Cisco Secure Remote Access

To remain productive and collaborate efficiently, remote users require access to a company's resources from anywhere and at any time, whether they are using a company-issued laptop, a personal computer, or a mobile device. IT departments face the challenge of providing secure mobility to an exponentially growing number of mobile devices, while ensuring that the company's data is safe and protected.

Choosing the Right Remote Access Solution for Your Organization

When choosing a remote access solution, IT administrators are faced with a variety of challenges, such as how to:

- Establish granular corporate security policies and protect critical company assets
- Enable employee productivity by providing anywhere, anytime secure collaboration both within and across organizations
- Provide users with flexibility and choice in terms of access methods, applications, and mobile endpoints, namely supporting securely employee-owned mobile devices securely
- Ensure business continuity in the event of natural disasters or unforeseen events
- Meet industry compliance requirements and legislation mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI) standards

Three Criteria to Consider

Security: IT teams need to be able to enforce security policies with maximum flexibility and granularity for each connection. Each policy needs to dynamically adapt to a user's unique security posture, location, workgroup, and connecting device. A secure remote access solution should also enable IT administrators to minimize risks of leaving corporate data behind during or after a remote user session.

Connectivity: Workforces are becoming increasingly mobile. In turn, global IT administrators need to enable safe and productive remote access over a broad range of connection media. A secure remote access solution should ensure that remote users remain seamlessly connected when roaming between different networks, both in and out of the office, or transitioning through hibernation or standby. The solution must also automatically select the most optimal network access point and adapt its tunneling protocol to the most efficient method for the user's specific connections and application sets.

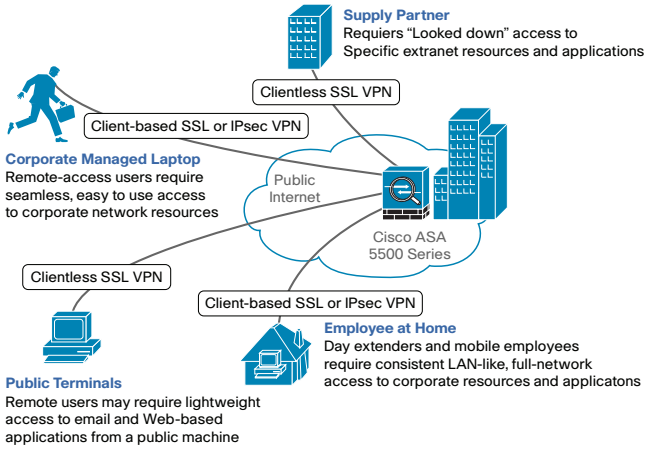
Mobility: Enterprise workers are often avid consumers who follow the smartphone and tablet PC trends. With the proliferation of mobile devices, such as Apple iPhones, Android smartphones, tablet PCs and Windows Mobile handhelds, IT administrators need to enable users to securely connect from various endpoints and operating systems. A strong solution should offer a large array of supported endpoints and ensure that the VPN connection is persistent, consequently enhancing productivity, promoting collaboration and boosting employee satisfaction.

Cisco Secure Remote Access: The Industry-Leading Secure Mobility Solution

The Cisco® Secure Remote Access Solution is a single-appliance VPN solution that extends network access safely and easily to a wide range of users and devices. It offers the most comprehensive and versatile secure mobility solution in the industry and supports the widest range of connectivity options, endpoints and platforms to meet your organization's changing and diverse remote access needs.

The solution is powered by the Cisco ASA 5500 Series Adaptive Security Appliance, which gives IT administrators a single point of control to assign granular access based on both the user and the device. The Cisco ASA 5500 Series provides a protocol-agnostic solution offering both client-based, full network access (SSL/DTLS, IPsec, L2TP/IPsec) and controlled clientless access to administrator-selected web-based applications or network resources. It is designed to enable highly secure, flexible secure mobility deployments (Figure 1).

Figure 1. Customizable SSL VPN and IPsec Services for Any Deployment Scenario



The Cisco Secure Remote Access Solution is easy to deploy, simple to use, and integrates a robust endpoint security design that helps maintain the integrity of confidential information and corporate resources. The solution is by design integrated with the Cisco ASA 5500 Series appliance's advanced security services, such as its powerful, market-proven firewall, intrusion prevention (IPS) and content security technologies, for incremental levels of security.

Cisco Secure Remote Access

At-A-Glance

Cisco Secure Remote Access Solution	• Industry's most versatile and integrated secure remote access solution offering clientless and client-based remote access while providing the highest security confidence • Most complete single-appliance solution to the evolving secure mobility and web threat challenges • Widest range of connectivity and mobility options, providing maximum flexibility, scalability, and manageability for all remote access deployments • Robust, granular security allowing IT to dynamically enforce a multilayer secure mobility policy including endpoint posture, integrated web threat protection, dynamic access policies, acceptable use policies
Cisco Secure Remote Access Solution Profile and Benefits	
Deployment flexibility	• Provides client and clientless access for a broad spectrum of desktop and mobile platforms on a single appliance. Extends the appropriate VPN technology (clientless or IPsec/SSL/DTLS client network access) on a per-session basis, depending on the user group and the endpoint accessing the network.
Granular control	• Empowers network and IT management with additional tools to provide controlled access to corporate resources and applications by leveraging granular policy setting and enforcement for each user group and device.
Versatile access	• Delivers ubiquitous clientless access to authenticated users on both managed and unmanaged endpoints, helping to increase productivity by providing "anytime access" to the right corporate resources, and enabling your company's plan for business continuity.
Comprehensive, optimized network access	• Enables broad application and network resource access through the Cisco AnyConnect Secure Mobility client, an automatically downloadable, versatile, user-friendly client that provides an in-office experience for virtually any application or resource and is optimized for voice, video and latency-sensitive applications access.
Widest range of connectivity choices	• Offers secure remote access on the widest range of mobile and PC devices. Enables businesses to securely respond to the growing user requirements for new endpoints and applications support, including support for the Apple iPhone; Windows Mobile 5.0, 6.0, and 6.1; Windows 7, XP, Vista (32- and 64-bit); and Mac OS X 10.5, and 10.6.
Mobility-friendly connectivity	• The AnyConnect Secure Mobility automatically selects the most optimal network access point and adapts its tunneling protocol to the most efficient method. AnyConnect ensures that the session is always on as required by the user or the administrator: it automates secure link level connection to the appropriate access point and dynamically manages the VPN session. AnyConnect seamlessly and securely connects, reconnects and disconnects the user session as appropriate, for instance during IP address changes, loss of network connectivity, hibernation or standby, or when the end user arrives at/ exits the corporate premises.
Advanced web security	• Powers secure deployments with scalable always-on user protection via reputation-based threat defense and universal usage policy enforcement, deployed either on premises with the Cisco IronPort® Web Security Appliance or in the cloud with the Cisco ScanSafe cloud-based services.
High scale and performance levels	• Designed to deliver the highest VPN session counts. Supports up to 10,000 secure endpoint connections per appliance, and up to 100,000 endpoints with the ASA's built-in load balancing feature.
Low total cost of ownership	• Reduces expensive help-desk calls associated with network connectivity issues, eliminates the cost of manually managing client software on every endpoint and offers a converged, single client that provides enterprises with a lower cost of endpoint administration, by unifying four Cisco clients into one.
Flexible licensing	• Offers shared VPN FLEX business continuity and AnyConnect Essentials licensing options to allow maximum flexibility in deployment, management, and scalability.
Cisco Secure Remote Access Solution Licensing	
Cisco AnyConnect Premium Clientless VPN License	• The AnyConnect Premium license enables customers to provide secure, granular, and flexible AnyConnect client and clientless VPN access to their remote users and business partners. Deployments benefit from an incremental level of security with the Cisco Secure Desktop feature suite: Secure Vault, Hostscan, Keystroke Logger Detection, and Cache Cleaner. • Web security and malware protection features available with the Cisco AnyConnect Secure Mobility solution enforce security policy, independent of user location. • AnyConnect Premium Licensing is based on the number of simultaneous users, and is available as a single device or shared license.
Cisco AnyConnect Essentials License	• The AnyConnect Essentials license provides access to enterprise applications by enabling Cisco AnyConnect VPN client capabilities on the ASA appliance. The AnyConnect Essentials license does not include Premium capabilities such as clientless SSL VPN access and the Cisco Secure Desktop feature suite, but it includes optimized client deployment and upgrades functions. • AnyConnect Essentials enables the maximum number of AnyConnect client connections on the ASA appliance.
Cisco AnyConnect Mobile License	• The AnyConnect Mobile license enables the AnyConnect VPN client on mobile smartphones. The Mobile license requires an AnyConnect Essentials or Premium license. It includes the user-acclaimed session persistence feature, which optimizes VPN connections for environments with intermittent connectivity.

Cisco ASA 5500 Series Models

The Cisco ASA 5500 Series delivers site-specific scalability, from the smallest SMB and home office deployments to the largest enterprise networks, with its eleven models: the 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40, 5585-S10, 5585-S20, 5585-S40 and 5585-S60 (Figure 2). Each model is built with concurrent services scalability, investment protection, and future technology extensibility as its foundation.

Figure 2. Cisco ASA 5500 Series Products

Table 1 provides performance information for the Cisco ASA 5500 Series.

Table 1. Performance Information for Cisco ASA 5500 Series Appliances

Platform	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40	Cisco ASA 5585-S10	Cisco ASA 5585-S20	Cisco ASA 5585-S40	Cisco ASA 5585-S60
Maximum VPN throughput[1]	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Maximum concurrent SSL VPN sessions[1]	25	250	750	2500	5000	10,000	10,000	5000	10,000	10,000	10,000
Maximum concurrent IPsec VPN sessions[1]	25	250	750	5000	5000	10,000	10,000	5000	10,000	10,000	10,000
Interfaces	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, 4 SFP (With 4GE SSM)	4, 10/100/1000, 1, 10/100 +4-10/100/1000, 4 SFP (With 4GE SSM)	4, 10/100/1000, 1, 10/100 +4, 10/100/1000, 4 SFP (With 4GE SSM)	8, 10/100/1000, 4 SFP, 1, 10/100	2, 10/100/1000 Management +4, 10/100/1000 (with ASA 5580-4GE-CU) +4, GE SR LC (With ASA5580-4GE-FI) +2, 10GE SR LC (With ASA 5580-2X10GE-SR)	2, 10/100/1000 Management +4, 10/100/1000 (with ASA 5580-4GE-CU) +4, GE SR LC (With ASA 5580-4GE-FI) +2, 10GE SR LC (With ASA 5580-2X10GE-SR)	8-port 10/100/1000, 2-port 10 Gigabit Ethernet* (SFP+) Maximum interfaces: 16-port 10/100/1000, 4-port 10 Gigabit Ethernet* (SFP+) (Requires IPS SSP-10)	8-port 10/100/1000, 2-port 10 Gigabit Ethernet* (SFP+) Maximum interfaces: 16-port 10/100/1000, 4- port 10 Gigabit Ethernet* (SFP+) (Requires IPS SSP-20)	6-port 10/100/1000, 4-port 10 Gigabit Ethernet (SFP+) Maximum interfaces: 12-port 10/100/1000, 8-port 10 Gigabit Ethernet (SFP+) (Requires IPS SSP-40)	6-port 10/100/1000, 4-port 10 Gigabit Ethernet (SFP+) Maximum interfaces: 12-port 10/100/1000, 8-port 10 Gigabit Ethernet (SFP+) (Requires IPS SSP-60)
Profile	Desktop	1-RU	1-RU	1-RU	1-RU	4-RU	4-RU	2-RU	2-RU	2-RU	2-RU
Stateful failover	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VPN load balancing	No	Licensed feature[2]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Shared VPN License Option	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] Devices include a license for two Premium 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 (clientless or AnyConnect client) may also not exceed the number of licensed sessions on the device. The ASA 5580 supports greater simultaneous users than the ASA 5550 at comparable overall SSL VPN throughput to the ASA 5550. 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.

[2] Upgrade is available with Cisco ASA 5510 Security Plus license.

Ordering Information

Tables 2 and 3 provide a subset of ordering information for the Cisco Secure Remote Access solution enabled by the ASA 5500 Series VPN Edition. All Cisco ASA 5500 Series appliances include the maximum number of IPsec (IKEv1) concurrent users in the base configuration of the chassis. Every Cisco ASA 5500 Series model can support clientless VPN and or Cisco Secure Desktop (CSD) through the purchase of a Premium VPN license. Premium VPN on the Cisco ASA 5500 Series may be purchased under a single part number as an edition bundle, or the chassis and SSL VPN feature license may be purchased separately, as indicated in Table 3. To place an order, visit the Cisco Ordering homepage.

Table 2. Ordering Information for Edition Bundles (AnyConnect Premium)

SSL VPN User Requirements	Edition Bundles	Edition Bundles
10 SSL VPN users	Cisco ASA 5505 SSL/IPsec VPN Edition for 10 concurrent SSL VPN users	ASA5505-SSL10-K9
25 SSL VPN users	Cisco ASA 5505 SSL/IPsec VPN Edition for 25 concurrent SSL VPN users	ASA5505-SSL25-K9
50 SSL VPN users	Cisco ASA 5510 SSL/IPsec VPN Edition for 50 concurrent SSL VPN users	ASA5510-SSL50-K9
100 SSL VPN users	Cisco ASA 5510 SSL/IPsec VPN Edition for 100 concurrent SSL VPN users	ASA5510-SSL100-K9
250 SSL VPN users	Cisco ASA 5510 SSL/IPsec VPN Edition for 250 concurrent SSL VPN users	ASA5510-SSL250-K9
500 SSL VPN users	Cisco ASA 5520 SSL/IPsec VPN Edition for 500 concurrent SSL VPN users	ASA5520-SSL500-K9
1000 SSL VPN users	Cisco ASA 5540 SSL/IPsec VPN Edition for 1000 concurrent SSL VPN users	ASA5540-SSL1000-K9
2500 SSL VPN users	Cisco ASA 5540 SSL/IPsec VPN Edition for 2500 concurrent SSL VPN users	ASA5540-SSL2500-K9
2500 SSL VPN users	Cisco ASA 5550 SSL/IPsec VPN Edition for 500 concurrent SSL VPN users	ASA5550-SSL2500-K9
5000 SSL VPN users	Cisco ASA 5550 SSL/IPsec VPN Edition for 5000 concurrent SSL VPN users	ASA5550-SSL5000-K9
5000 SSL VPN users	Cisco ASA 5585-S10 SSL/IPsec VPN Edition for 5000 concurrent SSL VPN users	ASA5585-S10-5K-K9
10000 SSL VPN users	Cisco ASA 5580-20 SSL/IPsec VPN Edition for 10,000 concurrent SSL VPN users	ASA5580-20-10K-K9
10000 SSL VPN users	Cisco ASA 5585-S20/S40/S60 SSL/IPsec VPN Edition for 10,000 concurrent SSL VPN users	ASA5585S20-10K-K9 ASA5585S40-10K-K9 ASA5585S60-10K-K9

Table 3. Ordering Information for Individual Licenses (AnyConnect Premium)

Cisco ASA Chassis and Applicable SSL VPN Licenses										
SSL VPN User Requirements	Part Number	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5585-S10	Cisco ASA 5580-20	Cisco ASA 5580-40	Cisco ASA 5585-S20/40/60
10SSL VPN users	ASA5500-SSL-10	X	X	X	X	X	X	X	X	X
25 SSL VPN users	ASA5500-SSL-25	X	X	X	X	X	X	X	X	X
50 SSL VPN users	ASA5500-SSL-50		X	X	X	X	X	X	X	X
100 SSL VPN users	ASA5500-SSL-100		X	X	X	X	X	X	X	X
250 SSL VPN users	ASA5500-SSL-250		X	X	X	X	X	X	X	X
500 SSL VPN users	ASA5500-SSL-500			X	X	X	X	X	X	X
750 SSL VPN users	ASA5500-SSL-750			X	X	X	X	X	X	X
1000 SSL VPN users	ASA5500-SSL-1000				X	X	X	X	X	X
2500 SSL VPN users	ASA5500-SSL-2500				X	X	X	X	X	X
5000 SSL VPN users	ASA5500-SSL-5000					X	X	X	X	X
10,000 SSL VPN users	ASA5500-SSL-10K							X	X	X

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, as well as 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

For more information, please visit the following links:

- Cisco ASA 5500 Series: http://www.cisco.com/go/asa
- Cisco AnyConnect Secure Mobility Solution with the WSA (Web Security Appliance): http://www.cisco.com/go/asm
- Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect
  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.html
- Cisco VPN solutions: http://www.cisco.com/go/vpn
- Licensing overview for Cisco ASA 5500 Series appliances: http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.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
- VPN licensing overview for Cisco Secure Remote Access:
  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/overview_c78-527488.html

Acknowledgement

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