet Traffic Filter feature on all traffic and additionally enables dropping of connections going to IP addresses with a severity of moderate and higher.

```
! identify the traffic that you want to monitor or drop.
access-list btf-filter-acl extended permit ip any any
! enable Botnet Traffic Filter on the outside interface for traffic classified by the
! btf-filter-acl access list
dynamic-filter enable interface outside classify-list btf-filter-acl
! enable automatic dropping of traffic with threat level moderate or higher
dynamic-filter drop blacklist interface outside action-classify-list btf-filter-acl
threat-level range moderate very-high
```

Monitoring and Verifying the Botnet Traffic Filter

To monitor and verify the operation of the Botnet Traffic Filter feature, use the following commands:

- **show dynamic-filter updater-client**—Shows information about the updater server, including the server IP address, the next time the adaptive security appliance will connect with the server, and the database version last installed.

```
cr12-asa-1-ie# show dynamic-filter updater-client
Dynamic Filter updater client is enabled
Updater server URL is https://update-manifests.ironport.com
Application name: threatcast, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8a8c5097dc1d252b9cff62d26d4ec58e202883d704fc62b85bf8629
fa757fe36b
Last update attempted at 15:14:11 UTC Apr 7 2010,
  with result: Downloaded file successfully
Next update is in 00:52:14
Database file version is '1270651144' fetched at 15:14:11 UTC Apr 7 2010, size:
2097152
cr12-asa-1-ie#
```

- **show dynamic-filter data**—Shows information about the updater server, including the server IP address, the next time the adaptive security appliance will connect with the server, and the database version last installed.

```
cr12-asa-1-ie# show dynamic-filter data
Dynamic Filter is using downloaded database version '1270651144'
Fetched at 15:14:11 UTC Apr 7 2010, size: 2097152
Sample contents from downloaded database:
  win-antimalware2.com  firstlook.com  red-devil-sport-club.gymdb.com
mswindowsupdate.info
  zardoz.wizardz.com  exchange.bg  bisexual-photo.com  lookmbbox.com
Sample meta data from downloaded database:
  threat-level: very-high,      category: Malware,
  description: "These are sources that use various exploits to deliver adware, spyware
and other malware to victim computers. Some of these are associated with rogue online
vendors and distributors of dialers which deceptively call premium-rate phone
numbers."
  threat-level: high,      category: Bot and Threat Networks,
  description: "These are rogue systems that control infected computers. They are
either systems hosted on threat networks or systems that are part of the botnet
itself."
  threat-level: moderate,      category: Spyware,
```

```
description: "These are sources that distribute spyware, adware, greyware, and other
potentially unwanted advertising software. Some of these also run exploits to install
such software."
```

```
threat-level: low, category: Ads,
```

```
description: "These are advertising networks that deliver banner ads, interstitials,
rich media ads, pop-ups, and pop-unders for websites, spyware and adware. Some of
these networks send ad-oriented HTML emails and email verification services."
```

```
Total entries in Dynamic Filter database:
```

```
Dynamic data: 82119 domain names , 2565 IPv4 addresses
```

```
Local data: 0 domain names , 0 IPv4 addresses
```

```
Active rules in Dynamic Filter asp table:
```

```
Dynamic data: 0 domain names , 2565 IPv4 addresses
```

```
Local data: 0 domain names , 0 IPv4 addresses
```

```
cr12-asa-1-ie#
```

- **show dynamic-filter statistics detail**—Shows how many connections were monitored and dropped with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist. (The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.) The detail keyword shows how many packets at each threat level were classified or dropped.

```
cr12-asa-1-ie# show dynamic-filter statistics detail
```

```
Enabled on interface outside using classify-list btf-filter-acl
```

```
Total conns classified 35, ingress 0, egress 35
```

```
Total whitelist classified 0, ingress 0, egress 0
```

```
Total greylist classified 16, dropped 0, ingress 0, egress 16
```

```
Threat-level very-high: classified 0, dropped 0, ingress 0,
egress 0
```

```
Threat-level high: classified 0, dropped 0, ingress 0,
egress 0
```

```
Threat-level moderate: classified 0, dropped 0, ingress 0,
egress 0
```

```
Threat-level low: classified 16, dropped 0, ingress 0,
egress 16
```

```
Threat-level very-low: classified 0, dropped 0, ingress 0,
egress 0
```

```
Total blacklist classified 19, dropped 0, ingress 0, egress 19
```

```
Threat-level very-high: classified 9, dropped 0, ingress 0,
egress 9
```

```
Threat-level high: classified 0, dropped 0, ingress 0,
egress 0
```

```
Threat-level moderate: classified 0, dropped 0, ingress 0,
egress 0
```

```
Threat-level low: classified 10, dropped 0, ingress 0,
egress 10
```

```
Threat-level very-low: classified 0, dropped 0, ingress 0,
egress 0
```

```
cr12-asa-1-ie#
```



Note

To clear the statistics, enter the **clear dynamic-filter statistics** *[interface name]* command.

Other commands that are useful for monitoring the Botnet Traffic Filter include the following:

- **show dynamic-filter reports top [malware-sites | malware-ports | infected-hosts]**—Generates reports of the top 10 malware sites, ports, and infected hosts monitored. The top 10 malware-sites report includes the number of connections dropped, and the threat level and category of each site. This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected.

- **show dynamic-filter reports infected-hosts {max-connections | latest-active | highest-threat | subnet ip_address netmask | all}**—Generates reports about infected hosts. These reports contain detailed history about infected hosts, showing the correlation between infected hosts, visited malware sites, and malware ports. The max-connections keyword shows the 20 infected hosts with the most number of connections. The latest-active keyword shows the 20 hosts with the most recent activity. The highest-threat keyword shows the 20 hosts that connected to the malware sites with the highest threat level. The subnet keyword shows up to 20 hosts within the specified subnet. The all keyword shows all buffered infected-hosts information. This display might include thousands of entries. You might want to use ASDM to generate a PDF file instead of using the CLI.
- **show dynamic-filter dns-snoop [detail]**—Shows the Botnet Traffic Filter DNS Snooping summary, or with the detail keyword, the actual IP addresses and names. All inspected DNS data is included in this output, and not just matching names in the blacklist. DNS data from static entries are not included.
- **show asp table dynamic-filter [hits]**—Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.

Intrusion Prevention Deployment

The medium enterprise security design implements Intrusion Prevention using an Advanced Inspection and Prevention Security Services Module (AIP SSM) on the Cisco ASA appliance deployed at the Internet perimeter. This section describes some of the best practices for integrating and configuring the IPS service module for maximum threat control and visibility as well as the deployment of the IPS Global Correlation feature.

Deploying IPS with the Cisco ASA

The AIP SSM is supported in the Cisco ASA 5510 and higher platforms. The AIP SSM runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic including worms and network viruses before they can affect your network.

The AIP SSM may be deployed in inline or promiscuous mode as described in [Intrusion Prevention Guidelines](#). In inline mode, the AIP SSM is placed directly in the traffic flow; in promiscuous mode, the Cisco ASA sends a duplicate stream of traffic to the AIP SSM for inspection.

When deploying the AIP SSM in inline mode, it is important to determine how traffic should be treated in case of module failure. The AIP SSM may be configured to fail open or close when the module becomes unavailable. When configured to fail open, the Cisco ASA appliance allows all traffic through uninspected, if the AIP SSM becomes unavailable leaving your network unprotected. Conversely, when configured to fail close, the Cisco ASA blocks all traffic in case of an AIP SSM failure. This is more secure but impacts traffic during a failure.

The following example illustrates how a Cisco ASA can be configured to divert all IP traffic to the AIP SSM in inline mode, and to block all IP traffic in the AIP SSM card fails for any reason:

```
access-list IPS extended permit ip any any
class-map ips_class
  match access-list IPS
policy-map ips_policy
  class ips_class
    ips inline fail-close
service-policy ips_policy global
```

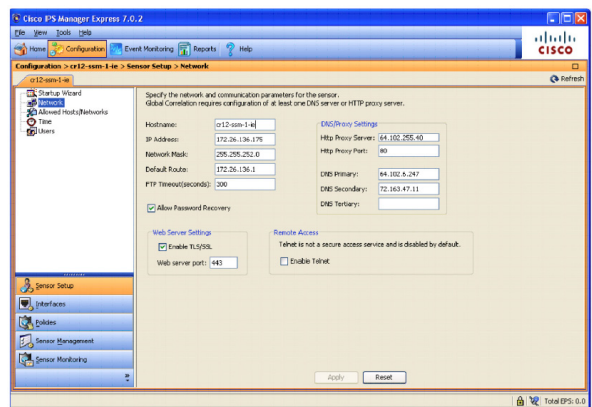
IPS Global Correlation Deployment

Before configuring IPS Global Correlation, be sure that you are using Cisco IPS Version 7.0 with the latest patch and signature updates and that Cisco IPS is configured for network connectivity in either IDS or IPS mode.

The configuration of Global Correlation can be performed using the command-line interface (CLI), Cisco IDS Device Manager (IDM), Cisco IME, or Cisco Security Manager. The following screenshots from Cisco IME illustrate the basic steps in the configuration of the IPS Global Correlation.

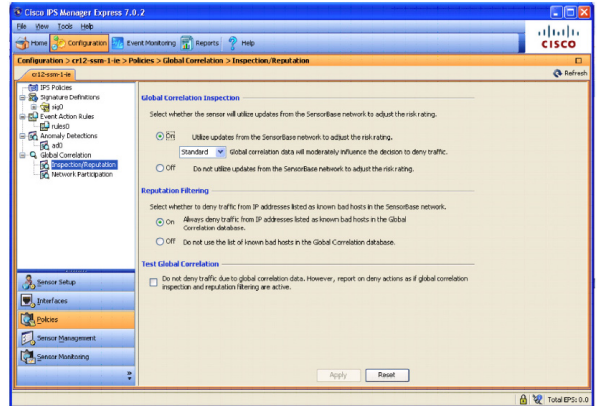
The first step in configuring the IPS sensor (module or appliance) to use Global Correlation is to add either a DNS address and/or the proxy server setup. This step enables a connection to Cisco SensorBase and is illustrated in [Figure 26](#). After you configure the DNS and proxy settings, the Global Correlation settings goes into effect as soon as the sensor has downloaded the latest Global Correlation updates.

Figure 26 *DNS and HTTP Proxy Within the Network Setting Configuration Screen*

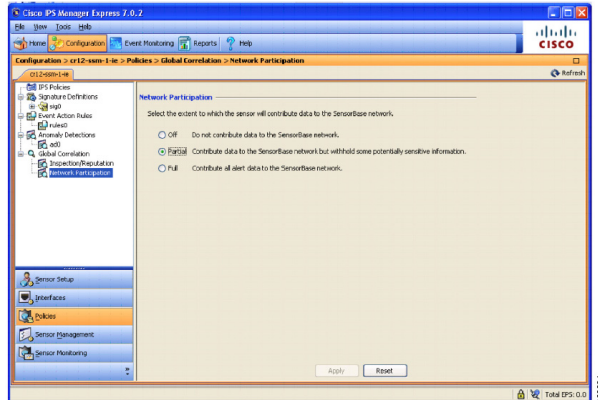


By default, a sensor runs Global Correlation Inspection in Standard mode and enables the reputation filters, as illustrated in [Figure 27](#). A good practice is to configure Global Correlation Inspection initially in permissive mode while monitoring the effects, and then later change the configuration to Standard or Aggressive mode as desired.

Figure 27 **Global Correlation Inspection Settings**



By default, network participation is disabled, which means the sensor does not share any event data back to the Cisco SensorBase network. The event data provided by all devices participating in the Cisco SensorBase network is a key element that provides realtime and worldwide visibility into threat activity, which accelerates the identification and mitigation of threats propagating throughout the Internet. For this reason, it is recommended to configure the IPS sensors with partial or full network participation. Network participation configuration is illustrated in [Figure 28](#).

Figure 28 **Network Participation Settings (Off by Default)**

Event Monitoring with Global Correlation

Event monitoring with IPS Global Correlation is similar to event monitoring with signature-only IPS. The primary difference is the potential addition of reputation scores representing the Global Correlation data. [Figure 29](#) shows Cisco IPS events with reputation scores in Cisco IME.

Figure 29 Event Monitoring with Global Correlation in Cisco ISE

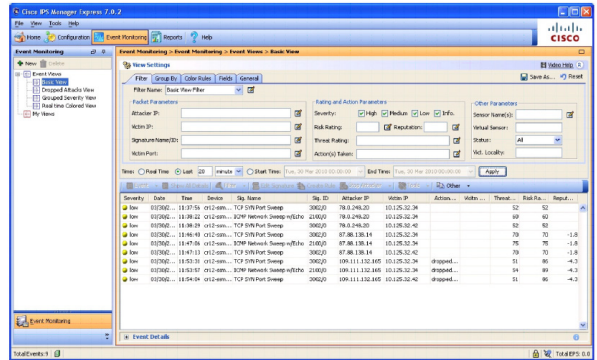
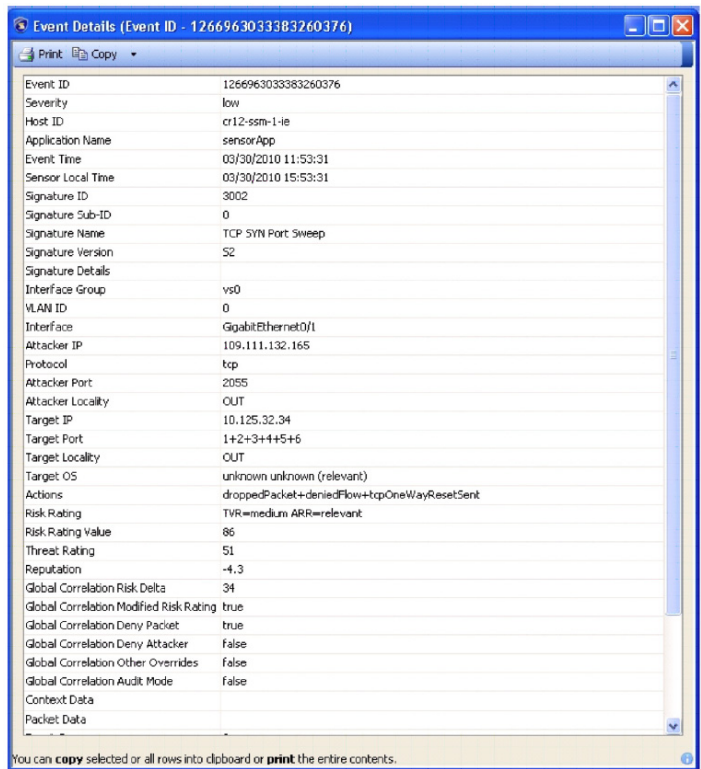


Figure 29 shows several TCP SYN Port Sweep and ICMP Network Sweep attacks that were seen by the sensor. The first three events had no reputation, and the event's risk ratings were 52 and 60, which did not meet the threshold for the packets to be dropped. The next three events were identical except that the attacker had a negative reputation of -1.8 , which elevated the risk ratings to 70 and 75 but still did not meet the thresholds to be dropped in Standard mode. The last events were also identical, except this time the attacker has a negative reputation of -4.3 , which elevated the risk ratings to 86 and 89. This time the risk rating was high enough for the packets to be dropped.

Figure 30 illustrates the detailed view of the TCP SYN Port Sweep event coming from the attacker with a negative reputation of -4.3 .

Figure 30 *Detailed View of a TCP SYN Port Sweep from an Attacker with a Negative Reputation Score*

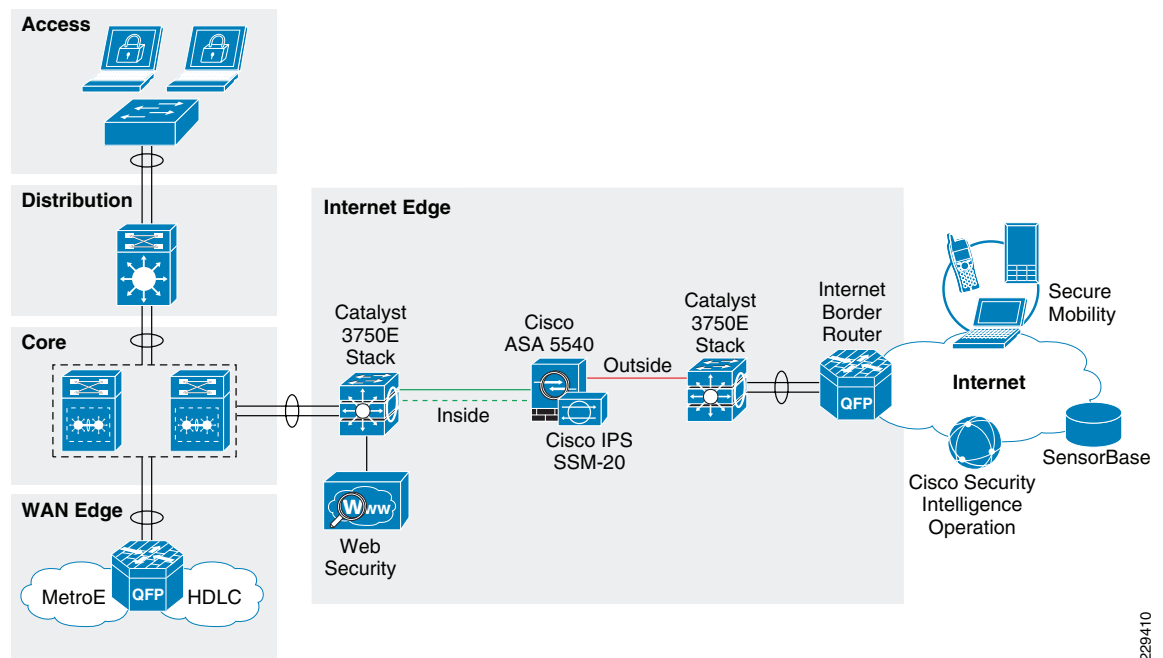


Event Details (Event ID - 126696303383260376)	
Event ID	126696303383260376
Severity	low
Host ID	cr12-ssm-1-1e
Application Name	sensorApp
Event Time	03/30/2010 11:53:31
Sensor Local Time	03/30/2010 15:53:31
Signature ID	3002
Signature Sub-ID	0
Signature Name	TCP SYN Port Sweep
Signature Version	S2
Signature Details	
Interface Group	vs0
VLAN ID	0
Interface	GigabitEthernet0/1
Attacker IP	109.111.132.165
Protocol	tcp
Attacker Port	2055
Attacker Locality	OUT
Target IP	10.125.32.34
Target Port	1+2+3+4+5+6
Target Locality	OUT
Target OS	unknown unknown (relevant)
Actions	droppedPacket+deniedFlow+tcpOneWayResetSent
Risk Rating	TVR=medium ARR=relevant
Risk Rating Value	86
Threat Rating	51
Reputation	-4.3
Global Correlation Risk Delta	34
Global Correlation Modified Risk Rating	true
Global Correlation Deny Packet	true
Global Correlation Deny Attacker	false
Global Correlation Other Overrides	false
Global Correlation Audit Mode	false
Context Data	
Packet Data	

You can **copy** selected or all rows into clipboard or **print** the entire contents.

Web Security Deployment

The medium enterprise security design implements a Cisco IronPort WSA at the Internet edge distribution layer at the main site, as illustrated in [Figure 31](#). The WSA is located at the inside of the Cisco ASA acting as the Internet firewall. Deploying the WSA at the Internet edge distribution layer gives the WSA complete visibility on the traffic before getting out to the Internet through the firewall.

Figure 31 WSA Deployment

229410

The following subsections provide guidelines for the WSA configuration and deployment.

Initial System Setup Wizard

The WSA provides a browser-based system setup wizard that must be executed the first time the appliance is installed. The System Setup Wizard guides the user through the initial system configuration, such as network and security settings. Note that running the initial system setup wizard completely reconfigures the WSA appliance and resets the administrator password. Only use the system setup wizard the first time you install the appliance, or if you want to completely overwrite the existing configuration.

The following are some of the default settings when running the System Setup Wizard:

- Web Proxy is deployed in transparent mode.
- The L4 Traffic Monitor is active and set to monitor traffic on all ports.

Interface and Network Configuration

As part of the initial setup of the WSA, the following steps need to be completed:

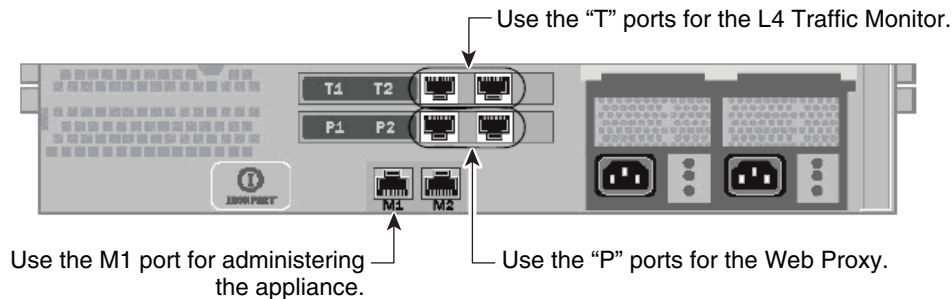
1. Configuring network interfaces
2. Adding routes
3. Configuring DNS
4. Setting time

These settings are configured as part of an initial setup using the system setup wizard, but can be later modified using the Cisco WSA Web-based GUI.

Configuring Network Interfaces

Independent of the model, all Cisco IronPort WSA appliances are equipped with six Ethernet interfaces, as shown in [Figure 32](#).

Figure 32 **WSA Interfaces**



227435

The WSA interfaces are grouped for the following functions:

- **Management**—Interfaces M1 and M2 are out-of-band (OOB) management interfaces. However, only M1 is enabled. In the medium enterprise network, interface M1 connects to the out-of-band management network. Interface M1 can optionally be used to handle data traffic in case the enterprise does not have an out-of-band management network.
- **Web Proxy**—Interfaces P1 and P2 are Web Proxy interfaces used for data traffic. Only the P1 interface is used in the medium enterprise network security design. P1 connects to the inside subnet of the firewall.
- **L4 Traffic Monitor (L4TM)**—T1 and T2 are the L4TM interfaces. These ports are used to capture traffic for inspection using either SPAN on a switch or a network tap. L4TM was not validated as part of the Medium Enterprise Design Profile, Cisco IPS Global Correlation and the Cisco ASA Botnet Traffic Filter features were used instead. For more information on L4TM, see the WSA configuration guides at:
http://www.cisco.com/en/US/docs/security/wsa/wsa6.3/user_guide/WSA_6.3.0_GA_UserGuide.pdf.

[Figure 33](#) illustrates the network topology for the WSA design in the validation lab.

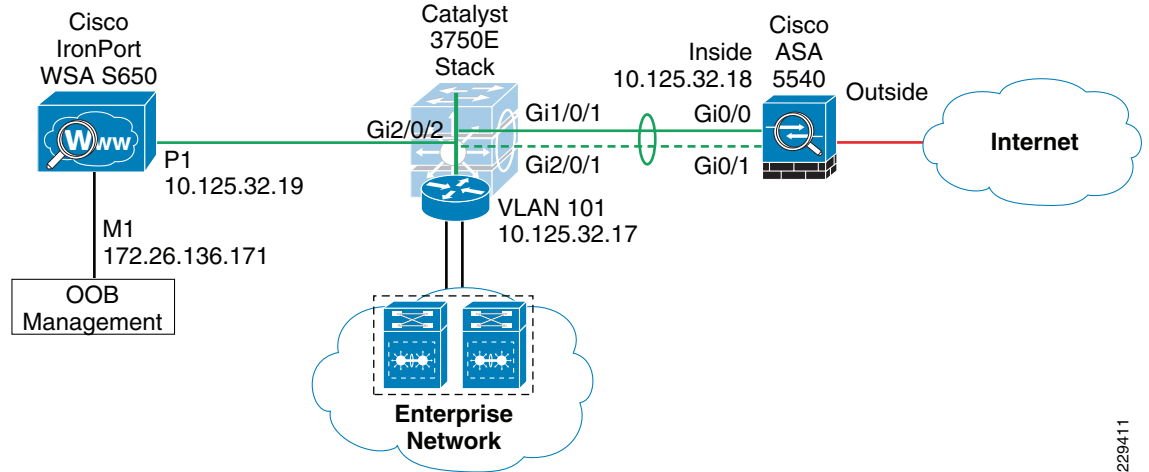
Figure 33 WSA Network Topology

Figure 34 shows the IP address and hostname configurations for the interfaces used within the WSA Web-based GUI. In this case, an OOB management network is used where the M1 port is configured with an IP address in the management subnet. In addition, the WSA is configured to maintain a separate routing instance for the M1 management interface. This allows the definition of a default route for management traffic separate from the default route used for data traffic.

Figure 34 WSA Interface Configuration**Interfaces**

Interfaces				
Interfaces:	Ethernet Port	IP Address	Netmask	Hostname
	M1	172.26.136.171	255.255.252.0	ironport.cisco.com
	P1	10.125.32.19	255.255.255.240	ironport.cisco.com
Separate Routing for Management Services:	Separate routing (M1 port restricted to appliance management services only)			
Appliance Management Services:	HTTP on port 8080, HTTPS on port 8443, Redirect HTTP request to HTTPS			
L4 Traffic Monitor Wiring:	Duplex TAP: T1 (In/Out)			
				Edit Settings...

Adding Routes

A default route is defined for management traffic pointing to the OOB management default gateway (172.26.136.1). A separate default route is defined for the data traffic pointing to the inside IP address of the firewall (10.125.32.18). Because all internal networks are reachable through the Internet edge distribution switch, a route to 10.0.0.0/8 is defined, pointing to the switch IP address (10.125.32.17) to allow the WSA to communicate with the clients directly. These settings are illustrated in Figure 35.

Figure 35 *WSA Route Configuration*

Routes

Routes for Management Traffic (Interface M1: 172.26.136.171, Interface P1: 10.125.32.19)

Add Route...
Save Route Table...
Load Route Table...

Name	Destination Network	Gateway	<input type="checkbox"/> All Delete
Default Route	All Others	172.26.136.1	<input type="checkbox"/> Delete

Routes for Data Traffic (Interface P1: 10.125.32.19)

Add Route...
Save Route Table...
Load Route Table...

Name	Destination Network	Gateway	<input type="checkbox"/> All Delete
Default Route	All Others (Including External)	10.125.32.18	<input type="checkbox"/> Delete
Internal-10	10.0.0.0/8	10.125.32.17	<input type="checkbox"/> Delete

228876

Configuring DNS

The initial setup requires the configuration of a host name for the WSA appliance, and defining the DNS servers. [Figure 36](#) shows the DNS configuration.

Figure 36 *WSA DNS Configuration*

DNS

DNS Server Settings

DNS Servers:

Use these DNS Servers:

Priority	IP Address
0	10.125.31.2
0	68.238.112.12

Routing Table for DNS traffic: Data

Wait Before Timing out Reverse DNS Lookups: 20 seconds

DNS Domain Search List: None

Clear DNS Cache
Edit Settings...

228877

Setting Time

Time synchronization is critical for forensic analysis and troubleshooting; therefore, enabling NTP is highly recommended. [Figure 37](#) shows how the WSA is configured to synchronize its clock with an NTP server located on the OOB management network.

Figure 37 WSA NTP Configuration**Time Settings**

Time Keeping Method: Using NTP Servers:	
1	172.26.129.252

Routing Table for NTP Server Queries: Management

Edit Settings...

**Note**

If Internet access is provided by an upstream proxy, the WSA must be configured to use the proxy for component updates and system upgrades. For information on configuring upstream proxies for upgrades, see the WSA configuration guides at:

http://www.cisco.com/en/US/docs/security/wsa/wsa6.3/user_guide/WSA_6.3.0_GA_UserGuide.pdf.

WCCP Transparent Web Proxy

The configuration of the WCCP Transparent Web Proxy includes the following steps:

1. Defining a WSA WCCP service group
2. Enabling WSA Transparent Redirection
3. Enabling WCCP redirection on the Cisco ASA
4. Enabling WSA HTTPS scanning

Defining WSA WCCP Service Group

Web Proxy settings are configured as part of an initial setup using the system setup wizard and can be later modified with the WSA Web-based GUI. The Web Proxy settings include the following:

- HTTP Ports to Proxy—Lists the ports to be proxied. Default is 80 and 3128.
- Caching—Defines whether or not the WSA should cache response and requests. Caching helps reduce latency and the load on the Internet links. Default is enabled.
- IP Spoofing—Defines whether or not the Web Proxy should spoof IP addresses when forwarding requests to upstream proxies and servers.

Figure 38 illustrates the Web Proxy settings.

Figure 38 WSA Proxy Settings

Proxy Settings

Web Proxy Settings	
Basic Settings	
Proxy:	Enabled
HTTP Ports to Proxy:	80, 3128
Caching:	Enabled Clear Cache
Proxy Mode:	Transparent
IP Spoofing:	Not Enabled
Advanced Settings	
Persistent Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
In-Use Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
Simultaneous Persistent Connections:	Server Maximum Number: 2000
Headers:	X-Forwarded-For: Do Not Send VIA: Send
Edit Settings...	

228879

Enabling WSA Transparent Redirection

Configuring WCCP Transparent Redirection requires the definition of a WCCP service profile in the WSA. If redirecting HTTP and HTTPS, define a dynamic service ID to be used with the Cisco Catalyst Internet edge distribution switch. Use MD5 authentication to protect the WCCP communication between the WSA and Cisco Catalyst Switch. [Figure 39](#) shows an example.

Figure 39 WSA WCCP Settings

WCCP v2 Service	
Service Profile Name:	web-https-cache
Service:	<input type="radio"/> Standard service ID: 0 web-cache (destination port 80) <input checked="" type="radio"/> Dynamic service ID: <input type="text" value="10"/> 0-255 <div> Port numbers: <input type="text" value="80,443"/> <small>(up to 8 port numbers, separated by commas)</small> </div> <div> <input checked="" type="radio"/> Redirect based on destination port <input type="radio"/> Redirect based on source port (return path) <small>For IP spoofing, define two services, one based on destination port and another based on source port (return path).</small> </div> <div> <input checked="" type="radio"/> Load balance based on server address <input type="radio"/> Load balance based on client address <small>Applies only if more than one Web Security Appliance is in use.</small> </div>
Router IP Addresses:	<input type="text" value="10.125.32.17"/> <small>Separate multiple entries with line breaks or commas.</small>
Router Security:	<input checked="" type="checkbox"/> Enable Security for Service <div> Password: <input type="password" value="....."/> Confirm Password: <input type="password" value="....."/> </div>
Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.	

228880

Enabling WCCP Redirection on Cisco Catalyst 3750E Distribution Switch

The configuration of WCCP on the Cisco Catalyst 3750 switch requires the following components:

- A group-list indicating the IP addresses of the WSA appliances that are members of the service group. In the example provided below, the group-list is called *wsa-farm*.
- A redirect-list indicating the ports and subnets of traffic to be redirected. In the example, the ACL named *proxylist* is configured to redirect any HTTP and HTTPS traffic coming from the 10.0.0.0/8 subnet.
- WCCP service indicating the service ID. The service ID defined on the Cisco Catalyst switch must be the same as the service ID defined on the WSAs. Use a password for MD5 authentication.
- Enabling WCCP redirection on an interface. Apply the WCCP service on the Internet edge distribution switch interface facing the core switch.

The following is a Cisco Catalyst switch configuration example:

```
! Group-list defining the IP addresses of all WSAs
ip access-list standard wsa-farm
  permit 10.125.32.19
!
! Redirect-list defining what ports and hosts/subnets should be redirected
ip access-list extended proxylist
  permit tcp 10.0.0.0 0.255.255.255 any eq www
  permit tcp 10.0.0.0 0.255.255.255 any eq 443
!
! Configure WCCP service
ip wccp 10 redirect-list proxylist group-list wsa-farm password <MD5-password>
!
! Apply WCCP on an interface
interface Port-channel1
ip wccp 10 redirect in
!
```

The WCCP connection status and configuration can be monitored on the Cisco Catalyst 3750 Switch with the **show ip wccp** command, as shown by the following example:

```
cr12-3750s-ie#show ip wccp
Global WCCP information:
  Router information:
    Router Identifier:          10.125.200.23
    Protocol Version:          2.0
  Service Identifier: 10
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets s/w Redirected: 0
      Process: 0
      CEF: 0
    Redirect access-list: proxylist
    Total Packets Denied Redirect: 0
    Total Packets Unassigned: 5
    Group access-list: wsa-farm
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0

cr12-3750s-ie#
```



Note

Cisco Catalyst 3750 Switches support switching in hardware only at Layer 2; therefore, no counters increment when the **show ip wccp** command is issued on the switch.

Enabling WSA HTTPS Scanning

To monitor and decrypt HTTPS traffic, you must enable HTTPS scanning on the WSA. The HTTPS Proxy configuration is illustrated in Figure 40.

Figure 40 **WSA HTTPS Proxy**

HTTPS Proxy

HTTPS Proxy Settings	
HTTPS Proxy:	Enabled
Transparent HTTPS Ports to Proxy:	443
Root Certificate and Key for Signing:	Using Generated Certificate: Common name: Cisco Systems, Inc Organization: CMO Organizational Unit: ESE Country: US Expiration Date: Oct 14 16:30:47 2010 GMT Basic Constraints: Not Critical
Invalid Certificate Handling:	Expired: Monitor Mismatched Hostname: Monitor Unrecognized Root Authority: Monitor All other error types: Monitor

2288831

[Edit Settings...](#)



Note

In cases where Internet access is handled by upstream proxies, you must configure the WSA to route through the upstream proxies. For information regarding the configuration of upstream proxies, see the Cisco IronPort WSA configuration guide at:

http://www.cisco.com/en/US/docs/security/wsa/wsa6.3/user_guide/WSA_6.3.0_GA_UserGuide.pdf.

Web Access Policies

The access policies define how the Web Proxy handles HTTP requests and decrypted HTTPS connections for network users. By configuring access policies, the enterprise can control what Internet applications (instant messaging clients, peer-to-peer file-sharing, Web browsers, Internet phone services, and so on) and URL categories users can access. In addition, access policies can be used to block file downloads based on file characteristics, such as file size and file type.

The WSA comes with a default global policy that applies to all users. However, multiple policies can be defined when different policies need to be applied to different group of users. Figure 41 shows the global policy.

Figure 41 Global Access Policy**Access Policies**

Policies						
Add Policy...						
Order	Group	Applications	URL Categories	Objects	Web Reputation and Anti-Malware Filtering	Delete
	Global Policy Identity: All	Allow: FTP over HTTP, HTTP, Native FTP Block: User Agents Allow: Ports 8080, 21,...	Redirect: 0 Allow: 0 Monitor: 51 Warn: 0 Block: 3 Time-Based: 0	HTTP/HTTPS Object Max Size: None FTP Object Max Size: None	(enabled)	

228882

URL categories corresponding to non-business related content should be blocked in compliance with the company's Internet access policies. Figure 42 provides an example on how the Adult/Sexually Explicit and Chat categories are blocked.

Figure 42 URL Categories**Access Policies: URL Categories: Global Policy**

Custom URL Category Filtering				
No Custom URL Categories are defined. Add categories in the Custom URL Categories page.				
Predefined URL Category Filtering				
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.				
Category	Monitor 	Warn 	Block 	Time-Based
Adult/Sexually Explicit	Select all	Select all	Select all	(Unavailable)
Advertisements & Popups				—
Alcohol & Tobacco				—
Arts				—
Blogs & Forums				—
Business				—
Chat				—
Computing & Internet				—

228883

Cisco Catalyst Integrated Security Features Deployment

Within the medium enterprise network, the Cisco Catalyst Integrated Security Features (CISF) were implemented in the access layer switches. CISF is a set of native security features available on the Cisco Catalyst switches that protect the infrastructure and users from spoofing, man-in-the-middle (MITM), DoS, and other access layer attacks. The following configuration illustrates an example of the CISF configurations used on a Cisco 3750E switch in the access layer in the medium enterprise network.

```
! configure dhcp snooping on the access VLANs in global configuration mode
ip dhcp snooping vlan 101-113
no ip dhcp snooping information option
ip dhcp snooping
!
! configure arp inspection on the access VLANs in global configuration mode
ip arp inspection vlan 101-113
ip arp inspection validate src-mac dst-mac ip allow zeros
!
```

```

! configure the port recovery parameters for ports being disabled by dhcp snooping,
arp-inspection, or storm control
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery interval 120
!
! configure port specific parameters on access ports
interface GigabitEthernet1/0/1
! configure port security parameters
switchport port-security
switchport port-security aging time 5
switchport port-security violation restrict
switchport port-security aging type inactivity
! configure arp inspection rate limiting
ip arp inspection limit rate 100
! configure storm control parameters
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
! configure IP Source Guard parameters
ip verify source

```

**Note**

When deploying Cisco Catalyst 3000 Switches in the access layer in a routed Layer 3 deployment, configuring IP Source Guard causes edge router ACLs and VLAN ACLs to be ineffective for blocking traffic. When IP Source Guard is enabled, it creates a port-based ACL to permit only traffic from IP addresses that were assigned via the DHCP server. On Cisco Catalyst 3000 Switches, port-based ACLs override router and VLAN ACLs, resulting in all traffic being permitted to all destinations.

Cisco NAC Appliance Deployment

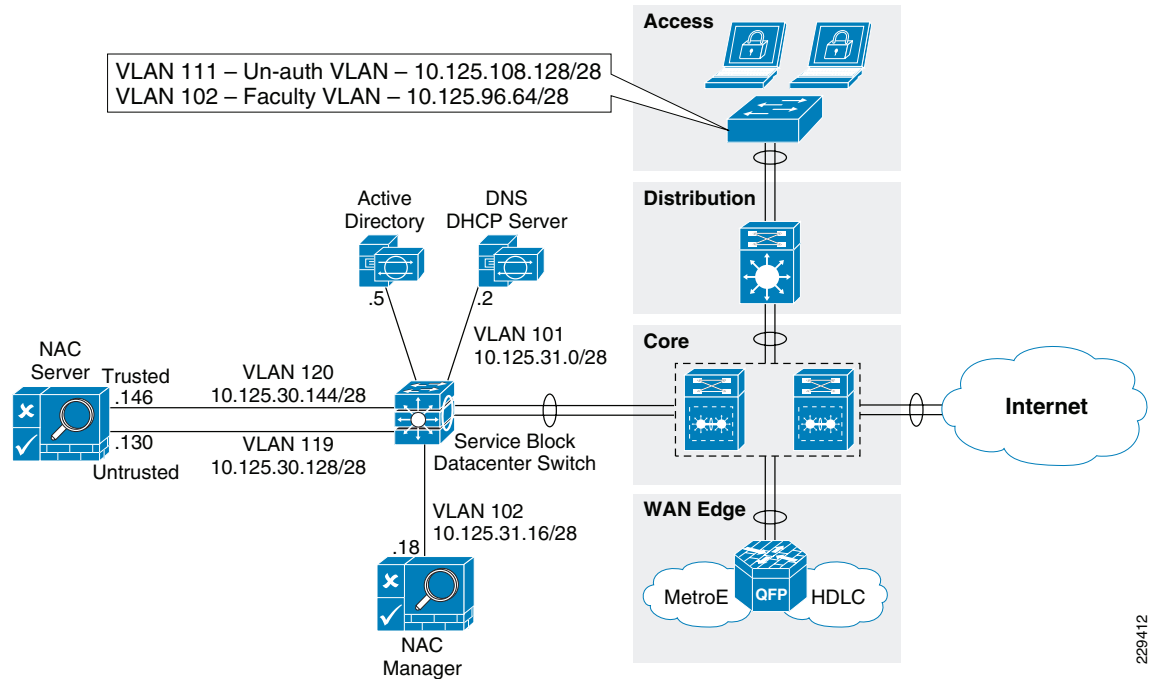
In the medium enterprise network, a NAC Appliance solution is deployed at all locations; the main site and each of the remote offices. A centralized NAC Manager is deployed at the main site and is deployed within the data center at that site. A NAC server is deployed at the main site and each of the remote sites, and is connected within the service block connecting to the core switches at each of the sites.

The medium enterprise network provides host network connectivity using wired and wireless technologies. As such, the Cisco NAC Appliance solution must provide a solution for both connectivity options. For wireless clients, a Layer 2 OOB NAC solution is deployed; and for wired clients, a Layer 2 OOB or a Layer 3 OOB NAC solution may be deployed.

The following subsections provide configuration steps for configuring a Layer 3 OOB NAC solution for wired clients and a Layer 2 OOB NAC solution for wireless clients.

NAC Deployment for Wired Clients

Within the medium enterprise network, a NAC Layer 3 OOB deployment using ACLs was used for the wired clients. [Figure 43](#) shows a diagram of the Layer 3 OOB logical network that was used to validate NAC for wired clients in the medium enterprise network.

Figure 43 NAC L3 OOB Logical Topology Diagram

The following subsections illustrate the needed steps to configure a Layer 3 real-IP OOB NAC deployment using ACLs.

Configuring the Edge Access Switch for Enforcement

VLANs and edge ACLs are used on the access switches to restrict access to the network based on the NAC assigned user roles. The following configuration snippets provide sample configurations for two VLANs (Unauthenticated and Employee) and the associated edge ACLs. Edge ACLs and VLANs should be configured on all access switches to which users are connecting.

- Unauthenticated role—VLAN 111 and ACL Name: *nac-unauth-acl*

```
! create NAC unauthenticated VLAN
vlan 111
  name nac-unauth-vlan
! create SVI for unauthenticated VLAN
interface Vlan111
  ip address 10.125.108.129 255.255.255.192
  ip helper-address 10.125.31.2
!
! configure ACL for the unauthenticated role
ip access-list extended nac-unauth-acl
! allow Discovery packets from the NAC Agent to the NAC Server
  permit udp any host 10.125.30.130 eq 8906
! allow Discovery packets from the NAC Agent to the NAC Server for ADSSO
  permit udp any host 10.125.30.130 eq 8910
! allow web traffic from the PC to the NAC Server
  permit tcp any host 10.125.30.130 eq www
! allow SSL traffic from the PC to the NAC Server
  permit tcp any host 10.125.30.130 eq 443
! allow DHCP traffic to the DHCP server
  permit udp any host 255.255.255.255 eq bootps
  permit udp any host 10.125.31.2 eq bootps
! allow DNS traffic to the DNS Server
```

```

permit udp any host 10.125.31.2 eq domain
permit tcp any host 10.125.31.2 eq domain
! allow traffic to the remediation servers
permit tcp any host 12.120.79.206 eq www
permit tcp any host 12.120.10.243 eq www
permit tcp any host 12.120.11.243 eq www
permit tcp any host 12.120.78.208 eq www
permit tcp any host 216.151.177.81 eq ftp
!
! apply ACL to the Unauthenticated VLAN
interface Vlan111
ip access-group nac-unauth-acl in

```

- Employee role—VLAN 102 and ACL name: *employee-acl*

When the client is moved to this VLAN, if the native NAC Agent is used, it still attempts to discover the NAC Server. This NAC Agent behavior is by design. If the Agent is able to reach the NAC Server, the Agent pops up, trying to perform the login process again, even though the client is already granted access. To prevent this, an ACL entry needs to be added to the ACL on the employee VLAN to prevent UDP 8906 Discovery packets originating from the Agent being dropped after the client is authenticated. The following configuration snippet illustrates the ACL entry needed to drop these discovery packets on the authenticated employee VLAN.

```

! create NAC employee VLAN
vlan 102
name employee-vlan
! create SVI for employee VLAN
interface Vlan102
ip address 10.125.96.65 255.255.255.192
ip helper-address 10.125.31.2
! configure ACL for the employee role to prevent NAC Discovery packets from
! reaching NAC Server
ip access-list extended employee-acl
deny udp any host 10.125.30.130 eq 8906
permit ip any any
!
! apply ACL to the employee VLAN
interface Vlan102
ip access-group employee-acl in

```

NAC Manager and NAC Servers Initial Setup

The initial installation and configuration of the NAC Manager and NAC Server is performed via console access, and the install utility guides you through the initial configuration for both NAC Manager and NAC Server. To perform initial setup, see:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html.

Applying the License to the NAC Manager

After performing the initial setup through the console, the rest of the configuration of the NAC Manager and Server is performed using the NAC Manager GUI. The first step is to upload the NAC Manager and Server licenses that came with the appliances. For more details on uploading the licenses, see:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html#wp1113597.

Updating Policies from Cisco.com on the NAC Manager

The NAC Manager needs to be configured to retrieve periodic updates from the central update server located at Cisco. The Cisco NAC Appliance Supported AV/AS Product List is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported AV and AS vendors and product versions used to configure AV or AS Rules and AV or AS Definition Update requirements for posture assessment/remediation. This list is updated regularly for the AV/AS products and versions supported in each Agent release and include new products for new Agent versions. The list provides version information only. When the CAM downloads the Supported AV/AS Product List, it is downloading the information about what the latest versions are for AV/AS products; it is not downloading actual patch files or virus definition files. Based on this information, the Agent can then trigger the native AV/AS application to perform updates. For details on setting this up, see:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html#wp1351880.

Installing Certificates from Third-Party Certificate Authority (CA)

During installation, the initial configuration utility script for both the NAC Manager and NAC Server requires you to generate a temporary SSL certificate. For a lab environment, you may continue to use the self-signed CERTs. However, the self-signed CERTs are not recommended for a production network. For more information on installing certificates on the NAC Manager from a third-party certificate authority (CA), see:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_admin.html#wp1078189.

For more information on installing certificates on the NAC Server from a third-party CA, see:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_admin.html#wp1040111.



Note

If you are using the self-signed certificates in the lab environment, the NAC Manager and NAC Server need to trust the certificate of each other, which requires you to upload each other's certificates as a Trusted Certificate Authority under SSL > Trusted Certificate Authorities.

Adding the NAC Server to the NAC Manager

To add the NAC Server to the NAC Manager, from within the NAC Manager GUI, do the following:

- Step 1** Click **CCA Servers > New Server**.
- Step 2** Add the IP address of the NAC Server's Trusted interface, select **Out-of-Band Real-IP-Gateway** from the *Server Type* dropdown list, and click **Add Clean Access Server**. See [Figure 44](#).

Figure 44 Adding the NAC Server to the NAC Manager

The screenshot shows the Cisco Clean Access Standard Manager interface. On the left is a navigation menu with sections: Device Management (containing CCA Servers, Filters, and Clean Access), OOB Management (containing Profiles and Devices), and User Management (containing User Roles, Auth Servers, and Local Users). The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and 'Device Management > Clean Access Servers'. It has three tabs: 'List of Servers', 'New Server', and 'Authorization'. The 'New Server' tab is active, showing a form to add a new server. The form fields are: Server IP Address (10.125.30.146), Server Location (Main Site DC), and Server Type (Virtual Gateway). There is an 'Add Clean Access Server' button at the bottom.

Once added, the NAC Server appears in the list.



Note

The NAC Manager and NAC Server have to trust each other's CA for NAC Manager to successfully add the NAC server.

Configuring the NAC Server

Step 3 Click the **Manage** icon for the NAC Server to continue the configuration. See [Figure 45](#).

Figure 45 NAC Server Managed by NAC Manager

The screenshot shows the Cisco Clean Access Standard Manager interface. On the left is a navigation menu with sections: Device Management (containing CCA Servers, Filters, and Clean Access), OOB Management (containing Profiles and Devices), and User Management (containing User Roles, Auth Servers, and Local Users). The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and 'Device Management > Clean Access Servers'. It has three tabs: 'List of Servers', 'New Server', and 'Authorization'. The 'List of Servers' tab is active, showing a table of NAC servers.

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.125.30.146	Out-of-Band Real-IP Gateway	Main Site DC	Connected				
10.125.30.114	Out-of-Band Virtual Gateway	Wireless L2 OOB	Connected				

Step 4 After clicking the **Manage** icon, click the **Network** tab.

Layer 3 Support

Step 5 To enable Layer 3 support for L3 OOB, check (enable) the options for the following:

- Enable L3 Support
- Enable L3 strict mode to block NAT devices with Clean Access Agent

Step 6 Click **Update** and reboot the NAC Server as instructed, as shown in [Figure 46](#).

Figure 46 NAC Server Network Details

The screenshot shows the Cisco Clean Access Standard Manager web interface, Version 4.7.2. The breadcrumb navigation is "Device Management > Clean Access Servers > 10.125.30.146". The left sidebar contains a navigation menu with sections: Device Management (CCA Servers, Filters, Clean Access), OOB Management (Profiles, Devices), User Management (User Roles, Auth Servers, Local Users), Monitoring (Summary, Online Users, Event Logs, SNMP), and Administration (CCA Manager). The main content area has tabs for Status, Network, Filter, Advanced, Authentication, and Misc. The "Network" tab is active, showing the "IP" sub-tab. The "Clean Access Server Type" is set to "Out-of-Band Real-IP Gateway". Checkboxes for "Enable L3 support", "Enable L3 strict mode to block NAT devices with NAC Agent", and "Enable L2 strict mode to block L3 devices with NAC Agent" are all checked. The "Platform" is set to "APPLIANCE". Below this, there are two sections: "Trusted Interface (to protected network)" and "Untrusted Interface (to managed network)". Each section has fields for IP Address, Subnet Mask, and Default Gateway. For the Trusted Interface, the values are IP: 10.125.30.146, Subnet Mask: 255.255.255.240, and Default Gateway: 10.125.30.145. For the Untrusted Interface, the values are IP: 10.125.30.130, Subnet Mask: 255.255.255.240, and Default Gateway: 10.125.30.129. There are also checkboxes for "Set management VLAN ID" and "Pass through VLAN ID to managed/protected network". A note at the bottom states: "(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)". At the bottom right are "Update" and "Reboot" buttons.

**Note**

Always generate the certificate for the NAC Server with the IP address of its untrusted interface. For name-based certificate, the name should resolve to the untrusted interface IP address. When the endpoint communicates with the untrusted interface of the NAC Server to begin the NAC process, the NAC Server will redirect the user to the certificate hostname or IP. If the certificate points to the trusted interface, the login process does not function correctly.

Static Routes

Once the NAC Server reboots, return to managing the NAC Server and continue the configuration. The NAC Server will need to communicate with endpoints on the unauthenticated VLAN with the untrusted interface.

- Step 1** Go to **Advanced > Static Routes** to add routes to the unauthenticated VLAN.
- Step 2** Fill in the appropriate subnets for the unauthenticated VLANs and click **Add Route**. Be sure to select **untrusted interface [eth1]** for these routes. See [Figure 47](#).

Figure 47 Adding Static Route to Reach the Unauthenticated User Subnet

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar contains navigation menus for Device Management, OOB Management, User Management, and Monitoring. The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and shows the path 'Device Management > Clean Access Servers > 10.125.30.146'. Below this, there are tabs for Status, Network, Filter, Advanced, Authentication, and Misc. The 'Static Routes' tab is selected, showing a form to add a static route. The form fields are: Dest. Subnet Address/Mask (10.125.108.128 / 26), Gateway (optional) (10.125.30.129), Link (Untrusted [eth1]), and Description (static route for unauthenticated users on cr22-4). An 'Add Route' button is at the bottom right.

Setup Profiles for Managed Switches in the NAC Manager

- Step 3** Each switch will be associated with a profile. Add a profile for each type of edge switch the NAC Manager will manage by going to **Profiles** and clicking on the **Device** tab. In the example shown in [Figure 48](#), a Cisco Catalyst 4507 switch is added.

Figure 48 SNMP Profile Used to Manage a Cisco Catalyst 4507 Switch

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar contains navigation menus for Device Management, OOB Management, User Management, and Monitoring. The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and shows the path 'OOB Management > Profiles'. Below this, there are tabs for Group, Device, Port, VLAN, and SNMP Receiver. The 'Device' tab is selected, showing a form to add a profile. The form fields are: Profile Name (CR22_4507_LB), Device Model (Cisco Catalyst 4000/4500 series), SNMP Port (161), and Description (Cisco 4507 L3 Access Switch in Ma). Below these are sections for SNMP Read Settings and SNMP Write Settings, each with fields for SNMP Version (SNMP V2C) and Community String (cisco123 for read, enterprise for write). 'Update' and 'Reset' buttons are at the bottom right.

Switch Configuration for SNMP

- Step 4** The edge access switches should be configured for SNMP read/write community strings, which are the same as those configured on the NAC Manager.

```
snmp-server community enterprise RW
snmp-server community cisco123 RO
```

Configuring Port Profiles

Step 5 For individual port control, configure a port profile under **OOB Management > Profiles > Ports** that includes the default unauthenticated VLAN and default access VLAN.

Step 6 In the access VLAN section, specify the User Role VLAN. The NAC Manager changes the unauthenticated VLAN to the access VLAN based on the VLAN defined in the role where the user belongs.

The next step is to define the port profile to control the port's VLAN based upon User Roles and VLANs implemented.

In the example shown in [Figure 49](#), the Auth VLAN is the unauthenticated VLAN to which unauthenticated devices are initially assigned. The default access VLAN is the employee VLAN. This is used if the authenticated user does not have a role-based VLAN defined.

Step 7 For the access VLAN, select **User Role VLAN** to map users to the VLAN configured in the user's role. The **Access VLAN** can override the default VLAN to a user role VLAN, which is defined under the **User Role**.

Figure 49 Port Profile to Manage the Switch Port

The screenshot shows the Cisco Clean Access Standard Manager web interface, Version 4.7.2. The left sidebar contains navigation menus for Device Management, OOB Management (with 'Profiles' highlighted), User Management, and Monitoring. The main content area is titled 'OOB Management > Profiles' and shows a table with columns for Group, Device, Port, VLAN, and SNMP Receiver. Below the table, the configuration for a profile named 'Employee_Port' is displayed. The description is 'Access Switches in Large'. The 'Manage this port' checkbox is checked. Under 'VLAN Settings', the 'Auth VLAN' is set to 'VLAN ID' 111, the 'Default Access VLAN' is set to 'VLAN ID' 102, the 'Access VLAN' is set to 'User Role VLAN', and the 'VLAN Profile' is set to 'Default'. A note at the bottom of the VLAN settings states: 'Supported VLAN Name format: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name.'



Note

You can also define VLAN names instead of IDs. This offers the flexibility of having different VLAN IDs on different switches across the site, but the same VLAN name attached to a particular Role.

Step 8 Additional options are available under the port profile for IP release/renew options. If the user is behind an IP phone, uncheck the option for bouncing the port, which will likely reboot the IP phone when the port is bounced. See [Figure 50](#).

Figure 50 Various Options Available under Port Profile

Cisco Clean Access Standard Manager Version 4.7.2

Options: Device Connected to Port

The CAM discovers the device connected to the switch port when it receives SNMP mac-notification or linkup traps for the device. The CAM then instructs the switch to assign the **Auth VLAN** to the port if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated. You can additionally configure the following options:

- ☒ Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (ALLOW=Default Access VLAN, DENY=Auth VLAN, ROLE/CHECK=User Role VLAN, IGNORE=ignore SNMP traps from managed switches (IP Phones)).
- ☒ Change to **Auth VLAN** if the device is certified but not in the out-of-band user list.
Select the VLAN to assign when device is certified and user is reconnecting to network.
- ☐ Bounce the port after VLAN is changed.
Check this box to help clients update their IP settings for non-Virtual Gateways. You can leave this field unchecked for Virtual Gateways.
- ☒ Bounce the port based on role settings after VLAN is changed.
- ☒ Generate event logs when there are multiple MAC addresses detected on the same switch port.

Options: Device Disconnected from Port

The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:

- ☒ Remove out-of-band online user when SNMP linkdown trap is received, and then **change to Auth VLAN**.
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.
- ☒ Remove other out-of-band online users on the switch port when a new user is detected on the same port.
Ensure only one valid user is allowed on one switch port at the same time.
- ☐ Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.

Update

SNMP Receiver Setting

In addition to setting up the SNMP community string for Read/Write, you also need to configure the NAC Manager to receive SNMP traps from the switch. These traps are sent when the user connects and disconnects from the port. When the NAC Server sends the MAC/IP address information of a particular end point to the NAC Manager, the Manager is able to build a mapping table internally for MAC/IP and switch port. See [Figure 51](#).

Figure 51 NAC Manager SNMP Receiver Setting to Collect SNMP Traps/Informs

Cisco Clean Access Standard Manager Version 4.7.2

OOB Management > Profiles

Group	Device	Port	VLAN	SNMP Receiver
SNMP Trap				Advanced Settings

(Configure the SNMP daemon running on the Clean Access Manager. The device setup must match these settings to be able to send traps to the Clean Access Manager)

Trap Port on Clean Access Manager:

SNMP V1 Settings

Community String:

SNMP V2c Settings

Community String:

SNMP V3 Settings

Security Method (Auth/Priv):

User Name:

User Auth:

User Priv:

Update

The switch needs to be configured to enable SNMP traps to be sent to the NAC Manager. In addition, it is recommended to increase the default switch CAM table entry flush timer to one hour per Cisco best practice recommendations for NAC OOB. This reduces the frequency of MAC notifications that are sent out from already connected devices to the NAC Manager. Having a source trap command ensures a consistent source address will be used to send out the traps.

```
! global applicable SNMP configurations
snmp-server trap-source Loopback0
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.125.31.18 version 2c NacTraps
! interface specific configurations
mac-address-table aging-time 3600
```

You can optionally configure Linkup/Linkdown traps to send to the NAC Manager. They are used only in a deployment scenario where the end hosts are *not* connected behind an IP phone.

Adding Switches as Devices in the NAC Manager

- Step 1** The switch profile created in the previous section is used to add the managed switches. Under the **Device Profile**, use the profile you created, but do not change the default port profile value when adding the switch. See [Figure 52](#).

Figure 52 Adding Edge Switch in the NAC Manager to Control via SNMP

Configure Switch Ports for the Devices to be Managed by NAC

- Step 2** Once the switch is added to the NAC Manager, you can select the ports that you want to manage. See [Figure 53](#).

Figure 53 Port Control Selection for a Managed Switch

The screenshot displays the Cisco Clean Access Standard Manager interface, version 4.7.2. The left sidebar contains navigation menus for Device Management, OOB Management, User Management, Monitoring, and Administration. The main content area is titled 'Cisco Clean Access Standard Manager' and shows the configuration for a switch at 10.125.200.1. The 'Ports' tab is selected, showing a table of port configurations. The table includes columns for Name, Index, Description, Status, Bounce, Initial VLAN, Current VLAN, MAC Notif., Client MAC, Profile, and Note. The table lists 12 ports, with the first 11 being GigabitEthernet ports and the last being a TenGigabitEthernet port. The status of the ports is indicated by colored dots: red for uncontrolled and green for controlled. The 'Profile' column shows the assigned profile for each port, such as 'Default [uncontrolled]' or 'Employee_Port'.

Name	Index	Description	Status	Bounce	Initial VLAN	Current VLAN	MAC Notif.	Client MAC	Profile	Note
Te2/2	4	TenGigabitEthernet2/2	Red	Icon	1	1	X	Icon	Default [uncontrolled]	
Gi2/3	5	GigabitEthernet2/3	Red	Icon	1	111	X	Icon	Employee_Port	
Gi2/4	6	GigabitEthernet2/4	Red	Icon	1	111	X	Icon	Employee_Port	
Gi2/5	7	GigabitEthernet2/5	Red	Icon	1	111	X	Icon	Employee_Port	
Gi2/6	8	GigabitEthernet2/6	Red	Icon	1	111	X	Icon	Employee_Port	
Gi3/1	9	GigabitEthernet3/1	Green	Icon	N/A	102	✓	Icon	Employee_Port	
Gi3/2	10	GigabitEthernet3/2	Green	Icon	1	111	X	Icon	Employee_Port	
Gi3/3	11	GigabitEthernet3/3	Green	Icon	1	111	X	Icon	Employee_Port	
Gi3/4	12	GigabitEthernet3/4	Green	Icon	1	104	X	Icon	Default [uncontrolled]	

Configure User Roles

- Step 3** The next step is to configure the user roles and map the appropriate VLANs to these roles. The screenshot in [Figure 54](#) shows the creation of the employee role for the employee clients. The VLANs were already created in the edge access switches that correspond to each role. Additional roles and VLAN can be created for more granular access control if desired.

Figure 54 *Creating Employee Role and Mapping it to VLAN 102*

The screenshot shows the Cisco Clean Access Standard Manager web interface, Version 4.7.2. The left sidebar contains navigation menus for Device Management, OOB Management, User Management (with 'User Roles' selected), Monitoring, and Administration. The main content area is titled 'User Management > User Roles' and has tabs for 'List of Roles', 'New Role', 'Traffic Control', 'Bandwidth', and 'Schedule'. The 'New Role' tab is active, showing a form to create a new role. The form includes fields for Role Name (Employee), Role Description (Employee Role), Role Type (Normal Login Role), and *Max Sessions per User Account (0). It also has checkboxes for 'Disable this role' and 'Case-Insensitive'. A section for 'Retag Trusted-side Egress Traffic with VLAN (In-Band)' has a dropdown for 'VLAN ID' set to 102. Below this are sections for '*Out-of-Band User Role VLAN', '*Bounce Switch Port After Login (OOB)', '*Refresh IP After Login (OOB)', and '*After Successful Login Redirect to'. The 'VLAN ID' dropdown is set to 102, and the 'Bounce Switch Port After Login (OOB)' section has 'Enable' selected. The 'Refresh IP After Login (OOB)' section has 'Enable' selected. The 'After Successful Login Redirect to' section has 'previously requested URL' selected. A vertical timestamp '22:04:39' is visible on the right edge of the interface.

Adding Users and Assign to Appropriate User Role

For user authentication, a local user database can be defined on the NAC Manager. However, in environments where there is a large user base or pre-existing authentication servers, integrating NAC with external authentication servers using RADIUS, LDAP, Kerberos, and so on, is typically preferred. When using external authentication servers, users are mapped to a particular role via RADIUS or LDAP attributes. For information on configuring external authentication servers with NAC, see:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_auth.html.

Customize User Login Page for Web Login

A default login page is already created in the NAC Manager. However, the login page can be customized to change the appearance of the Web portal. For a NAC L3 OOB solution, it is important to download the ActiveX or Java component to the end client. This is done to perform the following:

- Fetch the MAC address of the client machine
- Perform IP address release/renew

Step 1 To do this, Go to **Administration > User Pages**. Edit the page to make sure these options are enabled as shown in [Figure 55](#).

Figure 55 *User Page Settings for Web Login*

The screenshot shows the Cisco Clean Access Standard Manager interface, Version 4.7.2. The left sidebar contains navigation menus for Device Management, OOB Management, User Management, Monitoring, and Administration. The main content area is titled 'Administration > User Pages'. It features three tabs: 'Login Page', 'File Upload', and 'Guest Registration Page'. The 'Login Page' tab is active, showing a 'General' sub-tab. The configuration includes a checkbox to 'Enable this login page', fields for 'VLAN ID' and 'Subnet (IP/Mask)', a dropdown for 'Operating System' (set to 'ALL'), a dropdown for 'Page Type' (set to 'Frameless'), and a text field for 'Page Description'. The 'Web Client (ActiveX/Applet)' is set to 'ActiveX on IE, Java Applet on non-IE Browser'. There are three checkboxes: 'Use web client to detect client MAC address and Operating System.', 'Use web client to release and renew IP address when necessary (OOB).', and 'Install DHCP Refresh tool into Linux/MacOS system directory.' The 'Update', 'Cancel', and 'View' buttons are at the bottom right.

Customize the Agent for the User Roles

The NAC Manager can be configured to make the Agent mandatory for any user role. The agent should be made mandatory for any role that you want to perform posture assessment prior to granting them access to the network. In the example in Figure 56, the NAC Agent is made mandatory for the employee role.

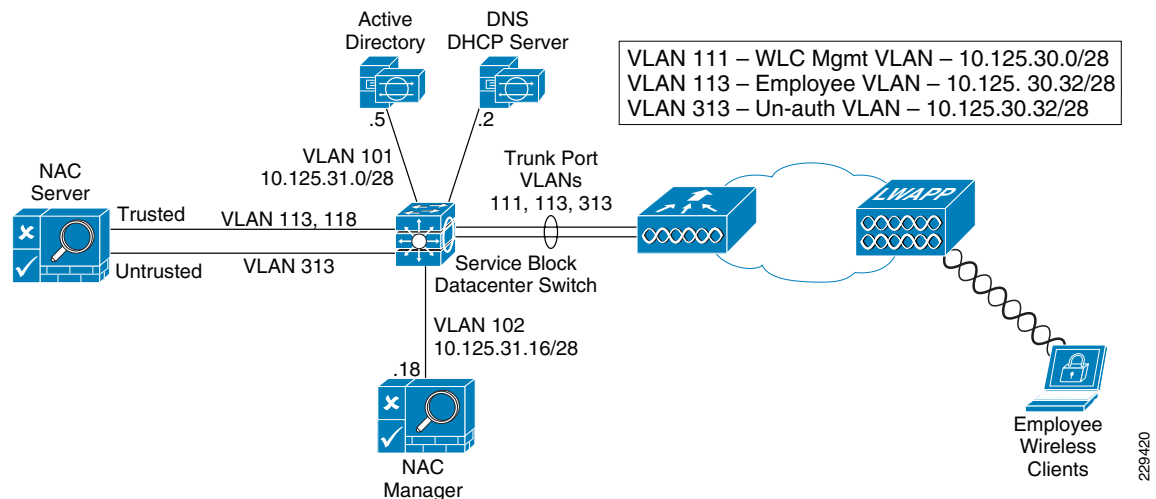
Figure 56 *Agent Login Required for Employee Role*

The screenshot shows the Cisco Clean Access Standard Manager interface, Version 4.7.2. The left sidebar is the same as in Figure 55. The main content area is titled 'Device Management > Clean Access'. It features four tabs: 'Certified Devices', 'General Setup', 'Network Scanner', and 'Clean Access Agent'. The 'Clean Access Agent' tab is active, showing a 'Web Login' sub-tab. The configuration includes a dropdown for 'User Role' (set to 'Employee') and a dropdown for 'Operating System' (set to 'ALL'). There are two checkboxes: 'Require use of Agent (for Windows & Macintosh OSX only)' and 'Require use of Cisco NAC Web Agent (for Windows 7/2000/XP/Vista only)'. Both checkboxes are checked. Below each checkbox is a text field for the 'Agent Download Page Message (or URL)' and the 'Cisco NAC Web Agent Launch Page Message (or URL)'. The messages are: 'Network Security Notice: This network is protected by a Cisco NAC Appliance Agent, a component of the Cisco NAC Appliance Suite. The Agent ensures that your computer' and 'Network Security Notice: This network is protected by the Cisco NAC Web Agent, a component of the Cisco NAC Appliance Suite. The Cisco NAC Web Agent ensures that your'.

NAC Deployment for Wireless Clients

Within the medium enterprise network security design, a NAC Layer 2 OOB deployment was used for wireless clients. Figure 57 shows the L2 OOB logical network diagram that was used to validate the NAC L2 OOB deployment in the Medium Enterprise Design Profile. Figure 57 shows the specifics for the employee wireless clients.

Figure 57 Layer 2 OOB NAC Deployment Topology for Employee Wireless Clients



As illustrated in Figure 57, the WLC is connected to a trunk port that carries the quarantine VLAN and access VLAN for the employee clients (VLANs 113 and 313). On the switch, the quarantine VLAN traffic is trunked to the NAC appliance, and the access VLAN traffic is trunked directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to access the VLAN based on static mapping configuration. When the client associates and completes the L2 Auth, it checks whether the quarantine interface is associated; if yes, the data is sent on the quarantine interface. The client traffic that flows in the quarantine VLAN is trunked to the NAC appliance. After posture validation is done, the NAC server (CAS) sends an SNMP set message that updates the access VLAN ID to the controller, and the data traffic starts to switch from the WLC directly to the network without going through the NAC server.

The following subsections illustrate the configurations needed for deploying L2 OOB NAC for the Employee clients. Similar steps would be taken to enable NAC for additional clients/roles as needed.

Cisco Catalyst Switch Configuration

The following Cisco Catalyst 3750E configuration example illustrates the configurations used on the service block switch in the medium enterprise network for the NAC wireless deployment.

```
interface GigabitEthernet2/0/9
description Connected to cr25-nac-mgr-1
switchport access vlan 102
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet2/0/19
description NAC Server trusted interface - Ethernet 0
switchport trunk encapsulation dot1q
switchport trunk native vlan 802
switchport trunk allowed vlan 113,118
switchport mode trunk
```

```

!
interface GigabitEthernet2/0/20
description NAC Server untrusted interface - ethernet 1
switchport trunk encapsulation dot1q
switchport trunk native vlan 803
switchport trunk allowed vlan 313
switchport mode trunk
!
interface Port-channel11
description Connection to WLC cr23-5508-1
switchport trunk encapsulation dot1q
switchport trunk native vlan 801
switchport trunk allowed vlan 111,113,313
switchport mode trunk
switchport nonegotiate
!
interface Vlan111
description WLC Management VLAN
ip address 10.125.30.1 255.255.255.240
!
interface Vlan113
description Employee Client Subnet Access VLAN
ip address 10.125.30.33 255.255.255.240
!

```

NAC OOB Configuration Steps on the WLC and NAC Manager

The following outlines the steps needed to configure the WLC and the NAC Manager for a NAC L2 OOB deployment:

- Step 1** Enable SNMPv2 mode on the controller. See [Figure 58](#).

Figure 58 Enabling SNMPv2

The screenshot shows the Cisco WLC Management GUI. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu on the left lists various management sections: Summary, SNMP (General, SNMP V3 Users, Communities, Trap Receivers, Trap Controls, Trap Logs), HTTP, Telnet-SSH, Serial Port, Local Management Users, User Sessions, Logs, Mgmt Via Wireless, Software Activation, and Tech Support. The right pane displays the 'SNMP System Summary' configuration page. It includes fields for Name (cr23-5508-1), Location, and Contact. The System Description is set to 'Cisco Controller' and the System Object ID is '1.3.6.1.4.1.9.1.1069'. The SNMP Port Number is 161 and the Trap Port Number is 162. The SNMP v1 Mode is set to 'Disable', the SNMP v2c Mode is set to 'Enable', and the SNMP v3 Mode is set to 'Disable'. An 'Apply' button is located at the top right of the configuration pane.

- Step 2** Create a profile for WLC on the NAC Manager. Click **OOB Management Profile > Device > New** from within the NAC Manager GUI. See [Figure 59](#).

Figure 59 **Creating Profile for WLC**

Cisco Clean Access Standard Manager Version 4.7.2

OOB Management > Profiles

Group Device Port VLAN SNMP Receiver

List · New · Edit

(These settings must match the device setup to ensure that the Clean Access Manager can read/write to the device correctly)

Profile Name: WLC_Main_Site

Device Model: Cisco Wireless LAN Controllers

SNMP Port: 161

Description: Main Site WLC

SNMP Read Settings

SNMP Version: SNMP V2C

Community String: cisco123

SNMP Write Settings

SNMP Version: SNMP V2C

Community String: enterprise

Update Reset

229441

Step 3 After the profile is created in the NAC Manager, add the WLC in the profile; go to **OOB Management > Devices > New** and enter the management IP address of WLC. See [Figure 60](#).

Figure 60 **Adding WLC in Profile**

Cisco Clean Access Standard Manager Version 4.7.2

OOB Management > Devices

Devices Discovered Clients

List · New · Search

Device Profile: WLC_Main_Site

Device Group: default

IP Addresses: 10.125.30.2

Description: WLC 1 at Main Site

Add Reset

229442

Step 4 Add the NAC Manager as the SNMP trap receiver in the WLC. Use the exact name of the trap receiver in the NAC Manager as the SNMP receiver. (See [Figure 61](#).)

Figure 61 Adding MAC Manager as the SNMP Trap Receiver

The screenshot shows the Cisco WLC Management interface. The left sidebar has a 'Management' section with a 'Summary' link. The main content area is titled 'SNMP Trap Receiver > New'. It contains three input fields: 'Community Name' with the value 'NacTraps', 'IP Address' with the value '10.125.31.18', and 'Status' with a dropdown menu set to 'Enable'. There are '< Back' and 'Apply' buttons at the top right. The top navigation bar includes links for 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The top right corner has links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'.

- Step 5** Configure the SNMP trap receiver in the NAC Manager with the same name that was specified in the WLC controller; click **OOB Management > Profiles > SNMP Receiver**. (See [Figure 62](#).)

Figure 62 Configure the SNMP Trap Receiver in the NAC Manager

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar has a 'Device Management' section with links for 'CCA Servers', 'Filters', and 'Clean Access'. The main content area is titled 'OOB Management > Profiles'. It has a tabbed interface with 'SNMP Trap' selected. The 'Advanced Settings' section contains the following fields: 'Trap Port on Clean Access Manager' (162), 'SNMP V1 Settings' (Community String), 'SNMP V2c Settings' (Community String: NacTraps), and 'SNMP V3 Settings' (Security Method: No Auth, No Priv; User Name, User Auth, User Priv). There is an 'Update' button at the bottom right. The top navigation bar includes links for 'Device Management', 'OOB Management', 'User Management', 'Monitoring', and 'Administration'. The top right corner has a 'Version 4.7.2' label.

At this stage, the WLC and the NAC Manager can talk to each other for client posture validation and access/quarantine state updates.

- Step 6** In the controller, create a dynamic interface with access and quarantine VLAN mapped to it. (See [Figure 63](#).)

Figure 63 *Creating Dynamic Interface in the Controller*

The screenshot shows the Cisco WLC Controller configuration page for a dynamic interface. The left sidebar lists various configuration categories, with 'Advanced' selected. The main content area is divided into several sections:

- General Information:** Interface Name: staff data, MAC Address: 00:24:97:cf:3f:af.
- Configuration:** Guest Lan: ☐, Quarantine: ☒, Quarantine Vlan Id: 313.
- Physical Information:** The interface is attached to a LAG. Enable Dynamic AP Management: ☐.
- Interface Address:** VLAN Identifier: 113, IP Address: 10.125.30.34, Netmask: 255.255.255.240, Gateway: 10.125.30.33.
- DHCP Information:** Primary DHCP Server: 10.125.31.2.

Step 7 Create the WLAN and associate it with the dynamic interface. (See [Figure 64](#).)

Figure 64 *Creating the WLAN*

The screenshot shows the Cisco WLC Controller configuration page for a new WLAN. The left sidebar lists various configuration categories, with 'Advanced' selected. The main content area is divided into several sections:

- General:** Profile Name: Staff Data, Type: WLAN, SSID: data, Status: ☒ Enabled.
- Security Policies:** [WPA2][Auth(802.1X + CCKM)] (Modifications done under security tab will appear after applying the changes.)
- Radio Policy:** All (dropdown).
- Interface:** staff data (dropdown).
- Broadcast SSID:** ☒ Enabled.

Step 8 Enable NAC in the WLAN on the WLC Controller. (See [Figure 65](#).)

Figure 65 Enabling NAC in the WLAN on the WLC Controller

The screenshot shows the Cisco WLC Controller configuration page for WLANs. The 'Advanced' tab is selected, and the 'NAC' section is expanded. The 'State' checkbox is checked, indicating NAC is enabled. Other settings visible include 'Allow AAA Override' (unchecked), 'Coverage Hole Detection' (checked), 'Enable Session Timeout' (checked, 1800 seconds), 'Aironet IE' (checked), 'Diagnostic Channel' (unchecked), 'IPv6 Enable' (unchecked), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Client Exclusion' (checked, 60 seconds), 'Media Session Snooping' (unchecked), 'DHCP Server' (unchecked), 'DHCP Addr. Assignment' (unchecked), 'Management Frame Protection (MFP)' (Infrastructure MFP Protection checked, MFP Client Protection set to Optional), and 'DTIM Period (in beacon intervals)' (802.11a/n: 1, 802.11b/g/n: 1). The 'Off Channel Scanning Defer' and 'Load Balancing and Band Select' sections are also visible.

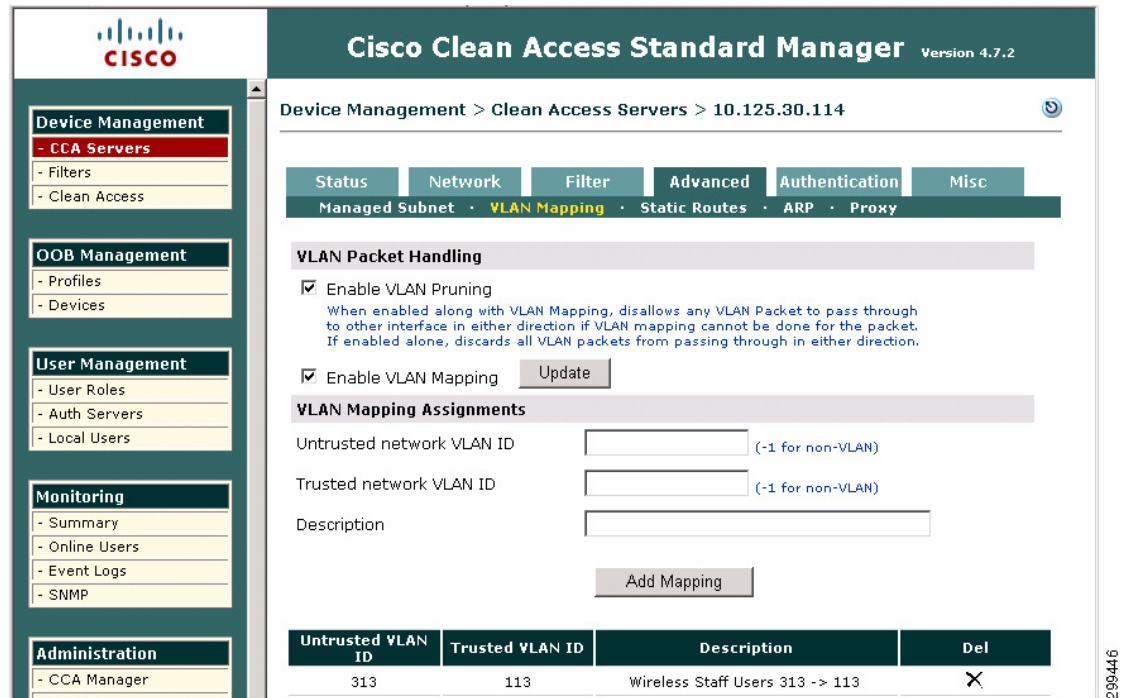
- Step 9** Add the client subnet in the CAS server as the managed subnet by clicking **CAS server > Select your CAS server > Manage > Advanced > Managed Subnets**. Add an unused IP address from the client subnet and put the quarantine VLAN (untrusted VLAN) for the managed subnet. (See [Figure 66](#).)

Figure 66 Adding the Client Subnet in the CAS Server

The screenshot shows the Cisco Clean Access Standard Manager configuration page for Managed Subnets. The 'Advanced' tab is selected, and the 'Managed Subnet' section is expanded. The 'Enable subnet-based VLAN retag' checkbox is unchecked. The 'Update' button is visible. The 'IP Address' field is set to 10.125.30.36, the 'Subnet Mask' field is set to 255.255.255.240, the 'VLAN ID' field is set to 313 (with a note: (-1 for non-VLAN)), and the 'Description' field is set to Staff Wireless Subnet (PEAP). The 'Add Managed Subnet' button is visible at the bottom.

- Step 10** Create VLAN mappings on the CAS. Click **CAS server > Select your CAS server > Manage > Advanced > VLAN Mapping**. Add the access VLAN as trusted and the quarantine VLAN as untrusted. (See [Figure 67](#).)

Figure 67 **Creating VLAN Mappings**



Configuring Single SignOn (SSO) with the OOB Wireless Solution

The following is required to enable VPN SSO for a wireless NAC OOB deployment:

- Enable VPN authentication on the NAC server with the WLC defined as the VPN concentrator in the NAC appliance.
- Enable RADIUS accounting on the WLC controller. The WLC that is defined in the NAC appliance must be configured to send RADIUS accounting records to the NAC appliance for each 802.1x/EAP WLAN that is a managed subnet in the NAC.

The following steps outline the needed configuration on the NAC Manager to enable SSO.

- Step 11** From the NAC Manager GUI, click **CAS server > Select your CAS server > Manage > Authentication > VPN Auth.** (See [Figure 68.](#))

Figure 68 NAC Manager Configuration—Enabling SSO

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar contains navigation menus for Device Management, OOB Management, User Management, and Monitoring. The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and shows the configuration for 'Clean Access Servers > 10.125.30.114'. The 'Authentication' tab is selected, showing options for Single Sign-On (checked), Agent VPN Detection Delay (0 seconds), Auto Logout (checked), and RADIUS Accounting Port (1813). An 'Update' button is at the bottom.

- Step 12** Select the **VPN Concentrators** tab to add a new entry for the WLC. Populate the entry fields for the WLC Management IP address and shared secret you want to use between the WLC and NAC server. (See [Figure 69](#).)

Figure 69 Adding New Entry for WLC

The screenshot shows the Cisco Clean Access Standard Manager interface. The left sidebar is the same as in Figure 68. The main content area is titled 'Cisco Clean Access Standard Manager Version 4.7.2' and shows the configuration for 'Clean Access Servers > 10.125.30.114'. The 'VPN Concentrators' tab is selected. The form includes fields for Name, IP Address, Shared Secret, Confirm Shared Secret, and Description. An 'Add VPN Concentrator' button is below the fields. A table at the bottom lists the configured VPN Concentrators.

VPN Concentrator	IP Address	Description	Del
cr23-5508	10.125.30.2	WLC-1 at Main Site	X

- Step 13** For role mapping, add the new authentication server with type **vpn sso** under **User Management > Auth Servers**. (See [Figure 70](#).)

Figure 70 Adding New Authentication Server for Role Mapping

Cisco Clean Access Standard Manager Version 4.7.2

User Management > Auth Servers

Auth Servers | Lookup Servers | Mapping Rules | Auth Test | Accounting

Authentication Cache Timeout (seconds): 120

Provider Name	Authentication Type	Description	Mapping	Edit	Delete
Local DB	local	Cisco local authentication			
Cisco VPN	vpn sso	Single Sign-on			

- Step 14** Click the **Mapping** icon and then add **Mapping Rule**. The mapping varies depending on the class attribute 25 value that WLC sends in the accounting packet. This attribute value is configured in the RADIUS server and varies based on the user authorization. In this example, the attribute value is *employee*, and it is placed in the Wireless_Employee role. (See [Figure 71](#).)

Figure 71 Mapping Class Attribute From WLC to User Roles

Cisco Clean Access Standard Manager Version 4.7.2

User Management -> Auth Servers

Auth Servers | Lookup Servers | Mapping Rules | Auth Test | Accounting

Configure one or more conditions first using the Add/Save Condition form, then add or save the mapping rule to the selected Role using the Add/Save Mapping form. Note that if the mapping is not added or saved, conditions are not preserved.

Provider Name: Cisco VPN Priority: 1

Role Name: Wireless_Employee Description: Wireless Employee mapping

Rule Expression: (0,25 equals employee)

Condition Type: VLAN ID Operator: equals

Property Name: VLAN ID Property Value:

VLAN IDs may not be available for mapping if there are multiple hops between the CAS and the VPN concentrator.

#	Type	Left Operand	Operator	Right Operand	Edit	Del
1	Attribute	0,25	equals	employee		

- Step 15** To configure VPN SSO on the Wireless LAN Controller, RADIUS accounting needs to be enabled and sent to the NAC Server. (See [Figure 72](#).)

Figure 72 *Enabling RADIUS Accounting for VPN SSO*

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1	IP:10.125.31.66, Port:1812	Server 1	IP:10.125.30.114, Port:1813
Server 2	None	Server 2	None
Server 3	None	Server 3	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☐ Enabled

Authentication priority order for web-auth user

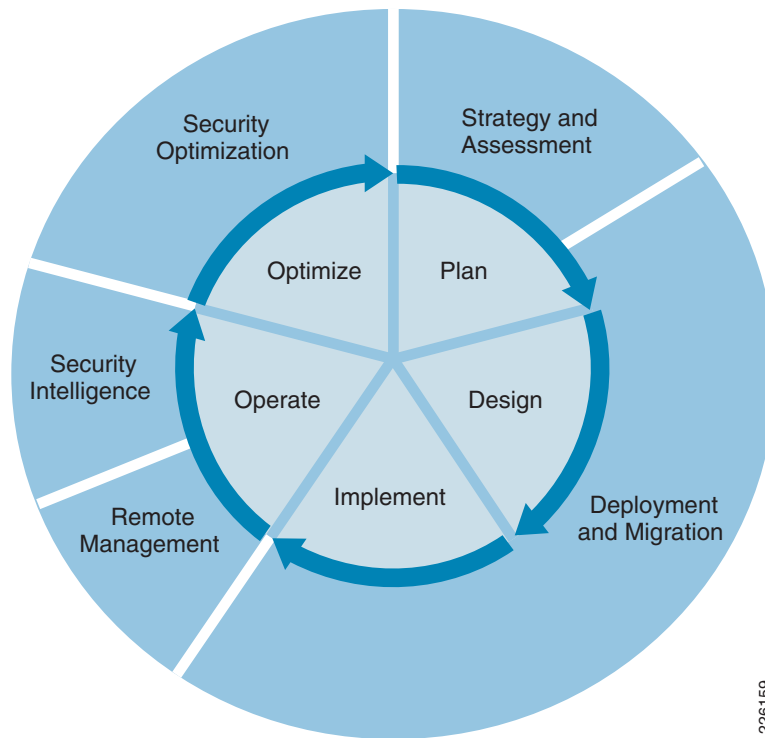
Not Used Order Used For Authentication

**Note**

When deploying a wireless NAC solution that requires single sign-on for some WLANs and non-single sign-on for other WLANs, RADIUS accounting must be disabled for the WLANs not requiring SSO. Otherwise, NAC mistakenly authenticates the non-single sign-on clients without prompting them.

Cisco Security Services

The Cisco SAFE Security Architecture is complemented by Cisco's rich portfolio of security services designed to support the entire solution lifecycle. Security is integrated everywhere, and with the help of a lifecycle services approach, enterprises can deploy, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls. [Figure 73](#) shows how the Cisco Lifecycle Security Services support the entire lifecycle.

Figure 73 Cisco Lifecycle Security Services

226159

Strategy and Assessments

Cisco offers a comprehensive set of assessment services based on a structured IT governance, risk management, and compliance approach to information security. These services help the customer understand the needs and gaps, recommend remediation based on industry and international best practices, and help the customer to strategically plan the evolution of an information security program, including updates to security policy, processes, and technology.

Deployment and Migration

Cisco offers deployment services to support the customer in planning, designing, and implementing Cisco security products and solutions. In addition, Cisco has services to support the customer in evolving its security policy and process-based controls to make people and the security architecture more effective.

Remote Management

Cisco Remote Management services engineers become an extension of the customer's IT staff, proactively monitoring the security technology infrastructure and providing incident, problem, change, configuration, and release management as well as management reporting 24 hours a day, 365 days a year.

Security Intelligence

The Cisco Security Intelligence services provide early warning intelligence, analysis, and proven mitigation techniques to help security professionals respond to the latest threats. The customer's IT staff can use the latest threat alerts, vulnerability analysis, and applied mitigation techniques developed by Cisco experts who use in-depth knowledge and sophisticated tools to verify anomalies and develop techniques that help ensure timely, accurate, and quick resolution to potential vulnerabilities and attacks.

Security Optimization

The Cisco security optimization service is an integrated service offering designed to assess, develop, and optimize the customer's security infrastructure on an ongoing basis. Through quarterly site visits and continual analysis and tuning, the Cisco security team becomes an extension of the customer's security staff, supporting them in long-term business security and risk management, as well as near-term tactical solutions to evolving security threats.