Cisco ASA 5500 Series Anti-X Edition

Trend Micro & Cisco

Gateway Collaboration between **Cisco© and Trend Micro™** Continues Commitment to Integrated, Layered Content Security Solutions

White Paper I November 2006

CONTENT

I. EXECUTIVE SUMMARY

Traditionally, businesses have deployed enterprise security solutions to mitigate the risks of virus, worm, and hacker attacks upon their IT infrastructures[1]. While these risks remain, an increasingly complex threat landscape means that organizations now face far more insidious—and potentially more devastating—consequences than system downtime. Loss of intellectual property, identity theft, inadvertent spreading of malware, exposure to legal liabilities, and a damaged business reputation are very real possibilities for businesses that are not adequately protected against endpoint and network threats.

Consolidated, multi function security appliances—ones that combine traditional firewall protection with integrated malware protection—offer organizations increased security against an evolving threat landscape, while mitigating the costs and administrative complexities of layered security solutions. Cisco, pioneers of the Self-Defending Network, and Trend Micro, leaders in secure content and threat management solutions—have partnered to create an integrated security appliance that provides system-level solutions with multiple levels of defense. This solution is called the Cisco ASA 5500 Series Anti-X Edition.

II. BACKGROUND

In order to enable and leverage a more flexible, agile business model, today's small and medium-sized enterprises are pushing their networks further than ever before. Remote and mobile workers are accessing critical company resources over the Internet via a virtual private network (VPN) remote-access connection; supply chain partners—in a collaborative effort to their core competencies and streamline operations—are connecting directly to back-end systems via the Internet; and customers are interacting with secure corporate data to update contact information, purchase goods and services, and execute financial transactions such as wire transfers or stock trades.

> Networks are ". . . no longer just about data. They provide essential communications and services across many lines of business. The explosive growth of mobile communications has deep ramifications. Networking is moving from a passive topology carrying data to an active one. Networks must effectively manage secure, authenticated client connections and reliably enable prioritized traffic flows, such as IP communications traffic."[2]

[1] Business Insights, "Emerging Security Trends and Market Opportunities." V. Furness. June 2006 (p. 20)

[2] Canalys.com, "Enterprise Security Analysis", 9 February 2005.

While this increased interactivity can produce greater efficiency, profitability, and customer satisfaction, it also exposes corporate assets to greater security risks. Remote users often access corporate resources without the protection of a firewall—and frequently use unmanaged devices to do so. With today's rapidly evolving threat landscape—including the increased automation of attacks—this means the traditional perimeter ". . . no longer provides a single point of leverage capable of protecting corporate IT assets from external attacks."[3] Viruses, worms, and hackers remain a serious threat; now, these threats are compounded by content vulnerabilities launched—often unwittingly—by internal and external users accessing the Internet. In order to safeguard data, comply with regulatory mandates, and ensure productivity, organizations must implement an additional layer of security at the Internet gateway—one that complements endpoint and perimeter network defense—to control unwanted content and protect against malicious code such as spyware, spam, and phishing scams.

This, of course, can cause major operational and administrative problems. Layering additional point products on top of existing network security solutions increases both the cost and complexity of an enterprise security infrastructure. Lack of interoperability among products increases the burden on IT staff, and perpetuates an environment of having to add more and more solutions as the threat landscape changes.

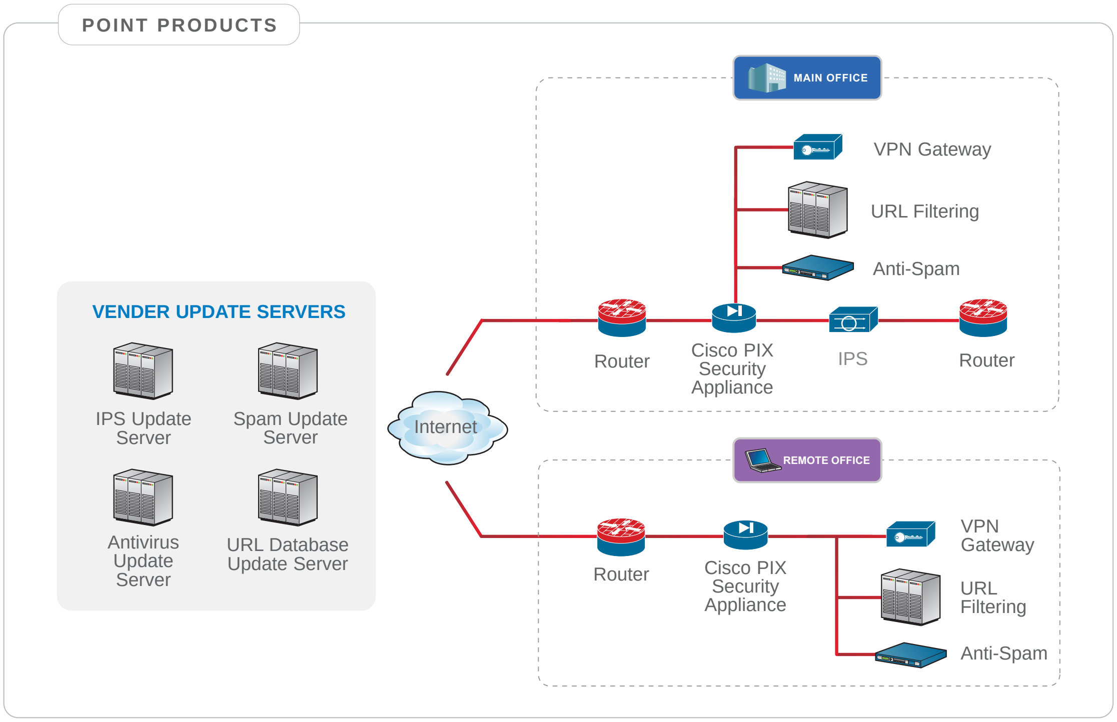


Figure 1 shows a constantly evolving threat landscape means that network security administrators must implement appropriate gateway and endpoint security measures. However, layering multi vendor point product solutions to address discrete security issues causes network complexities that become increasingly difficult to manage.

[3] Gartner Research Note. "Recommendations for Infrastructure Protection." J. Heiser. February 2006.

Because of this, "emerging trends in security include a shift toward appliances, the emergence of multi function security appliances, embedded security and proactivity."[4] Solutions that combine traditional firewall protection with integrated malware protection provide system-level solutions with multiple levels of defense—enabling organizations to more effectively address existing and future threats, while minimizing costs and management challenges.

Cisco and Trend Micro joined forces several years ago to develop ways to migrate security capabilities into the network infrastructure. The Cisco Self-Defending Network strategy and Trend Micro's Enterprise Protection Strategy came together in 2004, with the companies' agreement to deliver security technologies that are not loosely federated, but truly integrated. This shared vision and collaboration among industry leaders provides system-level solutions with multiple levels of defense.

III. CISCO ASA 5500 SERIES ANTI-X EDITION

The ASA 5500 Series Anti-X Edition gateway security appliance—the latest result of the Cisco and Trend Micro collaboration—combines enterprise-grade firewall, VPN, and malware protection into a single platform that combats content threats at the network gateway. The ASA 5500 Series Anti-X Edition delivers secure network access both inside the corporate environment and remotely via IP Security (IPsec) or Secure Sockets Layer (SSL) VPN, and includes antivirus, anti-spam, anti-spyware, anti-phishing, URL blocking, content filtering, and e-mail content filtering capabilities. Its scalable, customizable design enables organizations to protect against existing and new threats as their networks grow and evolve—without compromising budgets or overburdening administrative staff.

As opposed to a loosely federated solution, the joint security features of the ASA 5500 Series Anti-X Edition are truly interoperable. For example, data packets arriving through Port 80 are scanned by the firewall security policy and then passed directly to the Anti-X module. This prevents having to use another protocol such as Internet Content Adaptation Protocol (ICAP) or Web Cache Communication Protocol (WCCP) to transport the packets to an external, or "off-box," product for scanning—providing a distinct performance advantage. Additionally, if a failure occurs in the Anti-X module, a failure in the network chassis is also triggered—meaning that all traffic can automatically be shifted to a failover, or back up, ASA configuration for scanning.

[4] Business Insights, "Emerging Security Trends and Market Opportunities." V. Furness. June 2006 (p. 12)

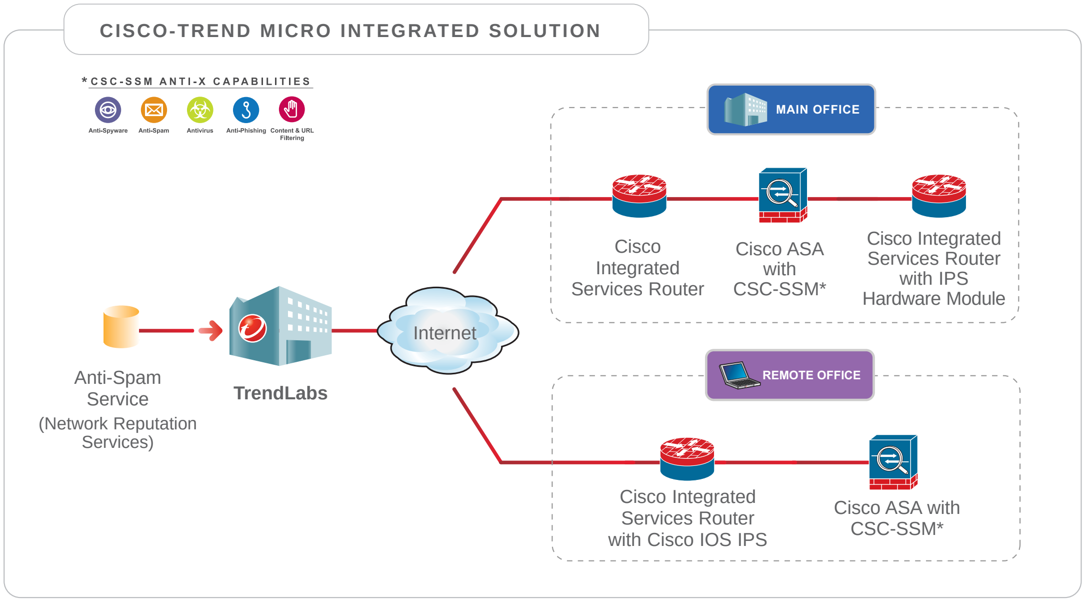

CISCO-TREND MICRO INTEGRATED SOLUTION
*CSC-SSM ANTI-X CAPABILITIES
Anti-Spyware
Anti-Spam
Antivirus
Anti-Phishing
Content & URL Filtering
MAIN OFFICE
Cisco Integrated Services Router
Cisco ASA with CSC-SSM*
Cisco Integrated Services Router with IPS Hardware Module
Anti-Spam Service (Network Reputation Services)
TrendLabs
Internet
REMOTE OFFICE
Cisco Integrated Services Router with Cisco IOS IPS
Cisco ASA with CSC-SSM*

Figure 2 shows the ASA 5500 Series Anti-X Edition combines Trend Micro's market-leading content security solutions with Cisco's market-leading firewall and VPN solutions into a single adaptive security appliance to enable comprehensive gateway security for both local and remote users.

THE ASA 5500 SERIES ANTI-X EDITION INCLUDES THE FOLLOWING CAPABILITIES:

Network Chassis

- **Firewall**

  Building on the Cisco PIX® family of security appliances, the Cisco ASA 5500 Series of adaptive security appliances allows valid business traffic to flow, while prohibiting unwelcome visitors. Its application control capabilities can limit peer-to-peer file sharing, instant messaging, and malicious traffic, while enabling secure deployment of new business applications for improved profitability and competitiveness. This prevents security leaks and the introduction of threats to the network.

- **VPN**

  The Cisco ASA 5500 Series extends the same services to remote-access users, providing a threat-protected VPN connection. Both site-to-site and remote-user access to internal network systems and services are provided, and the solution combines SSL and IPsec VPN capabilities for maximum flexibility. And, since the solution combines firewall and anti-X services with VPN services, the VPN traffic should be free of malware or other threats to the business.

Content Security Module

THREATS			
SPYWARE	SPAM	VIRUS	PHISHING
A software application that monitors a user's computing habits and personal information. This information is sent to third parties without the user's authorization or knowledge.	Unsolicited junk email and a means for planting malware on user's computers.	A piece of executable code —that can corrupt and destroy data	Attacks aim to "fish" or obtain personal information or financial information.
ORGANIZATIONAL IMPACT			
Can harm computer operation and performance, increase privacy and confidentiality risks, make computers less secure, and impose significant costs on business.	Cost to corporations in bandwidth, delayed email, and employee productivity.	Network disruptions to critical systems, loss in employee productivity, costs to remove viruses from network.	Identity theft and loss of confidential information.

- **Anti-spam**
  Originally implemented as the electronic equivalent of junk mail, spam has evolved to include more insidious motivations—including identity theft, widespread distribution of malware, and computer hijacking to promulgate more spam (via the creation of "zombies"). Spam's cost to companies ranges from lost productivity and clogging network bandwidth to legal liability—and it is becoming increasingly difficult to manage. The Cisco ASA 5500 Series Anti-X Edition blocks and removes spam using a sophisticated two-layer defense mechanism. First it uses the network anti-spam service to block up to 80 percent of spam at the ISP level—before it ever reaches the network appliance—by comparing the IP addresses of all incoming mail against Trend Micro's Network Reputation Service (NRS)—the world's largest network reputation database of known spam sources, including zombies and botnets. Next, a sophisticated spam engine combining heuristics, statistical analysis, and signature filters removes remaining spam while minimizing false positives. The ASA 5500 Series Anti-X Edition provides a new delivery paradigm for NRS; instead of the NRS running locally on the network chassis, the chassis can access TrendLabs' Threat Prevention Network universally, in real time—which translates to immediate NRS updates whenever a new spam threat is identified.

- **Antivirus**
  Most organizations have deployed an enterprise-wide desktop antivirus solution. However, this is no longer enough. As the ways into the corporate network (direct on-site access, VPN access, and Internet access, to name a few) become more complex, the need for a layered antivirus solution—one that protects all entry points—becomes increasingly important. For example, third parties such as customers, partners, and contractors are using the corporate network for collaborative advantage—and their devices are beyond the control of internal IT staff and security policies. It is imperative to layer a gateway antivirus solution over existing endpoint solutions in order to ensure a standard level of protection for all network users—regardless of location or relationship to the organization.

Using rules, pattern matching, and heuristics, the Cisco ASA 5500 Series Anti-X Edition blocks viruses—including the newest variants—at the network edge before they can proliferate and cause damage. A scan engine, combined with a pattern matching process, uses a virus pattern to compare files traveling through the gateway with binary patterns of known viruses. If a virus is detected, the scan engine cleans the file by removing the virus code.

Similar to the delivery mechanism of the NRS, the network chassis can access TrendLabs' regional antivirus research and support centers in real time, which guarantees up-to-date virus definitions and effective mitigation strategies.

- **Anti-phishing**
  Phishing scams—serious and increasingly prolific forms of spam—are one of the primary tactics employed in business and consumer identity theft, and are a growing concern among global businesses, their partners, and their customers. In October 2005, the Anti-Phishing Working Group received 15,820 unique phishing reports, compared with only 6,957 in October 2004[5]. Due to the exploitation of emerging threats such as botnets to perpetrate phishing attacks, they are also increasingly difficult to combat.

  The ASA 5500 Series Anti-X Edition offers an additional means of protection against phishing attacks with its identity theft protection capability, which blocks communications with fraudulent Web sites and uses signature file detection to block phishing-related e-mail messages.

- **Anti-spyware**
  Spyware—which conceals itself on Web sites, in downloadable files, and within adware—is a serious threat to today's organizations. Beyond causing system slowdowns and crashes, spyware that monitors users' computing habits and personal information—and sends it to third parties without the users' knowledge—can cause the loss of intellectual property, identity theft, and fraud. And, with a recent IDC survey indicating that "the increasing sophistication of attacks [spyware] is regarded as the top security challenge organizations face over the next 12 months,"[6] it is imperative that those organizations effectively address this threat before it proliferates within the network.

  The ASA 5500 Series Anti-X Edition blocks spyware at the gateway, preventing it from entering the network through Internet (HTTP and FTP) and e-mail traffic. It protects against a broad array of spyware vehicles, including adware, key loggers, event loggers, cookies, screen captors, security disablers, and browser hijackers.

TrendLabs

The ASA 5500 Series Anti-X Edition is backed by timely, high-quality service from TrendLabs—Trend Micro's global network of 7 regional antivirus research and support centers with ISO 9001:2000 and COPC standards certification. A team of more than 700 engineers and antivirus specialists operate around the clock to offer the following real-time services:

- 24x7 virus activity monitoring, threat identification, and defense strategy development
- Outbreak prevention policies and signatures via ActiveUpdate—for real-time deployment to customers around the world
- Replication of each network virus in a lab, and behavior tracking to develop new signatures and improve on existing antivirus technology
- Rigorous testing on new signatures —before any file is released

[5] Anti-Phishing Working Group, www.antiphishing.org

[6] IDC, Worldwide Antispyware 2006-2010 Forecast and Analysis: Boom or Bust? Doc# 202020, June 2006

- **URL blocking and filtering**
  Since the advent of the Internet as a mission-critical business technology, employees have exploited "free" Web access for personal use. While often permitted as a perk to maintain corporate morale, unbridled access can cause decreased productivity, violation of HR policies, security breaches, and legal liability.

  The ASA 5500 Series Anti-X Edition delivers high-performance security for HTTP and FTP traffic at the Internet gateway—blocking access to offensive, inappropriate, or non-work-related Web-sites in real time by querying TrendLabs' comprehensive database of "blacklisted" URLs. This database is updated 24/7, and can be accessed directly by the solution any time a user calls a URL.

- **Content filtering and file blocking**
  E-mail and file-sharing are a perennial risk for organizations. Beyond enabling inadvertent distribution of spam, viruses, and other malware, users who exploit company e-mail for personal pursuits—or who download "free" music or video files via the company network onto company PCs—expose the organization to additional liabilities associated with inappropriate, offensive, or illegal content.

  With the ASA 5500 Series Anti-X Edition, organizations can analyze downloaded files, as well as e-mail messages and attachments, for appropriate content—and automatically block those that do not comply with corporate policies. This helps safeguard intellectual property and confidential information, and minimizes the legal liabilities caused by exposure to offensive material distributed via e-mail.

- **FTP traffic filtering**
  Internet-borne threats can easily be spread via employees directly downloading programs or files from Website and servers—such as instant messengers—that may be contaminated. The ASA 5500 Series Anti-X Edition provides real-time protection of all Web traffic at the Internet gateway, and prevents download of unauthorized or infected content.

BENEFITS:

- **Mitigates risk**
  The Internet has become a critical business tool for organizations of all sizes. It enables new opportunities for growth of the business, provides connectivity with partners and remote workers via VPN connections, and powers critical enterprise services such as communications, supply chain management, and procurement. Small and medium-sized businesses, especially—once unable to fully leverage the Internet due to tight budgets and small staffs—can now avail themselves of the competitive services offered by telecommunications providers, including Wi-Fi® and VoIP, to improve business performance and operational efficiencies, strengthen customer loyalty, and achieve greater market position.

  However, this strategy of using telecommunications services as the "public highway" of corporate information also provides a conduit for threats to enter the network—potentially causing harm to network performance, loss of intellectual property, and identity theft. Because telecom providers' security measures are not designed to protect individual customers' corporate assets, it is imperative that any small or medium-sized business accessing Internet services in this manner install an appropriate layer of protection.

The ASA 5500 Series Anti-X Edition reduces the risks of using Internet-based services with a single, integrated network and content security that provides continuous protection against known and unknown threats, as well as comprehensive access controls. Smaller organizations will also benefit from its ease of use and administration.

- **Helps increase customer satisfaction and loyalty**
  Marketers have long known that the cost of retaining an existing customer is much lower than recruiting a new one. In today's increasingly competitive, global marketplace, customer satisfaction and loyalty have become key drivers toward differentiation.

  In the healthcare industry, for example, hospitals and other entities are fostering loyalty through the creation of patient-centric environments—those in which providers, insurance companies, and patients are linked via secure Web portals offering 24/7 access to medical information, and where caregivers might carry wireless devices to the bedside in order to more efficiently access medical records, physician orders, and prescriptions. While both of these situations help improve patient care and experience, they also expose the network to outside threats such as viruses, keyloggers, and data miners—threats that can compromise the security of confidential patient information and violate Health Insurance Portability and Accountability Act (HIPAA) regulations. If such a compromise were to happen, it would be difficult to recover from the loss of patient confidence, adverse publicity, and litigation.

  The ASA Series 5500 Anti-X Edition enables healthcare providers—and any other organization seeking to extend its network to third-party partners and customers—to implement network-based customer loyalty initiatives with confidence. This integrated solution prevents information leaks (such as medical records) via e-mail, blocks infected PCs from connecting to the network, and effectively manages end-to-end security needs, both at the network gateway and beyond.

- **Improves operational efficiencies**
  Due to their extensive experiences with online shopping, banking, and other Web-centric services, public-sector constituents—students, taxpayers, and employees—are demanding more of these same services from their schools, municipalities, and employers. Traditionally, the public sector has been unable to meet these demands due to small budgets and under-resourced staff—and has suffered major frustrations on the part of its customers and employees as a result. As technologies have become less expensive and more easily managed, however, public agencies have begun piloting new Web-based services such as online class registrations, voter registration, tax payments, and the like—and the resulting efficiencies and positive customer feedback has caused a new wave of demand for Internet-enabled operations. For example, smart-card-based systems for paying turnpike tolls (which use real-time access to drivers' debit accounts), are gaining a foothold across the country as municipalities realize the staff savings, and drivers realize the time savings, effected by such systems.

  However, once an organization opens its network, it faces new security and management challenges. How can it extend back-end systems beyond traditional boundaries without compromising network and data security, for example? How can it effectively protect its constituents from identity theft? And, once the network is opened, how many other risks—such as spam and viruses—must be protected against? How many technical staff will be required to address these new challenges?

The ASA Series 5500 Anti-X Edition enables operational efficiencies at the enterprise level—by protecting network resources accessed via the Internet; and at the administrative level—by reducing the costs associated with the deployment, management, and ongoing monitoring of the security solution with a single, easy-to-install, easy-to-use security solution. This all-in-one solution means that over-worked IT departments can leverage the operational advantages of the Internet without having to manage multiple point security products.

- **Enables compliance**
  Regulatory bodies across the spectrum of verticals have become increasingly concerned with protecting online transactions, and data, from fraudulent activity. For example, the Gramm-Leach Bliley Act expressly prohibits theft of corporate and personal information via pretexting, phishing, and other scams, and requires financial institutions to take demonstrable precautions against such scams. Similarly, HIPAA contains specific rules against misuse of personally identifiable health information, and provides for significant fines to be levied against healthcare entities that do not adequately protect its patients' online data. Sarbanes-Oxley, Basel II, and other acts also include strict regulations for protecting the privacy and security of confidential company and customer information.

  The ASA 5500 Series Anti-X Edition enables industries to comply with a broad range of regulatory requirements by preventing unauthorized access to applications or information assets via identity-based access control services contained within its firewall function. This capability can tie into services like Microsoft® Active directory®, Lightweight Directory Access Protocol (LDAP), or RSA SecurID.

- **Helps safeguard brand equity and reputation**
  Hijacking bank accounts (via Internet-based phishing attacks, keystroke logging, and malware plants on customers' PCs) is the most rapidly proliferating form of fraud, and increased coverage of the threat by major media outlets is causing customers to be highly concerned with using online services. A lack of consumer confidence can quickly erode brand equity; no industry is immune from the deleterious effects of phishing scams and other fraudulent online activites.

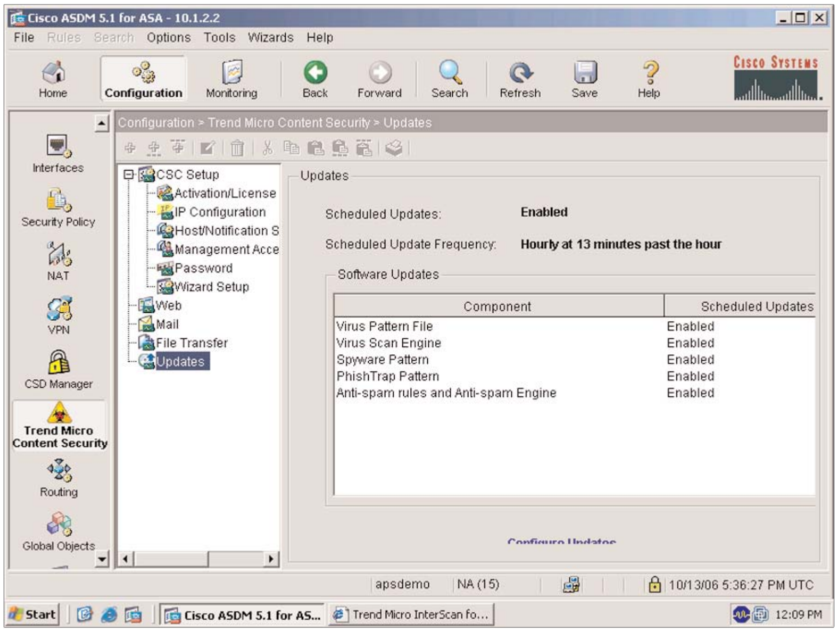
  In fact, a recent Deloitte Touche Tohmatsu report posits that "customers instill a great deal of trust in contemporary . . . companies, and may increasingly migrate towards those which are able to demonstrate a comprehensive and credible approach to securing all of their digital assets, processes and transactions."[7] A recent Privacy Trust Survey for Online Banking, conducted by the Ponemon Institute, supports this claim. In March 2005, 57 percent of 2300 users of online banking services reported that only one privacy incident—such as identity theft or unauthorized access to their accounts—would cause them to take their business to a competitor.[8] And, with recent high-profile incidents, such as lawsuits against major national banks by customers who have fallen prey to phishing scams, erosion of thrust and brand damage is a very real concern.

  The ASA 5500 Series Anti-X Edition's signature file detection capabilities block viruses, spyware, and fraudulent e-mail messages related to phishing attacks, which are difficult for traditional spam filters to distinguish from legitimate mail. This improves protection against identity theft and loss of confidential information, such as credit card and bank account numbers, usernames, and passwords—and can alleviate consumer concerns about fraud.

[7] Deloitte Touche Tohmatsu, "Protecting the Digital Assets: The 2006 Technology, Media, and Telecommunications Survey." www.deloitte.com/dtt/cda/doc/content/UK_DR_Protectingthedigitalassets_TMT.pdf

[8] Computerworld. "Trust in Online Banking: Hard to Earn, Easy to Lose." Larry Ponemon, April 26, 2005. www.computerworld.com/securitytopics/security/story/0,10801,101341,00.html

- **Provides ease of administration**
  The streamlined management features of the ASA 5500 Series Anti-X Edition enables even the smallest organizations to access market-leading security capabilities. The convergence of a network device with a content security system into a single, interoperable appliance means that existing IT staff can quickly install, deploy, and manage the solution—with little or no additional training required.



Updates

Scheduled Updates: **Enabled**

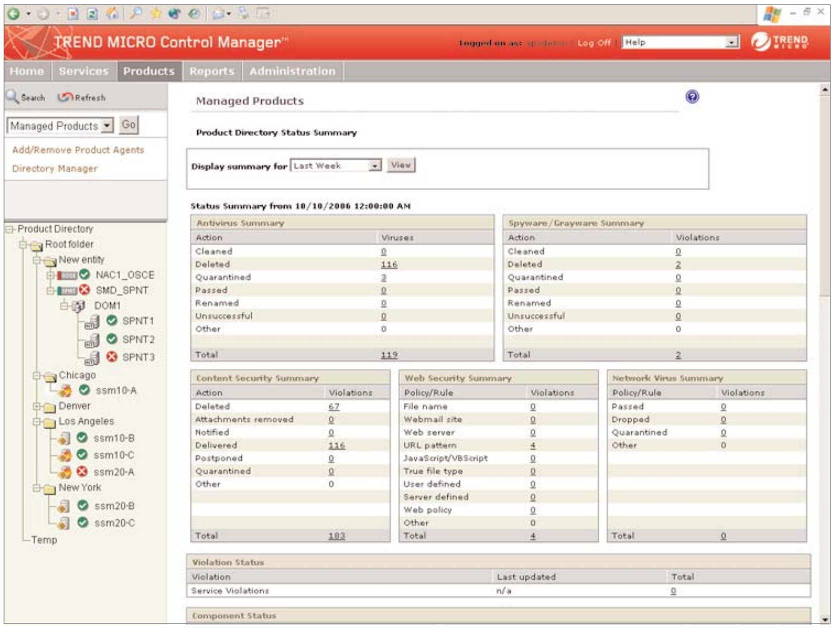
Scheduled Update Frequency: **Hourly at 13 minutes past the hour**

Software Updates

Component	Scheduled Updates
Virus Pattern File	Enabled
Virus Scan Engine	Enabled
Spyware Pattern	Enabled
PhishTrap Pattern	Enabled
Anti-spam rules and Anti-spam Engine	Enabled

Figure 3 shows the ASA 5500 Series Anti-X Edition includes a centralized management console that provides a powerful yet easy-to-use browser-based management and monitoring interface. This single solution provides comprehensive configuration and monitoring of all the services in a single application. And to help with quick deployment, wizards guide administrators through initial and ongoing configuration of their ASA 5500 Series appliances.

Additionally, the Trend Micro Control Manager™ enables organizations with more than one ASA 5500 Series Anti-X Edition appliance to manage all Cisco content security modules and Trend Micro products from one central location. Control Manager provides a unified view of malware activity in an organization from a single console, helps enforce one common security policy across all content security devices and guarantees protection against the latest threats with its timely update and deployment using industry proven technology. It also consolidates data for easier reporting and analysis.



Managed Products

Product Directory Status Summary

Display summary for: Last Week

Status Summary from 10/10/2006 12:00:00 AM

Antivirus Summary

Action	Viruses
Cleaned	0
Deleted	116
Quarantined	3
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	119

Spyware/Grayware Summary

Action	Violations
Cleaned	0
Deleted	2
Quarantined	0
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	2

Content Security Summary

Action	Violations
Deleted	67
Attachments removed	0
Notified	0
Delivered	116
Postponed	0
Quarantined	0
Other	0
Total	183

Web Security Summary

Policy/Rule	Violations
File name	0
Webmail site	0
Web server	0
URL pattern	4
JavaScript/VBScript	0
True file type	0
User defined	0
Server defined	0
Web policy	0
Other	0
Total	4

Network Virus Summary

Policy/Rule	Violations
Passed	0
Dropped	0
Quarantined	0
Other	0
Total	0

Violation Status

Violation	Last updated	Total
Service Violations	n/a	0

Component Status

Figure 4 shows the ASA 5500 Series Anti-X Edition includes a centralized management console that provides a powerful, yet easy-to-use, browser-based management and monitoring interface. This single solution provides comprehensive configuration and monitoring of all the services in a single application. And to help with quick deployment, wizards guide administrators through initial and ongoing configuration of their ASA 5500 Series appliances.

- **Maintains employee productivity**
  The ASA 5500 Series Anti-X Edition safeguards both non-technical and IT staff alike from drops in productivity. By blocking spam and spyware, it prevents IT staff from being bogged down by help desk tickets and other system slowdown-related activities. By blocking inappropriate Web browsing, it prevents employees from sinking company time into personal pursuits.

IV. TREND MICRO AND CISCO—A LONG-TERM, VISIONARY PARTNERSHIP DEDICATED TO TIGHTER INTEGRATION BEYOND THE NETWORK GATEWAY

Recognizing the increasing operational and fiscal challenges faced by organizations seeking to implement effective security solutions, Trend Micro and Cisco joined forces in 2004 with the express goal of alleviating some of those pressures. The foundational principles of the relationship, which persist today, are based upon a joint commitment to integrate Trend Micro threat defense technologies into Cisco products; to ensure interoperability of Trend Micro security solutions and Cisco network infrastructures; and to strive for a seamless customer service experience. Historically, the two companies have successfully leveraged these principles via the following collaborative projects:

- **Co-development of outbreak signatures for Cisco appliances (August 2004)**
  TrendLabs' global monitoring capabilities—including threat intelligence, IPS signatures, and rapid response to and proactive prevention of threats—empowers existing Cisco network devices to adapt in real time for a coordinated, network-wide response to attack.

- **Charter member of the Network Admission Control (NAC) initiative**
  In November 2003, Cisco launched the Network Admission Control (NAC) initiative—an industry wide, multi vendor collaboration conceived to minimize the damage organizations face from emerging security threats through product interoperability. This foundational collaboration between Trend Micro and Cisco provides network admission policy enforcement, antivirus software, and network resources to dramatically improve network security at the endpoints. To date, more than 75 third-party vendors participate in this initiative.

NAC FRAMEWORK SOLUTIONS OFFICESCAN ENDPOINT SECURITY

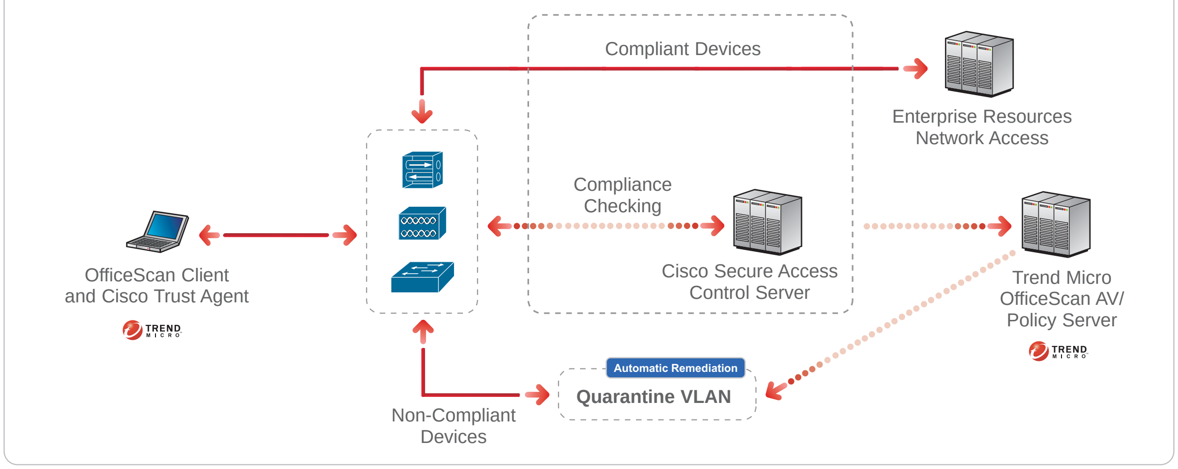


Figure 5 show the Trend Micro™–Cisco® NAC solution integrates network admission policy enforcement, antivirus software, and network resources to dramatically improve network security and terminate viruses and threats.

The ASA 5500 Series Anti-X Edition adaptive security appliance is the latest demonstration of the companies' continuing commitment to support organizations of all types and sizes as they combat a constantly changing threat landscape.

V. ABOUT TREND MICRO

Trend Micro Incorporated (TSE: 4704, NASDAQ: TMIC) is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit www.trendmicro.com.

VI. ABOUT CISCO SYSTEMS

Cisco Systems, Inc. (NASDAQ: CSCO) is the worldwide leader in networking for the Internet. News and information are available at www.cisco.com.

VII. FOR MORE INFORMATION

For more information about the ASA-5500 Series Anti-X Edition product, contact:

TREND MICRO INCORPORATED
Corporate Headquarters
10101 N. De Anza Blvd.
Cupertino, CA 95014 USA
Phone: (408) 257-1500 or (800) 228-5651
Web: www.trendmicro.com

Direct product information link:
www.trendmicro.com/en/partners/alliances/cisco/csc-ssm/overview.htm

CISCO SYSTEMS, INC.
Corporate Headquarters
170 West Tasman Dr.
San Jose, CA 95134 USA
Phone: (408) 526-4000 or (800) 553-6387
Web: www.cisco.com

Direct product information link:
www.cisco.com/en/US/products/ps6120/prod_brochure0900aecd80402e88.html

CISCO
Cisco has more than 2000 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

CISCO SYSTEMS, INC.
170 West Tasman Drive
San Jose, CA. 95134, USA
toll free: 1+800-553-NETS (6387)
phone: 1+408-526-4000
fax: 1+408-526-4100

TREND MICRO™
Trend Micro, Inc. is a global leader in network antivirus and Internet content security products and services. The company is focused on providing customers with customized and comprehensive security strategies to manage the impacts of known and unknown threats. Trend Micro has offices in 30 countries and its stock trades on the Tokyo Stock Exchange (4704) and on NASDAQ (TMIC).

TREND MICRO INC.
10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com