



Sikker IP-telefoni Security by design

Jørgen Gammelgaard
System Engineer, Cisco Systems Danmark

IP Consolidation

- The same IP technology that enables IP Communications solutions to:
 - Boost productivity
 - Increase mobility
 - Enhance flexibility
- Also creates additional **MANAGEABLE** security challenges
- These new challenges exist whether the IP upgrade is incremental or total



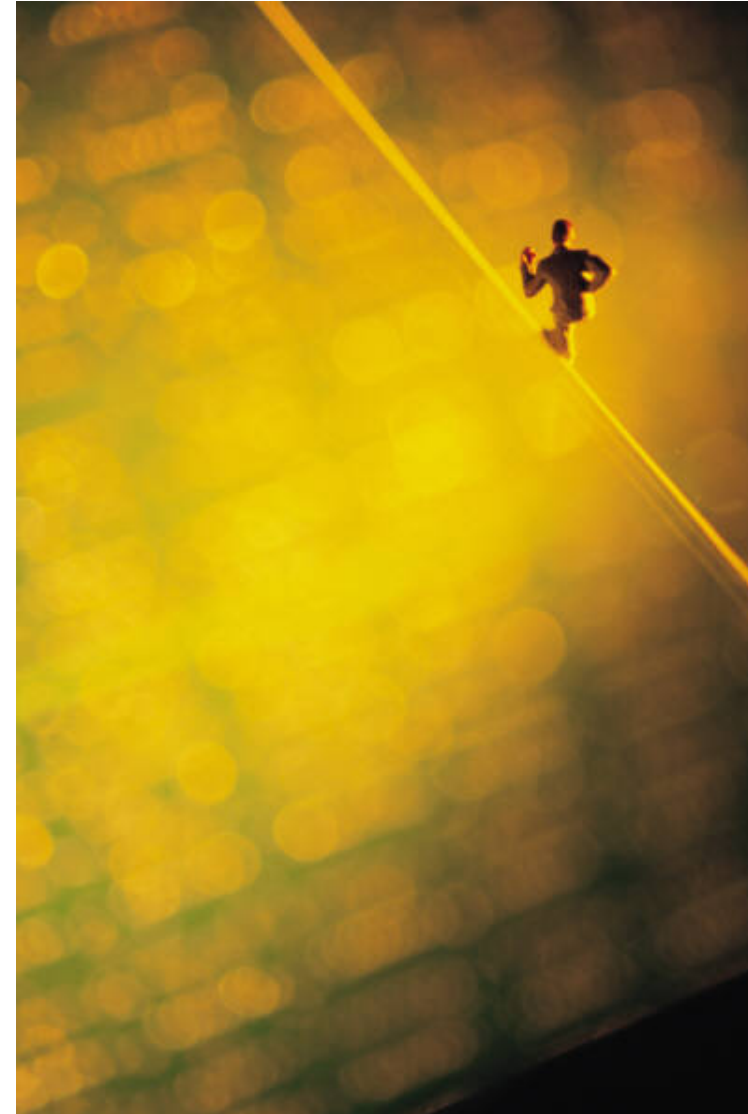
The Challenge of Securing IP Voice

- The threats are familiar to both voice and data professionals:
 - Eavesdropping**
 - Impersonation**
 - Toll fraud**
 - Denial of service**
- The protection of both voice and data communication is critical to the business



Security policy

- Understand the costs of security incidents:
 - Measurable:** fraud, downtime, man-hours, physical destruction, intellectual property, lawsuits
 - Non-measurable:** reputation, customer privacy, medical information, loss of life
- Assign risk and quantify the costs
- Determine appropriate levels of protection



The Paradigm Must Change: A Network-Based Systems Approach

- **Deploying Self Defending Network**
 - An **automated** security system is required to address unknown (or “Day Zero”) threats
 - Security must be applied at **multiple layers** of the system to address sophisticated blended threats and defend against multiple avenues of attack
 - All elements of the security system must be **integrated** to initiate a coordinated response



Protect All Levels of IP Communications

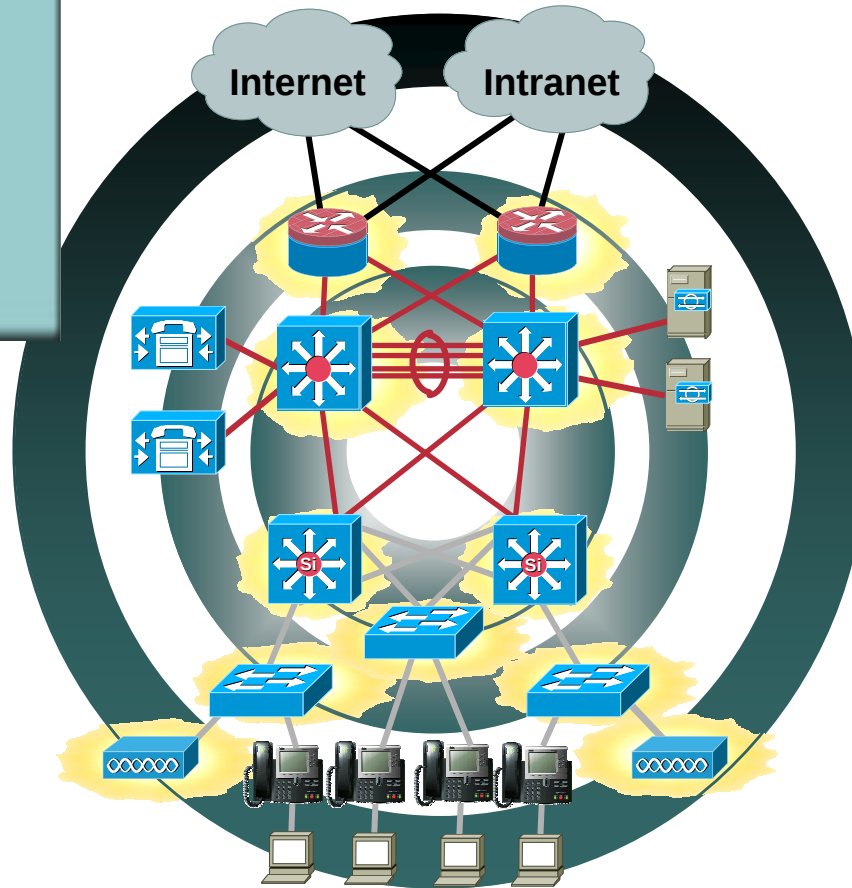
APPLICATIONS	VALUE-ADDED COMPONENTS	Messaging, Customer Care, and Other Application Software	IP COMMUNICATIONS SYSTEM 
ENDPOINTS	USER INTERFACES	IP Phones, Video Terminals, and Other Delivery Devices	
CALL CONTROL	SYSTEM CONFIG AND OPERATION	Infrastructure and Protocols for Call Management and Operation	
INFRASTRUCTURE	TRANSPORT	Secure, Reliable Communications that Connects All of the Other Components	

Secure IP Communications Systems Approach in Action



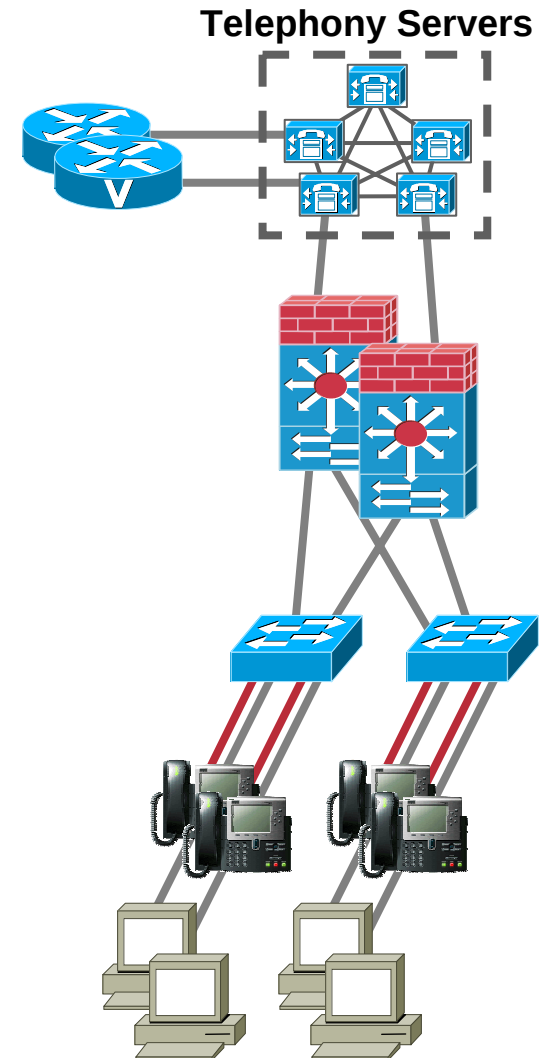
Infrastructure

- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

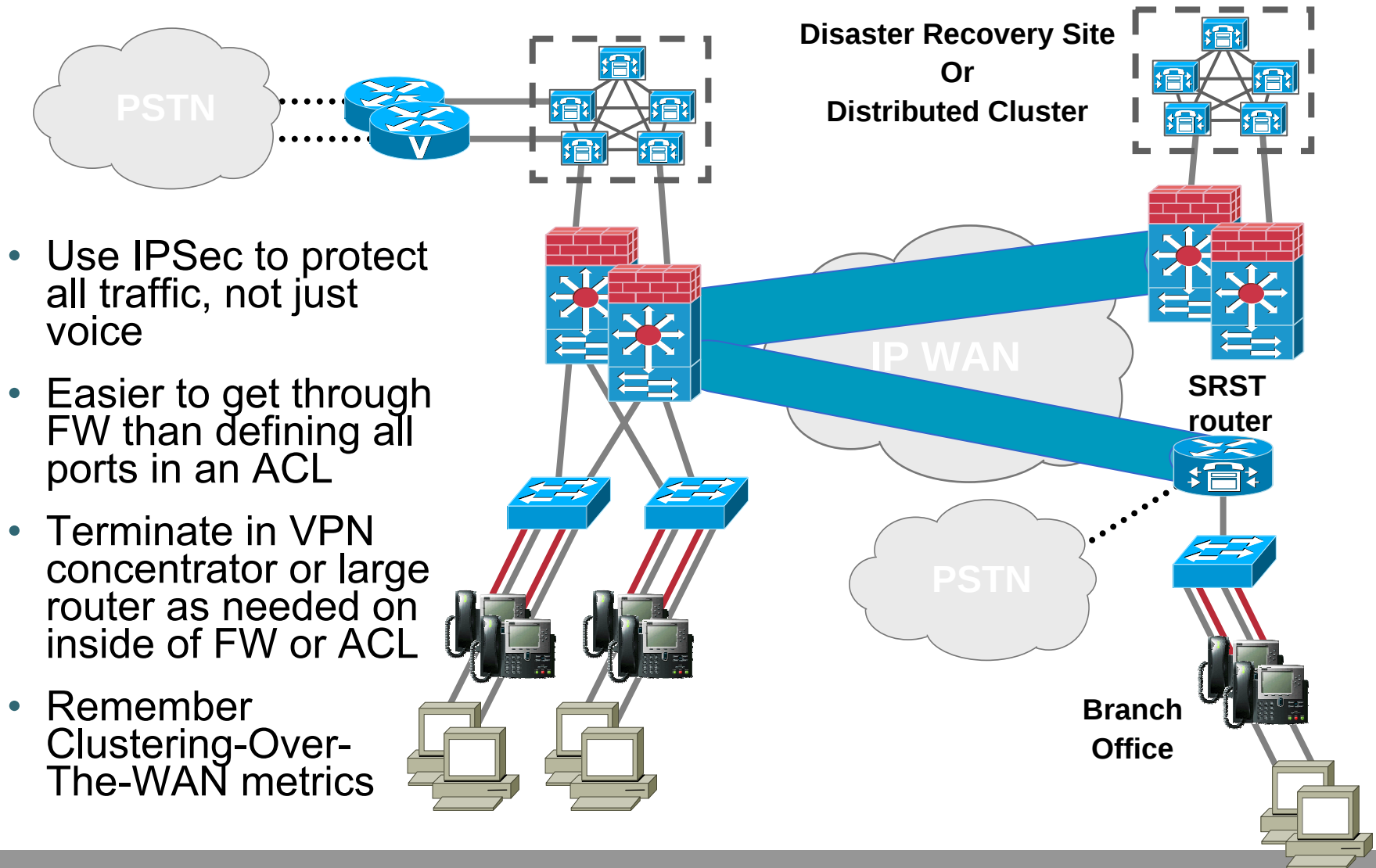


VLAN and Layer 2 Protection

- Voice and data on separate VLANs
- Block PC port access to voice VLAN
- Use VACLs to limit traffic
- Defend against GARP and DHCP abuse
- Use dynamic ARP inspection and IP source guard

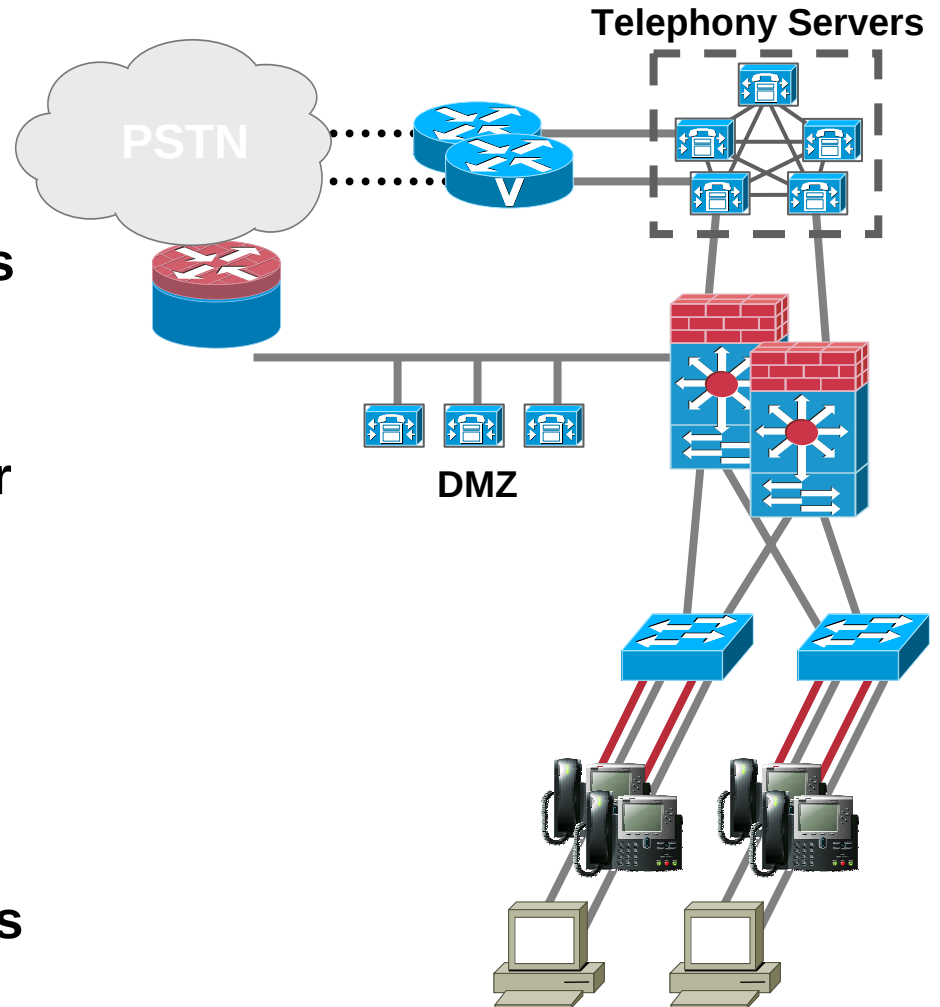


V3PN and IPsec

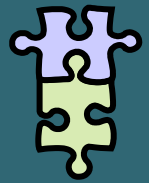


Firewall, IDS, and Anomaly Detection

- **Stateful, rules-based firewalls control traffic**
- **Intrusion Detection Systems look for signature-based exploits**
- **Anomaly detection looks for unusual events**
- **Rate limiting thwarts DoS and DDoS attacks from impacting voice**
- **Processor thresholds protect routers and switches from overload**



Secure IP Communications Systems Approach in Action

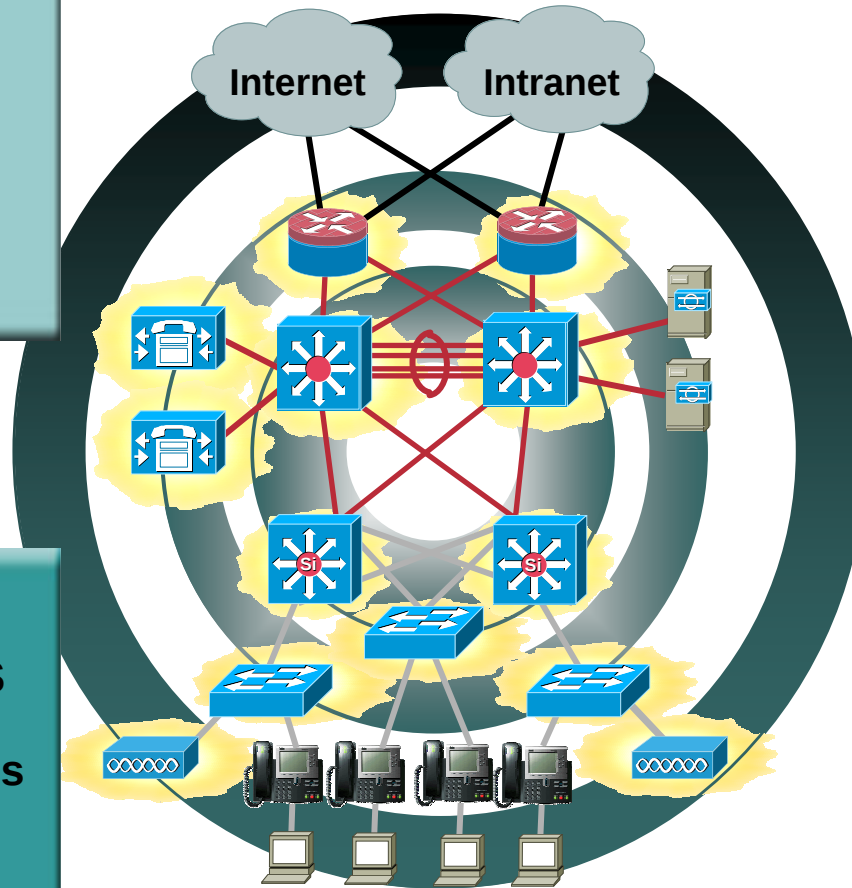


Infrastructure

- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Call Management

- Hardened Windows OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA



Hardened Call Management Platform

- Hardened Win2K OS Shipped By Default, and downloadable from Cisco Connection Online

Every version gets incrementally more secure

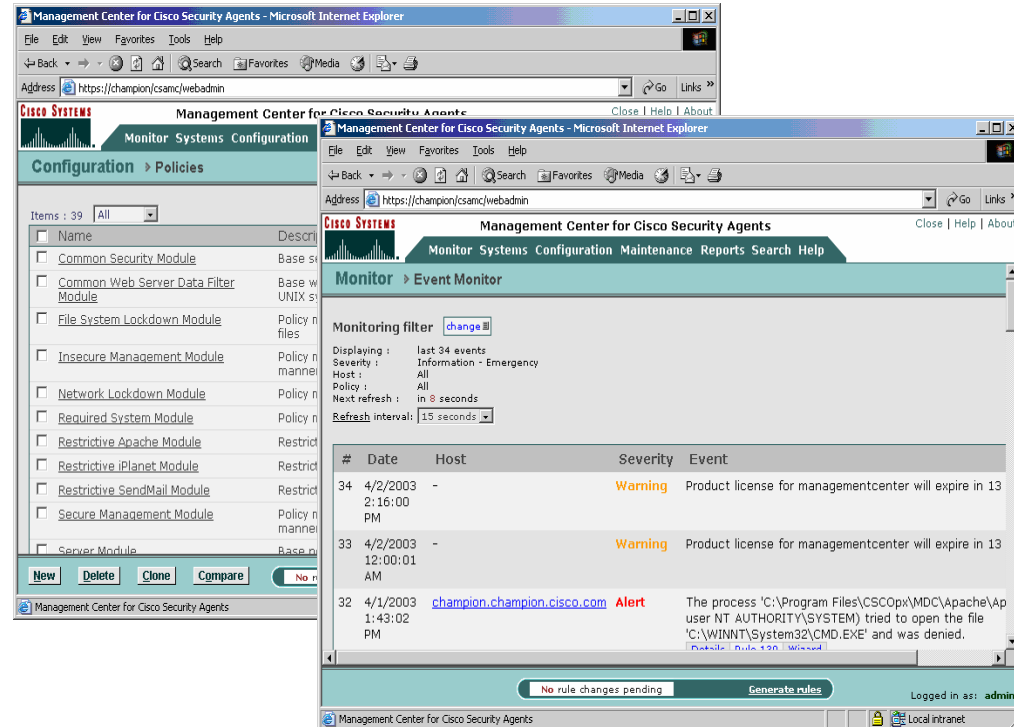
- Aggressive Security Patch and Hotfix Policy
 - Critical: Tested and posted to CCO within 24 hours
 - Others: Consolidated and posted once per month
 - New email alias tells you when new patches are available (http://www.cisco.com/warp/public/779/largeent/software_patch.html)

Sasser patch was available on CCO two weeks before it hit the Internet!

- Install McAfee, Symantec, or Trend Micro ServerProtect Anti-Virus Protection

Integrated Intrusion Prevention

- Cisco Security Agent available for all telephony applications
 - Headless Bundled
 - Managed Optional
- **Policy-Based**, not signature based
- **Zero Updates**
- **“Day Zero”** support
- Centrally administered, with distributed, autonomous policy enforcement
- Effective against existing & previously unseen attacks
- Stopped Slammer, nimda & code red sight unseen with out-of-the-box policies



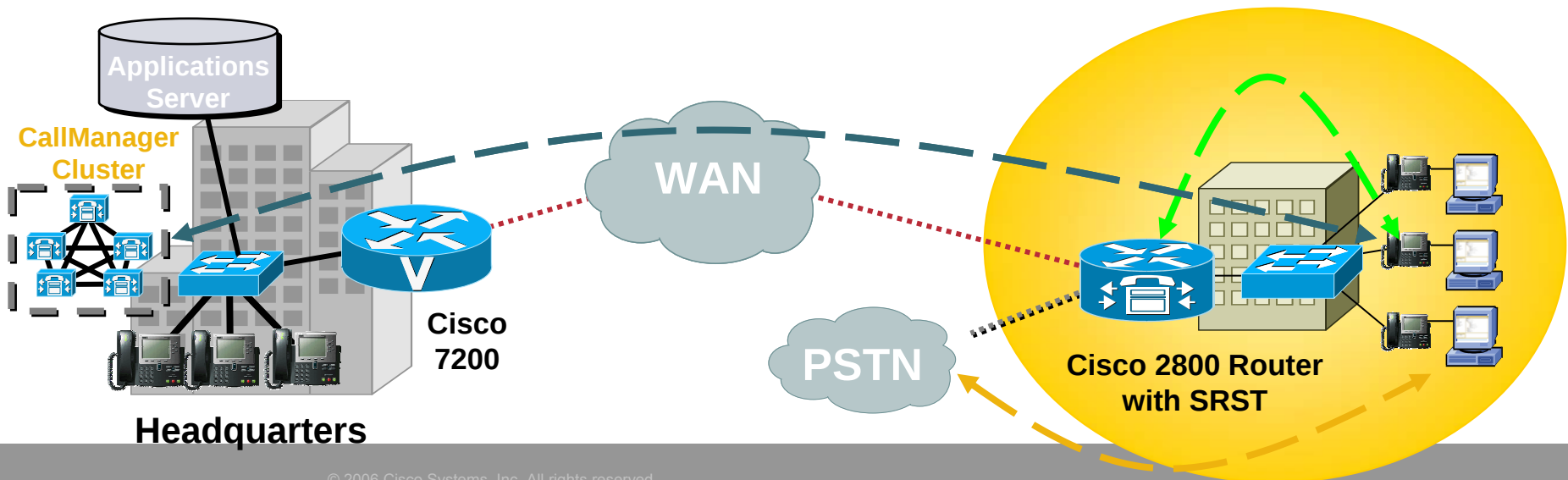
CSA Server Protection:

- Host-based Intrusion Protection
- Buffer Overflow Protection
- Network Worm Protection
- Operating System Hardening
- Web Server Protection
- Security for other applications

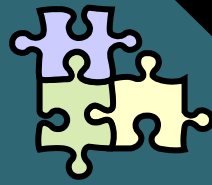
Resilience:

Secure Survivable Remote Site Telephony

- Resiliency for remote IP Telephony users with central CallManager
- Minimizes business impact of WAN link failure:
 - Cisco router auto-configures, provides local call processing -- no manual intervention required
 - SRST IP phone calls remain secure
 - When WAN is available, IP Phones auto-revert back to CallManager



Secure IP Communications Systems Approach in Action

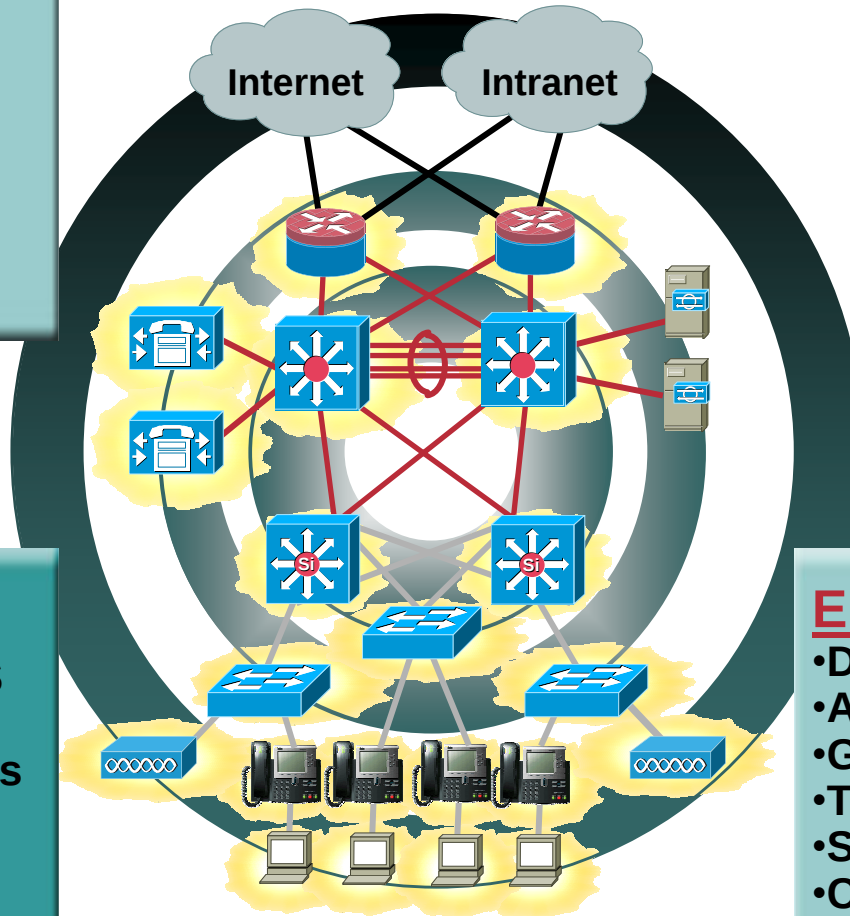


Infrastructure

- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Call Management

- Hardened Windows OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA



Endpoints

- Digital certificates
- Authenticated phones
- GARP protection
- TLS protected signaling
- SRTP media encryption
- Centralized management

Authenticated Endpoints

- **X.509 v.3 certificates in phones and CallManager**

Self-Signed (CCM)

MIC from Cisco Mnfg

LSC from CAPF

Certificates ensure reliable device authentication

- **Scalable solution**
- **Customized Config**
 - Disable PC Port
 - Speaker phone
 - Web Access
 - ...



Stop Rogue Images From Entering Phones

- **Signed Firmware Images**

Guaranteed from Cisco

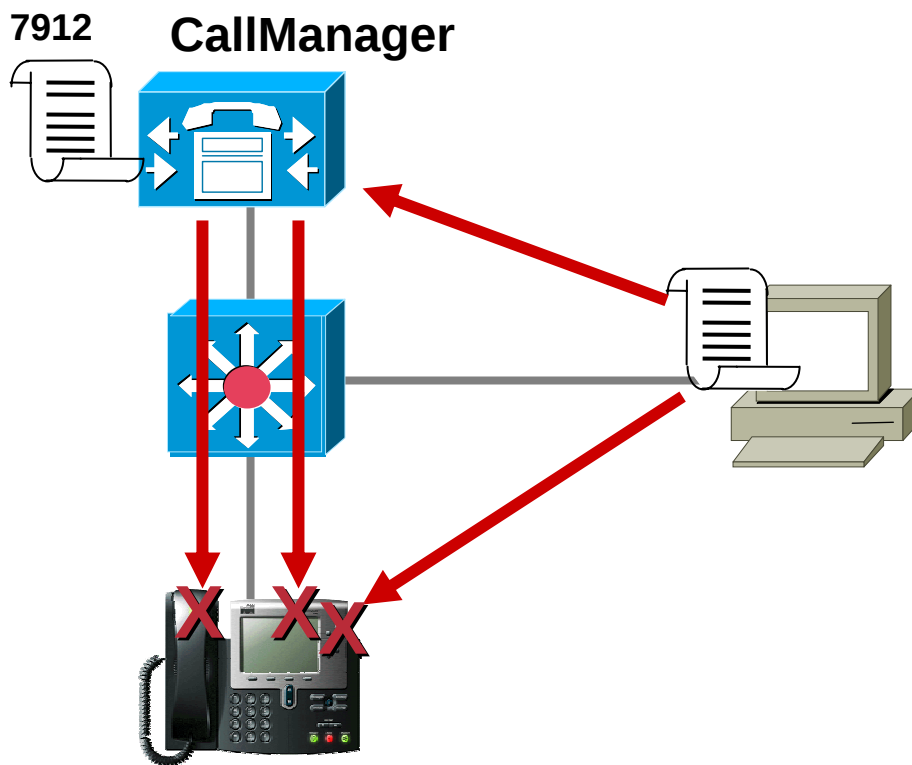
Unique signature for each phone model

Can't subvert security features!

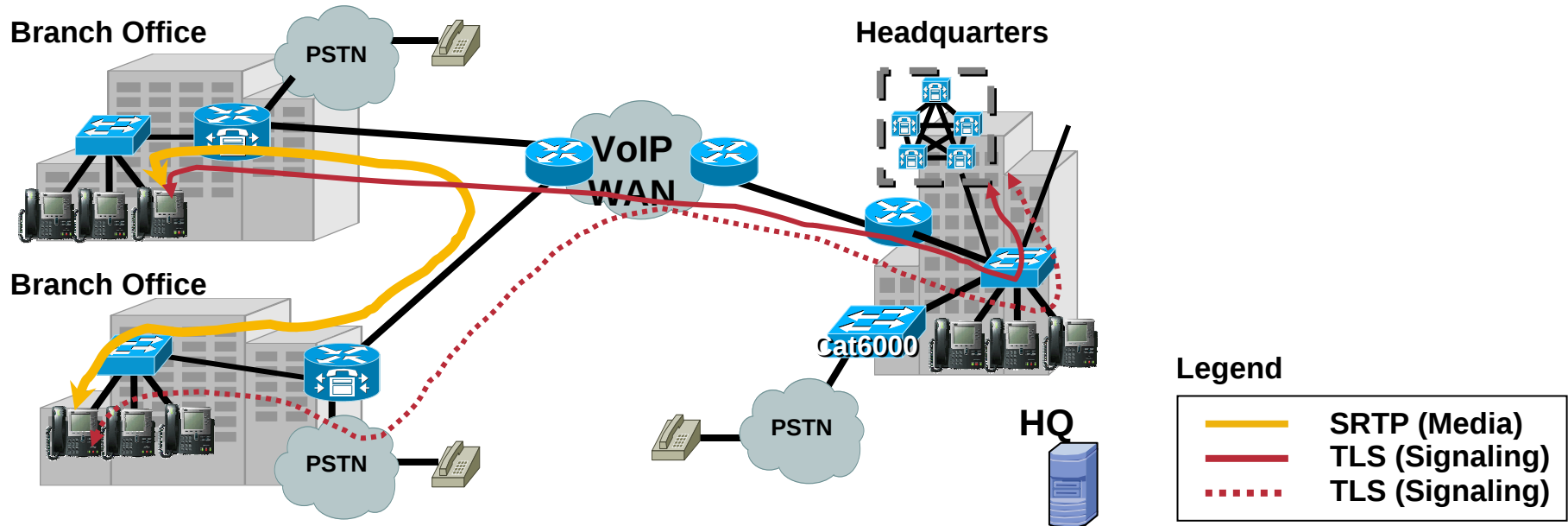
- **Signed Config Files**

7940, 7960 and 7970

CCM 4.0 and above

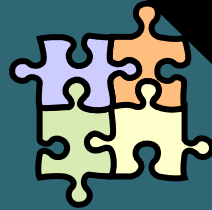


Authentication and Encryption on Cisco CallManager and IP Phones



- Media and signaling authentication and encryption
 - Media authentication and encryption (IP phone to IP phone) uses SRTP
 - Signaling authentication and encryption (IP phone to CCM) uses TLS
- Manufacturing-installed certificates on IP phones
- X.509 certificates on Cisco CallManager
- Digitally-signed IP phone loads

Secure IP Communications Systems Approach in Action



Infrastructure

- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Call Management

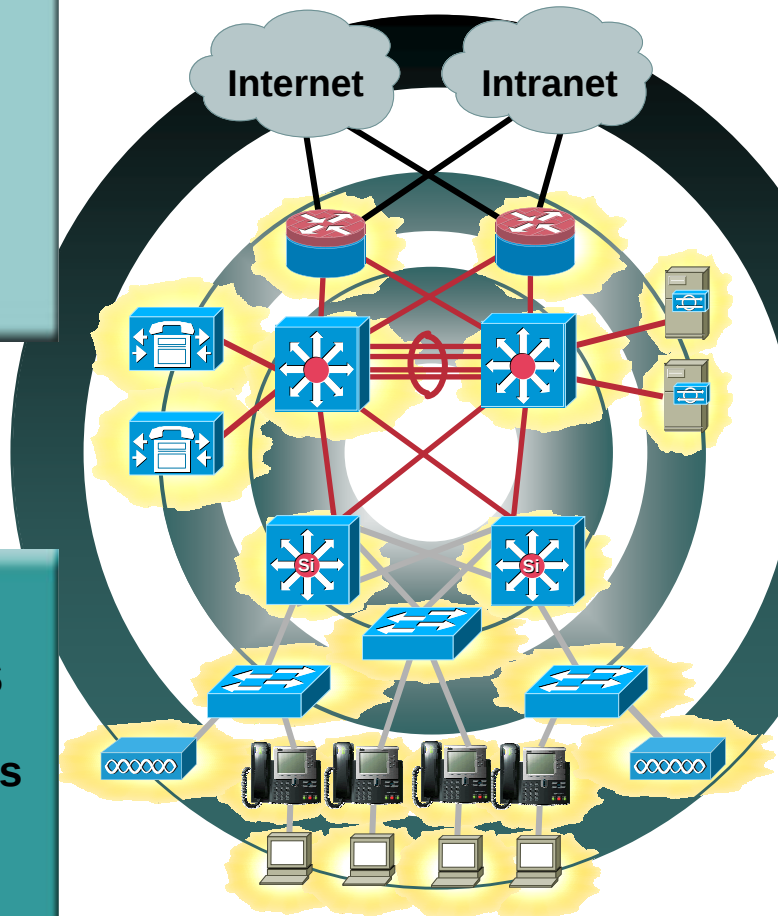
- Hardened Windows OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA

Applications

- Multi-level administration
- Toll fraud protection
- Secure management
- Hardened platforms
- h.323 and SIP signaling

Endpoints

- Digital certificates
- Authenticated phones
- GARP protection
- TLS protected signaling
- SRTP media encryption
- Centralized management



Secure Private Messaging

- **Private**

Only intended recipients can listen to a private message addressed to them

Messages marked private, if (accidentally or intentionally) forwarded, cannot be listened to

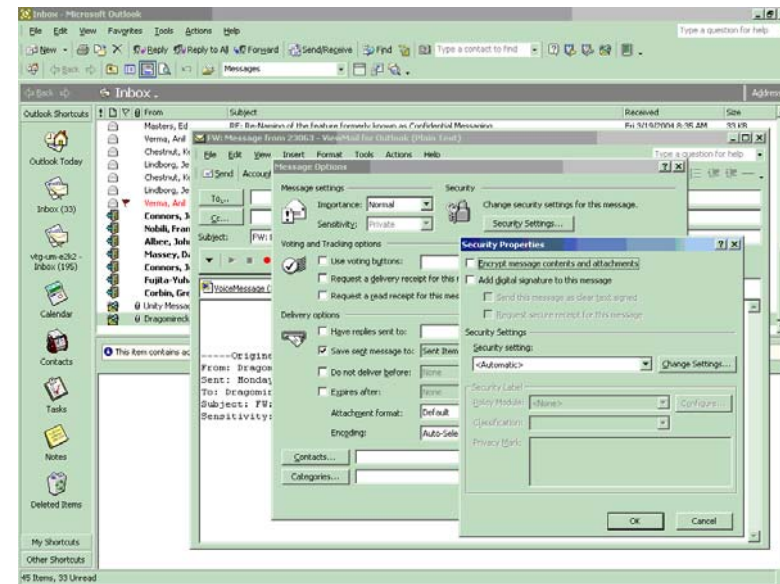
Messages forwarded to internet email addresses or 3rd party voice mail systems (VPIM/AMIS/OctelNet) cannot be listened to

- **Secure**

Actual message content is protected using public-key encryption

Unauthorized users will hear a warning message

Can be set on a per subscriber (all messages from John Chambers) or system-wide (legal firms) basis



Application Platform Protection

- **Carefully hardened platforms**
- **Control access to admin functions**
- **Cisco Security Agent host-based protection**
- **Secure remote management via https**



Multi-Level Admin (MLA)

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Assign Privileges to User Group

[View Privileges Report](#)
[Add a New Functional Group](#)
[Add a New User Group](#)

User Groups

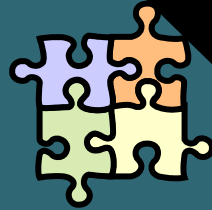
- GatewayAdministration
- PhoneAdministration
- ReadOnly
- ServerMaintenance
- ServerMonitoring
- SuperUserGroup

User Group: GatewayAdministration
Status: Ready

Functional Group	Access Privilege
Standard Feature	Read Only
Standard Plugin	Read Only
Standard Serviceability	Read Only
Standard RoutePlan	Full Access
Standard Gateway	Full Access
Standard Service Management	Read Only
Standard User Privilege Management	Read Only
Standard System	Read Only
Standard Phone	Read Only
Standard Service	Read Only
Standard User Management	Read Only

- Users are added to LDAP directory and assigned to “User Groups”.
- User Groups are then given access to “Functional Groups”.
- Functional Groups have access to individual pages
- LDAP lookups to AD is done over SSL

Secure IP Communications Systems Approach in Action



Infrastructure

- VLAN segmentation
- Layer 2 protection
- Firewall
- Intrusion detection
- QoS and thresholds
- Secure VPN
- Wireless security

Applications

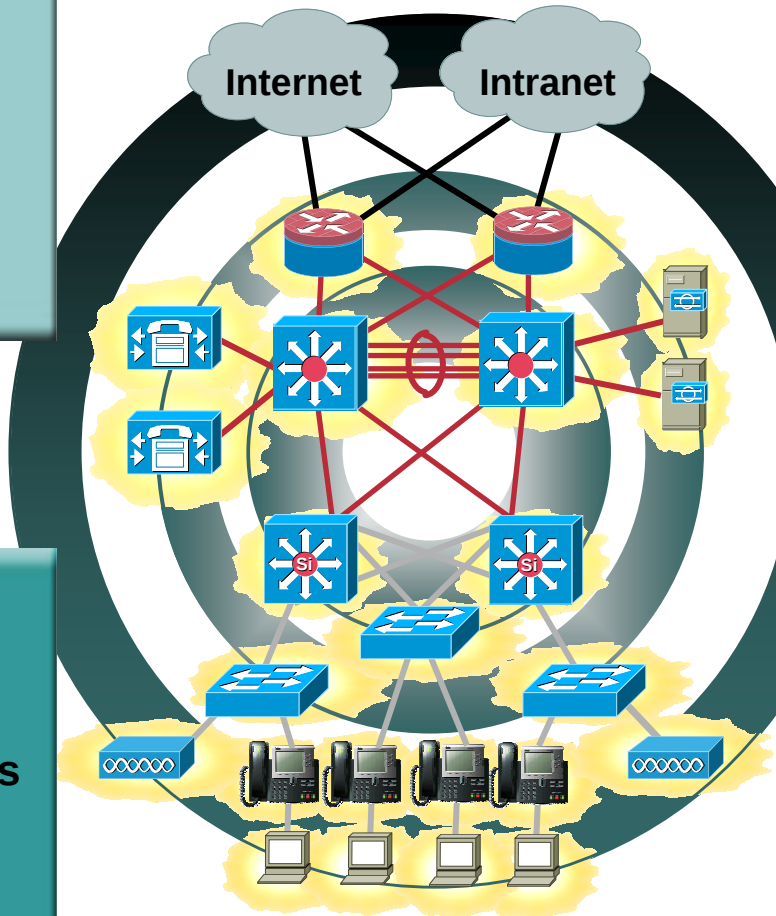
- Multi-level administration
- Toll fraud protection
- Secure management
- Hardened platforms
- h.323 and SIP signaling

Call Management

- Hardened Windows OS
- Digital certificates
- Signed software images
- TLS signaling
- Integrated CSA

Endpoints

- Digital certificates
- Authenticated phones
- GARP protection
- TLS protected signaling
- SRTP media encryption
- Centralized management



Cisco – Independently Recognized as *the* Secure IP Communications Solution

- Cisco is the only vendor to earn Miercom/Network World's highest security rating—May 2004
- BCR – Most secure Large IP-PBX, January, 2005
- BCR – Most secure Mid-Size IP-PBX, February, 2005
- Only fully IP-PBX system to achieve DoD PBX-1 certification - 2005



**BUSINESS
COMMUNICATIONS
REVIEW**

Most Secure IP-PBX
Large-Size



**BUSINESS
COMMUNICATIONS
REVIEW**

Most Secure Mid-
Size IP-PBX



DoD JITC PBX1
Certification

The Intelligent Choice for Secure IPC

- **IP Communications solutions from Cisco can be as secure, or more secure, than traditional PBX systems**

Security remains a top issue of IP Communications customers

Cisco is committed to delivering the most secure, reliable solution possible – at all layers of the network

Recent enhancements further increase the security capabilities of the industry leading Cisco IP Communications solution

Independent testing says Cisco provides the most secure IP Communications solution available*

***As tested by Miercom Labs and reported by Network World**

Q AND A



CISCO SYSTEMS

