RFP Boiler Plate

From ASApedia

Contents

Material Under Review

Please contact asa-tme@cisco.com, asa-pm@cisco.com for accuracy before quoting the material to your customers.

ASA VPN Solution RFI/RFP Boilerplate

General Features

Question	Response
	The Cisco ASA 5500 Series VPN Edition offers flexible VPN technologies for any connectivity scenario with scalability up to 5000 concurrent users per appliance. Providing easy-to-manage full-tunnel network access through both SSL VPN and IPSec VPN client technologies, advanced clientless SSL VPN capabilities, and network-aware site-to-site VPN connectivity, the VPN Edition enables businesses to

create secure connections across public networks to mobile users, remote sites, contractors, and business partners. Furthermore, the VPN Edition reduces costs associated with VPN deployment and operations by eliminating ancillary equipment required to scale and secure the VPN deployment.

The Cisco ASA 5500 Series VPN Edition provides complete security for VPN deployments through its integrated network and endpoint security technologies. Additionally, detailed application and access control policy can be applied to VPN traffic, so individuals and groups of users have access to the applications, network services, and resources to which they are entitled. 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 and spreads.

ASA Product Highlights

- SSL and IPSec-based full network remote access—Full network access provides network-layer remote-user connectivity to virtually any application or network resource. Connectivity is provided either through the dynamically downloaded Cisco SSL-VPN client for web-VPN or the Cisco IPSec-VPN client. Full network access is generally extended to managed desktops such as company-owned employee laptops. By supporting both SSL- and IPSec-based remote-access VPN technologies, the Cisco ASA 5500 Series delivers industry-leading flexibility to meet the needs of the most diverse deployment scenarios.
- Superior clientless network access—Clientless remote access provides access to network applications and resources, regardless of location, without the need for desktop VPN client software. Using the ubiquity of SSL encryption available in Internet browsers, the Cisco ASA 5500 Series delivers clientless access to any web-based application or resource, terminal services applications such as Citrix, and optimized Microsoft Outlook Web Access and Lotus iNotes, as well as access to common thick-client applications like e-mail, instant messaging, calendars, and Telnet. Furthermore, the superior content rewriting capabilities of the Cisco ASA 5500 Series help ensure reliable rendering of complex web pages with Java, Java Script, and ActiveX content.
- Network-aware site-to-site VPNs—Enables secure, high-speed communications between multiple office locations. With support for quality of service (QoS) and routing across the VPN, the Cisco ASA 5500 Series helps ensure reliable, business-quality delivery of latency-sensitive applications like voice, video, and terminal services.
- Threat-Protected VPN—VPNs are a primary source of malware infiltration into organizations' networks. The depth and breadth of intrusion prevention, antivirus, application-aware firewall, and VPN endpoint security capabilities in the Cisco ASA 5500 Series helps ensure that the VPN connection does not become a conduit for security threats.
- More cost-effective VPN deployment and operations—Scaling and securing VPNs often require adjunct load balancing and security equipment, which increases both equipment and operational costs. The Cisco ASA 5500 Series integrates these functions, delivering an industry-leading level of network and security integration among the VPN products available today. And by offering

Provide an overview of the solution?	both SSL and IPSec VPN on one platform, the Cisco ASA 5500 Series provides customers with cost-effective alternatives to deploying parallel VPN infrastructures. **ASA Advanced Features** Enterprises are concerned about the probability of viruses and worms propagating into their network environment by workstations using remote access. To address these concerns, the Cisco SSL-VPN solutions provide the following safeguards: ▪ Extensive Malware Mitigation—Worms, viruses, spyware, keyloggers, Trojan horses and rootkits are thwarted at the Cisco ASA 5500 Series VPN gateway, thereby eliminating threats before they spread throughout the network ▪ Application-Aware Firewall and Access Control—Application-aware traffic inspection enables thorough user access control and helps prevent abuse of unwanted applications, such as peer-to-peer file sharing across the VPN connection ▪ Intrusion Prevention—The Cisco ASA 5500 Series guards against a multitude of network exploits. And ASA's pre-connection Posture Assessment for Host integrity verification checking confirms the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access. ▪ Comprehensive Session Protection—Absolute protection is provided for all data associated with the session, including passwords, file downloads, history, cookies, and cache files. All session data is encrypted to the secure vault of the Cisco Secure Desktop. ▪ End-of-Session Data Cleanup—All data in the secure vault is overwritten at the end of the session. ▪ Keystroke Logger Detection—Performs an initial check for keystroke logging software at the start of the session. If an anomalous program begins running inside the secure vault, after session initiation, the user is prompted to stop the suspicious activity. ▪ Available with Guest Permissions—Users accessing the network from remote machines may not have administrator privileges on all systems. Cisco Secure Desktop can be installed with only guest permissions; this helps to ensure delivery and installation on all systems. In addition to the features mentioned above, the Cisco Secure Desktop (L3 client) also has the ability to define different policies and profiles based on identification of the specific network locations and the types of network devices (home PC, Internet kiosk, or corporate laptop), helping to ensure that all confidential data is protected without impacting user productivity. Features can be activated based on host integrity checking, which confirms the presence of antivirus software, personal firewall software, and the Windows operating system and service packs on the endpoint system. For example, a company may have a policy that all contractors must have personal firewall software running on their PCs to access the corporate network. If

	the firewall is not present, or present but not operating, the user can be denied access or be directed to a separate web page where additional instructions can be found, such as instructions on how to download the personal firewall software. A company may also have a policy for when to download Cisco Secure Desktop, dependent upon the endpoint device. Remote employees using their corporate laptops may not need the high level of protection found in Cisco Secure Desktop; however, those same employees accessing the network from an Internet kiosk would require this protection. Cisco Secure Desktop allows full customization of when and where it is downloaded.
What are key difference in the models?	The ASA Security Appliance models include ASA 5505, 5510, 5520, 5540and 5550 all using the same software. The model differences are: ■ Throughput performance and connections/sec ■ IPSec and SSL concurrent sessions ■ Numbers of physical and logical interfaces supported ■ Memory ■ Security contexts The detailed capabilities and differences between the units are in the chart following this section titled Hardware Model.
List key product VPN related features	■ High performance VPN throughput up to 360 Mbps ■ Integrated IPSec and SSL support in one device. ■ DTLS support for SSL Client, first in the industry. ■ SSL Clientless: Multiple application support via Plug-ins, SmartTunnels, Port-Forwarding. ■ Customized web-portals and authentication pages. ■ Advanced End-Point Assessment with Dynamic Access Policies ■ Secure Desktop ■ Expandable to support up to 10 interfaces ■ Web based management software and command line interface support
These responses are based on what version of production code?	Cisco ASA Security Appliance 8.0(2), ASDM 6.0(2), Cisco VPN Client 4.0, AnyConnect 2.0, Cisco Secure Desktop 3.2.
How long has your proposed solution been in production?	The ASASecurity Appliance has been introduced in May 2005. The ASA was developed by leveraging the features already available in the Cisco PIX security appliance and Cisco VPN3000 concentrator which were available from September 1996.
	Cisco Security Training Cisco develops uniquely tailored training courses that help users secure, monitor, test, and improve their network security. Training on security products and technologies reaches professionals in every corner of the world through

Summarize documentation available?	the global network of Cisco Learning Partners as well as through Cisco Press books, CD-ROMs, web-based training, Quick Learning Modules and virtual classrooms. Quick Learning Modules are a quick and easy way to learn a specific configuration task on Cisco security products. Learning modules are a great way to supplement formal training classes. For formal web-based or instructor-led training, Cisco utilizes several training partners, and our Learning Credits program, to deliver the most effective knowledge to our customers. [TBD: Following list needs to be updated with ASA classes]. To find a training class in your region, visit the Cisco Learning Locator at http://www.cisco.com/go/class_locator and search for any of the following Cisco security courses: ▪ Cisco Secure PIX Security Appliance Advanced ▪ Cisco Secure Intrusion Detection System ▪ Cisco Secure IDS Host Sensor ▪ Cisco Secure Virtual Private Networks ▪ Managing Cisco Network Security ▪ Cisco Secure Policy Manager ▪ Cisco SAFE Implementation v1.0 Training on CD-ROM Security training is now available on CD-ROM to Channels/Resellers through the Learning Store. ▪ CSPFA #TRNG-800238 ▪ CSIDS #TRNG-800237 ▪ CSVPN #TRNG-800200 Cisco Press Books for security are now available through your favorite local and/or online bookseller. ▪ Cisco Secure PIX Security Appliance Advanced ▪ Cisco Secure Virtual Private Network ▪ Cisco Secure Intrusion Detection System ▪ Managing Cisco Network Security

Hardware Features

Question	Response
Does the device have 100/1000Mbps RJ45 Ethernet connectors?	The low-end ASA5505 appliance has 8-port 10/100 RJ45 Ethernet connectors including 5510 Platform 5 Fast Ethernet ports; (2 Gigabit Ethernet + 3 Fast Ethernet ports are avai All other ASA firewall/VPN appliances (5520, 5540 and 5550) ship with four 10/100/1(interfaces and a single 10/100 interface. Additional interfaces can be installed into the S 10/100/1000 module is available that provides both copper and fiber optic connections.

	In addition, all interfaces on ASA support 802.1q VLAN interfaces. Detailed informatio (http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_
Does the device provide 100 Mbps RJ45 Ethernet connector for Management?	All ASA firewall/VPN appliances(except 5505) have a 10/100 RJ45 copper Ethernet int used for out-of-band device management. In addition, ASA also has a dedicated console
Does the device have redundant storage (Hard Disk, Flash)?	ASA does not use a general purpose operating system, and has no need for hard drives. provide additional operating system images and configuration files.
Does the device have dual power supplies and fans?	ASA5580 series appliances support redundant power supplies, and have multiple coolin

Secure Gateway Features

Question	Response
Does the security appliance support basic firewall capabilities?	The ASA-5500 family provides advanced firewalling capabilities, both towards itself, and for traffic that traverses through it or through IPsec or SSL VPN tunnels that terminate on it. The ASA supports filtering based on source and destination addresses, ports, and protocols, as well as the ability to filter based on time-of-day. ASA's superior stateful inspection capabilities enable deep packet inspection for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports
	The ASA is a full-featured stateful inspection firewall with enhanced application inspection capabilities. Basic application inspection is supported on all major protocols. Enhanced inspection is available on HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMPT, DNS, RPC, CIFS, MSRPC, and NETBIOS. With the enhanced application inspection features, it is possible to exercise a great deal of control over the behavior of network communications using those protocols. For example, with SIP inspection, you can utilize regular expressions (REGEX) to deny SIP-based VOIP communications with certain addresses or countries. The Cisco Modular Policy Framework provides a powerful, highly flexible

Describe the stateful inspection capability available in the security appliance?	framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on different conditions, and then apply a set of customizable services to each flow or class. The framework improves control over applications by introducing the ability to have flow- or class-specific firewall and inspection policies, QoS policies, connection limits and timers, and more. In addition to its inherent application inspection capabilities, the ASA can be enhanced by installing specialized hardware modules. There are currently two modules available: the CSC-SSM and the AIP-SSM. The CSC-SSM module provides content filtering and inspection of web and FTP traffic. It also provides file-based anti-virus, anti-worm, anti-phishing, anti-spam, and anti-spyware. This is used most often for protecting end-user PC's that are connecting through the ASA, both for traditional firewalling and VPN connections. The AIP-SSM module provides full-featured network-based intrusion detection and protection services, with the full signature-based capabilities of the dedicated IPS appliances offered by Cisco. In addition, the AIP-SSM module supports custom signatures, zero-day anomaly detection, and passive OS detection for optimized protection capabilities.
Does the device provide application or protocol bandwidth management?	ASA delivers per-flow, policy-based QoS services, with support for LLQ and Traffic Policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications. ASA enables businesses to have end-to-end QoS policies for their extended networks.
Does the proposed solution support remote access and site-to-site IPSec VPN services on a single device?	In addition to terminating remote access users, ASA can also act as Site-to-Site VPN Gateway. ASA extends networks securely over the Internet by helping ensure data privacy, data integrity, and strong authentication to remote networks, with support for up to 10,000 simultaneous remotely connected sites. ASA supports Internet Key Exchange (IKE) and IPSec VPN standards with hub-and-spoke or meshed VPN configurations. ASA improves network reliability and performance through support of OSPF dynamic routing and reverse-route injection over the site-to-site VPN tunnels.
Does the proposed solution support SSL and IPSec remote access on a single device?	Yes. Streamlined operations for SSL (Clientless and Client) and IPSec deployments serve both user populations.
Explain the VPN performance degradation when some or all of the firewall and stateful inspections are	Performance is not significantly affected by enabling the firewall features. SSL and IPsec encryption is performed by dedicated hardware processors. IPS and content security is performed by dedicated add-in modules, each with its own processors, storage, and memory. Advertised numbers for ASA performance is based on Internet MIX traffic, with all normal features enabled.

enabled?	
Does the device support idle session timeout for remote access users?	Yes. The administrator can define an idle timeout period on a user or group basis. Additionally, one can define maximum session duration and access policies based on time of day (i.e. access hours).

Authentication, Authorization and Access Policies

Question	Response
Please list the authentication methods supported by the device?	The ASA VPN solution supports all popular authentication mechanisms, including but not limited to Local user database, RADIUS, Windows NT LAN Manager (NTLM), Active Directory Kerberos, Native RSA SecurID, RADIUS with Expiry, one-time password (OTP) via RADIUS (State/Reply message attributes), Lightweight Directory Access Protocol (LDAP) with password expiry capabilities (including pre-expiry warning), digital certificates (including X.509), smartcards, SSO and SPNEGO. ASA supports CRL and OCSP for certification revocation checks. ASA also supports AAA and Certificate authentication simultaneously. Additionally, the ASA can look at fields in the certificate to make additional policy decisions. Finally, the ASA can also act as a certificate authority. The ASA is designed to bind granular policies to specific users or groups across multiple identity management systems via Dynamic Access Policies (DAP). DAPs are created by setting a collection of access control attributes associated with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security.
Describe any integration with enterprise SSO systems?	The ASA supports the following Single Sign On (SSO) methods: ■ Computer Associates Siteminder (Netegrity) ■ RSA Access Manager (ClearTrust) ■ Security Assertion Markup Language (SAML v1.1) ■ Basic/NTLM/FTP/CIFS authentication pass-through ■ Forms-based authentication pass-through;HTTP-POST via variable substitution (macros)
Does the device offer local user database?	Yes, supports complete Authentication and limited Authorization features.
Does the device support virtual keyboard to bypass keystroke loggers?	Yes. ASA provides additional protection against software keystroke loggers by allowing a user to click password characters on the screen instead of entering information through the keyboard.

List the CA servers that are supported by the device for authentication purposes?	Following CA servers are supported: Cisco IOS CS, Baltimore Technologies, Entrust, Microsoft Certificate Services, Netscape CMS, RSA Keon, VeriSign. Finally, the ASA can also act as a certificate authority.
Does the device support authentication based on Machine store certificates?	Machine certificates are supported with AnyConnect client only when making a pre-login (Start Before Logon) connection. However, it is not supported for Clientless connections.
Does the device support multi-factor login option?	Yes. ASA gives administrators the flexibility to support a combined certificate and username/password login for additional security. ASA supports AAA and Certificate authentication simultaneously.
Does the device support RSA softID and secureID cards?	Yes. The ASA supports RSA softID and secureID cards in the “next pin mode” and “new pin mode” in the AnyConnect client. Detailed Answer: The security appliance can use RSA SecureID servers for VPN authentication. These servers are also known as SDI servers. When a user attempts to establish VPN access and the applicable tunnel-group record specifies a SDI authentication server group, the security appliance sends to the SDI server the username and one-time password and grants or denies user access based on the response from the server. The security appliance offers the following SDI version support: ▪ Versions before version 5.0—SDI versions before 5.0 use the concept of an SDI master and an SDI slave server which share a single node secret file (SECURID). ▪ Versions 5.0—SDI version 5.0 uses the concepts of an SDI primary and SDI replica servers. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .sdi appended. A version 5.0 SDI server that you configure on the security appliance can be either the primary or any one of the replicas. SDI version 5.0 uses a two-step process to prevent an intruder from capturing information from an RSA SecurID authentication request and using it to authenticate to another server. The Agent first sends a lock request to the SecurID server before sending the user authentication request. The server locks the username, preventing another (replica) server from accepting it. This means that the same user cannot authenticate to two security appliances using the same authentication servers simultaneously. After a successful username lock, the security appliance sends the passcode. The security appliance obtains the server list when the first user authenticates to the configured server, which can be either

	a primary or a replica. The security appliance then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.
Can I enforce AAA authentication for access to the device?	Yes. Both Local and AAA authentication can be enforced for SSH (CLI) or ASDM access to the device.
List the authorization mechanism supported by the device?	The ASA supports following authorization methods: ▪ Policy mapping from RADIUS and LDAP ▪ Dynamic access policies directly leverage domain membership and posture status for creation of user policy
Does the device support separate authentication and authorization servers for the same session?	Yes, A user can be mapped to a group With RADIUS, LDAP or Certificate based authentication. The group can be configured to contact a separate LDAP or Active Directory server for authorization purposes.
Does the device support ACL lists?	ASA supports network ACL's so that authorization can be overruled with access controls. In addition, the clientless solution supports web-type ACL's to restrict access to various web-pages.
Can I map users by type of access method into various groups?	Yes. You can configure tunnel groups (ASDM Connection profiles) to assign session attributes for users using the same access method.
Can the device create groups dynamically by querying the directory?	Yes. ASA can query Active Directory and derive group information that can be used to enforce access policies.
Does the device support dynamic per user access-list upon successful authentication?	The security appliance supports per user authorization for network access using dynamic ACLs (or ACL names). When the user authenticates, the RADIUS server sends a downloadable ACL to the security appliance. Access to a given service is either permitted or denied by the ACL. The security appliance deletes the ACL when the authentication session expires. Alternatively, the RADIUS server can send a name of an ACL. If an ACL with the name specified exists on the security appliance, access to a given service is either permitted or denied by the ACL. You can specify the same ACL for multiple users.

How does the device apply granular access controls based on users, source ip, authentication and end-point type?	Extensive access control capabilities are available. The ASA Host Scan functions and Dynamic Access Policy functions can provide extensive location checks including IP address and type of host etc. As ASA is also a fully featured firewall product, standard access controls covering address, ports and protocol information. Several of the ASA platforms are also available with modules providing Network Intrusion Prevention and Anti-Virus functions. Detailed web filter for l7 technology Source IP(Location) endpoints are done by DAP.
How does the device identify different trust levels and apply appropriate data protection?	The Host Scan feature checks for registry, process and file entries to identify trust levels (i.e home access or kiosk etc). In addition, the new pre-login policy editor, with its easy to develop graphical flow charts, allows the administrators to define trust levels based on a combination of registry, file, certificate, OS version and IP address range checks. The Cisco Secure Desktop can be customized for various trust levels. For example, Cache cleaner may be mandated for home access while virtual desktop is enforced for Kiosk users. In addition, the end-point information is compared against the configured DAP records to enforce access policies.
What type of accounting information can be captured about a user's usage once logged in?	The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

IPSec Features

Question	Response
Does the device support standards based IKE and IPSec for remote access VPN services?	Yes. ASA delivers the industry leading IPSec VPN solution that is compliant with the following RFC: RFC 2408 (http://tools.ietf.org/html/rfc2408) - Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 (http://tools.ietf.org/html/rfc2409) - The Internet Key Exchange (IKE) RFC 2412 (http://tools.ietf.org/html/rfc2412) - The OAKLEY Key Determination Protocol.
Describe the device support for Diffie-Hellman groups for IKE key exchange purposes?	Diffie-Hellman (DH) groups 1, 2, 5, and 7 (ECDH) are supported, as well as, RSA certificates.
Does the device support Perfect Forward Secrecy (PFS) for IPSec?	Yes. ASA supports PFS using Diffie-Hellman (DH) groups 1,2,5 and 7.

Does the device support any standard X-Auth flavor for authentication?	IKE Extended Authenticate (Xauth) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt ("extended authentication" draft). This protocol provides the capability of authenticating a user within IKE using TACACS+ or RADIUS.
Does the device support NAT-T for IKE/IPSec?	Yes. The IPSec client can attempt to use NAT-T when needed or can also be set up to use TCP.
List the encryption standards that are supported by the device for IPSec Encapsulation using ESP?	The security appliance supports the following encryption standards for ESP: ▪ DES, 3DES, AES-128, AES-192, AES-256 The security appliance supports the following hashing algorithms: ▪ MD5, SHA The security appliance does not support SHA256.
Does the device support IPSec rekey when the SA lifetime expires?	The IKE peers retain the security association until the lifetime expires. The peers negotiate new security associations before current security associations expire.
Does the device preserve TOS bits as per RFC 2401 (http://tools.ietf.org/html/rfc2401)?	Yes. TOS bits in the original IP header are copied to the IP header of the encrypted packet so that QoS policies can be enforced after encryption.
Explain the device support L2TP/IPSec?	ASA delivers support for acting as a L2TP/IPSec VPN headend, terminating VPN connections from native VPN clients included with Microsoft Windows 2000, Windows XP, Windows 2003, and Windows Pocket PC ASA also upports variety of authentication methods including user ID/password, pre-shared keys, certificate, and two-factor authentication. Integrates with a wide range of authentication backends including a local user database, Microsoft Active Directory, Microsoft Windows Domains, Kerberos, LDAP, RSA SecurID, RADIUS, and TACACS+ ASA Provides support for passing a variety of configuration information dynamically to VPN clients as they connect, including DNS and WINS information. Able to assign IP address to VPN clients via local address pool, AAA, DHCP, or DHCP-relay ASA Offers support for optional client-side compression for improved performance in low-bandwidth environments ASA Delivers ability to NAT multiple Microsoft L2TP/IPSec clients

	as their encrypted tunnels pass through a Cisco ASA 5500 Series appliance to one or more VPN headends.
List the PPP authentication types supported?	The security appliance supports the following PPP auth types for L2TP/IPSec: ▪ PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-PROXY The following PPP authentication types are supported with AAA: ▪ RADIUS -> All the above PPP ▪ LOCAL -> PAP, MSCHAPv1, MSCHAPv2, ▪ LDAP -> PAP only ▪ NT -> PAP only ▪ Kerberos -> PAP only ▪ SDI -> PAP only ▪ TACACS+ -> PAP, CHAP, MSCHAPv1

VPN Client (IPSec and AnyConnect) Features

Question	Response
Does the device provide Full Tunnel (or LAN-like) access for remote users?	Yes. IPSec VPN client and SSL based AnyConnect client support full-tunnel access.
List the platform/OS support for your IPSec client?	▪ Windows 2000, XP x86 and 64-bit ▪ Windows Vista x86 ▪ Mac OS X Power PC and Intel 10.4 and 10.5 ▪ Linux Intel (2.6.x kernel)
List the IPSec client support on PDAs and smartphones?	Latest list can be found here (http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp75627) ▪ For Windows Mobile, the following third-party vendors offer a VPN client that works with the ASA: Antha, Apani, Bluefire, Microsoft, and NCP.DE. Cisco supports the Microsoft client; the respective vendors support the other clients. ▪ Bluefire offers a version of the Palm Treo that has an IPSec client that works with the ASA. ▪ Nokia provides support for Symbian on the Nokia 92xx Communicator series, Nokia 6600 and Nokia E61

Does your device inter-operate with native L2TP/IPSec client on PDAs and Smartphones?	Latest status can be found here (http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp90223) The following mobile OS's support a built-in L2TP-over-IPSec client that Cisco has tested successfully with the ASA: ▪ Microsoft Windows Mobile 2003 for Pocket PC PDA ▪ Microsoft Windows Mobile 5.0 PDA and PDA Phones. ▪ Apple iPhone Windows mobile based handheld devices support MS-CHAP v1 and v2, and pre-shared keys. Some Windows Mobile 2003 (HP iPAQ h4150) and 5.0 (HP iPAQ hx 2495b) PDAs support enrollment with an available certificate authority server and can use certificate-based authentication. The iPhone supports MS-CHAP v2 (preferred) for PPP. It has also been tested for MS-CHAP v1 and PAP support for PPP authentication. The iPhone supports pre-shared keys but no certificates.
Do you have the SecurID software based token integrated in your client? What types of authentications are integrated into the connection process?	Yes, You can configure the Cisco VPN Client to handle RADIUS SDI authentication the same way it handles "native" SDI authentication, which is more seamless and easier to use. With this configuration, users do not have to deal with the RSA SecurID software interface; the Cisco VPN Client software directly interfaces with the RSA SecureID software for the user.
Does the client have a tunnel connection created before logging onto the local machine?	Yes. ASA Start Before Logon (SBL) feature allows a full network logon from GINA (Windows 2000) and allow Active Directory group policies to be applied. Supported with both IPSec and SSL based clients.
Does the device support split tunneling to enable services that do not use VPN (e.g. home printing)?	Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling. Both IPSec and AnyConnect clients support split tunneling as a configurable option. ▪ To create a network list for split tunneling, use the split-tunnel-network-list command in group-policy configuration mode. ▪ To delete a network list, use the no form of this command. ▪ To delete all split tunneling network lists, use the no split-tunnel-network-list command without arguments. This deletes all configured network lists, including a null list created by issuing the split-tunnel-network-list none command.

What are the options available for assigning addresses to various remote clients?	The ASA supports setting client IP addresses via internal pool, internal DHCP server, and external DHCP server for both the IPSec and SSL based clients.
Does the gateway support all DHCP options as well as DNS push?	The internal DHCP server in ASA provides supports DHCP Options 2 through 254. Additionally, the following fields can be configured: Domain name, DNS Server 1, DNS Server 2, Primary WINS Server, Secondary WINS Server, Lease period, Ping timeout. Auto-configuration can also be enabled, which allows the ASA to learn certain fields from another DHCP server, including DNS Server settings, WINS Servers, and Domain name.
Does the gateway release DHCP lease for both graceful and ungraceful disconnections?	The internal DHCP server within the Cisco ASA appliance immediately releases DHCP leases when a VPN client session is terminated, whether graceful or ungraceful.
Does the device support mapping users to a specific VLAN?	Yes. ASA has the ability to map users to a specific VLAN based on user/end-point/group-policy. This functionality is available in both Client and Clientless mode.
If a VPN Gateway is unavailable, does the client automatically attempt to connect to the remaining gateways?	Yes. The VPN client profile can be configured to provide a list of VPN gateways. This is desirable when a global VPN network is deployed. While clustering provides high availability and scalability at a single site, the client dialer profiles provide global high availability. If an entire VPN cluster is unavailable for any reason, then the end user's VPN software automatically attempts to connect to the next cluster in the list, and continues rolling to the next listing until a successful connection is established.
Explain the troubleshooting options available for the client?	On windows based systems the SSL client logs are written in the event manager of the system. The IPsec client has its own log viewer which is different than the system event manager. Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. During a session, you can view the log from the Log tab and the Log Window. You can also view a saved log file with a text editor.
Does the client provide detailed error and events messages for the connection and	When you start the VPN Client and enable logging, the VPN Client creates a new, empty log file for your session. The log collects event messages from all processes that contribute to the client-peer connection. Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. During a session, you can

disconnection process?	view the log from the Log tab and the Log Window. You can also view a saved log file with a text editor. This section shows how to use the log to retrieve and manage this information.
Does your client use Virtual Adapters? If so, explain how they work on different OS?	The Cisco VPN client uses a virtual adapter for Windows 2000 and Windows XP. The Virtual Adapter installs at NIC level in the kernel. A route is inserted into the routing table of the host OS and VPN traffic is routed through the Virtual Adapter. The Virtual Adapter then routes the encrypted traffic out of the Local LAN adapter. The Virtual Adapter is used for both the IPSec and SSL VPN Client.

SSL Client (AnyConnect) specific Features

Question	Response
List the platform/OS support for your SSL client?	AnyConnect VPN client, with broader operating system support for Microsoft Windows 2000, XP, Vista (32 bit and the first to offer 64 bit), MAC OS X, and Linux supports enterprises with diverse client infrastructure.
Does the client require administrative privileges to install and update?	Yes, For the first AnyConnect client installation, administrative privileges are required. However, the subsequent upgrades don't require administrative privileges. The AnyConnect client is dynamically downloadable, thereby eliminating administration associated with VPN client software updates. The client can be installed either using a Pre-deployment MSI (Windows Installer) or it can be deployed automatically from the headend via ActiveX (Windows IE) and Java.
What is the size of the AnyConnect client?	With WebLaunch, we deliver a self-extracting binary, 'anyconnect-win-2.1.xxx.web-deploy-k9.exe', that contains the MSI used to install AnyConnect, and this is approximately 1.2 Mb. The uncompressed .MSI installer for Windows is around 1.4Mb and the package (.pkg) is ~1.9Mb.
Describe the acceleration and compression capabilities of the SSL Client?	AnyConnect uses Datagram Transport Layer Security (DTLS) or TLS. DTLS with SSL connections avoids latency and bandwidth problems associated with some SSL-only connections and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. For detailed information about DTLS, see RFC 4347 (http://tools.ietf.org/html/rfc4347) by accessing the following hyperlink: http://www.ietf.org/rfc/rfc4347.txt. The AnyConnect client will auto detect whether it can use DTLS or TLS.
	ASA adapts the tunneling protocol automatically to the most efficient

Describe the client's capabilities to provide optimized network access to remote users?	method possible based on network constraints. ASA provides a DTLS connection for latency-sensitive traffic, such as VoIP traffic or mission critical TCP-based application access. In addition, ASA compresses data to reduce the amount of data to transmit.
Does the client support SSL session persistence when the end-point IP address changes?	Yes. If the IP address changes due to change of network provides, the SSL session will not drop for client and clientless access.
Does the device support multiple clients originating from the same source IP? (remote conference, multiple home users)	Yes. Multiple clients on single IP address are supported. Each SSL session from an IP address will appear as a separate session.

SSL Clientless Features

Question	Response
List the browsers supported by your clientless solution?	Multiple browser support, including Internet Explorer, Firefox and Netscape on Windows 2000/XP/Vista, Opera and Safari on MAC OS X, Mozilla on Linux and Pocket Internet Explorer (PIE) on Pocket PC 2003 and Windows Mobile 2005 helps ensure broad connection compatibility from any location. The latest browser support can be found here (http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp80544).
List the microbrowsers (those used for PDAs and Smartphones) supported by your clientless solution?	Clientless SSL VPN can be accessed from Pocket PC or other certified personal digital assistant (PDA). Neither the ASA administrator nor the Clientless SSL VPN user need do anything special to use Clientless SSL VPN with a certified mobile device. Cisco certified mobile devices can be found here (http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html#wp75636).
Which applications are supported by your clientless SSL solution?	▪ Internal websites (both http and https). ▪ Web-enabled applications ▪ NT/Active Directory and CIFS file shares access through an easy-to-use web interface. ▪ E-mail proxies, including POP3S, IMAP4S, and SMTPS ▪ MS Outlook Web Access, Lotus iNotes ▪ Application Access (that is, port forwarding for access to other TCP-based applications) ▪ Microsoft sharepoint services.

	In addition, Plug-ins provide access to common client/server applications without the need for pre-deployed remote clients, granting rapid access to Telnet, SSH, Remote Desktop Protocol (RDP), Citrix Application Access and Virtual Network Computing (VNC) resources.
Does the device host and deliver third party and custom-built Java applets without the need for a separate internal hosting server?	Yes, Cisco ASA hosts JAVA applets for applications such as Citrix, RDP, VNC, Telnet, SSH, etc thus eliminating the need to pre-deploy remote clients.
List your device support for Common Thick client applications in a clientless environment?	Port forwarding enables clientless access to popular thick client applications like Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), e-mail, online calendars, instant messaging, Telnet, SSH, and other client-initiated TCP applications via a small Java applet. Smart tunneling allows Microsoft Windows users access to TCP applications without the prerequisite of administrative rights and allows VPN administrators to grant only approved applications access to internal resources.
Describe the device content transformation capabilities?	ASA's advanced transformation capability helps ensure compatibility with Web pages containing complex content, including HTML, Java, ActiveX, JavaScript, and Flash. In addition, ASA provides filtering of ActiveX and Java applets to prevent downloads of malware. Some web applications may have issues if they are not developed according to standards. Clientless SSL VPN includes an Application Profile Customization Framework option that lets the security appliance handle non-standard applications and web resources so they display correctly over a Clientless SSL VPN connection. Typically, Cisco TAC helps you write and apply an APCF.
Describe the device support for Microsoft SharePoint?	ASA fully supports editing Office documents off Sharepoint 2.0 and 3.0 in a pure clientless mode.
Describe the solutions support for Citrix Access?	The ASA doesn't require any extraneous helper applications to enable Citrix access over clientless SSL VPN. This capability ensures fast application initiation time and reduces the risk of desktop software conflicts.
Can the device replace the Citrix	Yes, the solution is able to work as the encryption device for unencrypted Citrix ICA sessions. The solution can replace the secure gateway but not the web

secure ICA solution?	interface.
Does the device support multiple hostnames for the same Security appliance?	Yes. The group-url feature allows the administrator to provide multiple hostnames for the same appliance in two different formats 1. https://marketing.CompanyA.com, https://sales.CompanyA.com or 2. https://CompanyA.com/marketing, https://CompanyA.com/sales
How does the device provide customizable user experience?	The ASA allows customization of the Web portal, to change the appearance of the windows that the user sees upon login. With this ability, the administrator can change the user homepages, modify URLs and specify available applications. The ASA also has the ability to have per-user Web portals. The portals are localizable and can have RSS feeds and personal bookmarks. Additionally, other parameters, such as the user's deny message and filters, are configurable.
Does the device support multiple customizable sign-in pages?	Yes, The login page is "fully customizable" which means we can build any html page as we see fit and place the ASA login/password dialog box at the desired location. This "full customization" capability allows the administrator to build sign-in pages which have a look-n-feel similar to customer's existing intranet pages thus providing consistent user experience while browsing ASA pages.
Does the device allow the end-users to add their own bookmarks?	Yes. The end-user can configure their own bookmarks for html links and other applications.
Does your device provide integrated Client and Clientless access?	Yes. The clientless web portal includes a tab for activating the full tunnel AnyConnect client. The end-user might first want to use the Clientless session to access frequently used bookmarks, but may occasionally decide to switch to AnyConnect Client for full tunnel access.
Provide a high level flow of your authentication process for clientless users?	1.The end user initiates the SSL VPN connection to the Web portal. This can be a DNS name or IP address. Depending on the method being used to log into the gateway, the user will have to enter the username and password. 2.The context which user is attempting to connect is identified by the URL or login information. Now the user must be authenticated under the context they belong to. 3.The secure gateway must determine if it will let this user into the Web portal, so it will send the username and password to the AAA server. The method of AAA does not matter, just so authentication can be done. 4.The AAA server authenticates the user and it will indicate this to the context. It may also push down any RADIUS attributes for that user. The Web portal will build a user session under the context, and apply the policy group information and RADIUS attributes.

	5.Now that the user session is established to the Web portal, the backend interfaces handle the access to the inside network. Once a user is authenticated under a given context, the user session is established. This user session will embody the parameters specified globally in the context, the group policy, and any RADIUS attributes pushed down during authentication for that user.

Secure Desktop Features

Question	Response
How does the device erase traces of a connection on an un-trusted end-point?	Cisco Secure Desktop provides a consistent and reliable means of eliminating all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. This ensures that cookies, browser history, temporary files, and downloaded content do not remain on a system after a remote user logs out or an SSL VPN session times out. CSD increases protection against data theft and client system malware (malicious software) by encrypting all data and files associated with or downloaded during the SSL VPN session. CSD encrypts all information in the session. This protection is valuable in case of an abrupt session termination, or if a session times out due to inactivity. Furthermore, CSD stores all session information in the secure vault desktop partition; when the session closes, CSD overwrites and removes all data using a U.S. Department of Defense (DoD) sanitation algorithm to provide endpoint security protection, a feature known as “cache cleaner”.
Does the device detect KeyLogger applications and prevent user access?	Yes. Keystroke logger detector runs once at start up of Cisco Secure Desktop and includes multiple inspections. If any suspicious software is detected, depending on the administrator specified policy, the user is presented with the binary name of the suspected module (exe, dll or sys). In this case, the user is given the choice to either accept the module in question as acceptable, or reject it as malicious, in which case CSD terminates its connection process immediately. Administrators can configure two modes of detection, “Forced Admin Control” or “User Based Control”. Forced admin control enables the administrator to specify a list of acceptable or safe modules. As a result, if these modules are detected, users will be allowed access. On the other hand, for any modules detected that are not on the trusted list, CSD terminates its connection process immediately. User-based control simply means disabling “forced admin control”. Thus, the user must decide whether a module is safe or not. In this case, the user must acknowledge which modules are safe by placing a check mark next to each module detected. Users will not be permitted to proceed with their login process until all modules are acknowledged with a check mark. For repeated login attempts, users can enable Cisco Secure Desktop to remember these acknowledgements for ease of use.
Does the device support deploying an Encrypted Sandbox and virtual	Yes. However, the secure vault function of the Cisco Secure Desktop is supported on Windows platform only. In addition, administrators have the flexibility to disable this feature.

desktop?	

Endpoint Assessment

Question	Response
Describe your device end-point verification and authorization/role assignment capabilities?	Dynamic access policies (DAP) on the Cisco ASA let you configure authorization tha many variables that can affect each VPN connection. You create a dynamic access po a collection of access control attributes that you associate with a specific user tunnel c These attributes address issues of multiple group membership and endpoint security. security appliance grants access to a particular user for a particular session based on t define. It generates a DAP at the time the user connects by selecting and/or aggregati from one or more DAP records. It selects these DAP records based on the endpoint se information of the remote device and the AAA authorization information for the auth It then applies the DAP record to the user tunnel or session. If the remote computer passes a pre login assessment associated with a particular end configured on the security appliance, a scan of the antivirus, anti spyware, personal fi other optional keylogger, file, registry, and process checks occurs. An advanced endp assessment option is available to automate the process of repairing out-of-compliance This scan can be turned on or off by the system administrator. Secure Session or Cach installs only if the pre login assessment associated with a particular endpoint profile p if the Secure Desktop or Cache Cleaner parameters are enabled for the matched endpo
Please list the end-point attributes that are checked by the device before allowing access to VPN?	The ASA works with a large number of other vendors' security products to strengther of the entire VPN session. These include checks for personal firewall, anti-virus, and products. These are used with the Dynamic Access Policy to determine the level of us authorization. For more details about the endpoint attributes that are checked, please a following hyperlink: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_dap.htr
Does the device quarantine and	ASA can restrict access to non compliant devices. In addition, the Advanced Endpoin license will allow the administrator to configure rules that will be enforced on the end for remediation purposes. These rules include: ▪ AntiVirus: Brand and version, Force File System Protection (if the AV program action), Force Virus Definitions Update - if not updated in last x days (if the A supports this action). ▪ Personal Firewall: Brand and version, Firewall Action (None, Enable or Disabl firewall supports that action), Rules - Allow or disallow applications or ports. (program supports this action). ▪ Anti-spyware: Brand and version, Force Spyware Definitions Update - if not up days. (If the AS program supports this action). In addition, sophisticated role-based posture checks with quarantine and remediation be provided using the Cisco NAC Appliance in conjunctions with the ASA.

remediate non-compliant end devices?	Comprehensive Security Policy Compliance with NAC NAC is an industry-wide coll effort led by Cisco Systems, established to help ensure that every endpoint complies v security policies before being granted access. ASA is NAC-enabled for IPSec remote- scenarios. NAC reduces the risk associated with extending network resources in remo scenarios by preventing vulnerable hosts from obtaining and retaining normal networ Cisco AYT feature enforces firewall policies for users connecting using the Cisco IPS Client. Administrators can configure the VPN to refuse endpoints that are in violation designated firewall policy. The Cisco IPSec VPN Client polls the firewall every 30 se sure it is still running. AYT checks for the Cisco Security Agent, Cisco Integrated Cli Network ICE BlackICE Defender, Sygate Personal Firewall, Sygate Personal Firewal Security Agent, Zone Labs ZoneAlarm, and Zone Labs ZoneAlarm Pro. A basic NAC consists of three components: a Network Access Device (NAD), an authentication, au and accounting (AAA) server, and a posture agent running on a NAC-compliant host. often Cisco routers or Cisco switches, the AAA server is the Cisco Secure Access Co (ACS), and the posture agent is the Cisco Trust Agent (CTA). An expanded NAC env additional NAC-enabled applications running on the host.

Scalability and Performance

Question	Response
What scalability tests have been performed and what are the results?	The Cisco ASA 5500 Series delivers site-specific scalability for small offices through ent through its five models: the 5505, 5510, 5520, 5540, and 5550. The Cisco ASA 5550 Cisc concurrent SSL VPN users and the Cisco ASA 5540 Series can scale to 2500 concurrent S scalability can be found by accessing the following hyperlink: http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html.
Please describe device performance capabilities?	There are currently five different size Adaptive Security Appliances. These are the ASAS ASA5540 and ASA5550: ▪ The ASA5505 handles 100 Mbps VPN traffic with 25 concurrent users. These user or IPsec. ▪ The ASA5510 handles 170 Mbps VPN traffic with 250 concurrent users. These use or IPsec. ▪ The ASA5520 handles 225 Mbps VPN traffic with 750 concurrent users. These use or IPsec. ▪ The ASA5540 handles 325 Mbps VPN traffic with up to 2500 concurrent SSL user Both IPsec and SSL VPN can be used simultaneously and the user limit will be bet ▪ The ASA5550 handles 425 Mbps VPN traffic with 5000 concurrent users. These us Up to ten devices can be clustered using built-in functionality for additional scalability.
How does the published	At larger packet sizes, the Cisco ASA 5500-series appliances provide the greatest through packet sizes, they are able to handle a greater number of packets per second. Cisco ASA-5

performance data change for carrying small size packets (64bytes)?	80Mbps VPN throughput using 64-byte packets. With 300-byte packets, VPN throughput With 1400-byte packets, it increases to 400 Mbps. The Cisco ASA-5550 can handle 156,(64-byte packets. This is a much greater number of packets per second than at larger packe great degree of Quality of Service when using applications that are sensitive to latency, su conferencing. All Cisco ASA-5500 series appliances support low-latency queuing (LLQ) support of multimedia appliances, such as IP telephony.
List the device performance in terms of new VPN connections per second?	The security appliances support 6,000, 9,000 or 20,000 new sessions per second dependin 5540 models respectively).
What is the latency added by the device in the worst-case scenario of load and feature activation?	IPsec, and SSL encryption and decryption are processed by dedicated processors within tl appliances, which allows for negligible added latency by the ASA appliance. Overall add determined by the client computer, and depends on many factors, such as CPU speed, ava connectivity method and speed.
How does the device provide sustained VPN connection for low-bandwidth connections?	The security appliance is not limited by low-bandwidth connections. In fact, it offers com scenario. Compression can reduce the size of the transferring packets and increase the cor especially for connections with bandwidth limitations, such as with dialup modems and h remote access. Compression is enabled by default, for both WebVPN and SSL Client bas disable compression for all WebVPN or AnyConnect connections or on a per group or us
Please list any third party testing results of throughput and performance?	Cisco Systems engaged Miercom to independently test the Cisco ASA 5520 Adaptive Sec other comparable, competitive Unified Threat Management (UTM) security appliances – Pro, the Fortinet® FortiGate 1000, and Juniper Networks® NetScreen-208. Performance unified firewall and IPS throughput performance, VPN throughput performance, IPS thre connections-per-second performance. The white paper can be found here (http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white

High Availability and Load Balancing

Question	Response

Describe your device stateful failover capabilities?	ASA has stateful failover for stateful firewall, IPsec and SSL VPN. However, VPN is supported in Active/Standby mode only. Appliances in an Active/Standby mode must have identical software, hardware and licenses.
Describe the load balancing requirements of the devices, including requirements for a third-party availability tools like load balancers?	There are multiple ways to achieve high availability with the ASA solution: Clustering with onboard load balancing; traditional external network load balancing devices with multiple ASA's; and multi-side redundancy with DNS/WAN load balancing. Clustering with On-Board Load Balancing: The Cisco ASA has the built in ability to load balance without requiring external load balancing devices. This is accomplished with Virtual Clustering. For example, when a new connection request comes in, the master ASA will decide the best path of the request. The master can either pass that request to the ASA with the least amount of traffic or terminate the request itself. If the ASA should fail then one of the additional ASAs in the cluster will take over the role as master. This is a key feature that allows the ASA to scale for future deployments. Multiple ASA's with external network Load Balancing: Second, in a network design with a load balancer, The ASA can sit behind a hardware load balancer. When using the ASA in a SSL VPN environment, the ASA looks and acts like a web server (from the hardware based load balancer perspective). Multi-Site DNS/WAN Load Balancing: Finally multi-site redundancy is accomplished by using DNS load balancing. This could be done with just standard DNS round robin or it could be done with advanced DNS services with the Cisco Global Site Selector appliance.
Does your device support clustering?	Yes. All ASA appliances support IPsec and SSL VPN clustering, which provides both scalability and high-availability. As needs increase for numbers of concurrent users at a location, additional ASAs can be installed and added to a cluster to incrementally increase the numbers of users that location can support. Appliances in a cluster do not need to be identical. When clustering with the ASA, VPN traffic will connect to the device that was elected as the Master. VPN traffic received at the master will either be handled by the Master or passed to one of the other ASAs in the cluster. In the unlikely event of a failure, user traffic can be reconnected to another device in the cluster.
Does your device support	Yes. The Cisco ASA has the built in ability to load balance without requiring external load balancing devices. This is accomplished with Virtual Clustering. For example, when a new connection request comes in,

load balancing without adding external load-balancers?	the master ASA will decide the best path of the request. The master can either pass that request to the ASA with the least amount of traffic or terminate the request itself. If the ASA should fail then one of the additional ASAs in the cluster will take over the role as master. This is a key feature that allows the ASA to scale for future deployments.
How does the device support cross-site clustering?	Cross site clustering can be achieved by using the fully qualified domain name (FQDN) and a global load balancing solution.
Does the device support all types of connection protocols in a load balancing configuration?	Yes. Load distribution, as provided by clustering, is transparent to all user traffic. It is supported by both IPsec and SSL connections.
In a fully loaded condition, does the VPN Gateway accept new connections?	No. When ASA is fully loaded, no new connections are permitted. Fully loaded is defined by number of concurrent connections. The ASA reports following syslog message when the device licenses are exhausted. Client: %ASA-4-716023: Group <DfltGrpPolicy> User <user1> IP <x.x.x.x> Session could not be established: session limit of xxx is reached. Clientless: %ASA-4-716007: Group <DfltGrpPolicy> User <user1> IP <x.x.x.x> WebVPN Unable to create session.
Does the device support redundant ISP?	Yes. ASA appliances automatically failover to a standby ISP link when the primary ISP link fails. ASA utilizes static routing and object tracking to determine the availability of the primary route and to activate the secondary route incase of primary route failure.

Standards and Certification

Question	Response
List the device certifications?	FIPS 140-2 Level 2 compliant Cisco has an ongoing certification program for FIPS and CC EAL4 on a wide product range. The latest status of the certification, incl. a copy of the granted certificate is available on http://www.cisco.com/go/securitycert
	The security appliance supports the following RFCs (not an exhaustive list) and is interoperable with equipment that also supports these RFCs: RFC 959 (http://tools.ietf.org/html/rfc959) - FILE TRANSFER PROTOCOL (FTP) RFC 1321 (http://tools.ietf.org/html/rfc1321) - The MD5 Message-Digest Algorithm RFC 1350 (http://tools.ietf.org/html/rfc1350) - THE TFTP PROTOCOL (REVISION 2) RFC 1945 (http://tools.ietf.org/html/rfc1945) - Hypertext Transfer Protocol --

List the relevant RFC supported by the device?	HTTP/1.0 RFC 2058 (http://tools.ietf.org/html/rfc2058) - Remote Authentication Dial In User Service (RADIUS) RFC 2059 (http://tools.ietf.org/html/rfc2059) - RADIUS Accounting RFC 2085 (http://tools.ietf.org/html/rfc2085) - HMAC-MD5 IP Authentication with Replay Prevention RFC 2104 (http://tools.ietf.org/html/rfc2104) - HMAC: Keyed-Hashing for Message Authentication RFC 2246 (http://tools.ietf.org/html/rfc2246) - The TLS Protocol RFC 2403 (http://tools.ietf.org/html/rfc2403) - The Use of HMAC-MD5-96 within ESP and AH (Exception: ASA does not support AH) RFC 2404 (http://tools.ietf.org/html/rfc2404) - The Use of HMAC-SHA1-96 within ESP and AH (Exception: ASA does not support AH) RFC 2406 (http://tools.ietf.org/html/rfc2406) - IP Encapsulating Security Payload (ESP) RFC 2407 (http://tools.ietf.org/html/rfc2407) - The Internet IP Security Domain of Interpretation for ISAKMP RFC 2408 (http://tools.ietf.org/html/rfc2408) - Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 (http://tools.ietf.org/html/rfc2409) - The Internet Key Exchange (IKE) RFC 2412 (http://tools.ietf.org/html/rfc2412) - The OAKLEY Key Determination Protocol RFC 2451 (http://tools.ietf.org/html/rfc2451) - The ESP CBC-Mode Cipher Algorithms RFC 2616 (http://tools.ietf.org/html/rfc2616) - Hypertext Transfer Protocol, HTTP/1.1 RFC 2818 (http://tools.ietf.org/html/rfc2818) - HTTP Over TLS RFC 2865 (http://tools.ietf.org/html/rfc2865) - Remote Authentication Dial In User Service (RADIUS) RFC 3377 (http://tools.ietf.org/html/rfc3377) - Lightweight Directory Access Protocol (v3) RFC 4347 (http://tools.ietf.org/html/rfc4347) - Datagram Transport Layer Security (DTLS)
How is key management performed for SSL connections?	Session keys for the SSL connections are generated in accordance with the SSL, TLS, and DTLS standards. These keys are stored in cleartext data structures in system memory and are transmitted via internal system interfaces to the hardware crypto accelerator for use. The session keys are not accessible via external user interfaces. All session keys are zeroized when the associated connections are dropped.
How are the SSL session keys protected from unauthorized	There are no mechanisms in place in the ASA for anyone to display, modify, or otherwise access SSL session keys. SSL session keys can only be destroyed when an associated connection is deleted. Deletion of an SSL connection can occur when the end user terminates the connection or when an authorized administrator drops the connection at the ASA. Only an authorized

disclosure, alteration, and destruction?	administrator of the ASA has permission to terminate SSL connections and, thereby, destroy SSL session keys.

Management Features

Question	Response
What are the options available to manage the device?	The Command Line Interface for the ASA can be accessed by SSH. Cisco ASA can be managed as a single device using Cisco Adaptive Security Device M (ASDM) which comes embedded with the ASA. It uses an intuitive, easy-to-use Web-b management interface. The Cisco Adaptive Security Device Manager accelerates securi appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services. Its secure, Web-based design enables anytime, anywhere access. The ASA can also be managed through enterprise-class, multi device management of C Security Manager. Access rights can be defined for multiple administrators, with approp controls. The CS-M also has workflow capabilities. ▪ Current CSM software supports features that are included in ASA v7.2. The supp the new features introduced in ASA v8.0 will be available in a future CSM releas
List the OS support for your management application?	The ASDM runs as a java applet or it can be installed on the administrators PC. ASDM runs on the following platforms: ▪ Windows 2000 ▪ Windows XP ▪ Windows 2003 Server with Internet Explorer or Firefox. ▪ Linux Red Hat Desktop, Red Hat Enterprise Linux with Firefox ▪ Solaris 8 or Solaris 9 with Mozilla Suite 1.7 When the ASA is upgraded with ASDM, all installed clients will be prompted with an u
Does the management solution include any Startup Wizards or Task guides to allow easy configuration?	The ASDM includes following wizards to enable easy configuration: ▪ Start up Wizard ▪ IPSec VPN Wizard ▪ SSL VPN Wizard (Both Client and Clientless VPN) ▪ High Availability and Load-Balancing wizard In addition, ASDM Demo mode enables the administrator to familiarize with the config screens even without access to or affecting a real device. Administrators can also create object groups that contain TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) objects for simplified policy management

How does your management solution support role-based administration?	There are five built in user roles in the Cisco Security Manager. These include Help Des Network Operator, Approver, Network Administrator, and System Administrator. Optic CS-M can be integrated with Cisco Secure Access Control Server for additional flexibil control over user roles. This integration would allow administrators to lock users out of specific devices, policies and rules while giving them access to others.
Describe the reporting available for Clientless SSL VPN sessions?	For Clientless SSL VPN the following session information is available in ASDM: ■ Username/IP Address —shows the username or login name for the session and th address of the client. ■ Protocol/Encryption —shows the protocol and the data encryption algorithm this is using, if any. ■ Login Time/Duration —Shows the date and time (MMM DD HH:MM:SS) that th session logged in. and the length of the session. Time is displayed in 24-hour nota ■ Client Type/Version —shows the type and software version number (for example 7.0_int 50) for connected clients, sorted by username. ■ Bytes Tx/Bytes Rx —shows the total number of bytes transmitted to/received fro remote peer or client by the security appliance.
Describe the reporting capability for load balancing?	ASDM for servers in a VPN load-balancing cluster displays the following information: ■ Public IP Address — displays the externally visible IP address for the server. ■ Role — indicates whether this server is a master or backup device in the cluster. ■ Priority — shows the priority assigned to this server in the cluster. The priority m an integer in the range of 1 (lowest) to 10 (highest). The priority is used in the ma election process as one way to determine which of the devices in a VPN load-bala cluster becomes the master or primary device for the cluster. ■ Model — Indicates the security appliance model name and number for this server ■ Load % — Indicates what percentage of a server's total capacity is in use, based u the capacity of that server. ■ Sessions — shows the number of currently active sessions.
Please describe the audit and logging system? Where is the log data stored?	Cisco ASA 5500 Series Security Appliances utilize 64MB of non-volatile solid state fla memory for reliable storage of software images and device configuration. When the log is full, the security appliance deletes the oldest system log message to make room in the for new system log messages. ASDM supports real-time device monitoring utilizing bot SNMP and syslog data. Additionally, ASDM incorporates an innovative packet capture capable of recording traffic in a standard format for offline analysis. The Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) recognizes and correlates real network attacks and then defines how to stop them resulti reduced false positives and simplified audit compliance.
	The logging configuration is very flexible and enables you to customize many aspects o the security appliance handles system log messages. Using the logging feature, you can following:

List the configuration options available to customize the device support for log messages?	▪ Specify which system log messages should be logged. ▪ Disable or change the severity level of a system log message. ▪ Specify one or more locations where system log messages should be sent, includi console, an internal buffer, one or more syslog servers, the ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions. ▪ Configure and manage system log messages in groups, such as by severity level o of message. ▪ Specify what happens to the contents of the internal buffer when the buffer becon and wraps around: you can configure the security appliance to send the buffer cor to an FTP server or to save the contents to internal Flash memory. ▪ Send log files to an FTP server. ▪ Save log files in internal Flash memory. You can choose to send all system log messages, or subsets of system log messages, to all output locations. You can filter which system log messages are sent to which locatio the severity of the system log message, the class of the system log message, or by creati custom log message list.
What are the real time monitoring and alerts available with the device? Does the device support SNMP? Please list the MIBs that are supported by the device?	The adaptive security appliance provides support for network monitoring using SNMP V V2c. The adaptive security appliance supports traps and SNMP read access, but does nc support SNMP write access. ASA provides services such as 64-bit counters (for monito Gigabit Ethernet interfaces) and support for bulk MIB data transfers You can configure the adaptive security appliance to send traps (event notifications) to a NMS, or you can use the NMS to browse the MIBs on the adaptive security appliance. M are a collection of definitions, and the adaptive security appliance maintains a database values for each definition. Browsing a MIB entails issuing an SNMP get request from th NMS. Use CiscoWorks for Windows or any other SNMP V1, MIB-II-compliant browse receive SNMP traps and browse a MIB. ASA provides complete visibility into VPN connections with detailed per-tunnel statisti including tunnel uptime, bytes and packets transferred, and more, through support for th Cisco IPSec Flow Monitoring MIB. ASA has support for many SNMP MIBs, including the SNMPv2 MIB (RFC 1907 (http://tools.ietf.org/html/rfc1907)), the Interfaces Group MIB (RFCs 1573 and 2233), t MIB (RFC 2011 (http://tools.ietf.org/html/rfc2011)), and the Entity MIB (RFC 2737 (http://tools.ietf.org/html/rfc2737)). The following table has the complete list of the supported MIBs and traps for the adapti security appliance and, in multiple mode, for each context. Cisco MIBs can be downloa accessing the following hyperlink: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. After downloading the MIBs, compile them for your
	The Cisco Adaptive Security Appliance provides in depth debugging functionality. This debugging functionality includes the ability to debug external servers, debug VPN sessi debug SSL VPN sessions, and debug IPSec. For a complete list of supported debugging commands, please see:

Describe the device support for session debugging?	http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_1/cmd_ref/a1_7 The ASA offers the innovative Packet Tracer feature, heralding in a new generation of troubleshooting capabilities that give administrators a step-by-step analysis of how pack processed within a Cisco ASA 5500 Series appliance. Administrator can learn the details of the affects of NAT, PAT, ACLs, inspection engin VPN, IPS, Anti-X, and QoS services on either captured traffic (using the built-in packet capture feature) or a hypothetical packet proposed by them.
Can we rollback the device to last known working configuration?	Yes. It is recommended to save the configuration periodically either through CLI or usi ASDM. If required, we can reload a previous configuration to the ASA. The configurati could be downloaded from a tftp server or it can be uploaded using the ASDM. In addit can optionally reload XML files for configuring Cisco Secure Desktop policy decision t Dynamic Access Policies and portal customizations.

Miscellaneous

Question	Response
How is the integrity and confidentiality of the passwords and access policies secured in the device?	The ASA encrypts sensitive data such as keys and passwords, storing them securely in the startup-config file, using AES.
List the routing protocols supported by the gateway?	ASA supports the following routing protocols: RIP v1 and v2, OSPF, Reverse Route Injection.
Describe the gateway support for IPV6?	The Cisco ASA 5500-series appliances support IPv6 addressing. In addition, the ASA appliances support dual IP stacks. It is possible to use both IPv4 and IPv6 addresses at the same time on the same interfaces. ASA also supports translation of IPV4 on one side to IPV6 on he other side. ASA provides access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4 and IPv6 network environments through dual-stack support. ASA also delivers IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP. In addition, ASA supports SSHv2, Telnet, HTTP and HTTPS, and ICMP-based management over IPv6.
List the device support for	Cisco may provide localized versions of the user interface which vary per release. In addition, customers have the option to localize the interface(s) in to a language of their choice.

Localization and Internationalization?	For a list of currently available translations, please see: http://www.cisco.com/cgi-bin/tablebuild.pl/asa Names begin with: translation-kit.

Categories: RFP | Competitive