

Security Across the Enterprise: Protect and Empower Your Branch Offices

Today's branch offices rely upon increasingly sophisticated business-critical applications to keep the distributed workforce as productive and efficient as possible. A branch office can be defined as a physical location that is separate from the primary headquarters of an enterprise. Branch offices range in size from a few people to a few thousand people. What they have in common is that they are part of a distributed network of applications and services. They may or may not have in-house IT staff that manages local servers, applications, and Internet access.

Underdefended branch offices make enterprises vulnerable to attacks that can harm productivity and breaches that can expose and compromise sensitive information. Successfully defending the enterprise at its branch offices requires a collaborative, defense-in-depth approach.

The Cisco[®] Empowered Branch integrates complex, remotely manageable networked services to accommodate today's increasingly mobile work styles and rich-media applications. It includes some or all of the following capabilities:

- Unified data, voice, and video converged on the network platform
- Optimized WAN with application-acceleration technologies
- Complete, integrated security that meets organization and compliance requirements
- Highly available, integrated wired-wireless connectivity
- Consistent headquarters-based applications and services available in all branch offices

The Cisco Empowered Branch incorporates security into the network and at the endpoints to mitigate attacks and breaches. Enterprises need to ensure that branch-office IT resources support regulatory compliance efforts to meet standards imposed by the Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLB), and other guidelines and legislation. The branch-office IT infrastructure must be held to the same security standards as the headquarters network, able to defend itself against the same threats and protect information privacy.

This document provides guidelines for setting and deploying network security policies for your branch office. It presents specific Cisco security product solutions and some of the Cisco services that can help your enterprise deploy and manage essential security solutions for Cisco Empowered Branches.

What Security Threats Affect My Business?

Understanding that security threats evolve is the basis for developing effective branch-office security policies. Security threats fall into one of two types: disruptive threats or loss and damage threats.

Disruptive threats are nonspecific, such as viruses, worms, and Trojan horses. More recently, disruptive threats come from malware and spyware inadvertently allowed into endpoint systems

through email (attachments and hyperlinks) and websites. These infections spread to other devices and systems throughout the enterprise. Branch offices need systems to enforce a security policy that quarantines affected systems to prevent proliferation while the system is scrubbed of malicious code.

Loss and damage threats are targeted attacks that use blended threats to obtain sensitive or confidential information that can be sold for profit, such as stealing personal records for identity theft. Privacyrights.org reports that in 2007, more than 160 million records were breached in the United States alone (this number is up from 50 million stolen records in 2006), not counting unreported breaches or those breaches where actual losses were unknown. In addition, more than 50 countries have enacted data-privacy legislation.

Data breaches damage customer trust, making it more expensive to acquire and retain customers—a cost difficult to calculate. Preventing such losses costs less than cleaning up after them. On cleanup costs, Forrester Research estimates that the average cost of a breach in the United States averages \$90 per record in an unregulated industry, and up to \$305 per record in a regulated industry. On prevention costs, Gartner Group Analyst Avivah Litan says, “A company with at least 10,000 accounts to protect can spend, in the first year, as little as \$6 per customer account for just data encryption, or as much as \$16 per customer account for data encryption, host-based intrusion prevention, and strong security audits combined.”

Enterprise Management Associates states that, “Disclosure of data security breaches can have a significant impact on share prices of publicly traded companies. Stock prices of those companies fell an average of 5 percent within the first month following the disclosure and remained between 2.4 and 8.5 percent below for the 8 months following. It took the stocks nearly one year to return to their original levels.”

Beyond Data Threats: Securing Voice and Video

Voice and video are also targets of security attacks. Concerns such as toll fraud remain the same in the unified communications (merging voice, video, and collaboration applications across the network) environment as in traditional telephone networks. Today's organizations also face increased regulatory requirements for conversation privacy, message confidentiality, and user and device authentication. Therefore, unified communications strategies must address the security aspects of Sarbanes-Oxley, GLB, HIPAA, PCI Data Security Standard, European Basel II, and other mandates affecting global organizations directly within the unified communications architecture. Integrating security within the underlying infrastructure also thwarts denial-of-service (DoS) attacks, worms, and other malicious activity that is usually aimed at the data network, but, if successful, could have ramifications for the voice network, too.

What Security Policies Do I Need to Employ?

To prevent and mitigate attacks in the Empowered Branch, security policies should address questions such as the following:

- Are all systems that connect to the network (wired and wireless computing and communication devices, video systems, and local servers) equipped with the latest system patches and endpoint-protection software?
- How does the branch office access the Internet? If locally, is the connection protected from hackers and malicious code?

- Do employee computing systems and other endpoints have software that protects against threats from web and email content?
- How does the branch-office network prevent viruses, malware, and spyware from gaining access to data center systems at headquarters?
- Are local server resources adequately defended?
- Are wireless networks configured for secure network access?
- Are your collaboration tools, including voice and video, secure?
- Can local systems automatically detect and prevent or mitigate attacks?

In addition, you can secure your unified communications systems by taking advantage of the security capabilities already built into your organization's network infrastructure for data protection. Secure unified communications requires considering data, voice, and video communications as a system and protecting all the system components, including:

- Underlying network and application infrastructure
- Phone switch (also called a call server)
- Individual phones
- Various unified applications

To protect each of these components, enterprises should merge different skill sets throughout the organization, bringing together voice, network operations, security operations, telephone operations, and business decision makers in an interdisciplinary manner. With more employees becoming geographically dispersed, enterprises should also build in redundant connections from remote locations to help prevent downtime between distributed unified communications equipment and centralized phone switches. IT and telecom staff will be able to logically segment all voice communications-related network traffic from data traffic and help ensure that the voice traffic segment is never sent to data network resources.

Questions to Consider When Designing Your Secure Branch-Office Network

Although a secure Empowered Branch should offer the same services as the headquarters network, it requires its own perimeter security, intrusion prevention, and content filtering. Securing a branch office begins with a design process that tailors the solution to both the functional considerations and physical requirements of the site. Deploying similar solutions at each site can simplify deployment and management, yet a universal approach may not suit organizational needs, where site requirements may vary for simple reasons such as number of employees, or complex ones such as local Internet access or servers.

Functional considerations may include the following:

- WAN type: Does the branch office connect to the headquarters through a dedicated leased line or use a VPN over the Internet? How much bandwidth does it support? Is there enough bandwidth?
- Internet access architecture: Do branch-office users access the Internet through a local connection (called split tunneling), or over the WAN through a single headquarters connection?
- Traffic mix: What applications do branch offices use? Which applications handle confidential data? Are applications transactional (such as Citrix) or do they use real-time

streaming, such as IP voice or video? What kinds of traffic traverse the WAN or local Internet connection?

- Server architecture: Do onsite local application or database servers need protection, or are all servers consolidated into centralized data centers?
- Endpoint control: How are endpoints protected, including user devices, servers, and network components, and how do you ensure that they have the latest system patches and signature files?
- Application types: The types and confidentiality of data, voice, and video passing between the headquarters data center and branch offices, along with factors such as regulatory compliance, determine whether to encrypt data through the WAN connection or VPN.
- User profiles: Who is using networked resources at the branch office: employees, contractors, partners, customers, and other guests? What are their access privileges?
- Guest access: Many branch offices interact with customers and partners who need network services when they visit. These users and endpoints are not predictable; is their accessibility to the network controlled, and are their actions monitored and limited to reduce risks?
- Wireless laptops and phones: Is there a local wireless network? Does it support user passwords or wireless encryption?
- Unified communications systems: How vulnerable are the phones, TelePresence, and unified messaging systems? Do voice calls require encryption? Can messages carry spyware and viruses to phones or PCs?

Physical considerations may include the following:

- Size: How many users and endpoints does the branch office support? This factor affects the choice of WAN type and speed, and whether to use a local or central Internet access.
- Number of branch offices: Enterprises with a few branch offices may have more budgetary flexibility than companies with hundreds—or thousands—of branch offices, where cost quickly becomes a limitation for both deployment and management.
- Available expertise: Most branch offices do not have IT personnel onsite; remotely manageable security is usually an essential requirement.

Cisco Security Solutions

Designed with a systems approach to information security, the Cisco Self-Defending Network offers industry-leading network and endpoint defenses that incorporate innovative application security, content security, security monitoring technologies, and policy enforcement. These technologies and solutions are ideal for securing the Empowered Branch. The Cisco Self-Defending Network adapts to detect and mitigate changing threat profiles. It includes collaborative capabilities that allow security functions to interoperate.

Defense in Depth at the Empowered Branch

The Cisco Self-Defending Network architecture for the Empowered Branch includes many of the same components as the headquarters security architecture, scaled to the size of the branch office. Deploying the same technologies throughout the organization, including the campus, data centers, and branch offices, facilitates consistency across your networks and reduces the number of management systems required to operate and secure them. This efficiency lowers both capital

expenditures and operating expenses. In addition, the convergence of network security contributes to environmental sustainability and lower energy costs.

The secure Empowered Branch should include the following security functions:

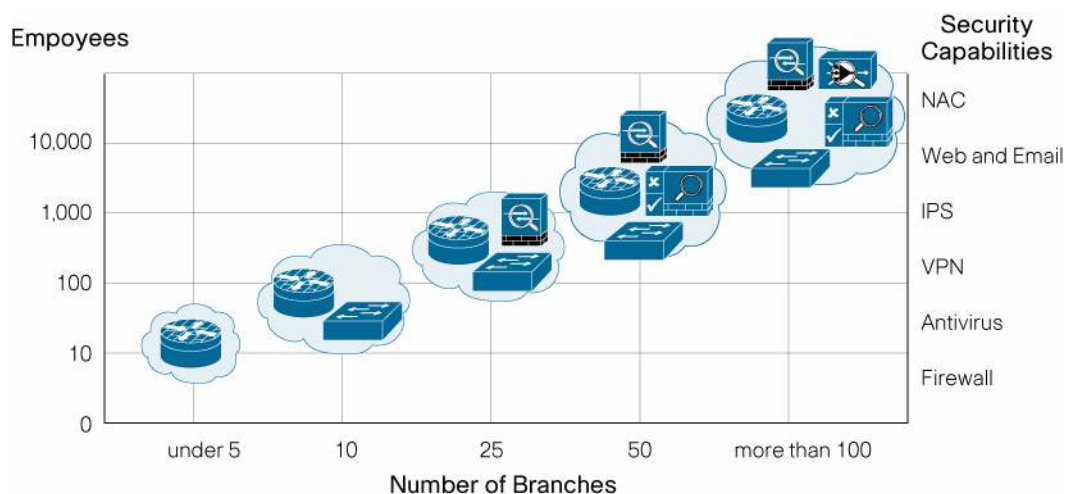
- **Perimeter access security:** This firewall function permits or denies access into the network at all entry points, including local Internet access and private WAN links to central resources. A perimeter defense in the branch office also protects headquarters resources from incidents that occur in the branch office, such as a spyware infection or attempted hacker penetration.
- **Intrusion prevention:** Intrusion prevention examines higher-layer content of network traffic, using signatures and anomalous-behavior-detection algorithms to detect, quarantine, or stop unusual or unpermitted behaviors such as deliberate hacking or malware proliferation within the network infrastructure.
- **Content security:** Content filtering helps protect against known and new Internet threats, improves employee productivity, and enforces business policies for regulatory compliance. This subscription-based, hosted solution monitors and regulates all Internet activities by blocking or restricting access to certain websites. In addition, it provides protection from malicious sites that are known to give out malware, adware, spyware, and phishing. And it is simple and easy to deploy, helping your organization better manage network resources.
- **Access control:** Access control enforces security policies defining who may enter the network through a VPN or LAN connection. Authentication verifies user identity and presents an opportunity to validate device configurations. Such validation helps ensure that devices allowed onto the network have the proper level of operating system patches and endpoint security software. Authorization permits or denies activities to a user or device, such as preventing a guest from logging into sensitive databases.
- **Endpoint security:** Software on endpoint devices such as laptop and desktop computers, servers, gateway routers, and other devices scans for anomalous behavior to detect and eradicate malware and other malicious activities.
- **Secure communications:** Secure communications protects voice and video streams and endpoints in a converged IP network through firewall filtering, call encryption, and malware filtering.
- **Remote management:** Remote management supports configuration and monitoring actions from the central management console.

One Box or Many?

After defining design requirements, the next decision is whether to deploy a single device or a multiple-appliance solution at each branch office (Figure 1). Security router solutions may be the best choice where cost and footprint are more important, such as a retailer with 1500 branch-office locations without onsite IT staff. This integrated security approach takes advantage of existing network infrastructure, without necessarily deploying additional hardware. This setup saves time and money because it reduces the number of devices in the network, lowering training and manageability costs for an overall lower total cost of ownership (TCO). Router network modules are also covered in existing Cisco SMARTnet[®] maintenance contracts for routers to further ease manageability. Integrated security on routers also provides the flexibility to apply security functions—such as firewall, inline intrusion prevention, and VPN—anywhere in the network to ensure the best defense against security threats.

Multiple-appliance solutions may be necessary where regulatory compliance requires more granular security or applications require higher security performance; they may also be necessary to cost-effectively supplement security capabilities in an existing network. In both solution architectures, remote manageability allows centralized control and policy enforcement.

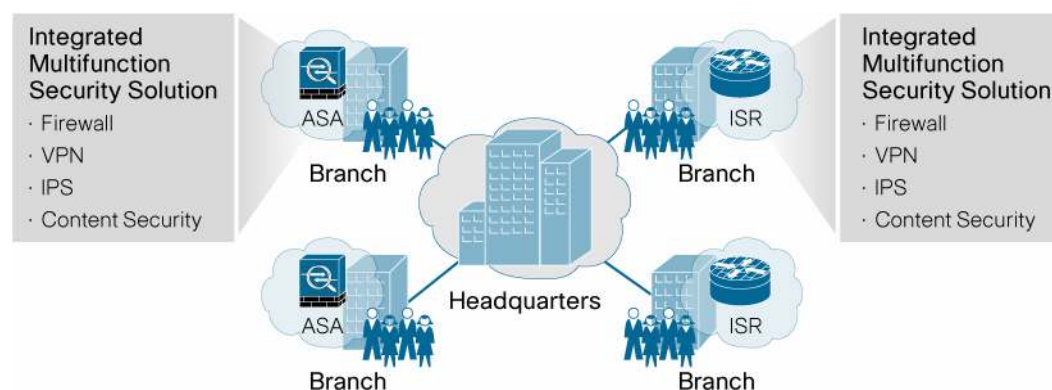
Figure 1. When to Choose Single—vs. Multiple-Box Solutions



All-in-One Multifunction Security Solutions

Cisco offers two solution options for a consolidated security architecture in the Empowered Branch: Cisco integrated services routers and Cisco ASA 5500 Series Adaptive Security Appliances—both of which support comprehensive, virtually identical suites of security technologies and functions (Figure 2). Although both multifunction platforms can also serve in a multiple-appliance architecture (refer to the next section), in general, the Cisco ASA 5500 Series is ideal for environments that require higher-performance security with larger scaling requirements. The Cisco integrated services router platform is the more cost-effective security option, ideal for deployments into a large number of branch offices or where green initiatives are at the forefront.

Figure 2. Multifunction Security Appliances



Cisco Integrated Services Routers

Founded on 20 years of leadership and innovation, Cisco integrated services routers ship with the industry's most comprehensive security services, intelligently embedding data, security, voice, and wireless networking into a single, resilient system for fast, scalable delivery of mission-critical business applications. The integrated services router family was designed with security as a

fundamental component, making hardware-based encryption a standard feature. This built-in, hardware-based encryption acceleration offloads the VPN processes to provide increased VPN throughput with minimal impact to the router CPU. If additional VPN tunnels or throughput is required, optional VPN encryption advanced integration modules (AIMs) are available.

Router security encompasses much more than just VPN, however. Cisco IOS® Software offers a suite of integrated threat-control technologies as well as other features to mitigate threats and secure your business. With comprehensive LAN and WAN connectivity options, an integrated solution is cost-effective, reducing the overall number of managed devices to lower the costs of training, management, power, and service contracts.

Cisco integrated router security solutions allow enterprises to equip the Empowered Branch to do the following:

- Protect the router itself, defending against attacks targeted directly at the network infrastructure
- Use existing infrastructure, delivering many security features on the router through Cisco IOS Software without deploying additional hardware
- Offer perimeter security with firewall, intrusion prevention system (IPS), and VPN features
- Protect gateways, both WAN connections to the data center and local Internet access

Cisco integrated services routers also deliver advanced protection with higher performance through three specialized security modules:

- Cisco IP Security (IPsec) VPN AIM: Optimizes VPN performance for both IPsec and Secure Sockets Layer (SSL) VPN deployments
- Cisco Intrusion Prevention System Advanced Integration Module (IPS AIM) and Cisco Intrusion Prevention System Network Module: Identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse
- Cisco Network Admission Control (NAC) Network Module: Integrates feature-rich Cisco NAC Appliance Server capabilities, allowing administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network.

Cisco ASA 5500 Series Adaptive Security Appliances are high-performance security solutions that integrate the latest technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators. These powerful multifunction network security appliances provide the security breadth and depth for protecting Empowered Branches while reducing overall deployment and operational costs and complexities. The Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity.

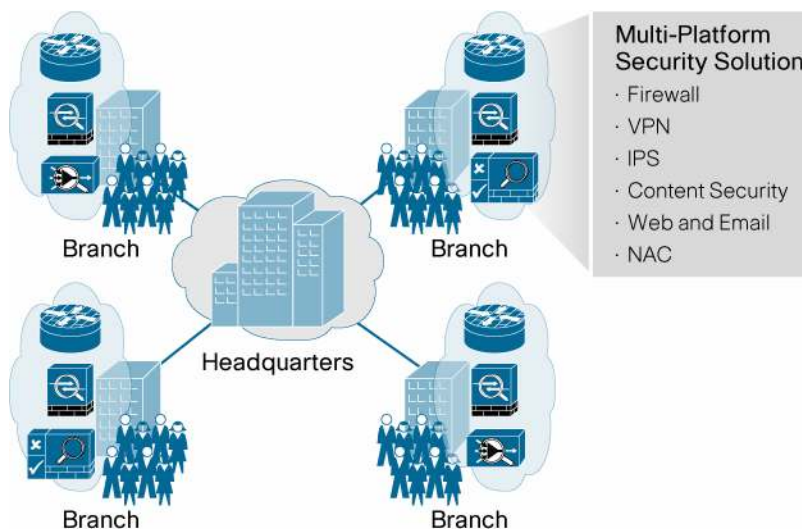
The flexible design of the Cisco ASA 5500 Series provides exceptional investment protection through programmable hardware, integrated Gigabit Ethernet connectivity, and a diskless, flash memory-based architecture. The series features a modular architecture and a flexible multiprocessor design, enabling high performance for multiple concurrent security services such as advanced firewall services, IPS services, content security services, and IPsec and SSL VPN services. Its module slot allows you to add other high-performance security services such as the Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM). The

CSC-SSM provides comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering capabilities in a remotely manageable solution.

Multiple Appliance Solutions

Larger branch offices or locations with high security requirements (such as strict regulatory compliance) may need a multiple-appliance security architecture, which allows more granular control and higher overall performance than a single-box architecture (Figure 3).

Figure 3. Multiple-Appliance Security Solution



The foundation of the multiple-appliance architecture is a Cisco ASA 5500 Series appliance or a Cisco integrated services router platform, which offer firewall, intrusion prevention, content security, and some access-control capabilities. In addition to these components, the Empowered Branch may require one of the following: Cisco IPS 4200 Series Sensors and Cisco IronPort® S-Series web security appliances.

The **Cisco IPS 4200 Series Sensor** offers the same IPS technology that is integrated into the IPS modules for the Cisco ASA 5500 Series appliance and Cisco integrated services routers. As a signature-based appliance, the sensor can accurately identify, classify, and stop malicious traffic before it affects your business. It delivers precision threat analysis and a rich set of response actions for flexible and precise response policies. Its management and correlation tools focus on policy, providing granularity to fine-tune the IPS configuration.

The **Cisco IronPort S-Series**, a web security appliance, combines a high-performance security platform with exclusive Cisco IronPort Web Reputation technology and the breakthrough Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine, a new scanning technology that enables signature-based spyware filtering. Robust management and reporting tools deliver ease of administration and complete visibility into threat-related activity. For automated, real-time signature updates, Cisco IronPort solutions can harness the Cisco IronPort SenderBase® Network, which provides an unprecedented real-time view into security threats from around the world. SenderBase data powers Cisco IronPort Virus Outbreak Filters, a preventive security service that protects enterprises from viruses well before antivirus vendors publish virus signatures. The SenderBase application examines the broadest set of data in the industry, currently examining more than 40 different parameters about web traffic. This data is derived from a highly diverse group of more

than 100,000 organizations, including the largest networks in the world, which contribute information to the SenderBase application in five billion messages per day.

Access and Endpoint Control

Access and endpoint control are vital components of Empowered Branch security. They form the first line of defense against threats such as spyware and viruses. The access-control system authenticates users and devices and authorizes their activities on the network. The authentication system should also include the ability to enforce the latest operating system patches and antivirus signature updates on fixed and mobile computing devices before permitting access. Authorization associates a specific user with a user profile that defines what the user may or may not do on the network.

At the Empowered Branch, the Cisco Self-Defending Network includes the NAC architecture in the network and Cisco Security Agent inside endpoints. At the Empowered Branch, NAC functions can be deployed as a **Cisco NAC Network Module** in the Cisco integrated services router. When router slots are full, or as performance requirements demand, a dedicated **Cisco NAC Appliance** can perform admission control for one or a group of branch offices. Both solutions communicate through the WAN with the Cisco NAC Appliance Manager at the central security operations console. A Cisco NAC agent on each endpoint helps the NAC architecture to identify each user and device requesting a network connection. Cisco NAC supports single sign-on through a Windows password, and is compatible with authentication systems that support a variety of protocols such as Lightweight Directory Access Protocol (LDAP), RADIUS, and Microsoft Active Directory. This discussion does not consider centralized access-control servers and third-party authentication and authorization solutions, because they are not deployed in a branch office.

The critical actions that the Cisco NAC Appliance performs are the following:

- It recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
- It evaluates whether machines are compliant with security policies. Security policies can include specific antivirus or antispymware software, OS updates, or security patches. The Cisco NAC Appliance supports policies that vary by user type, device type, or operating system.
- Cisco NAC enforces security policies by blocking, isolating, and repairing noncompliant machines.
- Noncompliant machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

Among the policies that Cisco NAC can enforce is a requirement for **Cisco Security Agent** in all endpoints attached to the network. Cisco Security Agent protects against threats in server, desktop, laptop, and point-of-sale (POS) computing systems. It goes beyond conventional endpoint security solutions, providing an industry-leading defense against targeted attacks, spyware, rootkits, and zero-day attacks. It offers proactive protection against unknown threats, new exploits, and variants trying to take advantage of recently announced vulnerabilities. Security operators can put granular controls in place to manage policy compliance for users, applications, systems, locations, and network addresses.

Cisco Security Agent provides “zero-update” system integrity protection for critical servers that cannot be taken out of service to apply OS—or application-specific vulnerability patches. It helps

reduce emergency patching of systems to respond to vulnerability announcements, minimizing patch-related downtime and IT labor. Cisco Security Agent offers more than a standalone endpoint security solution. It collaborates with network security devices to increase the effectiveness of the overall network deployment:

- **Firewall:** Cisco Security Agent can enhance the firewall and application-inspection capabilities of Cisco integrated services routers and Cisco ASA security appliances to examine particular applications based on Cisco Security Agent traffic markings.
- **Intrusion prevention:** Cisco Security Agent collects host information that it can share with Cisco IPS modules and devices to enhance the overall awareness and relevance of IPS actions in the network.
- **VPN:** Cisco VPN capabilities in the Cisco integrated services routers and Cisco ASA 5500 Series can take advantage of Cisco Security Agent personal firewall and host IPS features to provide robust endpoint security for IPsec and SSL VPN remote-access users.
- **NAC:** Cisco Security Agent prevents modification to the NAC agent, helping to ensure consistent NAC policy enforcement.

Centralized Management

The Cisco Self-Defending Network at the Empowered Branch supports remote manageability.

Centralized control enables consistent policy enforcement and facilitates rapid responses to security incidents at a remote location. Cisco offers two solutions that deliver manageability to the Empowered Branch. Cisco Security Manager supports security deployment and configuration, whereas Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) provides operational incident and performance monitoring for ongoing vigilance.

Cisco Security Manager delivers comprehensive policy administration and enforcement for the Cisco Self-Defending Network from a central management console. It delivers provisioning of Cisco firewall, VPN, and IPS services across Cisco routers, security appliances, and switch services modules. Its powerful policy-based management techniques allow provisioning and configuration management through a GUI that supports device—and map-centric views. It includes flexible configuration templates to speed deployment and security configuration changes to devices in all Empowered Branches.

Cisco Security MARS is deployed in the Empowered Branch as an appliance that communicates with a central device in the security operations center. It is an easy-to-use threat-mitigation appliance that enables operators to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed in the infrastructure.

Cisco Security MARS performs these activities:

- Integrates network intelligence to modernize correlation of network anomalies and security events
- Visualizes validated incidents and automating investigation
- Mitigates attacks by taking full advantage of your existing network and security infrastructure
- Monitors systems, network, and security operations to aid in compliance

Cisco Security MARS requires no endpoint software; instead, it reads and correlates event data generated by devices in its domain, which can be a single branch or a group of branch offices. The appliance centrally aggregates logs and events from a wide range of popular network devices (such as routers and switches), security devices and applications (such as firewalls, IPSs, vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), applications (such as databases, web servers, and authentication servers), and network traffic (such as Cisco NetFlow).

The Cisco Security MARS appliance supports event data from both Cisco and third-party security solutions, enabling complete visibility of the security posture of the network it monitors. Cisco maintains the current list of supported products online at http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html.

Cisco Security MARS integrates tightly with Cisco Security Manager. It also provides centralized reporting for Cisco NAC.

Cisco Security Services

Cisco Security Services deliver comprehensive security operations management to your enterprise, enabling you to control expenditures as you effectively maintain the integrity and privacy of sensitive information, and maximize network availability, reliability, and stability.

Cisco Security Remote Management Services help your enterprise manage security across dozens or hundreds of branch offices. These services can help you maximize the value of security investments by keeping devices available and operational, offloading the day-to-day security monitoring and management operations of the Empowered Branch infrastructure. Your enterprise saves time, money, and effort by scaling change, configuration, and release-management processes with Cisco support staff available 24 hours a day.

Cisco Security Remote Management Services help your enterprise manage security functions in Cisco Empowered Branch networks and increase security-posture awareness. This set of services delivers 24-hour access to a team of highly trained and certified security and networking experts who provide:

- Operational support for security-incident monitoring
- Security solution fault—and performance-incident management
- Problem resolution and security infrastructure tuning
- Secure network access-control support

Cisco Security Remote Management Services encompass three complementary services:

- **Cisco Security Access Control Remote Management Service** offers a detailed set of monitoring, management, and reporting methodologies for access control that help create a more tightly controlled, more closely monitored, and more secure environment.
- **Cisco Security Intrusion Prevention Remote Management Service** offers a detailed set of monitoring, managing, and reporting methodologies for accurately detecting known threats, helping your enterprise to closely patrol Empowered Branch networks for intrusions and to effectively mitigate security incidents.

- **Cisco Security VPN Remote Management Service** offers a detailed set of monitoring, management, and reporting methodologies that help improve the security and performance of VPN solutions.
- **Cisco IPS Signature Management Service** provides access to signature updates for Cisco IPSs deployed as dedicated appliances or integrated into Cisco ASA 5500 Series appliances or Cisco integrated services routers. This automated “push” service eliminates the need for staff to remember to check for updates. This remote release-management and signature-tuning service enables the Empowered Branch security infrastructure to adapt to emerging threats and to patch vulnerabilities, automatically preventing intrusions. Cisco security analysts help central security management staff to deploy signature updates and tune each new release to specific environments with lower cost and less effort than manual adjustments.

Security in a Changing Landscape

The Cisco Empowered Branch supports the increasingly mobile and collaborative work styles of the 21st century. The diversity and availability of networked services pose a daunting security challenge: providing high-quality data, voice, video, and mobility services to authorized users while preventing disruptive and targeted attacks on the enterprise network and its resources. The Cisco Self-Defending Network provides a manageable, integrated, adaptive, and collaborative architecture for protecting enterprise branch offices. Along with the expertise and cost-effectiveness of Cisco Security Services, the Cisco Self-Defending Network enables your enterprise to do business effectively—and safely—at your Cisco Empowered Branches.

For More Information

- Branch-Office Security Design Guide
http://www.cisco.com/application/pdf/en/us/quest/netsol/ns171/c649/ccmigration_09186a00807593b6.pdf
- Cisco Empowered Branch
http://www.cisco.com/en/US/netsol/ns477/networking_solutions_packages_list.html
- Design Zone for Security
http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html
- Cisco Security Services
http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html
- Cisco Router Security <http://www.cisco.com/go/routersecurity>
- Cisco Integrated Services Routers <http://www.cisco.com/go/isr>
- Cisco ASA 5500 Series <http://www.cisco.com/go/asa>



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)