

Cisco Powered Network Managed Security Services Designation



Overview

Network security is a primary concern for many enterprise organizations. Most of these organizations want to implement security throughout their corporate network but do not know how or where to begin. Additionally, these businesses might not have the resources to invest in security equipment, maintenance services, and training to build their own in-house expertise. As a result, enterprise organizations must rely on Internet service providers (ISPs) to deploy and manage their security equipment for them to mitigate network security threats such as malicious computer “worms” and viruses, and denial-of-service (DOS) incidents.

At the same time, ISPs regularly seek to add value to their service offerings in order to differentiate themselves from their competitors and generate revenue with new add-on services. The Cisco Powered Network Managed Security Services designation enables ISPs to market these security services through their network infrastructure and securely scale additional customer premises equipment (CPE) products.

Eligibility

To be eligible for the Managed Security Services designation, service providers must already have the Cisco Powered Network designation and must fulfill the following requirements.

1. Offer the following services, based on Cisco solutions:

Traffic filtering, rate limiting and bandwidth optimization at the perimeter of the public/private networks and at least one of the following:

- Managed firewall for inbound/outbound traffic
 - Managed intrusion detection systems (IDSs) deployed on the network perimeter on either side of the firewall or internally near or on critical corporate hosts
 - Managed customer premises-based virtual private networks (VPNs) using the industry standard: IP Security (IPSec)
2. Participate once annually in Cisco Security training.
 - This four-day training is provided at the Cisco facility in Austin, Texas, and is free to Cisco Powered Network partners. To register, go to: <http://www.regweb.com/intro.cfm?regwebID=1392>.

Traffic Filtering, Bandwidth Optimization, and Rate-Limiting Services

There are three components to this area: RFC1918 address filtering, RFC2827 address filtering, and rate limiting, or bandwidth optimization, of unexpected traffic.



The filtering of private addresses defined in RFC1918 should be part of any ISP's policy. Because these addresses are to be used only within enterprise networks, enterprises should translate these source addresses before the traffic reaches the ISP. The destination addresses must be blocked from penetrating the ISP network. In fact, part of the ISP's obligation as owner of an Autonomous System (AS), should be to not route any 1918 addresses nor send them in any routing updates.

RFC 2827 filtering mitigates the use of enterprise networks as launching points for security breaches of other networks. The practices in this RFC are designed to mitigate DOS attacks and better protect enterprise networks. At the ingress point of the ISP network, any traffic with a source address that is not part of the organization's public address space is filtered out. Although this filtering does not protect an organization's network performance, it discourages potential hackers from using the network for malicious activity and protects the organization from legal issues if its network is used as a launching point for attack.

Bandwidth optimization or rate limiting, through mechanisms such as Committed Access Rate (CAR), controls traffic either at the ingress and egress points of the ISP network, reducing DOS and distributed DOS (DDOS) attacks. DOS attacks either overload the access bandwidth between the ISP and the enterprise or overload a network resource with unwanted service requests, "starving" the resources available for legitimate traffic. Internet Message Control Protocol (ICMP) traffic is a common way to overload bandwidth because many, if not all, network devices reply to these requests. TCP SYN requests are a common way of occupying and overloading valuable public servers with unwanted session opening requests. An ISP should measure the baseline of this type of undesired traffic. After adding 50 percent for peak values, the ISP will have the parameters required to configure the rate limiting that should be configured at both points of the perimeter.

What are the criteria for supporting this service?

Service providers should deploy and manage Cisco network edge routers such as Cisco 2600, 3600, or 7000 Series routers. The customer-facing network interfaces within these routers must be configured with the appropriate access control lists (ACLs) and must enable rate limiting three types of traffic, as determined by customer requirements.

Managed Firewall Services

Firewalls typically provide three types of traffic management. The primary capability is filtering and translating inbound return traffic from sessions that were initiated by outbound traffic from a corporate network to the Internet. This typically means specifying which outbound traffic is authorized and letting the firewall use its dynamic state-machine to translate the outbound traffic and recognize the corresponding inbound return traffic.

The second type of traffic management involves setting up conduits or ACLs for certain types of inbound traffic, which are typically destined for public servers accessible from the Internet. Because these sessions are initiated by inbound traffic, the dynamic nature of the firewall does not come into action. If the inbound traffic is not return traffic but matches the conduit specification, then it is allowed to travel to the specific interface (usually to a demilitarized zone [DMZ]). Otherwise, the inbound traffic is dropped.

The third type of firewall traffic management is defined by general attack mitigation features that protect an organization's network. Typically, this traffic is detected by the public interface of the firewall and blocked from further penetration. In most scenarios these attacks are logged so the network administrator can review them in real time, or in the future, and take appropriate action.

The features described in this section can be remotely managed on a firewall. As part of this service, the ISP must maintain a customer profile or specification and ensure that the firewall configuration is kept updated. Part of the service might include monthly reports of the various types of traffic and a summary of the intrusions and events logged.



What are the criteria for supporting this managed service?

In addition to the criteria specified for traffic filtering, the service provider must deploy and manage Cisco PIX[®] Firewalls along with Cisco IOS[®] routers that support the firewall feature set. The service provider must offer the following services as a minimum:

- Configuration change management that can be scheduled to a date and time, including updating the PIX operating system (OS) and restoring previous firewall configurations
- Fault and performance management with trouble-ticket or incident tracking
- Traffic flow information for each physical interface on the firewall summarized by protocol, time-of-day and IP address
- The ability to manage multiple firewalls for one customer in a seamless fashion and preferably by policy
- A secure, authenticated method for remote management of the firewalls

Managed Intrusion Detection System Services

Intrusion detection systems (IDSs) can be installed on almost any LAN segment of a corporate network to passively monitor traffic, because network-based attacks can come from both external and internal sources.

Additionally, host-based IDS solutions protect valuable application servers and hosts running in the corporate infrastructure. Host-based IDS solutions offer intrusion prevention services and fortify Web and application servers from malevolent viruses and worms that typically attack such hosts.

The most common placement for host-based IDS solutions is on the critical hosts themselves. Valuable Windows and UNIX hosts running Web, e-mail, and database services can also run the system-saving host IDS application for advanced protection. These host-based intrusion prevention systems complement the network-based IDS appliances that might also be deployed throughout the network.

The most common placement for an IDS appliance or “sensor” is near one or more public servers within the DMZ of the network. Most external attacks are directed to vulnerabilities associated with public servers including DOS and buffer overflow attacks. Other common placements of IDS sensors include surrounding the perimeter firewall, monitoring “trusted” extranet and remote access connections, and protecting mission-critical internal assets (that is, internal servers) from attack.

Placed “around” a firewall, the IDS sensor monitors traffic passing through the firewall (in both directions) looking for malicious activity within the “permitted” traffic (for example, cgi-bin attacks launched against Web servers over HTTP, attacks against mail servers over SMTP, and so on). The sensor also monitors for general “reconnaissance” activity (for example, ping sweeps, port sweeps), indicative of the early stages of a network attack. The complementary nature of the IDS technology provides constant verification that the traditional network perimeter defenses that are enabled through firewalls have been correctly implemented and are operating correctly (for example, configuration errors are not uncommon). In addition, IDS sensors help to check for intrusions launched by trusted or internal network sources, which comprise a large majority of security breaches.

What are the criteria for supporting this managed service?

In addition to the criteria specified for traffic filtering, service providers must deploy and manage at least one of the IDS appliances provided within the product line. The Host IDS solution within the Cisco IDS product line can also be managed and supported within the service as well. Service providers have several options:

- Use commercially available management applications to monitor and configure IDS sensors and host IDS software
- Use the Cisco IDS Software Development Kit (SDK) to integrate data from Cisco IDS devices into its own network operations center (NOC) infrastructure management tools



- Evaluate third-party partner solutions, such as netForensics or NetSolve, to conduct large-scale IDS management
- Decide whether to manage the IDS devices and host-based IDS software, as well as managing the data coming from these devices (both models work, although the latter is more important in providing secure network services)

Managed CPE-Based VPN Services

VPNs offer secure connectivity between multiple business locations, as well as between remote users and business locations. IPSec is the industry standard used to efficiently provide data authentication and privacy within these VPN communications. This is particularly important when telecommunications traverse an IP backbone within the public Internet. Customers who want secure end-to-end connectivity require the secure connections to be terminated at the customer premises. CPE-based VPNs ensure secure intranet, extranet, and remote access, end-to-end connectivity.

Site-to-site and remote access VPNs can be deployed and supported on Cisco IOS Router platforms, Cisco PIX Firewalls, and Cisco VPN 3000 and 5000 Series Concentrators. The Cisco VPN Client used in these VPN offerings must be based on, and conform to, the Cisco unified client specification. Cisco VPN Client versions 3.0 and above conform to this specification.

In support of this managed CPE-based VPN service, service providers must deploy and manage at least one of the following solutions:

- Cisco IOS Routers with the IPSec VPN feature set enabled for site-to-site or remote access VPNs
- Cisco PIX Firewalls for site-to-site or remote access VPNs
- Cisco VPN 3000 Series Concentrators for site-to-site or remote access VPNs
- Cisco VPN 5000 Series Concentrators for site-to-site or remote access VPNs

In addition to the criteria above, service providers must offer the following services at a minimum:

- Configuration change management that can be scheduled to a date and time, including updating the VPN platform operating system (OS) and restoring previous VPN configurations
- Fault and performance management with trouble-ticket or incident tracking
- Traffic flow information for each physical interface on the VPN
- Ability to manage multiple VPN devices and for multiple types of VPN devices (for example Cisco PIX Firewalls, Cisco routers, and Cisco VPN 3000 Series Concentrators) for one customer in a seamless fashion
- A secure, authenticated method for remote management of one or more VPN platforms
- Support for timely and effective VPN client software distribution and updates

Required Training

Free of charge to Cisco Powered Network partners, network security training increases awareness of Cisco security and VPN solutions and keeps service providers current on the latest products and feature updates. As a result, service providers are in a better position to understand and leverage Cisco enterprise security solutions.

Cisco security training comprises four days of intensive, hands-on network security training. Participants receive an introduction to security, hacking, the SAFE network security blueprint, and a complete day each of Cisco PIX Firewall, Cisco VPN 3000 Concentrator, and Cisco Intrusion Detection System labs.

Security training must be attended by at least two security-focused personnel within three months of receiving the Cisco Powered Network Managed Security Services designation. This course must then be attended annually by at least two individuals within the service provider support organization in order to stay current on Cisco security and VPN technologies. Training is provided at no cost at the Cisco facility in Austin, Texas.



Benefits to Service Providers Offering Managed Security Services with the Cisco Powered Network Program

- Participants offering managed security services within the Cisco Powered Network program are the recommended service providers for securely supporting Cisco enterprise customers. Cisco sales teams will refer enterprise customers to qualified Cisco Powered Network members when customers prefer a managed security service solution. This reference model extends to Cisco reseller partners, VARs, and system integrators.

- Free Cisco Powered Network Security Posture Assessment (SPA)

http://www.cisco.com/cgi-bin/cpn/show_page.pl?file_name=security_process_assesment.html&type=

The Cisco Powered Network (SPA) is provided as a technical benefit to Cisco Powered Network members at no cost. By providing a security-oriented “snapshot in time” and by taking the unique perspective of quantifying the current level of network security, SPA services can help organizations effectively and objectively understand network security states and identify areas to improve.

- Free Cisco security training: <http://www.regweb.com/intro.cfm?regwebID=1392>.
- Network Operations Symposium—As a member of the Cisco Powered Network program, your technical managers are invited each year to a technical symposium where they learn about the world's most advanced networking technologies from industry experts and Cisco training partners. The next symposium scheduled for March 18-22, 2002. http://www.cisco.com/cgi-bin/cpn/show_page.pl?file_name=network_operations.html&type=
- Inclusion in Cisco collateral material directed to enterprise customers

- Promotion through Customer Case Studies. Write-ups promoting (1) the value of your secure network to your end customers; (2) how you have applied Cisco technology successfully to meet your business needs.
- Coverage in Packet™ Magazine, mailed quarterly to 85,000 Cisco customers globally.
- Inclusion in Cisco field announcements
- Promotion through co-authored technical white papers.
- Participation in Cisco product and service launches.
- Web seminars that are broadcast to Cisco enterprise customers.
- Participation in Cisco Security and VPN seminars.

**Disclaimer—The benefits listed are representative in nature and should not be construed as actual benefits delivered. Actual incentives extended will vary on a per-customer basis.*

For More Information

The Cisco Managed Security Services initiative offers exceptional value to both ISPs seeking to expand their service offerings and enterprise customers seeking assistance in securing their networks for e-business. Cisco provides two programs that support this initiative: the Cisco Powered Network Managed Security Services designation, and the services solutions offered within the Cisco AVVID (Architecture for Voice, Video and Integrated Data) Partner Program: Security and VPN Solutions set.

For more details on these programs, refer to the following information online:

- Cisco Powered Networks—Managed Security Services www.cisco.com/go/cpn
- Cisco AVVID Partner Program—Security and VPN Solutions www.cisco.com/go/securitypartners



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, Cisco Unity, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

DA 11/01