Cisco ASA 5500 Series Overview

A key component of the Cisco® Secure Borderless Network, the Cisco ASA 5500 Series Adaptive Security Appliances delivers superior scalability, a broad span of technology and solutions, and effective, always-on security designed to meet the needs of an array of deployments. By integrating the world's most proven firewall; a comprehensive, highly effective intrusion prevention system (IPS) with Cisco Global Correlation and guaranteed coverage; and a high-performance VPN, the Cisco ASA 5500 Series helps organizations provide secure, high performance connectivity and protects critical assets for maximum productivity.

Offering seamless client and clientless access for a broad spectrum of desktop and mobile platforms, the Cisco ASA 5500 Series delivers versatile, always-on secure mobility integrated with web security and IPS for a comprehensive solution. Unlike most security providers that force you to choose between a high-quality firewall and an effective intrusion prevention system (IPS), Cisco combines the world's most proven firewall with the industry's most comprehensive, effective IPS for a powerful security solution.

Figure 1. Cisco ASA 5500 Series

The Cisco ASA 5500 Series delivers superior real-time protection: Integrating innovative IPS with Global Correlation, firewall, and VPN technology, the Cisco ASA 5500 Series delivers highly effective intrusion prevention capabilities using hardware-accelerated IPS modules. And Cisco guaranteed coverage delivers peace of mind.

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 mobility: The Cisco ASA 5500 Series offers flexible technologies that deliver tailored solutions to suit connectivity and secure mobility requirements for company-managed assets such as desktops, laptops and smartphones, as well as unmanaged devices such as Internet kiosks or employee-owned desktops, laptops and handhelds. The Cisco ASA 5500 Series delivers both clientless and SSL/DTLS/IPsec VPN secure mobility client options.

Secure unified communications: The Cisco ASA 5500 Series provides extensive protocol support, signaling and media inspection, remote office and mobile user support, and simple provisioning to enable a secure, integrated voice and data network.

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

1. Advanced intrusion prevention services with guaranteed coverage
   With real-time reputation technology, the Cisco ASA 5500 Series IPS with Global Correlation is twice as effective as legacy IPS and includes guaranteed coverage for greater peace of mind. 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 for both IPv6 and IPv4 networks.
2. Industry-leading content security services
   With the Cisco ASA 5500 Series, customers have their choice of on-box threat protection and content control based on Trend Micro technology, or a proven off-box solution with the Cisco IronPort Web Security Appliance. Both solutions provide comprehensive antivirus, antispyware, file blocking, antispam, antiphishing, URL blocking and filtering, and content filtering services.

3. Secure mobility
   The Cisco AnyConnect Secure Mobility solution provides 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 from web-based threats and data leakage by enforcing acceptable use policies.
4. Unified communications
   The Cisco ASA 5500 Series delivers secure access by enabling protection for voice, video, and multimedia traffic. Businesses can securely take advantage of the improved productivity and lower operational costs of a Cisco Unified Communications solution.
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 supports distributed deployments of up to 500 devices.

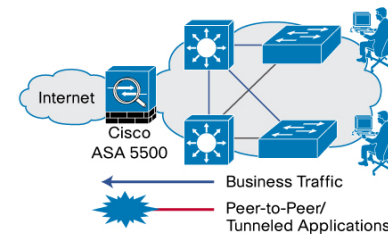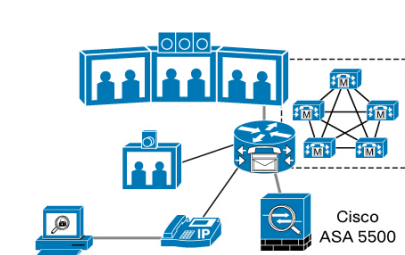**Figure 2.** Market-Leading Application/IPS/Content Security Services

Internet — Cisco ASA 5500

← Business Traffic
— Peer-to-Peer/Tunneled Applications

Figure 3. Secure Unified Communications

Cisco ASA 5500

Figure 4. Threat-Protected SSL and IPsec VPN Services

Branch Office Site-to-Site
Supply Partner Extranet
Mobile User Kiosk Access
Cisco ASA 5500
Employee at Home Unmanaged Desktop
- - - SSL VPN
— IPsec VPN
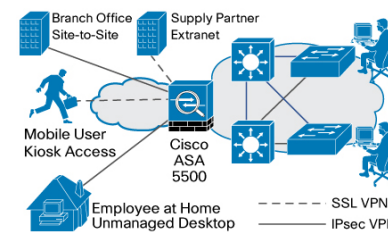
Figure 5. Industry-Leading IPS/Content Security Service

Compromised Websites
SQL injection
Cisco ASA 5500
Worms
Botnets
Targeted Attacks
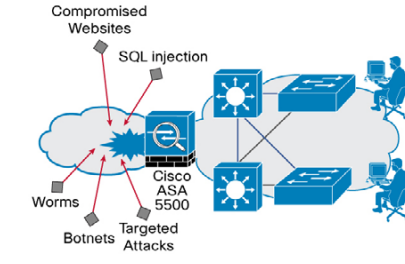
Acronyms

SSC: Security Services Card; **SSM:** Security Services Module; **SSM:** Security Services Module; **CSC SSM:** Content Security and Control Security Services Module; **4GE SSM:** 4 Gigabit Ethernet Security Services Module; **SSP:** Security Services Processor; **IPS SSP:** IPS Security Services Processor; **IEC:** Interface Expansion Card.

Table 1. Cisco ASA 5505, 5510, 5520, 5540, 5550 Product Comparison

Cisco ASA 5500 Series Model/License	Cisco ASA 5505 Base / Security Plus[1]	Cisco ASA 5510 Base / Security Plus[1]	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
Market	Branch Office/Small Business, Enterprise Teleworker	SMB and Small Enterprise	Small Enterprise	Medium-Sized Enterprise	Large Enterprise
Performance Summary					
Maximum Firewall Throughput (Mbps)	150	300	450	650	1200
Maximum 3DES/AES VPN Throughput (Mbps)[2]	100	170	225	325	425
Maximum Site-to-Site and IPsec IKEv1 client VPN Sessions	10/25	250	750	5000	5000
Maximum AnyConnect or Clientless User Sessions	25	250	750	2500	5000
Maximum Connections	10,000/25,000	50,000/130,000	280,000	400,000	650,000
Maximum Connections/Second	4000	9000	12,000	25,000	36,000
Packets per Second (64 byte)	85,000	190,000	320,000	500,000	600,000
Technical Summary					
Minimum Memory	512 MB	1 GB	2 GB	2 GB	4 GB
Minimum System Flash	128 MB	256 MB	256 MB	256 MB	256 MB
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
Maximum Virtual Interfaces (VLANs)	3 (trunking disabled)/20 (trunking enabled)	50/100	150	200	400
SSP/SSM/SSC/IEC Expansion Slot	Yes (1-SSC)	Yes (1-SSM)	Yes (1-SSM)	Yes (1-SSM)	Not Available
SSC/SSM/IEC Capabilities					
SSP/SSM/SSC/IEC Supported	AIP SSC	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	CSC SSM, AIP SSM, 4GE SSM	Not Available
Intrusion Prevention	Yes (with AIP SSC)	Yes (with AIP SSM)	Yes (with AIP SSM)	Yes (with AIP SSM)	Not Available
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)	Not Available
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
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
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
Features					
Application-Layer Security	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewalling	Yes	Yes	Yes	Yes	Yes
Security Contexts (Included/Maximum[1])	0/0	0/0/2/5	2/20	2/50	2/100
GTP/GPRS Inspection[1]	Not Available	Not Available	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
VPN Clustering and Load Balancing	Not Available	Not Available/Yes	Yes	Yes	Yes

[1] Licensed features

[2] VPN throughput and sessions count depend on the ASA device configuration and VPN traffic patterns. These elements should be taken in to consideration as part of your capacity planning

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

Table 2.   Cisco ASA 5580 and ASA 5585-X Product Comparison

Cisco ASA 5500 Series Model/License	Cisco ASA 5580-20	Cisco ASA 5580-40	Cisco ASA 5585-X SSP-10	Cisco ASA 5585-X SSP-20	Cisco ASA 5585-X SSP-40	Cisco ASA 5585-X SSP-60
Market	Large Enterprise, Data Center	Large Enterprise, Data Center	Large Enterprise	Large Enterprise, Data Center	Large Enterprise, Data Center	Large Enterprise, Data Center
Performance Summary						
Firewall Throughput (max[1])	10 Gbps	20 Gbs	4 Gbps	10 Gbps	20 Gbps	40 Gbps
Firewall Throughput	5 Gbps (real-world HTTP)	10 Gbps (real-world HTTP)	2 Gbps (multi-protocol)	5 Gbps (multi-protocol)	10 Gbps (multi-protocol)	20 Gbps (multi-protocol)
Maximum 3DES/AES VPN2 Throughput[2]	1 Gbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Maximum Site-to-Site and IPsec IKEv1 client VPN User Sessions	10,000	10,000	5000	10,000	10,000	10,000
Maximum AnyConnect or Clientless VPN User Sessions	10,000	10,000	5000	10,000	10,000	10,000
Maximum Connections	2,000,000	4,000,000	1,000,000	2,000,000	4,000,000	10,000,000
Maximum Connections/Second	90,000	150,000	50,000	125,000	200,000	350,000
Packets per Second (64 byte)	2,500,000	4,000,000	1,500,000	3,000,000	5,000,000	9,000,000
Technical Summary						
Minimum Memory	8 GB	12 GB	6 GB	12 GB	12 GB	24 GB
Minimum System Flash	1 GB	1 GB	2 GB	2 GB	2 GB	2 GB
Integrated Ports	2-10/100/1000 Mgmt	2-10/100/1000 Mgmt	8-10/100/1000, 2-10GE[3] (SSP-10) 16-10/100/1000, 4-10GE[3] (SSP-10 and IPS SSP-10)	8- 10/100/1000, 2-10GE[3] SFP+(SSP-20) 16-10/100/1000, 4-10GE[3] SFP+(SSP-20 and IPS SSP-20)	6- 10/100/10 00, 4-10GE SFP+(SSP-40) 12-10/100/1000, 8-10GE SFP+(SSP-40 and IPS SSP-40)	6-10/100/1000, 4-10GE SFP+(SSP-60) 12-10/100/1000, 8-10GE SFP+(SSP-60 and IPS SSP-60)
Maximum Virtual Interfaces (VLANs)	1024	1024	1024	1024	1024	1024
SSP/IEC Expansion Slot	Yes (6-IEC)	Yes (6-IEC)	Yes (1-IPS-SSP)	Yes (1-IPS-SSP)	Yes (1-IPS-SSP)	Yes (1-IPS-SSP)
SSP/IEC Capabilities						
SSP/IEC Supported	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC	4-10/100/1000, 4-GE SR LC, 2-10GE SR LC	SSP, IPS SSP	SSP, IPS SSP	SSP, IPS SSP	SSP, IPS SSP
Intrusion Prevention	Not Available	Not Available	Yes (with IPS SSP)	Yes (with IPS SSP)	Yes (with IPS SSP)	Yes (with IPS SSP)
Maximum Firewall and IPS Throughput	Not Available	Not Available	2 Gbps (with IPS SSP-10)	3 Gbps (with IPS SSP-20)	5 Gbps (with IPS SSP-40)	10 Gbps (with IPS SSP-60)
Features						
Application-Layer Security	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2 Transparent Firewalling	Yes	Yes	Yes	Yes	Yes	Yes
Security Contexts (Included/ Maximum)[3]	2/250	2/250	2/100	2/250	2/250	2/250
GTP/GPRS Inspection[3]	Yes	Yes	Yes	Yes	Yes	Yes
High-Availability Support[4]	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	Yes	Yes	Yes	Yes	Yes	Yes

[1] Max firewall throughput measured under ideal test conditions

[2] VPN throughput and sessions count depend on the ASA device configuration and VPN traffic patterns. These elements should be taken in to consideration as part of your capacity planning

[3] Licensed features

[4] A/S = Active/Standby; A/A = Active/Active

Note: Performance numbers tested and validated with the ASA 7.2 software release for ASA 5505 through ASA 5540, and the ASA 8.4 software release for ASA 5550 through ASA 5585-X.