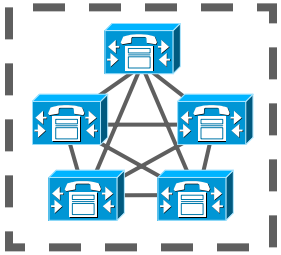
Cisco IP Telephony Security: Techniques to Protect Voice

Richard Dodsworth
Consulting Engineer
Cisco Systems, Singapore

Do You Know What a Phreaker (Voice) or a Hacker (Data) Looks Like?

- Attacks against IP Telephony endpoints
  - Reconnaissance
  - DHCP starvation
  - Eavesdropping/Man-in-the-middle
  - Directed TCP and ICMP attacks
- Attacks against IP Telephony servers
  - Worms, viruses and trojans
  - DoS and DDoS
  - Directed probes, floods
- Attacks against IP Telephony applications
  - Intercept administration and user traffic
  - Exploit programming weakness
  - Rogue servers
  - Toll fraud



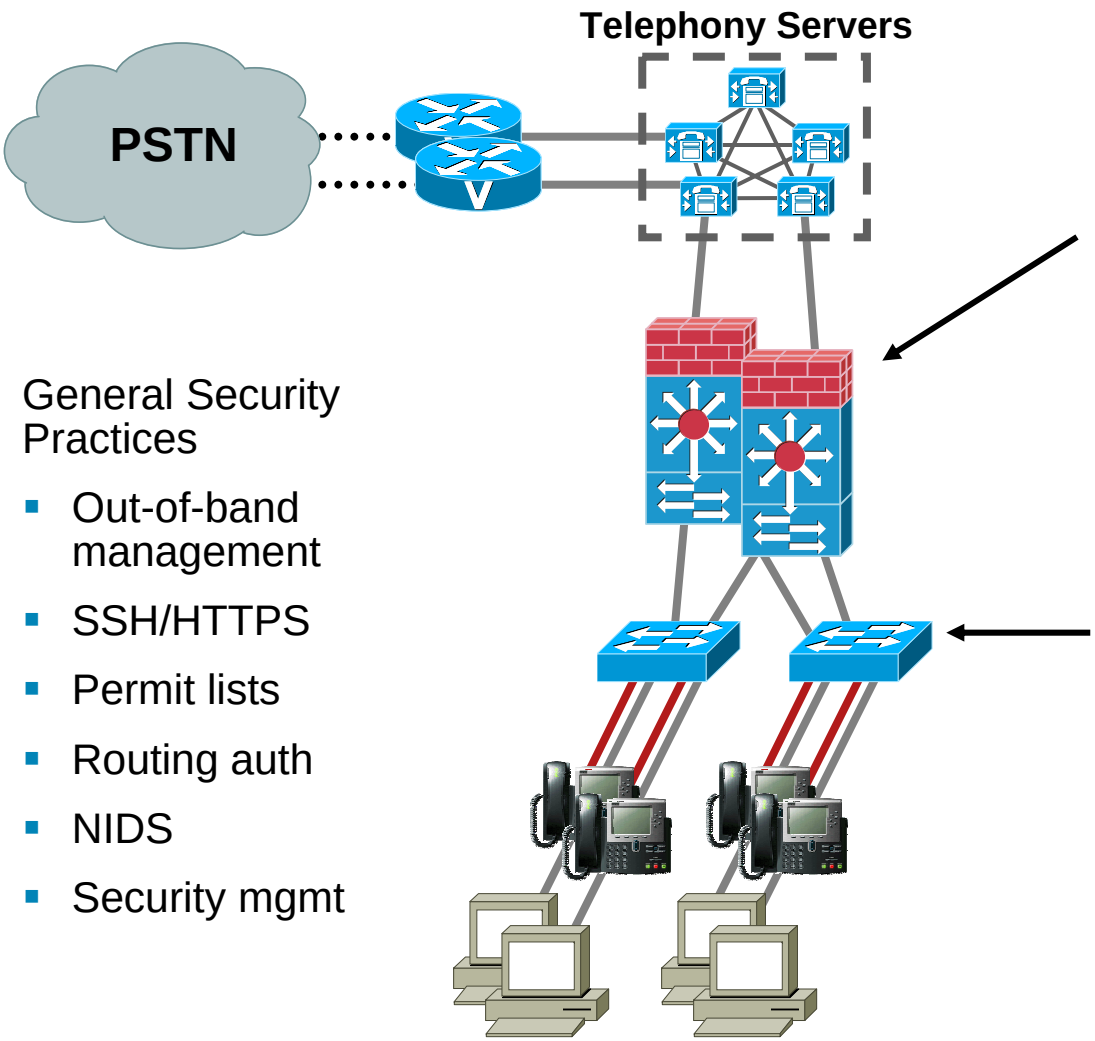
Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
- Protect IP Telephony Applications

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

Secure Voice by First Securing the Network



- Firewall or ACL in front of telephony servers
- Rate Limiting

  MicroFlow Policing in 6K

General Security Practices

- Out-of-band management
- SSH/HTTPS
- Permit lists
- Routing auth
- NIDS
- Security mgmt

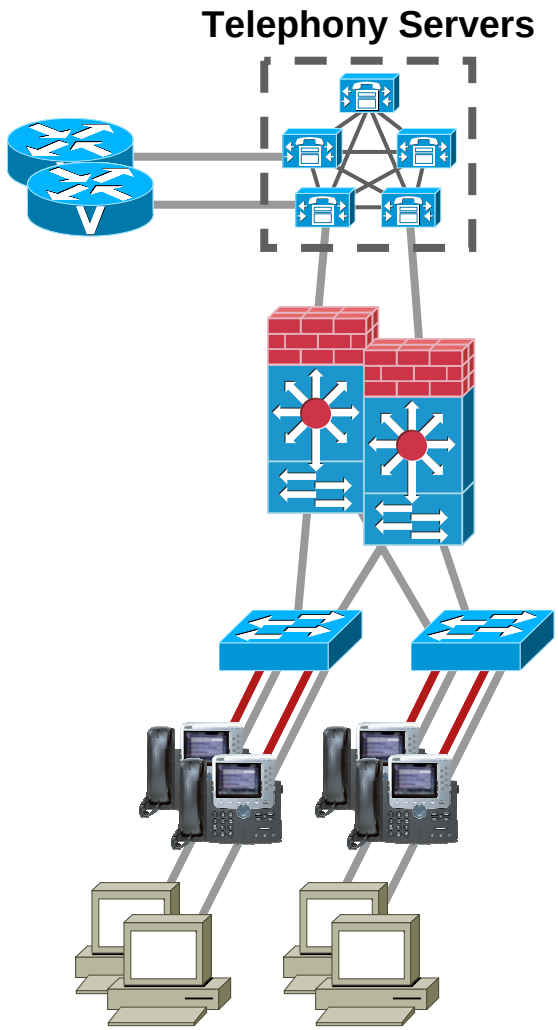
Catalyst Integrated Security Features (CISF)

- Separate voice & data VLANs
- VLAN ACLs (VACLs)
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- Scavenger-class QoS

Separate Voice and Data VLANs

VLAN Access Control Lists (VACLs)

- Phones only send signaling to servers and RTP to each other
- No reason to send TCP or ICMP to each other
- Stops TCP and ICMP attacks

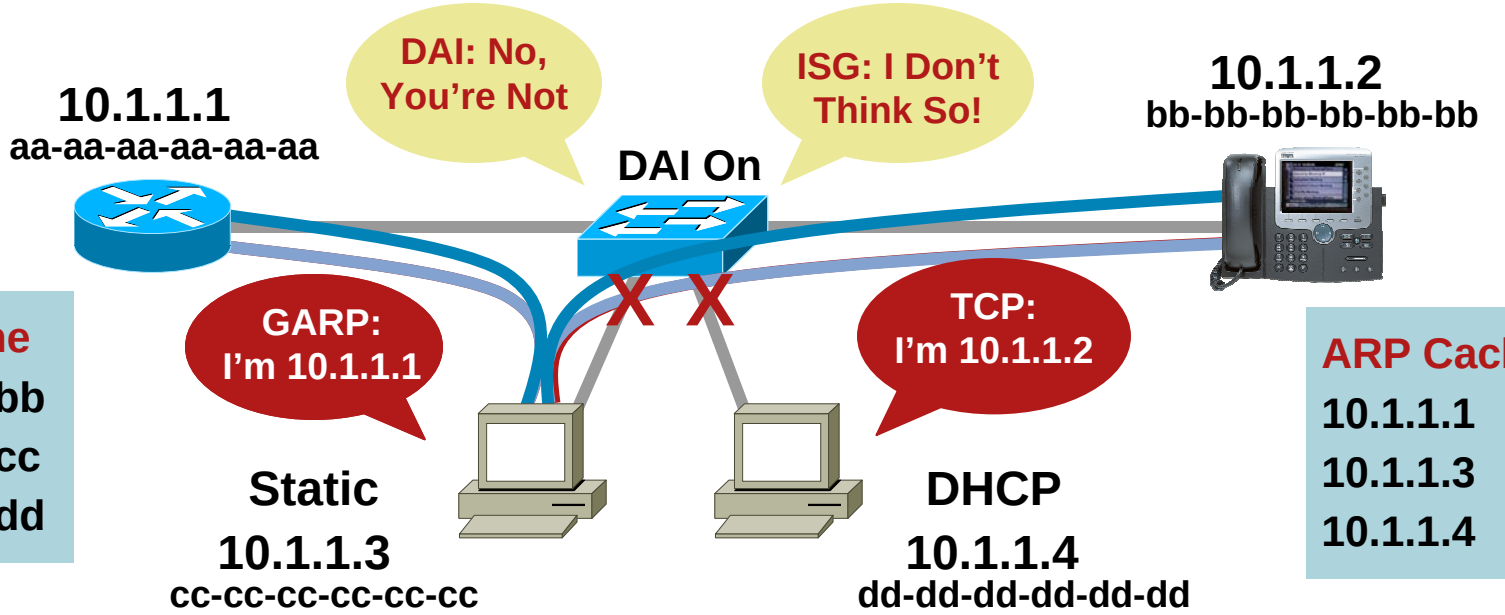


Stop Man-in-the-Middle Attacks

- Built on DHCP snooping binding table
- Dynamic ARP inspection watches ARP/GARP for violations
- IP source guard examines every IP packet
- Will drop packets or disable port

10.1.1.1	aa-aa-aa-aa-aa-aa	1/0
10.1.1.2	bb-bb-bb-bb-bb-bb	1/1
10.1.1.4	dd-dd-dd-dd-dd-dd	1/3

Successfully Stops ettercap, dsniff



ARP Cache

10.1.1.2	bb
10.1.1.3	cc
10.1.1.4	dd

ARP Cache

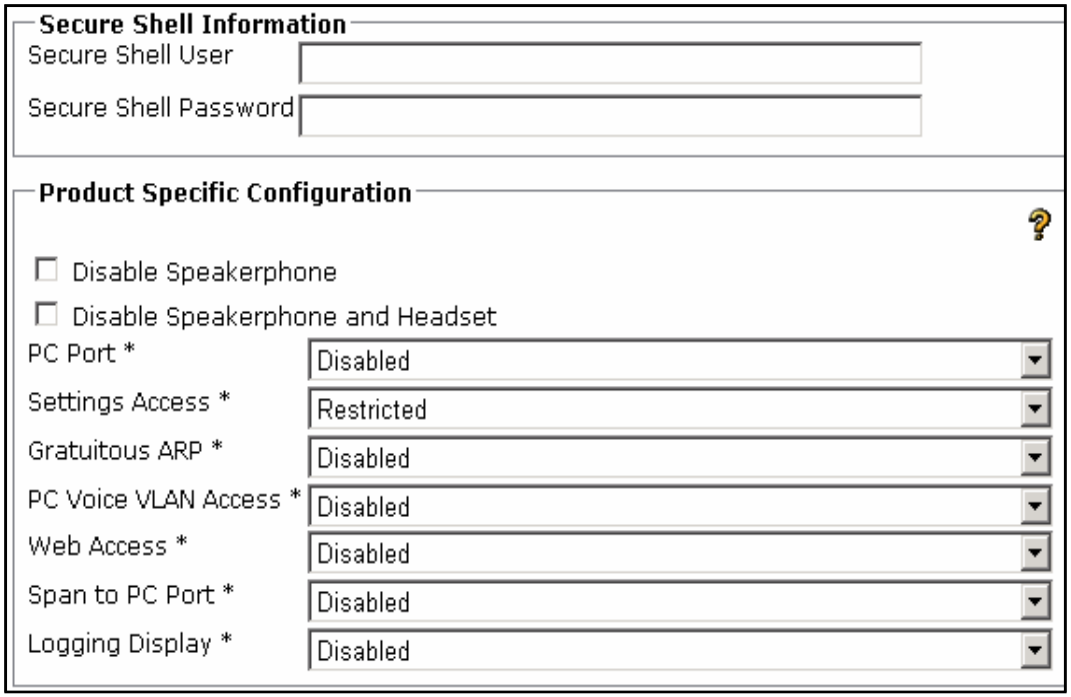
10.1.1.1	aa
10.1.1.3	cc
10.1.1.4	dd

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

Hardening the Endpoints

- Signed firmware
- Signed config files
- Disable
  - PC port
  - Settings button
  - Speakerphone
  - Web access

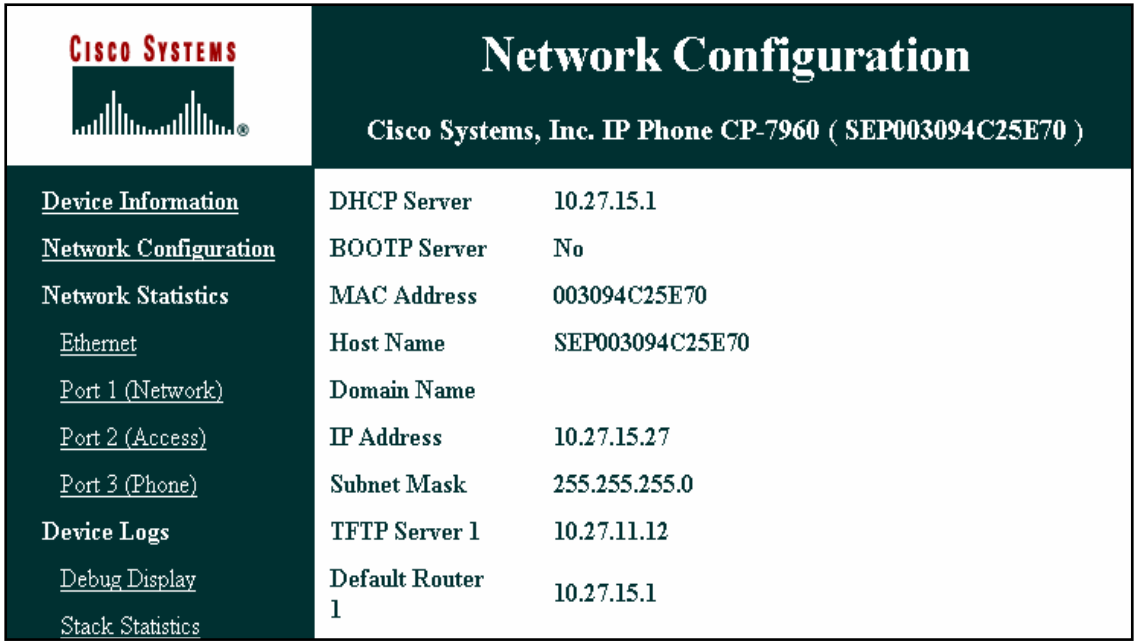


Cisco CallManager 5.0 View

Browse into a Phone

I Learn

- IP address/mask
- Default gateway
- DHCP server
- DNS server
- TFTP server
- Cisco CallManager(s)
- Directory server
- Logon server
- XML server



- If I'm reconning your network, I can learn an awful lot about your network by webbing into a single phone
- But, disabling web access also breaks XML pushing apps

  Instead, use ACLs to only allow port 80 between phones and servers

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

Securing TFTP

- Signed firmware images

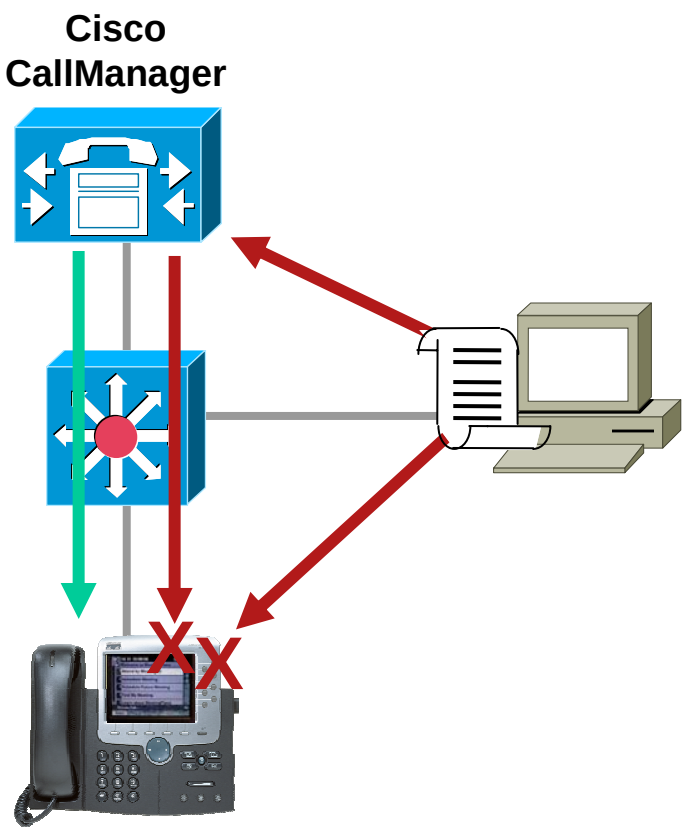
  Introduced in CCM 3.3(3)

- Signed config files [1]

  Introduced in CCM 4.0

- Encrypted config Files [1, 2]

  Introduced in CCM 5.0



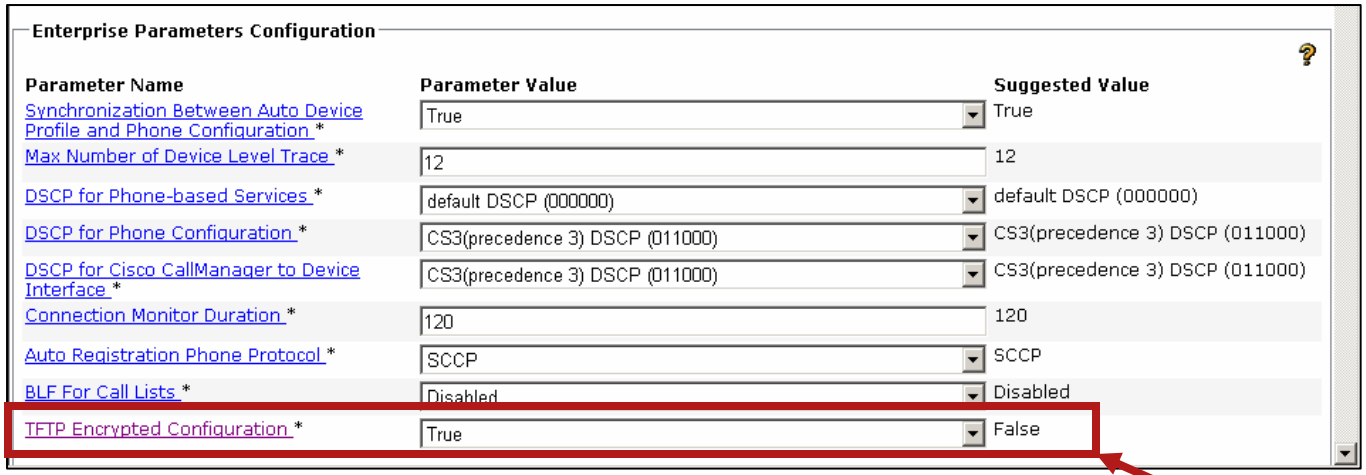
[1] On 7905/11/12/40/41/60/61/70/71
[2] Not on 05/12/40/60 SCCP Loads

Encrypted Configuration File Keys

Depends on if the Phone Has a Certificate

- Can use public key if phone has a certificate
  - CAPF used to cache keys in database
- Must manually enter into phone otherwise

Encrypted Configuration Parameter



Enterprise Parameters Configuration

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	Disabled	Disabled
TFTP Encrypted Configuration *	True	False

Now on Security Profile page

Encrypted Config = True

- If TFTP has key, config file is encrypted
- If TFTP doesn't have key, config file cannot be created

Encrypted Config = False

- Unencrypted config file contains NO credentials

Encrypted Config = Troubleshoot

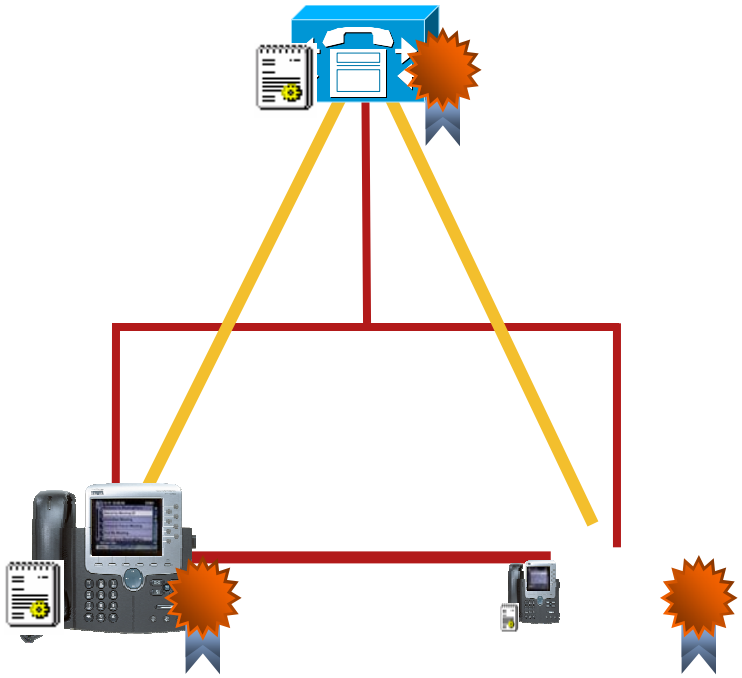
- Unencrypted config file contains Digest and SSH credentials

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

Certificate-Based Authentication and Encryption

- TLS—Transport Layer Security (RFC 2246) between Cisco CallManager and endpoints
  - RSA signatures
  - HMAC-SHA-1 auth tags
  - AES-128-CBC encryption
- SRTP—Secure RTP (rfc3711) between endpoints
  - HMAC-SHA-1 auth tags
  - AES-128-CM encryption



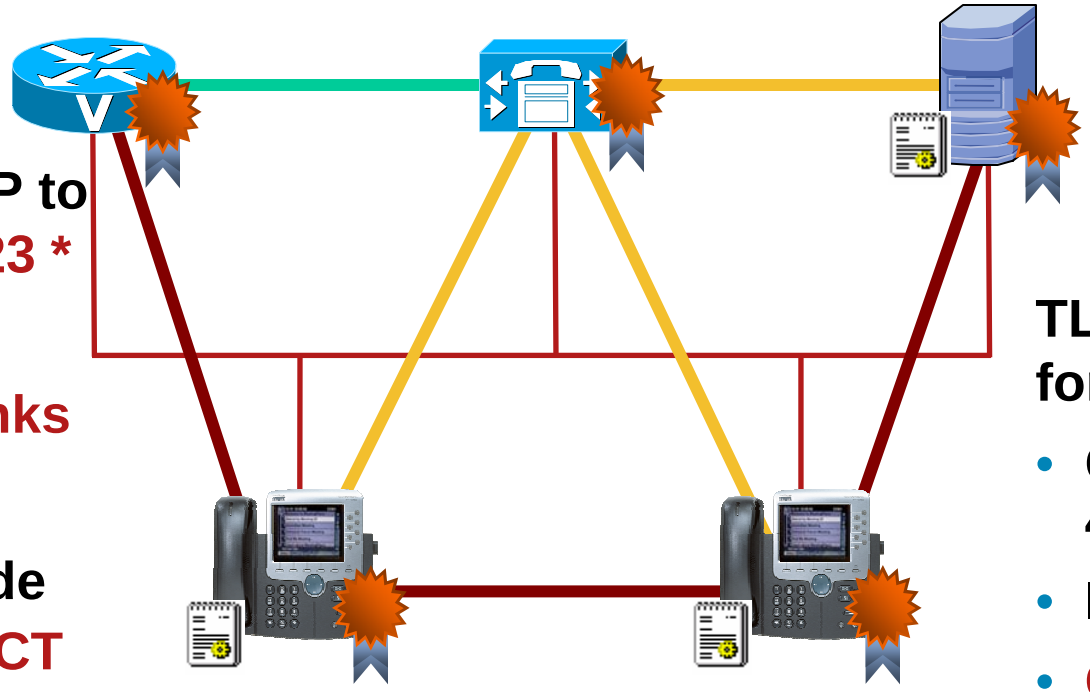
Certificate-Based Authentication and Encryption in CCM 4.1

IPSec and SRTP to MGCP and H.323 * Gateways

TLS to SIP Trunks

Including

- In SRST mode
- Over H.323 ICT



TLS and SRTP for Apps

- Cisco Unity® 4.0(5)
- IPCC 7.0
- CTI

SCCP TLS and SRTP Support in 7906/7911/7940/7960/7941/7961/7970/7971

SIP TLS and SRTP Support in 7906/7911/7941/7961/7970/7971

Full Interoperability Between Secure SCCP and Secure SIP

TLS
IPSec
SRTP

SRTP for SIP Phones

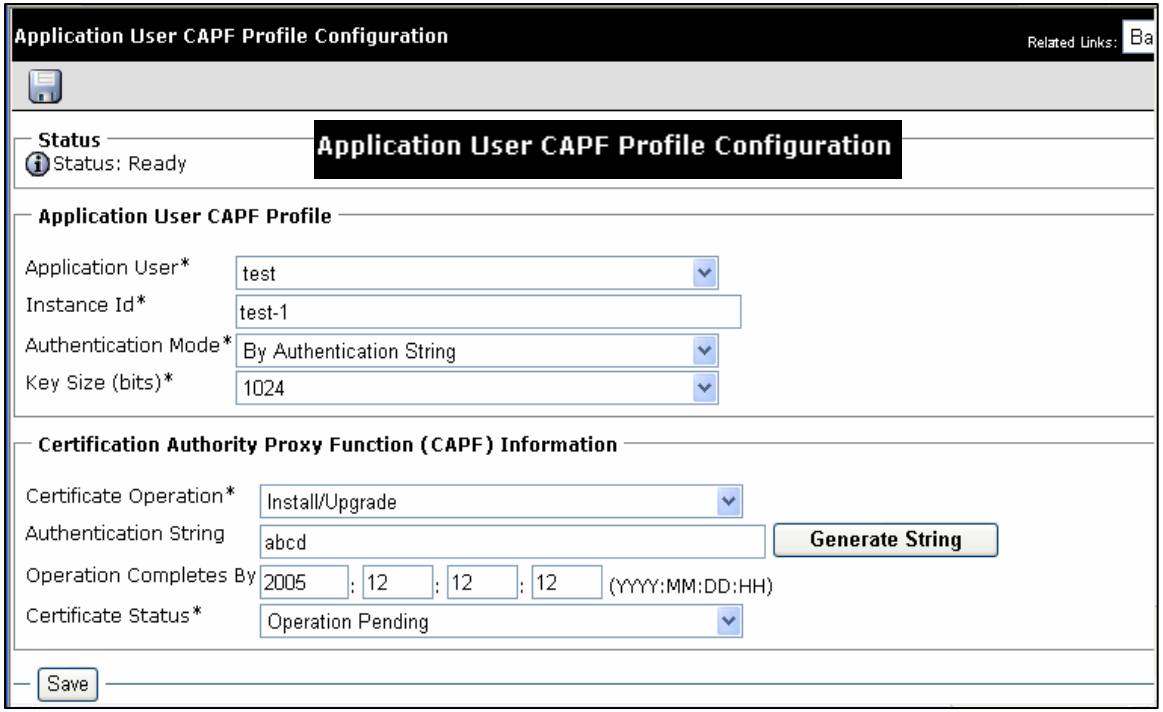
- Phones indicate capability for SRTP in SDP of SIP message
- SIP phones generate their own session keys, unlike SCCP
- Interoperates with secure SCCP, H.323, MGCP, etc.
- No support for encryption to third party phones—yet

CTI TLS and SRTP

Integrity and Privacy to CTI applications

- Works just like a phone – Cert / CTL / TLS / SRTP
- Cert tied to a user name/instance ID
- SRTP for MTP on Route Points
- Can share session keys for multiple call legs –

  used by partners to record encrypted calls



SIP Trunk TLS
Cisco CallManager Configuration

SIP Trunk Security Profile Configuration

Status
Status: Ready

SIP Trunk Security Profile Information

Name*	Encrypted TLS SIP Trunk
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
☐ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5061

SIP Information

Destination Address*	10.1.0.3
☐ Destination Address is an SRV	
Destination Port *	5060
MTP Preferred Originating Codec*	711ulaw
Presence Group*	San Jose
SIP Trunk Security Profile*	Encrypted TLS SIP Trunk
Rerouting Calling Search Space	San Jose
Out-Of-Dialog Refer Calling Search Space	San Jose
SUBSCRIBE Calling Search Space	San Jose
SIP Profile*	Customized SIP Profile
DTMF Signaling Method	No Preference

Save | Delete | Reset | Add New

- Create a SIP Trunk Security Profile
- Configure the SIP Trunk to use that profile

TLS Only

- No SRTP Yet

SIP TLS
Gateway Configuration

Build the PK Structure

```
CA Server: crypto pki server <ca-server-name>
RSA Key Pair: crypto key gen rsa general-keys label <label> mod 1024
Trustpoint:
    crypto pki trustpoint <ca-server-name>
    enrollment url <http://ca-server-ip>
    rsakeypair <rsa keypair label>
Auth Trustpoint: crypto pki authenticate <ca-server-name>
Enroll Trustpoint: crypto pki enroll <ca-server-name>
```

Configure TLS

```
session transport tcp tls
sip-ua
    crypto signaling default trustpoint <trustpoint-label>
    transport tcp tls
```

SIP URL

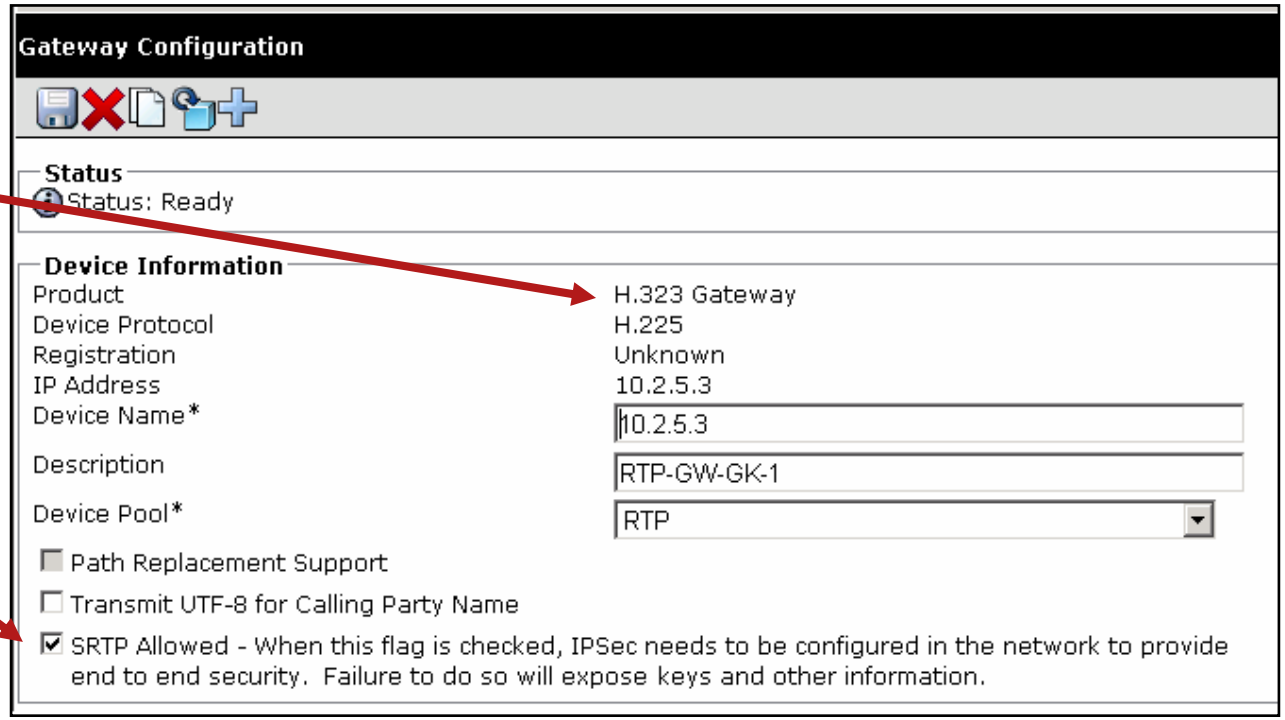
```
voice service voip
    sip
    url sips
```

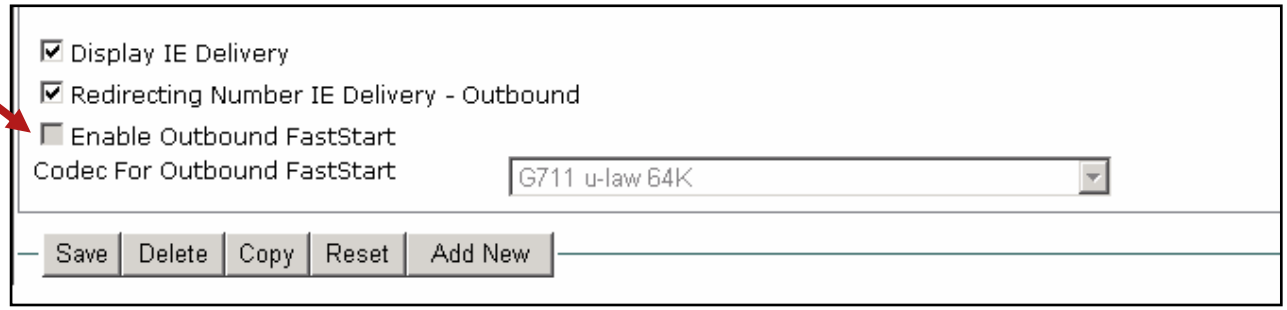
H.323 Trunk or Gateway Cisco CallManager Configuration

H323 Gateway

SRTP Allowed Checkbox

Outbound Faststart Checkbox Is Grayed out When SRTP Is Enabled





H.323 Gateway
Gateway Configuration

Gateway Configuration:

```
voice service voip
    srtp
      or
    srtp fallback
```

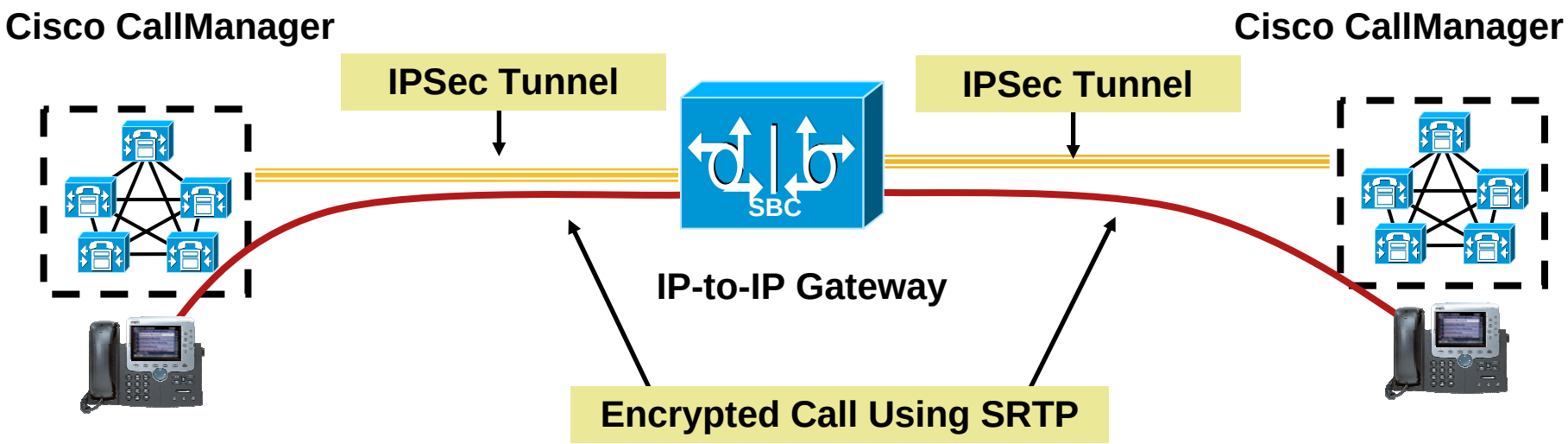
Hardware that supports SRTP (H.323, MGCP, SIP)

- **NM-HDV2 (all flavors)**
- **NM-HDV (all flavors)**
- **NM-HD-1V/2V/2VE**
- **PVDM2**
- **AIM-VOICE-30**
- **AIM-ATM-VOICE-30**

```
Voice-card 1
   codec complexity secure
```

* Command only used on DSP 549/5421 based voice-cards; not required on DSP 5510 (PVDM2) cards

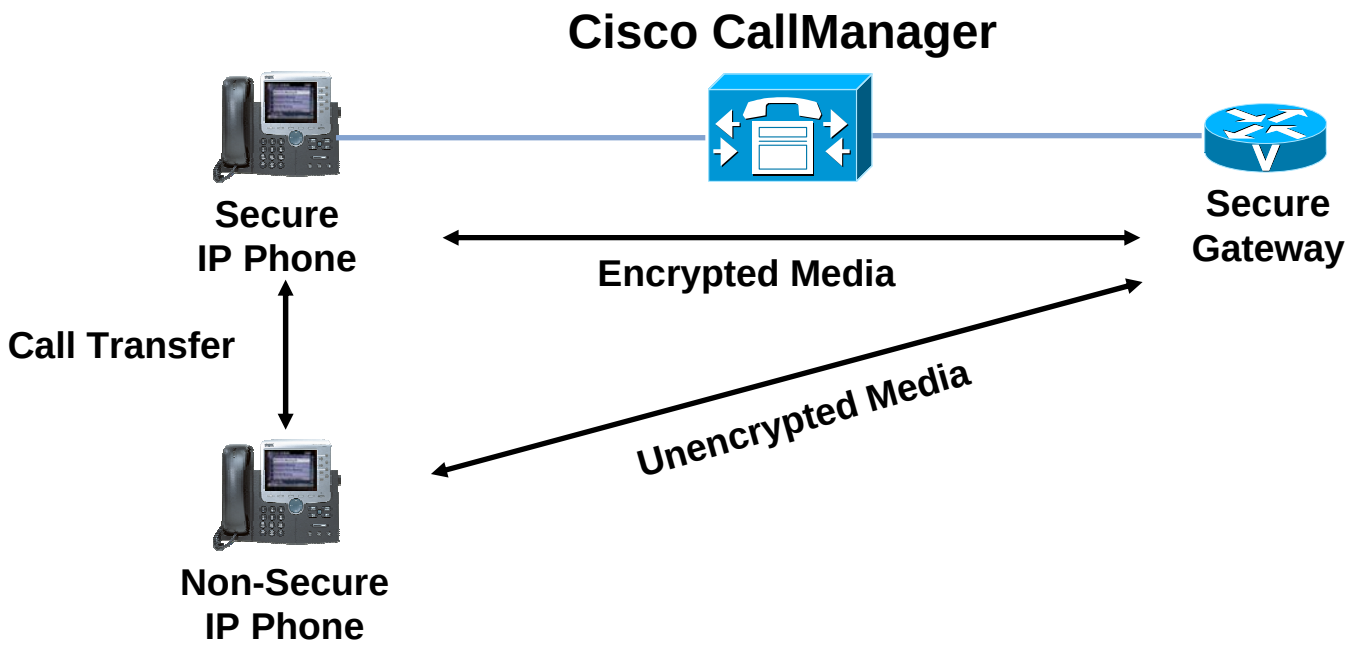
IPSec and SRTP Secure Calls Through IP-to-IP Gateway



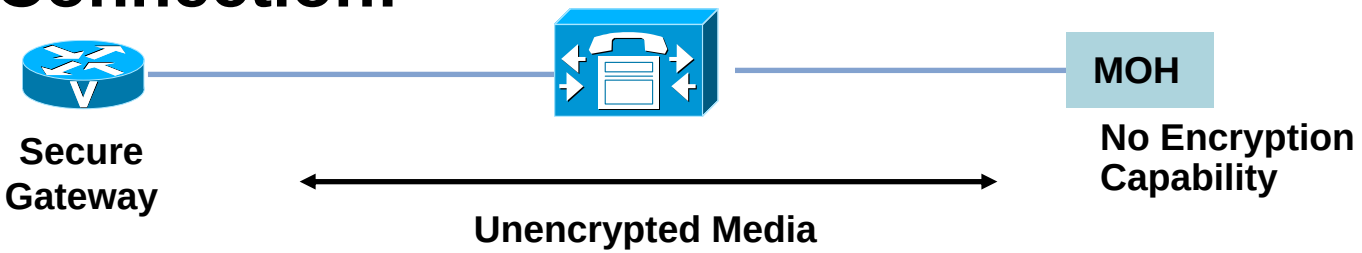
- Signaling over IPSec / Media over SRTP
- Works with or without IP-IP Gateway in place
  - Keys sent transparently across IP-to-IP Gateway
  - Works in flow-through and flow-around modes

RTP/SRTP Mixed-Mode

Secure Call Transfer:



MOH Connection:



Encryption Performance Considerations

- Cisco CallManager CPU and memory impact considered in device weight calculator
- 7940 / 7960 only support one SRTP stream and no wideband codec
- SRTP adds 4 bytes and 15 microseconds
- SRTP works with cRTP or IPSec
- IPSec design, admin, bandwidth and CPU implications

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

802.1X and IP Telephony

Requirement

- Phone only transmits on voice VLAN
- PC only transmits on data VLAN

Limitations – The 802.1X spec has no provision for

- More than one device on a port
- No authentication to a specific VLAN
- No binding to restrict an authenticated device to only transmit on authorized VLAN

Future Solution

- Supplicants on phones late 2006
- Switch changes to support multiple devices on different VLANs in late 2006
- 802.1AE – Link-layer integrity

- Landscape

  Many customers are asking for 802.1X in phones

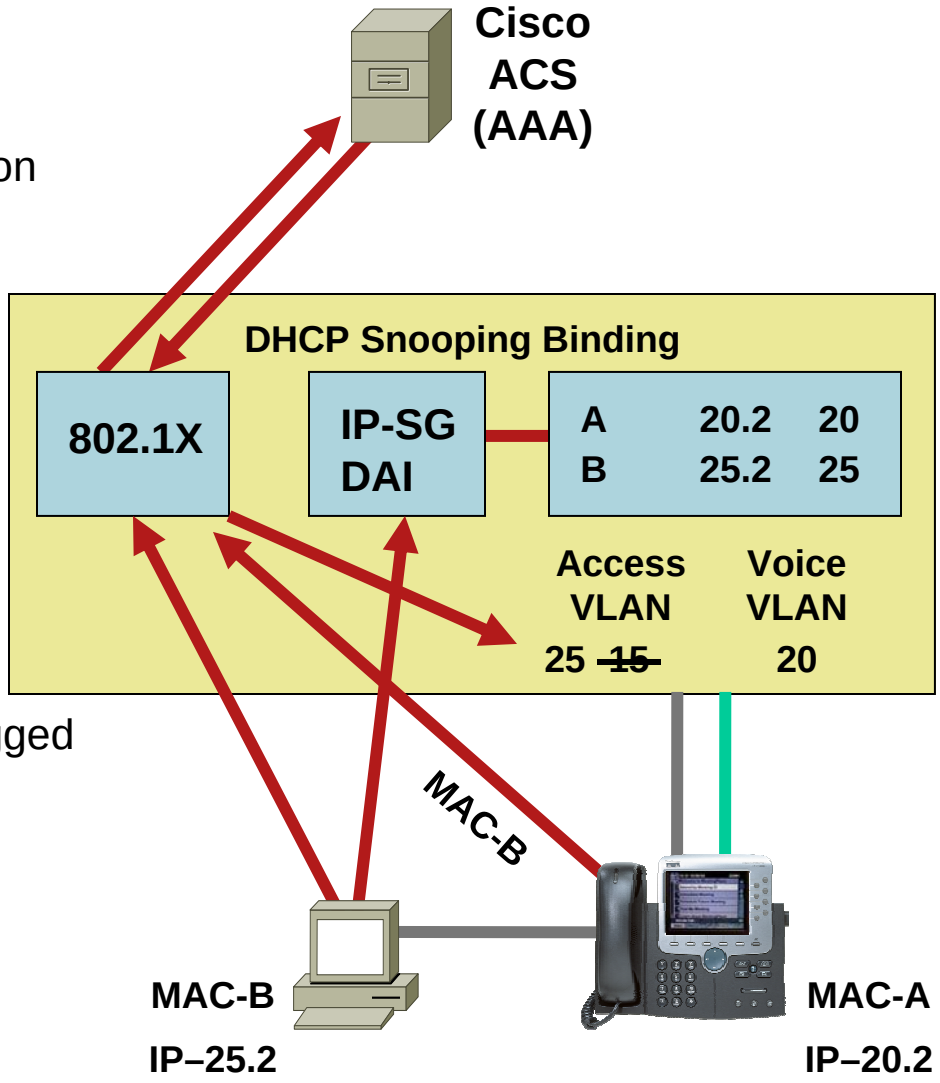
  Cisco phones support Proxy EAPOL-Logoff today

  Planned supplicant support in the future

802.1X Proxy EAPOL-Logoff Used with Other Security Features

- Phone monitors EAPOL transactions
- Sends Proxy EAPOL-Logoff with link loss on PC port

1. PC sends EAPOL-Logon—Phone watches
2. Authenticator queries AAA
3. AAA returns new VLAN ID
4. PC sends DHCP request
5. DHCP Snooping Binding created
6. IP-SG & DAI monitor for compliance
7. When PC disconnects, phone sends untagged EAPOL-Logoff

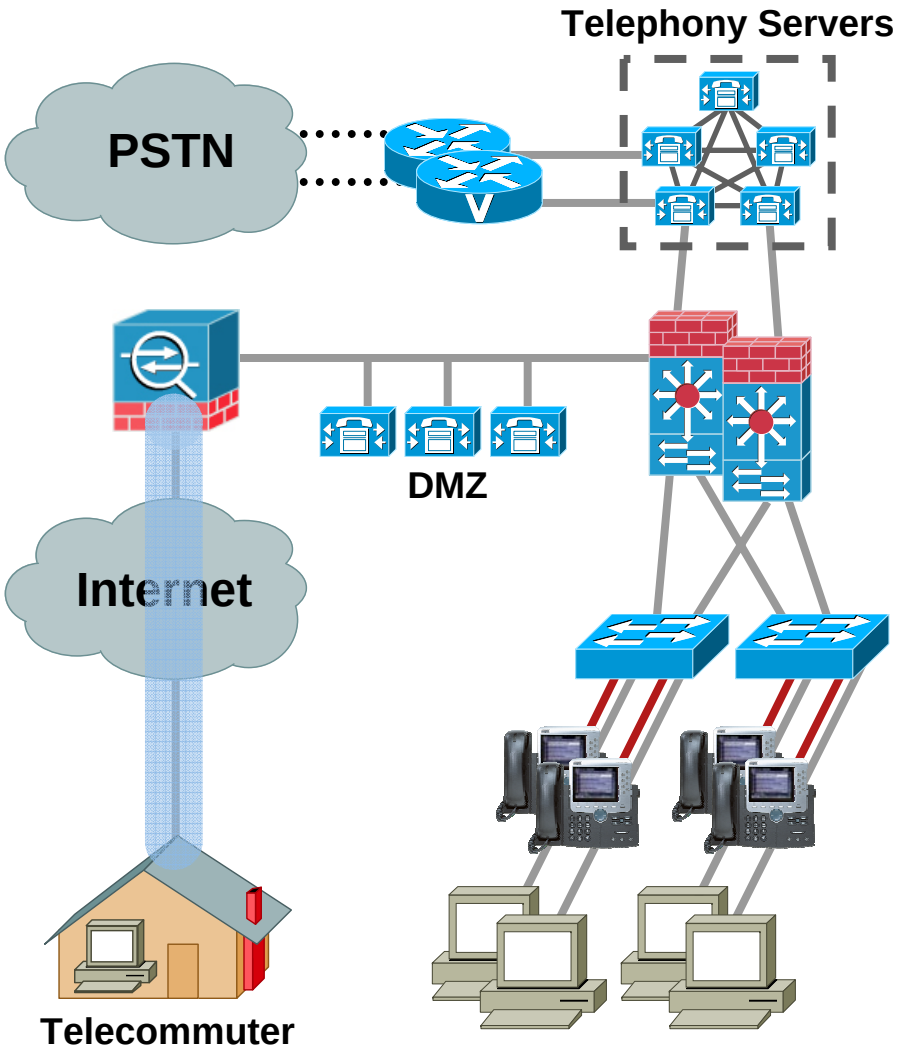


Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
  - Network Hardening for Phones
  - Phone Hardening
  - Securing TFTP
  - Encrypted Communications
  - 802.1X and IP Phones
  - Phones over the Internet
- Protect IP Telephony Servers
- Protect IP Telephony Applications

IP Phones over the Big I

- V3PNs protect all traffic, not just voice
- Terminate at HQ end in VPN concentrator or large router
- VPN Client in phones being considered
- Cisco PhoneProxy from Metreos aquisition



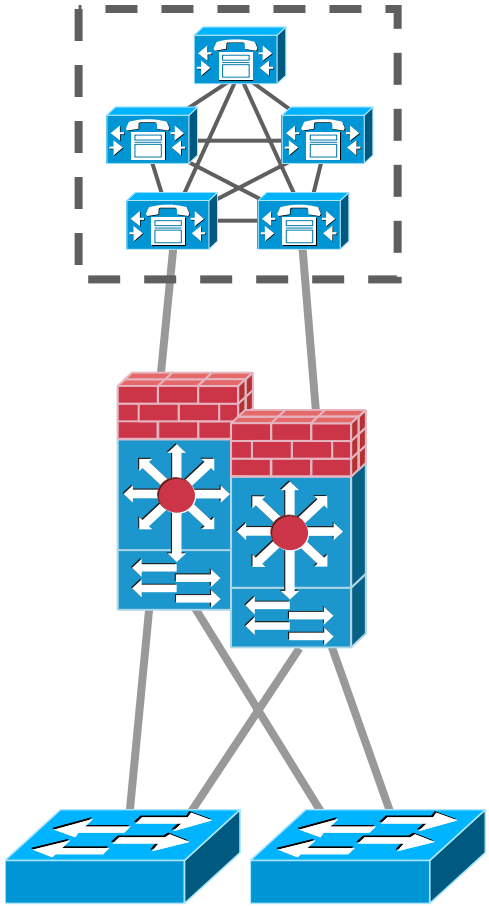
Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
  - Firewall Traversal
  - Cisco CallManager and IPSec
  - Windows for Cisco CallManager 4.x and Other Apps
  - Appliance Model for Cisco CallManager 5.0
- Protect IP Telephony Applications

Place a Firewall or ACL in Front of Telephony Servers

Why Firewall?

- Stateful inspection of protocols that use ephemeral port ranges
- Otherwise, have to open entire port range in static ACL
- LLQ and Rate Limiting now available in PIX® & ASA 7.0



Firewalls and Voice with Inspection Engines Enabled

How much firewall do I need? Generally …

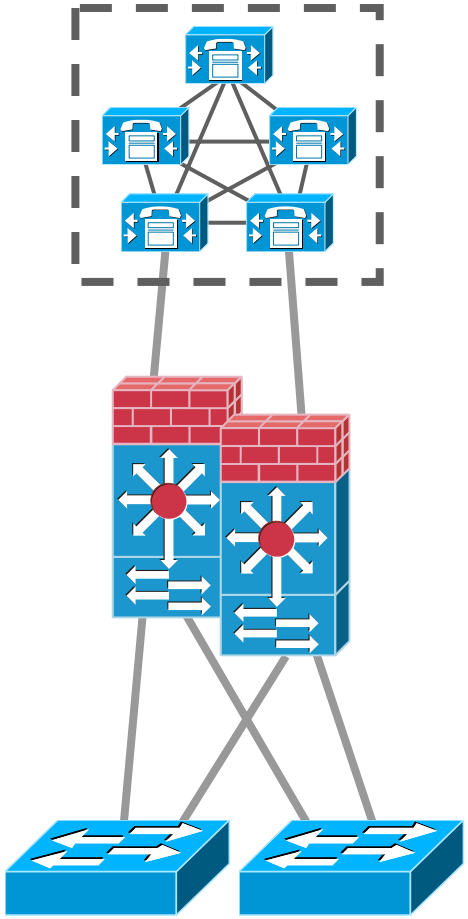
- 1–250 phones – ASA 5510, PIX 515E
- 250–1500 IP phones – ASA 5520, PIX 525
- 1500–30000 IP phones – ASA 5540*, PIX 535, FWSM

  If all it's doing is voice

Average 60% CPU or less

Stateful failover for VoIP Inspection Engines

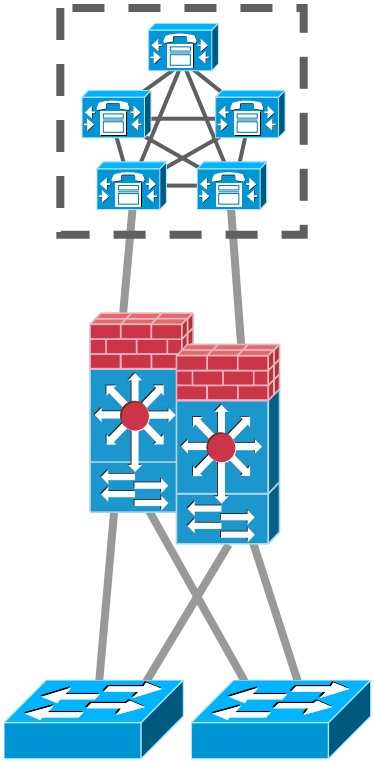
- Active/Stand-by or Active/Active



* ASA 5540 Can Outperform the Fastest Cisco CallManager Cluster

Firewalls and Encrypted Voice with Inspection Engines Disabled

- Fix-ups lose their ability to inspect
- Can use ACLs to allow signaling and RTP
  - PIX and ASA 7.0 supports “established” ACL – doesn’t work with UDP
- Packets arriving on the more trusted interface will open the connection
  - Doesn’t work with FWSM
  - Still need ACL for routing updates, RSVP, etc.
- Work in progress
  - STUN, ICE, midcom



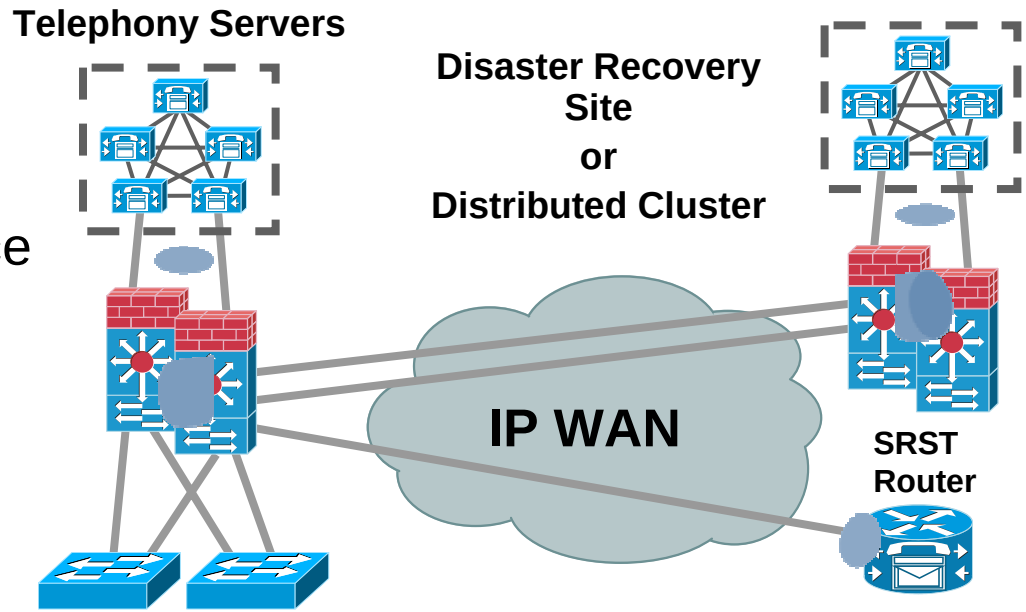
News Flash: Watch for TLS Proxy in PIX/ASA by year end!

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
  - Firewall Traversal
  - Cisco CallManager and IPSec
  - Windows for Cisco CallManager 4.x and Other Apps
  - Appliance Model for Cisco CallManager 5.0
- Protect IP Telephony Applications

IPSec to a Branch Office or DR Site

- Question of trust
- Protect all traffic, not just voice
- Clustering-over-the-WAN metrics
- Can config in CallManager



- Better to terminate in VPN concentrator or router
  - Performance
  - Configuration complexity
  - Organizational boundaries

A bit more on IPSec later

Voice Security Defense-in-Depth

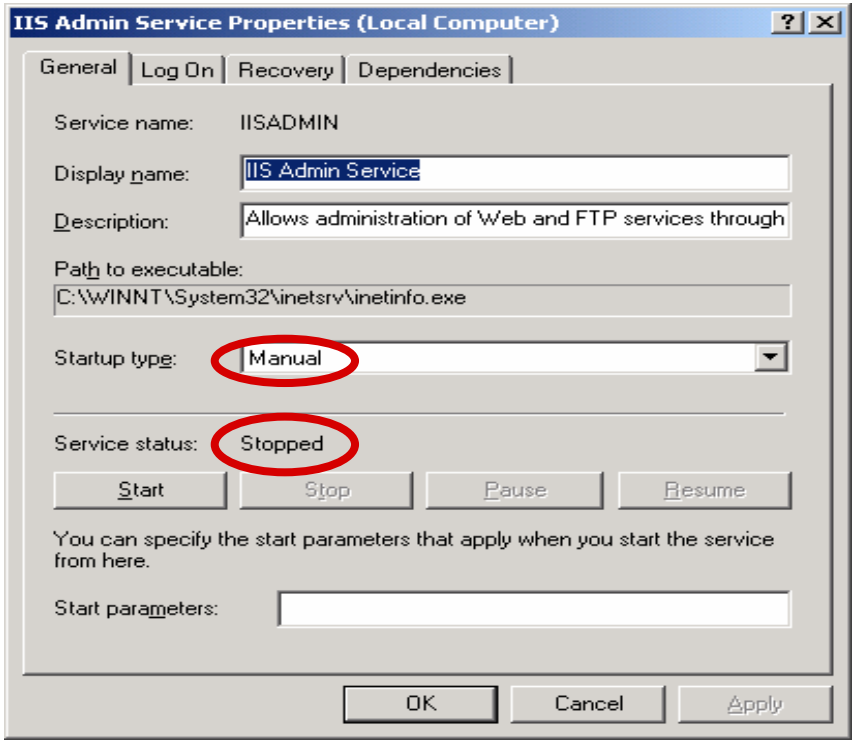
- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
  - Firewall Traversal
  - Cisco CallManager and IPSec
  - Windows for Cisco CallManager 4.x and Other Apps
  - Appliance Model for Cisco CallManager 5.0
- Protect IP Telephony Applications

Protecting the Windows Operating System for CallManager 4.x and Other Telephony Apps

- Hardened Win2K OS shipped by default
- Aggressive security patch and hotfix policy
- Cisco Security Agent (CSA) on all telephony apps
- AV from McAfee, Symantec, or Trend Micro
- Site-specific Optional Security features documented

80% of attacks against Windows are targeted at IIS !!!

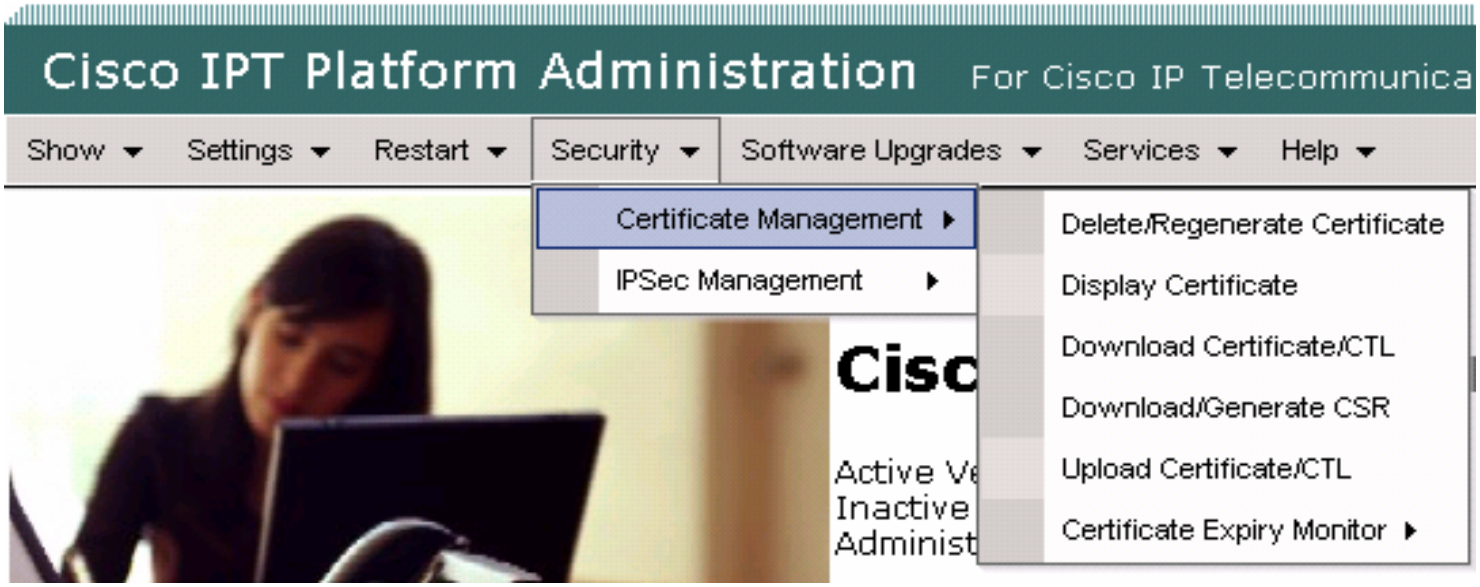
- **Turn off IIS & WWW on the Subscribers - Set to Manual for Installer**



Voice Security Defense-in-Depth

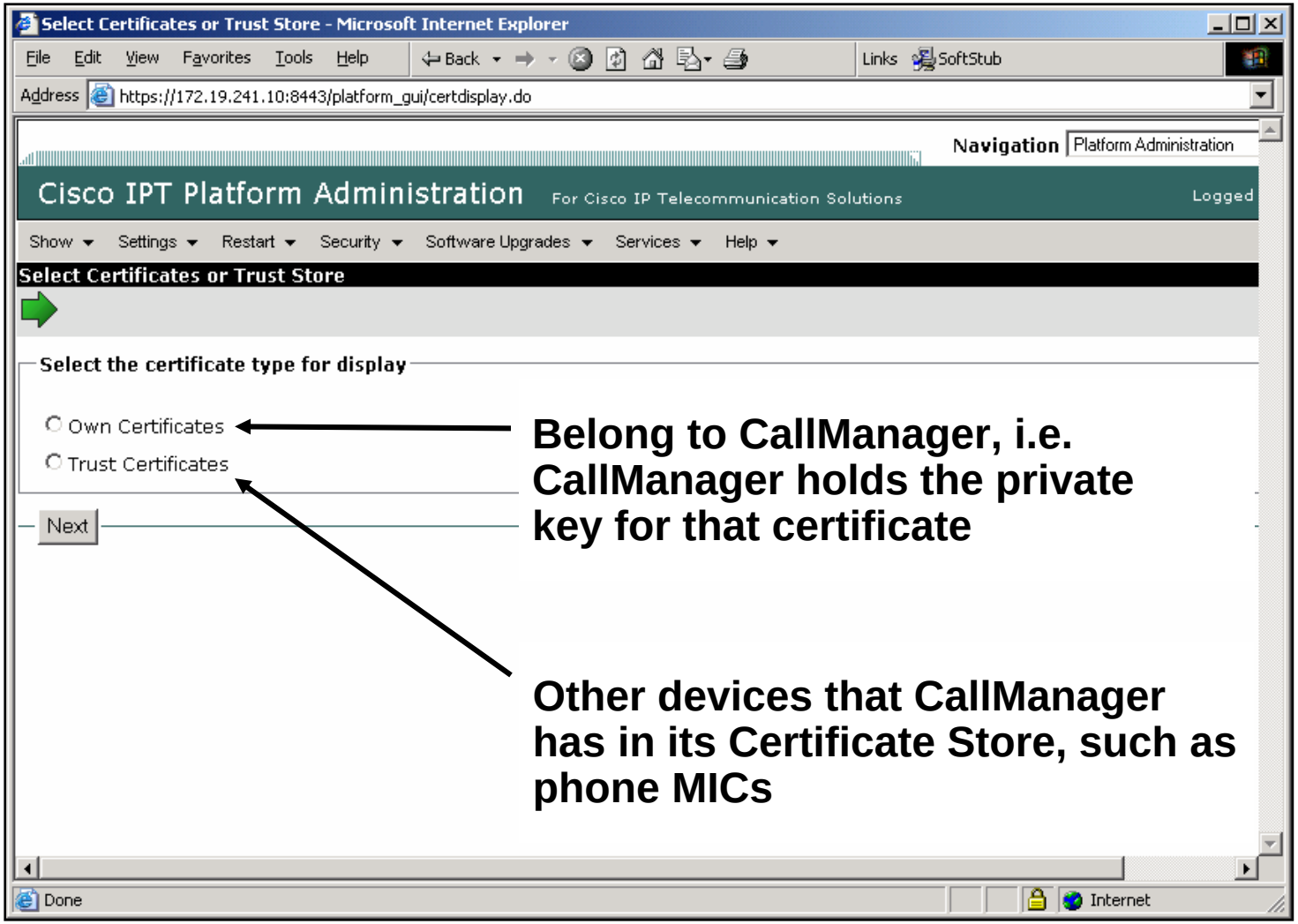
- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
  - Firewall Traversal
  - Cisco CallManager and IPSec
  - Windows for Cisco CallManager 4.x and Other Apps
  - Appliance Model for Cisco CallManager 5.0
- Protect IP Telephony Applications

CallManager 5.0 Appliance Model Security



- Appliance model makes file system and OS apps inaccessible
- Only allows images to be installed that have been signed by Cisco
- SSH / SFTP / SNMPv3 / Security Passphrase / Password Recovery
- Industry-recommended security practices followed
- Security events logged

X.509 Certificate Management UI: Display Certificate

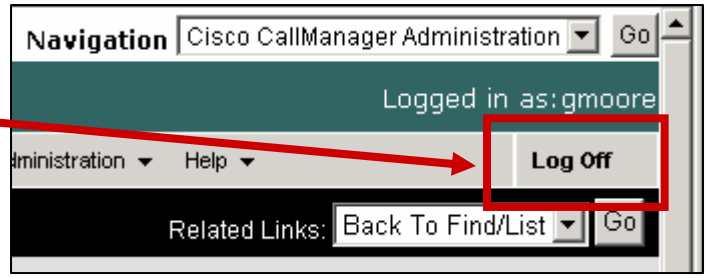


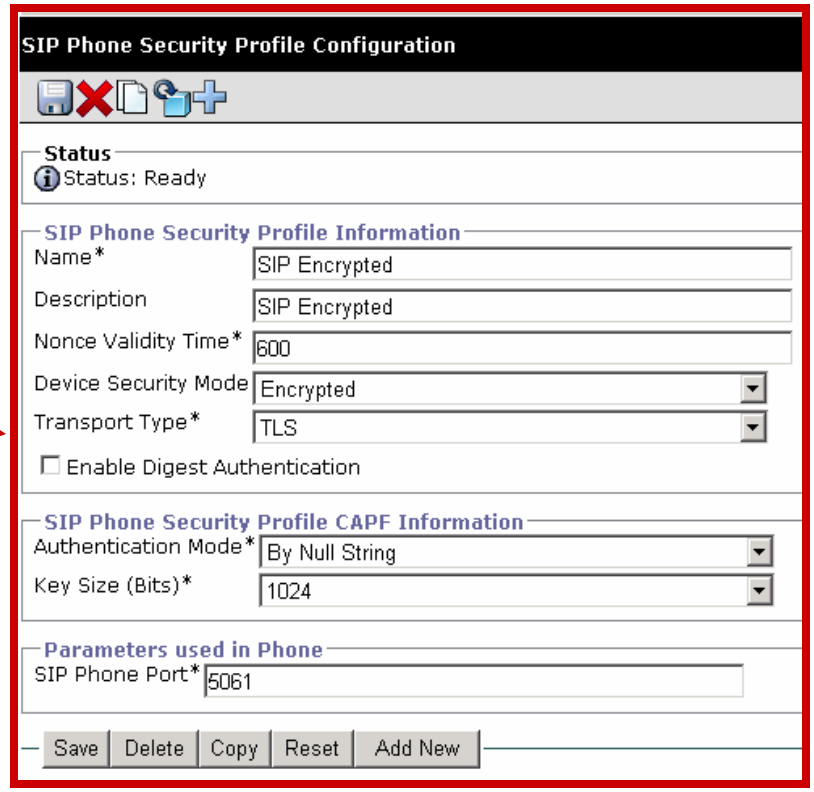
Belong to CallManager, i.e. CallManager holds the private key for that certificate

Other devices that CallManager has in its Certificate Store, such as phone MICs

Secure Remote Access
New in CallManager 5.0

- Log Off button on web pages
- 30 minute inactivity logout timer
- All web pages use HTTPS
- Directory queries can use LDAP over SSL
- New Security Profile abstract configures common security features to multiple devices
- Different CCMAdmin and Platform passwords





Cisco Security Agent

- Cisco Security Agent is installed as part of Cisco CallManager 5.0 platform
- No configuration necessary
- Start and Stop from Control Center or CLI
- No Managed Agent support with initial release

Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
- Protect IP Telephony Applications
  - Cisco CallManager
  - Cisco Unity
  - IPCC Enterprise

Digest Authentication for SIP CallManager 5.0

- Based on RFC 3261 & RFC 2617
- Username / Password Auth Mechanism
- Client / Server Model
  - Server Challenges, Client responds

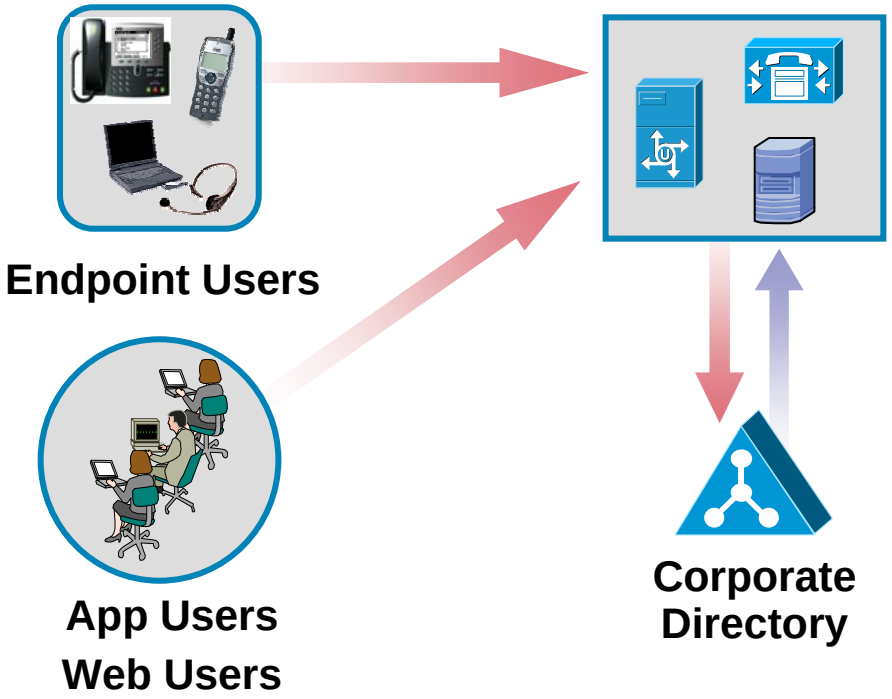
The trick is getting the password into the phone

- **Can use public key for phones with MIC**
- **Must manually enter into phone otherwise**

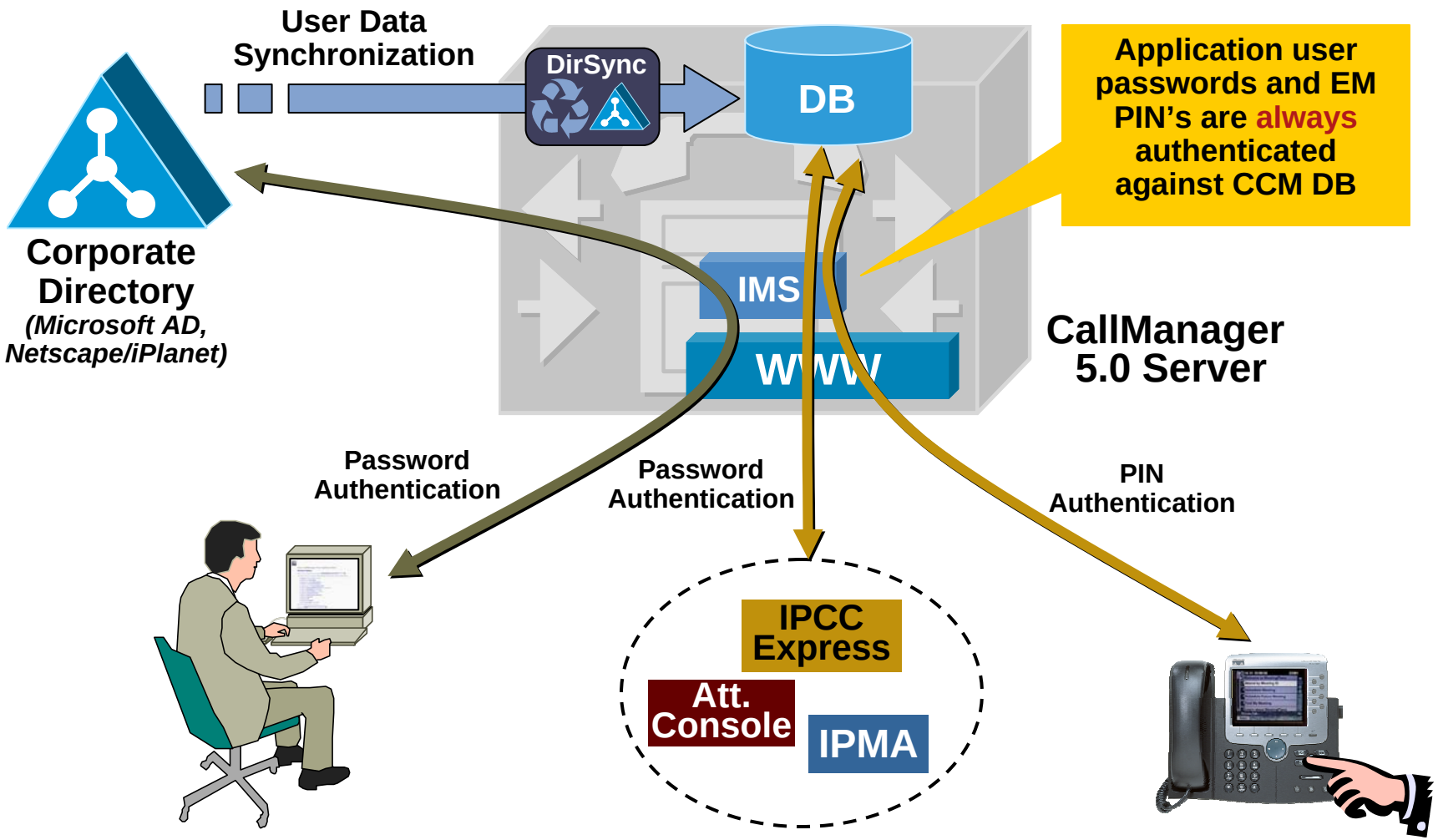
CallManager 5.0 Directory Integration

- Optional Directory Integration now native to CallManager admin
- All users stored in CallManager database
  - Can be configured locally – GUI or BAT
  - Can be 'Synchronized' (extracted) from LDAP directory – AD or Netscape
- Authentication can be local or against LDAP directory
- Queries can be sent from CallManager or other applications

  (Unity, MeetingPlace, IPCC, etc.)
- No more AD Plug-in
- No more schema extensions



Directory Authentication Architecture

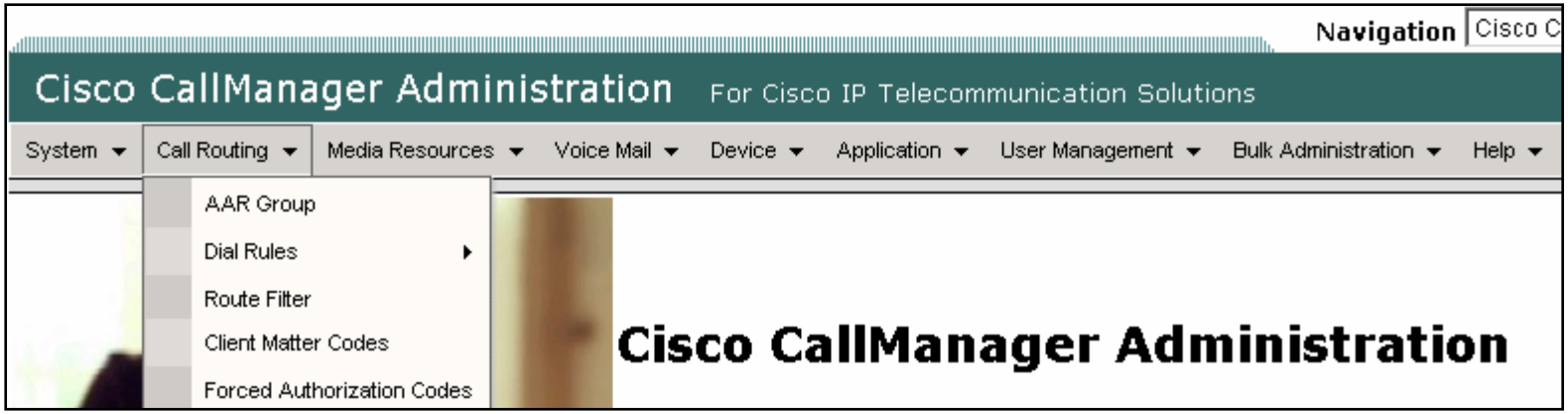


End users: password
(incl. CCM admins with MLA)

Application users
(ac, jtapi, CCMAdministrator)

End users:
EM login

Prevent User Toll Fraud



- Protect against call forwarding and trunk-to-trunk transfer exploits
- Partitions and Calling Search Spaces limit what parts of the dial plan phones have access to
- Dial plan filters control access to exploitive phone numbers, such as 900
- Forced authentication codes or client matter codes prevent unauthorized calls and provide a mechanism for billing and tracking

Voice Security Defense-in-Depth

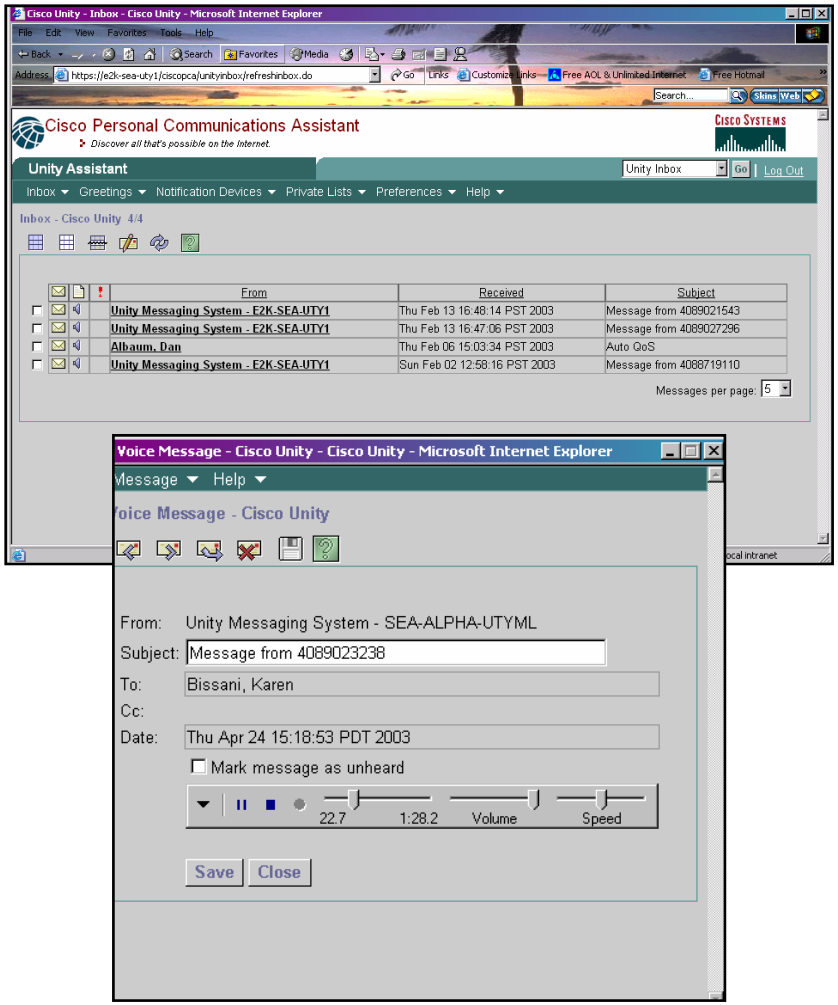
- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
- Protect IP Telephony Applications
  - Cisco CallManager
  - Cisco Unity
  - IPCC Enterprise

Host and Network Hardening

- Manually harden Win2K OS, SQL, LDAP and SMTP Exchange/Domino servers
  - http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpapr/secure40.htm
  - http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/whitpapr/tcpudp.htm
- User account policies
  - Minimum password/PIN lengths and complexity
  - Password/PIN reuse and expiration
  - One-time PIN tokens
  - Number of login failures
- Class-of-service restrictions
- Secure active directory infrastructure
- HTTPS for all web access—admin and user
- New in Unity 4.0(5)
  - TLS and SRTP support
  - Secure private messages

Private Secure Messaging

- Private secure messaging encrypts voice messages
- Secure private message forwarded outside the organization via Outlook results in a message telling the recipient the content not accessible
- Lotus Notes restricts private messages from being forwarded at all
- Secure private messages can only be accessed over the telephone by dialing into the Cisco Unity system



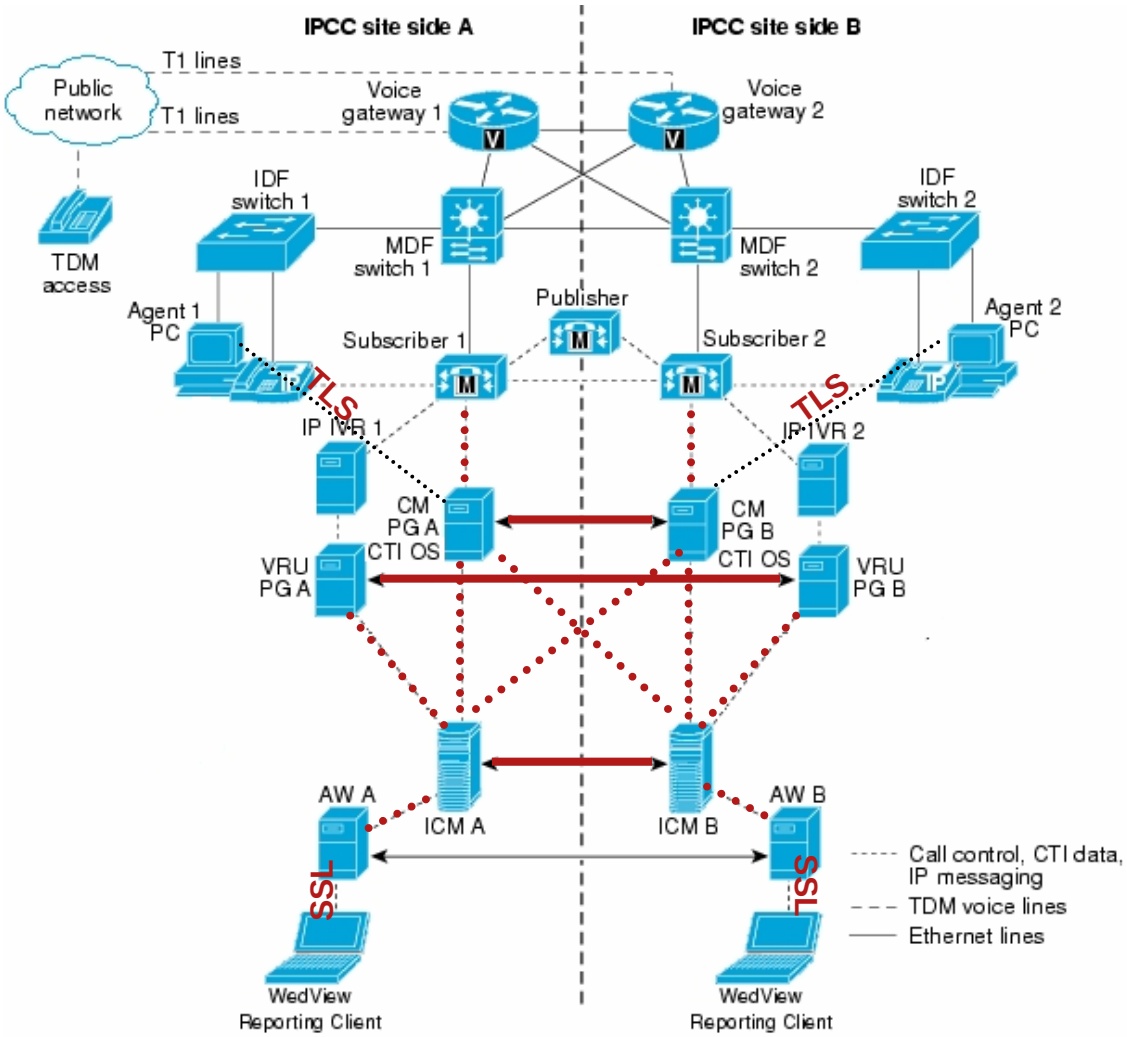
Voice Security Defense-in-Depth

- Protect IP Telephony Endpoints
- Protect IP Telephony Servers
- Protect IP Telephony Applications
  - Cisco CallManager
  - Cisco Unity
  - IPCC Enterprise

IPCC Enterprise 7.0

- Pervasive SSL (config, admin, reporting, management)
- TLS for agent desktops
- Application-level IPSec
- Secure VNC and encrypted terminal services
- Authenticated and encrypted SNMPv3
- Locked down IIS
- Windows—2003 Advanced Server

  Automated OS hardening



How Much Security Is Enough?

Security Is a Balance Between Risk and Cost

Cost—Complexity—Manpower—Overhead

Bronze Default, Easy, No-Brainer	Silver Moderate, Reasonable	Gold New, Hard, Not Integrated
Basic Layer 3 ACLs	Simple Firewalls	Complex Firewalls
Standard OS Hardening	Rate Limiting	NAC / 802.1X
Unmanaged CSA	Catalyst® Integrated Security	Network Anomaly Detection
Antivirus	VPN—SOHO/Mobile	Security Info Management
HTTPS	Optional OS Hardening	
SLDAP	Managed CSA/VMS	
Signed Firmware and Configs	Directory Integration	
Phone Security Settings	TLS / SRTP to Phones	
	IPSec / SRTP to Gateways	

Further Reading

Outside Publications

- NetworkWorldFusion: Breaking Through IP Telephony
  http://www.networkworld.com/reviews/2004/0524voipsecurity.html
- US DoD PBX1 and PBX2 Accreditation
  http://jitc.fhu.disa.mil/tssi/apl/apl_cisco.html
- NIST: 'Security Considerations for VoIP Systems'
  http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- eWeek: 'VoIP Is As Secure As You Make It'
  http://www.eweek.com/article2/0,1759,1592801,00.asp
- Ziff Davis: 'Securing Your Network for VoIP'

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd801e6159.pdf
- Converge!: 'Enterprise Security – An Enabler of VoIP'
  http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp?ID=141&ctgy=4

Further Reading

Cisco Whitepapers and App Notes

- VTG VP Discusses Cisco's Leadership in Protecting IPT
  http://newsroom.cisco.com/dlls/2005/hd_071805.html?CMP=AFC-001
- CallManager and IP Telephony Design Guides
  www.cisco.com/go/srnd
- SAFE Security Blueprints
  www.cisco.com/go/security
- Cisco IP Telephony Security Collateral
  www.cisco.com/go/ipcsecurity
- 802.1X and IPT Positioning Paper
  Cisco Internal – Contact Your Local Account Team

Further Reading

Cisco Documentation

- Cisco CallManager Security, Virus Protection Guides, and TCP / UDP Port Lists

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm

- Configuring IPSec Between a Microsoft Windows 2000

  http://www.cisco.com/en/US/partner/tech/tk583/tk372/technologies_configuration_example09186a00800b12b5.shtml#intro

- Proxy EAPOL-Logoff Release Note

  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7960/relnotes/72_200rn.htm#wp1104620

- Signed Firmware Release Note

  http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_note09186a00801c7164.html

Further Reading

CiscoPress – VoIP

- Cisco CallManager Fundamentals, 2nd Edition
  John Alexander, Chris Pearce, Anne Smith, Delon Whetten
  ISBN: 1587051923; Published: Sep 22, 2005; Copyright 2006
- Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization
  Salman Asadullah, Ramesh Kaza
  ISBN: 1587051575; Published: Feb 23, 2005; Copyright 2005
- Cisco CallManager Best Practices: A Cisco AVVID Solution
  Salvatore Collora, Ed Leonhardt, Anne Smith
  ISBN: 1587051397; Published: Jun 28, 2004; Copyright 2004

Further Reading

CiscoPress – Security and QoS

- The Complete Cisco VPN Configuration Guide
  Richard Deal
  ISBN: 1587052040; Published: Dec 15, 2005; Copyright 2006
- Cisco ASA and PIX Firewall Handbook
  David Hucaby
  ISBN: 1587051583; Published: Jun 7, 2005; Copyright 2005
- End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs
  Christina Hattingh, Tim Szigeti
  ISBN: 1587051761; Published: Nov 9, 2004; Copyright 2005