



DATA CENTER NETWORKING SECURITY

Enterprise data centers contain assets, applications, and data that are often the target of electronic attacks. Endpoints such as data center servers are important objectives of malicious attacks and must be protected. Attacks against server farms can result in lost business for e-commerce and business-to-business applications and theft of confidential or proprietary information. Both LANs and storage area networks (SANs) need to be secured to reduce the likelihood of these occurrences.

SANs have traditionally been considered “secure” primarily because of the fact that SAN deployments have been limited to a subset of a single data center—in essence, an isolated network. This view is simplistic at best; a single compromised host has the potential to disrupt other hosts attached to the SAN, access unauthorized data within the SAN, or bypass existing firewalls and intrusion detection systems if IP over Fibre Channel is being used.

Today it is not uncommon to find a SAN that spans outside a data center for business continuance and disaster recovery purposes. The adoption of technologies such as Small Computer System Interface over IP (iSCSI) and Fibre Channel over IP (FCIP), which use TCP/IP for the transport, emphasizes the need for SAN security as sensitive information passes over common data networks.

This paper will discuss techniques that are available in premiere Cisco data center switching products (Cisco Catalyst 6500 Series switches and Cisco MDS 9000 family switches) and solutions to make server farms less vulnerable to these threats whether they are related to the LANs or SANs.

ANATOMY OF A NETWORK ATTACK

Understanding the mechanics of two common network attacks clarifies how Cisco® data center technology mitigates or prevents the occurrence of such attacks.

This document describes two types of attacks: data theft and worm propagation. The objective of the first type of attack is stealing information, while the second attack makes applications unavailable, and can therefore be categorized as a denial-of-service (DoS) attack.

Data Theft

Attacks directed at stealing confidential information typically start with a probing and scanning phase to discover information about the target system. A hacker could use a publicly available tool such as nmap (<http://www.insecure.org>) to find information about the OS (probing) of the target host as well as the services configured on the server (scanning).

The next phase of the attack consists in identifying the vulnerabilities of the remote system. A hacker could use a publicly available tool such as nessus (<http://www.nessus.org>) and identify which vulnerability to exploit to carry the attack.

Next the attacker could install a piece of software that runs on the target host and executes unwanted functions (trojan). At this point the attacker controls the server in the data center and from this server can get access to other machines that store sensitive data (trust exploitation) or install attacking tools to carry other attacks from inside the server farm.

At this point the attacker can operate either on the LAN or on the SAN. If the compromised server is connected to the LAN, an attacker can make use of Layer 2 (Ethernet) attacks such as Address Resolution Protocol (ARP) spoofing or MAC flooding to facilitate the task of eavesdropping IP traffic including storage-over-IP traffic. If the compromised server is connected to the SAN with a host bus adapter (HBA), the attacker can potentially gain access to data stored on the SAN through attacks involving spoofed worldwide names (WWNs) or access to other servers using IP over Fibre Channel (IPFC).

Another well-known technique to control a server consists in performing TCP session hijacking. Servers whose Initial Sequence Number (ISN) is predictable can be controlled by a remote host by using a combination of source IP spoofing, trust exploitation, and ISN guessing.

Worms

Some of the attacks directed at preventing user access to the applications include DoS attacks and worms. These generate large amounts of traffic and connection requests (SYN flood, ping flood), resulting in servers running out of resources. Worms replicate themselves without any human intervention, further compounding the problem.

Worms are especially dangerous because of the speed at which they propagate. As an example the number of hosts infected by the “SQL slammer” worm doubled every 8.5 seconds and the traffic that it generated could grow to saturate a 1-Gbps link in less than a minute. The impacts of worms in a server farm are twofold: compromised servers and clogged network links.

Among well-known worms that have propagated in recent years there are Code Red (CERT Advisory CA-2001-19), Nimda (CERT Advisory CA-2001-26 Nimda Worm), SQL slammer (CERT Advisory CA-2003-04), and more. Each worm is unique in the type of vulnerability that is exploited yet the worms share similarities. A high-level description of one worm can help understanding of how to protect the server farm against others.

For example, Code Red sends TCP connection requests for port 80 to random IP addresses looking for a vulnerable host. Code Red exploits a specific buffer-overflow vulnerability in Microsoft Internet Information Server (IIS) (Microsoft Security Bulletin MS01-033). After a vulnerable host is found, Code Red causes a buffer overflow in the server, and then inserts a trojan which in turn attacks other servers.

Note: CAIDA provides information on the propagation of recent worms through the Internet: <http://www.caida.org/research/security/>

WHO TO PROTECT AGAINST?

OS vulnerabilities are continually being published. Sophisticated attack tools are publicly available and become more and more user-friendly. This means that anybody with Internet access can find a wide variety of tools and vulnerabilities to exploit.

In the 2002 CSI/FBI security survey, respondents noted that approximately 40 to 45 percent of all attacks on their systems occurred from sources residing on the internal network. The increasing need to protect internal devices and applications from attacks and unauthorized access attempts is directly reflected in these survey results.

Data centers should be designed to protect against attacks carried out by external client machines (on the Internet), internal client machines, and compromised servers.

LAN TOOLS

The Cisco Catalyst 6500 Series switches, the Catalyst 6500 Series service modules, and Cisco intrusion detection products provide security functions such as:

- **Controlled access to the server farm**—Most applications today are deployed in a multiple-tier architecture. The multiple-tier model consists of using separate server machines that provide different functions: presentation, business logic, and database. Multiple-tier server farms provide added security because a client can compromise a Web server without having access to the application itself, nor to the database. The

segregation between the tiers can be achieved by using VLANs. Client-to-server and server-to-server access is limited to the legitimate traffic by using technologies such as access control lists (ACLs), VLANs, and private VLANs all applied in hardware at wire speed.

- **Distributed denial-of-service (DDoS) protection**—The Cisco Guard module and Cisco Traffic Anomaly Detector module for the Cisco Catalyst 6500 Series deliver automated detection and mitigation of the broadest range of DDoS attacks that threaten businesses today. With these integrated security capabilities, the network infrastructure can withstand even the most massive DDoS attacks, protecting the data center and its critical applications.
- **TCP/IP protocols hardening**—Many IP protocols were not designed with security in mind and make spoofing very easy. As a protocol, TCP provides some safeguards to prevent spoofing, but is still vulnerable to more sophisticated attacks. The Cisco Catalyst 6500 Series hardens all these protocols with features such as ARP inspection, TCP SYN-COOKIES, Initial Sequence Number (ISN) randomization, routing protocol authentication, and so on.
- **Client and server authentication, data integrity, and confidentiality**—Secure Sockets Layer (SSL) and IP Security (IPSec) encryption can provide authentication for access to server applications as well as data integrity and confidentiality. The Cisco Catalyst 6500 Series can provide cryptographic operations offloading from the servers and Public Key Distribution functions.
- **Intrusion detection and prevention**—Intrusion detection solutions such as the Cisco Catalyst 6500 Series Intrusion Detection System (IDSM2) services module, and intrusion prevention solutions such as the Cisco Security Agent protect the server farm from attacks exploiting OS and application vulnerabilities. This technology is complemented by the use of the Catalyst 6500 Series mirroring technologies such as virtual ACL (VACL) capture, Remote Switched Port Analyzer (RSPAN), and NetFlow.
- **Network devices security**—The management of network devices in a data center needs to be secured to avoid unauthorized access and to prevent DoS attacks against the network. Secure management access is deployed using technologies such as ACLs, Authentication, Authorization, and Accounting (AAA), Secure Shell (SSH) Protocol, and syslog. The Cisco Catalyst 6500 Series Supervisor Engine 720 rate limiters protect the switch and router CPU from becoming overloaded in the event of a DoS attack.

Access Control and Segmentation

The Cisco Catalyst 6500 Series switches combined with the Catalyst 6500 Series Firewall Services Module (FWSM) can provide functions such as:

- **ACLs**—The Cisco Catalyst 6500 Series switches provide wire-speed packet filtering with Cisco IOS® Software ACLs and VLAN ACLs (VACLs). ACLs and VACLs allow granular traffic filtering at Layer 4 (port level), thus preventing access to services that have been left accidentally open on the servers. The Catalyst 6500 Series FWSM provides packet-filtering capabilities similar to the Catalyst 6500 Series Switch, allowing designs where the traffic from the client to the server has to pass through several layers of ACLs. Firewalls can open Layer 4 ports dynamically based on the control session negotiation, commonly referred to as fixups.
- **VLANs**—A Layer 2 switch is a device capable of grouping subsets of its ports into virtual broadcast domains isolated from each other. These domains are commonly known as virtual LANs (VLANs). The Cisco Catalyst 6500 Series works in accordance with popular VLAN-tagging technologies Inter-Switch Link (ISL) or 802.1Q across physical links (sometimes referred to as trunks) and employs advanced tagging techniques to preserve the VLAN information. VLANs can be used to segregate server farms and can be combined with the FWSM to filter VLAN-to-VLAN traffic.
- **Private VLANs (PVLANS)**—PVLANS provide isolation of ports from one another within the same VLAN. With private VLANs you can use a single subnet and force all the server-generated traffic to go to a promiscuous or upstream port, which typically is a router port, or a VLAN interface on a FWSM. By doing so, servers can be protected from Layer 2 attacks such as ARP spoofing, even where other devices in the same VLAN may be compromised. The Cisco Catalyst 6500 Series supports hardware-based PVLAN segregation.
- **MPLS VPNs**—Using MPLS to build VPNs provides network segmentation with address transparency. This facilitates an identity-aware network in the most scalable way while taking advantage of the benefits and flexibility of IP. MPLS VPNs provide privacy and security equal to that provided by Layer 2 VPNs by limiting the distribution of a VPN routes to only those routers that are members of the VPN. The Cisco Catalyst 6500 Series Supervisor Engine 720 in conjunction with the Cisco Policy Feature card 3B (PFC3BXL) provides hardware-based MPLS VPN support. MPLS VPNs can be combined with FWSM virtual firewalls for VPN-specific stateful inspection.

- **Port security**—Cisco data centers feature a fully switched topology, where no hub is present, and all links are full duplex. Layer 2 Flooding should only be used during topology changes to allow fast convergence of the Layer 2 network. Technologies that are based on flooding introduce performance degradation besides being a security concern. Flooding can also be the result of a security attack and that is why port security should be configured on the access ports. To prevent MAC flooding, port security is used, whereby specify MAC addresses are assigned to each port or to permit a limited number of MAC addresses. When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or learned on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port shuts down permanently (the default), shuts down for a specified length of time, or drops incoming packets from the insecure host.
- **IEEE 802.1X**—The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

TCP/IP Protocols Security

The Cisco Catalyst 6500 Series switches combined with the Catalyst 6500 Series Firewall Services Module (FWSM) and the Cisco Content Switching Module (CSM) provide security functions such as:

- **ARP inspection**—ARP inspection provides a mapping between a default gateway IP address and its MAC address. If the switch sees a gratuitous ARP carrying an invalid mapping, the switch drops the packet, thereby preventing ARP spoofing attacks.
- **Unicast Reverse Path Forwarding (URPF)**—URPF checks each packet to ensure it is coming from the intended sources and expected interfaces, helping mitigate source-address spoofing. The check consists of verifying that there is a routing-table entry for the source address matching the interface that the packet arrived on. The Cisco Catalyst 6500 Series switches and the Catalyst 6500 Series FWSM implement URPF checking in hardware. The Catalyst 6500 Series Supervisor Engine 720 supports URPF on up to six parallel paths.
- **Fragment filtering**—The Cisco Catalyst 6500 Series switches allow Cisco IOS Software ACLs and VACLs to be constructed to either permit or deny forwarding of fragments. Fragment filtering can be used to prevent fragment attacks (such as the ones described in RFC 1858). Fragment filtering can be further complemented with the stateful capabilities of the Cisco Catalyst 6500 Series FWSM, which provides fragment reassembly and validation (virtual reassembly) before forwarding the fragments.
- **ISN randomization**—The TCP/IP stack implementation of some operating systems generates TCP ISNs in a predictable fashion, making it possible to hijack TCP sessions. In the past this vulnerability has been identified on multiple operating systems (see CERT Advisory CA-1995.01, CERT Advisory CA-1998.13, CERT Advisory CA-2001-09, US CERT Vulnerability Note VU#498440). The Cisco Catalyst 6500 Series FWSM can randomize the ISN used by servers' TCP connections.
- **TCP SYN cookies**—SYN cookies are particular choices of initial TCP sequence numbers by TCP servers, SYN cookies can be used to protect the SYN queue of the TCP/IP stack of a device (either a network device or a server) from filling up by selecting an ISN (the cookie value) based on a Message Digest Algorithm 5 (MD5) of the source and destination IP addresses and port numbers. When a certain threshold in the queue is reached, a SYN/ACK response (the second part of the TCP three-way handshake) is still sent, but with no connection-state information kept. If the final ACK for the three-way handshake is received, the server recalculates the original information that had come with the initial SYN. SYN cookies are an effective mechanism to protect the server farm from DoS attacks. By using this technology the Cisco CSM can withstand attacks of hundreds of thousands of connections per second while preserving legitimate user connections.
- **TCP Connection State Tracking**—The Cisco Catalyst 6500 Series FWSM and the Cisco CSM keep connection-state information of the traffic that flows through them. As an example, a forged TCP segment sent to a router is subject to forwarding as any other IP packet. The Catalyst 6500 Series FWSM and the Cisco CSM will not forward this segment because there is no existing TCP connection for the forged segment.
- **VLAN Trunking Protocol (VTP) authentication**—VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and naming of VLANs on a network-wide basis. VTP authentication helps ensure authentication and integrity of switch-to-switch VTP messages. VTP Version 3 introduces an additional mechanism to authenticate the primary VTP server as the only device allowed to change the VLAN configuration on a network-wide basis.

- **Routing Protocol Authentication**—Neighbor router authentication, sometimes called “route authentication,” certifies the neighbors’ authenticity and the integrity of routing updates for router-to-router (Layer 3 switch-to-Layer 3 switch) communication and for host-to-router (Layer 3 switch) communication. Hosts can be Layer 3 multiple-homed servers or mainframes. Routing protocols that support authentication include Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP).

Client and Servers Authentication Data Integrity and Confidentiality

The Cisco Catalyst 6500 Series switches, the Catalyst 6500 Series SSL Services Module, and the Cisco 7600/Catalyst 6500 IPSec VPN Services Module provide security functions such as:

- **SSL encryption**—SSL provides authentication, data confidentiality, integrity, and nonrepudiation for client-to-server and server-to-server communications. Virtually any application that uses TCP/IP as the transport protocol can use the services provided by SSL and create SSL connections by using SSL sockets. The Cisco Catalyst 6500 Series SSL Services Module offloads servers from decrypting strong ciphers (like Triple Data Encryption Standard [3DES]) while still maintaining end-to-end encryption. The module also simplifies the management of digital certificates and can enforce a trust model that gives control on who is allowed to use a given application.
- **IPSec encryption**—IPSec helps ensure confidentiality, integrity, authentication, and anti-reply protection. The IPSec protocol operates between the network layer and the transport layer of the TCP/IP protocol stack. IPSec is completely transparent to the applications which, as a consequence, do not need to be IPSec-aware. IPSec is often used to build secured tunnels between data centers.

Traffic Analysis, Intrusion Detection, and Prevention

The Cisco Catalyst 6500 Series provides the following traffic-analysis functions:

- **Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN)**—SPAN is a technology for mirroring traffic from one or more ports on a Cisco Catalyst 6500 Series switch (the SPAN source) to another port on the same switch (the SPAN destination). This is frequently called “local SPAN.” RSPAN allows the scope of analysis to be extended to encompass multiple switches interconnected in the same Layer 2 domain. RSPAN and VACLs can be combined for very granular traffic analysis by differentiating mirrored traffic across up to 64 groups.
- **VACL capture**—The VACL capture technology provided by the Cisco Catalyst 6500 Series allows ACLs to be defined to provide granular control over what traffic is captured.
- **NetFlow**—NetFlow is a technology to efficiently collect and export statistics from traffic that flows through switches and routers. In the context of security, NetFlow is used for its DoS, Distributed Dos (DDoS), and worm detection. The Cisco Catalyst 6500 Series switches support NetFlow export in NetFlow versions 5, 7, and 8 formats. Sampled NetFlow and NetFlow aggregation can be used to reduce the volume of statistics collected.

The Cisco Catalyst 6500 Series switches combined with the Cisco IDS 4200 Series sensors or with the Cisco Catalyst 6500 Series Intrusion Detection System (IDS-M-2) Services Module provide the following intrusion detection functions:

- **Multigigabit IDS analysis**—IDS sensors can detect malicious activity in a server farm based on protocol or traffic anomalies, or based on the stateful matching of events described by signatures. An IDS sensor can detect an attack from its very beginning by identifying the probing activity, or it can identify the exploitation of well known vulnerabilities.

IDS sensors can work in conjunction with the Cisco Catalyst 6500 Series Switch or with a Cisco Catalyst 6500 Series FWSM to isolate a compromised server before it infects other devices. Traffic distribution to multiple IDS sensors can be achieved by using the Catalyst 6500 Series mirroring technologies (RSPAN and VACL capture) for multigigabit traffic analysis.

In addition to network-based traffic analysis, intrusion detection, and intrusion prevention, additional security safeguards can be installed on servers themselves through the use of Cisco Security Agent, which provides the following security functions:

- **Host intrusion prevention**—Cisco Security Agent software executes on a server and is capable of preventing buffer overflow, malicious registry, file system, and TCP/IP stack operations. In brief, the host-based intrusion-prevention software prevents servers from being infected by new worms and from being manipulated by an attacker, thereby eliminating known and unknown (Day Zero) security risks.

Network Devices Security

The management interfaces of network devices need to be secured to prevent unauthorized access: a malicious user who has access to the console of a network device can easily alter the network configuration, providing an opening to bypass security measures. Cisco Catalyst 6500 Series switches and service modules provide the following secure management functions:

- **Authentication, Authorization, and Accounting (AAA)**—AAA is an architecture that can be used to control the access to sensitive resources such as servers and network devices, based on users and groups. AAA can use the username/password database local to the switch or can use protocols such as TACACS+ or RADIUS to access an authentication server.
- **Secure Shell (SSH) Protocol Version 2**—SSHv2 provides secure remote access through the use of authentication and encryption. SSH Protocol should be used as an alternative to insecure protocols such as telnet and rlogin. SSHv2 can be used in conjunction with TACACS+ and RADIUS. The Cisco Catalyst 6500 Series switches support SSHv2.
- **SNMP Version 3 (SNMPv3)**—SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. The Cisco Catalyst 6500 Series switches support SNMPv1, v2c, and v3. SNMPv3 (RFC 2271-2275) provides authentication, integrity, and encryption. SNMPv3 traffic is encrypted with Data Encryption Standard (DES), and carries an MD5 HMAC or a SHA HMAC algorithm for authentication and integrity purposes.
- **Syslog**—Syslog messages are unsolicited notification that a network device can save in a log file or direct to a syslog server such as CiscoWorks2000 Resource Manager Essentials (RME). Syslog messages include a timestamp from the syslog server, a device name, a sequence number, the timestamp from the network device and the message itself. Syslog types are categorized as facilities. A complete list of the available syslog messages available on the Catalyst 6500 is available at http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_chapter09186a0080163dbe.html
- **Network Time Protocol Version 3 (NTPv3)**—This protocol (RFC1305) is used to synchronize system clocks in network devices and it is fundamental to be able to use syslog messages coming from multiple sources, whose timestamp allows to correlate the events that have been logged.

In addition to protecting the control plane from unauthorized access, it is equally important to protect it from DoS attacks and worms. The Cisco Catalyst 6500 Series switches provide features such as:

- **Cisco Express Forwarding**—Threats such as worms look for vulnerable devices by continuously generating connection requests for random destination IP addresses. Flow-based Layer 3 switches can be easily overwhelmed by the amount of traffic, because they process the first packet of a flow in software. Hardware-based Cisco Express Forwarding, which is supported on the Cisco Catalyst 6500 Series supervisor engines II and 720, solves this problem by keeping all forwarding in hardware, separate to the software-based control plane.
- **Hardware rate limiters**—Layer 3 switches typically forward and filter traffic in hardware. Some traffic types require software processing (Internet Control Message Protocol [ICMP] unreachable, ICMP redirect, or to manage IP packet maximum transmission unit [MTU] or time-to-live (TTL) failures for the purpose of generating ICMP packet too big or ICMP time exceeded messages). The Cisco Catalyst 6500 Series Supervisor Engine II provides predefined rate limiters, while the Catalyst 6500 Series Supervisor Engine 720 provides additional control with 12 special-case rate limiters.
- **Control Plane Policing (CoPP)**—Control Plane Policing allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of the switch against reconnaissance and DoS attacks. This helps maintain packet forwarding and protocol states despite an attack or heavy traffic load on the switch.
- **Address Resolution Protocol (ARP) throttling**—ARP throttling limits the rate at which packets destined to a connected network are forwarded to the route processor in case their MAC address has not been resolved yet (glean adjacency). The Cisco Catalyst 6500 Series Supervisor Engine II provides preconfigured rate limiting to the router processor, and Catalyst 6500 Series Supervisor Engine 720 provides configurable rate limiting.

Additional security is provided by configuring Role-Based Access Control (RBAC). RBAC is supported by Cisco Secure Access Control Server (ACS). The Cisco 1105 for Hosting Solution Engine and the CiscoWorks VPN/Security Management Solution also provide RBAC configuration capabilities.

SAN TOOLS

Traditionally, SANs have been considered “secure” primarily because SAN deployments have been limited to a subset of a single data center—in essence, an isolated network. This view is simplistic at best; a single compromised host has the potential to disrupt other hosts attached to the SAN, access unauthorized data within the SAN, or bypass existing firewalls and intrusion detection systems if IP over Fibre Channel (RFC 2625) is being used.

Today it is not uncommon to find a SAN that spans outside a data center for business continuance and disaster recovery purposes. The adoption of technologies such as iSCSI and FCIP, which use TCP/IP for the transport, emphasizes the need for SAN security as sensitive information passes over common data networks.

SAN security should be considered from three angles:

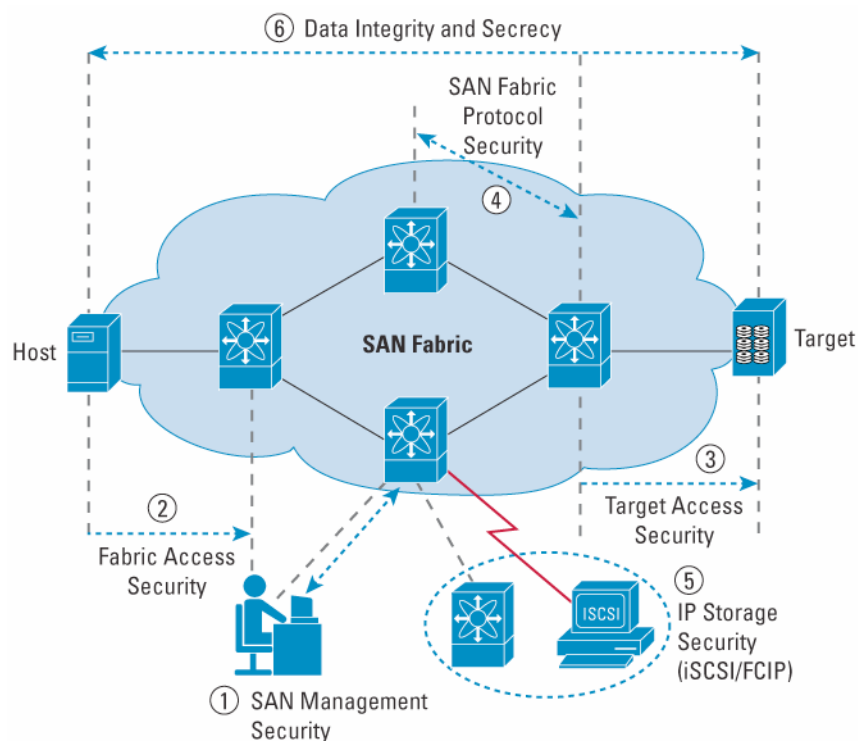
1. Securing the SAN from external threats (for example, hackers and people with malicious intent)
2. Securing the SAN from internal threats (for example, unauthorized staff and compromised devices)
3. Securing the SAN from unintentional threats from authorized users (misconfigurations and human errors)

The first two are relatively straightforward and well understood from a security standpoint. The third angle is less straightforward and only minimal or no attention in the past has been paid to unintentional security threats from authorized users. Just as in a UNIX or Windows environment it is prudent to minimize the practice of performing administrative tasks with root or administrator privileges, the same cautious approach of granting the minimum amount of privileges to perform a task holds true when working with a SAN. There are many facets to this—the benefits of locking down “operator” privileges on a switch using role-based authentication are easily understood, but others such as minimizing the probability of a disruptive fabric reconfiguration resulting from a misconfigured switch with an overlapping domain ID are less commonplace. Many of these approaches blur the boundaries between SAN security, best-practice SAN design, and high-availability SAN design, but all are important from the perspective that a correctly configured, secure switch can help prevent both deliberate and unintentional disruptions.

SAN security is best viewed from an architectural level, where there are six primary areas of focus (Figure 1). The six areas include:

- **Fabric access**—Secure fabric access to fabric services
- **Target access**—Secure access to targets and logical unit numbers (LUNs)
- **SAN protocol**—Secure switch-to-switch communication and authorization
- **IP storage access**—Secure FCIP and iSCSI services
- **Data integrity and secrecy**—Encryption of data in transit
- **SAN management access**—Secure access to management services

Figure 1. Areas of Focus for SAN Security



The following section explores each area along with the advanced security features of the Cisco MDS 9000 Series platform available in each of the areas.

Fabric and Target Access

Fibre Channel fabric and target access security features provided in the Cisco MDS 9000 family multilayer switches include:

- **Fibre Channel zoning**—Zoning is the security mechanism within Fibre Channel used to restrict communication between devices within the same Fibre Channel fabric. With many different types of servers and storage devices on the network, a host could gain access to a disk being used by another host, potentially with a different OS, and corrupt the data on this disk. Zoning can be of two types: soft zoning and hard zoning. Soft zoning refers to software-based zoning; that is, zoning enforced through control-plane software on Fibre Channel switches in the Fibre Channel Name Server service. Hard zoning refers to hardware-based zoning, enforced through hardware ACLs which are applied to every Fibre Channel frame that is switched.

While soft zoning provides sufficient security to prevent accidental loss of data, it does not provide sufficient security to prevent unauthorized access to data. Hard zoning does provide the additional security necessary to prevent unauthorized access to data, but only when no worldwide name (WWN) spoofing is used.

All members of the Cisco MDS 9000 family of multilayer intelligent switches support both soft zoning and hard zoning for up to 2000 zones and 20,000 zone members.

- **Logical unit number (LUN) zoning and read-only zones**—The Cisco MDS 9000 family can provide more detailed zoning than is generally available today. Based on deep frame inspection, hard zoning within Cisco MDS 9000 family switches can restrict access to explicit LUNs within a storage array and can even restrict write SCSI I/O operations, enforcing read-only access.

- **Virtual SANs (VSANs)**—VSANs can be used to create multiple logical SANs over a common physical infrastructure. Each VSAN runs its own set of fabric services, providing for absolute partitioning between virtual fabrics.

VSANs can be used to achieve higher security and greater stability in Fibre Channel fabrics by providing isolation among devices that are physically connected to the same set of switches. Faults within one fabric are contained within a single VSAN and are not propagated to other VSANs. No communication is possible between devices in different VSANs except where explicitly allowed through the use of Inter-VSAN Routing.

- **Inter-VSAN Routing (IVR)**—IVR can be used to securely create a path from a device in one VSAN to one or multiple devices in a different VSAN, without merging the individual VSAN fabrics (that is, without creating a single merged fault domain). Inter-VSAN Routing effectively provides Network Address Translation (NAT) for data traffic only (Fibre Channel Class 2 and 3).
- **Port security**—Port security allows access to Fibre Channel fabric based on the device identity attributes. Port security prevents unauthorized access to a switch port by binding specific worldwide names (WWNs) as having access to one or more switch ports. When port security is enabled on a switch port, all devices connecting to that port must be in the port-security database and must be listed in the database as bound to the given port. In the case of a storage device or host, the port name (pWWN) or node name (nWWN) can be used to lock authorized storage devices to a specific switch port. In the case of an E_Port/TE_Port, the switch name (sWWN) is used to bind authorized switches to a given switch port.
- **Port mode security**—Port mode security can be used to restrict the function of a port. For example, the port mode may be configured to prevent edge ports inadvertently being used for ISLs.
- **Fibre Channel Security Protocol**—Fibre Channel Security Protocol (FCSP) Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) can be used to help ensure data integrity (tamper-proof) and authentication (non-repudiation) for both host-to-switch and switch-to-switch communication. Authentication can be performed locally in the switch or remotely through a centralized RADIUS or TACACS+ server.

FCSP DH-CHAP provides absolute protection against WWN spoofing on a compromised port, even when physical security of the switch has been compromised and a rogue device has been installed on the same physical switch port as that of the rightful host.

FCSP DH-CHAP is supported by all major host bus adaptor (HBA) vendors and some SAN switch vendors.

SAN Protocol Security

Many of the fabric- and target-access security features such as VSANs, Inter-VSAN Routing, Port Security, Port Mode Security, and FCSP DH-CHAP are just as relevant to SAN Protocol security as they are to fabric- and target-access security. In addition to these, all switches in the Cisco MDS 9000 Series include additional SAN Protocol security functions:

- **Disruptive Reconfigure Fabric Rejection**—Ability to reject disruptive fabric-reconfiguration requests from rogue misconfigured or new unconfigured switches being attached to an existing fabric. Without this rejection, a rogue misconfigured or new unconfigured switch could cause a fabric outage.
- **IBM Fiber Connection (FICON) Fabric Binding**—Ability to limit what switches and domain IDs may participate in a FICON fabric.
- **Fibre Channel ID Caching, Persistent Fibre Channel ID Allocation, and Static Fibre Channel ID Assignment**—Ability to limit what Fibre Channel IDs are assigned to given pWWNs as well as offer persistent Fibre Channel IDs across system restarts.

IP STORAGE SECURITY

IP services modules for the Cisco MDS 9000 family provide Gigabit Ethernet ports that are capable of accepting both incoming connections from hosts (iSCSI initiators) as well as providing SAN Extension over IP (Fibre Channel over IP). IP storage security features of the Cisco MDS 9000 family include:

- **iSCSI authentication**—Incoming iSCSI sessions from iSCSI initiators are authenticated using Challenge Handshake Authentication Protocol (CHAP) prior to the iSCSI session being established.
- **iSCSI-initiator persistent dynamic WWN and static WWN allocation**—iSCSI initiators may be dynamically or statically mapped to virtual Fibre Channel initiators with a unique nWWN and pWWN per initiator, per VSAN (conceptually, each iSCSI initiator becomes a “virtual”

N_Port). Both nWWNs and pWWNs can be assigned in a persistent manner dynamically from a range of WWNs stored within the switch, or may be assigned a static nWWN or pWWN.

This allows for LUN Security, LUN Mapping, and LUN Masking to be employed on midrange and enterprise-class storage arrays because they can uniquely identify hosts connected using iSCSI in exactly the same manner that they can uniquely identify Fibre Channel HBA-attached hosts.

- **iSCSI access controls**—There are various forms of access controls that may be applied to iSCSI initiators. Firstly, an iSCSI initiator is only allowed to access Fibre Channel targets (virtual iSCSI targets) that they have been explicitly permitted to access. Secondly, an iSCSI initiator (virtual N_Port) is explicitly configured to be an initiator within a single VSAN. Standard Fibre Channel zoning can be used to zone the virtual N_Port(s) and storage devices. Finally, per-interface restrictions can be used to limit individual iSCSI targets to being advertised either globally (on all Gigabit Ethernet interfaces) or only on specific Gigabit Ethernet interfaces, subinterfaces, or VLANs.
- **Fibre Channel over IP (FCIP)**—FCIP transports Fibre Channel data across an IP network by tunneling the Fibre Channel frames across a pair of TCP connections between two switches. The raw Fibre Channel frames (including the complete Fibre Channel header) are encapsulated into TCP segments at the sending end of the tunnel and reconstructed into Fibre Channel frames at the receiving end.

FCIP itself does not have any explicit security, but it can use all of the existing security mechanisms available to native Fibre Channel. These include port security and FCSP DH-CHAP switch-to-switch authentication.

Data Integrity and Secrecy

Neither iSCSI nor FCIP provide any security of the data being transported. That is, if a rogue device in the path were able to eavesdrop, it could view all of the storage data being transferred across the link. Because of this, the IP Storage working group within the IETF has also developed a framework for securing IP-based storage communications: See “Securing Block Storage Protocols over IP” (draft-ietf-ips-security-19.txt). In essence, the IETF mandates the use of IPsec if the data network cannot be trusted. Both the multiprotocol switching 14+2 (MPS 14+2) line card and Cisco MDS 9216i Multilayer Fabric Switch offer integrated hardware-based IPsec support, providing wire-rate IPsec encryption and decryption with Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

For the Cisco 8-port IP Storage Services module (IPS-8) and Cisco 4-port IP Storage Services module (IPS-4), numerous security devices are available for creating an encrypted IPsec tunnel. The Cisco 7600/Catalyst 6500 IPsec VPN Services Module provides infrastructure-integrated IPsec VPN services capable of 1.9-Gbps 3DES performance, 8000 active tunnels, and tunnel creation of up to 60 tunnels per second.

Numerous other devices exist to create IPsec tunnels. These are covered within the SAFE Blueprint from Cisco on VPN security. The SAFE Blueprint is available at <http://www.cisco.com/go/safe>.

SAN Management Access

The management of the network device in a data center needs to be secured to avoid unauthorized access: a malicious user that has access to the console of a network device can easily alter the network configuration. The Cisco MDS 9000 family provides the following secure management functions:

- **Authentication, Authorization, and Accounting (AAA)**—AAA is an architecture that can be used to control the access to sensitive resources such as servers and network devices, based on users and groups. AAA can use the username/password database local to the switch or can use protocols such as TACACS+ or RADIUS to access an authentication server.
- **Role-Based Access Control (RBAC)**—RBAC allows different users to have different roles, responsibilities, management capabilities, and restrictions. Up to 64 roles may be defined within the system, with users allocated to roles either locally within the configuration of a switch or in a centralized manner through AAA.
- **VSAN-Based Roles Access**—Storage administrators may be granted access and rights selectively per VSAN, providing for further restrictions on the privileges and capabilities granted to an administrator.

- **Secure Shell (SSH) Protocol Version 2**—SSHv2 provides secure remote access through the use of authentication and encryption. SSHv2 should be used as an alternative to insecure protocols such as telnet, rlogin, and FTP. SSHv2 can be used in conjunction with TACACS+ and RADIUS. SSHv2 can also be used to securely transfer images, log files, and switch configuration through Secure Copy or Secure FTP.
- **SSL Version 2 and transparent LAN services (TLS) 1.0**—The Storage Management Initiative Specification (SMI-S) is the common interfaces based on Common Information Model (CIM) to allow multiple-vendor interoperability in a SAN environment. SMI-S allows SAN management clients to link with CIM servers to manage large numbers of storage resources with a unified interface.

The embedded agent inside the Cisco MDS 9000 family includes a CIM Object Manager and CIM Provider with access supported through SSL and TLS, and is tied into AAA and RBAC.

- **SNMPv3**—SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. All Cisco MDS 9000 family switches support SNMPv1, v2c, and v3. SNMPv3 (RFC 2271-2275) provides authentication, integrity, and encryption. SNMPv3 traffic is encrypted with DES, and carries an MD5 HMAC or a SHA HMAC algorithm for authentication and integrity purposes. The Cisco MDS 9000 family also supports stronger AES 128-based encryption with SNMPv3 (RFC 3826).
- **Syslog**—Syslog messages are unsolicited notification that a network device can save in a log file or direct to a server such as CiscoWorks Resource Manager Essentials (RME). Syslog messages include a timestamp from the syslog server, a device name, a sequence number, the timestamp from the network device, and the message itself.
- **Network Time Protocol Version 3 (NTPv3)**—NTPv3 (RFC1305) is used to synchronize system clocks in network devices and it is fundamental to be able to use syslog messages coming from multiple sources, whose timestamp allows to correlate the events that have been logged across multiple devices.
- **Accounting log**—An accounting audit trail of configuration commands is kept both within the switch (critical messages stored persistently in NVRAM) and can also be logged to centralized syslog and AAA servers through RADIUS accounting messages or TACACS+ accounting messages.
- **Call Home**—Call Home provides e-mail-based notification of critical system events. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a network operations center, and usage of Cisco AutoNotify services for direct case generation with the Cisco Technical Assistance Center (TAC). Multiple concurrent destinations, message categories, and message-delivery options mean that Call Home can be tailored to specific network-management and monitoring requirements. Message format options include short text (suitable for pagers and Short Message Service [SMS]), plain text, and Extensible Markup Language (XML)-based e-mails.
- **Fabric Consistency Checker**—Embedded within Fabric Manager (the JAVA-based GUI management suite that uses SNMP to communicate with Cisco MDS 9000 family switches) is a wizard called the Fabric Consistency Checker. This is a tool that can validate that configuration policy is consistent across multiple switches within a fabric. The tool will highlight configuration differences where there are exceptions from the configuration of a master “policy” switch and provide a mechanism to resolve configuration differences. Fabric Consistency Checker provides an effortless way to confirm that security policy and security configurations are consistent across all switches within a fabric.
- **ACLs**—ACLs may be applied on management interfaces and IPS-4, IPS-8 and MPS 14+2 IP Storage Service modules Gigabit Ethernet interfaces to limit management and IP access to a subset of IP addresses.
- **Switched Port Analyzer (SPAN)**—SPAN allows for any interfaces or VSANs being monitored to have a copy of each frame taken and sent out a SPAN destination port. Any Fibre Channel port in a switch can be configured as a SPAN destination port. A Fibre Channel Analyzer (such as a Finisar Analyzer) or a Cisco Port Adapter Analyzer may be connected to the SPAN destination port and receive a copy of all monitored traffic.

SPAN is a very powerful feature for problem diagnosis and traffic monitoring. Because the SPAN feature effectively allows one to take a copy of any Fibre Channel frames being switched inside the switch, this may be considered a security risk given sensitive data that previously could not be snooped can now be captured. Because of this, it is recommended that Role-Based Access Control (RBAC) be used to protect against unauthorized users being able to enable SPAN.

END-TO-END VALUE

The use of LAN and SAN technologies provides a cost-effective way of protecting data center applications through the use of network intelligence to minimize the risk of the most common threats.

A data center network can provide security to server farm applications because of the capability to segregate traffic of different server farms. Segregation is implemented on both the LAN and SAN by using these technologies:

- Virtual LANs (VLANs) on the LAN and virtual SANs (VSANs) on the SAN
- ACLs on the LAN and hard zoning on the SAN
- Ethernet port security on the LAN and Fibre Channel port security on the SAN

Layer 2 and 3 protocol security and Fibre Channel protocol security help ensure authentication and integrity for switch-to-switch communication with technologies such as:

- VLAN Trunking Protocol Version 3 (VTPv3) and Routing Protocol Authentication on the LAN and FCSP DH-CHAP authentication on the SAN

Data theft is made more difficult by the use of encryption, which provides authentication, data confidentiality, and integrity with technologies such as:

- SSL and IPSec on the LAN and in future Fibre Channel Security (FCSec) (part of FCSP) on the SAN

Traffic monitoring can help identifying malicious activity with the use of technologies such as:

- SPAN, RSPAN, VACL capture, NetFlow, and Call Home on the LAN and SPAN, RSPAN, Fibre Channel flow statistics, Call Home, and RMON Threshold Alarms on the SAN

Secure management limits the possibility that an attacker gains control of LAN or SAN devices, and is provided by the following technologies:

- AAA, SSHv2, SNMPv3, syslog, NTPv3, and RBAC available on both LAN devices and SAN switches.

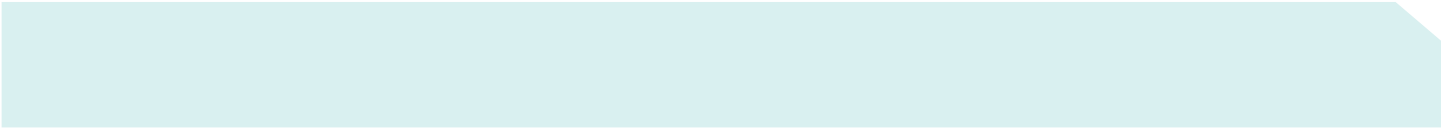
Servers and hosts are present within the data center on the LAN and for some servers, on both the LAN and the SAN. The Cisco Security Agent can be used to provide additional protection against threats.

An end-to-end Cisco solution in a data center provides comprehensive security that encompasses Layer 2 protocols, application-layer protocols, and the server OS. Segmentation is mirrored across LANs and SANs.

SECURITY ARCHITECTURE AND PRODUCTS

The individual products and components that form the security architecture include:

- **Cisco Catalyst 6500 Series Switch**—As the premier intelligent multilayer modular switch from Cisco, the Catalyst 6500 Series is uniquely qualified for the data center. Its forwarding performance and its support for Layer 4 to 7 service modules, 10/100/1000 ports, 10 Gigabit Ethernet, jumbo frames, 802.1s, 802.1w, VLAN ACLs, SPAN, QoS, Multicast, uRPF in hardware, etc. make it the obvious choice as an aggregation and access switch in the data center.
- **Cisco Catalyst 6500 Series Firewall Services Module (FWSM)**—This module provides a high-performance integrated firewall solution within the Catalyst 6500 Series with industry-leading performance of 5-Gbps throughput, 100,000 connections per second, and 1 million concurrent connections. Up to four modules can be installed in a single chassis, providing scalability to 20 Gbps per chassis. Based on Cisco PIX ® Firewall technology, the Catalyst 6500 Series FWSM provides large enterprises and service providers with unmatched security, reliability, and performance.
- **Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module or Cisco IDS 4200 Series Sensor**—Cisco IDS 4200 Series sensors use a combination of highly innovative and sophisticated detection techniques, including stateful pattern recognition, protocol parsing, heuristic detection, and anomaly detection, which provide comprehensive protection from a variety of both known and unknown cyber threats. Furthermore, the Cisco patent-pending Threat Analysis Micro-Engine (T.A.M.E) technology allows granular customization of sensor signatures, resulting in precisely tuned sensors that minimize the occurrence of “false positives.” The Cisco IDS 4200 Series includes four products: the Cisco IDS 4215, IDS 4235, IDS 4250, and IDS 4250 XL sensors. At 1 Gbps, the Cisco IDS 4250 XL provides unprecedented



performance through customized hardware acceleration to protect fully saturated gigabit links as well as multiple partially used gigabit subnets. The Cisco Catalyst 6500 Series IDSM-2 integrates into the Catalyst 6500 Series chassis for easier installation and better rack-space efficiency.

- **Cisco Catalyst 6500 Series SSL Services Module**—This module integrates into the Catalyst 6500 Series and provides an increased number of secure connections to support Web-based applications by offloading the processor-intensive tasks related to securing traffic with the SSL protocol. The use of SSL provides privacy, confidentiality, and authentication. SSL uses a wide range of certificates that reside on the module, thus centralizing certificate management, eliminating the need to manage certificates on individual servers, and reducing cost by requiring a single certificate copy versus a certificate copy for each server. The module provides up to 3000 connection setups per second, per module (12,000 per chassis); 300-Mbps bulk encrypted throughput per module (1.2 Gbps per chassis) while maintaining 60,000 concurrent client connections (240,000 per chassis).
- **Cisco Content Switching Module (CSM)**—The Cisco CSM integrates advanced Layer 4 to 7 content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing. With features such as full stateful redundancy, server slow-start and graceful shutdown, SYN cookies, HTTP 1.1 persistence, cookie- and URL-based persistence, global server load balancing, route health injection, scriptable keepalives, in-band health monitoring, and HTTP return code checking, the Cisco CSM provides the flexibility to improve the performance and reliability of large-scale server farms.
- **Cisco Guard modules and Cisco Traffic Anomaly detectors**—These modules for the Cisco Catalyst 6500 Series deliver automated detection and mitigation of the broadest range of DDoS attacks that threaten businesses today. With these integrated security capabilities, the network infrastructure can withstand even the most massive DDoS attacks, protecting the data center and its critical applications.
- **Cisco MDS 9000 family switches**—The Cisco MDS 9000 family provides a full line of products to meet requirements for storage networks of all sizes and architectures. The Cisco MDS 9000 family delivers intelligent network services such as VSANs, comprehensive security, advanced traffic management, sophisticated diagnostics, and unified SAN management. In addition, the Cisco MDS 9500 series director switches and the Cisco MDS 9200 series fabric switches provide multiprotocol and multitransport integration and an open platform for embedding intelligent storage services such as network-based virtualization. With its multilayer approach to network and storage intelligence, the Cisco MDS 9000 family ushers in a new era in storage networking.
- **Cisco Security Agent**—This host-based software identifies and prevents malicious behavior, thereby eliminating known and unknown (“Day Zero”) security risks and helping to reduce operational costs. Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, OS integrity assurance, and audit-log consolidation, all within a single product.

FOR MORE INFORMATION

For more information about Cisco security appliances, please visit the following Websites.

Cisco Catalyst 6500 Series switches

<http://www.cisco.com/en/US/products/hw/switches/ps708/index.html>

Cisco MDS 9000 family switches

<http://www.cisco.com/go/storagenetworking>

Cisco Catalyst 6500 Series Firewall Services Module

<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html>

Cisco IDS 4200 Series Sensor

<http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/>

Cisco Catalyst 6500 Series Intrusion Detection System Services Module

<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/>

Cisco Catalyst 6500 Series SSL Services Module

<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4156/index.html>

Cisco Content Switching Module

<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/index.html>

Cisco Security Agent

<http://www.cisco.com/en/US/products/sw/secursw/ps5057/>

VLAN security

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml



Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)