



Companies rely on remote access technologies to deliver safe, secure, and flexible remote network access to their workforces. Today, remote access VPN deployments require the ability to safely and easily extend corporate network access beyond managed desktops to different users, devices, and endpoints

### 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
- Provide users with flexibility and choice in the breadth of access methods, applications, and mobile devices/endpoints
- Allow secure collaboration both within and across organizations, including the use of voice, video, and various collaborative applications
- Ensure business continuity in the event of natural disasters or unforeseen events
- Meet industry compliance requirements and legislation mandates, such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI)

### Three Key Criteria to Consider

The following criteria should be considered when choosing a remote access solution:

**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 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 connectivity media. The solution must also enable users to use whichever protocol is best for their specific connection and application set.

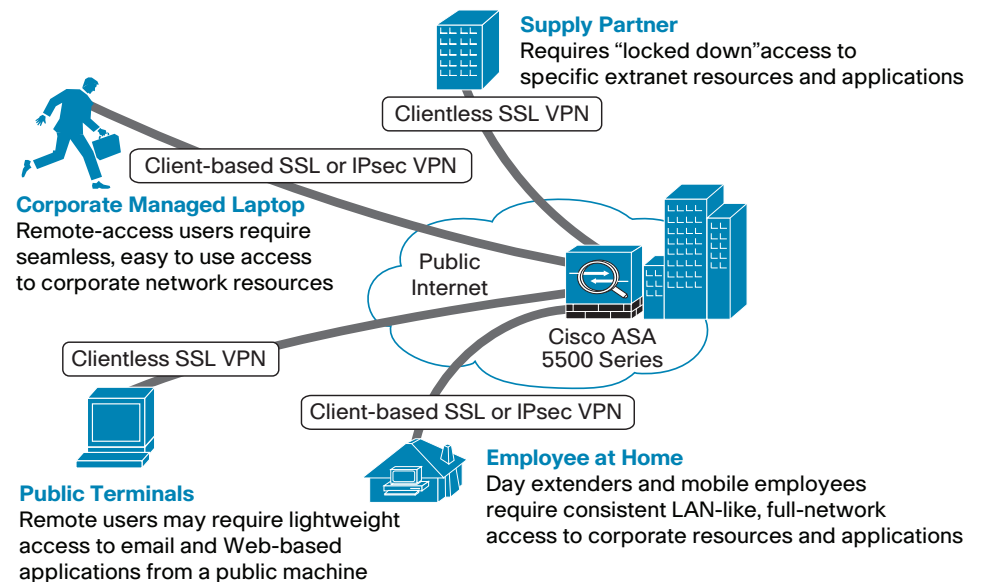
**Mobility:** With the proliferation of mobile devices, such as Apple iPhones or Windows Mobile handhelds, a secure remote access solution should enable users to connect from various endpoints and operating systems to improve collaboration and increase productivity. A strong solution should ensure that the VPN connection is persistent as users transition between different networks and through hibernation or standby.

### Cisco Secure Remote Access: Industry-leading VPN 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 remote access solution in the industry, which 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. It gives IT administrators a single point of control to assign granular access based on both the user and the device. It provides client-based, full network access and controlled access to administrator-selected web-based applications and network resources for a highly secure, flexible remote access deployment (Figure 1).

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



The Cisco Secure Remote access solution is easy to deploy and simple to use, and offers all remote access clientless and client-based options (SSL/DTLS, IPsec, L2TP/IPsec). Its robust endpoint security helps maintain the integrity of confidential information and corporate resources. The solution is designed to integrate with the ASA's advanced security services, such as the ASA's powerful, market-proven firewall, the intrusion prevention (IPS), and the content security technologies.



## Cisco Secure Remote Access Solution

- Industry's most versatile and integrated secure remote access solution offering clientless and client-based remote access
- Most complete single-appliance solution to the ever-evolving remote access 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 security policy (endpoint posture, integrated threat protection, dynamic access policies) on a single appliance
- High scale and performance levels, for up to 10,000 users on a single appliance or up to 100,000 users in loadbalancing configurations

### Cisco AnyConnect Premium-clientless VPN License

- The AnyConnect Premium license enables customers to provide secure, granular and flexible client and clientless SSL VPN access to their remote users and business partners. Deployments benefit from an incremental level of security with the Cisco Secure Desktop (CSD) suite of features: CSD Secure Vault, CSD Hostscan, keystroke logger detection and cache cleaner.
- The Cisco AnyConnect VPN Client is a new generation secure access client that provides full tunnel connectivity on fixed and mobile devices. It is a versatile, lightweight, and user-friendly, client enabling an in-office experience to virtually any application or resource. Unlike earlier remote access clients, AnyConnect is always up-to-date and remains so without requiring the end user to have administrative rights.
- The AnyConnect VPN Client provides an optimized VPN connection for latency-sensitive traffic, such as voice over IP (VoIP) traffic or TCP-based application access.
- The AnyConnect VPN Client can be pushed initially by the ASA appliance, as long as the end user has administrative rights. The installation package can also be manually installed as a Windows MSI or similar package for other operating systems.
- AnyConnect Premium Licensing is based on 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. The AnyConnect Essentials license does not include Premium capabilities such as clientless SSL VPN access and the Cisco Secure Desktop feature suite.

### Cisco AnyConnect Mobile License

- The AnyConnect Mobile license enables the AnyConnect VPN client on Mobile smartphones.
- The license is compatible with the AnyConnect Essentials and Premium licenses and includes the user-acclaimed session persistence feature, which optimizes VPN connections for environments with intermittent connectivity.

## Cisco ASA 5500 Series Secure Remote Access Solution Profile and Benefits

- **Deployment flexibility:** Extends the appropriate SSL VPN technology, either clientless or full network access, on a per session basis, depending on the user group or endpoint accessing the network.
- **Versatile access:** Offers full client access on the widest range of mobile and PC devices. Delivers ubiquitous clientless access to authenticated users on both managed and unmanaged endpoints, enabling increased productivity by providing "anytime access" to the network.
- **Flexible licensing:** Offers shared VPN FLEX business continuity and AnyConnect Essentials licensing options to allow maximum flexibility in deployment, management, and scalability.
- **Complete range of security options:** Enables flexible remote access for varied user groups with the highest security confidence.
- **Scalability:** 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.
- **Widest range of connectivity options:** Helps ensure that businesses can securely respond to the growing user requirements for new endpoint and applications support, including support for Windows Mobile 5.0, 6.0, and 6.1; the Apple iPhone; Windows XP and Vista (32 and 64 bit), Windows 7 (Beta); and Mac OS X 10.4 and 10.5.
- **Comprehensive, optimized network access:** Broad application and network resource access as well as optimized VPN connection for latency-sensitive traffic, such as voice over IP (VoIP) traffic or TCP-based application access through the Cisco AnyConnect VPN Client, an automatically downloadable network-tunneling client that provides access to virtually any application or resource.
- **Optimized network performance:** The Cisco AnyConnect VPN Client provides an optimized VPN connection for latency-sensitive traffic, such as voice over IP (VoIP) traffic or TCP-based application access.
- **Granular control:** Empowers network and IT management with additional tools to provide controlled access to corporate resources and applications. Allows granular policy setting and enforcement for remote access of various user groups on a single appliance.
- **Unparalleled management flexibility:** Simplifies the complexity of managing diverse remote access connectivity requirements common in today's enterprise.
- **Low total cost of ownership:** Reduces expensive help-desk calls associated with network connectivity issues and eliminates the administration costs of managing VPN client software on every endpoint.
- **Low cost of entry:** Offers client-based connectivity options on all supported endpoint platforms, including mobile endpoints, at a cost-effective price point.



## Cisco ASA 5500 Product Family

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

Figure 1. 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

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
<b>Maximum VPN Throughput</b>	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
<b>Maximum Concurrent SSL VPN Sessions<sup>1</sup></b>	25	250	750	2500	5000	10,000	10,000
<b>Maximum Concurrent IPsec VPN Sessions<sup>1</sup></b>	25	250	750	5000	5000	10,000	10,000
<b>Interfaces</b>	Eight 10/100 copper Ethernet ports with dynamic port grouping (includes two Power over Ethernet ports) and three USB ports	Five 10/100 copper Ethernet ports and two USB ports	Four 10/100/1000 copper Ethernet ports, one out-of-band management port, and two USB ports	Four 10/100/1000 copper Ethernet ports, one out-of-band management port, and two USB ports	Eight Gigabit Ethernet ports, four SFP fiber ports, and one Fast Ethernet port	Two USB ports, two RJ-45 management ports, two Gigabit Ethernet management ports with interface expansion cards Up to twelve 10 Gigabit Ethernet (10GE) ports Up to twenty-four Gigabit Ethernet ports Up to twenty-four 10/100/1000 Ethernet ports	Two USB ports, two RJ-45 management ports, two Gigabit Ethernet management ports with interface expansion cards Up to twelve 10GE ports Up to twenty-four Gigabit Ethernet ports Up to twenty-four 10/100/1000 Ethernet ports
Profile	Desktop	1 RU	1 RU	1 RU	1 RU	4 RU	4 RU
Stateful failover	No	Licensed feature <sup>2</sup>	Yes	Yes	Yes	Yes	Yes
VPN load balancing	No	Licensed feature <sup>2</sup>	Yes	Yes	Yes	Yes	Yes

<sup>1</sup> 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 appliance supports greater simultaneous users than the ASA 5550 appliance, at comparable overall SSL VPN throughput as the ASA 5550. These items should be taken in to consideration as part of your capacity planning.

<sup>2</sup> 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 ASA 5500 Series Remote access/VPN Edition. All Cisco ASA 5500 Series appliances include maximum IPsec concurrent users in the base configuration of the chassis. All SSL VPN features are included under a single feature license. Every Cisco ASA 5500 Series model can support SSL VPN through the purchase of an SSL VPN license. SSL 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 Home Page.

## 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 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](http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html)
- **Ordering Document:**  
[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/overview\\_c78-527488.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/overview_c78-527488.html)

**Table 2: Ordering Information for Edition Bundles (AnyConnect Premium)**

SSL VPN User Requirements	Edition Bundles	Edition Bundle Part Number
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 2500 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
10,000 SSL VPN users	Cisco ASA 5580-20 SSL/IPsec VPN Edition for 10,000 concurrent SSL VPN users	ASA5580-20-10K-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 5580-20	Cisco ASA 5580-40
10 SSL VPN users	ASA5500-SSL-10	X	X	X	X	X	X	X
25 SSL VPN users	ASA5500-SSL-25	X	X	X	X	X	X	X
50 SSL VPN users	ASA5500-SSL-50	-	X	X	X	X	X	X
100 SSL VPN users	ASA5500-SSL-100	-	X	X	X	X	X	X
250 SSL VPN users	ASA5500-SSL-250	-	X	X	X	X	X	X
500 SSL VPN users	ASA5500-SSL-500	-	-	X	X	X	X	X
750 SSL VPN users	ASA5500-SSL-750	-	-	X	X	X	X	X
1000 SSL VPN users	ASA5500-SSL-1000	-	-	-	X	X	X	X
2500 SSL VPN users	ASA5500-SSL-2500	-	-	-	X	X	X	X
5000 SSL VPN users	ASA5500-SSL-5000	-	-	-	-	X	X	X
10,000 SSL VPN users	ASA5500-SSL-10K	-	-	-	-	-	X	X