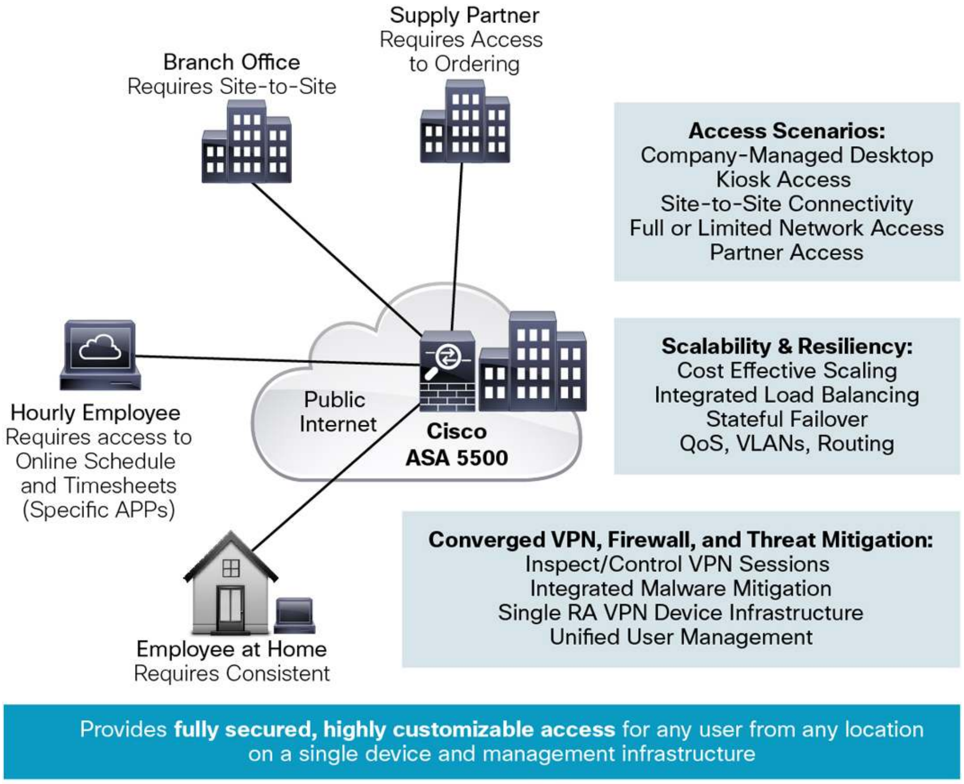
Data Sheet

Cisco AnyConnect Secure Mobility Solution: Cisco AnyConnect Secure Mobility Client and Cisco ASA 5500 Series (SSL/IPsec VPN Edition)

The Cisco® ASA 5500 Series Adaptive Security Appliance (ASA) is a purpose-built platform that combines best- in-class security and VPN services for small and medium-sized business (SMBs) and enterprise applications. The Cisco ASA 5500 Series helps enable customization for specific deployment environments and options, with special product editions for Remote Access (SSL/IPsec VPN), Site-To-Site VPN, Firewall, Content Security, and Intrusion Prevention.

The Cisco AnyConnect Secure Mobility Solution gives organizations 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


Supply Partner
Requires Access to Ordering
Branch Office
Requires Site-to-Site
Access Scenarios:
Company-Managed Desktop
Kiosk Access
Site-to-Site Connectivity
Full or Limited Network Access
Partner Access
Hourly Employee
Requires access to Online Schedule and Timesheets (Specific APPs)
Public Internet
Cisco ASA 5500
Scalability & Resiliency:
Cost Effective Scaling
Integrated Load Balancing
Stateful Failover
QoS, VLANs, Routing
Converged VPN, Firewall, and Threat Mitigation:
Inspect/Control VPN Sessions
Integrated Malware Mitigation
Single RA VPN Device Infrastructure
Unified User Management
Employee at Home
Requires Consistent
Provides fully secured, highly customizable access for any user from any location on a single device and management infrastructure

Cisco ASA 5500 Series SSL/IPsec VPN Edition

This edition 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 (DTLS and TLS)
- IPsec VPN client technologies
- Cisco AnyConnect Secure Mobility Solution optimized for Cisco Web Security
- Advanced clientless SSL VPN capabilities
- Network-aware site-to-site VPN connectivity

This supports highly 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 AnyConnect Secure Mobility Solution include:

- **SSL (TLS & 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 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 (TLS & 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:** Using the ubiquity of SSL encryption available in Internet browsers, the AnyConnect Secure Mobility Solution delivers clientless remote access. This provides access to network applications and resources, regardless of location, without the need for desktop VPN client software.

  The solution 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. It also provides 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 Solution:** 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 Cisco Web Security, and require an AnyConnect Premium license or a Secure Mobility license.

- **Network-aware site-to-site VPNs:** Highly 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 remote access VPNs:** 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.
- **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. 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 AnyConnect Secure Mobility Client 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	Benefit
Broad Operating System Support	• Windows 7 32-bit (x86) and 64 bit (x64) • Windows Vista 32-bit (x86) and 64-bit (x64), including Service Packs 1 and 2 (SP1/SP2) • XP SP2+ 32-bit (x86) and 64-bit (x64) • Mac OS X 10.6 and higher • Linux Intel
Software Access	• Available on Cisco.com for customers with active SMARTnet contracts on their Adaptive Security Appliances (ASA)
Optimized Network Access - VPN Protocol Choice SSL (TLS and DTLS), and IPsec/IKEv2	• AnyConnect now provides a choice of VPN protocols, allowing administrators to use whichever protocol best fits their business needs • Tunneling support includes SSL (Transport Layer Security [TLS] and Datagram Transport Layer Security [DTLS]) and next-generation IPsec (IKEv2) • DTLS provides an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access • TLS (HTTP over TLS/SSL) helps ensure availability of network connectivity through locked-down environments, including those using web proxy servers • IPsec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPsec
Optimal Gateway Selection	• Determines and establishes connectivity to the most optimal network access point, eliminating the need for end users to determine the nearest location

Feature	Benefit
Mobility-Friendly	• Designed for mobile users • Can be configured so that the VPN connection remains established during IP address changes, loss of connectivity, and hibernation or standby • Trusted Network Detection allows the VPN connection to automatically disconnect when an end user is in the office, and connect when a user is at a remote location
Encryption	• Supports strong encryption, including AES-256 and 3DES-168 (Security gateway device must have a strong crypto license enabled.) • Next-generation encryption, including NSA Suite B algorithms, ESPv3 with IKEv2, 4096-bit RSA keys, Diffie-Hellman Group 24, and enhanced SHA2 (SHA-256 and SHA-384) (only applies to IPsec IKEv2 connections; Premium ASA license required)
Wide Range of Deployment and Connection Options	Deployment options: • Pre-deployment, including Microsoft Installer • Automatic security gateway deployment (administrative rights are required for initial installation) using ActiveX (Windows only) and Java Connection modes: • Standalone using system icon • Browser-initiated (Weblaunch) • Clientless portal initiated • Command Line Interface (CLI)-initiated • Application Programming Interface (API)-initiated
Wide Range of 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 (including SoftID integration) • Active Directory/Kerberos • Embedded Certificate Authority (CA) • Digital Certificate/Smartcard (including Machine Certificate support), auto- or user-selected • Lightweight Directory Access Protocol (LDAP) with Password Expiry and Aging • Generic LDAP support • Combined certificate and username/password multifactor authentication (double authentication)
Consistent User Experience	• Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience • Multiple delivery methods help ensure broad compatibility of Cisco AnyConnect • User may defer pushed updates to AnyConnect • Customer experience feedback option
Centralized Policy Control and Management	• Policies can be preconfigured or configured locally, and can be automatically updated from the VPN security gateway • Application Programming Interface (API) for AnyConnect eases deployments through webpages or applications. • Untrusted Certificates checking and user warnings • Certificates can be viewed and managed locally
Advanced IP Network Connectivity	• Public connectivity to/from IPv4 and IPv6 networks • Access to internal IPv4 and IPv6 network resources over SSL (v6 internal requires TLS/DTLS) • Administrator-controlled split/all-tunneling network access policy • Access control policy IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP

Feature	Benefit
Pre-Connection Posture Assessment (premium license required)	• In conjunction with Cisco Secure Desktop, HostScan 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 • Administrators also have the option of defining custom posture checks based on the presence of running processes • Cisco Secure Desktop can detect the presence of a watermark on a remote system, which can be used to identify assets that are corporate-owned and provide differentiated access; watermark-checking capability includes: ◦ System registry values ◦ File existence matching a required CRC32 checksum ◦ IP address range matching ◦ Certificate issued by/to matching • An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications
Client Firewall Policy	• Added protection for split tunneling configurations • Used in conjunction with Cisco Secure Mobility to allow for local access exceptions (for example, printing, tethered device support, and more) • Supports port-based rules for IPv4 and network/IP access control lists (ACLs) for IPv6 • Available for Windows XP SP2, Vista, and Windows 7, and Mac OS X
Localization	In addition to English, the following language translations are included: • Czech (cs-cz) • German (de-de) • Latin American Spanish (es-co) • Canadian French (fr-ca) • Japanese (ja-jp) • Korean (ko-kr) • Polish (pl-pl) • Simplified Chinese (zh-cn)
Ease of Client Administration	• Allows an administrator to automatically distribute software and policy updates from the head-end 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 used • Administrators can fully customize and localize end-user-visible messages
AnyConnect Profile Editor	• AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM)
Diagnostics	• On-device statistics and logging information • View logs on device • Logs can be easily emailed to Cisco or an administrator for analysis
Federal Information Processing Standard (FIPS)	• FIPS 140-2 Level 2-compliant (platform, feature, and version restrictions apply)
Ease of Client Administration	• The Cisco AnyConnect Secure Mobility Client allows an administrator to automatically distribute software and policy updates from the security gateway, 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 used • 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

Feature	Benefit
Advanced IP Network Connectivity	- Public connectivity to/from IPv4 and IPv6 networks - Access to internal IPv4 and IPv6 network resources over SSL (v6 internal requires TLS/DTLS) - Administrator-controlled split/all-tunneling network access policy - Access control policy IP address assignment mechanisms: - Static - Internal pool - Dynamic Host Configuration Protocol (DHCP) - RADIUS/Lightweight Directory Access Protocol (LDAP)
Client Firewall Policy	- Added protection for Split Tunneling configurations. - Used in conjunction with Cisco Mobile User Security to allow for local access exceptions (for example, printing, tethered device support, and more) - 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	- AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM)

Table 2 summarizes Cisco AnyConnect licensing options,

Table 2. Cisco AnyConnect Licensing Options

License Requirements (each license below is required)	Description
Cisco ASA Platform License	**Cisco AnyConnect Essentials**[1] (P/N: (L-ASA-AC-E-55**=) 05, 10, 20, 40, 50,80, 85) - Highly secure remote-access connectivity - Single license per ASA device model (not a per user license); supports optimum simultaneous users on platform - Full-tunneling access to enterprise applications
	Cisco AnyConnect Premium[2] (P/N: (L-ASA-SSL-***=) 10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10K) - Provides support for clientless SSL VPN and capabilities available on desktop AnyConnect platforms, including Cisco Secure Desktop HostScan and Always-On VPN connectivity - License based on number of simultaneous users, and is available as a single device or shared license
Cisco AnyConnect Mobile License[5] P/N: (L-ASA-AC-M-55*=) 05, 10, 20, 40, 50,80, 85	- Supports Mobile OS platform compatibility - Single license per ASA device model (not a per user license), required in addition to Essentials or Premium 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. These can be accessed 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.

[1] Replace ** with the appropriate last two digits of the ASA model number.
[2] Replace *** with the number of total number of license seats.

Feature	Description
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 supports clientless access to popular thick-client applications through a small Java applet, including: • Post Office Protocol (POP) • Simple Mail Transfer Protocol (SMTP) • Internet Message Access Protocol (IMAP) • Email • Online calendars • Instant messaging • Telnet • SSH • Other client-initiated TCP applications 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.

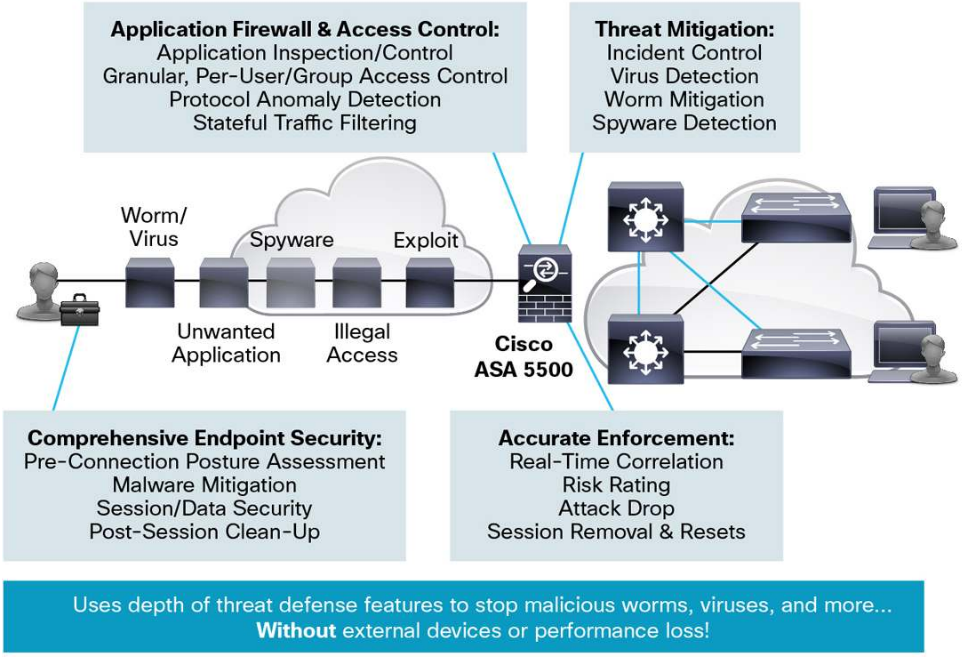
Table 4. Cisco ASA 5500 Series Authentication and Authorization Options

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 SSL/IPsec VPN Edition 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, and 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


Application Firewall & Access Control:
Application Inspection/Control
Granular, Per-User/Group Access Control
Protocol Anomaly Detection
Stateful Traffic Filtering
Threat Mitigation:
Incident Control
Virus Detection
Worm Mitigation
Spyware Detection
Worm/ Virus
Spyware
Exploit
Unwanted Application
Illegal Access
Cisco ASA 5500
Comprehensive Endpoint Security:
Pre-Connection Posture Assessment
Malware Mitigation
Session/Data Security
Post-Session Clean-Up
Accurate Enforcement:
Real-Time Correlation
Risk Rating
Attack Drop
Session Removal & Resets
Uses depth of threat defense features to stop malicious worms, viruses, and more...
Without external devices or performance loss!

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. The solution identifies a dangerous payload and drops 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 supports 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 allow universal access from both highly secure and non-corporate-managed endpoints, and provide the ability to extend network resources to diverse user communities. Users can access the network from a corporate-managed PC, personal network-accessible device, public terminal, or other device. With this extension of the network, the points for potential network security attacks also increase.

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
Preconnection 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 available to support new product releases. Administrators also have the option of defining custom posture checks based on the presence of running processes.
Preconnection Asset Assessment	Cisco Secure Desktop can detect the presence of a watermark on a remote system, which can be used to identify assets that are corporate-owned and provide differentiated access as a result; watermark checking capability includes: • System registry values • File existence matching a required CRC32 checksum • IP address range matching • 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, with session data encrypted to the highly secure vault of Cisco Secure Desktop.
End-of-Session Data Cleanup	Data in the highly 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	While 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

The Cisco ASA 5500 Series SSL/IPsec VPN Edition uses network-aware IPsec site-to-site VPN capabilities. This allows businesses to 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) and Border Gateway Protocol (BGP) support across tunneling neighbors helps enable 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 support multi-chassis 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, This scalability is delivered through its ten models: 5505, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-10, 5585-20, 5585-40, and 5585-60 (Figure 3). Models 5512 through 5555 share a common chassis, built with a foundation of concurrent services scalability, investment protection, and future technology extensibility.

Figure 3. The Cisco ASA 5500 Series Portfolio

Table 9 lists the specifications of the Cisco ASA 5500 Series models.

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

Platform	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585-S10	ASA 5585-S20	ASA 5585-S40	ASA 5585-S60
Maximum 3DES/AES VPN Throughput[1]	100 Mbps	200 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Maximum Site-to-Site and IPsec IKEv1 Client VPN User Sessions[1]	25	250	250	750	2500	5000	5000	10,000	10,000	10,000
Maximum Cisco AnyConnect or Clientless VPN User Sessions	25	250	250	750	2500	5000	5000	10,000	10,000	10,000

Platform	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585-S10	ASA 5585-S20	ASA 5585-S40	ASA 5585-S60
Bundled Premium User Sessions	2									
Stateful Failover	No	Yes								
VPN Load Balancing	No	Yes								
Shared VPN License Option	No	Yes								

	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585 SSP-10/20	ASA 5585 SSP-40/60
Hardware								
CPU	Single core	Multi-core, enterprise-class						
Memory (RAM)	512 MB	4 GB	8 GB		12 GB	16 GB	6/12 GB	12/24 GB
Flash	128 MB	4 GB	8 GB				2 GB	
Integrated Network (GE) Ports	8x 10/100 switch ports with 2 PoE ports	6		8			8x 10/100/1000 2x 10 GE3 SFP+ (SSP-10/20) 16x 10/100/1000 4x 10GE3 SFP+ (SSP-10/20 or IPS SSP-10/20)	6x 10/100/1000 4x 10 GE SFP+ (SSP-40/60) 12x 10/100/1000 8x 10GE SFP+ (SSP-40/6 or IPS SSP-40/60)
Interface Card Slots	1x SSC	1x SSM						
Interface Card Options	N/A	6-port 10/100/1000, 6-port GE SFP SX, LH, LX						
Redundant Power	No				Yes			
Power Supply	External, 96W	400W			450W		370W	
Physical Specifications								
Form Factor	Desktop	1 RU, 19-in. rack-mountable					2 RU, 19-in. rack-mountable	
Rack Mounting Options	Yes, with rack-mount or wall-mount kit	Brackets included (slide rails optional)			Slide rails included		Rack mounts included	
Dimensions (H x W x D)	1.75 x 7.89 x 6.87 in. (4.45 x 20.04 x 17.45 cm)	1.67 x 16.7 x 15.6 in. (4.24 x 42.9 x 39.5 cm)			1.67 x 16.7 x 19.1 in. (4.24 x 42.9 x 48.4 cm)		3.47 x 19 x 26.5 in. (8.8x 48.3 x 67.3 cm)	
Weight	4.0 lb (1.8 kg)	13.39 lb (6.07 kg)	13.39 lb (6.07 kg)	14.92 lb (6.77 kg)	16.82 lb (7.63 kg) with single power supply 18.86 lb (8.55 Kg) with dual power supplies		50 lbs (22.7 kg) with single power supply 62 lbs (28.2 kg) with dual power supplies	

[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 5512 Security Plus license.

Shared VPN License Option	No	Yes	Yes	Yes	Yes	Yes	Yes

Platform Compatibility

The Cisco AnyConnect Secure Mobility Client is compatible with all Cisco ASA 5500 and 5500-X Series Adaptive Security Appliance models (running Cisco ASA Software Release 8.0.3 and later) and various Cisco IOS® Software-based routers.

Additional compatibility information may be found at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html.

Electronic License Delivery

Most licenses are available for electronic delivery, which significantly speeds up license fulfillment time. To order a license electronically, if you have any questions regarding licensing, or would like evaluation licenses, be sure to order part number(s) that begin with “L.”

If you already have an Essentials or Premium ASA license, you may use the automated license request tool at: https://tools.cisco.com/SW IFT/Licensing/PrivateRegistrationServlet?FormId=717.

Warranty Information

Find warranty information at the Cisco Product Warranties page.

Ordering Information

To place an order for a security gateway license, visit the Cisco Ordering Home Page. See Table 1 for compatible platforms and software access information.

Security gateway licenses are required to begin connectivity. Please refer to the Cisco AnyConnect Licensing Options section above for additional information on the available options. For a list of available licensing options that enable connectivity with Cisco AnyConnect, please refer to the Cisco AnyConnect Secure Mobility Client Features, Licenses, and OSs webpage.

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: (http://www.openssl.org).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product incorporates the libcurl HTTP library: Copyright © 1996-2006, Daniel Stenberg, (Daniel@haax.se).

For More Information

Cisco AnyConnect Secure Mobility Client homepage: http://www.cisco.com/go/anyconnect

Cisco AnyConnect Documentation: http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco ASA 5500 Series Adaptive Security Appliances: http://www.cisco.com/go/asa

Cisco Adaptive Security Device Manager: http://www.cisco.com/go/asdm

Cisco ASA 5500 Series Adaptive Security Appliance Licensing Information:
http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

AnyConnect End User License Agreement and Privacy Policy:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm

Cisco Product Certifications: http://www.cisco.com/go/securitycert

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 C78-529285-02 09/12