TLS Proxy vs. Phone Proxy

Cisco® ASA 5500 Series Adaptive Security Appliances provide a range of security services for Cisco Unified Communications products. Two key functions are Transport Layer Security (TLS) Proxy and Phone Proxy. Although the functions are closely related, they solve differing security issues and provide different security services. This document explains where each will be deployed and their main functional differences.

TLS Proxy vs. Phone Proxy: Summary

TLS Proxy is used to provide interworking between the firewall function and encrypted voice calls in the campus network. This only applies to encrypted voice calls where both parties utilize encryption.

Phone Proxy is used to enable organizations to use the native phone encryption capability in Cisco IP phones to provide 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. It enables organizations to maintain a secure separation of voice and data VLANs, even when soft phones are placed on the data VLAN.

TLS Proxy: What Is It and Where Is It Used?

TLS Proxy is a Cisco ASA feature that enables seamless interoperability between campus or branch network firewalls and enables encryption for voice calls. Firewalls can provide a range of services to protect unified communications applications and servers but need to be able to inspect the signaling traffic sent from the phones. Where phone encryption is used, both the signaling traffic and the media are encrypted. Cisco TLS Proxy enables the ASA appliance to maintain signaling encryption and inspection of the signaling to protect the application servers (Figure 1).

Figure 1. TLS Connections used for the Cisco ASA TLS Proxy Solution

TLS Proxy is typically deployed in front of Cisco Unified Communications Manager and other unified communications application servers that utilize media encryption.

TLS Proxy is not designed to provide remote-access encryption services for remote phones or client endpoints. Other solutions such as Cisco ASA Phone Proxy or IP Security/Secure Sockets Layer (IPsec/SSL) VPN services are more appropriate.

TLS Proxy is not designed to provide a secure campus soft phone solution where the requirement is to provide secure data to phone VLAN traversal or for proxying connections to Cisco Unified Communications Manager.

TLS Proxy: Benefits

- TLS Proxy enables organizations to deploy encryption and firewall services within the campus or branch network environment. This avoids the need to either turn off encryption or to dilute the firewall security policies.

TLS Proxy: Common Questions and Other Considerations

TLS Proxy is designed to provide a solution for Cisco ASA appliances and Cisco Unified Communications Manager and Communications Manager Express. It does not provide interoperability for other firewall or unified communications vendors' equipment.

TLS Proxy first became available in Cisco ASA Software Release 8.0. It is interoperable with all Cisco Unified IP Phones that support Transport Layer Security and Secure Real-Time Transport Protocol (TLS/SRTP) encryption for signaling and media, respectively.

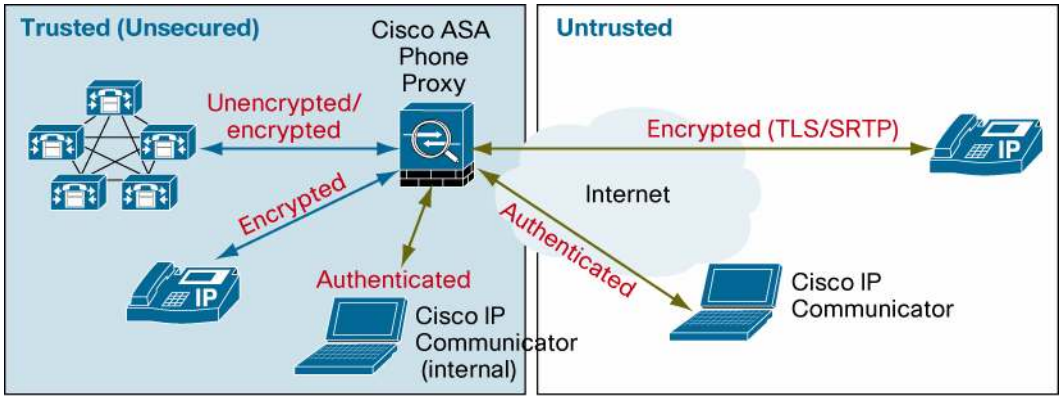
TLS Proxy: Useful Links

An application note that describes TLS Proxy in more detail is available on the Cisco Secure Unified Communications site at http://www.cisco.com/go/secureuc.

Phone Proxy: What Is It and Where Is It Used?

Cisco ASA Phone Proxy is a superset of the TLS Proxy. Phone Proxy builds upon the TLS Proxy's integration into the Cisco Unified Communications Manager authentication infrastructure and the proxy's ability to decrypt TLS sessions. In addition, the Phone Proxy function is an adaption that provides security for two deployment architectures (see Figure 2): secure remote access for Cisco Unified IP Phones and secure VLAN traversal.

Figure 2. Cisco ASA Phone Proxy Deployments



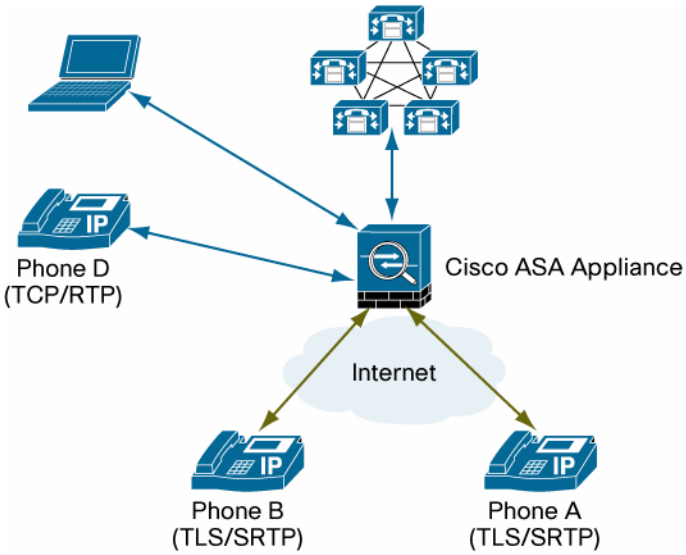
Secure Remote Access for Cisco Unified IP Phones

Cisco ASA Phone Proxy enables remote Cisco Unified IP Phones to utilize the existing encryption function (TLS/SRTP) to provide confidentiality and integrity as they connect back to a Cisco Unified Communications Manager cluster at the corporate office. Without relying on a remote device such as a router to provide these services, typically using IPsec VPN, the Cisco ASA supports the casual teleworker deployment by adapting the TLS Proxy to suit remotely deployed phones. This enables users to plug their IP phone directly into their home office DSL connection or network device and make secure calls through the centralized Communications Manager via the Internet.

In contrast to TLS Proxy, the Phone Proxy can be configured to support encrypted remote phones without the need for the Communications Manager cluster to run in secure mode. Internal phones that communicate with the remote phone also do not need to have encryption enabled. This is an important consideration, as most organizations do not encrypt all calls. If an internal phone or communications manager is not configured for encryption, the entire call would fall back to being unencrypted, including across the Internet. Cisco ASA Phone Proxy provides the necessary interworking to ensure that the external phone's traffic remains encrypted, even if the rest of the system is not encrypted.

The Cisco ASA Phone Proxy function also manipulates the call signaling to ensure that all media is routed via the ASA appliance. This allows the appliance to perform decryption of encrypted media traffic from the remote phone to the unencrypted internal phone. It also helps ensure that the remote phone can successfully send media to internal phones that most typically use unregistered IP address ranges, such as network 10.x.x.x addresses. Without the Phone Proxy forcing the media via itself, the remote phones would not be able to route the media traffic to a phone on the internal network.

Figure 3. Cisco ASA Phone Proxy deployment with Non-Secure Cisco Unified Communication Manager Clusters



The key differences between TLS Proxy and Phone Proxy functions are that the Phone Proxy provides decryption and proxies both the media and the signaling traffic. TLS Proxy is only concerned with decrypting and inspecting the signaling and is therefore only effective if encryption is used within the corporate network and between endpoints and communications managers. TLS Proxy cannot provide the necessary interworking required to ensure traffic is successfully routed and decrypted in a remote-access topology. Phone Proxy provides these integration services to enable the deployment of Cisco IP phones outside the corporate environment.

Phone Proxy: Secure Remote-Access Benefits

- A Cisco IP phone can be used in an external/Internet-based environment.
- Implementation does not require changes to communications manager clusters or internal phones.
- A simplified user experience eliminates the need to log on to the phone or a VPN.

- Certificate-based authentication of devices prevents rogue phone connections.
- Proxy of phone signaling with the optional use of Network Address Translation (NAT) ensures that communications managers are not directly exposed to the Internet.
- Proxy of phone media ensures that internal phones are not directly exposed to the Internet and can accommodate the use of unregistered, internal address ranges for phones within the corporate network.
- Phone Proxy supports multiple Cisco IP phones deployed behind a NAT/firewall device at a remote site.

Phone Proxy for Remote Access: Common Questions and Considerations

Supports all Cisco IP phones that support TLS encryption; this includes Cisco wireless phones as well as standard Cisco handsets.

Remote soft clients such as Cisco Unified Personal Communicator should utilize IPsec or SSL VPN connections from the user desktop rather than Phone Proxy.

Ideally, IP phones should be pre-provisioned in the corporate network environment for the most secure and user-friendly deployment.

To deploy existing, registered IP phones for Phone Proxy requires that any Cisco Unified Communications Manager CTL (Certificate Trust List) file is not already downloaded.

If the Phone Proxy is deployed behind a corporate firewall, the firewall must not perform NAT on the Phone Proxy traffic as it will be unable to perform NAT on the embedded addressing that is encrypted. These devices must also allow access for the TLS, SRTP, and Trivial File Transfer Protocol (TFTP) ports from the external network.

The media termination address used to proxy the media must use an address that the internal and external phones can route to.

Stateless failover is supported; this ensures that registration information is passed to the secondary unit, but active calls will drop and will need to be re-initiated.

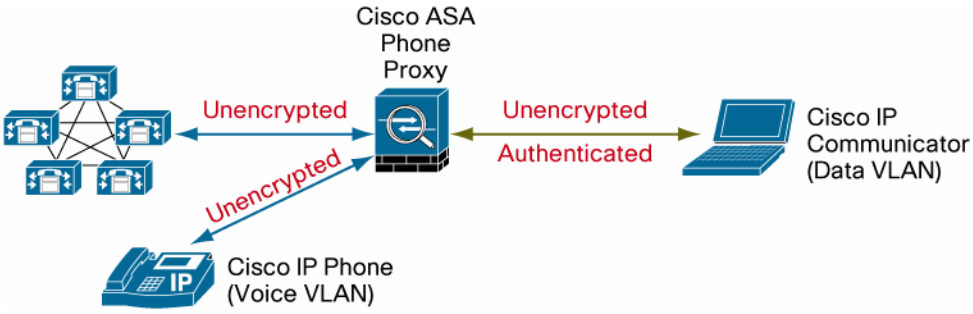
Phone Proxy requires Cisco ASA Unified Communications Proxy licenses—at least one per registered phone. If the phone has a backup Cisco Unified Communications Manager configured, this will consume two licenses per remote phone.

Phone Proxy: Secure VLAN Traversal

In addition to deploying Cisco ASA Phone Proxy for remote IP phones, the proxy can be deployed within the enterprise campus, primarily to support soft phone applications such as Cisco IP Communicator. A common customer concern for soft phone deployment is protecting Cisco Unified Communications Manager from rogue soft phones or attackers on the data VLAN. As most customers' campus security architectures for unified communications are based around VLAN separation, a solution is needed that allows soft phones to securely communicate from the data VLAN to the phone VLAN where the Cisco IP phones are deployed.

Cisco ASA Phone Proxy can satisfy both these requirements by intercepting and authenticating soft clients before they reach Cisco Unified Communications Manager clusters and by forcing all soft client media to proxy via the ASA appliance, ensuring a single, secure point of entry into the voice VLAN (Figure 4)

Figure 4. Cisco ASA Phone Proxy for Campus Softphone Deployments



In this scenario, the ASA appliance is positioned in front of the communications manager on the data VLANs that the soft clients reside upon. By authenticating the soft clients before they send signaling to the communications manager cluster, the ASA Phone Proxy can help mitigate the threat of a rogue phone connection.

By manipulating the signaling and forcing the soft phone media to proxy via the adaptive security appliance, organizations can avoid using stateless access lists that cannot control access on the range of possible RTP/SRTP media ports. Instead, media sent to the ASA appliance can be matched against legitimate authorized calls and the RTP media ports can be opened dynamically and closed at the end of the call.

There is no requirement for the ASA appliance to intercept and proxy signaling requests from phones in the phone VLAN. Phones in the phone VLAN are only directed to send media to the ASA appliance when they are in a call with a soft client that the appliance is providing proxy services for.

In contrast to TLS Proxy and Phone Proxy for remote IP phones, the Cisco IP Communicator clients currently do not support TLS encryption; therefore the calls are not encrypted. Instead, using TLS authentication, the architecture provides authentication and proxy functions only.

It is important to note that Cisco IP Communicator is the only soft client that is currently supported. Cisco Unified Personal Communicator support as well as support for encryption with Cisco IP Communicator will become available when these clients support encrypted TLS for signaling and SRTP for media.

Phone Proxy: Benefits of Secure VLAN Traversal

- Protects communications manager from rogue soft client devices and attackers on the data VLAN.
- Provides a secure VLAN traversal solution for soft clients on the data VLAN communicating with Cisco IP phones in the phone VLAN.

Phone Proxy for Secure VLAN Traversal: Common Questions and Other Considerations

Typically, organizations would deploy separate ASA appliances for the remote-access and campus soft client deployments.

Cisco IP Communicator is the only Cisco soft phone client currently supported. Other clients will be supported as they themselves support TLS and SRTP.

Cisco IP Communicator supports TLS authenticated mode. This means that the calls are not encrypted, only authenticated and proxied.

Phone Proxy vs. Cisco Unified Phone Proxy

The Cisco Unified Phone Proxy is the first-generation Cisco Phone Proxy. This platform has now reached end-of-sale status. Table 1 provides a comparison between the Cisco Unified Phone Proxy platform and the next generation ASA Phone Proxy that became available in August 2008.

Table 1. Phone Proxy Comparison

Features	Cisco Unified Phone Proxy	Cisco ASA Phone Proxy
Skinny Client Control Protocol (SCCP) Support	Yes	Yes
Session Initiation Protocol (SIP) Support	No	Yes
Soft Phone Support	Yes (in nonsecure mode); Cisco IP Communicator only	Yes (in nonsecure mode); Cisco IP Communicator support for SRTP/TLS is on the roadmap for both Cisco IP Communicator and Cisco Unified Personal Communicator clients
Device Authentication	No	Yes
Supports More than One Endpoint at Remote Location	No	Yes
Encryption for Cisco Unified Communications Manager in Nonsecure Mode	Yes	Yes
Encryption for Cisco Unified Communications Manager in Secure Mode	No	Yes
Multiple Cisco Unified Communications Manager Clusters Supported	Yes	Yes
Scalability	3000 phones per Cisco Unified Phone Proxy cluster	10,000 Unified Communications proxy sessions on Cisco ASA 5580 appliance

Phone Proxy: Useful Links

An application note that describes ASA Phone Proxy in more detail is available on the Cisco Secure Unified Communications site at http://www.cisco.com/go/secureuc.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-493584-00 09/08