WHITE PAPER

WHITEPAPER: CONVERGED VS. DEDICATED APPLIANCE DEPLOYMENT

WHEN TO DEPLOY THE CISCO ASA 5500 SERIES, CISCO PIX SECURITY APPLIANCE, CISCO IPS 4200 SERIES, OR CISCO VPN 3000 SERIES CONCENTRATOR

Cisco Systems® delivers customizable security solutions to meet the requirements of any deployment environment. With the introduction of the Cisco Adaptive Security Appliance 5500 Series, Cisco provides an appliance-based option for delivering converged, multifunction security and VPN services within a single platform. With its converged firewall, intrusion prevention system (IPS), and network antivirus services profile, customers may use the Cisco ASA 5500 Series to deploy a breadth of Adaptive Threat Defense services. For VPN services, the Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit remote-access and site-to-site connectivity requirements

The broad VPN and security services profile of the Cisco ASA 5500 Series makes it a single device for many uses. Deploy it as a converged threat prevention device at the central site by using its access control, application inspection, and worm, virus, and malware mitigation technologies. Use it as a dedicated remote-access device, taking advantage of its IP Security (IPSec) and Secure Sockets Layer (SSL) VPN capabilities. Move it into the network interior for interdepartmental access control and to guard against worms, viruses, and other malicious code that internal users may unwittingly bring into the network. In small business and branch office environments, the ASA 5500 serves as an “all-in-one” device, offering comprehensive threat prevention and VPN services while suiting the budgets and operational models of such deployments.

What are some of the deployment considerations associated with using a multifunction device like the Cisco ASA 5500, versus traditional “dedicated” security appliances such as Cisco PIX® security appliance, Cisco IPS 4200 Series sensor appliances, and Cisco VPN 3000 Series concentrators? This paper explores the functional, operational, and cost considerations of deploying a multifunction security appliance instead of dedicated appliances. Comparison of security/VPN appliance and Cisco router deployment considerations is out of scope for this paper, but is addressed in detail in the white paper “Positioning Integrated Router Security and Dedicated Security Appliances”, available on Cisco.com.

CISCO SECURITY APPLIANCE PRODUCT FAMILIES

For customers that choose appliance-based security for their security deployments, Cisco offers Cisco PIX security appliances, Cisco IPS 4200 Series appliances, the Cisco VPN 3000 Series concentrators, and Cisco ASA 5500 Series security appliances. Each of these products delivers solutions for a range of deployments and customer sizes---from small offices through headquarters locations, and from small businesses through the largest enterprises. Cisco PIX security appliances provides solution that reach into the small office/home office (SOHO) environment as well. Below is a brief overview of each product’s features and deployment scenarios.

Cisco PIX Security Appliance

Market-leading Cisco PIX security appliances deliver robust, application-aware firewall and VPN services, including user and application policy enforcement, multi-vector attack protection, and secure site-to-site connectivity services in cost-effective, easy-to-deploy solutions.

Cisco IPS 4200 Series Sensor Appliance

Cisco IPS 4200 Series sensors protect the network from malicious attacks, worms, and viruses before they can affect your data and resources. Cisco IPS sensors offer significant protection to your network by helping to detect, classify, and stop threats, including worms, spyware/adware, network viruses, and application abuse.

Cisco VPN 3000 Series Concentrator

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution providing both SSL and IPSec VPN connectivity. A standards-based, easy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote-access VPNs.

Cisco ASA 5500 Series Security Appliance

The Cisco ASA 5500 Series converges the latest advancements in security technologies, combining Cisco's market-proven firewall, intrusion prevention, network antivirus, and VPN services. Adding a unified management package and built for speed, the Cisco ASA 5500 Series delivers high concurrent services throughput with simplified management for enterprise and SMB applications.

FEATURE/FUNCTION COMPARISON

The Cisco ASA 5500 Series combines the market-proven feature sets of Cisco PIX, IPS 4200, and VPN 3000 platforms, as well as network antivirus capabilities from Trend Micro, in a single device and management framework. Convergence of these features enables new capabilities such as the ability to provide worm/virus/malware protection for remote-access VPN connections, broad worm/virus/malware mitigation at the network perimeter, and interior and enhanced application inspection and control. Consequently, the Cisco ASA 5500 Series often provides a superset of capabilities---derived from its highly converged, mutually aware services profile---relative to Cisco's dedicated security and VPN appliances.

The breadth of threat mitigation features provided in a single Cisco ASA 5500 Series footprint also enables greater protection against threats wherever it is deployed, from a remote office to a headquarters DMZ to the network interior. This enables worm/virus/malware mitigation and application security in neglected areas of the network, such as remote sites and the network interior, where such advanced security functions have not typically been economically or operationally feasible to deploy. From this perspective, the Cisco ASA 5500 Series increases the overall security posture of the network, thereby strengthening the network-wide security chain.

From an existing deployment integration perspective, the Cisco ASA 5500 Series is fully compatible with all existing Cisco PIX, IPS 4200, and VPN 3000 installations. As mentioned previously, all of these appliances have been built using the same market-proven technologies. As such, feature disparities between the ASA 5500 Series and the dedicated products are virtually eliminated. Furthermore, when deploying the ASA 5500 Series, security staff can build from their existing training and knowledge of PIX, IPS 4200, and VPN 3000 appliances.

Table 1 outlines application environment and capabilities of each platform:

Table 1. Functional Comparison

	Application	Additional ASA Services
Cisco ASA 5500 and Cisco PIX	• ASA targeted at typical PIX 515E and 525 environments • Compliments PIX 501, 506E and 535 at SOHO and large enterprise HQ	• Full IPS services • Worm and malware mitigation • Network anti-virus • Greater application inspection • VPN clustering • Modular services slot
Cisco ASA 5500 and IPS 4200	• ASA focused for converged firewall and IPS • IPS 4200 is optimized and favorably priced for IPS-only deployments	• Full firewall services • Full VPN services • Modular services slot

	Application	Additional ASA Services
Cisco ASA 5500 and Cisco VPN 3000	• ASA targeted at IPSec remote access and site-to-site VPN services for all sites • ASA interoperates with existing VPN 3000 clusters • VPN 3000 optimized for SSL VPN focused deployments	• 3x greater throughput • Stateful VPN failover • QOS, OSPF for site-to-site VPN • VPN with worm/malware/virus mitigation

SECURITY ARCHITECTURE AND IT ORGANIZATIONAL CONSIDERATIONS

The size, operational model, and segment of the network influence security and VPN platform decisions. There are scenarios where consolidating multiple security and VPN functions on a single device best meets requirements, as well as scenarios where dedicating devices to specific functions is more appropriate.

From a size perspective, the traffic volume and complexity of larger enterprise networks often results in deployment of more dedicated function devices. A security and VPN infrastructure built on devices performing focused or even single functions enables optimal scalability, simplifies software version selection and upgrade cycles, and allows for thorough configuration tuning and greater network segmentation. From an operations standpoint, deploying dedicated function devices also enables segmentation of network security responsibilities among different IT teams.

Typical examples of functional segmentation requiring dedicated security and VPN devices are:

- Deployment of dedicated remote-access VPN devices
- Deployment of dedicated IPS devices for security policy auditing and regulatory compliance or to mesh with IT organizational responsibilities
- High-speed, data-center-specific deployments focused on protecting Web server farms and application servers
- Network-edge firewalls for resilient, high-speed traffic inspection and access control

In smaller networks and organizations, the reverse tends to be true. Smaller networks, such as small businesses and remote offices, and smaller IT organizations tend to consolidate as many security and VPN functions on as few devices as possible. Having fewer devices reduces the complexity of the network and also reduces the breadth of knowledge that IT staff must possess to operate a network with multiple unique platforms. In essence, device consolidation generally simplifies operations for sites with smaller IT staffs that often have less specialized focus on security.

Cisco ASA 5500 Series is highly flexible, making it a good fit for most dedicated function and consolidated function scenarios. Its broad VPN and security services profile makes it a single device for many uses. Deploy the appliance as a converged threat prevention device at the central site by taking advantage of its access control, application inspection, and worm/virus/malware/attack mitigation technologies. Deploy it on the network edge as a traditional firewall, or as a dedicated remote-access device by using its VPN capabilities. In small business and branch office environments, the Cisco ASA 5500 Series serves as an “all-in-one” device offering comprehensive threat prevention and VPN services while suiting the budgets and operational models of such deployments.

In pure IPS deployments, such as environments where IPS provide security policy auditing and regulatory compliance data, the Cisco IPS 4200 Series remains the platform of choice. This audit infrastructure provides a “checks-and-balances” approach to securing and validating the posture of the network while layering rich attack, worm, virus, and spyware/adware protection on top of the policy enforcement devices. Furthermore, there is often separation of IT management teams for IPS and other security functions, like firewalls. Consequently, the organization managing the IPS infrastructure generally prefers to have devices dedicated to the service for which they are responsible.

For SSL VPN deployments, the Cisco VPN 3000 Series Concentrator provides the most advanced features, such as Cisco Secure Desktop for endpoint security, Clientless Citrix, and SSL VPN tunneling for full network and application access. For environments where SSL VPN is the primary application, the VPN 3000 Concentrator remains the platform of choice.

PLATFORM AND OPERATIONS COST CONSIDERATIONS

Platform Costs

In most cases, the converged capabilities of the Cisco ASA 5500 Series are equal to or less than the cost of a similar model dedicated-function Cisco PIX or VPN 3000 product. Consequently, cost of the device should not be a factor in deciding whether the converged ASA 5500 or a dedicated Cisco PIX or VPN 3000 device is the optimal choice for the deployment. This decision should be made by comparing product features, as well as the security architecture and operational model of the organization as discussed above.

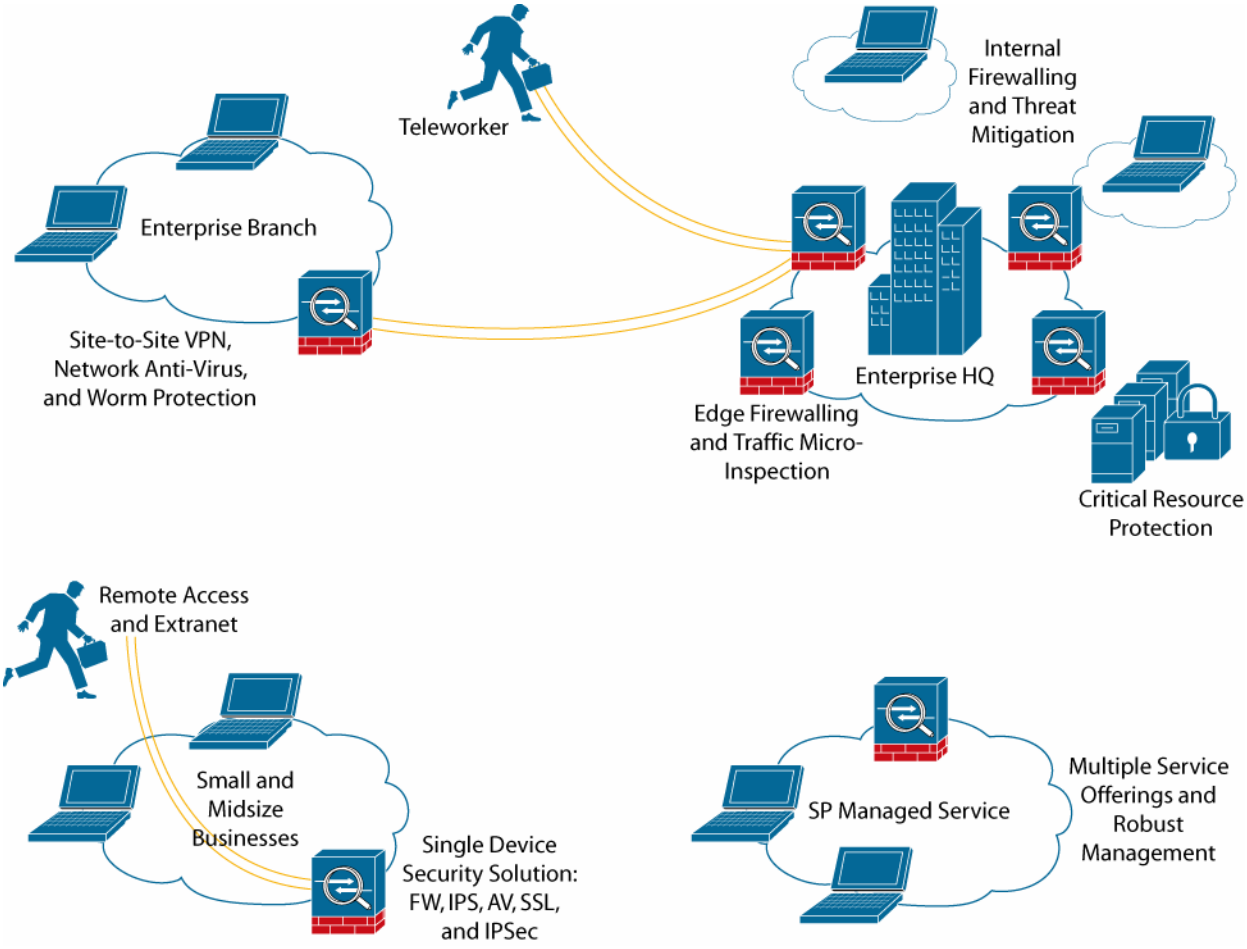
For pure IPS deployments, the Cisco IPS 4200 Series provides attractive price/performance relative to the ASA 5500 Series. The ASA 5500 Series is optimized for the broad threat mitigation and application security delivered by its converged firewall, IPS, and network antivirus capabilities, while the IPS 4200 Series remains optimized for focused IPS environments.

For SOHO or large headquarter firewall and site-to-site VPN deployments, Cisco PIX 501, PIX 506E, and PIX 535 security appliances remain the most cost-effective platforms. The Cisco ASA 5500 Series is optimized for converged services applications in smaller sites. If only a subset of threat mitigation features or pure VPN features are required, then Cisco PIX 501 and PIX 506E appliances are the most cost-effective choice for SOHO locations. At the high end, Cisco PIX 535 security appliance deliver extremely high performance at 1.7 Gbps, complementing the ASA 5500 Series on the price/performance curve. And, as mentioned previously, the Cisco ASA 5500 and Cisco PIX products are fully feature-compatible, designed for deployment together as the network architecture requires.

Operations Costs

The “single device, many uses” capability of the Cisco ASA 5500 Series gives it a unique advantage in the area of security and VPN operations costs (Figure 1). The breadth of services delivered by the Cisco ASA 5500 Series---which includes firewall, IPS, VPN, and network antivirus---enables deployment of the platform in many different environments with diverse functional requirements. Because each of these services is derived from Cisco’s market-proven security and VPN appliances, the ASA 5500 Series may be deployed without compromising features, performance, or manageability. This approach reduces the number of platforms that must be deployed and managed while offering a common operating and management environment across all those deployments, simplifying configuration, monitoring, troubleshooting, and security staff training.

Figure 1. Single Device, Many Uses



Common deployment scenarios for which the Cisco ASA 5500 Series provides a single, standardized platform include:

- Converged access control, traffic and application inspection, and worm/virus/malware mitigation for the network edge and/or DMZ
- Converged access control, traffic and application inspection, and worm/virus/malware mitigation for the network interior
- Traditional firewall and application inspection for the network edge and/or DMZ
- Traditional firewall and application inspection for the network interior
- Remote-access VPN with converged traffic and application inspection and worm/virus/malware mitigation
- Traditional standalone remote access VPN termination
- Site-to-site VPN services
- “All-in one” access control, traffic and application inspection, worm/virus/malware mitigation, remote-access VPN, and site-to-site VPN for any location

CONCLUSION

Both converged and dedicated function security and VPN deployments have a role to play in securing today's networks. The decision is driven primarily by the size of the network, the resulting network architecture, location within the network, and the IT support model. The Cisco ASA 5500 Series, with its services breadth, is highly flexible and can be adapted for both converged and dedicated function security and VPN deployments.

Standardizing on the Cisco ASA 5500 Series for multiple deployment environments and security functions within a network simplifies network architectures, thereby reducing deployment and operations costs. The Cisco ASA 5500 Series is a suitable replacement for scenarios where Cisco PIX 515E and PIX 525 security appliances are typically deployed, as well as for IPSec VPN services provided by Cisco VPN 3000 Series concentrators. However, since the ASA 5500 Series uses Cisco PIX and VPN 3000 Series technologies, it is fully feature/function-compatible with existing Cisco PIX and VPN 3000 deployments. For standalone IPS and SSL VPN deployments, the Cisco IPS 4200 Series and VPN 3000 Series Concentrator remain the optimized platforms of choice for those respective functions. For SOHO and large headquarter traditional firewall and site-to-site VPN deployments, Cisco PIX 501, PIX 506E, and PIX 535 security appliances remain the most cost-effective platforms and can complement any multisite Cisco ASA 5500 Series installation.

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

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

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

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

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

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

205226.s_ETMG_KM_4.05

Printed in the USA