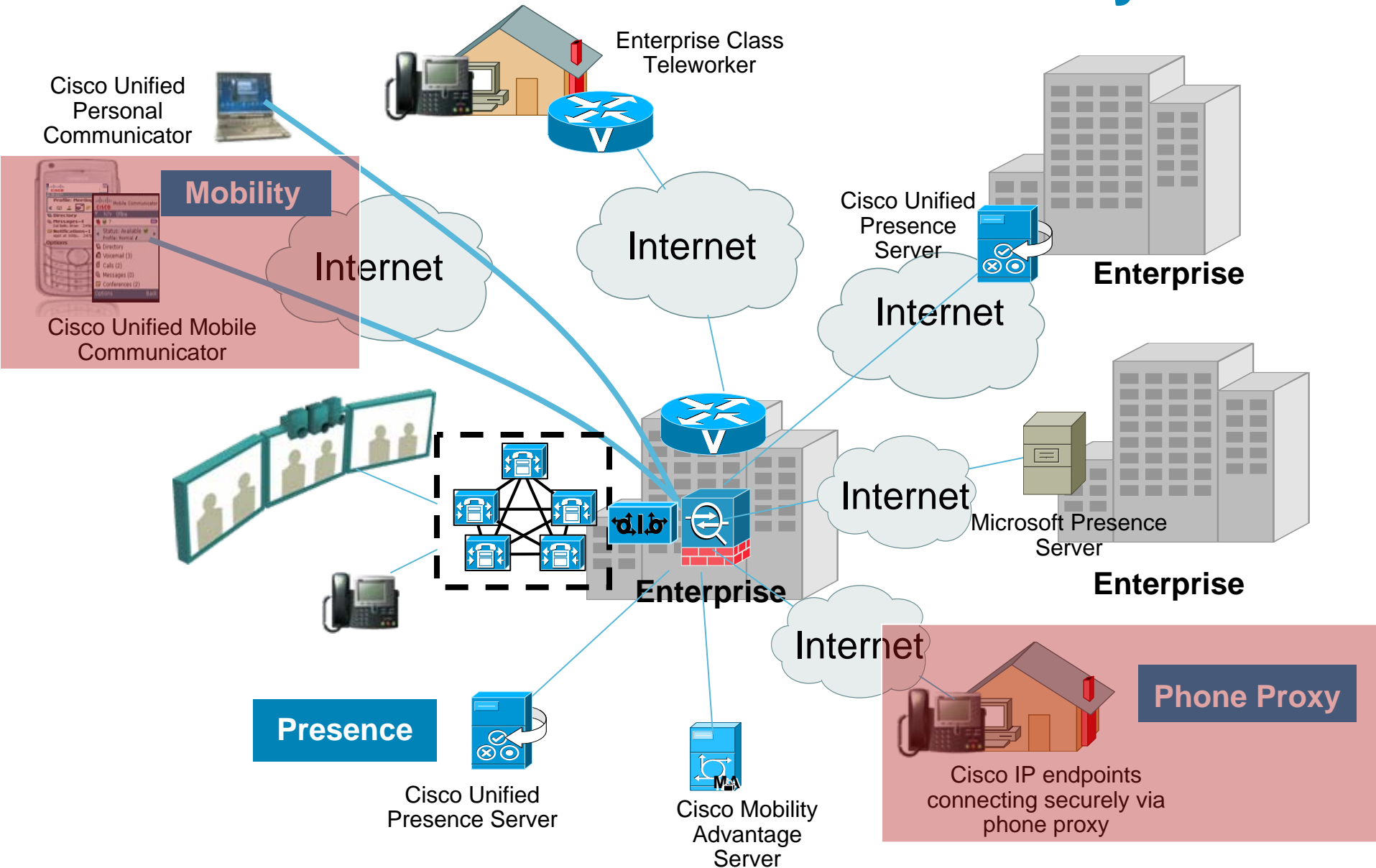


ASA Phone Proxy

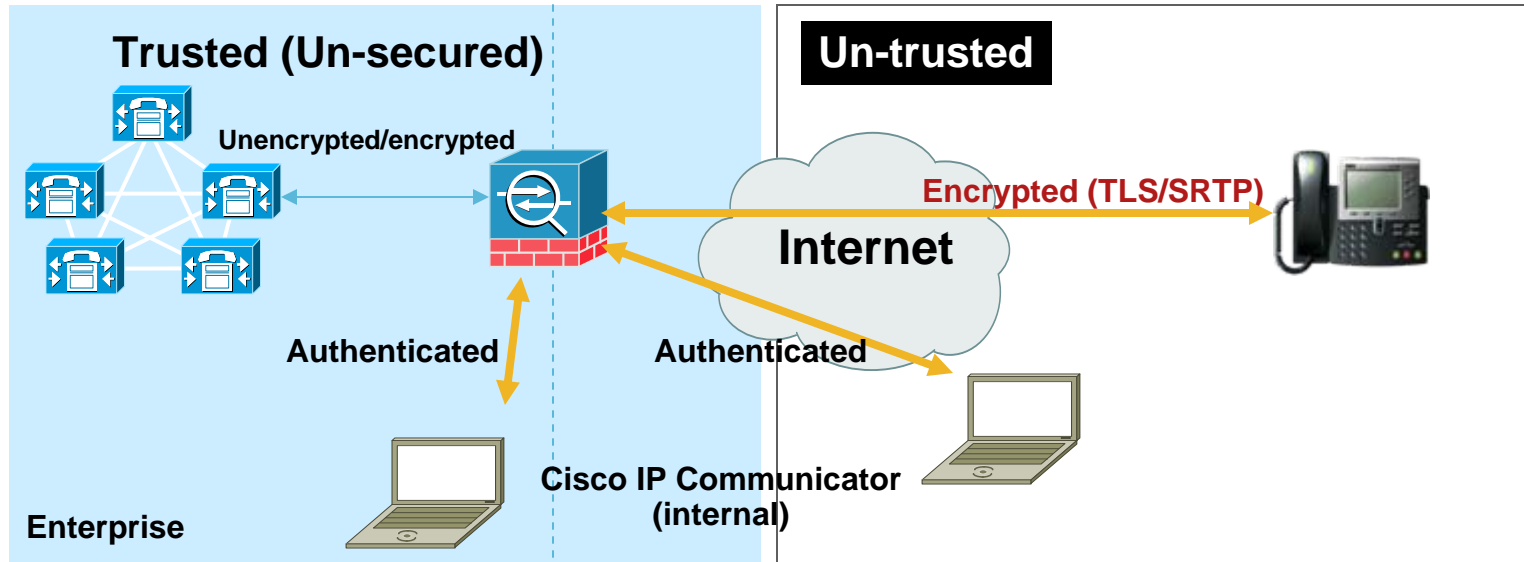


Secure UC – Remote Access/Mobility



Cisco ASA Phone Proxy - Deployments

Remote Access and Voice/Data Segmentation



Deployment Scenarios:

1. Secure Remote Access:

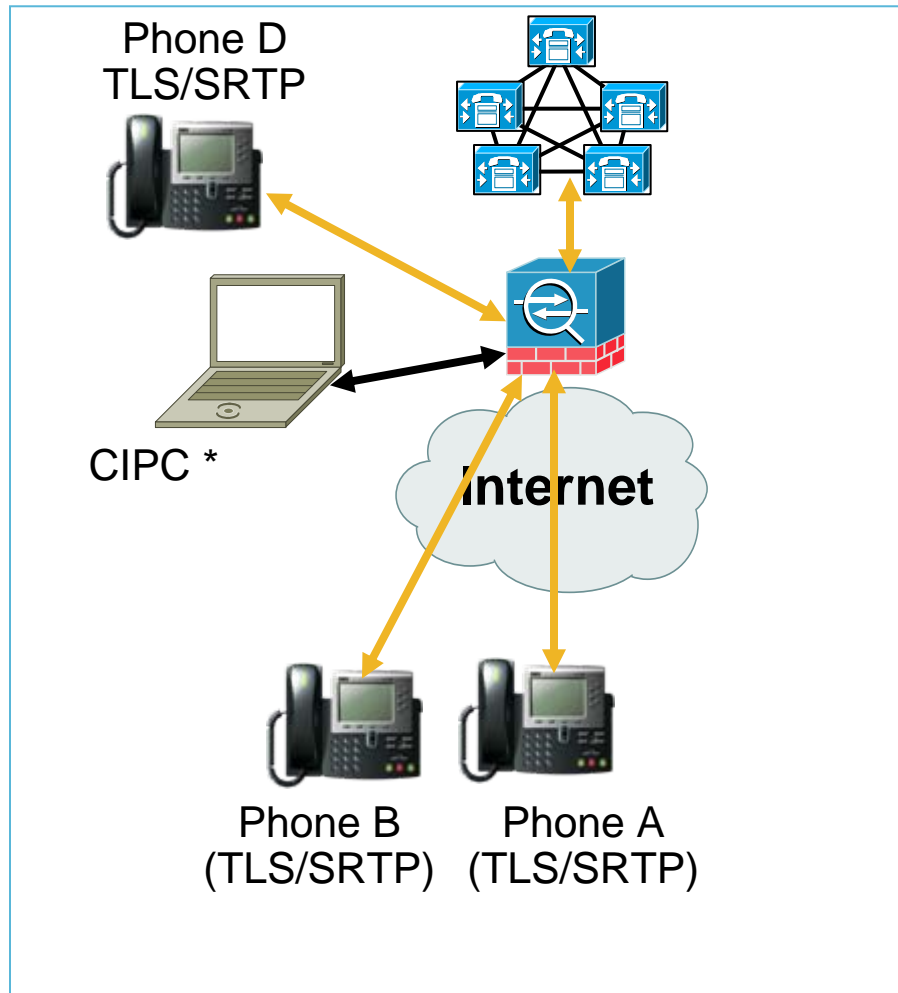
- Terminates encrypted endpoints for secure remote access

2. Voice/data VLAN segmentation for Softphone Applications:

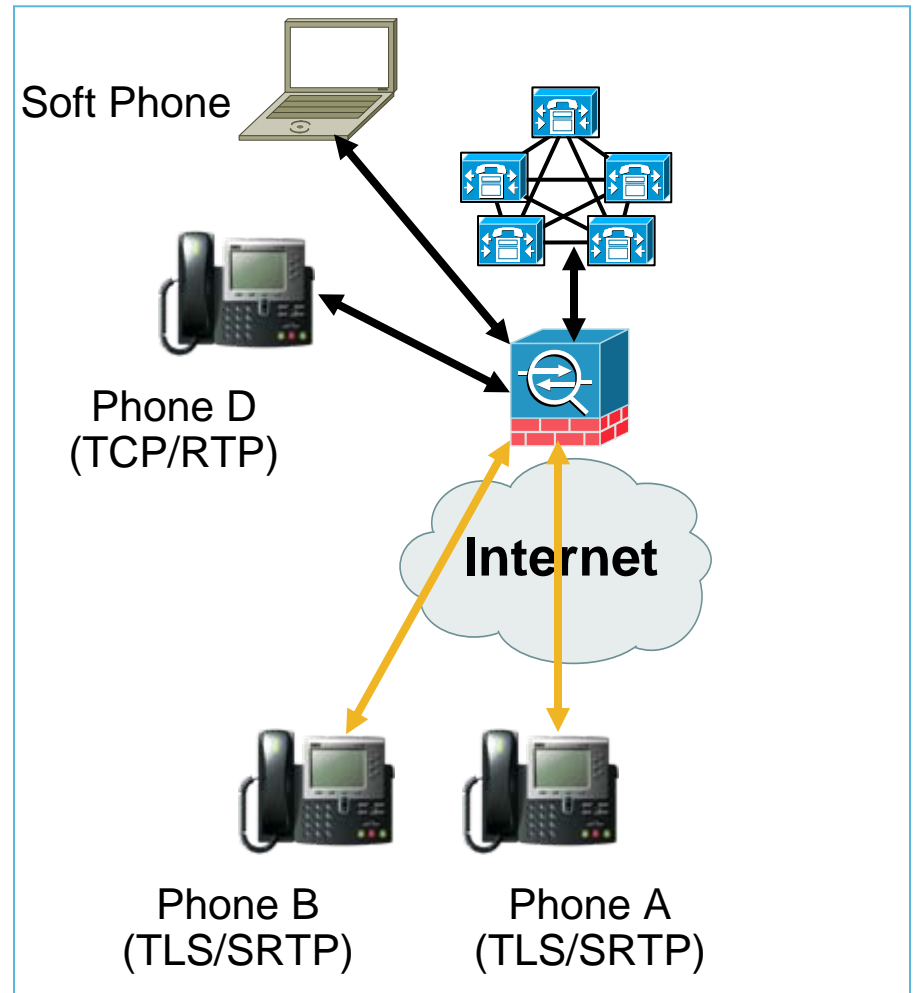
- All communicator traffic originating from soft clients must be “proxied”
- Soft client communication is restricted to specific VLAN on ASA
- Cisco ASA performs inspection on traffic and opens media port dynamically for soft clients
- Dependency on SRTP support on Cisco Unified IP Communicator (Roadmap for 2H CY2008)

ASA Phone Proxy For Remote Access

Mixed Mode CUCM Cluster



Non-Secure CUCM Cluster

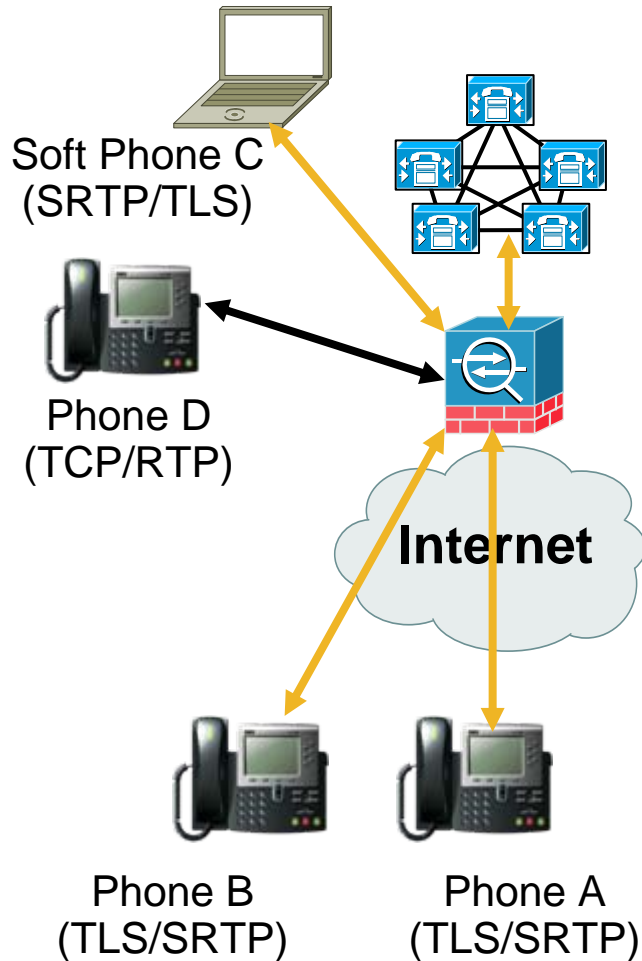


←→ Encrypted TLS

* CIPC only supports TLS Authenticated Mode – TLS/SRTP Roadmapped

ASA Phone Proxy

Feature and Design Summary



ASA vs Cisco Unified Phone Proxy

- Simplified User Experience
- Greater Security including Certificate Authentication and Firewall inspection for SIP/SCCP
- Supports SIP, SCCP and a range of UC clients (CIPC, 7921 etc but not CUPC)
- Supports multiple remote devices behind home office router/nat device
- Stateless Failover (Connections must re-establish)

Design Considerations

- CUCM can have a private network address but need to configure NAT on the ASA
- ASA Phone Proxy can be placed behind another firewall but the external firewall
 - Must NOT NAT the CUCM address
 - Must open up the TCP (SSL, TLS) and UDP (SRTP, TFTP) ports
 - Must ensure that the ASA Phone Proxy has a publicly routable address

Cisco ASA Phone Proxy and Cisco Unified Phone Proxy Comparison

Features	Cisco Unified Phone Proxy	Cisco ASA Phone Proxy
SCCP support	Yes	Yes
SIP support	No	Yes
User authentication using browser	Yes	No
Device authentication w/ CERTS	No	Yes
Supports more than one endpoint at remote location	No	Yes
Encryption for CUCM in non-secure mode	Yes	Yes
Encryption for CUCM in mixed mode	No	Yes
Clustering	Yes	Roadmapped
Multiple CUCM clusters supported	Yes	Roadmapped
Scalability	3000 phones per CUPP cluster	TBD. Targeted to be higher than CUPP

End-User Phone Provisioning

ASA Phone Proxy is a transparent proxy with respect to the TFTP and signaling transactions. If no NAT is configured for the CUCM TFTP server, then the phone needs to be configured with the CUCM cluster's TFTP server address. If NAT is configured for the CUCM TFTP server, then the CUCM TFTP servers's global address will be configured as the TFTP server on the phone.

- Option 1 (Recommended) – Stage phones at HQ before sending to end user:
 - Phones register inside the network. IT ensures there are no issues with phone configs, image downloads, and registration.
 - If CUCM cluster was in mixed mode, the CTL file should be erased before sending the phone to the end-user.
 - Advantages of this option are:
 - Easier to troubleshoot & isolate problems with the user's network or Phone Proxy if we know the phone is registered & working with the CUCM.
 - Better user experience since the phone doesn't have to download firmware from home on a broadband connection which may be slow and require the user to wait for a longer time.
- Option 2 – Send brand new phone to end user
 - User must be provided instructions to change the settings on phones with the appropriate CUCM TFTP server IP address
- In both options:
 - Deploying a remote IP Phone behind a commercial Cable/DSL router with NAT capabilities is supported.

High level configuration checklist

- ASA must have a publicly routable IP address for media termination.
- TFTP Server address on the phone:
 - If NAT is configured for the CUCM TFTP server, then use the CUCM TFTP server's global IP address
 - If no NAT is configured for the TFTP server, then use the CUCM TFTP server's internal IP address.
- The Cisco UCM can be on a private network on the inside, but you need to have a static mapping for the UCM on the ASA to a public routable address
- Inspection services for voice traffic should be configured.
- Access-list rules to permit TFTP, TLS traffic must be configured
- If Phone proxy is deployed behind an existing firewall, access-list rules to permit signaling, TFTP and media traffic to Phone proxy must be configured. If NAT is required for CUCM, it must be configured on the ASA, not on the existing firewall.
- No need to configure each of the Phone's MAC address on the ASA.

TLS Proxy v Phone Proxy

Positioning

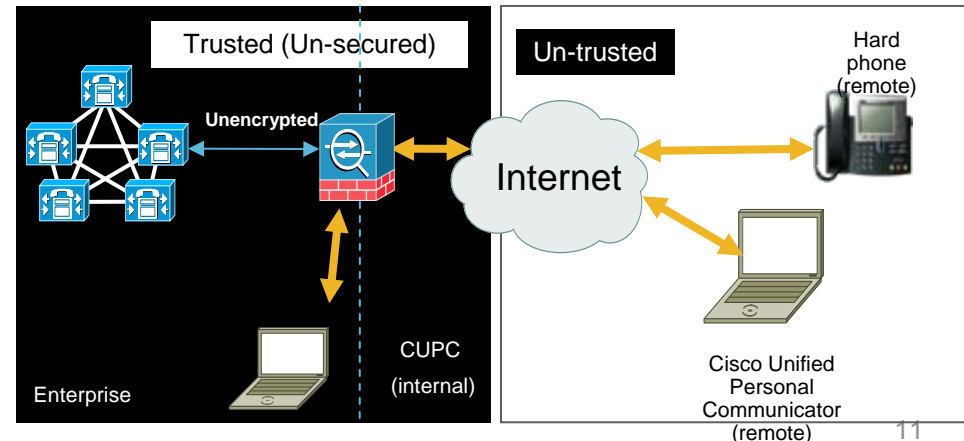
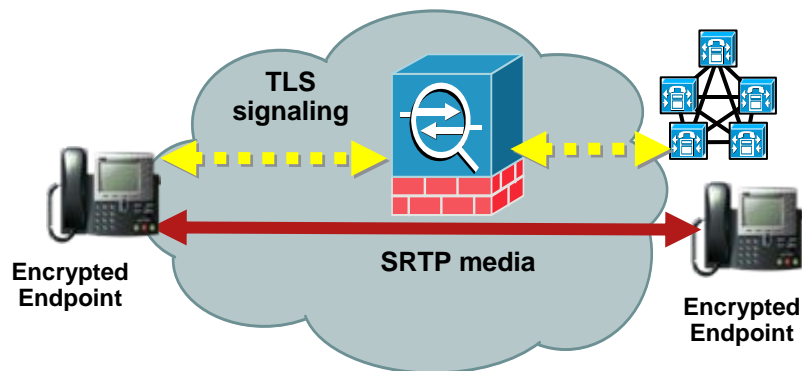
- TLS Proxy provides encryption and firewall interworking for CUCM clusters; A solution for encrypted phones and CUCM in Secure Mode
- Phone Proxy provides for remote access and softphone vlan traversal for encrypted and non-encrypted phones
- Phone Proxy is a super-set of TLS Proxy functionality

TLS Proxy

- Only manipulates TLS signaling – does not touch the media (SRTP/RTP)

Phone Proxy

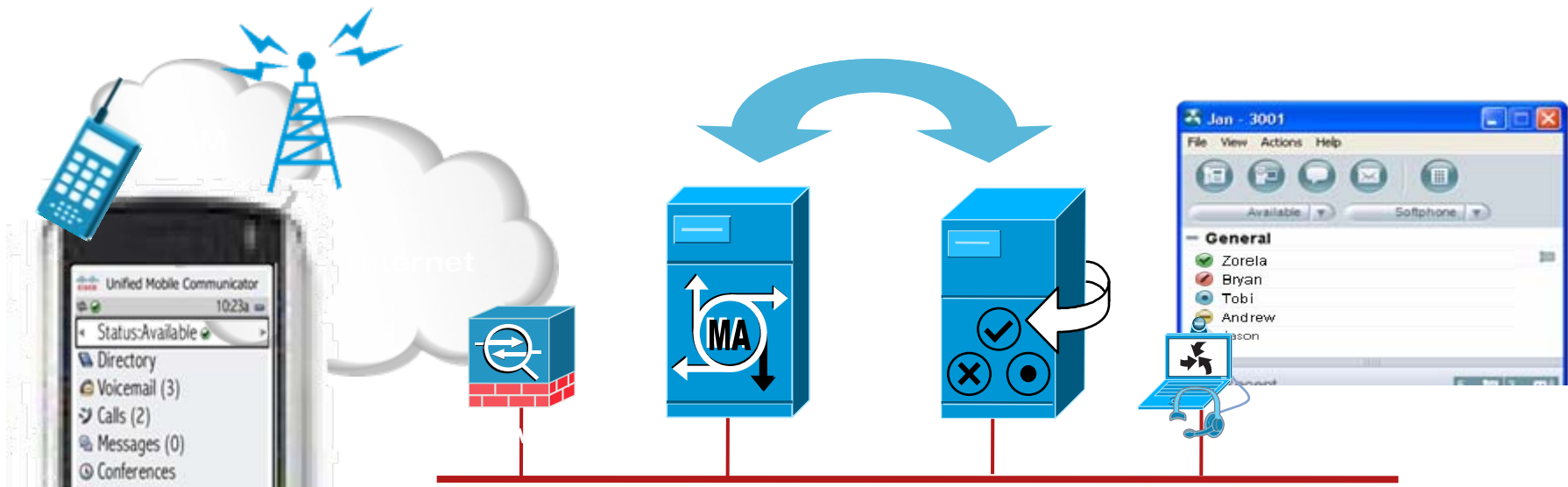
- Manipulates signaling, media and creates its own CTL file



Cisco Unified Presence 7.0

Mobility: Diagram and Key Points

- CUP 7.0 introduces common presence with CUMA/MC



Presence

•CUMC/CUMA will coordinate presence with CUP so it is in synch with other Cisco enterprise clients

Contact Lists

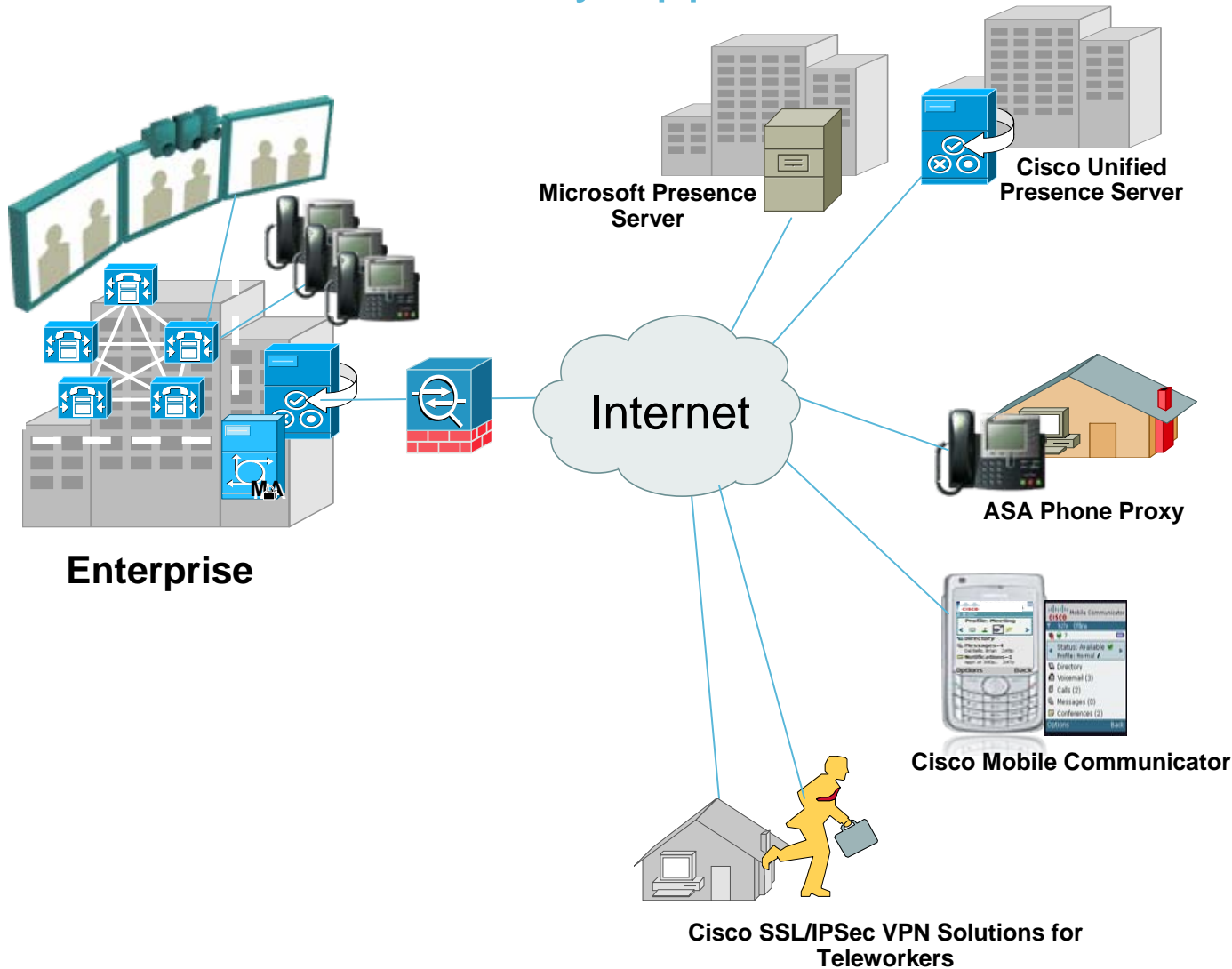
CUMC/ CUMA will coordinate its buddy list with CUP so it is in synch with other Cisco enterprise clients

Instant Messaging

IM is between CUPC and CUMC is NOT supported in this release. IM is road mapped to be supported in CUP 8.0

Cisco ASA 5500 Series

UC Perimeter Security Appliance for Collaborative Solutions



NEW

Presence Federation

Securely communicate with inter-enterprise Cisco and Microsoft Presence servers/endpoints

NEW

Phone proxy

Terminate SRTP/TLS-encrypted remote phones (and internal softphones support)

NEW

Mobility solutions

ASA terminates TLS signaling from mobile endpoints and enforce security policies

VPN solutions

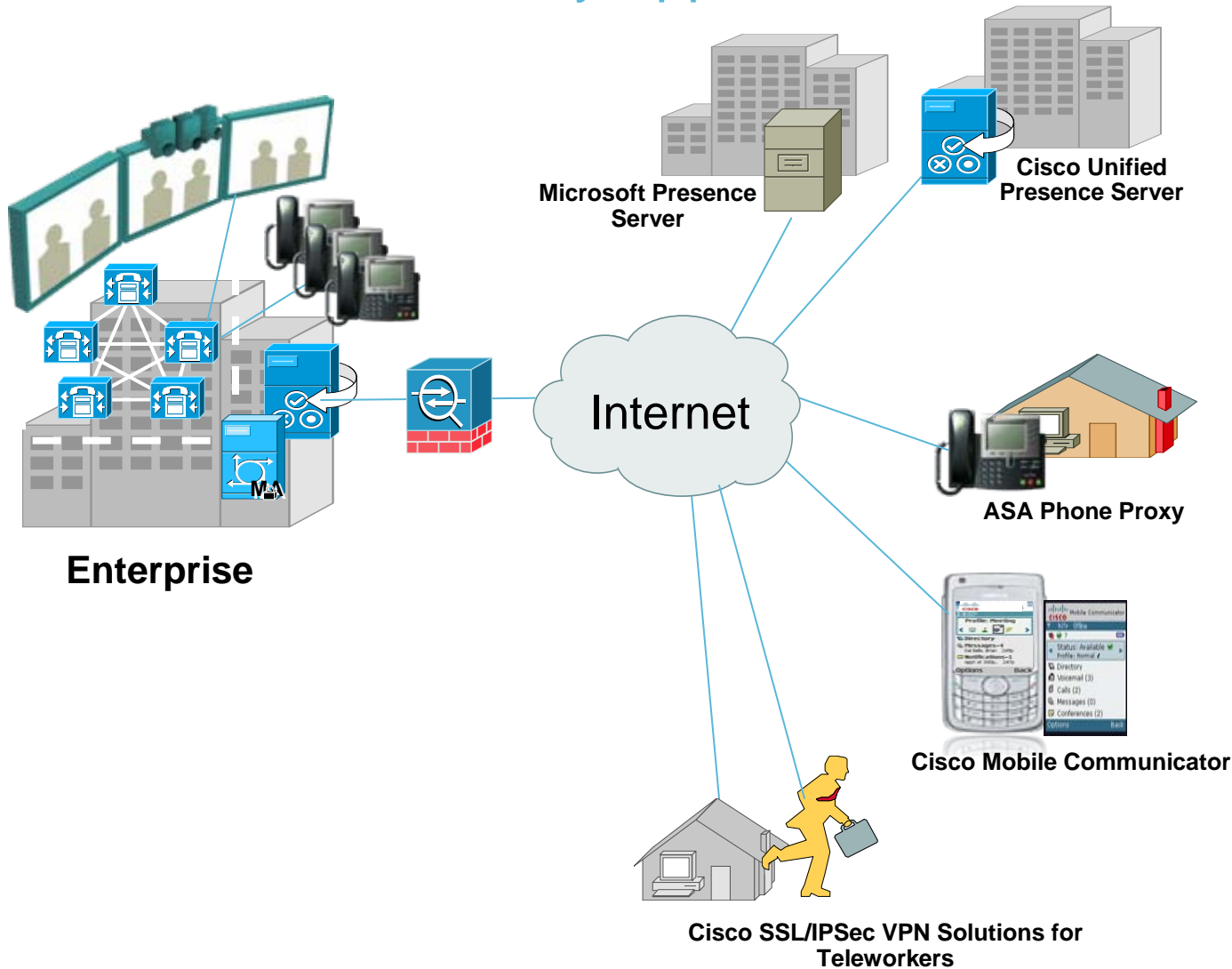
ASA supports other secure connectivity options – SSL/IPSec VPN clients

Key Takeaways



Cisco ASA 5500 Series

UC Perimeter Security Appliance for Collaborative Solutions



NEW

Presence Federation

Securely communicate with inter-enterprise Cisco and Microsoft Presence servers/endpoints

NEW

Phone proxy

Terminate SRTP/TLS-encrypted remote phones (and internal softphones support)

NEW

Mobility solutions

ASA terminates TLS signaling from mobile endpoints and enforce security policies

VPN solutions

ASA supports other secure connectivity options – SSL/IPSec VPN clients

