

Greatest Perceived Threat: Loss of Information

- POTS maintains an illusion of privacy through system separation
 - No voice encryption
 - Person in wiring closet can listen to calls
- Layer 3 and 4 threats can be mitigated with good security practices
- Application-level threats diminish with identity mechanisms adopted within endpoints and servers

Greatest Actual Threat: Denial of Service

- Need good physical infrastructure design
- Networks must be resilient and support QoS

Cisco® has the most secure VoIP solution in the industry, because Cisco provides means of securing VoIP at more layers than anyone in the industry.

Integrated Voice Security

- Simplifies Network Architecture
- Tighter security
- Easy-to-deploy solutions
- Greater threat manageability

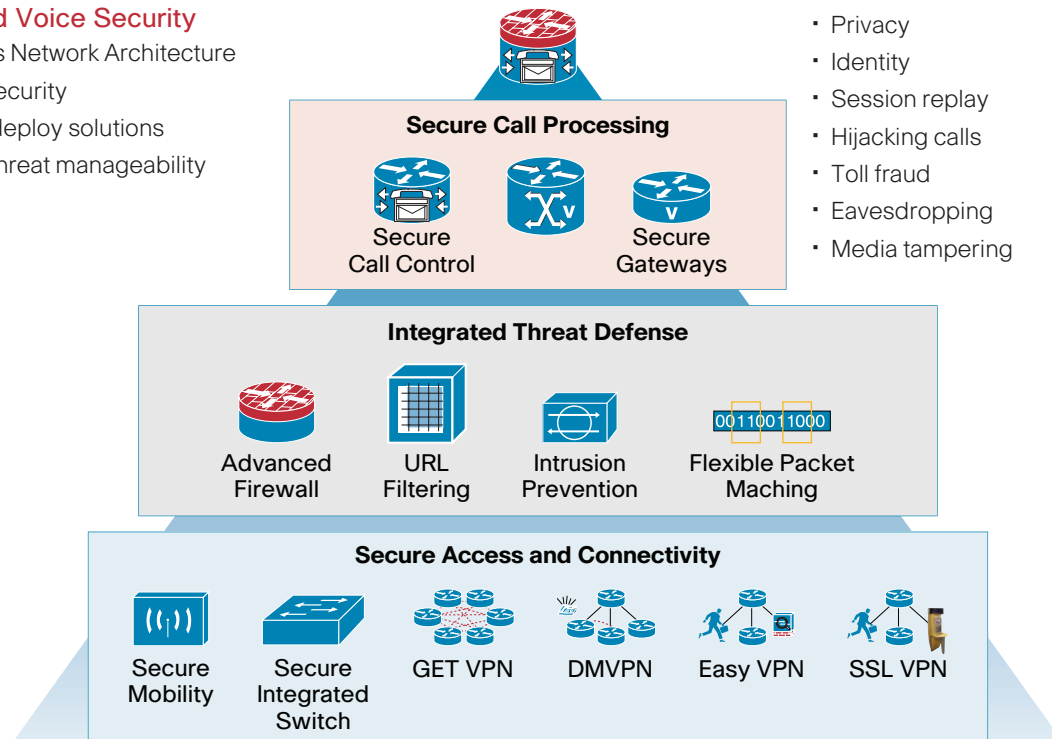
The Secure Network Is the System

- Security applied at multiple layers of the system:
 - Addresses sophisticated blended threats
 - Defends against multiple avenues of attack
- Security integrated within the voice network:
 - Eases provisioning
 - Increases manageability
 - Reduces TCO (compared to an overlay security solution)
 - Enables a coordinated response to attacks

Security is not a product that can be added onto the network. Security is a solution implemented deep within the VoIP network.

Checklist of Mitigated Threats

- DoS
- Privacy
- Identity
- Session replay
- Hijacking calls
- Toll fraud
- Eavesdropping
- Media tampering



Secure Call Processing Highlights

For Cisco Unified Communications Manager Express (CUCME), Cisco Unity Express (CUE), Survivable Remote Site Telephony (SRST) and Voice Gateways

- Secure Administration Access
- Toll fraud prevention
- Wired, Wireless, Soft and Hard Phone authentication and registration
- Identity Protection and Assertion
- Feature access restrictions
- Signaling authentication and encryption via TLS or IPSec to protect voice gateways, endpoints and applications
- Media encryption using Secure RTP (SRTP)

Integrated Threat Defense Highlights

- Integrated zone based Firewall Support for Unified Communications.
- Firewall Application Inspection and Control for signaling and media protection
- Network Virtualization support on the firewall
- Call Rate limiting for DOS Protection
- VoIP Turing based on reputation for SPAM protection
- Topology Hiding

Secure Access and Connectivity Highlights

- A range of QoS enabled site to site VPN architectures optimized to support Unified Communications: DMVPN, GETVPN
- Secure Remote Access with QoS Enabled: SSLVPN, EasyVPN
- Integrated Switch with Power over Ethernet (POE), Phone Detection and trust establishment
- Network Virtualization Support for Unified Communication over IP

Additional Resources

Cisco Secure Unified Communications
www.cisco.com/go/secureuc

Cisco Router Security and VPN Products
www.cisco.com/go/routersecurity