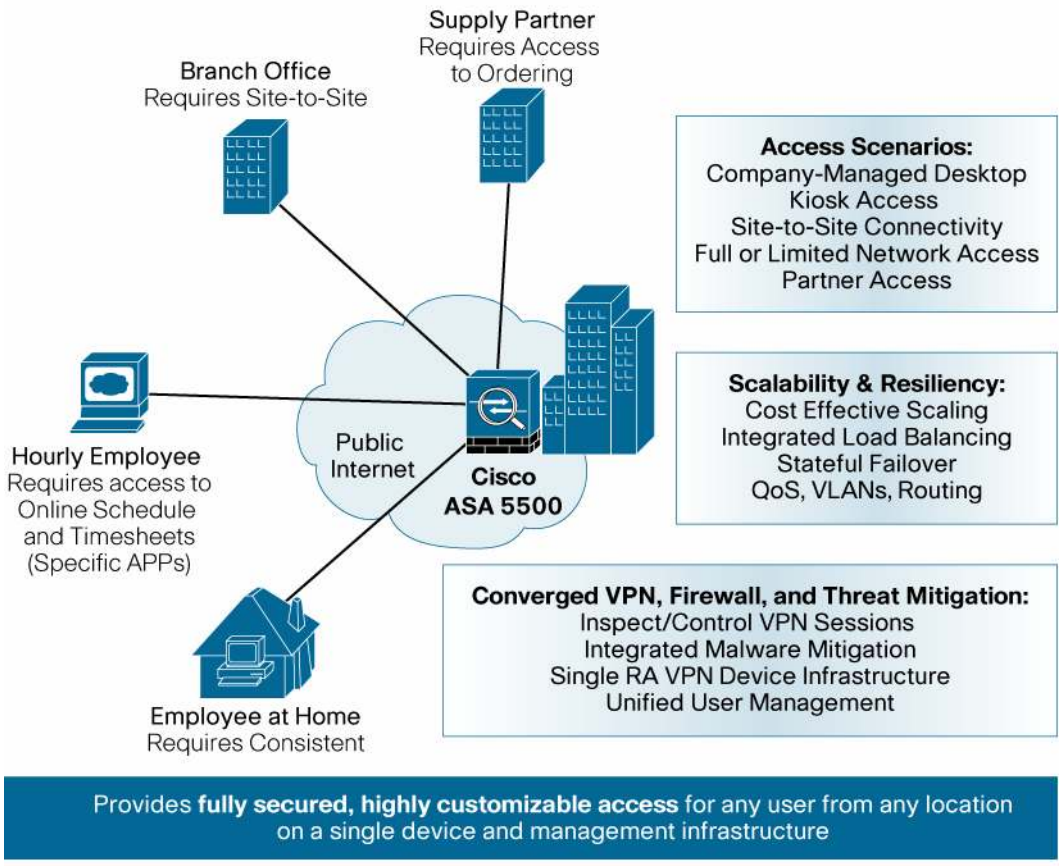
Cisco Secure Remote Access—Cisco ASA 5500 Series SSL/IPsec VPN Edition

The Cisco® ASA 5500 Series Adaptive Security Appliance is a purpose-built platform that combines best-in-class security and VPN services for small and medium-sized business (SMB) and enterprise applications. The Cisco ASA 5500 Series enables customization for specific deployment environments and options, with special product editions for secure remote access (SSL/IPsec VPN), firewall, content security, and intrusion prevention.

The Cisco ASA 5500 Series SSL/IPsec VPN Edition (also known as the Cisco Secure Remote Access solution) enables organizations to gain the connectivity and cost benefits of Internet transport without compromising the integrity of corporate security policies. By converging Secure Sockets Layer (SSL) and IP Security (IPsec) VPN services with comprehensive threat defense technologies, the Cisco ASA 5500 Series delivers highly customizable network access tailored to the requirements of diverse deployment environments while providing advanced endpoint and network-level security (Figure 1).

Figure 1. Customizable VPN Services for Any Deployment Scenario



Cisco ASA 5500 Series Secure Remote Access

The Cisco Secure Remote Access solution offers flexible VPN technologies for any connectivity scenario, with scalability up to 10,000 concurrent users per device. It provides easy-to-manage, full-tunnel network access through SSL, Datagram Transport Layer Security (DTLS), IPsec VPN client technologies, Cisco AnyConnect Secure Mobility optimized for the Cisco IronPort® Web Security Appliance, advanced clientless SSL VPN capabilities, and network-aware site-to-site VPN connectivity, enabling secure connections across public networks to mobile users, remote sites, contractors, and business partners. Costs associated with VPN deployment and operations are reduced by eliminating ancillary equipment required to scale and secure a VPN.

Benefits of a Cisco Secure Remote Access solution include:

- **SSL, DTLS, and IPsec-based full network access—**Full network access provides network-layer remote-user connectivity to virtually any application or network resource and is often used to extend access to managed computers such as company-owned laptops. Connectivity is available through the automatically downloaded Cisco AnyConnect Secure Mobility client, the Cisco IPsec VPN Client, the Microsoft Layer 2 Tunneling Protocol (L2TP)/IPsec VPN client, and the Apple iPhone / Mac OS X 10.6 IPsec VPN clients. The Cisco AnyConnect Secure Mobility client will automatically adapt its tunneling protocol to the most efficient method based on network constraints, and is the first VPN product to use the DTLS protocol to provide an optimized connection for latency-sensitive traffic, such as voice-over-IP (VoIP) traffic or TCP-based application access. By supporting SSL, DTLS, and IPsec-based remote-access VPN technologies, the Cisco ASA 5500 Series delivers unsurpassed flexibility to meet the needs of the most diverse deployment scenarios.
- **Superior clientless network access—**Clientless remote access provides access to network applications and resources, regardless of location, without the need for desktop VPN client software. Using the ubiquity of SSL encryption available in Internet browsers, the Cisco ASA 5500 Series delivers clientless access to any web-based application or resource, terminal services applications such as Citrix, and optimized Microsoft Outlook Web Access and Lotus iNotes, as well as access to common thick-client applications such as email, calendar, instant messaging, FTP, Telnet, and SSH applications. Additionally, the superior content rewriting capabilities of the Cisco ASA 5500 Series help ensure reliable rendering of complex webpages with Java, JavaScript, ActiveX, Flash, and other sophisticated content.
- **Cisco AnyConnect Secure Mobility—**Enforces security policy in every transaction independent of where the user is located, whether it is an enterprise, ”in-house” owned or a SaaS application. Secure Mobility allows the administrator to require always-on secure network connectivity with a policy to permit or deny network connectivity if access is unavailable. These services are optimized for use with the Cisco IronPort Web Security Appliance.
- **Network-aware site-to-site VPNs—**Secure, high-speed communications are possible between multiple office locations. Support for quality of service (QoS) and routing across the VPN helps ensure reliable, business-quality delivery of latency-sensitive applications such as voice, video, and terminal services.
- **Threat-protected VPN—**VPNs are a primary source of malware infiltration into networks. Malware includes worms, viruses, spyware, keyloggers, Trojan horses, and rootkits. In the Cisco ASA 5500 Series, the depth and breadth of intrusion prevention, antivirus, application-aware firewall, and VPN endpoint security capabilities minimizes the risk that a VPN connection will become a conduit for security threats.
- **More cost-effective VPN deployment and operations—**Scaling and securing VPNs often requires additional load balancing and security equipment, which increases both equipment and operational costs. The Cisco ASA 5500 Series integrates these functions, delivering an unprecedented level of network and security integration among the VPN products available today. And by offering support for flexible tunneling

options on a single platform, the Cisco ASA 5500 Series provides customers with cost-effective alternatives to deploying parallel VPN infrastructures.

- **Scalability and resiliency—**The Cisco ASA 5500 Series can support up to 10,000 simultaneous user sessions per device, with the ability to scale to tens of thousands of simultaneous user sessions through integrated clustering and load-balancing capabilities. Stateful failover features deliver high-availability services for unsurpassed uptime.
- **OpenSSL technology—**The Cisco Secure Remote Access solution includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org).

Customizable Remote-Access VPN Features

Full Network Access

The Cisco ASA 5500 Series SSL/IPsec VPN Edition provides broad application and network resource access through network tunneling features available in either the Cisco AnyConnect Secure Mobility Client, as shown in Table 1, or the Cisco IPsec VPN Client.

Table 1. Cisco AnyConnect Secure Mobility Client Features

Feature	Description
Optimal Gateway Selection	**New in Cisco AnyConnect 2.5** • Determines and establishes connectivity to the optimal network access point. • Automatically adapts its tunneling to the most efficient method possible based on network constraints. • Uses DTLS to provide an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access. • Uses TLS (HTTP over TLS/SSL) to ensure availability of network connectivity through locked-down environments, including those using web proxy servers. • Data compression may be used to reduce the amount of data transmitted.
Cisco AnyConnect Secure Mobility **(Premium or Cisco IronPort Web Security Appliance Mobile User Security license required)**	**New in Cisco AnyConnect 2.5** • Enforces security policy into every transaction independent of where the user is located, whether it is an enterprise/"in-house" owned or a SaaS application. • Requires always-on secure network connectivity with a policy to permit or deny network connectivity if access unavailable. • Hotspot / Captive Portal Detection. • Optimized for use with the Cisco IronPort Web Security Appliance.
Broad operating system support	• Microsoft Windows XP 32-bit (x86) and 64-bit (x64) • Windows Vista 32-bit (x86) and 64-bit (x64), including Service Pack 1 and 2 (SP1/SP2) • Windows 7 32-bit (x86) and 64-bit (x64) • Mac OS X 10.5 and 10.6.x • Linux Intel (2.6.x kernel) **Note:** Windows 2000 and Mac OS X 10.4 are no longer supported as of Cisco AnyConnect 2.4. • Cisco AnyConnect Mobile (requires optional AnyConnect Mobile license) ◦ Windows Mobile 6.x (Professional and Classic)
Wide range of deployment and connection options	Deployment options: • Predeployment, including Microsoft Installer • Automatic headend deployment (administrative rights are required for initial installation) via ActiveX (Windows only) and Java Connection modes: • Standalone via system icon • Browser-initiated (Weblaunch) • Clientless portal initiated • Command line interface (CLI)-initiated • API

Ease of client administration	• The Cisco AnyConnect Secure Mobility client allows an administrator to automatically distribute software and policy updates from the headend security appliance, thereby eliminating administration associated with client software updates. • Administrators can determine which capabilities to make available for end-user configuration. • Administrators can trigger an endpoint script at connect/disconnect time when domain login scripts cannot be utilized. • Administrators can fully customize and/or localize end-user visible messages.
Consistent user experience	• Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience. • Multiple delivery methods and small download size help ensure broad compatibility and rapid download of the Cisco AnyConnect Secure Mobility client.
Advanced IP network connectivity	• Access to internal IPv4 and IPv6 network resources • Centralized split tunneling control for optimized network access IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/Lightweight Directory Access Protocol (LDAP)
Client firewall policy	**New in Cisco AnyConnect 2.5** • Added protection for Split Tunneling configurations. • Used in conjunction with Cisco Mobile User Security to allow for local access exceptions (i.e. printing, tethered device support, etc). • Supports port-based rules for IPv4 and network/IP access control lists (ACLs) for IPv6. • Available for Windows XP SP2, Vista, Windows 7, and Mac OS X.
Cisco AnyConnect Profile Editor	**New in Cisco AnyConnect 2.5 and Cisco Adaptive Security Appliance 8.3** • AnyConnect policies may be customized directly from Cisco ASDM (Adaptive Security Device Manager).

Table 2 summarizes Cisco AnyConnect licensing options,

Table 2. Cisco AnyConnect Licensing Options

License Option	Description
Platform Licenses	
AnyConnect Essentials	• Cisco AnyConnect Secure Mobility client connectivity without clientless SSL VPN and Cisco Secure Desktop capabilities. • Cisco AnyConnect Secure Mobility capabilities when used in conjunction with a licensed Cisco IronPort Web Security Appliance. • Full tunneling access to enterprise applications. • Single license per device type.
AnyConnect Premium	• Includes clientless SSL VPN, Cisco AnyConnect Secure Mobility, and Cisco Secure Desktop capabilities (including Host Scan). Optionally provides full tunneling access to enterprise applications. • License is based on number of simultaneous users, and is available as a single-device license or a shared license.
Optional Feature Licenses	
AnyConnect Mobile	• Enables Mobile OS platform compatibility. • Required per device license, in addition to AnyConnect Essentials or Premium licenses.
Advanced Endpoint Assessment	• Enables advanced endpoint assessment capabilities (such as auto-remediation). • Required per device, in addition to AnyConnect Premium licenses. • Not available with AnyConnect Essentials licenses.

Clientless Network Access

Cisco ASA 5500 Series clientless SSL VPN access, with features shown in Table 3, allows precisely controlled, web-based access to specific network resources and applications from Internet kiosks, shared computers, extranet partners, employee-owned desktops, and company-owned employee desktops.

Table 3. Cisco ASA 5500 Series Web-Based Clientless Access

Feature	Description
Broad, reliable compatibility	An advanced transformation capability helps to ensure compatibility with webpages containing complex content, including HTML, Java, ActiveX, JavaScript, and Flash.
Integrated clientless application optimization	Integrated performance optimization for resource-intensive applications, such as Microsoft Outlook Web Access and Lotus iNotes, delivers exceptional response times and low latency to provide a high-quality SSL VPN end-user experience.
Customizable user experience	The enhanced clientless portal features group-based customization for detailed access, ease of use, and a customizable user experience: • Support for Multilanguage, clientless user portals • User-customizable resource bookmarks • Publishing of Really Simple Syndication (RSS)-based information resources for automatic updating of important real-time content
Fully clientless Citrix access	No extraneous helper applications are required for Citrix access over clientless SSL VPN, which helps ensure fast application initiation time and reduces the risk of desktop software conflicts.
Integrated client-server application support	Provides access to common client-server applications without the need for predeployed remote clients, granting rapid access to Telnet, SSH, Remote Desktop Protocol (RDP), and Virtual Network Computing (VNC) resources.
Support for common thick-client applications	Port forwarding enables clientless access to popular thick-client applications, such as Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), email, online calendars, instant messaging, Telnet, SSH, and other client-initiated TCP applications, through a small Java applet. Smart tunneling allows Microsoft Windows users to access TCP applications without the prerequisite of administrative rights and allows VPN administrators to grant only approved applications access to internal resources.
Broad browser support	Multiple browser support, including Microsoft Internet Explorer, Firefox, Opera, Safari, and Pocket Internet Explorer (PIE), helps ensure broad connection compatibility from any location.
Advanced IP network connectivity	Access to internal IPv4 and IPv6 network resources.

Comprehensive Authentication and Authorization Choices

The Cisco ASA 5500 Series provides a comprehensive set of options for authentication and authorization of users, as shown in Table 4.

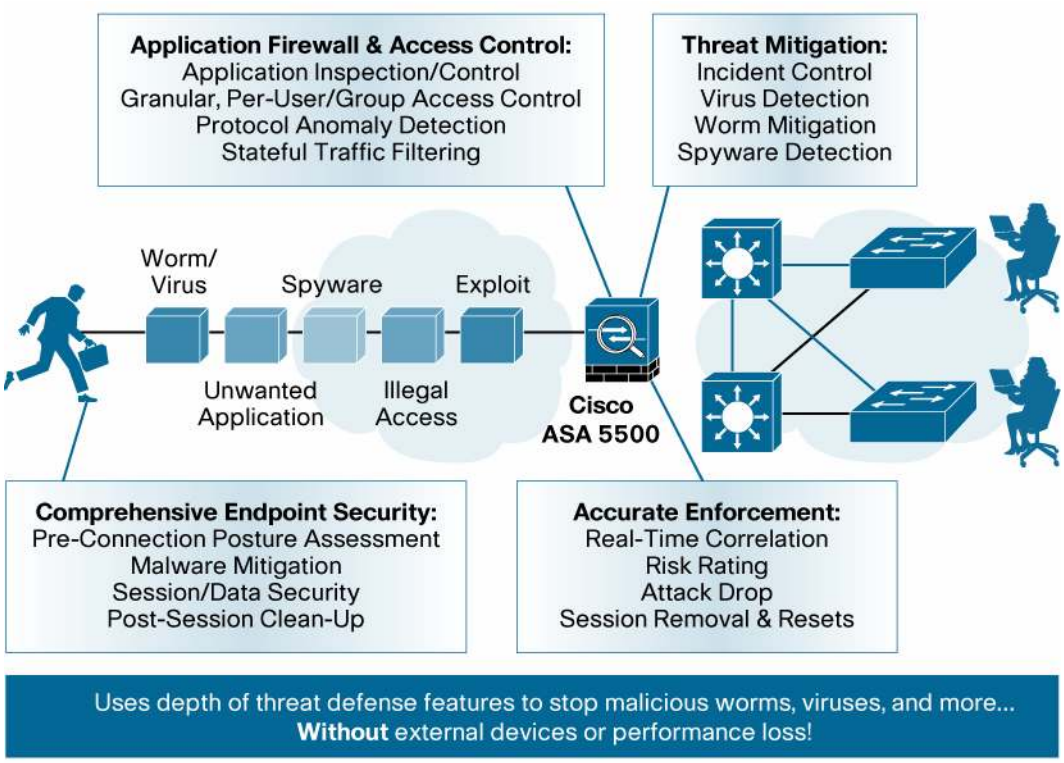
Table 4. Cisco ASA 5500 Series Authentication and Authorization Options

Feature	Description
Authentication options	• RADIUS • RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM) • RADIUS one-time password (OTP) support (state/reply message attributes) • RSA SecurID • Double authentication • Active Directory/Kerberos • Embedded Certificate Authority (CA) • Digital Certificate / Smartcard (including Machine Certificates for Cisco AnyConnect) • LDAP with password expiry and aging • Generic LDAP support • Combined certificate and username/password multifactor authentication • Internal domain password prompting for simplified single sign-on (SSO) • SSL VPN virtual keyboard authentication for additional protection against keystroke loggers
Sophisticated authorization	• Policy mapping from RADIUS and LDAP • Dynamic access policies directly use domain membership and posture status for creation of user policy
Single sign-on (SSO) for clientless SSL VPN users	• Computer Associates Siteminder • RSA Access Manager (ClearTrust) • Security Assertion Markup Language (SAML) • Basic/NTLM authentication pass-through • Forms-based authentication pass-through

Threat-Protected VPN Features

The Cisco ASA 5500 Series Secure Remote Access solution provides advanced security for VPN deployments through its integrated network and endpoint security technologies. Securing the VPN is necessary to prevent network attacks such as worms, viruses, spyware, keyloggers, Trojan horses, rootkits, or hacking. Detailed application and access control policy helps ensure that individuals and groups of users have access only to the applications and network services to which they are entitled (Figure 2).

Figure 2. Threat-Protected VPN Services Use Onboard Security to Protect Against VPN Threats



Network Security at the VPN Gateway

Worms, viruses, application-embedded attacks, and application abuse are among the greatest security challenges in today's networks. Remote access and remote-office VPN connectivity are common points of entry for such threats, due to limited security capabilities on VPN devices. VPNs are often deployed without proper inspection and threat mitigation applied at the tunnel termination point at the headquarters location, which allows malware from remote offices or users to infiltrate the network and spread. With the converged threat mitigation capabilities of the Cisco ASA 5500 Series, customers can detect malware and stop it before it enters the network interior. For application-embedded attacks, such as spyware or adware spread through file-sharing in peer-to-peer networks, the Cisco ASA 5500 Series deeply examines application traffic to identify a dangerous payload and drop its contents before it reaches its target and causes damage. Table 5 lists some VPN gateway security features provided by the Cisco ASA 5500 Series.

Table 5. Network Security at the Cisco ASA 5500 Series VPN Gateway

Feature	Description
Extensive malware mitigation	Worms, viruses, spyware, keyloggers, Trojan horses, and rootkits are thwarted at the Cisco ASA 5500 Series VPN gateway, thereby eliminating threats before they spread throughout the network.
Application-aware firewall and access control	Application-aware traffic inspection enables thorough user access control and helps prevent abuse of unwanted applications, such as peer-to-peer file sharing across the VPN connection.

Intrusion prevention	The Cisco ASA 5500 Series guards against a multitude of network exploits.
Access restrictions	The permission or denial of access to confidential resources is based on flexible configuration policies and current posture status.
Virtual LAN (VLAN) mapping	Enforcement of user- and group-based traffic access restrictions are based on a configured VLAN.

Comprehensive Endpoint Security for SSL VPN

SSL VPN deployments enable universal access from both secure and noncorporate-managed endpoints, and provide the ability to extend network resources to diverse user communities. With this extension of the network, the points for potential network security attacks also increase. Whether users are accessing the network from a corporate-managed PC, personal network-accessible device, or public terminal, Cisco Secure Desktop minimizes data such as cookies, browser history, temporary files, and downloaded content left behind after an SSL VPN session terminates. Endpoint posture checking for full network access users is also available through integration with the Cisco NAC Appliance and Cisco NAC Framework. Table 6 highlights Cisco Secure Desktop features. (Premium License required)

Table 6. Cisco Secure Desktop Provides Comprehensive Security of Information from the Network to the Endpoint

Feature	Description
Pre-connection posture assessment	Host integrity verification checking seeks to detect the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access. A significantly expanded list of applications and versions are now supported through this mechanism. Frequent updates are available to support new product releases. Administrators also have the option of defining custom posture checks based on the presence of running processes.
Pre-connection asset assessment	Cisco Secure Desktop can detect the presence of a watermark on a remote system. The watermark can be used to identify assets that are corporate-owned and provide differentiated access as a result. The watermark checking capability includes system registry values, file existence matching a required CRC32 checksum, IP address range matching, and certificate issued by/to matching.
Comprehensive session protection	Additional protection is provided for all data associated with the session, including passwords, file downloads, history, cookies, and cache files. Session data is encrypted to the secure vault of Cisco Secure Desktop.
End-of-session data cleanup	Data in the secure vault is overwritten at the end of the session.
Keystroke logger detection	Cisco Secure Desktop performs an initial check for certain software-based keystroke logging software at the start of the session. If an anomalous program begins running inside the secure vault, after session initiation, the user is prompted to stop the suspicious activity.
Available with guest permissions	Users accessing the network from remote machines may not have administrator privileges on all systems. Cisco Secure Desktop can often be installed with only guest permissions. This helps to ensure delivery and installation on all systems.
Advanced endpoint assessment license	An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications.

Network-Aware Site-to-Site VPN Features

Using the network-aware IPsec site-to-site VPN capabilities provided by the Cisco ASA 5500 Series SSL/IPsec VPN Edition, businesses can securely extend their networks across low-cost Internet connections to business partners and remote and satellite offices worldwide (Table 7).

Table 7. Cisco ASA 5500 Series SSL/IPsec VPN Edition Site-to-Site VPN Connectivity

Feature	Description
QoS-enabled	Supports latency-sensitive applications such as voice, video, and terminal services.
Network-aware routing	Open Shortest Path First (OSPF) support across tunneling neighbors enables network topology awareness for ease of network integration.

VPN Cost-Effectiveness Through Platform Integration

The Cisco ASA 5500 Series integrates numerous functions—such as security and load balancing—that can reduce the number of devices required to scale and secure the VPN, thereby decreasing equipment costs, architectural complexity, and operational costs (Table 8).

Table 8. Integrated Functions That Complement VPN Deployment

Feature	Description
Network and endpoint security	Onboard malware mitigation, IPS, and firewall capabilities increase VPN security while decreasing the amount of equipment that needs to be deployed.
Load balancing	Integrated load-balancing features enable multichassis clusters without expensive external load balancing equipment.

Cisco ASA 5500 Series Platform Overview

The Cisco ASA 5500 Series delivers site-specific scalability, from small offices to enterprise headquarters locations, through its seven models: 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40 (Figure 3). Models 5510 through 5550 share a common chassis, built with a foundation of concurrent services scalability, investment protection, and future technology extensibility. Table 9 lists the specifications of the Cisco ASA 5500 Series models.

Figure 3. The Cisco ASA 5500 Series Portfolio

Table 9. Specifications of Cisco ASA 5500 Series Adaptive Security Appliance Models

Platform	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Maximum VPN throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
Maximum concurrent SSL VPN sessions [1]	25	250	750	2500	5000	10,000	10,000
Maximum concurrent IPsec VPN sessions [2]	25	250	750	5000	5000	10,000	10,000
Interfaces	8-port 10/100 switch with 2 Power-over-Ethernet ports	5-port 10/100 / 2-port 10/100/1000, 3-port 10/100 +4-port 10/100/1000, 4 SFP (with 4 Gigabit Ethernet [4GE] SSM)	4-port 10/100/1000, 1-port 10/100 +4-port 10/100/1000, 4 SFP (with 4GE SSM)	4-port 10/100/1000, 1-port 10/100 +4-port 10/100/1000, 4 SFP (with 4GE SSM)	8-port 10/100/1000, 4-port SFP, 1-port 10/100	2-port 10/100/1000 Management +4-port 10/100/1000 (with ASA5580-4GE-CU) + 4-port GE SR LC (with ASA5580-4GE-FI) +2-port 10GE SR LC (with ASA5580-2X10GE-SR)	2-port 10/100/1000 Management +4-port 10/100/1000 (with ASA5580-4GE-CU) + 4-port GE SR LC (with ASA5580-4GE-FI) +2-port 10GE SR LC (with ASA5580-2X10GE-SR)
Profile	Desktop	1-RU	1-RU	1-RU	1-RU	4-RU	4-RU
Stateful failover	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes
VPN load balancing	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes

[1] Devices include a license for two SSL VPN users for evaluation and remote management purposes. The total concurrent IPsec and SSL (clientless and tunnel-based) VPN sessions may not exceed the maximum concurrent IPsec session count shown in the chart. The SSL VPN session number may also not exceed the number of licensed sessions on the device. The Cisco ASA 5580 supports a greater number of simultaneous users than the ASA 5550 at an overall SSL VPN throughput that is comparable to the ASA 5550. These items should be taken in to consideration as part of your capacity planning.
[2] Upgrade is available with Cisco ASA 5510 Security Plus license.

Shared VPN License Option	No	Yes	Yes	Yes	Yes	Yes	Yes

Cisco Services

Cisco and its partners provide services that can help you deploy and manage security solutions. Cisco has adopted a lifecycle approach to services that addresses the necessary set of requirements for deploying and operating Cisco adaptive security appliances and other Cisco security technologies. This approach can help you improve your network security posture to achieve a more available and reliable network, prepare for new applications, lower your network costs, and maintain network health through day-to-day operations. For more information about Cisco Security Services, visit: http://www.cisco.com/go/services/security.

For More Information

- Cisco ASA 5500 Series: http://www.cisco.com/go/asa
- Cisco ASA 5500 Series Adaptive Security Appliance Licensing Information: http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html
- Cisco Secure Remote Access: VPN Licensing Overview http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/overview_c78-527488.html
- Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.html
- Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm
- Cisco Product Certifications: http://www.cisco.com/go/securitycert
- Cisco Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

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.

Printed in USA C78-529285-01 03/10