Cisco and Public Sector Cyberdefense

Continue

Overview

On January 8, 2008 President George W. Bush set forth the nation's largest cybersecurity initiative to date by signing Presidential Directive 54 and Homeland Security Presidential Directive 23. These executive directives formally declare the cyberinfrastructure of the United States a national security asset and its criticality to the diplomatic, intelligence, military, and economic well-being of the nation. More recently, President Obama reaffirmed and extended this prioritization of cybersecurity and announced plans for a new office at the White House led by a cybersecurity coordinator.

"Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient." Obama said. "We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage." [1]

As a leader in the area of information security and a trusted advisor to many agencies within the federal government, Cisco is in a unique position to help provide the commercial off-the-shelf (COTS) elements for achieving these cybersecurity goals. Cisco provides an integrated approach to defense in depth that aligns with the government's strategy for information and systems security.

Providing cybersecurity requires a network-level approach, with specific emphasis on four different areas:

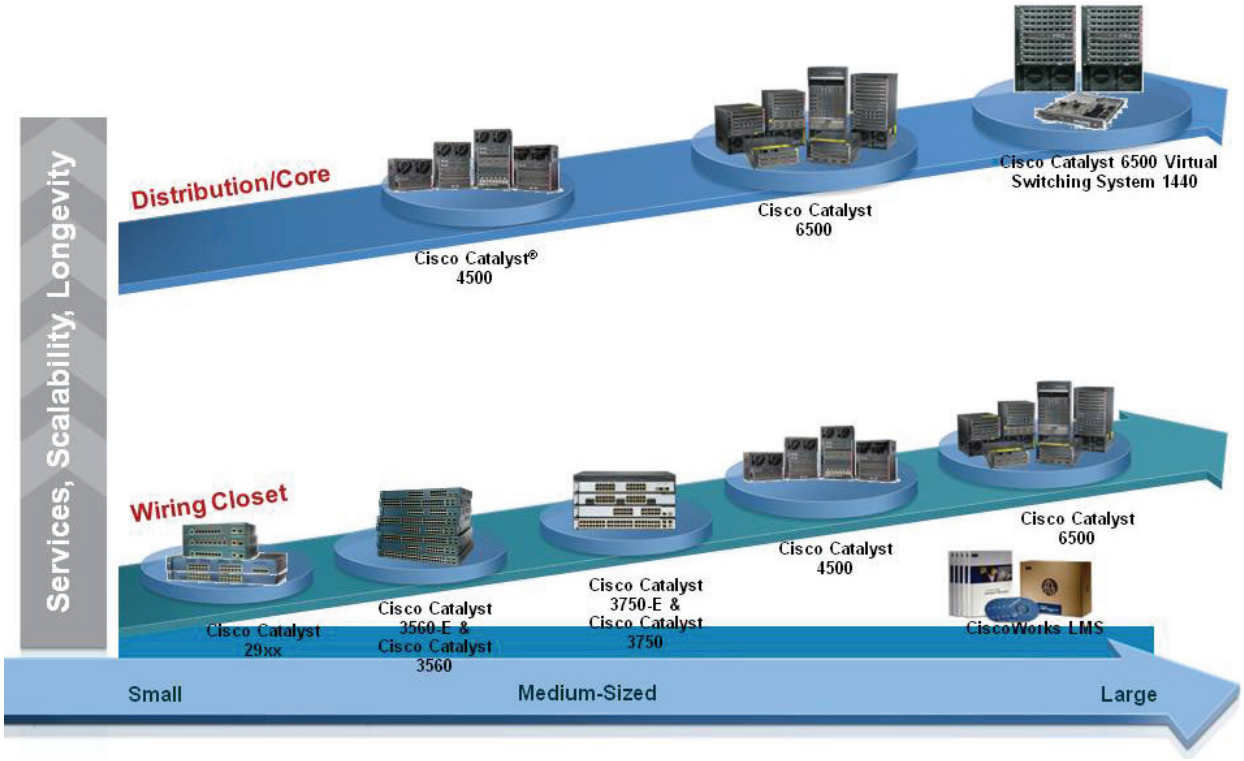
- **Assessment:** The first task in any comprehensive security plan requires technology for assessing risk within the existing infrastructure. The topics in this category address approaches, methods, technologies, and tools for evaluating, testing, and measuring security and risk in IT infrastructure components and systems and in the infrastructure as a whole.
- **Prevention:** This category focuses on the set of security capabilities, practices, and processes that are targeted at the prevention of well-known cybersecurity attacks and control of access to resources by valid consumers.
- **Detection:** This action focuses on automatically detecting activity outside the normal bounds of acceptable behavior and activity violating, or potentially violating, the defined security policy.
- **Response and recovery:** The category contains a collection of capabilities that provide automatic protective actions in the face of an attack and capabilities for analyzing and assessing damage as a result of an attack. The capabilities for response are intended to prevent pending attacks and mitigate the effects of an attack in progress in order to minimize damage or restore normal system and network operations. The capabilities for investigation are intended to provide tools and services for analyzing attacks, assessing attack damage, and gathering forensic evidence.

Cybersecurity is not limited to a single portion of the network. An effective cybersecurity plan must be networkwide. Moreover, certain portions of the network will have specific security requirements based on the role the switches and routers play in that security domain. An access-layer switch, for example, will have different security requirements than an Internet router. In the remainder of this document, we will explore the differing places in the network and the security technologies that can be deployed to achieve the goals of assessment, prevention, detection, response, and recovery.

[1] Washington Post, "Obama: Cyber Security Is a National Security Priority," May 29, 2009.

Securing the LAN (Access, Distribution, Core)

The first area for examination is the LAN (as distinguished from the data center, the wide area network [WAN], and remote agency offices). Usually, this portion of the network is constructed from Cisco® Catalyst® Series switches. The Cisco Catalyst Series comes in a variety of form factors, with increasing scalability, performance, and high-touch features as you progress toward the higher end of the series. Figure 1 illustrates the different switches within the series and their typical use within different sized networks.



Prevention in the LAN

The Cisco Catalyst Series switches share many common security characteristics, especially when used as access-layer switches. As this is the portion of the network that provides basic access, either wired or wireless, to the rest of the network infrastructure, establishing user identity, policy, and services are important features. Collectively these capabilities are described as **identity-based network services (IBNS).**

The first component of IBNS is the IEEE 802.1x protocol, a MAC-layer protocol that communicates with a RADIUS server—such as the Cisco Secure ACS to associate the end station with a username and password. The access switch acts as an intelligent mediator for the transaction and enables the user port only upon successful completion of the authentication process. The actual authentication mechanism used is Extensible Authentication Protocol (EAP). EAP is carried in the 802.1x frame, passed through the network by the switched infrastructure, and conveyed to the authentication server.

If the client device supports 802.1x, then the end station replies with its credentials, and the switch forwards that information to the Cisco Secure ACS. If the client does not support 802.1x or does not authenticate, the Cisco Catalyst switches offer several fallback mechanisms for authenticating devices, including MAC Authentication Bypass (authentication via MAC address) and Web Authentication. This provides you with the maximum flexibility in providing a secure identity-based access architecture, while still allowing for devices that might not support 802.1x such as printers or other network devices.

In addition, customers who require providing network access to the hosts when the RADIUS server is not reachable by the switch can designate the hosts connected to a port as critical. Cisco Catalyst 4500 and 6500 Series Switches can grant network access to the hosts by putting the port in the critical-authentication state when the RADIUS server is unavailable. When a RADIUS server becomes available, all critical ports in critical-authentication state will be automatically reauthenticated.

Upon successful authentication, the switch fully enables that port and allows access to the networked resources. Based on the information provided by the Cisco Secure ACS, however, the network can enable other policies. Such policies could include assigning the user to a specific VLAN or setting up specific per-user access control lists (ACLs).

It is this combination of identification with policy that elevates Cisco IBNS beyond simple 802.1x authentication and allows a more comprehensive set of capabilities and restrictions to be applied to the end user. Table 1 illustrates some of the basic security questions that need to be resolved on a per-network-user basis and the technologies used to resolve them.

Table 1 Elements of Cisco Identity-Based Network Services

Questions	Actions Taken
Who are you?	Cisco IBNS uses 802.1X or other authentication methods to authenticate the user.
Where can you go?	Based on authentication, the user is placed in the correct workgroup or VLAN.
What service level do you receive?	The user can be given a per-user access control list to explicitly restrict or allow access to specific resources on the network or given specific QoS priority on the network.
What are you doing?	Using the identity and location of the user, tracking and accounting can be better managed.

Of course, the use of 802.1x or NAC presupposes the existence of a back-end authentication, authorization, and accounting (AAA) server. **The Cisco Secure Access Control Server (ACS)** can serve as an integral part of this overall system. ACS is a scalable, high-performance RADIUS and TACACS+ security server. As the centralized control point for managing network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco information networks.

ACS extends network-access security by combining AAA with policy control from a centralized identity-based networking framework. This combination gives networks greater flexibility, mobility, and security, resulting in user-productivity gains. ACS supports a broad variety of Cisco and other network-access devices, including:

- Wired and wireless LAN switches and access points
- Edge and core routers
- Dialup and broadband terminators
- Content and storage devices
- Voice over IP (VoIP)
- Firewalls
- Virtual private networks (VPNs)

Making sure that the user's identity is verified prior to network access is an important component of the trust and identity system. This helps address the category of prevention.

Assessment in the LAN

Nevertheless, identifying the user solves only part of the problem. Although users might be allowed on the network based on the overall security policy, the computers or devices they are using might not be desired on the network. The pervasiveness of laptop computers and handheld devices has increased worker mobility and productivity. However, these devices are far more likely to become infected with a virus or worm, which might be unintentionally carried into the network environment. There must be a continual assessment of devices before they are allowed on the network.

Cisco Network Admission Control (NAC) is an important part of the Cisco security architecture. Whereas Cisco IBNS verifies the identity of the user, NAC can verify both the identity of the user and the "posture" of the user's device.[2] The Cisco Catalyst switching platforms act in conjunction with the Cisco NAC appliance and agent to form the NAC system. The Cisco NAC Agent collects security state information from multiple security software clients, such as antivirus clients, and communicates this information to the connected Cisco network, where access control decisions are enforced. Application and operating system status, such as antivirus and operating system patch levels or credentials, can be used to determine the appropriate network admission decision.

The switches demand host credentials from the Cisco NAC Agent and relay this information to policy servers, where NAC decisions are made. Based on customer-defined policy, the network enforces the appropriate admission control decision: permit, deny, quarantine, or restrict. These ACLs are configured automatically in the edge switches based on the policy returned to the switch. If clients do not authenticate correctly, they can be placed in the "quarantine VLAN" so that they can update their virus-checking software or client-based security agents. It is possible that, based on 802.1x authentication, the port is enabled, only to be restricted or denied because a device is not considered "safe."

Cisco NAC is an important element in providing ongoing network assessment of new threat vectors. While periodic point-in-time security audits are a recommended best practice for any evolving network, Cisco NAC provides ongoing, dynamic assessment of security status in the intervals between such audits.

Detection in the LAN

While 802.1x and NAC can be very useful in normal network operations, some focus must also be given to anomalous events in the network. Fully authenticated users can still run programs that might threaten security. New viruses, intrusion methods, and other threats are developing every day. How can the network detect and protect itself from the unknown?

Cisco **NetFlow** is an embedded instrumentation within Cisco IOS® Software to characterize network operation. Visibility into the network is an indispensable tool for IT professionals. Cisco NetFlow creates an environment where administrators have the tools to understand who, what, when, where, and how network traffic is flowing. When the network behavior is understood, an audit trail of how the network is utilized is available. Cisco NetFlow has played an important role in the first version of the US-CERT Einstein monitoring system, which is deployed at several U.S. federal agencies[3] This increased awareness reduces vulnerability of the network as related to outage and allows efficient operation of the network.

The ability to characterize IP traffic and understand how and where it flows is critical for network availability, performance, and troubleshooting. Monitoring IP traffic flows facilitates more accurate capacity planning and makes sure that resources are used appropriately in support of organizational goals. It helps IT determine where to apply quality of service (QoS) and optimize resource usage, and it plays a vital role in network security to detect denial-of-service (DoS) attacks, network-propagated worms, and other undesirable network events. Cisco NetFlow can be used for anomaly detection and worm diagnosis along with applications such as the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). Several third-party COTS applications also use Cisco NetFlow to detect and respond to anomalous traffic flows.

[2] Cisco NAC is flexible and interoperable with IBNS. It can be configured to use IBNS to check user identity, or it can check user identity by itself (without IBNS).

[3] The US-CERT Einstein Program is a project that builds cyber-related situational awareness across the federal government. The program monitors government agencies' networks to facilitate the identification and response to cyberthreats and attacks, improve network security, increase the resiliency of critical electronically delivered government services, and enhance the survivability of the Internet. It is a combination of government off-the-shelf (GOTS), COTS, and open source technologies and software.

Cisco NetFlow is supported on the Cisco Catalyst 6500 and 4500 Series switches. Depending on the supervisor engine in use, an additional service module might be required to provide hardware-accelerated NetFlow.

The Cisco Catalyst 6500 Series switch can also play an important role in the detection of new security threats with its comprehensive support of capability-enhancing **service modules**.[4] Service modules provide an integrated services architecture, where security capabilities can be handled in-line with the switches that provide forwarding capabilities. Some benefits of an integrated services model include:

- Scalable and "pay-as-you-grow" designs integrating security with existing and new deployment of technologies, such as data center server load balancing, wireless, IP telephony, and Multiprotocol Label Switching (MPLS) segmentation
- Depth and breadth of security services integrated with the switch in hardware and software to enable "defense in depth" to mitigate increasing complexity of network security threats
- High performance with dedicated hardware acceleration and high availability to meet demands of large and mission-critical environments
- More granular and differentiated control of network access and security at lower TCO with advanced capabilities such as managed virtualization, allowing a single firewall or VPN service module to act as multiple logical devices, each with its own management and policy
- Simplified network operations and management lowering operation costs

Some of the more commonly deployed security-related Cisco Catalyst 6500 service modules are listed in Table 2.

Table 2 Cisco Catalyst 6500 Series Switch Service Modules

Service Module	Capabilities
Firewall Services Module (FWSM)	High-performance firewall with 5.5Gbps throughput per FWSM and up to 20Gbps per chassis; 100,000 connections/sec and 1 million concurrent connections; and up to 256 virtual firewalls with resource management.
IPsec VPN SPA	Provides IPsec VPN services without need for overlay equipment or network alteration. Delivers 2.5Gbps encryption throughput with 3DES and AES, supports 16,000 active tunnels simultaneously.
Network Analysis Module (NAM):	Provides application-level visibility for real-time traffic analysis. Information can be used for VoIP quality monitoring, curbing unproductive network traffic, optimizing WAN bandwidth.
Application Control Engine (ACE):	Provides rich levels of application and network security. Includes bidirectional support for content inspection, SSL encryption/decryption, and transaction logging for application security forensics.

The modular architecture of the Cisco Catalyst 6500 Series switch makes it extremely versatile for positioning anywhere within the network. The functionality provided by these service modules will be further explored when we discuss the data center and the WAN.

[4] Many of the service module capabilities referenced here are also available as standalone Cisco appliances. Ultimately, the choice between an appliance-based or integrated service-based architecture is up to the network designer. To provide customers with the maximum flexibility, Cisco supports both architectures.

Response and Recovery in the LAN

While some security intrusions are meant to gain access to confidential information, others have the much simpler goal of disruption. The sole purpose of distributed-denial-of-service (DDoS) attacks, for example, is to introduce failure. Indeed, any failures, whether malicious or even accidental, disrupt the orderly operation of government and are therefore a national security concern.

This places two additional requirements on the network:

- The ability to continue operating even during the event of a security attack or other system outage
- The need for a sophisticated tool set to quickly analyze, respond to, and remediate an attack or failure while it is in progress

One technology that allows for continued operation even during a system failure is **Cisco Nonstop Forwarding with Stateful Switchover (NSF/SSO).** It allows a switch or router experiencing a failure of an active supervisor to continue forwarding data packets along known routes while the routing protocol information is recovered and validated. Data-plane forwarding can continue to occur even though peering arrangements with neighbor routers have been lost on the restarting router.

NSF relies on the separation of the control plane and the data plane during supervisor switchover. The data plane continues to forward packets based on preswitchover Cisco Express Forwarding information. The control plane implements the graceful restart routing protocol extensions to signal a supervisor restart to NSF-aware neighbor routers, reform its neighbor adjacencies, and rebuild its routing protocol database following a switchover.

An *NSF-capable router* implements the NSF functionality and continues to forward data packets after a supervisor failure. An *NSF-aware router* understands the NSF graceful restart mechanisms: it does not tear down its neighbor relationships with the NSF-capable restarting router and can help a neighboring NSF-capable router restart, thus avoiding unnecessary route flaps and network instability. An NSF-capable router is also NSF-aware.

A further extension of NSF/SSO capabilities is **Cisco In-Service Software Upgrade (ISSU).** ISSU takes the concepts of NSF/SSO and applies them to another source of potential network downtime, software upgrades. A switch or router implementing ISSU will continue to forward packets throughout the upgrade process.

A unique feature of the Cisco Catalyst 6500 Series switch is **Cisco IOS Software modularity**. This capability allows the Cisco Catalyst 6500 Series to offer runtime patching of security updates. This means that there is no downtime when patching security updates and reduced code certification time after the patching.

Because NSF/SSO and ISSU require redundant supervisors, they are limited to the modular switching products, the Cisco Catalyst 6500 and 4500 Series switches.

For Cisco Catalyst fixed switches, Cisco **StackWise**® can help limit the failure domain. Cisco StackWise technology provides a method for collectively utilizing the capabilities of a stack of switches. Individual switches intelligently join to create a single switching unit with a switching stack interconnect. Configuration and routing information is shared by every switch in the stack, creating a single switching unit. All stack members have full access to the stack interconnect bandwidth. The stack is managed as a single unit by a master switch, which is elected from one of the stack member switches.

Master redundancy allows each stack member to serve as a master, providing the highest reliability for forwarding. Each switch in the stack can serve as a master, creating a 1:N availability scheme for network control. In the unlikely event of a single unit failure, all other units continue to forward traffic and maintain operation.

While each of the above technologies plays a part in maintaining the operation of the network during a system failure, there is another aspect of the problem that must be addressed. How can the attacks that are

causing the failure be identified and remediated? To counter these attacks, features are needed that are as flexible as possible, in terms of both classification and mitigation capabilities. While antivirus, intrusion detection, and other capabilities can respond to well-known attacks, there is also a need to quickly take action against new attacks, for which the attack signature might not be known.

Cisco **Flexible Packet Matching (FPM)** provides the means to configure match criteria for any or all fields in a packet's header, as well as bit-patterns within the packet's payload within the first 256 bytes. This allows the characteristics of an attack (source port, packet size, byte string) to be uniquely matched and for a designated action to be taken. FPM provides a flexible Layer 2–7 stateless classification mechanism. The user can specify classification criteria based on any protocol and any field of the traffic's protocol stack. Based on the classification result, actions such as drop or log can be taken.

The offset or depth at which to begin matching can be referenced from several locations in the packet. Some of these locations are dependent upon loading a Protocol Header Definition File (PHDF). FPM can work with well-known, established protocols such as IP, TCP, and UDP (PHDFs for these and other protocols are available for download) or with custom protocols that are described with a user-defined PHDF. The ability to define and dynamically upload protocol definitions to a Cisco switch or router is the key capability here. The attack signature for an Internet virus, worm, or DDoS attack might be identified before security vendors have an opportunity to update their software definitions to defend against the attack. FPM provides the user with the capability to encode that signature in the switch or router on the fly, and be protected while waiting for a more comprehensive solution.

Another technology that increases the flexibility of response to security incidents is Cisco IOS Embedded Event Manager (EEM). A series of event detector processes designed to monitor explicit operational aspects of the switch are built into Cisco IOS Software. They can be primed to look for a specific event, and when that event occurs, they can act as a trigger to start up a user-loaded script. That script can then be invoked to perform a series of actions to remedy, troubleshoot, or facilitate a set of actions. This unique capability, which is integrated into the Cisco Catalyst switching platforms, can significantly enhance the network's operational efficiency and speed the response to security threats.

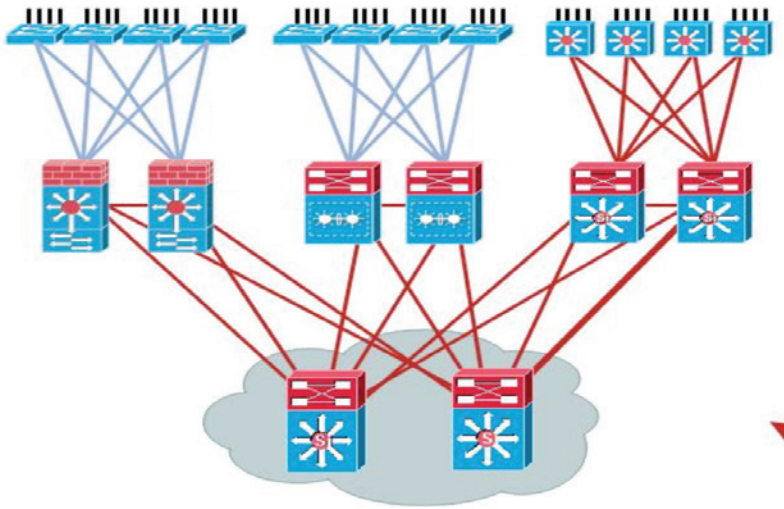
Many Cisco customers are starting to utilize EEM, which has numerous uses that are enabled through its scripting capabilities. The user can define an event (or multiple events) on which EEM should take action: for example, generating a specific syslog message, invoking a specific CLI command, inserting or removing a line card, or having a system resource such as CPU or memory usage cross a threshold to trigger invoking a script. When that event occurs, a script can be invoked to start a series of predetermined actions. The script has the ability to invoke any combination of CLI commands, generate custom Simple Network Management Protocol (SNMP) traps or syslog messages, conduct email and page alert network operations, and more. Its abilities are only limited by the imagination of the administrator. The power of EEM is now available across both the Cisco Catalyst 6500 and 4500 modular switching platforms as well as the Cisco Catalyst 3750 family of switches.

Before moving on to other areas of the network, it should be noted that the technologies discussed above are just part of the rich portfolio of security capabilities of Cisco Catalyst Switches. Table 3 calls out some additional capabilities on Cisco Catalyst Series switches which can be used to provide network security. Some of these capabilities will be discussed further in subsequent sections. Figure 2 maps specific technologies to places in the network where they would likely be deployed.

Table 3 Additional Cisco Catalyst Security Capabilities

Capability	Description
DHCP Snooping	Build a table connecting IP address to the MAC address of each client. This table is used by the next two features to prevent man-in-the-middle attacks.
Dynamic ARP Inspection	Consults DHCP snooping table to prevent hackers from tampering with the switch ARP table.
IP Source Guard	Consults DHCP snooping table to prevent hacker from using spoofed IP address.
Private VLAN	PVLAN provides the capability to insulate one user from another. It provides enhanced Layer 2 security for data centers, wiring closets, and Metro Ethernet deployments.
Control Plane Policing	Control plane rate limiters and policers are hardware based and will limit traffic directed to the CPU to mitigate denial-of-service attacks.
Dedicated TCAM for Access Controls Lists (ACL)	Shared TCAM space can lead to ACL overflow. ACL overflow triggers software-based forwarding and severely downgraded performance. The Cisco Catalyst 6500 Series provides extensive ACL capability with 32K dedicated TCAM space. Chances of ACL overflow minimized.
Hardware-based MAC learning	For switches that learn MAC addresses in software, a hacker can generate thousands of bogus MAC addresses and dominate the CPU. The Cisco Catalyst 6500 Series learns MAC addresses in hardware and is not susceptible to such DoS attacks.
Multipath uRPF	Typical DoS attacks start with address spoofing. Multipath unicast RPF prevents source address spoofing by doing reverse path forwarding checks on packets, even when there are multiple paths leading to the source.
User-Based Rate Limiting	To prevent a user from using too many network resources, dynamically learn traffic flows and rate limit each unique flow in hardware.
Broadcast suppression	A hacker can flood a network with broadcast traffic and bring it down to an unusable state. The Cisco Catalyst 6500 Series provides a set of flood control tools—traffic storm control, unknown unicast flood blocking, and unicast flood protection—to protect the network from such DoS attacks.
Cisco Security Manager	Provides security managers a centralized security management tool to manage Cisco Security products, including the Cisco Catalyst 6500 Series secure ACLs, VLANs, and PISA flexible packet matching polices.
AutoSecure	AutoSecure saves security managers considerable time by automatically setting a standard security policy on the switch, thereby quickly bringing the entire network to a security baseline.

Figure 2 Security Capabilities for Different Places in the Network



Access
- Network Access Control
- 802.1x/IBNS
- Firewall Services Module
- Flexible Packet Match
- DHCP Snooping/ARP/IP Source guard
- Multipath uRPF
- StackWise

Distribution
- Netflow
- Network Analysis Module
- NSF/SSO
- ISSU

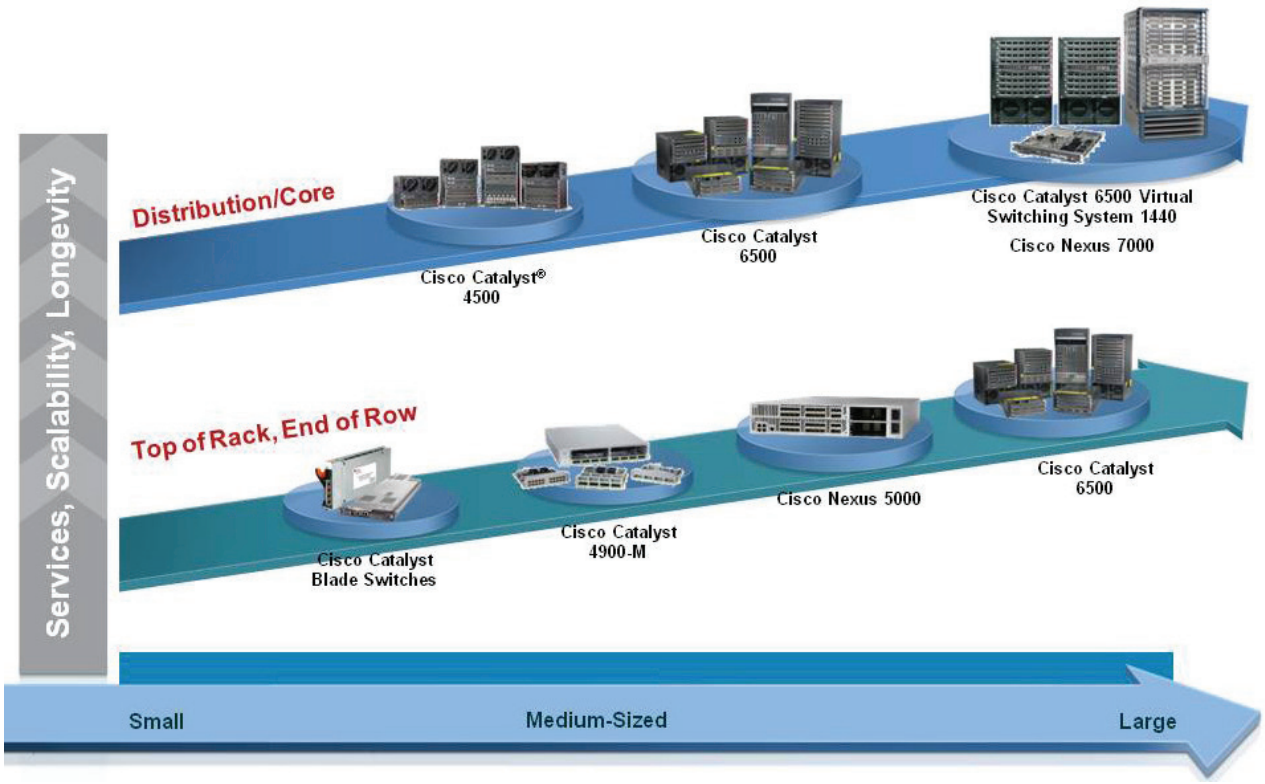
Core
- NSF/SSO
- ISSU

End-to-End
- Embedded Event Manager
- Control Plane Policing
- Cisco Security Manager
- AutoSecure

Securing the Data Center

As with the LAN, Cisco offers multiple platform choices in the data center, with varying form factors, performance levels, and capabilities. Performance ranges from the 320 Gbps available on the Cisco Catalyst 4500 Series switch, through 1.4 terabits on the Cisco Catalyst 6500 Virtual Switching System (VSS) and all the way up to 15 terabits and beyond with the Cisco Nexus 7000 Series switch. (See Figure 3.)

Figure 3 Data Center Platforms



Prevention in the Data Center

No discussion of the data center would be complete without consideration of **virtualization**. Virtualization of servers in the data center was designed as a method to combat the rising space, energy, and management costs of deploying multiple single-purpose servers. However, as virtualization becomes more prevalent, it soon became apparent that it could also provide a security purpose. If servers are virtualized to provide different services on a per-user-group basis, the network infrastructure could also be divided to maintain that separation within the data center, and indeed across the entire LAN.

There are many methods for providing virtualization of the LAN infrastructure, and proper selection of a single method, or even constructing a hybrid architecture integrating multiple methods, will depend on the capabilities of the individual platforms and the purpose of the overall design.

The Cisco Nexus 7000 Series switch has been extended to support the notion of virtual device contexts (VDCs). A VDC can be used to virtualize the device itself, presenting the physical switch as multiple logical devices. Within that VDC, it can contain its own unique and independent set of VLANs and virtual routing and forwarding (VRF) instances. Each VDC can have physical ports assigned to it, thus allowing for the hardware data plane to be virtualized as well. Within each VDC, a separate management domain can manage the VDC itself, thus allowing the management plane itself to also be virtualized.

VDCs on the Cisco Nexus 7000 can connect to individual VLAN or VRF contexts on both the server and network infrastructure sides. Traffic for individual virtual machine instances on the servers is segregated from other traffic, even traffic on the same physical machine. This provides privacy for the data, as well as isolating each context from attacks that might occur in other device contexts.

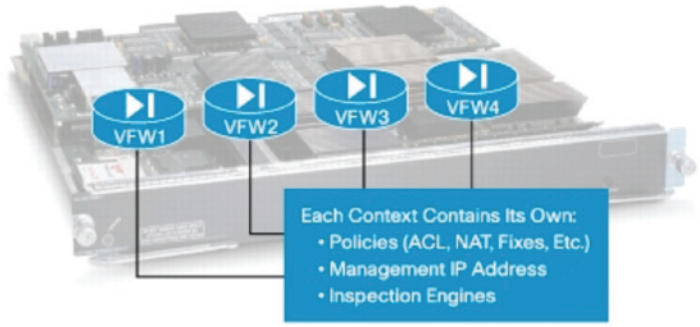
If you want to extend this virtualization by user group further into the network, the VDCs on the Cisco Nexus 7000 Series switch can interoperate with the Cisco Catalyst Series switches. Thus, the VDC could be mapped into MPLS contexts on the Cisco Catalyst 6500 series switch or into VLANs or VRFs, available across the entire Cisco Catalyst Switching Series. [5]

[5] The Cisco Nexus 7000 series switch also supports VLANs and VRFs within a single device context. VDCs are not required for virtualization, but do provide the added benefit of physical hardware isolation.

Assessment in the Data Center

Virtualization becomes even more important when combined with the virtual services capabilities of the FWSM for the Cisco Catalyst 6500 Series switch. A single FWSM can be partitioned into a maximum of 250 virtual firewalls (security contexts) in FWSM 3.1, allowing you to implement policies for different user groups or functional areas (such as DMZs) over the same physical infrastructure. This reduces the cost and complexity of managing multiple devices. The Resource Manager helps ensure high availability by limiting resource usage per context. Role-based management allows multiple IT owners to configure and manage network and application-layer security policies. (See Figure 4.)

Figure 4 FWSM Virtual Firewalls



The Cisco FWSM provides industry-leading 100,000 connections per second, 5 Gbps throughput, and 1 million concurrent connections. Up to four FWSMs can be deployed in the same chassis for a total of 20 Gbps throughput. A single FWSM can support up to 1000 virtual interfaces (256 per context), and a single chassis can scale up to a maximum of 4000 VLANs. Full firewall protection is applied across the switch backplane, giving the lowest latency figures (30 microseconds for small frames) possible. FWSM is based on high-speed network processors that provide high performance but retain the flexibility of general-purpose CPUs.

The business cases for virtualized, firewalled user groups in the federal government are many:

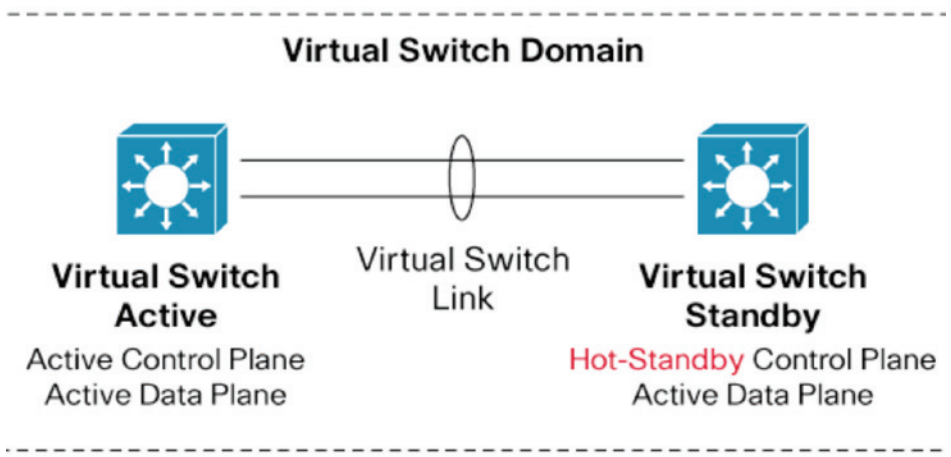
- Differentiating access to information between federal employees, contractors, and the general public
- Limiting access to national security-related material
- Complying with standards on information security
- Protecting confidential information such as social security numbers or health-related data

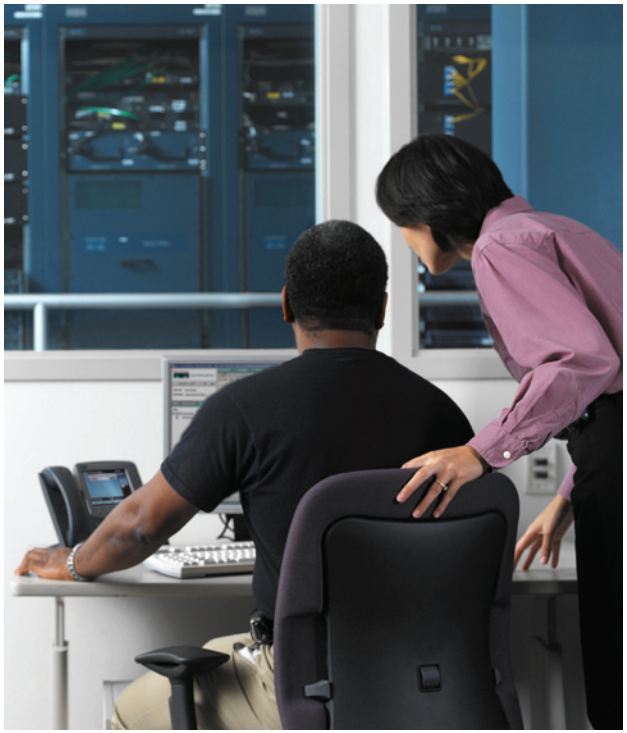
Response and Recovery in the Data Center

The concept of virtualization just discussed is a one-to-many model, where a single physical resource is made to look like many logical resources. Another important innovation for the data center is the reverse concept, making multiple physical resources look like one logical resources. This can be accomplished with the **Virtual Switching System (VSS) 1440** for the Cisco Catalyst 6500 Series switch.

The initial release of VSS 1440 allows for the merging of two physical Cisco Catalyst 6500 Series switches together into a single, logically managed entity. The key enabler of the Cisco Virtual Switching System technology is a special link that binds the two chassis together, called a Virtual Switch Link (VSL). The VSL carries special control information and encapsulates every frame with a header that passes across this link. (See Figure 5.)

Figure 5 Logical Architecture of Virtual Switching System





The primary benefits of this logical grouping include:

- Increased availability and resiliency using interchassis SSO and NSF
- Increased operational efficiency of a simplified network architecture using virtualization
- Increased forwarding performance using Multichassis EtherChannel (MEC)

Detection in the Data Center

One common design element in some data center architectures is to route all critical traffic (or, depending on traffic volumes, *all* traffic) through a **services switch**[6]. Typically this would be a Cisco Catalyst 6500 Series switch, with multiple services modules.

In addition to the FWSM (discussed above), some other capabilities supplied by the services switch might include:

- **Network Analysis Module (NAM):** provides traffic monitoring services for visibility into network and application usage, helping network managers troubleshoot delivery issues, improve the utilization of network resources, and ease the deployment of new network services. It includes an embedded, web-accessible Traffic Analyzer interface that presents both configuration menus and real-time and historical reports. It also offers web-based captures and decodes for anytime, anywhere troubleshooting.
- **Application Control Engine (ACE) Module:** Although more often thought of as an application acceleration tool, the ACE module can also serve a security purpose. First, by acting as a front end for a server farm, it effectively hides the true IP addresses of the servers from both internal and external clients in the network. Second, its server load-balancing capabilities, as well as off-load application acceleration, provide greater levels of resiliency to the server farm.
- **Secure Sockets Layer Service Module (SSL-SM):** offloads processor-intensive tasks related to securing traffic, increasing the number of secure connections supported by a website, and reducing the operational complexity of high-performance web server farms. The SSL-SM simplifies security management while encrypting user data to the web servers, providing privacy, confidentiality, and authentication using a wide range of certificates, including Netscape and VeriSign.
- **Encapsulated Remote Switched Port Analyzer (ERSPAN):** is an embedded capability within the Cisco Catalyst 6500 Switch that mirrors traffic across the network to a central location, where it can be analyzed. Because the mirrored traffic is encapsulated in IP, it can cross Layer 3 boundaries and be directed anywhere in the network. This can significantly increase the speed and flexibility of troubleshooting security problems. This technology can also be used to redirect traffic to security devices such as intrusion detection systems (IDSs).

The Cisco SAFE blueprint for network security also provides detailed configuration guidance on how to provide a security architecture using Cisco standalone security appliances. In many cases, operational administration of security within an IT department is a separate role from network operations. For this and other reasons, customers have the flexibility to deploy security as an integrated service within the switches/routers, as a standalone appliance, or as a hybrid of the two approaches. Some of the most commonly deployed Cisco security appliances include:

- **The Cisco ASA 5500 Series Adaptive Security Appliances:** The Cisco ASA 5500 Series converges best-in-class firewall, IPS, network antivirus, and VPN services to deliver application security, user- and application-based access control, worm/virus mitigation, spyware protection, and remote user/site connectivity. This convergence of market-proven technologies provides a proactive threat mitigation that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. Intrusion protection can be integrated with the firewall and VPN functionality or be separated out through the deployment of the **Cisco IPS 4200 Series Sensors.**
- **Cisco ACE 4700 Series Application Control Engine Appliance:** Manages up to 4 Gbps of application traffic in a one-rack-unit (1RU) form factor and is upgradable through software licenses. Its innovative virtualization and role-based access control capabilities enable IT to provision and deliver a broad range of multiple applications from a single Cisco ACE appliance, bringing increased scalability for application provisioning to the data center. The Cisco ACE 4710 greatly improves server efficiency through highly flexible application traffic management and the offloading of CPU-intensive tasks such as Secure Sockets Layer (SSL) encryption and decryption processing, HTTP compression, and TCP session management. The Cisco ACE

[6] There are many options for designing a services switch. For design considerations, including advice on optimal traffic redirection and high availability, see www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/dc_servchas/service-chassis_design.html#wp58610.

platform is designed to serve as a last line of defense for servers and applications in data centers. The Cisco ACE appliance performs deep packet inspection and blocks malicious attacks.

- **IronPort Email and Web Security Appliances:** By reducing the downtime associated with spam, viruses, and blended threats, IronPort email security appliances improve the administration of email systems, reduce the burden on technical staff, and provide state-of-the-art network protection. IronPort email security appliances provide a multilayer approach to stopping email-based threats. For spam protection, email and web reputation filtering technology is combined with Cisco IronPort Anti-Spam. Cisco IronPort Virus Outbreak Filters are paired with fully integrated traditional antivirus technology to enable powerful virus defense. Cisco IronPort PXE encryption technology fulfills secure messaging, compliance, and regulatory requirements.

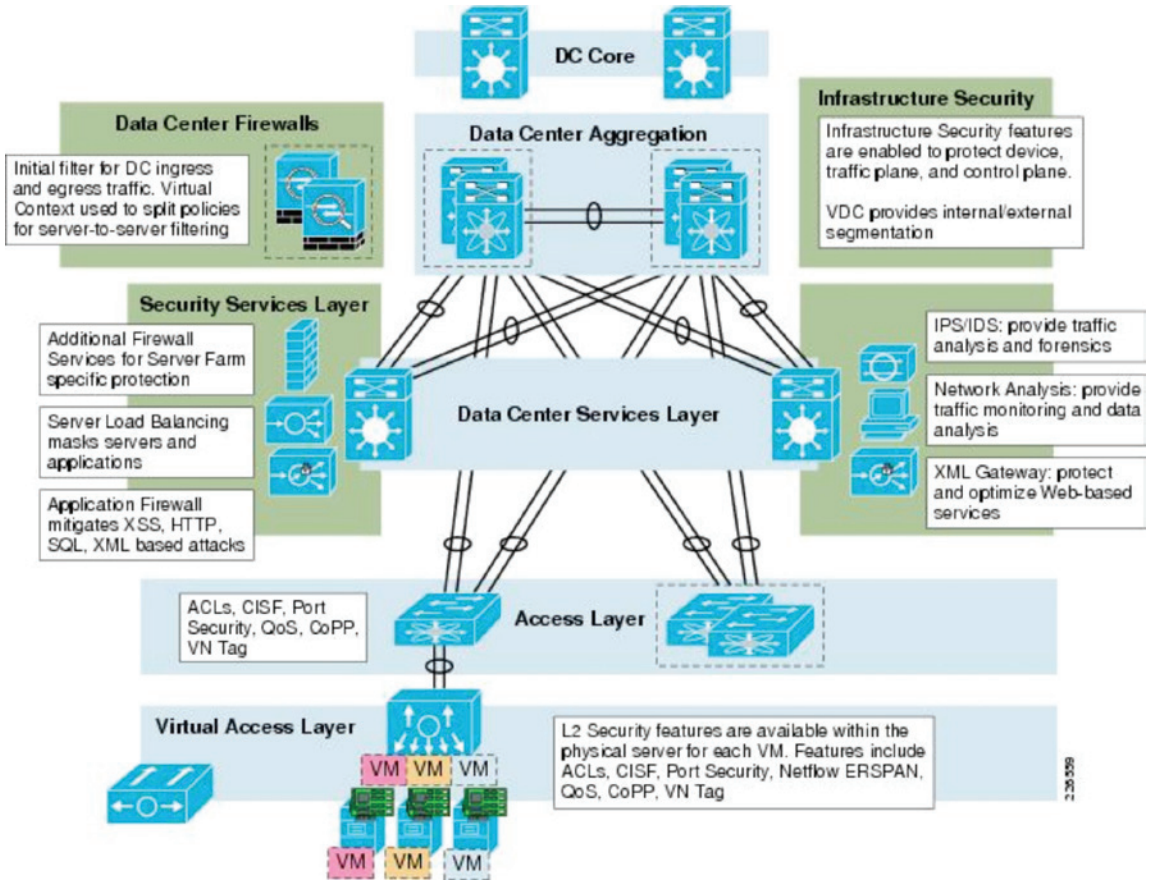
As the data center is where most of the valuable data sources in a network reside, providing security in the data center extends beyond preventing cyberattacks. It also requires providing a stable and highly resilient infrastructure. Table 4 contains a list of additional technologies that should be considered for deployment in the data center to help increase the availability and security of data center assets.

Nor should it be forgotten that the data center is also susceptible to the same sorts of threats detailed in the "Securing the LAN" portion of this document. Figure 6 illustrates a typical data center with appropriately deployed security services. Depending on the requirements, the data center services layer could be collapsed into a pair of redundant service switches.

Technology	Benefit
NSF/SSO for Multicast	The Cisco Catalyst 6500 Series Switch can extend its NSF/SSO support (discussed earlier) to include extremely fast recovery for multicast streams.
Protocol Independent Multicast (PIM) Register Accept	Prevents unauthorized sources from initiating multicast streams on a network. Avoids multicast spoofing.
Hot Standby Router Protocol	One of several first-hop routing protocols (alongside Virtual Router Redundancy Protocol [VRRP] and Gateway Load Balancing Protocol [GLBP]) that provide redundant and resilient paths for data exiting the data center. A typical deployment would be to have parallel routers or switches front-ending the server farm.
Portfast BPDU Guard Unidirectional Link Detection Loop Guard Root Guard Multiple Spanning Tree (IEEE 802.1s) Rapid Spanning Tree (IEEE 802.1w)	A suite of protocols designed to provide better stability, scalability, and faster convergence for the Spanning Tree Protocol in the Layer 2 portion of the data center.
IP SLA Tracking	Cisco IP SLAs can be used to monitor the availability of devices or services in the data center (or at other places in the network as required). The tracking feature of IP SLAs allows it to communicate availability failures to other protocols such as HSRP or EEM and to take user-defined corrective actions.

Table 4 Additional Data Center Technologies

Figure 6 Data Center Security Technologies

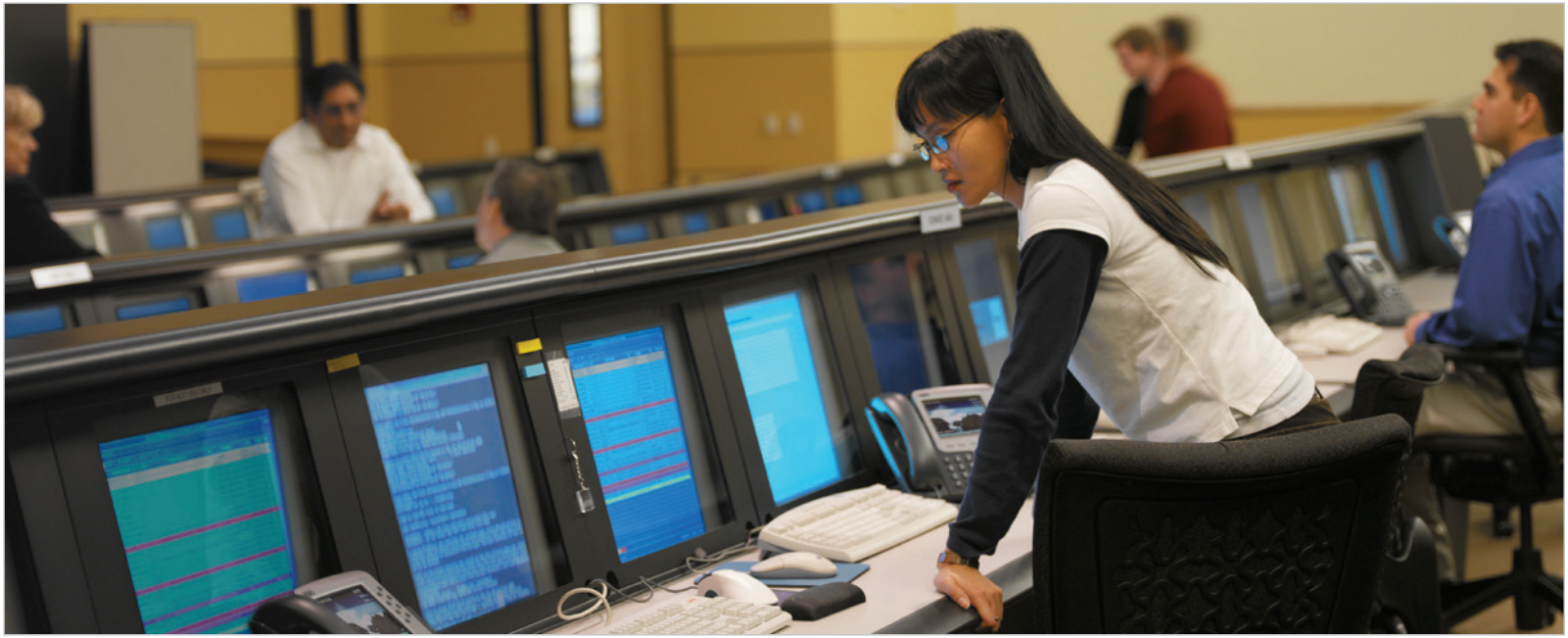


Securing the WAN and Remote Agency Offices

The WAN in a federal installation will serve multiple purposes:

- To prove headquarters access to smaller remote agency offices
- To provide secure incoming access via the Internet or dedicated lines to associated business partners and contractors
- Connecting geographically remote data centers across the WAN
- To act as one of the prime mechanisms for citizen access to information and services [7]

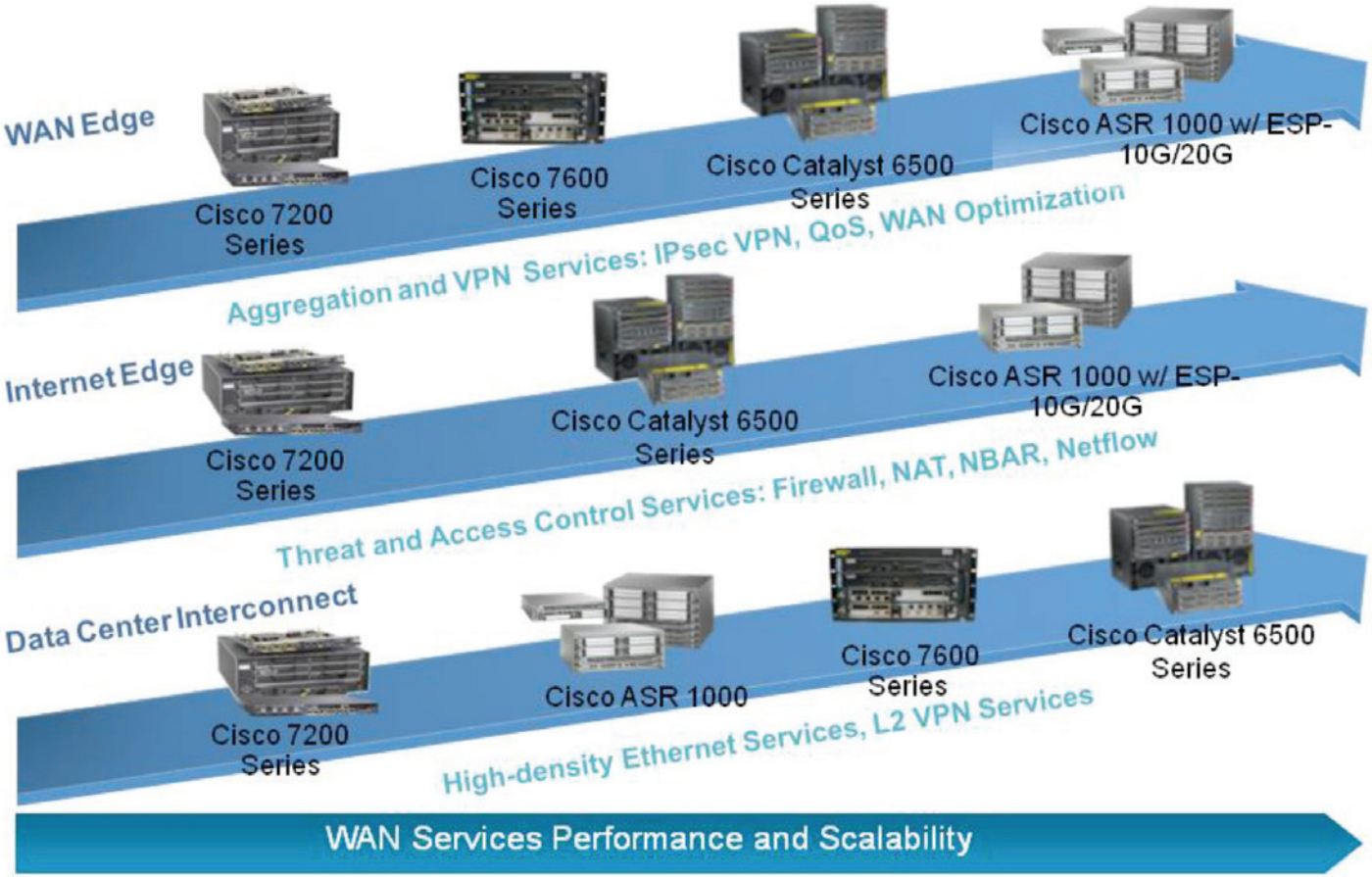
All of these are necessary functions, but providing such openness also requires security controls in place to assure that it is not abused. There are several different areas that need to be examined here, including the headquarters aggregation router/switch, the architecture of the remote agency office, and the Internet portal.



[7] Although one or more of these functions can be combined within a single switch or router, the Trusted Internet Connection (TIC) initiative, part of the Cyber Defense project, will likely separate out the Internet process as a discrete design element.

Figure 7 illustrates the portfolio of switches and routers that might be typically be used at a headquarters site or a large remote agency site for providing wide area connectivity. As we have seen before in each place in the network, Cisco provides a scalable range of platform choices to accommodate different requirements for speed, scalability, and services.

Figure 7 Headquarters Switches and Routers



Prevention in the WAN

In addition to incorporating all of the security services mentioned in previous sections, the emphasis for the headquarters router/switch is twofold:

- To provide highly scalable VPN and encryption services
- To enable high-touch packet services to inspect, identify, prioritize, or reject traffic according to policy

The Cisco ASR 1000 Series Aggregation Services Routers are Cisco's premier WAN routing platforms that represent a dramatic advance in technology innovation based on the company's understanding of evolving customer requirements. These routers set new expectations for industry-leading performance and scalability of embedded services atop a secure, resilient hardware and software architecture and are perfect suited to help provide federal agencies with high-performance WAN services in a secure and resilient manner.

A key functionality of the ASR 1000 Series router as a WAN routing platform is to provide secure connectivity to remote regional offices and remote users over a private WAN or cost-effective, third-party Internet access. A VPN provides the highest possible level of security through encryption and authentication technologies that protect data traversing the VPN from unauthorized access. In addition to standard remote-access solutions such as MPLS VPN and IPsec VPN, the Cisco ASR 1000 Series also supports innovations such as **Cisco Group Encrypted Transport VPN (GET VPN)**.Cisco GET VPN is a next-generation WAN solution that defines a new category of VPN, one that does not use traditional point-to-point tunnels. This new security model introduces the concept of "trusted" group member routers, which use a common security methodology that is independent of any point-to-point relationship. By eliminating point-to-point tunnels, Cisco GET VPNs can scale much higher while accommodating multicast applications and instantaneous branch office-to-branch office transactions. (See Figure 8.)

Figure 8 Cisco Group Encrypted Transport VPN

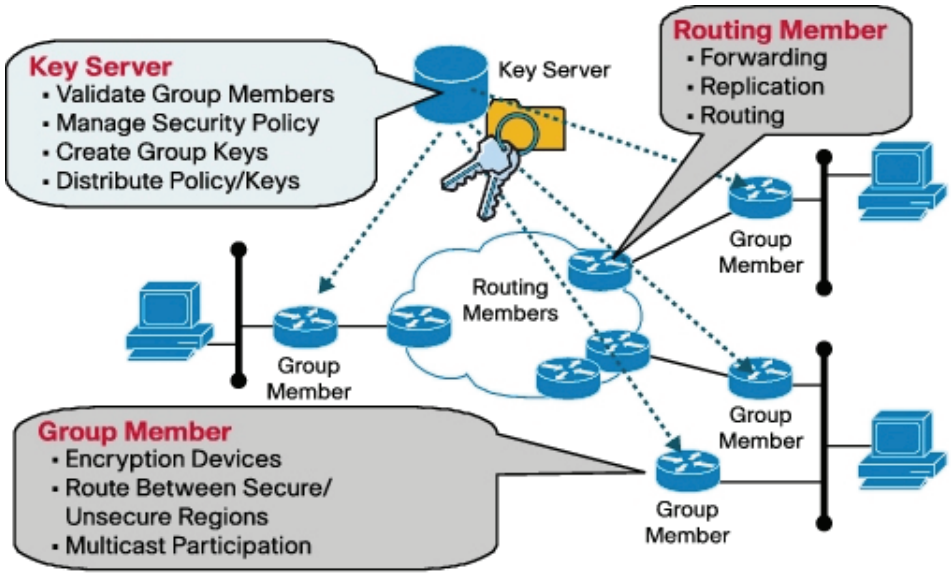


Table 5 lists some of the other key features that Cisco's ASR 1000 Series routers support to provide site-to-site or remote-access secure WAN connectivity.

Table 5 Secure WAN Connectivity Technologies

Secure VPN Connectivity Features	Description and Benefits
IPsec	IPsec standards supported include Digital Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES; 128, 192, and 256) for encryption; Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication; and Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity. With the built-in cryptographic engine in the ESP, the Cisco ASR 1000 Series Routers can deliver up to 7-Gbps IPsec throughput.
Hardware QoS	A dedicated QoS chip within the QuantumFlow Processor facilitates traffic shaping and policing functions for thousands of VPN spokes, as well as Low Latency Queuing (LLQ) before and after cryptography, all aimed at preserving quality of voice and real-time data.
Hardware IP Multicast handling	A powerful multicore cryptography engine with an extensive 2-Gb buffer, along with sophisticated full-circle back-pressure mechanisms between the cryptography engine and process engine, solving historical burst problems associated with high-scale IP multicast.
Cisco Easy VPN and Enhanced Easy VPN	Providing advanced value-add to IPsec standards, these features ease administration and management of point-to-point VPNs by actively pushing new security policies from the central headend router to remote sites. Enhanced Easy VPN features integrate with dynamic VTI for maximum ease of use and advanced per-user and tunnel-specific capabilities.
Dynamic Multipoint VPN (DMVPN)	This Cisco innovation for site-to-site VPNs provides a scalable and flexible way to establish virtual full-meshed IPsec connectivity between multiple locations. DMVPN features advanced spoke-to-spoke capabilities that enhance the performance of latency-sensitive voice applications. For the traditional hub-and-spoke model, DMVPN significantly reduces deployment complexity.
Group Encrypted Transport VPN	Group Encrypted Transport VPN eliminates the need for compromise between network intelligence and data privacy in private WAN environments. Service providers can finally offer managed encryption without a provisioning and management nightmare because Group Encrypted Transport VPN simplifies the provisioning and management of VPN. Group Encrypted Transport VPN defines a new category of VPN, one that does not use tunnels.
Virtual Tunnel Interface (VTI)	You can configure these virtual interfaces directly with IPsec. VTI greatly simplifies VPN configuration and design over alternatives such as encapsulating IPsec inside generic routing encapsulation (GRE). It allows for per-user attributes and tunnel-specific features, offering administrators greater flexibility to respond to granular requirements. Both static and dynamic VTI are supported.

Both the **Cisco ASR 1000 Series Aggregation Services Router** and Cisco Catalyst 6500 Series Switch provide excellent scalability for VPN termination. The Cisco ASR 1000 Series Router can be configured with an Embedded Services Processor (ESP) providing up to 20 Gbps of forwarding with services enabled. It also has an onboard encryption engine that can provide up to 7 Gbps of hardware accelerated encryption.

The modular architecture of the Cisco Catalyst 6500 Series switch allows it to provide VPN, IPSec, and AES encryption with the help of the Cisco VPN Services Port Adapter (VSPA). Each VSPA supports up to 8 Gbps of AES IPsec throughput. Up to 10 VSPAs can be placed in a Cisco Catalyst 6500 chassis, providing a platform for very high-density VPN aggregation.

Although IPSec and AES 256-bit encryption is usually deployed for VPN sessions transiting the Internet, government agencies that handle highly confidential information, such as the Social Security Administration, Health and Human Services, and the Department of Veterans Affairs, might also want to encrypt traffic going site to site across a private network provided by a service provider. Although such networks are already highly secured, this added element to preserve privacy of information is recommended.

For large-scale secure networks, **Public Key Infrastructure (PKI)** provides you with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information. Every entity (a person or a device) participating in the secured communication is enrolled in the PKI in a process where the entity generates a Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has its identity validated by a trusted entity (also known as a certificate authority or trustpoint). A Cisco router or switch can act as a certificate authority, if you want to manage your own certificates.

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a certificate authority. When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

In practice, PKI has two key benefits:

- PKI allows centralized management of encryption keys, making the task of managing multiple remote agency offices much simpler.
- PKI makes it very difficult for hackers to spoof being an approved remote agency office, as they would need to know both the public and private keys and obtain a certificate. This will prevent most types of brute force attacks.

PKI also features the dynamic renewal and revocation of certificates that enables the dynamic commissioning and decommissioning of remote agency offices with ease. The Cisco ASR 1000 Series router also forms a key part of the **Cisco Virtual Office solution**. The Cisco Virtual Office solution provides secure, rich network services to workers at locations outside of the traditional corporate office, including teleworkers, full- and part-time home-office workers, mobile contractors, and executives. The Cisco WAN routers provide VPN convergence, terminating different VPN endpoints, devices, and technologies on a single device. In addition, the headend architecture includes Cisco Security Manager, Cisco Secure Access Control Server (ACS), and the Cisco Configuration Engine. Together, these features incorporate the ability to define networkwide policy, use identity for authorization, and actively update configurations at remote sites through a zero-touch deployment model.

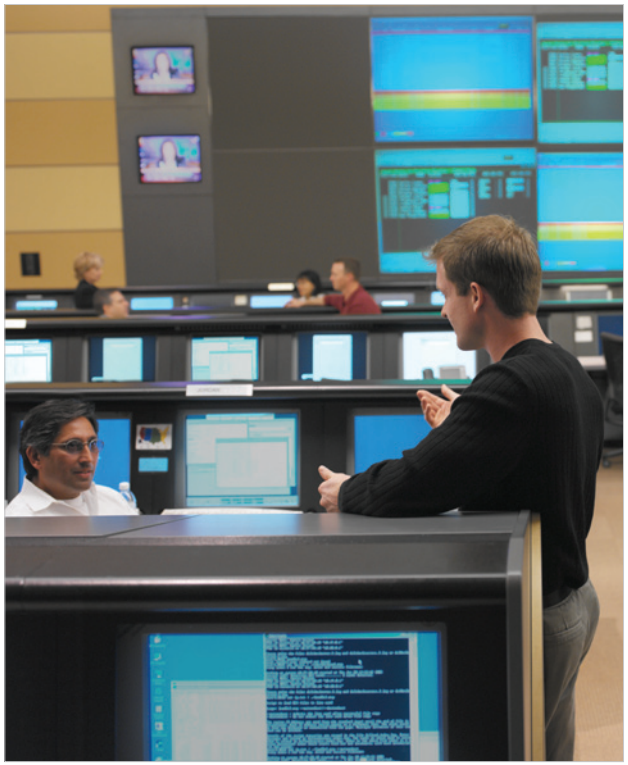
Assessment in the WAN

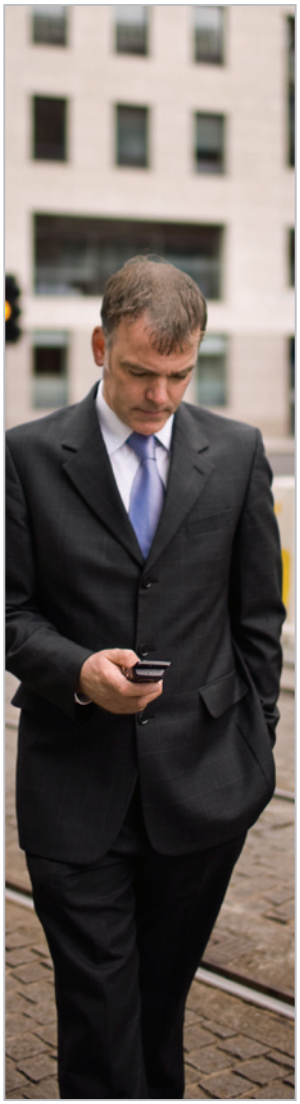
With many remote agency offices, and without dedicated security administrators at each office, providing consistent security policies throughout the WAN can be a challenge. **Cisco AutoSecure** provides vital security requirements to networks by incorporating a straightforward "one touch" device lockdown process. Cisco AutoSecure enables rapid implementation of security policies and procedures to simplify the security process, without having to understand all the Cisco IOS Software features and execute each of the many command line interface (CLI) commands manually. This feature uses a single command that instantly configures the security posture of routers and disables nonessential system processes and services, thereby eliminating potential security threats.

- Disabling often unnecessary and potentially insecure global services
- Enabling certain services that help further secure often necessary global services
- Disabling often unnecessary, and potentially insecure interface services, which can be configured on a per interface level
- Securing administrative access to the router
- Enabling appropriate security-related logging

With highly sensitive and confidential information such as national security-related information, social security numbers, and health-related data traversing your WAN, having a highly reliable firewall at your WAN edge is critical in keeping unauthorized visitors from accessing valuable and highly confidential resources. Instead of providing only point products that set a base level of security, Cisco embeds network firewall security throughout the network and integrates security services in all its products. As a result, network firewall security becomes a transparent, scalable, and manageable aspect of your federal infrastructure.

A key such firewall functionality for your WAN edge on the Cisco ASR 1000 Series Routers is the **Cisco IOS Zone-Based Firewall**, which performs multigigabit stateful firewall inspection, facilitating an ideal single-box security and routing solution for protecting the WAN entry point into the network. The firewall service is embedded in the Cisco QuantumFlow Processor within the Cisco ASR 1000 Series Routers: no additional firewall blades or modules are required. Simultaneously, the system can perform other functions such as QoS, IPv4, IPv6, NetFlow, and so on at multigigabit speeds.





Primary Cisco IOS Firewall features supported follow:

- Zone-based policies: Zone-based policies allow the Cisco ASR 1000 Series Router to act as a barrier between any interfaces that are not members of the same zone. Packets are not forwarded unless explicit zone-pair policies are specified in each direction, between each zone pair. The policy is written using Cisco Policy Language (that is, Modular QoS CLI [MQC]) and establishes the type of stateful inspection and session parameters that apply to each zone pairing.
- Multigigabit performance: The architecture delivers firewall and NAT performance up to 20 Gbps with routing, QoS, and other common Cisco IOS Software features enabled.
- In-box high availability: The Cisco ASR 1006 supports hardware redundancy by supporting redundant route processors and ESPs within the chassis. When a fault occurs on the active route processor or ESP, the hot standby component picks up the processing with nearly zero packet loss. All firewall and NAT sessions are preserved during this process. The Cisco ASR 1002, Cisco ASR1002-F, and ASR 1004 provide software redundancy capabilities by running dual Cisco IOS Software images, one running as active and the other as standby, in a single route processor. When a fault occurs in the active image, the hot standby image picks up the process, and all firewall and NAT sessions remain established.
- Advanced protocol inspection for voice, video, and other data applications
- Per-interface or per-subinterface security policies
- Per-subscriber firewall: This solution is deployed on the Cisco ASR 1000 Series as the L2TP Network Server (LNS). This feature integrates the Cisco IOS Zone-Based Policy Firewall with the Cisco ASR 1000 Series rich broadband feature set to enable Internet service providers to offer firewall services to their broadband subscribers.
- Role-Based CLI Access: This feature provides the network administrator to define different views depending on the roles of users who need access to the router. Each view includes a subset of all Cisco IOS Software CLI commands accessible to the user of a particular role, such as network operator and security operator.

Understanding, classifying, and prioritizing high-value traffic is another important function of a WAN router. **Network-Based Application Recognition (NBAR)** is an integrated classification engine in Cisco IOS Software that can recognize a wide variety of applications, including web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality-of-service (QoS) features to help ensure that the network bandwidth is best used and that important applications can be prioritized.

Both the Cisco Catalyst 6500 Series Switch and the Cisco ASR 1000 Series Router have accelerated support for NBAR in hardware.

Detection in the WAN

While it is important to recognize and prioritize good traffic, it is also necessary to recognize and drop suspicious traffic. **Unicast Reverse Path Forwarding (uRPF)** offers a dynamic technique for enabling ingress traffic filtering, discarding packets with invalid source IP addresses based on a reverse-path look-up. uRPF is a highly attractive alternative to traditional ACLs, which typically demand significant management overhead and have a greater effect on device performance. uRPF is typically deployed as an edge technology in order to be most effective, minimizing the valid IP address space range and enforcing the discard of anomalous packets as close to their origin as possible.

The key function of uRPF is to verify that the path of an incoming packet is consistent with the local packet forwarding information. This is achieved by performing a reverse path look-up (hence the feature's name) using the source IP address of an incoming packet in order to determine the current path (adjacency) to that IP address. The validity of this path determines whether uRPF will pass or drop the packet. If the path is valid, the packet will be passed. If the path is not valid, the packet will be silently discarded (unless an ACL exemption is configured).

uRPF is a useful defense against an IP Source Spoofing attack, wherein a packet from the Internet is specially crafted to have a source address within the range of the local Intranet.

A key use of uRPF, independent of its deployment mode, is to enable **source-based remote triggered black hole (SRTBH)**. SRTBH is a highly effective, dynamic, and highly efficient rapid reaction attack tool to mitigate DDoS attacks. RTBH uses routing protocol updates to manipulate route tables at the network edge or anywhere else in the network to specifically drop undesirable traffic before it enters the service provider network.

Most of the other detection technologies discussed previously such as NetFlow, ERSPAN, DDoS detection, and protection are supported on Cisco WAN platforms to provide a comprehensive integrated threat detection solution.

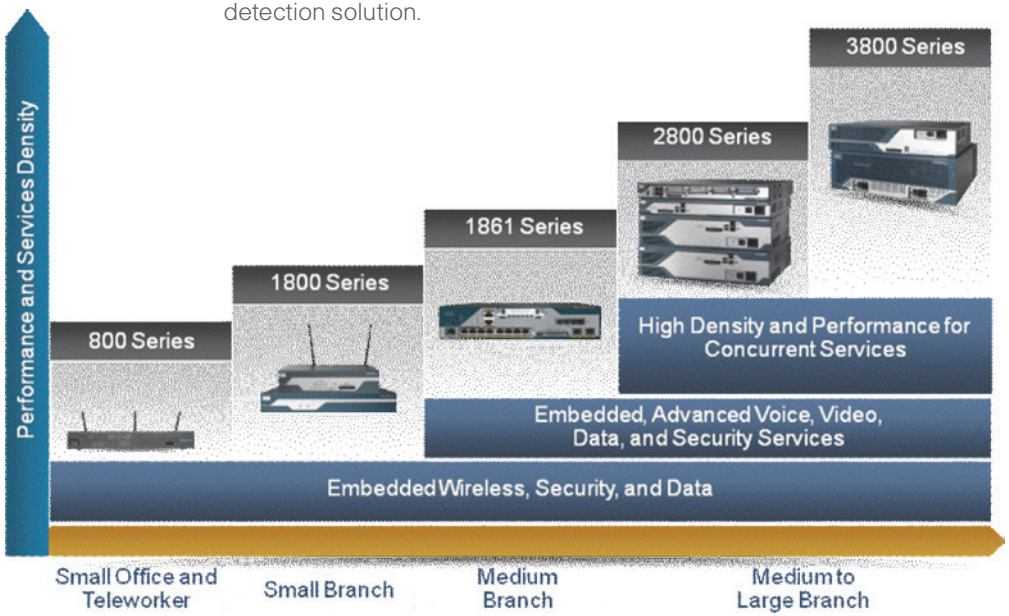


Figure 9 Cisco Integrated Services Router Series

Recovery in the WAN

Many of the recovery technologies previously discussed, such as NSF/SSO, ISSU, FPM, VSS, and EEM, also apply and can be utilized at the headquarters WAN edge, for either Internet or site-to-site remote agency office connectivity. Another problem to solve is the remote agency offices themselves. If they are cut off from the headquarters site, how effectively can they operate in stand-alone mode?

The typical deployment for remote agency offices is a **Cisco Integrated Services Router**, with either a **Cisco EtherSwitch® Service Module** or a Cisco Catalyst Series Fixed switch. Figure 9 shows the different models in the integrated services router portfolio.

The Cisco integrated services routers are known for the capability to easily integrate the functions of standalone network appliances and components into the chassis itself. By integrating multiple branch services into a single platform, the Cisco integrated services router series can help your organization optimize branch services and deliver a consistent user experience with a lower total cost of ownership. Built on a foundation of comprehensive routing and switching management capabilities, Cisco integrated services routers help maximize the power of your organization's network with unified network services, integrated security, mobility, and application intelligence.

One such example of Cisco integrated services router series service integration and recovery is **Survivable Remote Site Telephony (SRST).** This mode helps guarantee call quality and preserves communication locally during network outages, promoting higher availability. This complements other availability features like such as Unified CME autoregistration and Cisco Unified CME DSP-based conferencing. Voicemail and automated attendant services can be delivered directly inside the Cisco integrated services router using Cisco Unity® Express or delivered centrally using Cisco Unity software. Customers can also implement Secure SRST to enable authentication and encryption support for both signaling and media transmission during a WAN outage.

Cisco integrated services routers also offer several other integrated security capabilities to protect voice and unified communications applications. Advanced VPN and Cisco IOS Firewall features deliver secure, high-quality voice and video and protect against call eavesdropping, toll fraud, and DoS attacks. Cisco IOS Firewall also transparently supports voice traffic, including application-level conformance of media protocol call flow and the associated open channels. It supports voice protocols such as H.323v2, v3, and v4; Skinny Client Control Protocol (SCCP); and Session Initiation Protocol (SIP) and assures protection of unified communications components such as Cisco Unified Communications Manager, Cisco Unified Border Element, and their endpoints. By enabling advanced teleworking, these solutions provide business resilience during disasters and pandemics.

Video surveillance is a key component of the safety and security procedures of many federal agencies. It provides real-time monitoring of the environment, people, and assets and provides a recorded archive for investigative purposes. The benefits of Cisco's Video Surveillance Solution include the following:

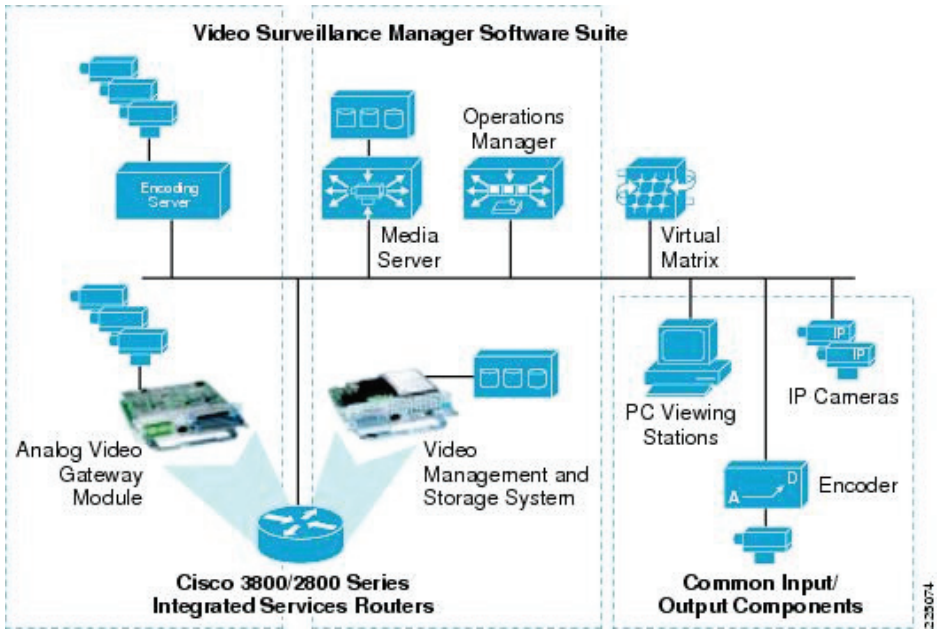
- Provides access to video at any time from any network location within the constraints of available bandwidth, allowing remote monitoring, investigation, and incident response via remote physical security staff or law enforcement personnel.
- Uses existing investment in video surveillance and physical security equipment and technology.
- Networkwide Management—IP cameras and servers are monitored and managed over a single network for fault, configuration, and centralized logging.
- Increased Availability—IP networks offer a high level of redundancy that can extend to different physical locations.
- Scalability—The system can be expanded to new locations as business needs change.
- Digitized images can be transported and duplicated worldwide with no reduction in quality, economically stored, and efficiently indexed and retrieved.
- Employs an open, standards-based infrastructure that enables the deployment and control of new security applications from a variety of vendors.
- The Cisco Video Surveillance Solution relies on an IP network infrastructure to link all components, providing high availability, QoS, performance routing, WAN optimization, and privacy of data through IPSec encryption.

In addition to the standalone dedicated implementation of the Cisco Video Surveillance Solution on Linux servers, the Cisco 2800 and Cisco 3800 integrated services routers support the necessary components of the solution to implement a self-contained instance at the branch location.

The video surveillance solution on the Cisco integrated services router series consists of two main components:

- The Cisco Video Management and Storage System (VMSS) Network Module implements the Operations Manager and Media Server functions for the branch. It supports IP-based video cameras as well as analog cameras attached to the Analog Video Gateway Module. The Operations Manager provides a web-based browser console to configure, manage, display, and control video supported at the branch location.
- The Analog Video Gateway Module installed in the Cisco integrated services router series branch router provides support for analog cameras, analog Pan Tilt Zoom (PTZ), alarm input and control relay output. It supports up to 16 analog cameras. (See Figure 10.)

Figure 10 Video Surveillance Deployment with Cisco Integrated Services Router Series



The Cisco integrated services router series also has embedded support for many of the security services previously discussed, including:

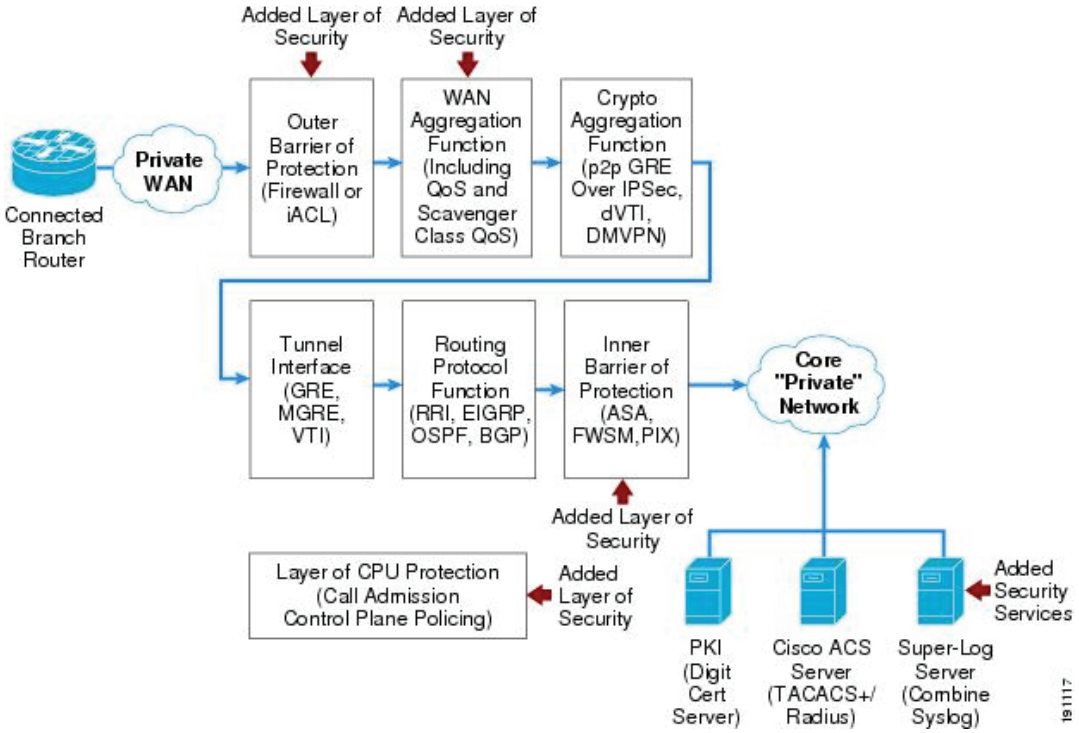
- Stateful firewall
- VPN services mentioned earlier, including SSL VPNs, which offer a flexible and highly secure way to extend network resources to virtually any remote user with access to the Internet and a web browser
- Intrusion prevention system (IPS)
- Trust and identity (802.1x)
- Cisco Network Admission Control (NAC)
- DDoS mitigation
- NBAR
- Control-plane policing
- AutoSecure

As with the other areas of the network we have examined, there are many more security-related technologies that could be discussed. We have presented the highlights in this section. Table 6 provides a look at some other relevant technologies. Figure 11 provides an architectural look at where these technologies could be deployed.

Table 6 Additional WAN and Remote Agency Office Technologies

Technology	Benefit
Dynamic Multipoint VPN (DMVPN)	DMVPN is a popular IPsec-based Cisco IOS Software solution that supports hub-and-spoke IPsec + GRE VPN deployments by building secure meshed tunnels. It relies on two proven Cisco technologies, the Next Hop Resolution Protocol (NHRP) and Multipoint Generic Routing Encapsulation (GRE) tunnel interface. The simplicity of configuration with DMVPN has helped ensure its successful deployment in hundreds of customer locations worldwide.
Quality of Service (QoS)	QoS is critical to the optimal performance and availability of critical services in a remote agency office, even under adverse network conditions, such as high data rates and worm outbreaks. In addition, since some service control and all remote management are in-band, it is critical that QoS is employed to accurately classify, prioritize, and control management traffic.
Cisco Easy VPN Server	Cisco Easy VPN greatly simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client VPN Framework, the Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, reducing the management complexity of VPN deployments.
CPU and memory thresholding	Cisco IOS Software enables users to set global memory thresholds on memory utilization of the router and generate notifications when the thresholds are hit. By reserving CPU and memory, this feature allows the router to stay operational under high loads, such as those created by attacks.
Cisco IOS Software Content Filtering	The Cisco IOS Software Content Filtering solution monitors and regulates all web activities by blocking specific websites or restricting access to certain websites. This hosted solution uses Trend Micro's global TrendLabs threat database and is closely integrated with Cisco IOS Software. It enforces compliance regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Children's Internet Protection Act (CIPA) to mandate reliable content filtering.
Physical Security Integration	The EVM-IPS-16A module on Cisco Integrated Services Routers aggregates older analog video streams with up to 16 analog ports and migrates them to the IP network. The NME-VMSS module provides the interface to manage and monitor video streams, links directly to IP Security cameras that are connected to PoE-enabled switches, and even locally stores some video footage.

Figure 11 Branch to WAN Connectivity, with Security



Conclusion

This document has been a broad overview of some of the more important security-related services available on Cisco networking platforms. While not exhaustive, it does provide some context for the depth and breadth of Cisco security technologies.

Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide. With Cisco, organizations can save time researching threats and vulnerabilities and focus more on taking a proactive approach to security.
Technology alone is only part of the story. Cisco has a long history as a supplier to the federal government and works closely with many agencies in a "trusted advisor" capacity. Beyond technology, Cisco has many attributes that put it at the forefront of cybersecurity.

- **Cisco Security Intelligence Operations (SIO)** is an advanced security infrastructure that enables the highest level of security and threat detection and prevention for Cisco customers. Cisco SIO relies on tightly integrated data derived from multiple Cisco divisions and devices to assess and correlate Internet threats and vulnerabilities. As threats continue to evolve, Cisco SIO enhances the ability to identify global threat activities and trends and provide expert analysis and services to help protect users. With a team of global research engineers, sophisticated security intelligence, and automated update systems, Cisco SIO allows customers to embrace new technologies—securely—so they can collaborate with confidence.
- **Product and Solution Portfolio:** Cisco has the broadest range of networking and security products in the industry, with solutions designed to address every deployment scenario, large and small.
- **Product Lifecycle:** Cisco has established leading practices to help ensure the integrity of our products through the ordering, manufacturing, and receiving lifecycle.
- **Investment Protection:** Longevity of platform life is an important consideration when selecting a networking vendor. Longer-lived platforms forestall the creation of electronic waste. But, as seen from a business benefit point of view, they also provide significant investment protection. Extensible hardware designs, Cisco IOS Software services, and platform scalability all extend the service life of Cisco routers and switches.
- **Design Guidance:** Cisco has a history of working with large customers and the largest networks in the world. This knowledge and experience have been captured in best practices and design recommendations. These include the SAFE blueprint for network security and the Cisco Validated Designs series, which provide detailed advice on how to architect, configure, deploy, and manage every aspect of your network.
- **Best-in-Class Support:** With over 1500 engineers in five Technical Assistance Centers, Cisco provides round-the-clock support to help keep your network running. In 2006, Cisco was the first global networking company to earn the prestigious J.D. Power and Associates Certified Technology Service & Support (CTSS) certification.
- **Cisco Technology Migration Program:** The Cisco Technology Migration Program encourages Cisco customers to trade in their outdated equipment, allowing for responsible disposal by Cisco. In turn, customers receive credits toward the purchase of the newest generation of Cisco networking equipment.
- **Cisco CapitalSM:** When financing a solution, Cisco Capital can provide attractive interest rates and leasing options. For the federal government, Cisco Capital offers agreements with a nonappropriations clause. This clause allows a customer to terminate a lease with no further payment obligation in the event that its governing body fails to appropriate funds to continue lease payments into the next fiscal year.

Cisco has well-defined and proven architectures and solutions that help increase the security posture of federal agencies. Cisco is fully prepared to support federal agencies in the planning, testing, and deployment of these architectures and solutions.

Additional Information

Cisco solutions for government:
www.cisco.com/web/strategy/government/us_government.html

Cisco SAFE blueprint for security:
www.cisco.com/en/US/netsol/ns954/index.html

Cisco Design Zone (CVDs):
www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**