Cisco ASA 5500 Series Adaptive Security Appliance

Protecting Unified Communications Call Control Systems, Endpoints, and Applications

At-A-Glance

What Is the Value of the Cisco ASA 5500 Series Adaptive Security Appliance?

The Cisco ASA 5500 Series is a family of multifunction security appliances for small businesses, branch offices, enterprises, and data center environments. These appliances deliver market-leading voice and video security services for unified communications, including robust firewall, full-featured IPsec and SSL VPN, intrusion prevention, and content security features. For unified communications deployments, these platforms can protect up to 30,000 phones and deliver application inspection for the broadest range of unified communications protocols.

How Can the Cisco ASA 5500 Series Help Secure My Unified Communications Network?

The Cisco ASA 5500 Series is designed to secure real-time unified communications applications such as voice and video. The Cisco ASA 5500 Series can protect all the critical elements of a unified communications deployment (network infrastructure, call control platforms, IP endpoints, and unified communications applications). This security appliance delivers several security features that enhance the embedded security within a unified communications system, including:

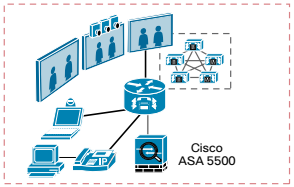
- Dynamic and granular access control to prevent unauthorized access to unified communications services.
- Threat protection for the unified communications infrastructure, such as protection against denial-of-service (DoS) or protocol fuzzing attacks.
- Network security policy enforcement to administer effective unified communications policies for applications and users, such as general whitelists, blacklists, or specific SIP policies such as preventing instant messaging over SIP.
- Service protection to help ensure maximum uptime for unified communications applications.
- Voice and video encryption services that enable customers to encrypt signaling and media to prevent eavesdropping while maintaining their security policies.

The Cisco ASA 5500 Series supports the widest range of voice and video protocols in the market today, including SCCP, SIP, H.323, MGCP, RTP/RTCP, and protocols supported by Cisco applications like CTIQBE.

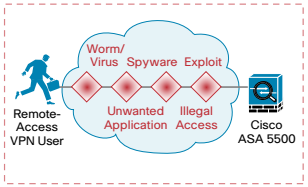
Deployment Topologies for Cisco ASA in Unified Communications Networks

The Cisco ASA 5500 Series can be used across the network to protect the call control system, endpoints, applications, and the underlying infrastructure from attacks. Topologies include:

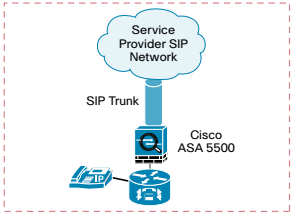
- Protection of call control servers: By controlling access from clients to these servers, the Cisco ASA appliance can prevent malicious or unauthorized network connections being made that could impact performance or availability. By statefully inspecting the connections to ascertain that they meet the access control policy and the connection conforms to expected behavior, the Protection Cisco ASA platform provides a first line of defense for a secure unified communications deployment.
- Remote-access security: The Cisco ASA 5500 Series delivers SSL and IPsec VPN services to provide secure connectivity for remote users (teleworkers, mobile workers, remote offices).
- SIP trunk security: Businesses are migrating to SIP trunk architectures for cost reasons. The Cisco ASA 5500 Series' robust SIP security capabilities provide protection from any attacks through the SIP trunks.
- Trusted/untrusted boundaries: The Cisco ASA 5500 Series can also be positioned as a security device between a trusted and untrusted network to help ensure that vulnerabilities from the untrusted network do not impact the trusted network. This can include a Cisco ASA 5500 Series appliance being used to proxy traffic between voice and data VLANs, or a DMZ architecture where a Cisco ASA appliance is used to secure an internal network against external access.



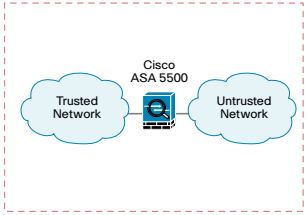
Data Center or IP PBX Security



Remote-Access Security



SIP Trunk Security



Trust Boundary Security

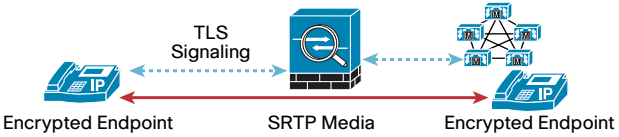
Protecting Cisco Unified Communications Manager

Many flexible, granular Layer 7 policies can be implemented by positioning a Cisco ASA 5500 Series appliance in front of Cisco Unified Communications Manager. These policies include:

- Preventing users and applications from directly accessing Cisco Unified Communications Manager through application inspection of all traffic to the server. Ports are opened only for a specific session or protocol, and are closed when the session is over.
- Protocol conformance to help ensure that SIP, SCCP, H.323, and MGCP requests conform to standards; the most common unified communications attack is a form of protocol fuzzing (malformed packets).
- Rate-limit SIP requests to the Cisco Unified Communications Manager to prevent DoS attacks.
- Policy enforcement of calls through whitelists, blacklists, caller/called party, SIP URI (uniform resource identifier).
- Allow only phones that are registered to Cisco Unified Communications Manager to place calls through the Cisco ASA appliance.
- Hardware accelerated IPS module with specific UC signatures to protect Cisco Unified Communications Manager.
- Enable inspection of encrypted phone calls within a Cisco Unified Communications Manager environment (using the Cisco TLS Proxy feature).

Cisco TLS Proxy

For compliance or security policy reasons, organizations may be required to provide confidentiality to the voice and video traffic using Transport Layer Security (TLS) and Secure RTP (SRTP). End-to-end encryption often leaves network security appliances "blind" to media and signaling traffic, compromising security functions. Starting with Cisco ASA Software Release 8.0, the Cisco ASA, as a proxy, is able to decrypt these TLS connections, apply the required threat protection and access control, and then ensure confidentiality by re-encrypting the traffic to the Cisco Unified Communications Manager servers. This is an industry first.



Why Cisco?

The combination of superior UC inspection capabilities, granular policy control for UC and Cisco industry-first capabilities like TLS proxy set Cisco ASA apart from other security products.

For more information, visit: http://www.cisco.com/go/asa

C45-450090-00 01/08