



What Are Cisco TLS Proxy and Phone Proxy?

Firewalls can provide a range of services to protect unified communications applications and servers, but need to be able to inspect encrypted signaling and media traffic. Beginning with Cisco ASA Software Release 8.0(4), Cisco ASA 5500 Series Adaptive Security Appliances support both TLS Proxy and Phone Proxy for protecting unified communications solutions deployments.

Cisco TLS Proxy provides secure interworking between the firewall and encrypted voice calls within the campus or branch network. Cisco Phone Proxy enables organizations to use the native phone encryption capability in Cisco IP phones to create secure calls from the Internet or externally connected phones. Phone Proxy can also be used to provide a secure VLAN traversal solution for Cisco IP Communicator soft phones on the data VLAN that are connecting to IP phones on the phone VLAN.

What Problems Do These Proxy Services Help Solve?

TLS Proxy: Secure Interworking

Cisco TLS Proxy enables organizations to deploy encryption and firewall services within the campus or branch network environment to inspect and secure voice traffic.

- Extends firewall services to include strong firewall policies for internal voice traffic by decrypting, inspecting, and re-encrypting signaling traffic and media
- Protects the Cisco Unified Communications Manager and other unified communications application servers
- Is fully interoperable with all Cisco IP phones that support Transport Layer Security and Secure Real-Time Transport Protocol (TLS/SRTP) encryption for signaling and media

Phone Proxy: Secure Remote Access

Cisco Phone Proxy enables remote Cisco IP phones to use their existing encryption function (TLS/SRTP) as they connect back to a Cisco Unified Communications Manager cluster.

- Enables users to plug a Cisco IP phone directly into their home network and make secure calls through the centralized Communications Manager via the Internet
- Eliminates the need to log into the phone or deploy additional remote routers or VPN devices
- Does not require changes to Communications Manager clusters or internal phones
- Secures communication with internal phones that are unencrypted or use unregistered IP addresses
- Uses certificate-based authentication of devices to prevent rogue phone connections

Phone Proxy: VLAN Traversal

Cisco Phone Proxy can be also be deployed within the enterprise or branch campus to support soft phone applications such as Cisco IP Communicator.

- Allows soft phones to securely traverse from the data VLAN to the phone VLAN
- Protects Cisco Unified Communications Manager from rogue soft phones or attackers on the data VLAN attempting to access the phone VLAN
- Helps ensure a single, secure point of entry into the voice VLAN by forcing all soft client media to proxy via the ASA appliance

Business Benefits

- Improves collaboration and productivity for remote workers
- Reduces help desk calls by eliminating deployment of additional routers and VPN devices
- Addresses compliance requirements by restricting and securing voice traffic from interception or attack
- Addresses compliance requirements by protecting critical unified communications devices, such as the Cisco Unified Communications Manager and other unified communications application servers

Cisco ASA 5500 Series and Cisco ASA Software Release 8.0(4)

Cisco ASA 5500 Series Adaptive Security Appliances provide a range of security services for Cisco Unified Communications products. Cisco ASA Software Release 8.0 introduced the TLS Proxy, and Release 8.0(4) introduced the Phone Proxy. Although the functions are closely related, they solve differing security issues and provide different security services.

What Are the Benefits of TLS Proxy and Phone Proxy on Cisco ASA 5500 Series Adaptive Security Appliances?

The Cisco ASA 5500 Series provides a single support architecture for simplifying and securing the deployment of remote phones, clients, and presence architectures. Cisco TLS Proxy and Phone Proxy provide world-class security for organizations looking to deploy new IP voice services, or who wish to extend their current deployment to include remote phones. Business benefits include:

- Increases productivity for remote workers
- Secures both external and internal voice communications
- Reduces operating costs by unifying connection services (voice, mobile devices, and IPsec and SSL VPN) into a single appliance
- Expands Cisco ASA 5500 Series sales for placement in front of Cisco Unified Communications Manager and other unified communications application servers
- Eliminates the deployment and support of remote routers and VPN devices, which helps increase employee satisfaction while reducing help desk and IT costs

Why Cisco?

Cisco is the market leader in network security solutions. Because we build both network and security solutions, we are uniquely able to provide the highest level of integration and collaboration between solutions, as well as security support for the latest business-critical applications and services, such as unified communications deployments.

For More Information

More information about Cisco TLS Proxy and Phone Proxy can be found at <http://www.cisco.com/go/secureuc>