New Features for ASA Version 9.0(2)

FIREWALL Features

Cisco® Adaptive Security Appliance (ASA) Software Release 9.0 is the latest release of the software that powers the Cisco ASA family. The same core ASA code delivers enterprise-class security capabilities for ASA devices in a variety of form factors, including a wide range of standalone appliances, hardware blades that integrate with the organization's existing network infrastructure and software that can secure and protect public and private clouds.

Cisco TrustSec integration - The ASA integrates with Cisco TrustSec to provide security group based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses.

Cisco Cloud Web Security (ScanSafe) - Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. Integration with Cisco Cloud Web Security (formerly ScanSafe), which allows enterprises to enforce granular web access and web application policy while providing protection from viruses and malware.

Extended ACL and object enhancement to filter ICMP traffic by ICMP code - ICMP traffic can now be permitted/denied based on ICMP code.

Unified communications support on the ASASM - The ASASM now supports all Unified Communications features.

Per-session PAT - The per-session PAT feature improves the scalability of PAT and, for ASA clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For "hit-and-run" traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address.

SunRPC change from dynamic ACL to pin-hole mechanism - When you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic.

Inspection reset action change - When you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions: The ASA sends a TCP reset to the inside host when the **service resetoutbound** command is enabled. (The **service resetoutbound** command is disabled by default.); The ASA sends a TCP reset to the outside host when the **service resetinbound** command is enabled. (The **service resetinbound** command is disabled by default.)

Increased maximum connection limits for service policy rules - The maximum number of connections for service policy rules was increased from 65535 to 2000000.

High Availability and Scalability Features

ASA Clustering for the ASA 5580 and 5585-X - ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

OSPF, EIGRP, and Multicast for clustering - For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. For EIGRP, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment. Multicast routing supports clustering.

Packet capture for clustering - To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the **cluster exec capture** command, which is then automatically enabled on all of the slave units in the cluster.

Logging for clustering - Each unit in the cluster generates syslog messages independently. You can use the **logging device-id** command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster.

Configure the connection replication rate during a bulk sync - You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover.

IPv6 Features

IPv6 Support on the ASA's outside interface for VPN Features - This release of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols.

Remote Access VPN support for IPv6: IPv6 Address Assignment Policy - You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.

Remote Access VPN support for IPv6: Assigning DNS Servers with IPv6 Addresses to group policies - DNS servers can be defined in a Network (Client) Access internal group policy on the ASA. You can specify up to four DNS server addresses including up to two IPv4 addresses and up to two IPv6 addresses.

Remote Access VPN support for IPv6: Split tunneling - Split tunneling enables you to route some network traffic through the VPN tunnel (encrypted) and to route other network traffic outside the VPN tunnel (unencrypted or "in the clear"). You can now perform split tunneling on IPv6 network traffic by defining an IPv6 policy which specifies a unified access control rule.

Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules - Access control rules for client firewalls support access list entries for both IPv4 and IPv6 addresses.

Remote Access VPN support for IPv6: Client Protocol Bypass - The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

Remote Access VPN support for IPv6: IPv6 Interface ID and prefix - You can now specify a dedicated IPv6 address for local VPN users.

Remote Access VPN support for IPv6: Sending ASA FQDN to AnyConnect client - You can return the FQDN of the ASA to the AnyConnect client to facilitate load balancing and session roaming.

Remote Access VPN support for IPv6: ASA VPN Load Balancing - Clients with IPv6 addresses can make AnyConnect connections through the public-facing IPv6 address of the ASA cluster or through a GSS server. Likewise, clients with IPv6 addresses can make AnyConnect VPN connections through the public-facing IPv4 address of the ASA cluster or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.

Remote Access VPN support for IPv6: Dynamic Access Policies support IPv6 attributes - When using ASA 9.0 or later with ASDM 6.8 or later, you can now specify these attributes as part of a dynamic access policy (DAP): IPv6 addresses as a Cisco AAA attribute; IPv6 TCP and UDP ports as part of a Device endpoint attribute; Network ACL Filters (client).

Remote Access VPN support for IPv6: Session Management - Session management output displays the IPv6 addresses in Public/Assigned address fields for AnyConnect connections, site-to-site VPN connections, and Clientless SSL VPN connections.

NAT support for IPv6 - NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6 (NAT64). Translating between IPv4 and IPv6 is not supported in transparent mode.

DHCPv6 relay - DHCP relay is supported for IPv6.

OSPFv3 - OSPFv3 routing is supported for IPv6.

Unified ACL for IPv4 and IPv6 - ACLs now support IPv4 and IPv6 addresses.

Mixed IPv4 and IPv6 object groups - Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses.

Range of IPv6 addresses for a Network object - You can now configure a range of IPv6 addresses for a network object.

Inspection support for IPv6 and NAT64 - We now support DNS inspection for IPv6 traffic.

Remote Access Features

Clientless SSL VPN: Additional Support - We have added additional support for these browsers, operating systems, web technologies and applications: **Internet browser support**: Microsoft Internet Explorer 9, Firefox 4, 5, 6, 7, and 8; **Operating system support**: Mac OS X 10.7; **Web technology support**: HTML 5; **Application Support**: Sharepoint 2010.

Clientless SSL VPN: Enhanced quality for rewriter engines - The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users.

Clientless SSL VPN: Citrix Mobile Receiver - This feature provides secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA.

Clientless SSL VPN: Enhanced Auto-sign-on - This feature improves support for web applications that require dynamic parameters for authentication.

Clientless SSL VPN: Clientless Java Rewriter Proxy Support - This feature provides proxy support for clientless Java plug-ins when a proxy is configured in client machines' browsers.

Clientless SSL VPN: Remote File Explorer - The Remote File Explorer provides users with a way to browse the corporate network from their web browser. When users click the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user's system displaying the remote file system in a tree and folder view.

Clientless SSL VPN: Server Certificate Validation - This feature enhances clientless SSL VPN support to enable SSL server certificate verification for remote HTTPS sites against a list of trusted CA certificates.

AnyConnect Performance Improvements - This feature improves throughput performance for AnyConnect TLS/DTLS traffic in multi-core platforms. It accelerates the SSL VPN datapath and provides customer-visible performance gains in AnyConnect, smart tunnels, and port forwarding.

Custom Attributes - Custom attributes define and configure AnyConnect features that have not yet been added to ASDM. You add custom attributes to a group policy, and define values for those attributes.

Next Generation Encryption - The National Standards Association (NSA) specified a set of cryptographic algorithms that devices must support to meet U.S. federal standards for cryptographic strength. RFC 6379 defines the Suite B cryptographic suites. Because the collective set of algorithms defined as NSA Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only) and public key infrastructure (PKI) subsystems now support them. The next generation encryption (NGE) includes a larger superset of this set adding cryptographic algorithms for IPsec V3 VPN, Diffie-Hellman Groups 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS and IKEv2.

Support for VPN on the ASASM - The ASASM now supports all VPN features.

SSL VPN Clientless: Windows 8 Support; This release adds support for Windows 8 x86 (32-bit) and Windows 8 x64 (64-bit) operating systems.

We support the following browsers on Windows 8:

- Internet Explorer 10 (desktop only)
- Firefox (all supported Windows 8 versions)
- Chrome (all supported Windows 8 versions)

Cisco Secure Desktop: Windows 8 Support; CSD 3.6.6215 was updated to enable selection of Windows 8 in the Prelogin Policy operating system check.

Multiple Context Mode Features

Site-to-Site VPN in multiple context mode - Site-to-site VPN tunnels are now supported in multiple context mode.

New resource type for site-to-site VPN tunnels - New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Dynamic routing in Security Contexts - EIGRP and OSPFv2 dynamic routing protocols are now supported in multiple context mode. OSPFv3, RIP, and multicast routing are not supported.

New resource type for routing table entries - A new resource class, routes, was created to set the maximum number of routing table entries in each context.

Mixed firewall mode support in multiple context mode - You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode.

Module Features

ASA Services Module support on the Cisco 7600 switch - The Cisco 7600 series now supports the ASASM.

ASA 5585-X support for the ASA CX SSP-10 and -20 - The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees.

ASA 5585-X Dual SSP support for the SSP-10 and SSP-20 (in addition to the SSP-40 and SSP-60); VPN support for Dual SSPs - The ASA 5585-X now supports dual SSPs using all SSP models (you can use two SSPs of the same level in the same chassis). VPN is now supported when using dual SSPs.