



# Unified Communications Security:

Cisco ASA 5500 Adaptive  
Security Appliance Series



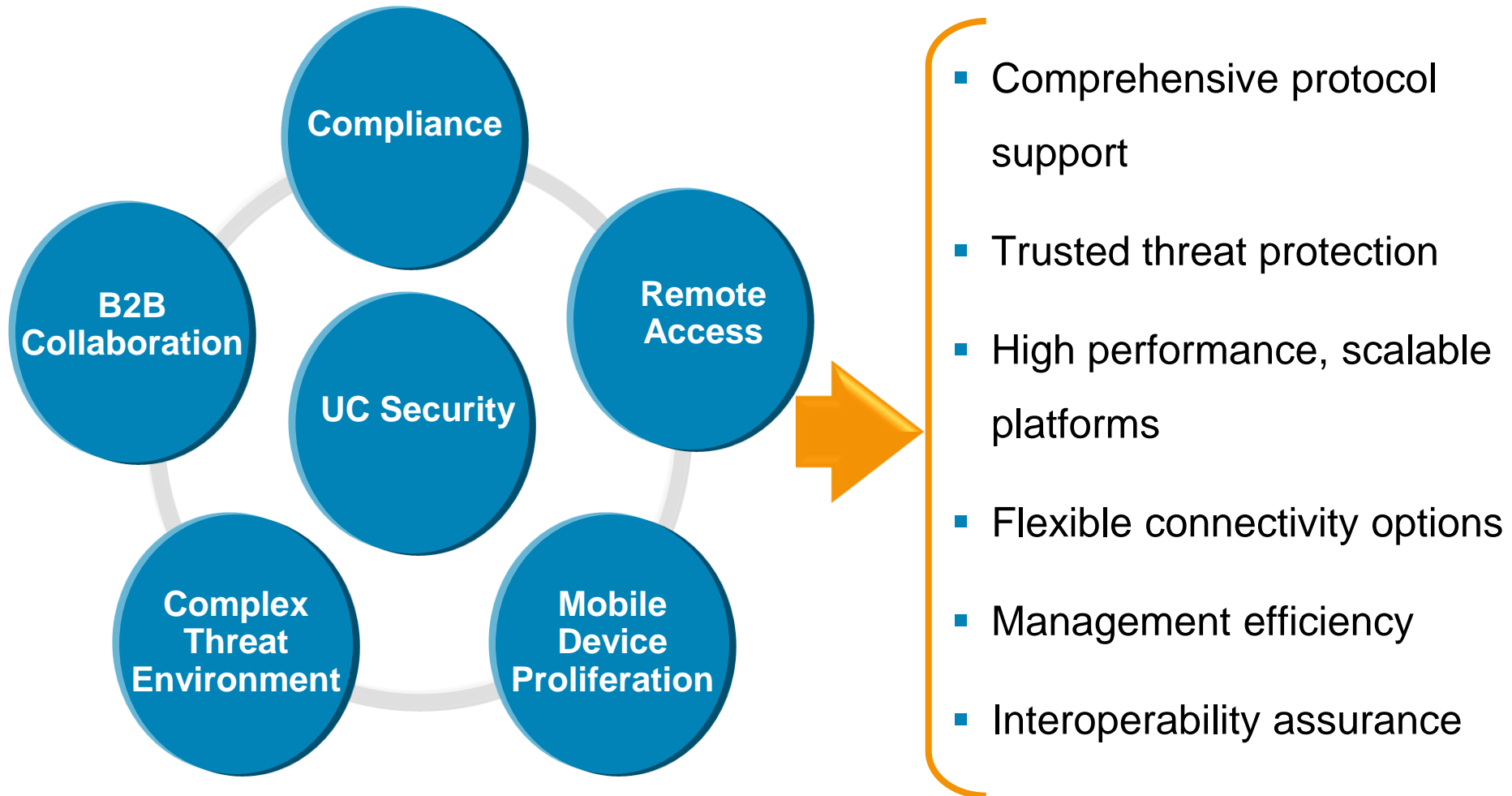
**Alin David**

Systems Engineer

Cisco Systems Romania

# Unified Communications Challenge Today

## Security as an Enabler



# Cisco Adaptive Security Appliance

## Industry's Most Proven Security Appliance

- Most widely deployed network security platform
  - Millions of devices deployed
  - 100,000s of installations
- High performance, adaptive solution
- 15 years of investment, 1,000s of security engineers
- Common Criteria EAL4+; industry's broadest coverage

---

### Cisco Adaptive Security Appliances



Granular Access Controls

Advanced Threat Protection

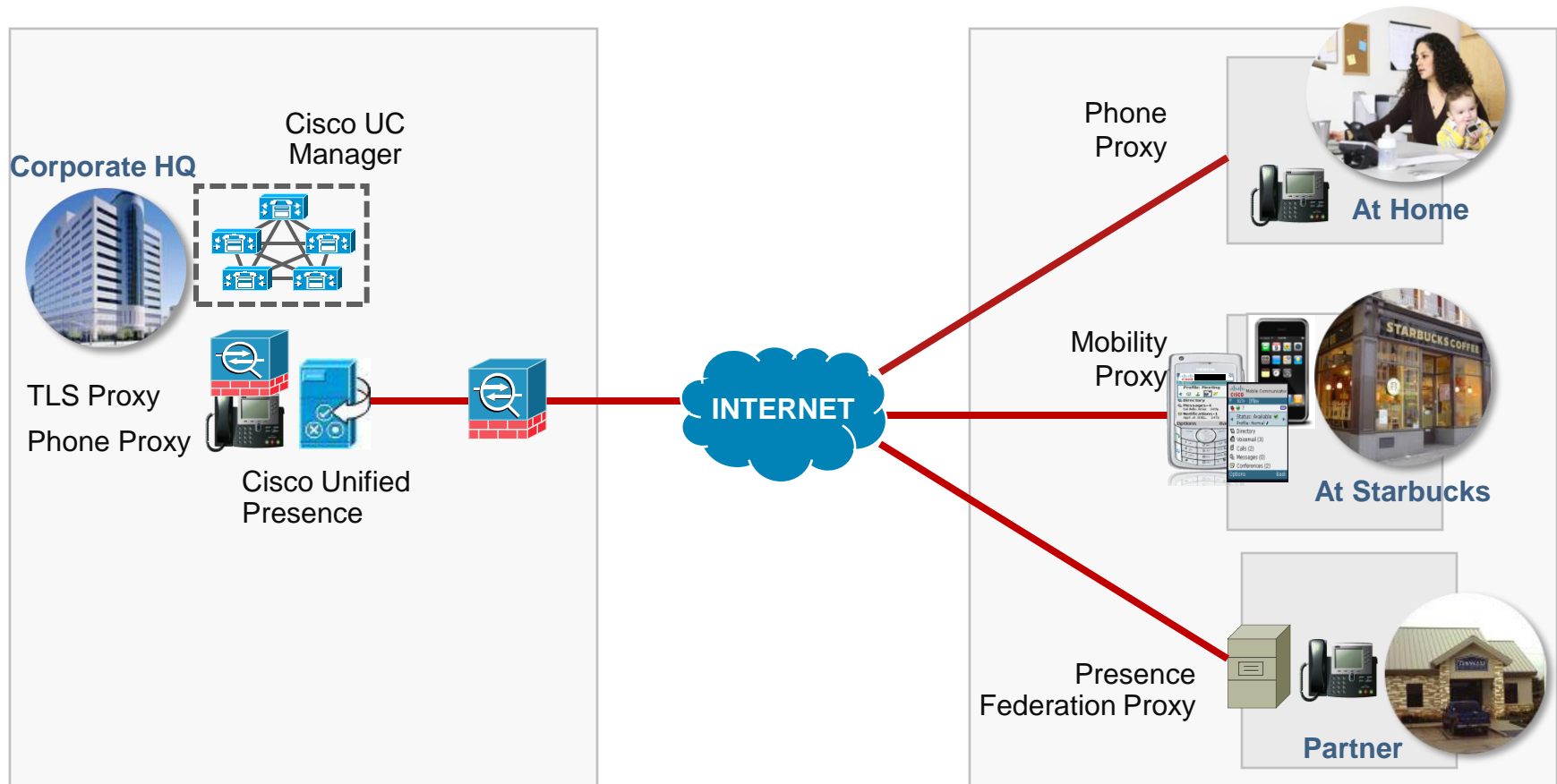
Secure Connectivity

Secure Unified Communications

Comprehensive Management

---

# ASA UC Deployments



## Call Control Security

- UC-Aware Firewall for protection of Cisco UC Manager
- TLS Proxy for inspection of encrypted calls
- Phone Proxy for VLAN traversal



## Perimeter Security

- Remote Access and Business-to-Business Security
- Connectivity for secure IP phones, mobile phones



# Call Control Security



# Cisco Unified Communications Manager

Protecting Your Most Important Asset



## How Much Does Telephony Downtime Cost If....

You cannot dial 112

Your call center is down

You cannot make a sales call

A confidential call is intercepted

# Cisco UC Manager Security

Defense In-Depth Security with UC-Aware Firewall



# Cisco ASA UC Security Features

Inspection of SIP, SCCP, MGCP, H.323  
Inspection of encrypted traffic  
Dynamic port opening

Protocol Conformance  
Malformed packets & state checks  
DOS prevention  
IPS UC Signatures

## Access Control



## Threat Prevention



## Policy Enforcement



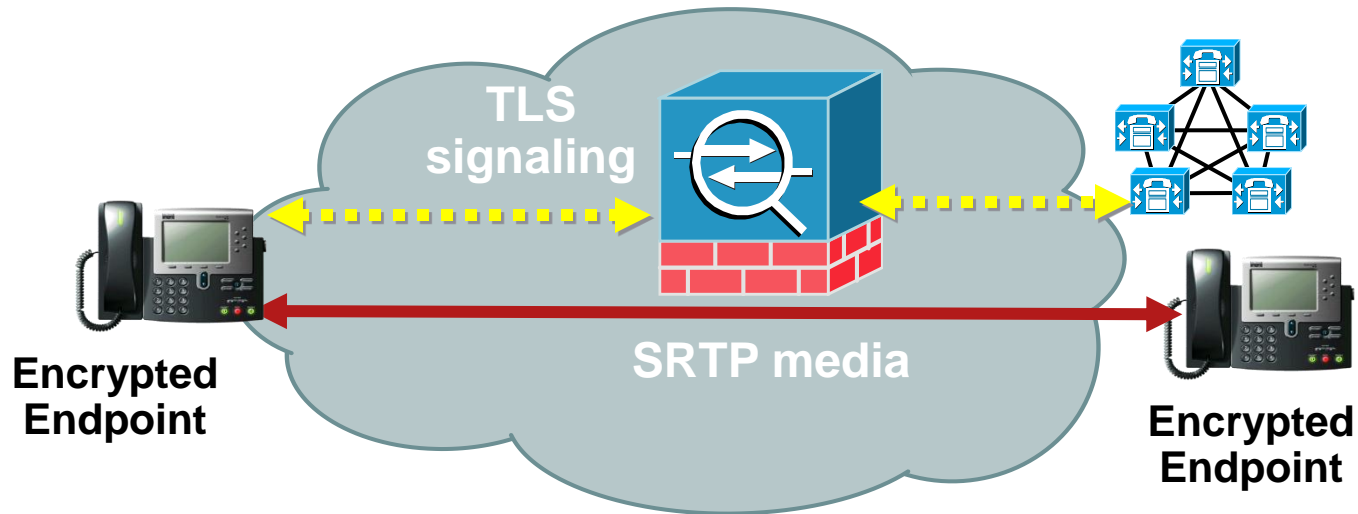
## Remote Access

Whitelist, Blacklists, Caller/Called ID  
SIP URI  
SIP Services

UC-Optimized VPN  
Phone Proxy  
Mobility Proxy  
Presence Federation Proxy

# ASA TLS Proxy

## Industry-First Firewall Inspection for Encrypted Voice

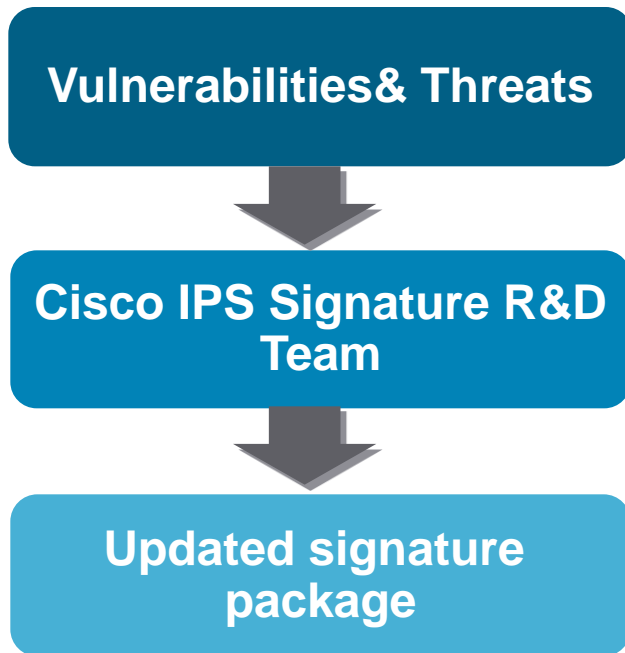


**Any Cisco voice/video communications encrypted with SRTP/TLS can now be inspected:**

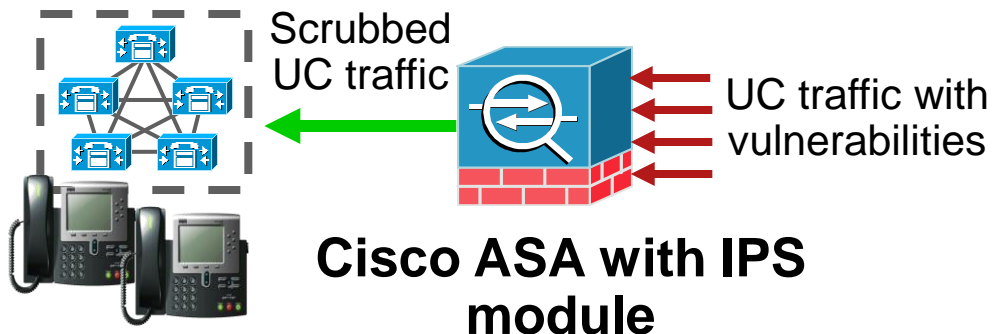
- **Maintains integrity and confidentiality** of call while enforcing security policy through advanced SIP/SCCP firewall services
- **TLS signaling is terminated and inspected**, then re-encrypted
- **Dynamic port is opened for SRTP encrypted media stream**, and automatically closed when call ends

# Cisco IPS UC Signatures

Supported on ASA IPS Module

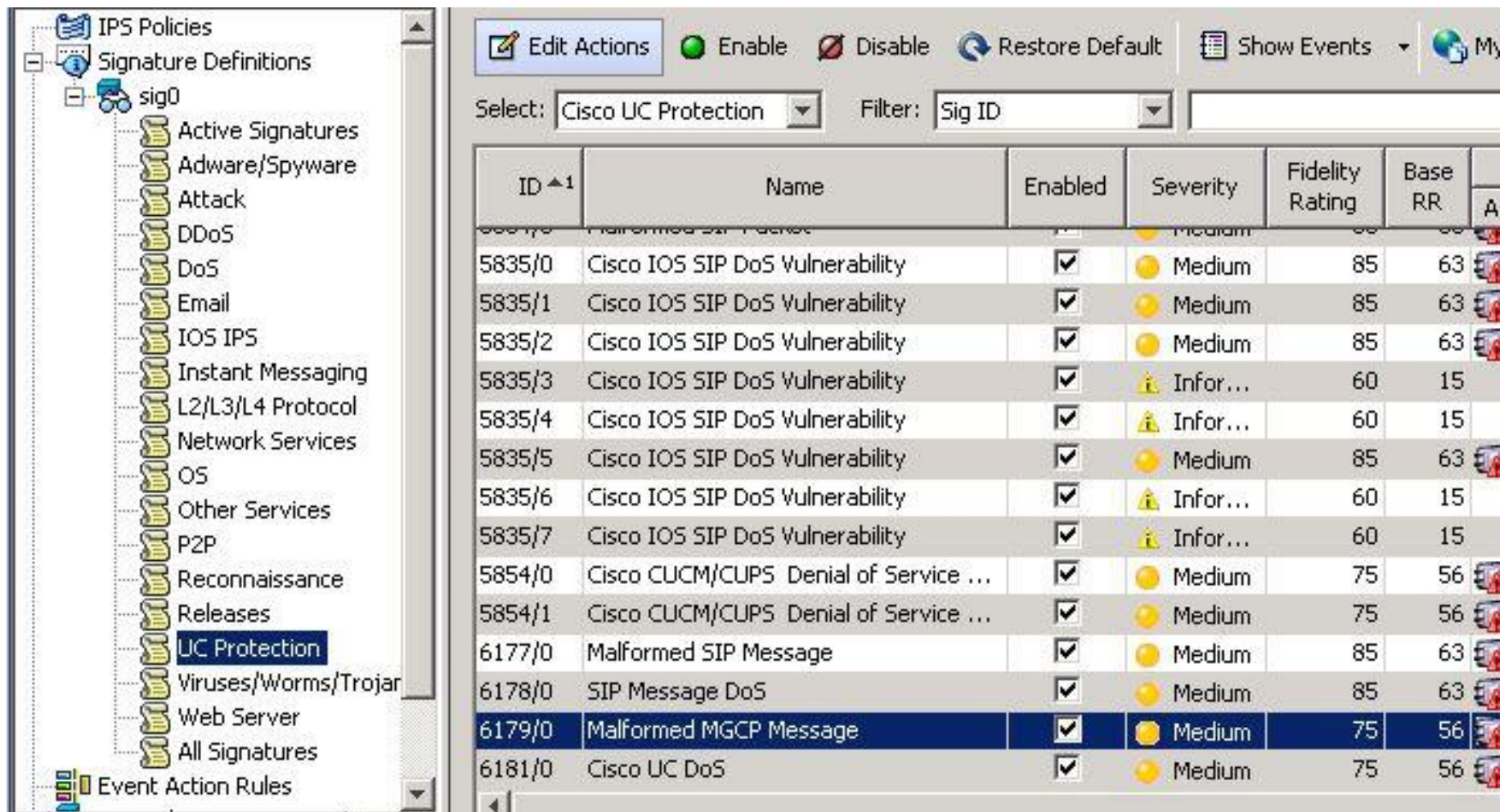


- First Layer of Defense for Cisco Unified Communications Manager
- Signatures created within hours of classification
- Benefits:
  - Target known vulnerabilities
  - Flexibility in patching
  - Faster Response
  - Optimize performance



# Cisco IPS UC Signatures

## Supporting Cisco UC Manager and UC Manager Express



The screenshot displays the Cisco IPS configuration interface. On the left, the 'Signature Definitions' tree is expanded, showing the 'UC Protection' category selected. The right pane shows a list of signatures with the following columns: ID, Name, Enabled, Severity, Fidelity Rating, Base RR, and A. The 'Cisco UC Protection' filter is applied, and the 'Sig ID' filter is set. The table lists various signatures, including 'Cisco IOS SIP DoS Vulnerability', 'Cisco CUCM/CUPS Denial of Service', and 'Malformed MGCP Message'.

ID	Name	Enabled	Severity	Fidelity Rating	Base RR	A
5835/0	Cisco IOS SIP DoS Vulnerability	✓	Medium	85	63	
5835/1	Cisco IOS SIP DoS Vulnerability	✓	Medium	85	63	
5835/2	Cisco IOS SIP DoS Vulnerability	✓	Medium	85	63	
5835/3	Cisco IOS SIP DoS Vulnerability	✓	Inform...	60	15	
5835/4	Cisco IOS SIP DoS Vulnerability	✓	Inform...	60	15	
5835/5	Cisco IOS SIP DoS Vulnerability	✓	Medium	85	63	
5835/6	Cisco IOS SIP DoS Vulnerability	✓	Inform...	60	15	
5835/7	Cisco IOS SIP DoS Vulnerability	✓	Inform...	60	15	
5854/0	Cisco CUCM/CUPS Denial of Service ...	✓	Medium	75	56	
5854/1	Cisco CUCM/CUPS Denial of Service ...	✓	Medium	75	56	
6177/0	Malformed SIP Message	✓	Medium	85	63	
6178/0	SIP Message DoS	✓	Medium	85	63	
6179/0	Malformed MGCP Message	✓	Medium	75	56	
6181/0	Cisco UC DoS	✓	Medium	75	56	



# Perimeter Security



# Growth in Remote Workers

- Teleworker population expected to grow to 112 million\* by 2011, with a CAGR of 4.3%
- Corporate teleworking: individuals who spend at least 1 day a week or a month working from home
- Growth influenced by:
  - Increased pressure by employees for flexible working options
  - Environmental pressure
  - Rising price of fuel
  - Reduction in TCO for equipment and services required for secure remote access
  - Collaborative Applications

Source: Gartner May 2007 Report, "Dataquest Insight: Teleworking, The Quiet Revolution (2007 Update)"

\* For workers who work from home at least 1 day a month

# Secure Remote Access

Technical Challenges – Data to UC enabled remote access



## Demands on Secure Connectivity Today

- Seamless user experience
- Access to a variety of applications including UC and collaboration tools
- Consistent access from a number of diverse clients (IP Phones, Mobile, Laptop)

User Expectations



### Increased Mobility

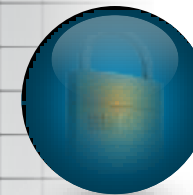
-Digital nomads, full-time remote employees, teleworkers



### Device Proliferation

-iPhone, Windows Mobile, Android

-Thin Client/ Embedded



### Platform Diversification

-Windows, MacOS, Linux

Device Proliferation

# Cisco ASA Secure Remote Access

One Solution for Diverse Remote Access Needs

IPsec VPN



Clientless  
VPN



SSL VPN



UC Proxy



Mobile VPN



Powered by the Cisco ASA

# Cisco ASA UC Security Features

SIP, SCCP, MGCP, H.323

Dynamic port opening

Encrypted traffic Inspection (TLS Proxy)

Protocol Conformance

Malformed packets & state checks

DOS prevention

IPS UC Signatures

## Access Control



## Threat Prevention



## Policy Enforcement



## Remote Access



Whitelist, Blacklists

Caller/Called ID

SIP URI

SIP Services

UC-Optimized VPN

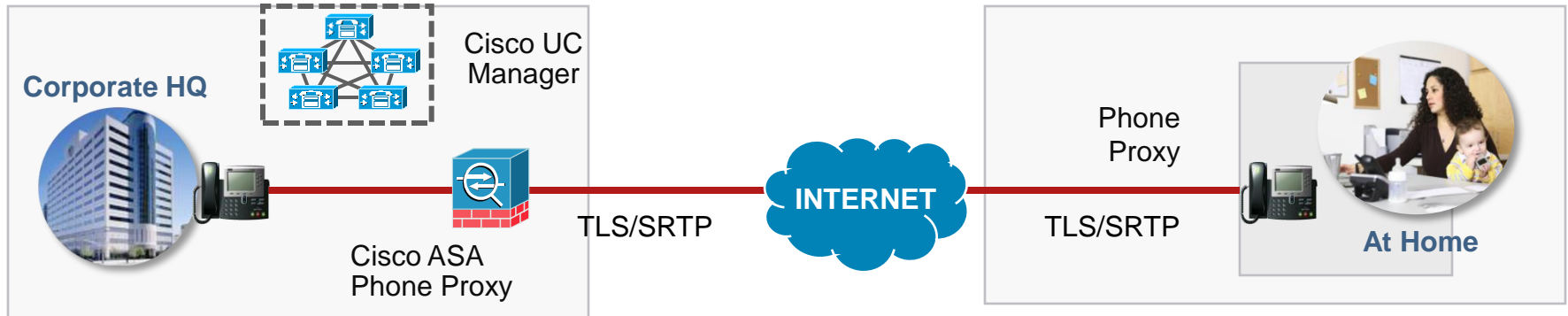
Phone Proxy

Mobility Proxy

Presence Federation Proxy

# ASA Phone Proxy

## Secure Communications For Cisco IP Endpoints

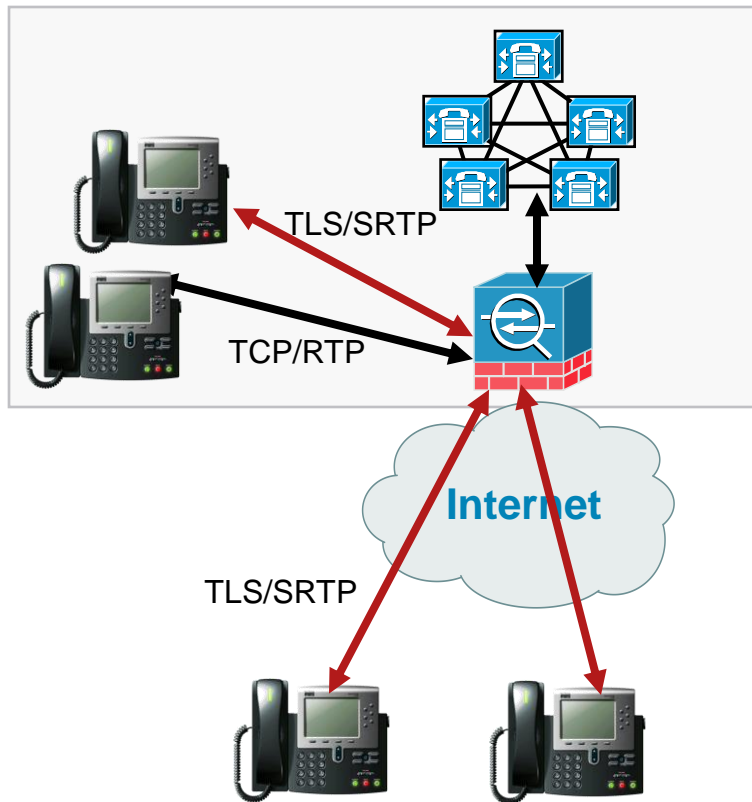


- Direct secure connectivity between phones and corporate Cisco UC Manager through ASA
- Secure Communications without VPN Remote Access device
  - Secure RTP for media/voice conversation
  - Transport Layer Security (TLS) for signaling
  - Option to Reencrypt communications inside network

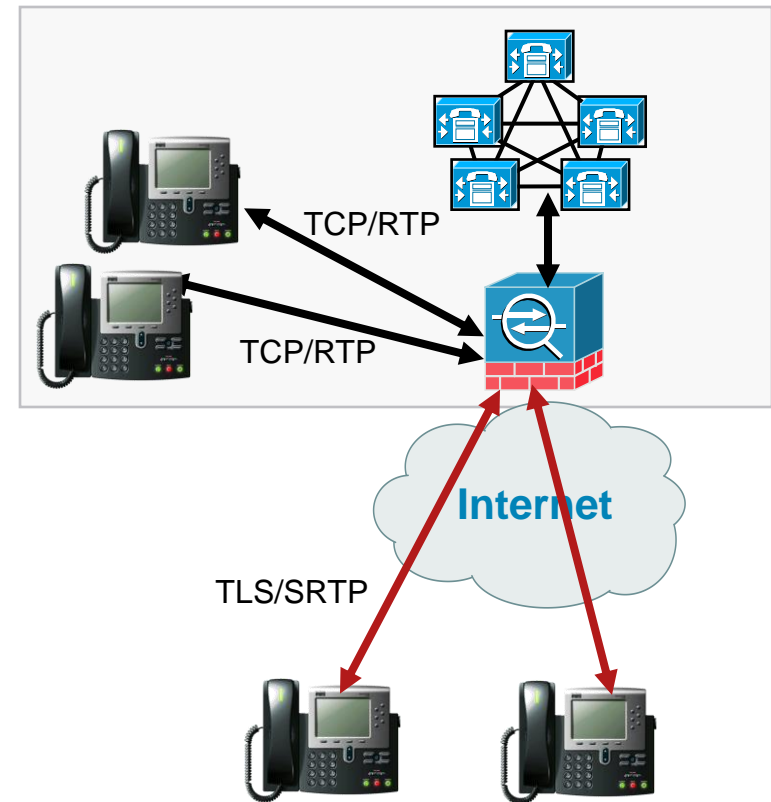
# Phone Proxy Deployment Scenarios

## Cisco UC Manager Clusters

### Mixed Mode UC Manager Cluster ASA 8.2



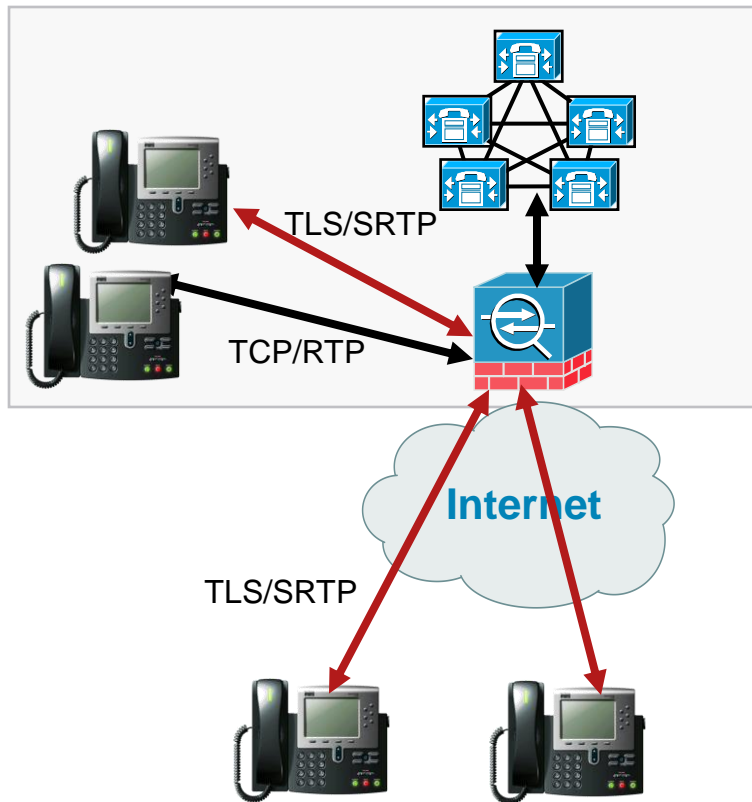
### Non-Secure CUCM Cluster ASA 8.04



# Phone Proxy Deployment Scenarios

## Firewall Deployments – ASA Perimeter Security Appliance

### ASA As Perimeter Firewall

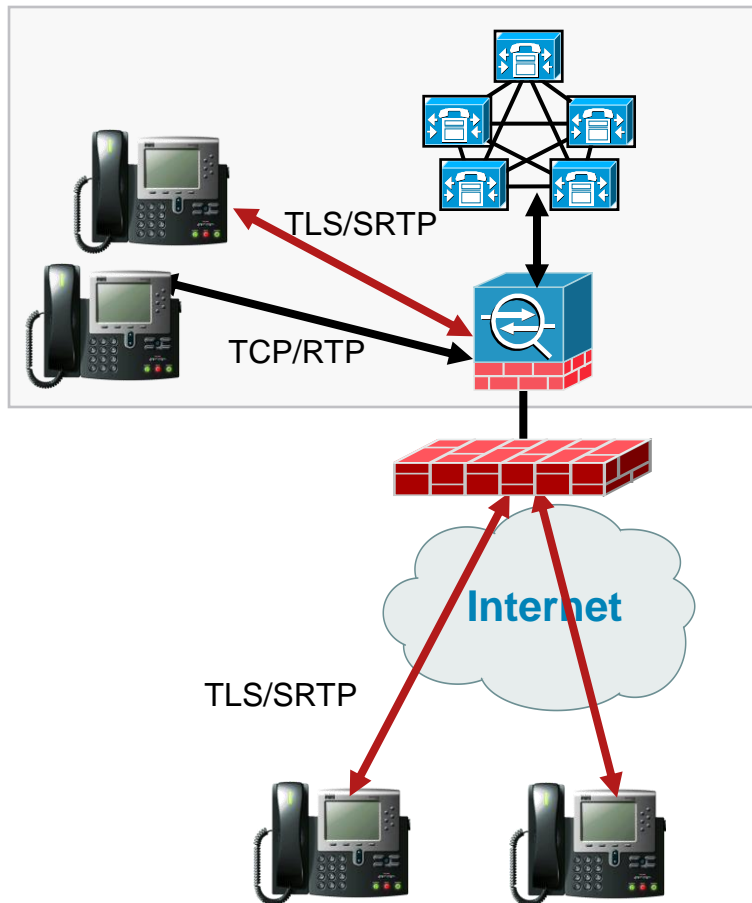


- Ideal for optimizing perimeter security function
- ASA Provides:
  - Phone proxy capability for phones
  - SIP/SCCP inspection on phones traffic
  - Optional SSL/IPsec VPN concentrator
- ASA Details:
  - Publicly routable IP address
  - Configure Interface PAT for TFTP Server
  - Remote IP phones point to the ASA
  - Media termination address can be configured per interface
  - ASA provides config and CTL file

# Phone Proxy Deployment Scenarios

## Firewall Deployments – ASA Behind Existing Firewall

### ASA As Phone Proxy Behind Existing Firewall



- Ideal for maintaining existing security infrastructure
- Existing firewall:
  - Must send packets to the ASA phone proxy
  - Open ports– TCP (SSL, TLS), UDP (SRTP, TFTP)
  - MUST NOT enable NAT - ASA must handle NAT for embedded and external IP address for phones
- ASA Details:
  - Optional SCCP/SIP inspection on phone traffic
  - NAT embedded and external IP address for phones
  - ASA provides config and CTL file

# Cisco ASA Phone Proxy Features

- **Call Control Supported**

Cisco Unified Communications Manager 4.x and higher  
Cisco UC Manager Express (IOS 12.4.20T2 – UCME 7.0/4.3)



- **Endpoint Support**

SIP and SCCP phones  
Cisco IP Phones (Must be TLS/SRTP-capable)  
Cisco IP Communicator support is roadmapped  
Cisco Unified Personal Communicator not supported  
Wireless LAN Phones (IP Phone 7921 etc) – SCCP only  
Supports more than one endpoint per remote location (behind home office router)

- **Device authentication**

X.509 Certificates

- **Supported on all Cisco ASA platforms:**

Cisco ASA 5505, 5510, 5520, 5540, 5550 – ASA 8.0.4  
Cisco ASA 5580 – ASA 8.2

- **ASA Stateless failover:**

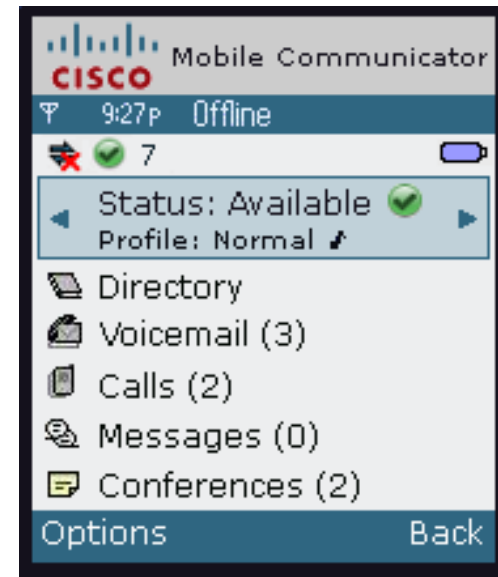
Failover pair syncs up with all the configurations, keys, certificates  
Active sessions are not replicated.

# End-User/Phone Provisioning

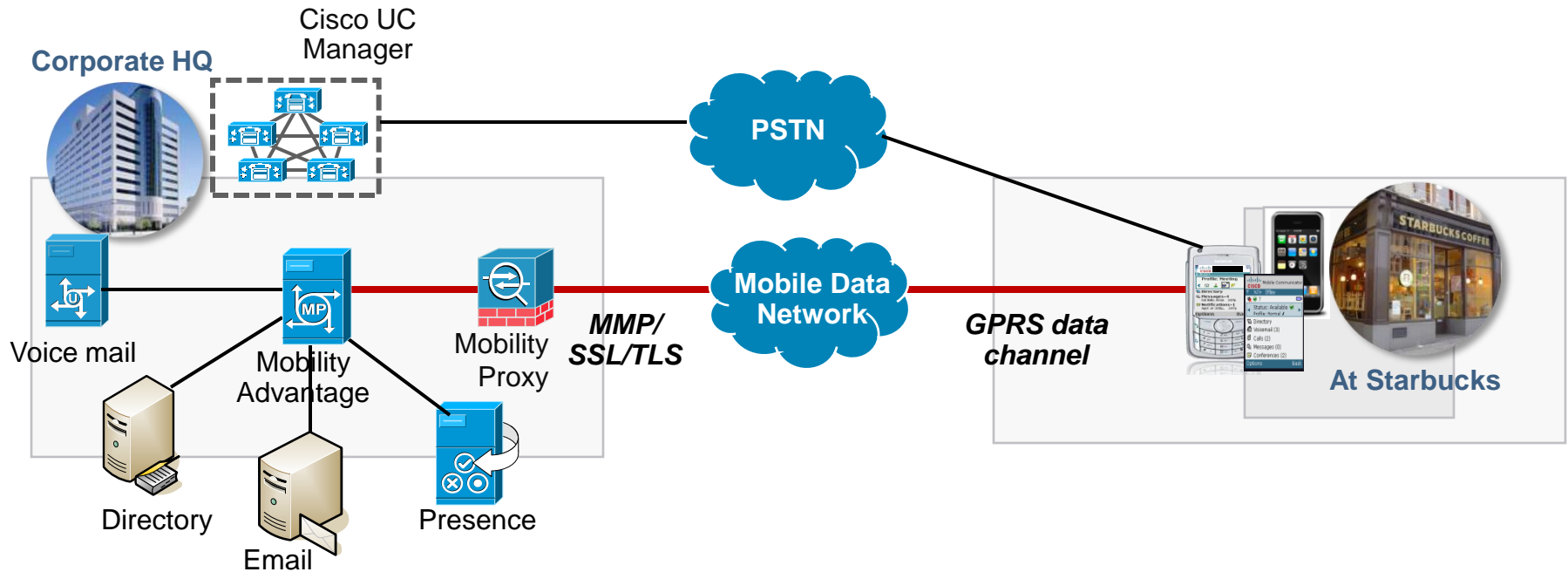
- **Option 1– Stage phones at HQ before sending to end user**
  - Phones register inside the network, and proxy to ASA.
  - IT ensures no issues with phone configs/registration.
  - Phone registers inside the network to Cisco UC Manager
  - CTL file is erased before sending to end user
- **Option 2 – Send brand new phone to end user**
  - User must be provided instructions to change the settings on phones with the appropriate TFTP server IP address
- In both options:
  - Deploying a remote IP Phone behind a commercial Cable/DSL router with NAT capabilities is supported.
  - Most modern DSL routers should provide minimal functionality out of the box
  - For the best audio experience, the router must support UDP port forwarding

# Cisco Unified Mobility Solution

- Extends unified communications to mobile phones
- Intuitive, common user experience across different mobile handsets
  - Presence enabled directories
  - Single business number reach
  - Enterprise voicemail notification and playback
  - Enterprise Call logs
  - Conference notifications
  - Secure Text messaging
- Preserves enterprise flexibility and user choice
  - Support for BlackBerry, Symbian OS and Windows Mobile
  - Support for multiple mobile operators and networks

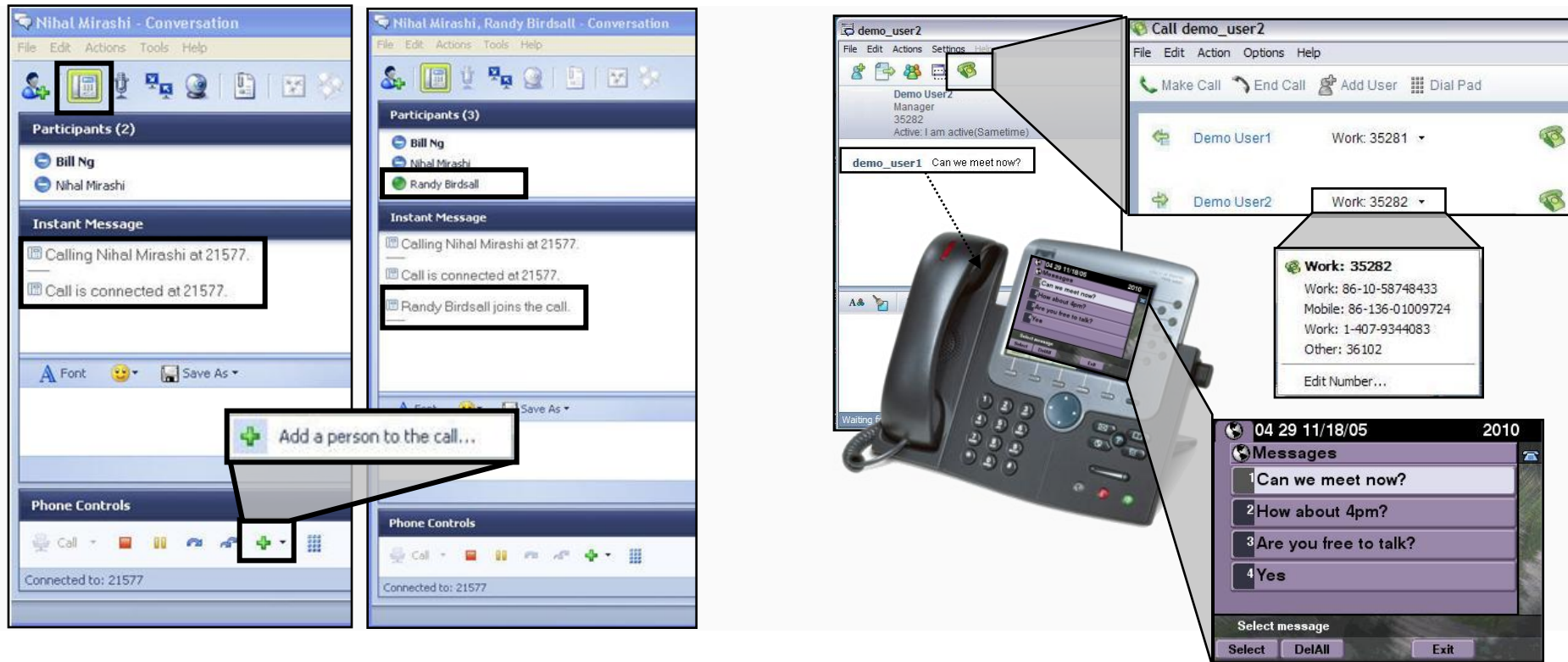


# ASA Mobility Proxy



- Businesses can now extend their communications to mobile endpoints
- ASA mandatory within Unified Mobility architecture
- ASA Mobility Proxy:
  - Terminates encrypted mobility signaling
  - MMP Inspection Engine validates traffic, performs protocol conformance
- Supported with Cisco Unified Communications Manager/Mobility 7.0

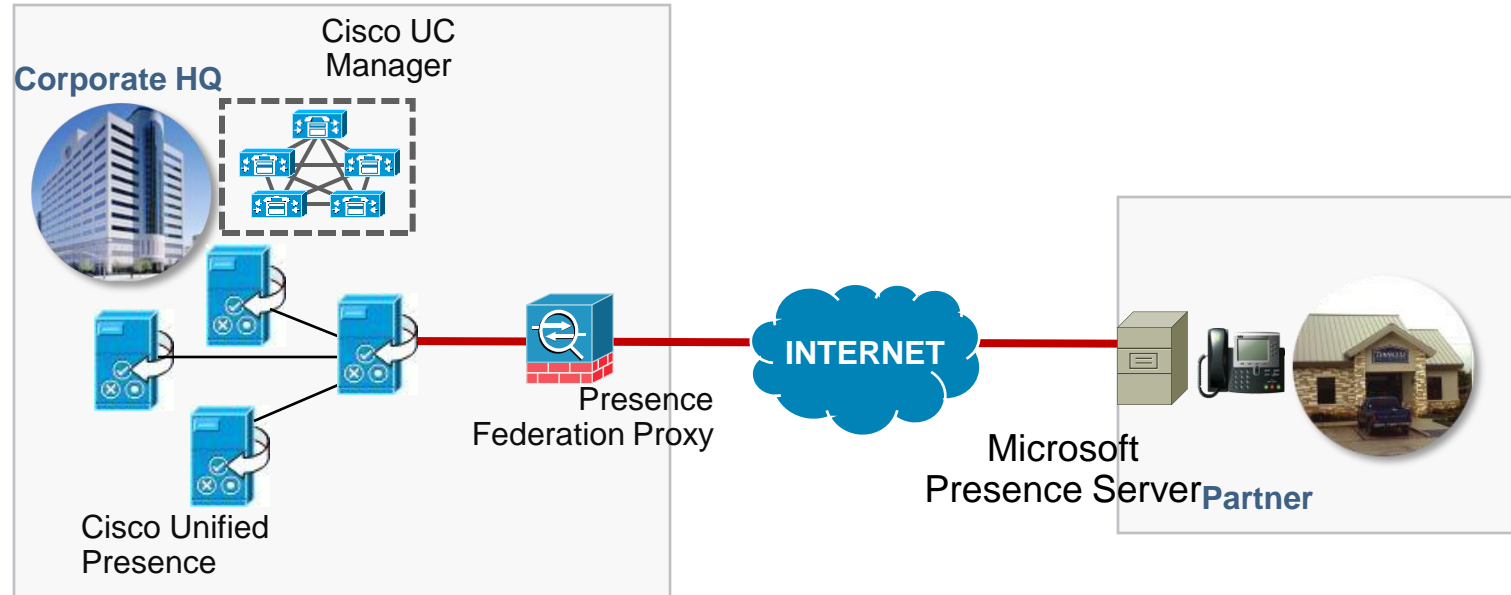
# Cisco Unified Presence Solution



- Integrate communications with PC applications
- Information about a person's willingness and availability to communicate
- Examples of presence in action today

IM "Buddy List" status indication, "Busy" tone on traditional phone, Contact Center Agent status

# ASA Presence Federation Proxy

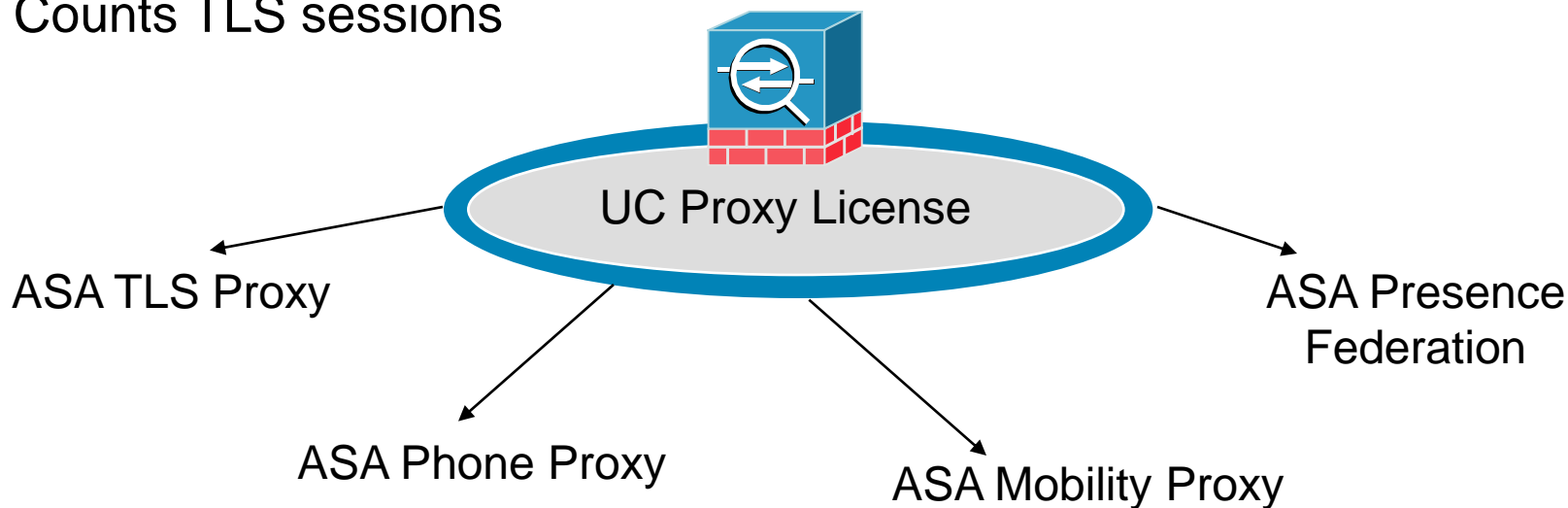


- Businesses with Cisco UC Presence solutions can now federate and share presence information with other businesses
- Federation supported between Cisco and Microsoft
- ASA secures inter-enterprise presence federation
  - Terminates encrypted SIP signaling
  - SIP inspection engine performs access control and policy enforcement
  - Supported with Cisco Unified Communications Manager/Presence 7.0

# ASA UC Proxy Licensing

## Enables Proxy Functions

- Cisco ASA UC Proxy Licensing enables ASA for TLS proxy, phone proxy, mobility proxy and presence federation deployments
- Mix and match as appropriate
- Counts TLS sessions





# Scalability and Licensing



# Cisco ASA and Secure UC Scalability

- Extensive performance testing with Cisco CallManager
- How much firewall do I need?

Firewall	Phones
ASA 5505	Position for SMBs, small enterprises, teleworker
ASA 5510	Position for SMBs, small enterprises
ASA 5520	500-5,000 phones
ASA 5540	5000-15,000 phones
ASA 5550	15,000-30000 phones
ASA 5580-20	30000-60000 phones
ASA 5580--40	60000 – 130000 phones

- Numbers assume:

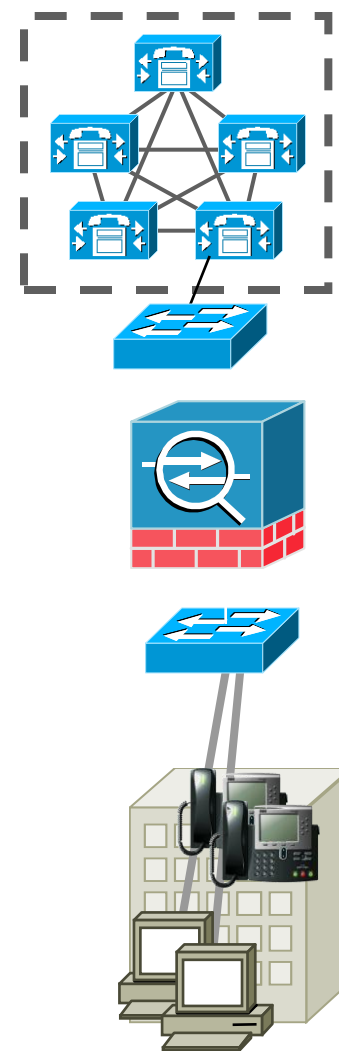
Endpoints are SIP or SCCP

Nat configuration used

CPU below 60% to protect against jitter and latency

Assumes 10% active calls (example – ASA 5550 supports 3000 calls)

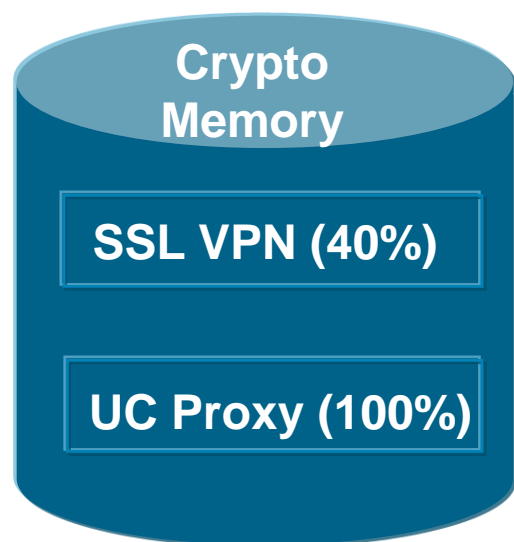
G.711 ulaw codec



# Cisco ASA and Secure UC Scalability

	UC Proxy Sessions*	Software Release Availability
ASA 5505	24	ASA 8.0.4
ASA 5510	100	ASA 8.0.4
ASA 5520	1000	ASA 8.0.4
ASA 5540	2000	ASA 8.0.4
ASA 5550	3000	ASA 8.0.4
ASA 5580	10,000 for TLS Proxy, Mobility Proxy, Presence Federation Proxy  5,000 for Phone Proxy	ASA 8.2(1)

# Cisco ASA and Secure UC Scalability



- **UC Proxy and SSL VPN will consume the same set of crypto memory resources**

**1 UC Proxy session ~ 2.5 SSL VPN sessions**

- **Example: ASA 5520**

**User wants to deploy 800 UC Proxy sessions**

**How many SSL VPN users can be deployed?**

Max UC Proxy Capacity on 5520	1000 sessions
Max UC Proxy sessions used	800 sessions
Capacity Left	200 sessions
Translating this to SSL VPN	$200 * 2.5 = 500$ SSL VPN

# Max UC Proxy Sessions

Appliance	Max UC Proxy Sessions
Cisco ASA 5505	24
Cisco ASA 5510	100
Cisco ASA 5520	1000
Cisco ASA 5540	2000
Cisco ASA 5550	3000
Cisco ASA 5580 (available with 8.2)	10000 – TLS, Mobility, Presence Federation Proxy 5,000 - Phone Proxy

# Summary

- Security remains a top of mind for many Unified Communications customers
- The secure data network is the foundation... Unified Communications security should be an incremental leverage
- Cisco ASA is the premier security appliance for Unified Communications security
- ASA Unified Communications Proxy features enable businesses to securely collaborate and extend communications to remote and mobile users

# Useful Links

- ASA Website:

[www.cisco.com/go/asa](http://www.cisco.com/go/asa)

UC Proxy Licensing at a glance:

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/at\\_a\\_glance\\_c45-509624.pdf](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/at_a_glance_c45-509624.pdf)

UC Security Datasheet

[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product\\_data\\_sheet0900aecd8073cbbf.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd8073cbbf.html)

- Secure UC Solutions page:

[www.cisco.com/go/secureuc](http://www.cisco.com/go/secureuc)

