



# Demystify CUCM Security



**Jerry de Boer**  
Consulting Systems Engineer  
UC & Collaboration TCMO Europe

# What's this session all about?

- Answers to never-ending stream of requests from customers for more detail
- Based on actual customer queries
- Reduce time to RFP/RFI responses
- Cover what exists today in Unified CM 7.0(1)
- When important, mention futures
- Focus on Unified CM and underlying operating system
- A chance to ask me anything, about security

# What This Presentation Is Not

- Rehashing of CAPF, CTI, SRTP, TLS, phone settings
- Designed to explain Unified CM fundamentals
- Applicable to Unified CM <4.3(2)
- Roadmap of security features
- Primer on security principles or protocols
- Guidebook for evildoers

# Securing Cisco UC – layered approach

- Securing the ‘box’
- New Infrastructure Features
- Endpoint Security

# Securing the 'Box'



# User Types

## Platform User

- Accounts in */etc/password*
- Salted MD5 hashed passwords in */etc/shadow*
- Unique 8-byte salts
- Username = [a-zA-Z0-9\-\\_\.\]{1,32}
- Password = .{6,99}
- Cracklib used to enforce complexity
- Inactivity timeout set to 30 minutes
- No lockout, expiration, password history, etc.
- Case-sensitive username
- Username stored in cleartext

## Application Users

- Accounts in *applicationuser* table
- AES-128-CBC encrypted password in *applicationuser* and *credential* tables
- Username = [a-zA-Z0-9\-\\_\.\]{1,50}
- Password = .{5,127}
- Credential Policies are used
- Inactivity timeout 30 minutes
- Case insensitive username
- Username stored in cleartext

## End Users

- Accounts in *enduser* table
- Salted SHA-1 hashed password and PIN in *credential* table
- Salts are all unique
- Username = [a-zA-Z0-9\-\\_\.\]{1,50}
- Password = .{5,127}
- Credential Policies are used
- Inactivity timeout 30 minutes
- Case insensitive username
- Username stored in cleartext

## Remote Support User

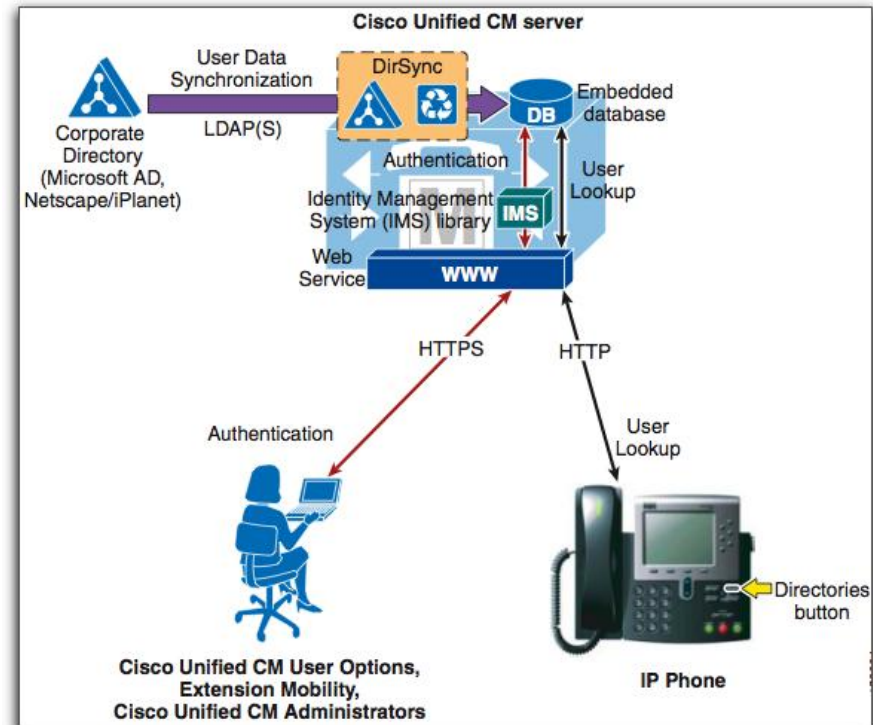
- Accounts in */etc/password*
- Salted MD5 hashed passwords in */etc/shadow*
- Unique 8-byte salts
- Username = [a-z]{6,30}
- Password = [0-9A-Z]{10}
- Expiration from 1 to 30 days
- Inactivity timeout 30 minutes
- No lockout, password history, etc.
- Case-sensitive username
- Username stored in cleartext

# Certificates

- Completely managed from Unified OS Administration
- Can be viewed from Unified OS CLI or Administration
- 1024-bit RSA Public Keys, digital signatures use SHA-1 with RSA
- Self-signed by default, but can be signed by third-party
- CN can be manipulated by modifying CUCM hostname
- SAN can be defined for Tomcat certificate in future release
- No management access to keys and no key passphrases
- No revocation support
- *show ctl* on Unified OS CLI
  - Displays envelope information about CTL certificates
  - Extracts certs to tftp section of filesystem

# LDAP User Sync and Authentication

- Just for End Users, but not their PINs
- Distinguished Name passwords in AES-128-CBC
- Credential policies for password handled by directory, PIN is still in Unified CM DB
- Existing users are deleted if not in directory
- Authentication success/failure in `/syslog/CiscoSyslog`, detail in `/tomcat/logs/security/log4j/securityNNNNN.log`
- Deleting account in AD doesn't change acct status till resync for PIN if doing LDAP authentication



# Network-related Security Measures



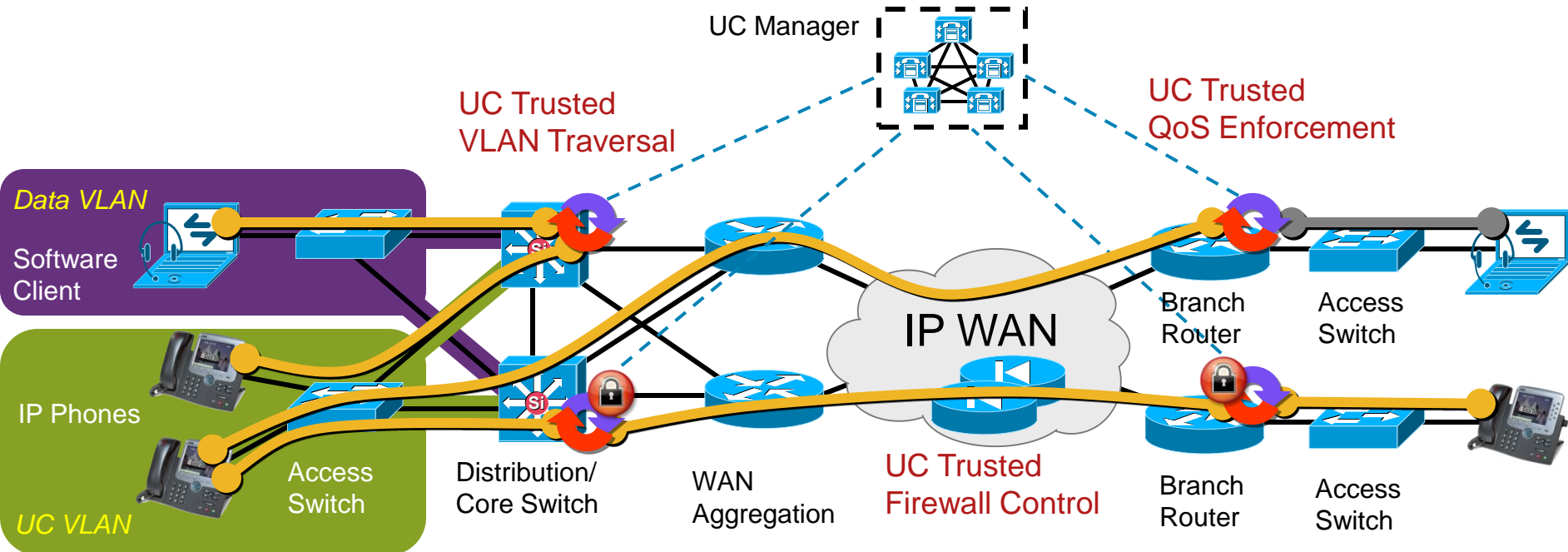
# Host Firewall Overview

- Restrict IPv4 traffic to and from the server
- Dynamic rules define the behavior of the firewall
- Uses cluster node list maintained by Cluster Manager
- ipprefs is new service that updates firewall

# Host Firewall Rules

- All localhost traffic is allowed
- All outgoing traffic is allowed
- All established connections are allowed
- All ICMP traffic is allowed, but rate-limited to 10/sec with 5 burst
- All other traffic is dropped
- “utils firewall list” from Unified OS CLI

# Trusted Relay Point (TRP) Overview



- Software function that runs on Cisco network devices such as campus switches and routers (*similar to an MTP*)
- Inserted in the call flow by CUCM 7.0 (or CUCME 4.0) based on config
- Provides **trusted** anchoring point for media to enable several functionalities (QoS enforcement, Trusted VLAN traversal, ...)



# Unified IP Phones Security



# Signing & Encryption

## FIRMWARE

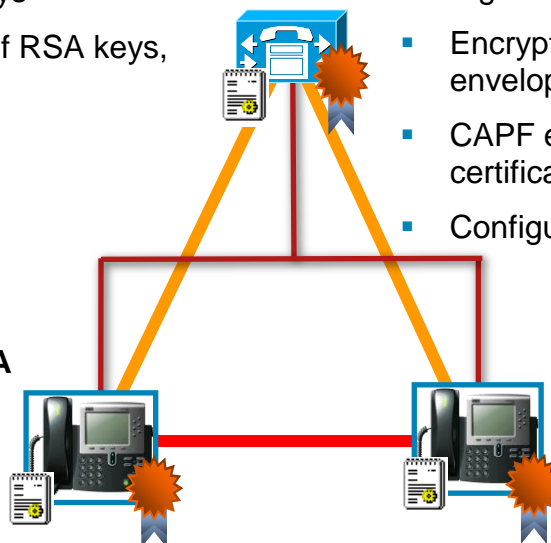
- Firmware + Envelope + Signature
- Signature is RSA 2048 Encrypted SHA-1 hash of firmware and envelope
- Contains primary and backup public keys
- Each phone model uses different pair of RSA keys, sidecars share keys

## CONFIG

- Config contains sensitive information  
SSH credentials, SIP digest, IPs of voice network components, SRST certificate
- Signed using SHA-1, RSA-1024 from *callmanager cert*
- Encrypted using AES-128-CBC symmetric key in envelope
- CAPF extracts phone public key and stores with certificate
- Configuration update means new symmetric key

## SIGNALING & MEDIA

- SRTP
  - Authenticated using HMAC-SHA-1-32
  - HMAC adds 4 bytes to packet size
  - Encrypted using AES-128-CM
  - SIP – Both endpoints decide on their enc and auth SRTP keys
  - SCCP – CUCM picks enc and auth SRTP keys
- TLS
  - RSA-1024 with SHA-1 signature for Unified CM
  - RSA-512 -1024 -2048 with SHA-1 signature for phones
  - Encrypted using AES-128-CBC
  - Authenticated using HMAC-SHA-1



# 802.1x

- MD5 Supplicant, TLS supplicant is planned
- EAPOL-Proxy Logoff allows for PC behind phone to also use 802.1x
- CDP is not impacted by 802.1x
- Requires user for each phone in authentication server
- Each phone must be manually configured with shared secret

# Management



# Secure Management

- Backups

SFTP or tape drive

- HTTPS

SSL for IE 6/7

TLS for Firefox

- Secure Shell

SSH v2 only

Log level is INFO, sent to /syslog/secure

TCP Forwarding disabled

Supported encryption algorithms

aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr

# Logging

- Logs can be viewed from RTMT and Unified OS CLI
- Unified OS CLI allows users to delete and remote copy log files
- Invalid usernames, but not passwords are logged
- Logs of interest
  - /syslog/secure* – Unified OS creation of users, failed logins
  - /syslog/CiscoSyslog* – All web application login success and failures
  - /syslog/messages* – Service state changes
  - /syslog/csalog* – CSA deny and permit events
  - /syslog/csaupdate\_log* – Updates to CSA
  - /platform/log/certm.log* – Certificate monitoring
  - /platform/log/certMgmtNNNNN.log* – Certificate management from Unified OS CLI and Administration
  - /platform/log/authenticateFile.log*
  - /platform/log/cli.log* – Unified OS CLI activity
  - /platform/log/clustermgrNNNNNNNN.log* – HMAC keepalive errors
  - /platform/log/ipprefsd* – Firewall port registration activity
  - /platform/log/createaccount.log\_MM-DD-YYYY\_HH\_mm\_SS* – Creation of Remote Support Account
  - /platform/log/remote\_activity.log\_MM-DD-YYYY\_HH\_mm\_SS* – Activity of Remote Support Account
  - /syslog/cron* – Shows removal of Remote Support via hourly cron
  - /tomcat/logs/axl/log4j/axlNNNNNN.log* – All AXL queries
  - /tomcat/logs/security/log4j/securityNNNNNN.log* – All app and end user logins, only place to get car logins
  - /tomcat/logs/rbs/log4j/rbsaccessNNNNNN.log* – Actions from ccmadmin and ccmuser

# Key Takeaways

- Light has been shed on Unified CM security topics rarely discussed
- Unified CM uses a layered approach to security
- Secure UC is not just TLS/SRTP



# Host Firewall Configuration

- Each service registers ports with *ipprefs*
- Port types
  - Public ports – permit external clients
  - Private ports – permit cluster nodes
  - Translated ports – external port mapped to internal port
- Port must be enabled

# Host Firewall Management

- Disable

  - “utils firewall disable” from the CLI

  - Time limit from 5m to 24h

  - Automatically revert back

- Debug

  - “utils firewall debug” at the CLI

  - Log blocked packets

  - Entries rate-limited

  - /syslog/messages

# Host Firewall Leverages HMAC Keepalives

- Key is munged security password
- HMAC-SHA-1-120
- Cluster Manager maintains keepalives
- 8500/udp
- 3 minute timeout
- Sent every 10 seconds
- /platform/log/clustermgrNNNNNNNNN.log
- RTMT and /syslog/CiscoSyslog for alerts

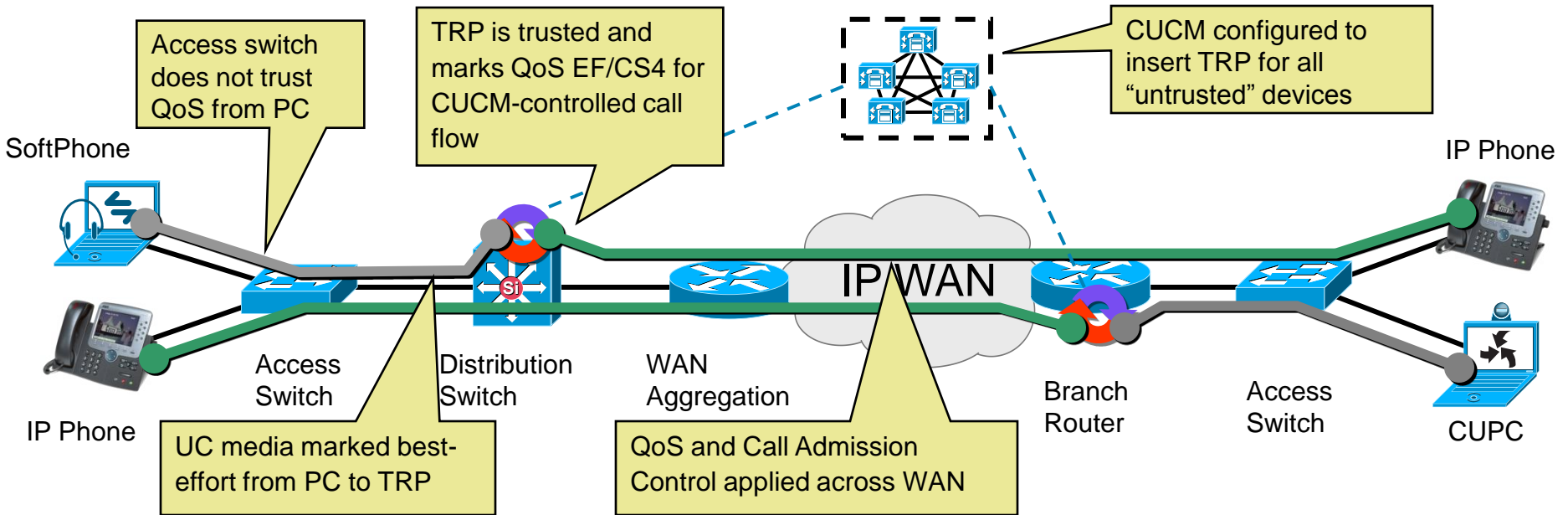
# Host Firewall Logs

- /platform/log/ipprefsd – log of daemon used to enable/disable ports during runtime
- /syslog/messages – firewall debug log
- /syslog/secure – will show changes to port information

# IPsec

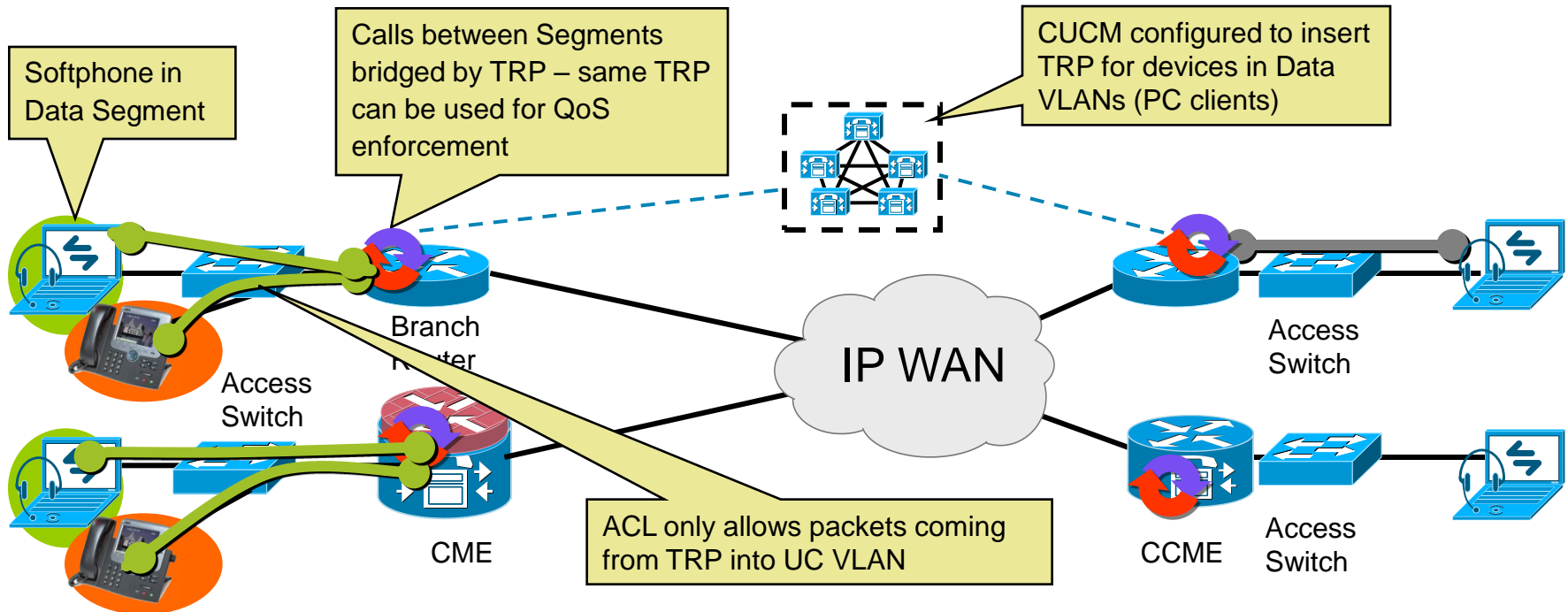
- Transport only, no tunnel mode
- Shared secret or certificate
- Can't be between cluster nodes, planned for future release
- Phase 1
  - Encryption = DES,3DES
  - Authentication = HMAC-SHA-1, HMAC-MD5
- Phase 2
  - ESP = Null,DES,3DES,Blowfish 448,RIJNDAEL (AES planned for future release)
  - AH = HMAC-SHA-1, HMAC-MD5
- Unified CM is configured to use aggressive mode if it is the initiator
- Allows either main or aggressive mode as a responder
- No requirement on pre-shared key complexity
- Pre-shared key and private key stored in clear text not accessible from any interface
- One certificate for all IPsec policies, CA certificates in *ipsec-trust*, CSR is supported for *ipsec* certificate

# UC-Trusted QoS Enforcement



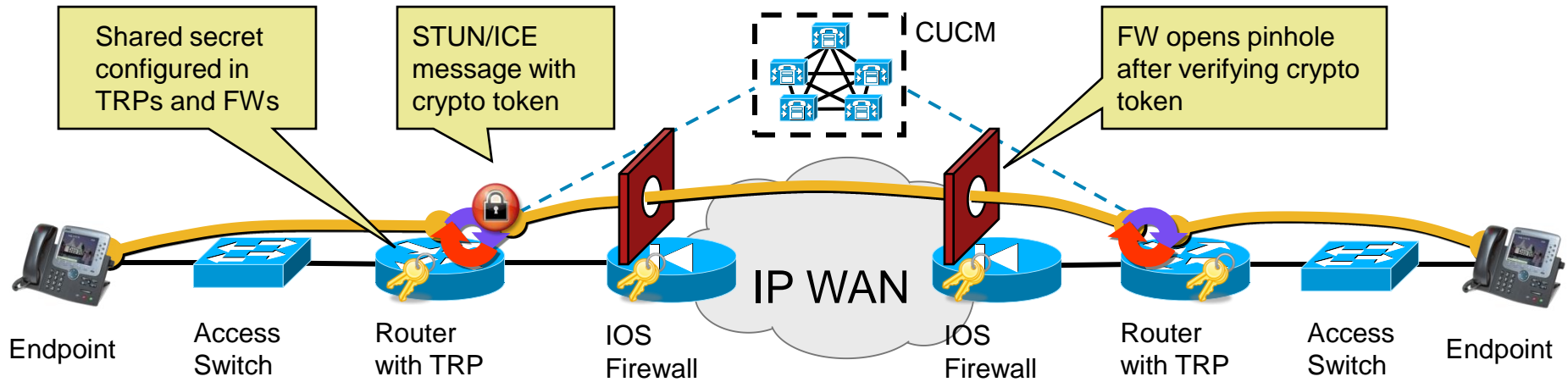
- Feature may be enabled for all “untrusted” endpoints that register to CUCM/CME (software-based, video, 3rd party, ...)
- To minimize number of MTPs involved in a call, ensure the same network device can perform all needed functions (TRP, RSVP Agent, Xcoder, ...)
- Use a plain MTP configuration on the router – no changes in router config. CUCM 7.0 allows “Use TRP” checkbox

# UC-Trusted VLAN Traversal



- TRP enables Secure IP Phone Connectivity by securely bridging only “authorized” (CUCM or CME) media from Data to UC VLAN
- TRP can also remark the QoS for “authorized traffic” from the Softphone
- CUCM 7.0 and CME 4.0 (12.4.9T)

# UC-Trusted Firewall Control



- Cisco UC cooperates with Cisco firewalls to enable trusted media control
- Innovative Cisco solution based on STUN/ICE standards
- Implemented on CME and IOS FW in 12.4.22T
- Future (roadmap) on CUCM and other Firewalls

# Alerting

- Syslog

CiscoSyslog – login failures at Critical for car, drf, ccmadmin, ccmservice, cmplatform (CallManager User Console Login), ccmuser, cucreports, cli, RTMT; login success for everything above except CLI at Informational; invalid HMAC or IP for keepalives

Secure syslog – login success and failure for CLI, console

Enterprise Param -> Remote Syslog Server – All Unified CM syslog events

- Certificate Monitor – E-Mail notification of certificate expiration
- SNMP Traps – Configured serviceability alarms
- Administrative actions are not alerted on