Remote Access with Cisco Adaptive Security Appliance (ASA) Software Version 9.0

New Remote Access Features in Cisco Adaptive Security Appliance (ASA) Software Version 9.0.

Q. Does the new Cisco Adaptive Security Appliance Software support IPv6 remote access connections? What IPv6 support does the Cisco Adaptive Security Appliance Software Version 9.0 include?

A. Starting with Cisco Adaptive Security Appliance Software Version 8.4, IPv4/IPv6 dual-stack inside a Secure Sockets Layer (SSL) tunnel is supported.

Cisco Adaptive Security Appliance Software Version 9.0 expands this support, offering IPv4 and IPv6 outside either an SSL or IPsec Internet Key Exchange (IKEv2) tunnel (on the public interface) when used in conjunction with Cisco AnyConnect® Version 3.1 or later. The Cisco Adaptive Security Appliance Software 9.0 also enables IPv6 clientless support.

Q. Does the Cisco Adaptive Security Appliance support Next-Generation Encryption (including Suite B)?

A. Starting with the Cisco Adaptive Security Appliance Software Version 9.0, the Cisco Adaptive Security Appliance supports Suite B remote access and LAN-to-LAN connections using an IPsec tunnel. For more information, see AnyConnect VPN - Next-Generation Encryption.

Q. Is Next-Generation Encryption available on all platforms?

A. Next-Generation Encryption is fully supported on the following Cisco Adaptive Security Appliance Series: ASA 5500-X (5515, 5525, 5545, and 5555), ASA 5580, ASA 5585, and ASA-SM. Next-Generation Encryption is only partially supported on the Cisco ASA 5505, 5510, 5520, 5540, and 5550 Series Adaptive Security Appliances due to hardware limitations. Cisco AnyConnect Secure Mobility Client 3.1 or later and an AnyConnect™ Premium license are also required to use Next-Generation Encryption for remote access connections.

Q. Can we use the Cisco VPN Client with Cisco Adaptive Security Appliance Software Version 9.0?

A. Yes, the Cisco VPN Client is supported in Cisco Adaptive Security Appliance Software Version 9.0. The Cisco VPN Client is no longer under active development and customers are encouraged to migrate to Cisco AnyConnect Secure Mobility Client as soon as possible.

Q. Does the Cisco Secure Remote Access VPN solution support Cisco virtual desktop infrastructure (VDI)?

A. With Cisco Adaptive Security Appliance Software Version 9.0, native clientless support for Citrix VDI deployments has been updated to include XenApp 6.5, and the latest versions of XenDesktop (up to 5.5) both for laptops, desktops, and mobile devices (Citrix Mobile Receiver). Support for VMware VDI deployments is offered as well (through smart tunnels). As in past releases, AnyConnect supports VDI deployments, whether Citrix or VMware.

Q. Is there an easier way to setup network single sign-on (SSO) for end users?

A. Yes, with the Cisco Adaptive Security Appliance Software Version 9.0 software release, Cisco has provided templates and wizards for Auto Sign-On configuration for various applications such as Outlook Web Access (OWA), SharePoint, Citrix-based applications, and so on.

Q. Has a new file browser plug-in been made available with the Cisco Adaptive Security Appliance Software Version 9.0?

A. Yes, Cisco has created a new Java-based plug-in that can be used for file browsing over the network with the Cisco Adaptive Security Appliance Software Version 9.0. The plug-in works with the latest browsers supported by the Cisco Adaptive Security Appliance Software Version 9.0.

Cisco Adaptive Security Appliance Secure Remote Access

Q. Can we use the Cisco Adaptive Security Appliance for both firewall and remote access on the same platform?

A. Yes, the Cisco Adaptive Security Appliance is designed for just that purpose. Smaller installations are likely to use the Cisco Adaptive Security Appliance as both a firewall and remote access solution. Larger installations tend towards using the Cisco Adaptive Security Appliance as either a dedicated firewall or remote access solution.

Q. Does the Cisco Adaptive Security Appliance support remote access hardware acceleration? I don't see an option to purchase hardware acceleration.

A. Yes, by default, the Cisco Adaptive Security Appliance has cryptographic accelerators. The cryptographic accelerators are built-into the Cisco Adaptive Security Appliance and are not optional.

Q. Does the Cisco Adaptive Security Appliance support load balancing for remote access connections?

A. Yes, the Cisco Adaptive Security Appliance has its own internal load balancing capabilities but can also support external load balancers. DNS-based load balancing devices are compatible only with the Cisco AnyConnect Secure Mobility Client connections and not Cisco Clientless Remote Access connections.

Q. Does the Cisco Adaptive Security Appliance support failover if another Cisco Adaptive Security Appliance fails?

A. Yes, the Cisco Adaptive Security Appliance has a high availability mode where there is a second Cisco Adaptive Security Appliance standing by. The second Cisco Adaptive Security Appliance keeps state information. If the first Cisco Adaptive Security Appliance fails, the second Cisco Adaptive Security Appliance takes over without dropping connections.

Q. Does the Cisco Adaptive Security Appliance support emergency scenarios such as natural disasters, when a larger than usual employee population needs to work from home for a few days?

A. Yes, the Cisco Adaptive Security Appliance supports a flexible licensing concept where the number of connections can burst to the maximum capabilities of the appliance. This is called Flex licensing and is a consumable license offering 56 days of burst licensing that is consumed in one-day increments.

Q. Can I establish a remote access connection to the Cisco Adaptive Security Appliance using a third-party client?

A. Yes, the Cisco Adaptive Security Appliance supports remote access connections using VPN clients in many of the popular operating systems. These clients use Layer 2 Tunneling Protocol over IPsec (L2TP/IPsec) as their underlying protocol. While Cisco strives to adhere to industry standards such as L2TP/IPsec, Cisco cannot certify interoperability with every L2TP/IPsec client on the market.

Q. Does the Cisco Adaptive Security Appliance support site-to-site VPN connections?

A. Yes, the Cisco Adaptive Security Appliance supports both site-to-site and remote access VPN connections.

Q. Can users be authenticated using an external database?

A. Yes, the Cisco Adaptive Security Appliance supports connection to Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) to authenticate remote users.

Q. Can the Cisco Adaptive Security Appliance be connected to a RADIUS infrastructure to authenticate users?

A. Yes, the Cisco Adaptive Security Appliance supports RADIUS for authenticating remote access users.

Q. Does the Cisco Adaptive Security Appliance have a local database to authenticate remote access users?

A. Yes, the Cisco Adaptive Security Appliance supports the use of a local database to authenticate remote access users. However, Cisco typically recommends using an external authentication server for production deployments.

Q. Does the Cisco Adaptive Security Appliance support token authentication such as RSA SecureID?

A. Yes, RSA SecureID is supported natively by the Cisco Adaptive Security Appliance for remote access authentication. Other token methods may be used with the Cisco Adaptive Security Appliance for remote access through a RADIUS server such as Cisco Secure Access Control Server (ACS).

Q. Our authorization policy is more granular than simply permitting remote access users onto the enterprise network. What capabilities does the Cisco Adaptive Security Appliance have to support our needs?

A. The Cisco Adaptive Security Appliance provides granular control over the authorization of VPN users through Dynamic Access Policies (DAP). DAP provides a configurable set of authorization attributes that are useful in situations where the endpoint that is connecting is not static and its circumstances, such as location or posture, may have changed.

Q. Does the Cisco Adaptive Security Appliance support split-tunneling with remote access connections?

A. Strictly speaking, split tunneling is a function of Cisco AnyConnect client and not of the Cisco Adaptive Security Appliance. Cisco AnyConnect supports split tunneling such that packets can be conditionally directed over a tunnel in encrypted form or to a local network interface on the client machine in clear text form.

Q. What kinds of logging does the Cisco Adaptive Security Appliance support for remote access?

A. The Cisco Adaptive Security Appliance supports console logging, terminal logging, Cisco Adaptive Security Device Manager (ASDM) logging, email logging, external syslog server logging, external Simple Network Management Protocol (SNMP) logging, buffered logging, and RADIUS accounting.

Q. Is SSL VPN better than IPsec for remote access?

A. There has been an ongoing debate whether IPsec or SSL is better for remote access connections. While each method has advantages too numerous to be discussed here, the Cisco Adaptive Security Appliance supports both IPsec and SSL for remote access connections.

Q. What methods can be used to assign an IP address to a remote access connection?

A. The Cisco Adaptive Security Appliance supports a local address pool, Dynamic Host Configuration Protocol (DHCP), and authentication/authorization databases that support the assignment of IP addresses.

Q. Does the Cisco Adaptive Security Appliance support both Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers?

A. Yes, the Cisco Adaptive Security Appliance can be configured to use primary and secondary DNS and WINS servers for remote access connections.

Q. Does the Cisco Adaptive Security Appliance support either Certificate Revocation List (CRL) checking or Online Certificate Status Protocol (OCSP)?

A. Yes, the Cisco Adaptive Security Appliance can be configured to make CRL or OCSP checks either mandatory or optional. If the check is optional, the certificate authentication will succeed if the Validation Authority is unavailable to provide updated data.

Q. Does the Cisco Adaptive Security Appliance support a local certificate authority?

A. Yes, the Cisco Adaptive Security Appliance local certificate authority integrates basic certificate authority functionality including certificate generation, deployment, and secure revocation checking of issued certificates.

Starting with Cisco Adaptive Security Appliance Software Version 9.0, the local certificate authority on the Cisco Adaptive Security Appliance will support a key size up to 4096 bits.

Q. What certificate authority servers are supported by the Cisco Adaptive Security Appliance?

A. The Cisco Adaptive Security Appliance supports Cisco IOS® Software Certificate Server (CS), Baltimore Technologies, Entrust, Microsoft Certificate Services, Netscape CMS, RSA Keon, and VeriSign certificate authority servers.

Q. Can I establish a remote access session using nothing more than a browser?

A. Yes, the Cisco Adaptive Security Appliance supports remote access connections using a browser. The technology is called clientless remote access. See the Cisco Clientless Remote Access section for details.

Q. I understand Cisco has a remote access client called Cisco AnyConnect Secure Mobility Client. Why would I use the AnyConnect client rather than just using a third-party client or using clientless remote access?

A. There are two end-user remote access methodologies: client and clientless. Clientless is typically used on non-corporate assets while a client-based solution is used on corporate assets. With Cisco AnyConnect Secure Mobility Client, Cisco controls both ends of the remote access connection. Therefore, remote access connections using AnyConnect can offer a richer user experience and more granular controls than third-party clients.

Q. Can I do posture assessment as part of a remote access connection?

A. Yes, you can do posture assessment with client and clientless connections.

Q. Is there a special license for posture?

A. Please see the Cisco Secure Desktop section.

Q. I have client-focused remote access questions. Where can I go to get my questions answered?

A. There is AnyConnect focused Q&A here.

Cisco Adaptive Security Appliance Secure Remote Access Licensing

Q. Can Cisco the Cisco Adaptive Security Appliance share client licenses?

A. Yes, the Cisco Adaptive Security Appliance can support shared AnyConnect Premium licenses. One Cisco Adaptive Security Appliance acts as a license server and issues licenses as necessary to participant Cisco Adaptive Security Appliances. This capability is helpful with large Cisco Adaptive Security Appliance remote access pools. Cisco offers both shared and non-shared Premium SSL license options.

Q. What happens if the Cisco Adaptive Security Appliance that is acting as the shared license server fails?

A. If the Cisco Adaptive Security Appliance that is acting as the license server fails, another Cisco Adaptive Security Appliance (designated as a backup) will automatically pick up the license server function.

Q. What licenses are required for my employee's mobile devices and tablets to connect?

A. The Cisco Adaptive Security Appliance requires a Cisco AnyConnect Essentials or a Premium license, enabling remote access plus a Mobile license for mobile device connectivity.

Q. How many Essentials or Mobile licenses do I need per user?

A. Both the AnyConnect Essentials and Mobile licenses are per Cisco Adaptive Security Appliance and **not** per user. This means that a single AnyConnect Essentials and a single AnyConnect Mobile license are required per Cisco Adaptive Security Appliance. Both licenses are required to support mobile operating systems such as iOS or Android.

Q. Where can I get a trial Mobile license?

A. A 3-month trial Mobile license can be obtained here.

Q. When ordering licenses, what does L-mean in front of some of the licenses?

A. Licenses that begin with L- are electronically delivered (versus normal paper license ordering). E-delivery licenses are delivered significantly faster than paper licenses as they do not need to be manufactured and shipped to you.

Q. Where can I find more information about Cisco Secure Remote Access licensing?

A. Please refer to our licensing documentation here.

About the Cisco AnyConnect Secure Mobility Solution

Q. What is the Cisco AnyConnect Secure Mobility Solution?

A. The Cisco AnyConnect Secure Mobility Solution combines web security and remote access VPN for an exceptionally comprehensive and secure enterprise mobility solution. Most enterprise traffic is web-based, which dramatically increases the level of security threats. The Cisco AnyConnect Secure Mobility Solution uses the Cisco AnyConnect Secure Mobility Client and Cisco ASA 5500 Series Adaptive Security Appliance with either a premises-based Cisco Web Security Appliance or Cisco Cloud Web Security to provide acceptable use policy (AUP) controls, malware filtering, data security, and application visibility and control.

Q. How can I learn more about the Cisco AnyConnect Secure Mobility Solution?

A. More information is available at http://www.cisco.com/en/US/netsol/ns1049/index.html.

Cisco Clientless Remote Access

Q. What is clientless remote access?

A. Clientless remote access lets users establish a secure, remote-access VPN tunnel to a Cisco Adaptive Security Appliance through a web browser using SSL technology. Users do not need a software or hardware client. Clientless remote access provides secure and easy access to a broad range of web resources and applications from almost any computer with Internet access.

Q. What applications can I access using clientless remote access?

A. You can provision a wide variety of applications that can be accessed through the clientless portal. These include web-enabled applications, such as Outlook Web Access, Domino Web Access, and SharePoint, as well as various TCP/IP applications, such as Common Internet File System (CIFS), FTP, Remote Desktop Protocol (RDP), Secure Shell (SSH) Protocol, Telnet, and so on.

Q. What operating systems and browsers are supported?

A. Information on the operating systems and browsers supported with clientless remote access can be found here.

Q. How is clientless remote access licensed?

A. Clientless remote access is licensed as part of the Cisco AnyConnect Premium license.

Q. Can I provide access to Virtual Desktop Integration (VDI) resources using clientless remote access?

A. Yes, one can provide access to VDI resources that are published through other VDI vendors such as Citrix, through the clientless portal, plugins, or the Mobile Receiver to gain access to the published apps or desktop.

Q. Does the Cisco Adaptive Security Appliance have granular controls of the ICA connection such as prevent cut and paste, control printer, drive, clipboard, or USB redirection?

A. The Cisco Adaptive Security Appliance does not modify functionality for cut and paste, control printer, drive, clipboard or USB redirection. Those policies are controlled using XenApp or XenDesktop and will be reflected on the receiver client.

Q. Can we provide our users seamless access to enterprise web applications protected by Kerberos authentication?

A. Yes, clientless remote access supports Kerberos Constrained Delegation (KCD) for seamless access to enterprise web applications protected by Kerberos authentication.

Q. Does the new feature Citrix Receiver Proxy retain the granular controls configured on the XenServer?

A. Yes, controls such as client drive redirection, client printer redirection, client clipboard redirection, and client USB devices redirection are defined on the XenServer and are part of the ICA file.

Q. Does clientless remote access support Security Assertion Markup Language (SAML) for Single Sign-On?

A. Yes, the Cisco Adaptive Security Appliance clientless interface supports SAML for single sign-on logs to web services that support SAML 1.1.

Q. Is there any failover to clientless remote access in the event of a hardware failure or power loss?

A. Yes, the Cisco Adaptive Security Appliance supports two failover methods - Active/Standby and Load Balancing. Active/Standby mode where a second Cisco Adaptive Security Appliance acts as a standby machine in case of a failure of the primary Cisco Adaptive Security Appliance. Session state is maintained between the two machines so connections are not lost in the event of a failure. With load balancing, however, actual applications that are in use over the connection may require interaction to re-establish connectivity. With load balancing, multiple Cisco Adaptive Security Appliances are used simultaneously but the state is not maintained between the appliances.

Q. Can the Cisco Adaptive Security Appliance host a custom HTML page?

A. Yes, custom HTML pages can be uploaded to the Cisco Adaptive Security Appliance provided they contain only HTML and/or JavaScript. No server side processing such as PHP is supported.

Cisco Secure Desktop

Q. What is Cisco Secure Desktop?

A. Cisco Secure Desktop seeks to minimize the risks posed by the use of remote devices to establish a Cisco clientless remote access or Cisco AnyConnect Secure Mobility Client session. Cisco Secure Desktop provides a number of features that you can configure to work independently or together**.**

Q. What are the features of Cisco Secure Desktop?

A. Cisco Secure Desktop is a suite of features enabling end-to-end security during remote access connections. Cisco Secure Desktop features include: HostScanning and pre-login posture assessment, whose result is integrated with Dynamic Access Policies (DAP), cache cleaner, and secure vault (session desktop emulation).

Q. What operating systems and browsers are supported?

A. Operating system and browser support information can be found here.

Q. How is Cisco Secure Desktop licensed?

A. Cisco Secure Desktop is licensed as part of the AnyConnect Premium license.

Q. I have many questions about Cisco Secure Desktop. How can I get my questions answered?

A. There is a separate FAQ on Cisco Secure Desktop that can be found here.

Additional Information

Q. Where can I find more information on the Cisco AnyConnect Secure Mobility Client?

A. See the Cisco AnyConnect Secure Mobility Client site at: http://www.cisco.com/go/anyconnect.

Q. Where can I find more information on the Cisco AnyConnect Secure Mobility Solution?

A. See the Cisco AnyConnect Secure Mobility Solution site at: http://www.cisco.com/go/asm.

Q. Where should I direct questions regarding mobile licenses?

A. Please send email to ac-mobile-license-request AT cisco.com.

Q. Where can I direct feedback and questions about AnyConnect on Mobile devices?

A. Please send email to the ac-mobile-feedback AT cisco.com.

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 C67-713763-00 09/12