Q&A

Securing the Wiring Closet with Cisco Catalyst Switches

Q. Why should I deploy network security in the wiring closet?

A. Until very recently, network security in the wiring closet was often limited merely to physical security. With the advent of increasingly sophisticated attacks and new worms and viruses that spread in a matter of minutes, those policies need to change. Because most internal security attacks are launched from the wiring closet, its LAN infrastructure presents a critical first line of defense against security attacks in an enterprise LAN.

Q. I have a firewall between my network and the rest of the world. Isn't that sufficient?

A. As many enterprises are discovering, the answer is no. Today's worms and viruses are typically brought into the network unsuspectingly by mobile PCs bypassing the firewalls. Furthermore, a 2005 CSI/FBI, USA based survey reports that majority of security attacks are launched from the inside of the network.

Q. What are the most common types of security threats facing enterprises?

A. According to the 2005 CSI/FBI survey, virus and worms are the most common threats to an enterprise, followed by unauthorized access, theft of data, and denial of service (DoS). Based on 639 respondents, the total cost to their businesses due to these attacks was approximately US$112 million.

Q. What kind of security attacks can be launched from the wiring closet?

A. The most common attacks that are launched from the wiring closet fit in two main categories:

- **Denial of Service attacks**—Can interrupt the entire Enterprise network. DoS attacks can be maliciously launched or unknowingly introduced in to the network by an infected PC
- **Man in the middle attacks**—Allow a hacker to snoop and intercept LAN traffic, compromising network privacy.

Q. How can I prevent these types of security threats?

A. The Cisco® Self-Defending Network strategy employs a comprehensive Cisco Systems® vision for end-to-end security across the entire enterprise. Integrated security features in the Cisco Catalyst® switches are essential to the self-defending network. Cisco Catalyst switches provide the first line of defense in the wiring closet to effectively mitigate these threats.

Q. How does a DoS attack work?

A. With a DoS attack, a program, either on an unauthorized device that has gained access to the network or on a legitimate device that has been infected, floods the network. This flooding generates so much traffic that important devices, such as gateways, are quickly overloaded and unable to respond to legitimate requests, resulting in a network outage. A new and more detrimental form of this attack is a distributed-denial-of-service (DDoS) attack. With a DDoS, attacks are launched simultaneously from multiple devices on the network.

Q. How can Cisco Catalyst switches help prevent DoS attacks?

A. The first line of defense against DoS attacks is to ensure that malicious users cannot gain access to the network and that devices that are permitted access to the network conform to corporate security policies. Cisco Identity-Based Networking Services (IBNS) and Network Admission Control (NAC) provide these capabilities. Both these features can be enabled on Cisco Catalyst switches in the wiring closet to help prevent DoS threats from occurring.

Q. What is Cisco Identity-Based Networking Services?

A. Cisco Identity-Based Networking Services (IBNS) is a technology solution that can improve the security of physical and logical LAN access. Cisco IBNS incorporates all of the capabilities defined in 802.1x while providing enhancements and extensions for improving identity-based access control and for making 802.1x technology easier to deploy.

Cisco IBNS lets you implement identity-based network access control and policy enforcement at the port level. It provides user or device identification and authentication. This solution associates the identity of authenticated network clients with policies that you create and administer and that provide increased granularity of control. By providing flexible port-based access control and policy-enforcement capabilities at the network edge, Cisco IBNS delivers a powerful tool for securing your network.

Q. What is Cisco Network Admission Control?

A. As employees connect to the Internet or office from outside the corporate network, their devices become the unwitting carriers of network viruses and worms. Cisco Network Admission Control (NAC) is an industry wide collaboration led by Cisco, which focuses on limiting the damage of these security threats. Using NAC and Cisco Catalyst switches, administrators can restrict network access to only compliant and trusted endpoint devices (such as PCs, servers, and personal digital assistants [PDAs]). NAC enables Cisco switches to enforce access privileges when an endpoint device attempts to connect to a network. This decision can be based on information about the endpoint device such as its current antivirus state and OS patch level. NAC allows administrators to manage noncompliant devices in several ways: they can be denied access, placed in a quarantined area, or given restricted access to computing resources.

NAC is part of the Cisco Self-Defending Network, a strategy to dramatically improve the network's ability to automatically identify, prevent, and adapt to security threats.

Q. Why is NAC important?

A. Day-zero virus and worm invasions continue to disrupt business, causing downtime and requiring continual patching. NAC helps organizations to reduce this risk by preventing vulnerable hosts from obtaining and retaining normal network access. NAC ensures that all hosts comply with the latest corporate antivirus, security software, and OS patch policies prior to obtaining normal network access. Vulnerable and noncompliant hosts may be isolated and given reduced network access until they are patched and secured, thus preventing them from being the targets of—or the sources for—worm and virus infections.

Q. What benefits does NAC provide?

A. NAC provides the following customer benefits:

- **Dramatically improves security**—NAC helps ensure that endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy in order to proactively protect against worms, viruses, spyware, and malware. It also helps organizations focus operations on prevention, not reaction.
- **Extends existing investment**—NAC provides broad integration with multivendor security and management software, and enhances existing investments in network infrastructure and vendor software.
- **Increases enterprise resilience**—NAC provides comprehensive admission control to prevent noncompliant and rogue endpoints from impacting network availability.
- **Reduces operational costs**—NAC reduces operational expenses (OpEx) related to identifying and repairing noncompliant, rogue, and infected systems.

Q. How do Cisco Catalyst switches help mitigate a DoS attack if it does occur?

A. Cisco Catalyst switches provide an array of features in the wiring closet to defend against these disruptive attacks. Some of the primary features are:

- **Port Security**—Used to prevent MAC-based attacks. This feature allows administrator to restrict the number of MAC addresses that can transmit from a switch port.
- **Scavenger Class QoS**—Used to reprioritize traffic from systems with abnormally high traffic rates that could be potential DoS attackers.

- **Control Plane Policing**—Controls the type and quantity of traffic that is forwarded to the CPU for processing. Limits malicious traffic.
- **NetFlow Anomaly Detection**—Provides flow-based statistics to identify DoS attacks and apply port-level access control lists (ACLs) to mitigate the attacks.

Q. What is NetFlow?

A. NetFlow is a Cisco technology for monitoring network traffic and is supported by basic Cisco IOS® Software images. NetFlow periodically report on flows seen by Cisco Catalyst switches. A flow is a Layer 7 concept consisting of a session setup, data transfer, and session teardown. For every flow, a NetFlow-enabled Catalyst switch records several flow parameters including:

- **Flow identifiers**—Source and destination addresses, ports, and protocol
- Ingress and egress interfaces
- Packets exchanged
- Bytes transferred

Periodically a collection of flows and its associated parameters are packed in a User Datagram Protocol (UDP) packet according to the NetFlow protocol and sent to specified collection points.

Q. How is NetFlow information used to detect DoS attacks?

A. NetFlow works in conjunction with the Cisco Security Monitoring, Analysis and Response System event correlation tool to:

- Profile network usage and create a baseline
- Detect statistically significant anomalous behavior (from computed baseline)
- Correlate anomalous behavior to attacks and other events reported by network IDSs

After being deployed in a network, the Cisco Security Monitoring, Analysis and Response System learns the typical network usage for a few days using NetFlow data.

After determining thresholds for normal network behavior, the system switches to a detection mode where it looks for statistically significant behavior. When thresholds are exceeded, it sends an alert and can shuts down the problematic port.

Q. What is a man-in-the-middle attack?

A. With a man-in-the-middle attack, an unauthorized device assumes the identity (MAC or IP address) of a legitimate network device (such as a gateway). All traffic intended for the legitimate device is passed through the unauthorized device, which allows the hacker to scan the packets for useful information, such as passwords or the addresses of other devices.

Q. What features help prevent man-in-the-middle attacks?

A. The suite of Cisco Catalyst integrated security features that mitigate man-in-the-middle attack are:

- **DHCP Snooping**—A per-port security mechanism used to differentiate an untrusted switch port connected to an end user from a trusted switch port connected to a Dynamic Host Configuration Protocol (DHCP) server or another switch. It can be enabled on a per-VLAN basis.
- **Dynamic ARP Inspection**—Used to prevent man-in-the-middle attacks by not relaying invalid or gratuitous Address Resolution Protocol (ARP) replies out to other ports in the same VLAN. Dynamic ARP Inspection intercepts all ARP requests and replies on the untrusted ports. Each intercepted packet is verified for valid IP-to-MAC bindings (which are gathered through DHCP Snooping).
- **IP Source Guard**—Used to mitigate IP spoofing. IP Source Guard provides per-port IP traffic filtering of the assigned source IP addresses at wire speed. It dynamically maintains per-port VLAN ACLs based on IP-to-MAC-to-switch port bindings. The binding table is populated either by the DHCP Snooping feature or through static configuration of entries. IP Source Guard is typically deployed for untrusted switch ports in the access layer.

Q. What features do the Cisco Catalyst switches support?

A. The Cisco Catalyst switches support the following features (Table 1).

Table 1. Security Features on Cisco Catalyst Switches

Security Feature	Catalyst 6500 Series	Catalyst 4500 Series	Catalyst 3750/3560 Series
Trust and Identity			
IBNS (802.1X)	Yes	Yes	Yes
NAC	Yes	Yes	Yes
Threat Prevention			
Port Security	Yes	Yes	Yes
Scavenger Class QoS	Yes	Yes	Yes
Control Plane Policing	Yes	Yes	No
NetFlow Anomaly Detection	Yes	Yes	No
Data Theft Prevention			
DHCP Snooping	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes

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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus 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

Printed in the USA C67-341342-00 03/06