

Cisco ASA 5500 Series Overview

Cisco® ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that integrate world-class firewall, unified communications security, VPN, intrusion prevention (IPS), and content security services in a unified platform. The series builds upon proven technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators. Cisco ASA 5500 Series Adaptive Security Appliances are a key component of the Cisco Self-Defending Network. The Cisco ASA 5500 Series provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network and application activity, and flexibly delivers granular, secure remote access and site-to-site connectivity.

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, and 5580 Adaptive Security Appliances—purpose-built, high-performance security solutions that take advantage of Cisco's expertise in developing industry-leading, award-winning security and VPN solutions. Through its unique Modular Policy Framework (MPF), the Cisco ASA 5500 Series enables highly customizable, flow-specific security policies that can be tailored to application requirements. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs.

Secure unified communications: With extensive protocol support, signaling and media inspection, remote office and mobile user support, and simple provisioning, the Cisco ASA 5500 Series delivers market-leading protection for voice, video, and multimedia traffic to enable businesses to take advantage of the benefits of an integrated voice and data network.

Site-to-Site VPN: Using the hardware-accelerated site-to-site IPsec VPN capabilities provided by the Cisco ASA 5500 Series, businesses can securely augment or even replace legacy WANs by using low-cost Internet connections and IPsec VPN tunnels to connect to business partners and to remote and satellite offices worldwide.

Secure remote access: The Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit connectivity requirements for employee desktops and laptops that are company managed and for remote access for non-company-managed endpoints, such as Internet kiosks or employee-owned desktops and handhelds the Cisco ASA 5500 Series delivers both clientless and web-deployed SSL/DTLS VPN remote-access client options.

Figure 2. Market Leading Application/IPS/Content Security Services

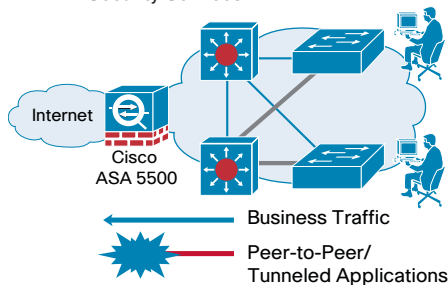


Figure 1. ASA 5500 Series



Figure 3. Secure Unified Communications

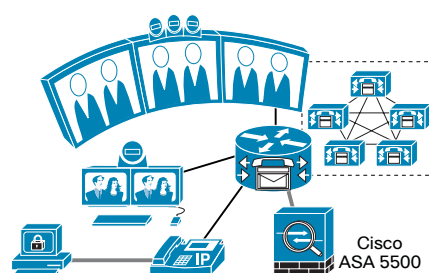


Figure 4. Threat Protected SSL and IPsec VPN Services

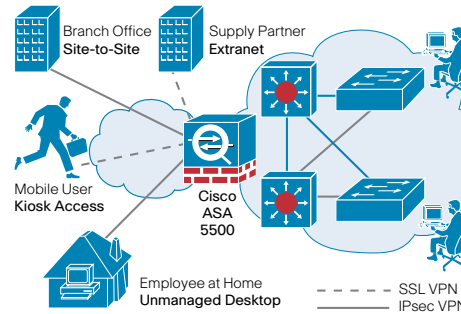
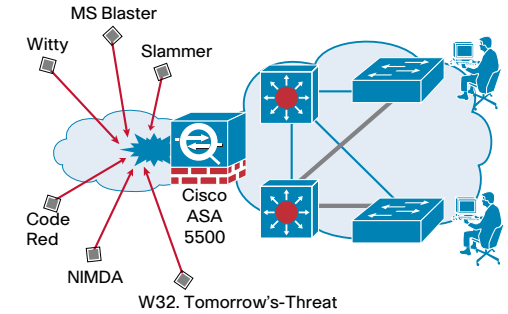


Figure 5. Industry Leading IPS/Content Security Service



Top 5 Reasons to Purchase Cisco ASA 5500 Series Adaptive Security Appliances

1. Reduced Deployment Costs and Proven Technology

The Cisco ASA 5500 Series is built upon extensively deployed and trusted Cisco PIX and Cisco VPN concentrator technology. By providing a design and interface consistent with existing Cisco security solutions, the Cisco ASA 5500 Series enables significantly lower ownership costs for both initial security deployments and day-to-day management.

2. Advanced Intrusion Prevention Services

The Cisco ASA 5500 Series combines vulnerability-based and exploit-based signatures to provide unparalleled detection of both known and tested exploits, as well as exploits yet to be written (zero-day exploits), for both IPv6 and IPv4 networks. It protects against a wide range of threats, including worms, application-layer attacks, operating-system-level attacks, rootkits, spyware, peer-to-peer file sharing, and instant messaging.

3. Industry-Leading Content Security Services

The Cisco ASA 5500 Series combines Trend Micro's expertise in threat protection and content control at the Internet edge with proven Cisco solutions, providing comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering services.

4. Secure Remote Access and Unified Communications

The Cisco ASA 5500 Series delivers market-leading secure access by enabling protection for voice, video, and multimedia traffic and remote access. Businesses can securely take advantage of the improved productivity and lower operational costs of a Cisco Unified Communications solution. Cisco secure remote access solutions provide business employees and partners with ubiquitous, highly secure access to enable employee mobility, enhance collaboration, and improve productivity, while protecting the company's resources and data.

5. Comprehensive Management and Monitoring Services

Several elements round out a rich complement of management options: with Cisco Adaptive Security Device Manager (ASDM), a comprehensive CLI, verbose syslog, and support for Simple Network Management Protocol (SNMP). Cisco Security Manager (CSM) and Cisco Security Monitoring, Analysis, and Response System (MARS) support distributed deployments of up to 5000 devices.



Cisco ASA 5500 Series Adaptive Security Appliances

Acronyms

SSC: Security Services Card, **SSM:** Security Services Module, **AIP SSM:** Advanced Inspection and Prevention Security Services Module, **CSC SSM:** Content Security and Control Security Services Module, **4GE SSM:** 4 Gigabit Ethernet Security Services Module, **IEC:** Interface Expansion Card,

Cisco ASA 5500 Series Model/License	Cisco ASA 5505 Base / Security Plus ²	Cisco ASA 5510 Base / Security Plus ²	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Market	Branch office/Small Business, Enterprise Teleworker	SMB and Small Enterprise	Small Enterprise	Medium-Sized Enterprise	Large Enterprise	Large Enterprise, Data Center	Large Enterprise, Data Center
Performance Summary							
Maximum Firewall Throughput (Mbps)	150	300	450	650	1200	5 Gbps (real-world HTTP), 10 Gbps (jumbo frames)	10 Gbps (real-world HTTP), 20 Gbps (jumbo frames)
Maximum 3DES/AES VPN Throughput (Mbps)	100	170	225	325	425	1000	1000
Maximum Site-to-Site and Remote-Access VPN User Sessions	10 / 25	250	750	5000	5000	10000	10000
Maximum SSL VPN User Sessions ¹	25	250	750	2500	5000	10000	10000
Maximum Connections	10000 / 25,000	50,000 / 130,000	280,000	400,000	650,000	1,000,000	2,000,000
Maximum Connections/Second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per Second (64 byte)	85,000	190,000	320,000	500,000	600,000	2,500,000	4,000,000
Technical Summary							
Memory	256 MB	256 MB	512 MB	1 GB	4 GB	8 GB	12 GB
System Flash	64 MB	64 MB	64 MB	64 MB	64 MB	1 GB	1 GB
Integrated Ports	8 port 10/100 switch with 2 Power over Ethernet ports	5-10/100 / 2-10/100/1000, 3-10/100	4-10/100/1000, 1-10/100	4-10/100/1000, 1-10/100	8-10/100/1000, 4-GE SFP, 1-10/100	2-10/100/1000 Mgmt	2-10/100/1000 Mgmt
Maximum Virtual Interfaces (VLANs)	3 (trunking disabled) / 20 (trunking enabled)	50 / 100	150	200	250	250	250
SSC/SSM/IEC Expansion Slot	Yes (1-SSC)	Yes (1-SSM)	Yes (1-SSM)	Yes (1-SSM)	Not Available	Yes (6-IEC)	Yes (6-IEC)
SSC/SSM/IEC Capabilities							
SSC/SSM/IEC Supported	AIP SSC	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	Not Available	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC
Intrusion Prevention	Yes (with AIP SSC)	Yes (with AIP SSM)	Yes (with AIP SSM)	Yes (with AIP SSM)	Yes (with AIP SSC)	Yes (with AIP SSC)	Yes (with AIP SSC)
Maximum Firewall and IPS Throughput (Mbps)	75 (with AIP SSC-5)	150 (with AIP SSM-10) 300 (with AIP SSM-20)	225 (with AIP SSM-10) 375 (with AIP SSM-20) 450 (with AIP SSM-40)	500 (with AIP SSM-20) 650 (with AIP SSM-40)	75 (with AIP SSC-5)	75 (with AIP SSC-5)	75 (with AIP SSC-5)
Content Security (Antivirus, Anti-Spyware, File Blocking, Anti-Spam, Anti-Phishing, and URL Filtering)	Not available	Yes (with CSC SSM)	Yes (with CSC SSM)	Yes (with CSC SSM)	Not Available	Not Available	Not Available
Maximum Number of Users for Antivirus, Anti-Spyware, File Blocking (CSC-SSM Only)	Not available	500 (CSC SSM-10) 1000 (CSC SSM-20)	500 (CSC SSM-10) 1000 (CSC SSM-20)	500 (CSC SSM-10) 1000 (CSC SSM-20)	Not Available	Not Available	Not Available
CSC SSM Plus License Features	Not available	Anti-spam, anti-phishing, URL filtering	Anti-spam, anti-phishing, URL filtering	Anti-spam, anti-phishing, URL filtering	Not Available	Not Available	Not Available
Features							
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewalling	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security Contexts (Included/Maximum) ²	0/0	0/0 / 2/5	2/20	2/50	2/50	2/50	2/50
GTP/GPRS Inspection ²	Not available	Not available	Yes	Yes	Yes	Yes	Yes
High-Availability Support ³	Not available / Stateless A/S	Not available / A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S
VPN Clustering and Load Balancing	Not available	Not available / Yes	Yes	Yes	Yes	Yes	Yes

¹ Beginning with Cisco ASA Software v7.1, SSL VPN (WebVPN) capability requires a license. Systems include 2 SSL VPN users by default for evaluation and remote management purposes

² Licensed features

³ A/S = Active/Standby; A/A = Active/Active

Note: Performance numbers tested and validated with the ASA 72 Software Release