Security

Security Overview

When comparing IPv4 and IPv6 in terms of how secure each protocol is, IPv6 has some advantages and some disadvantages, but overall it is no more or less secure than IPv4. One inherent benefit of IPv6 is the enormous size of IPv6 subnets and networks, which offer improvements in protection against automated scanning and worm propagation. Typical security drawbacks are the addressing complexity of IPv6 and the likelihood that network administrators will not be familiar with the IPv6 protocol and IPv6 security tools.

In general, most of the legacy issues with IPv4 security remain in IPv6. For example, Address Resolution Protocol (ARP) security issues in IPv4 are replaced with neighbor discovery (ND) security issues in IPv6.

IPv6 security settings have the same functionality as IPv4, such as Firewall, sRTP and TLS.

Privacy and Encryption for IPv6 Voice Signaling and Media

The Internet Engineering Task Force (IETF) and RFCs 4301-4303 mandate authentication and encryption for IPv6 using IP Security (IPsec). However, to avoid interworking issues with legacy IPv4 Unified Communications endpoints, Cisco Unified Communications Manager (Unified CM) IPv4 and IPv6 deployments continue to use Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for authentication and encryption between IP phones and between IP phones and SIP gateways and trunks.

IPsec can also be used for IPv4-based H.323 and Media Gateway Control Protocol (MGCP) gateway connections.

Cisco Unified CM provides the following secure transport protocols:

- Transport Layer Security (TLS)

  TSL provides secure and reliable data transfer between two systems or devices by using secure ports and certificate exchange. TLS secures and controls connections between Unified CM-controlled systems,

devices, and processes to prevent access to the voice domain. Unified CM uses TLS to secure Skinny Client Control Protocol (SCCP) calls to phones that are running SCCP, and to secure SIP calls to phones or trunks that are running SIP.

- IP Security (IPsec)

  IPsec provides secure and reliable data transfer between Unified CM and gateways. IPv4-based IPsec implements signaling authentication and encryption to Cisco IOS MGCP and H.323 gateways.

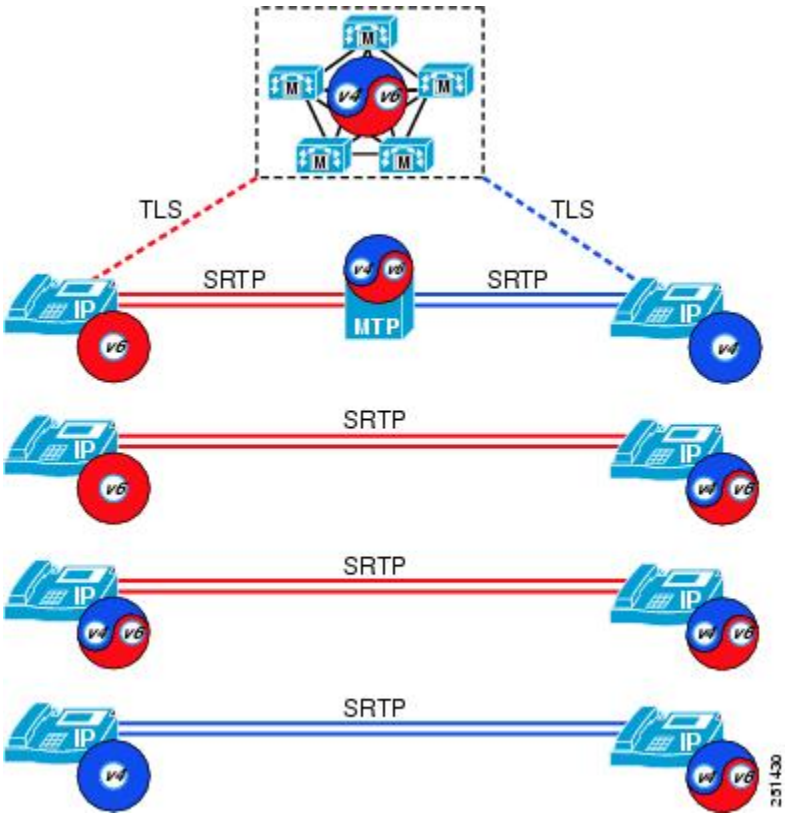
You can add Secure Real-Time Transport Protocol (SRTP) to TLS and IPsec transport services for the next level of security on devices that support SRTP. SRTP authenticates and encrypts the media stream to ensure that voice conversations originating or terminating on Cisco Unified IP Phones and either TDM or analog voice gateway ports, are protected from eavesdroppers who might have gained access to the voice domain. SRTP adds protection against replay attacks.

For more information on Unified CM security, refer to the *Cisco Unified Communications Manager Security Guide*, available at: Link.

Encrypted Media and MTPs Between IPv4 and IPv6

Unified CM supports encrypted calls between dual-stack (IPv4 and IPv6) and single-stack (IPv4 or IPv6) devices. If an IP addressing version mismatch exists between the called and calling device, Unified CM dynamically inserts an MTP to convert the IP header of the encrypted voice stream. This dynamically inserted MTP uses its pass-through codec for the encrypted media stream and changes only the IP headers from IPv4 to IPv6 and conversely.

Figure 1: Addressing Mode Resolution by Unified CM



CAPF and CTL

Certificate Authority Proxy Function (CAPF) supports both IPv4 and IPv6 addressing and uses TCP/IP to communicate with phones and to perform its standard security certificate functions. In an IPv6-enabled Unified CM cluster, CAPF has the following capabilities:

- Issuing and upgrading certificates to IPv4-only IP phones
- Issuing and upgrading certificates to IPv6-only IP phones
- Issuing and upgrading certificates to dual-stack (IPv4 and IPv6) IP phones

No new IPv6 functionality is needed for Certificate Trust List (CTL).

IPv6 Collaboration Traffic and Firewalls

The Cisco Adaptive Security Appliance (ASA) supports SCCP or SIP for IPv6, therefore can be used to open pinholes dynamically for IPv6 voice traffic. This product supports basic firewall and traffic filtering function for IPv6 traffic.

If you want to implement basic firewall capability for IPv6, refer to the following documents:

- Cisco ASA 5500-X Series Firewalls Configuration Guides

  Reference: Link
- Catalyst 6500 Series Switch Configuration Guides

  Reference: Link

Cisco Unified Border Element

The Cisco IOS-based Cisco Unified Border Element can:

- Terminate a SIP IPv6 call on one leg of a session, and generate a SIP IPv4 call on the other leg.
- Terminate a SIP IPv6 call on one leg of a session, and generate a SIP IPv6 call on the other leg.

This functionality allows for basic interconnection between enterprise IPv6 networks and service provider IPv4 networks.

Basic calls with both media and signaling processing are supported. Basic Supplementary Services over IPv6 are supported, but H.323 IPv6 calls are not supported.