Innovative Kommunikationslösungen - aber sicher:

Mit einer flexiblen und skalierbaren ASA 5500 Security Appliance

Christian Vogt & Michael Hartl, Systems Engineers, Cisco Systems GmbH

Wir zeigen Ihnen,

- an welche Bedrohungsszenarien Sie im Bereich Unified Communications denken müssen.
- welche Teile des Netzes betroffen sein können.
- welche Auswirkungen dies auf ihr Betriebskonzept hat.
- und - wie die Cisco ASA Ihnen hierbei nicht nur helfen kann, sondern auch neue Kommunikationsmodelle ermöglicht.

Agenda

- Unified Communications-Bedrohungen
- Aufbau und Bestandteile eines sicheren UC-Systems
- Die neuen UC-Funktionalitäten der Cisco ASA
  - ASA für Secure Unified Communications
  - ASA TLS Proxy
  - ASA Phone Proxy
  - ASA Presence Federation
  - ASA Mobility Proxy

Unified Communications-Bedrohungen

Heutige Bedrohungen

- Gebührenbetrug
- Unerwünschtes Mithören
- Physical Security
- Social Engineering
- DoS, Würmer, *Virus-De-Jour*
- Rogue Device Insertion

Zukünftige Bedrohungen

- Externe UC-Dienste
  - Secure Mobility
  - Remote Access
- B2B Unified Communications
  - SPIT (SPAM over IPT)
  - Identity Theft
  - External DoS

Vollständige UC-Sicherheit erfordert ein SICHERES Netzwerk UND eine SICHERE IP-Telefonie

Secure Network

Secure Unified Communications

Secure Telephony

Alle Verantwortungsbereiche müssen zusammen arbeiten

"Participation of a cross-section of relevant IT personnel in the planning process is crucial to a comprehensive and actionable UCC strategic plan." Gartner, March 2007

Aufbau eines sicheren UC Systems
Umfassender Schutz aller Bestandteile

Infrastruktur

Sichere Verbindungen und Datentransport

Endgeräte

Authentifizierte IP-Telefone, Soft Clients und andere Geräte

Unified Communications

Vermittlung

Sichere Protokolle für Call Management-Funktionen

Anwendungen

Autoattendant, Messaging, und Kundenpflege

"Network as the Platform"

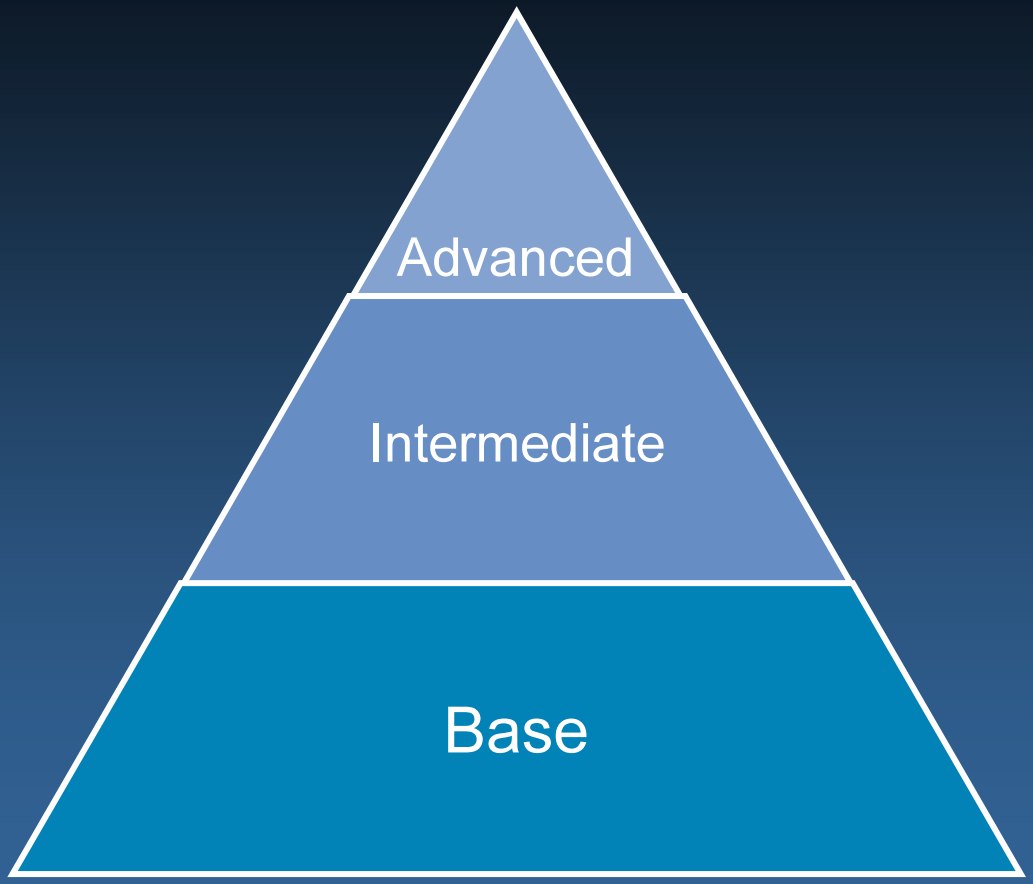
Sprache = Daten

- Sicherheit nicht als Selbstzweck
- Einordnung des Sprachverkehrs anhand der eigenen Geschäftsprozesse
- Prüfung der vorhandenen Sicherheitsrichtlinien, ob Sie den Anforderungen für Sprache ebenfalls genügen

Banking
Oracle
Trading
Billing
POS
Voice
Web Traffic
E-Mail
Directory

Sicherheitsstufen

€€€
Komplexität
Betriebsaufwand



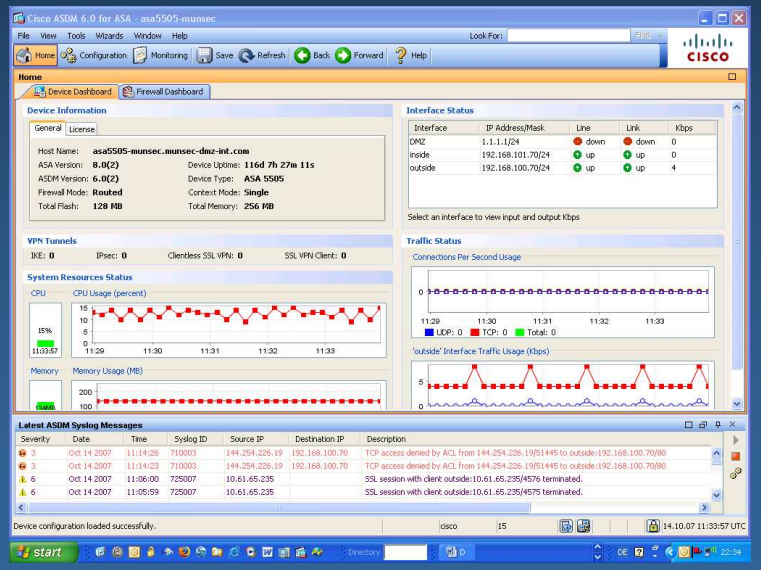
Best Practice für Sichere Unified Communications

Base	Intermediate	Advanced
Basic Layer 3 ACLs	Firewalls mit statefull inspection	Firewall mit erweiterter Application Inspection (inkl. Verschlüsselter Sprache)
Getrennte Sprach/Daten VLAN	Rate Limiting	NAC / 802.1X
Standalone Cisco Security Agent (CSA)	Limit MAC Address Learning	TLS / SRTP zu den Telefonen
Approved Antivirus	Dynamic ARP Inspection	IPSec/TLS & SRTP zu den Gateways
Deaktivieren von Gratuitous ARP	IP Source Guard	TLS/SRTP zu den Anwendungen (Unity)
Smart Ports (Auto QoS)	Dynamic Port Security	Verschlüsselte Config Files
Signierte Firmware and Konfigurationen	DHCP Snooping	Erweitertes O/S Hardening
Classes of restriction (Toll Fraud prevention)	Managed CSA	
Cisco Patches	Intrusion prevention services	

Die neuen UC-Funktionalitäten der Cisco ASA

Cisco *Adaptive Security Appliance* (ASA): Unified Threat Mitigation

- Firewalling
- VPN (S2S, RA)
- Network Services
- IPS (in HW)
- Anti-X (in HW)
- Einfaches und über-sichtliches Management

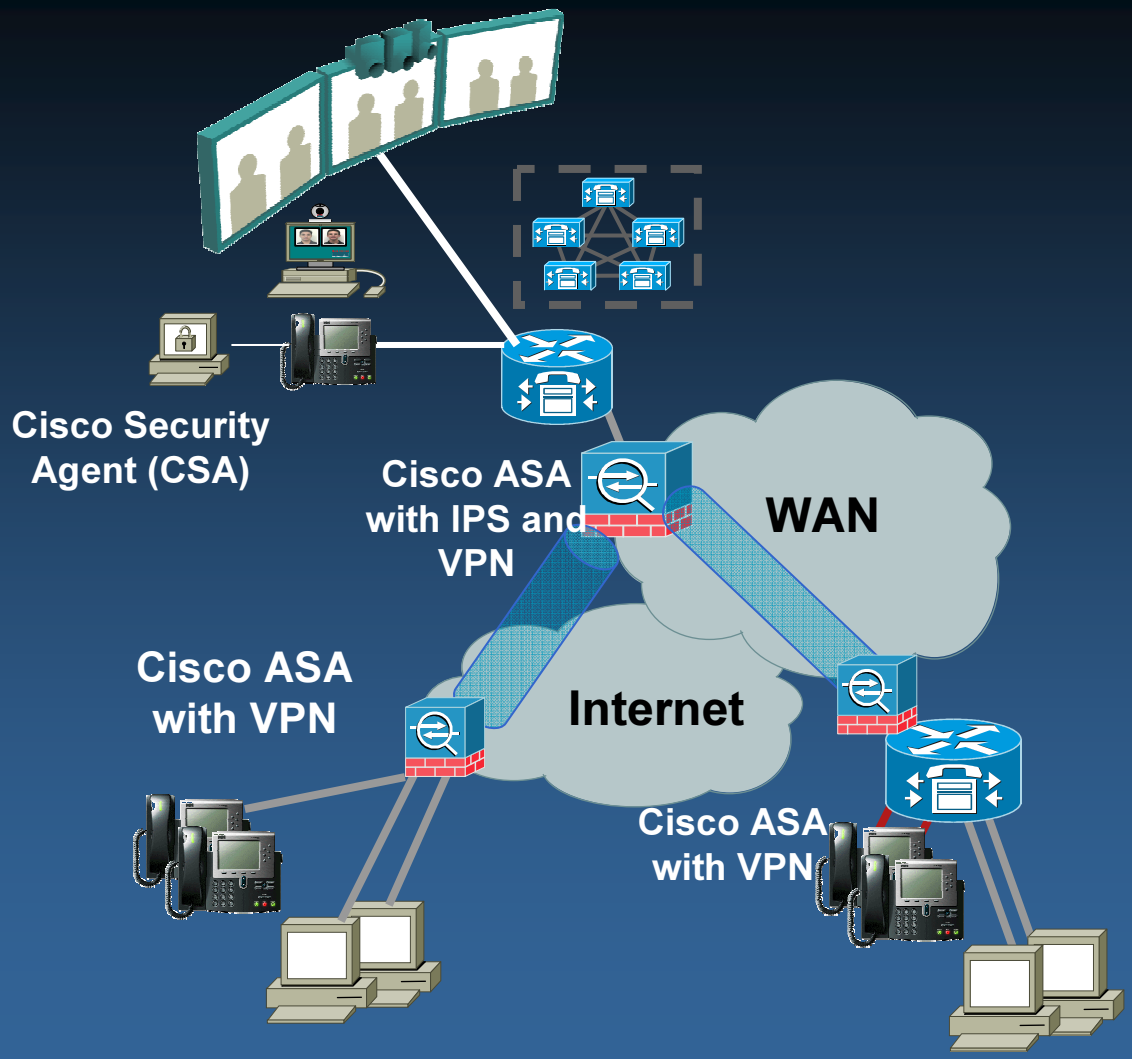


Anforderungen an Firewall-Systeme

- Dynamisches Öffnen von Ports (z.B. RTP,SRTP)
- NAT-Umsetzung
- RFC-Compliance, Protocol Compliance
  - Filtern von Signalisierungsinformationen
  - Verhalten bei „Corrupted Header“ und „Corrupted Packets“
  - DoS (i.e. SIP-Invite Flooding,...)
- Encrypted Voice

ASA für Sichere Unified Communications

Schutz der Telefonie-Infrastruktur

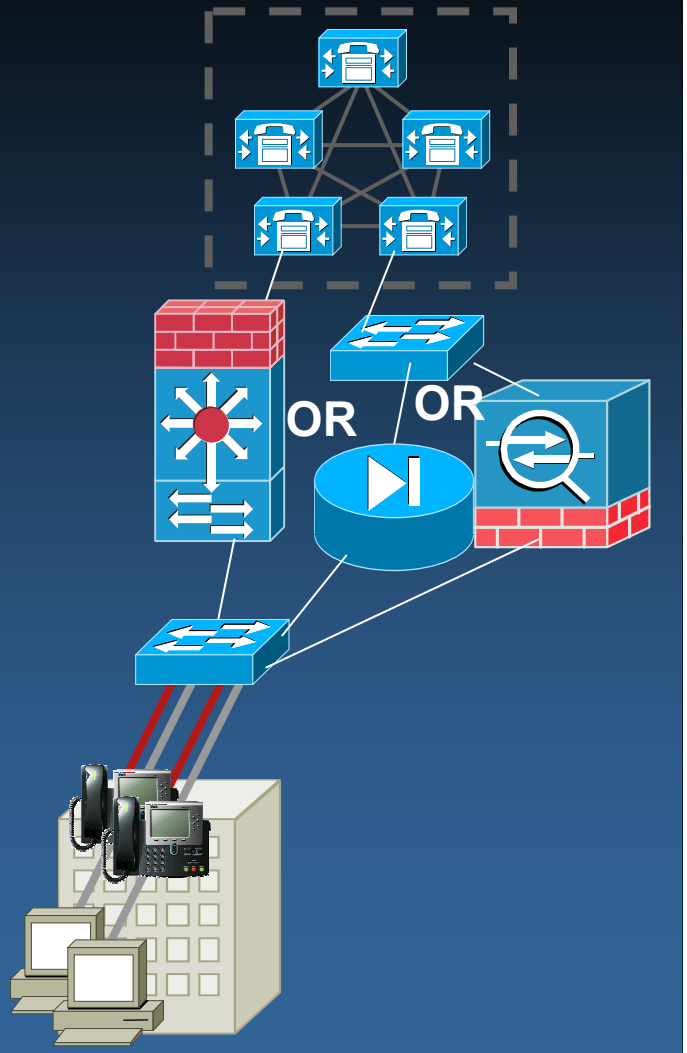


- Gewährleistet SIP, SCCP, H.323, MGCP Standard-konformität
- Schutz vor ungewollten SIP Requests für den Communication Manager
- Begrenzung (Rate Limit) von SIP Requests
- Sicherheitsrichtlinien für Anrufe (whitelist, blacklist, caller/called party, SIP URI)
- Dynamisches Öffnen von Ports für beispielsweise RTP
- Erlaubt nur “Registrierten Phones” den Verbindungsaufbau
- **Ermöglicht Kontrolle von verschlüsselten Verbindungen**

Interoperabilität zum Cisco Unified Communications Manager

ASA Skalierbarkeit
(getestet mit CUCM 6.0)

Phones	Firewall
1-100 phones	ASA 5505, IOS FW
100-250 phones	ASA 5510, IOS FW
250-1500 phones	ASA 5520
1500-22,500 phones	ASA 5540
22,500-30,000 phones	ASA 5550

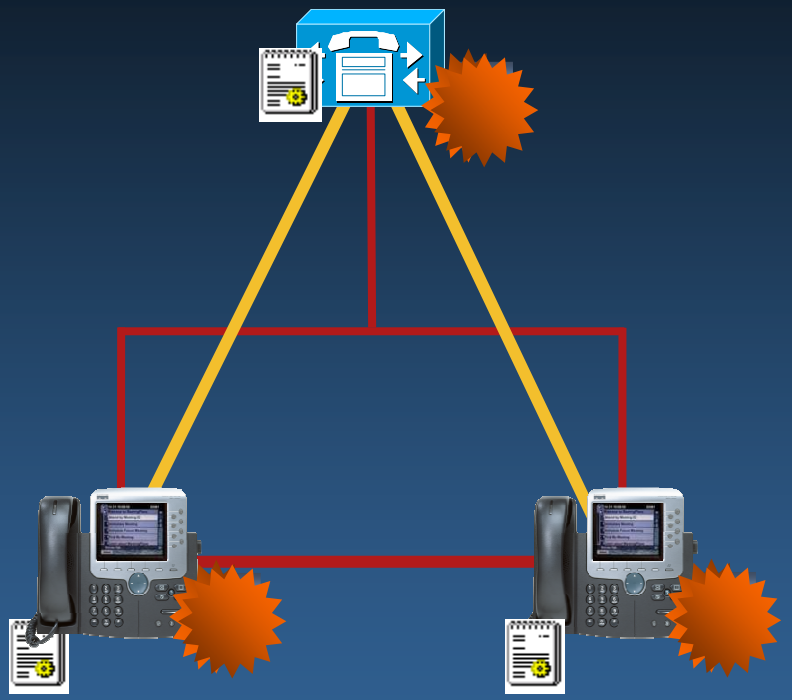


- **FIPS und EAL4 Certified**
- **Inklusive Zertifizierung der UC Protokollunterstützung (SCCP, SIP, H.323, MGCP etc).**

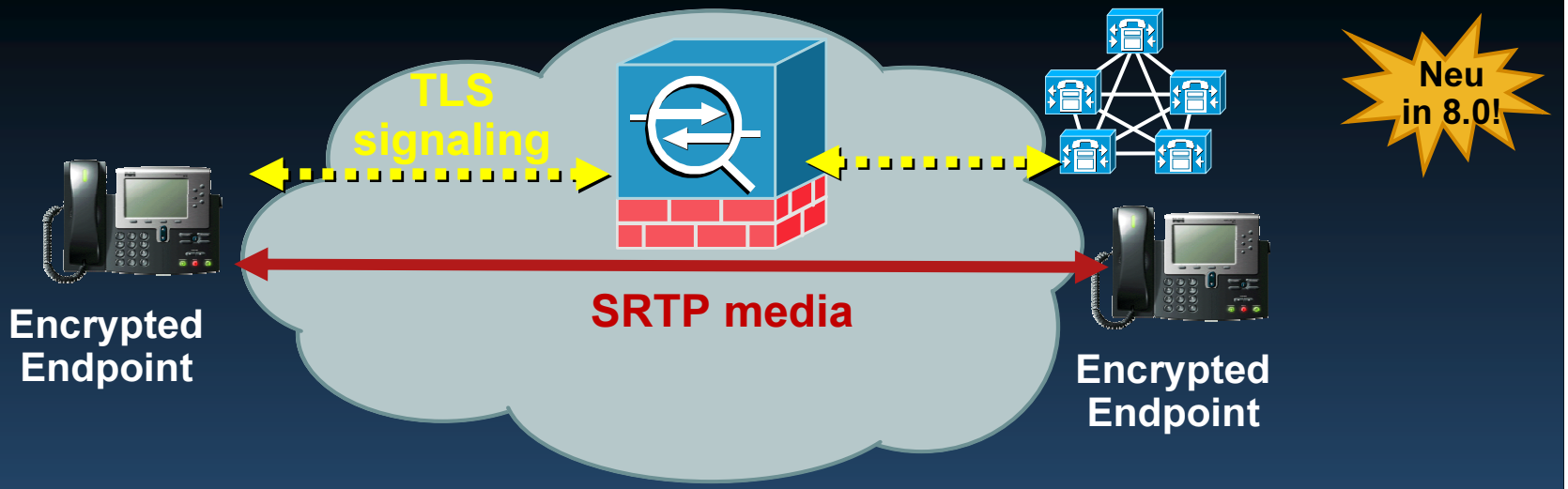
ASA TLS Proxy

Zertifikatbasierte Authentifizierung und Verschlüsselung

- TLS—Transport Layer Security (RFC 2246) schützt die Signalisierung zwischen Cisco CallManager und Endgeräten
  - RSA signatures
  - HMAC-SHA-1 auth tags
  - AES-128-CBC encryption
- SRTP—Secure RTP (RFC 3711) schützt Datenstrom zwischen den Endgeräten
  - HMAC-SHA-1 auth tags
  - AES-128-CM encryption



Integration der Cisco ASA in die TLS Kommunikation zwischen Telefon & CUCM

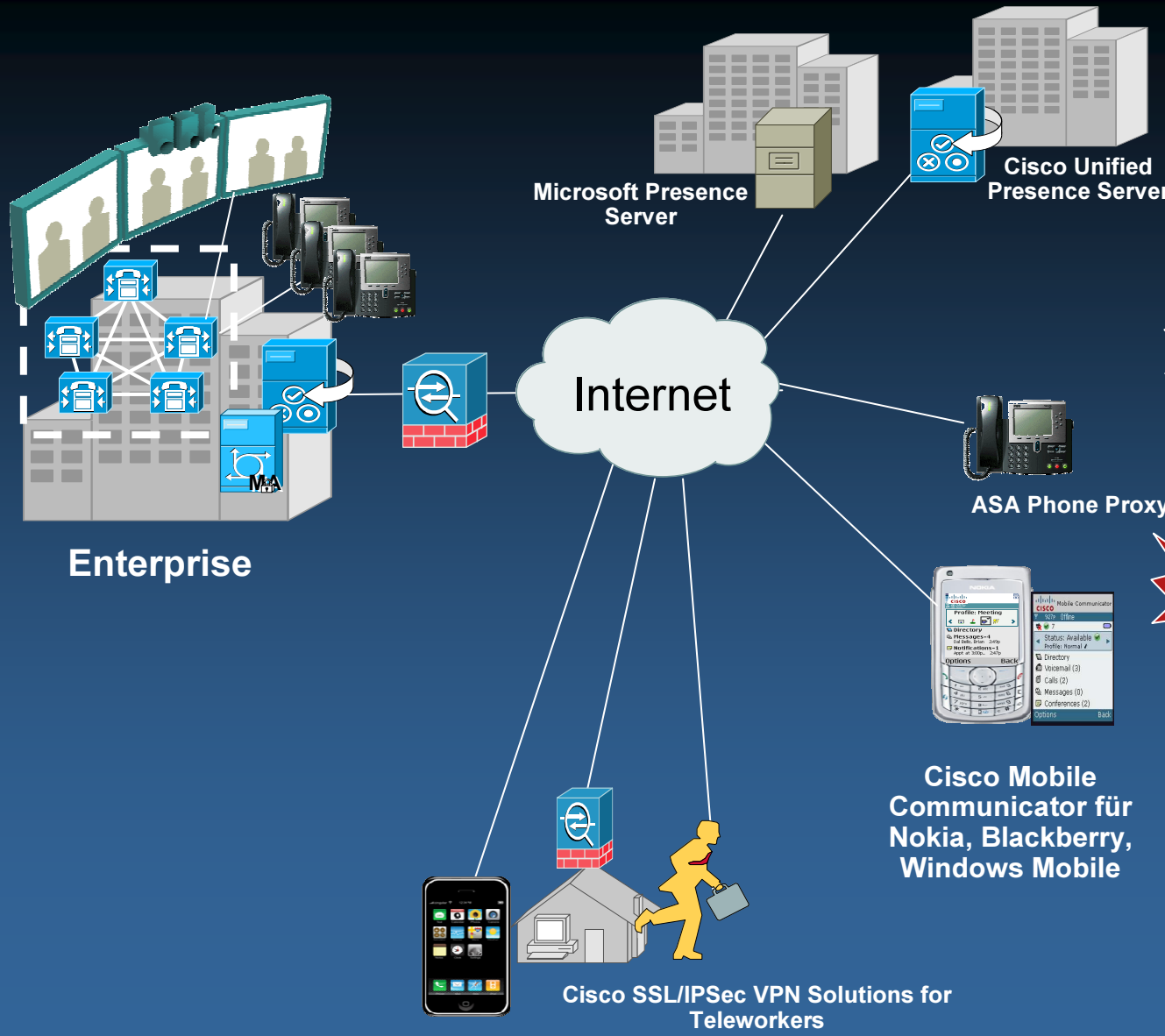


Jede Cisco Voice/Video Kommunikation, welche durch SRTP/TLS verschlüsselt ist, kann nun durch die Cisco ASA 5500 Appliance kontrolliert werden:

- Sichert **Integrität und Vertraulichkeit** der Verbindung bei gleichzeitiger Durchsetzung der Sicherheitsrichtlinien für Voice-Protokolle
- TLS-**Signalisierung wird terminiert und kontrolliert** (dazu ent- und verschlüsselt in Hardware)
- Für den SRTP-Datenstrom werden dynamisch Ports geöffnet und nach Beendigung der Verbindung wieder geschlossen.

Die neuen UC Features in ASA Release 8.0.4

Cisco ASA Release 8.0.4 im Überblick



NEU

Presence Federation
Sichere Kommunikation zwischen externen Presence Servern von MS und Cisco

NEU

Phone proxy
Terminiert SRTP/TLS-verschlüsselte Telefone (und interne Softphones)

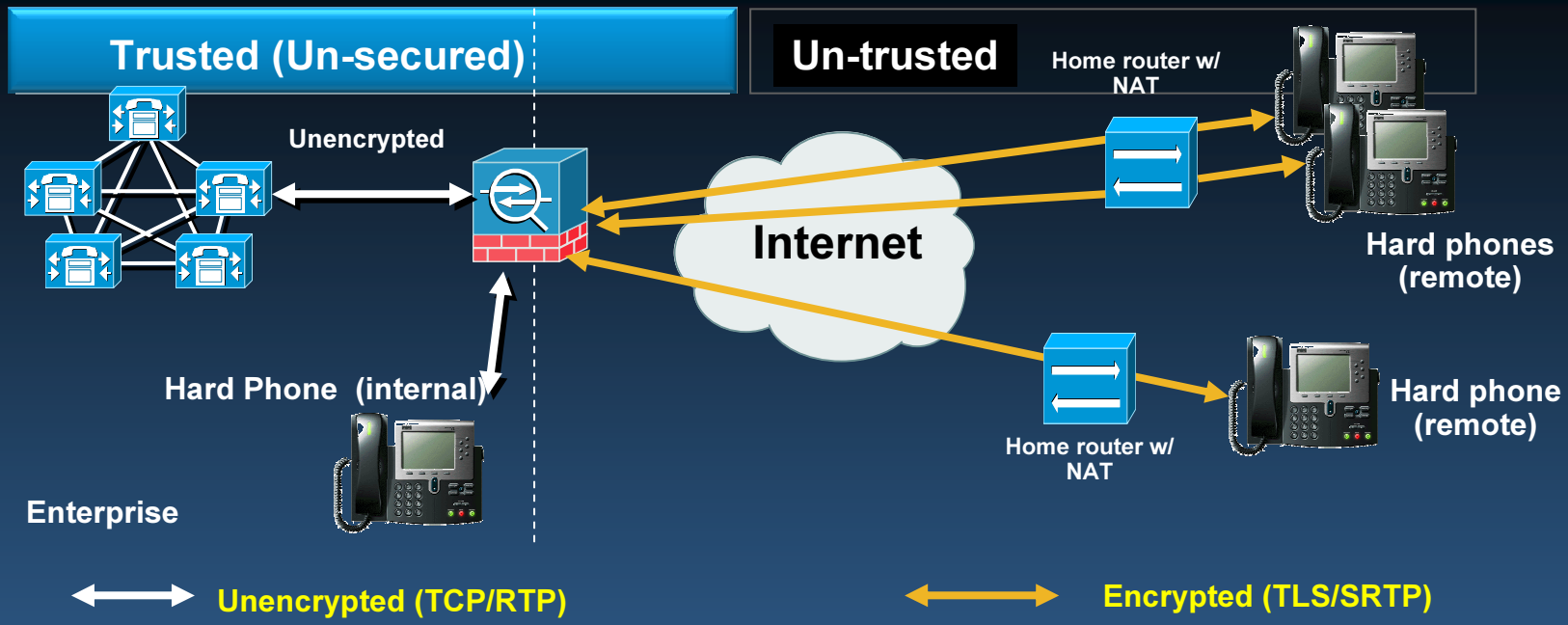
NEU

Mobility proxy
ASA terminiert TLS Signalisierung von mobilen Endgeräten und setzt Sicherheitsrichtlinien durch

VPN solutions
ASA unterstützt weitere Sicherheitsfunktionen – SSL/IPSec VPN Clients und Linksys VPN phones

ASA Phone Proxy

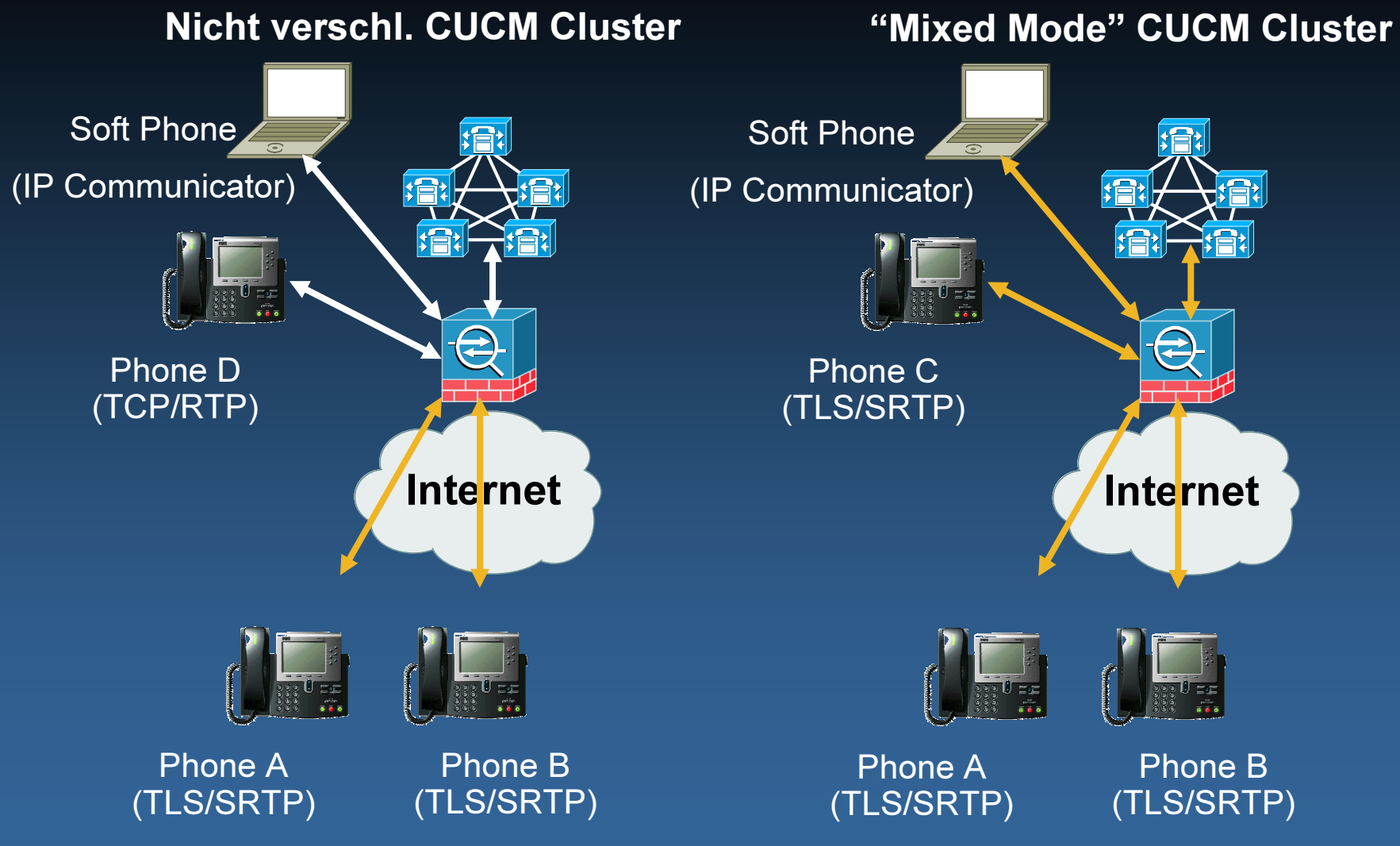
Cisco ASA Phone Proxy



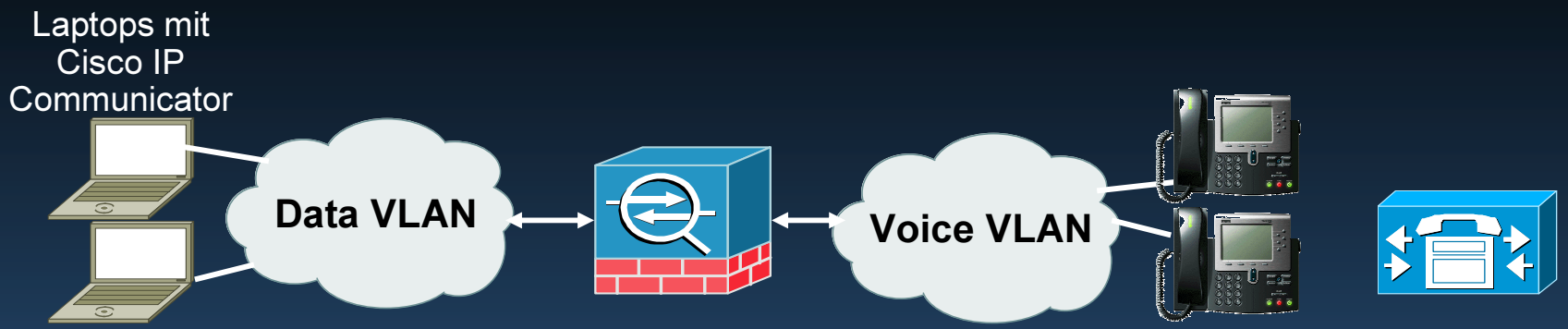
Der ASA Phone Proxy bietet folgende Funktionen:

- **Sichere Signalisierung und Medienstromübertragung für Telefone in Aussenstellen ohne VPN Anbindung**
- **Zertifikatsbasierte Authentifizierung**
- **Terminiert TLS Signalisierung des Telefons und initiiert TCP zum CUCM**
- **Terminiert SRTP und initiiert RTP/SRTP zum angerufenen Teilnehmer**

ASA Phone Proxy für Remote Access

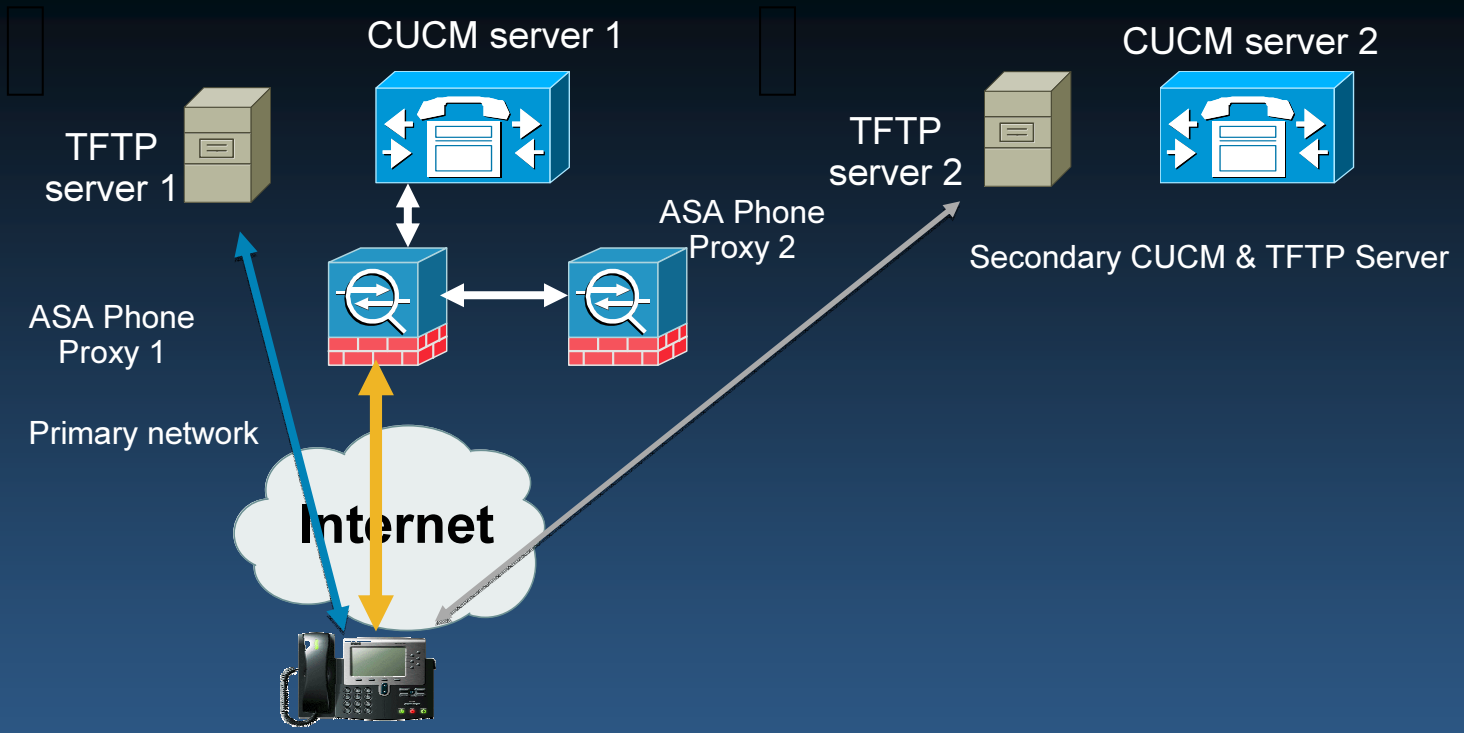


VLAN Traversal (Voice & Daten VLAN) mit Phone Proxy



- Ideal für Firmen, die den IP Communicator einsetzen wollen, aber sichere Trennung von Voice und Daten VLAN wünschen.
- PhoneProxy erlaubt dem Kunden die Voice-/Daten-Trennung aufrecht zu erhalten und nicht den vollständigen Datenverkehr für den IP Communicator freizugeben
- Zu diesem Zweck wird die IP Communicator-Verbindung durch den ASA Proxy terminiert

ASA Phone Proxy Failover Szenario



Failover Optionen:

- **CUCM 1 fällt aus -> Telefonfunktion wird vom CUCM 2 übernommen. Keine Auswirkungen auf den ASA Phone Proxy**
- **TFTP server 1 fällt aus -> Telefon verbindet sich mit TFTP server 2. Keine Auswirkungen auf den ASA Phone Proxy**
- **ASA phone proxy 1 fällt aus -> Stateless failover auf ASA phone proxy 2. Private keys, Zertifikate werden mit primary synchronisiert. Aktive Sessions werden in Phase 1 nicht repliziert.**

UC Proxy-Lizensierung (release 8.0.4)

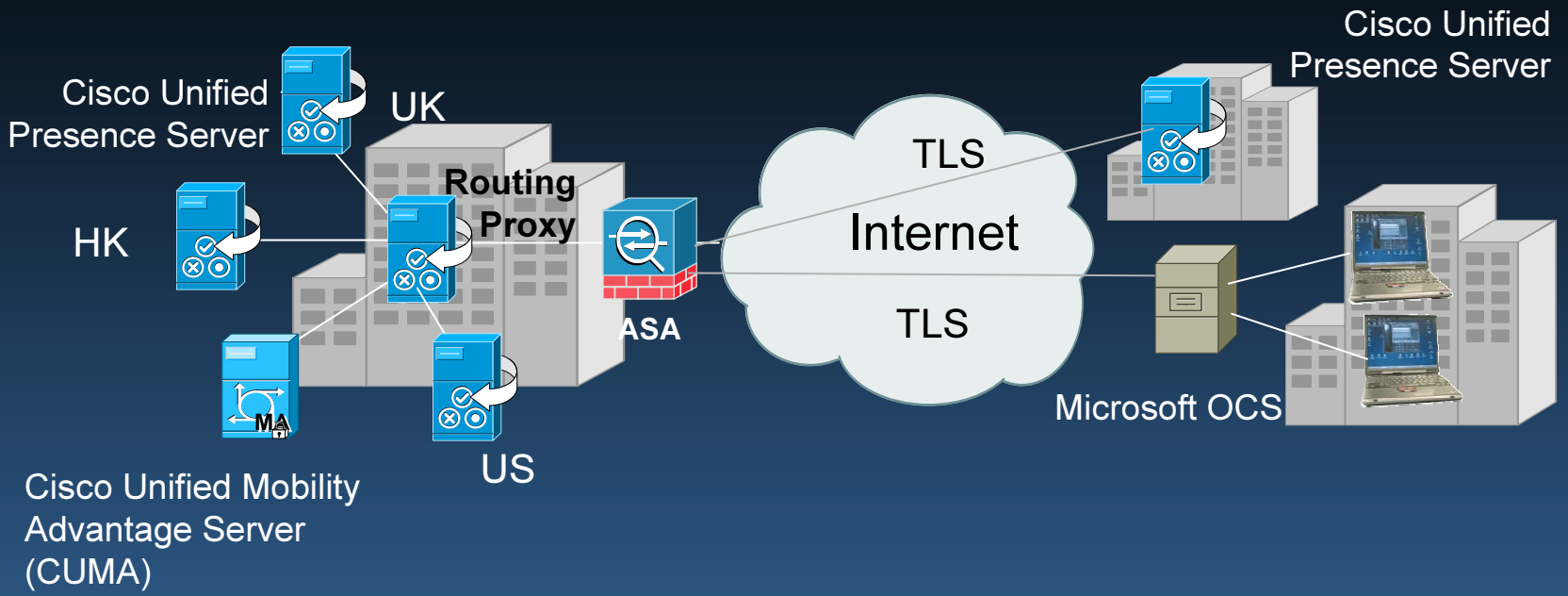
ASA Platform	Tiers for Licenses	Max UC Proxy Licenses
ASA 5505	24	24
ASA 5510	24, 50, 100	100
ASA 5520	24, 50, 100, 250, 500, 750, 1000	1000
ASA 5540	24, 50, 100, 250, 500, 750, 1000, 2000	2000
ASA 5550	24, 50, 100, 250, 500, 750, 1000, 2000, 3000	3000

- Eine UC Proxy-Lizenz entspricht einer TLS Proxy Session
- Zwei UC Proxy-Lizenzen in der ASA-Basislizenz enthalten

ASA Presence Federation

Cisco ASA und “Presence”

Austausch von Präsenzinformationen über Unternehmensgrenzen



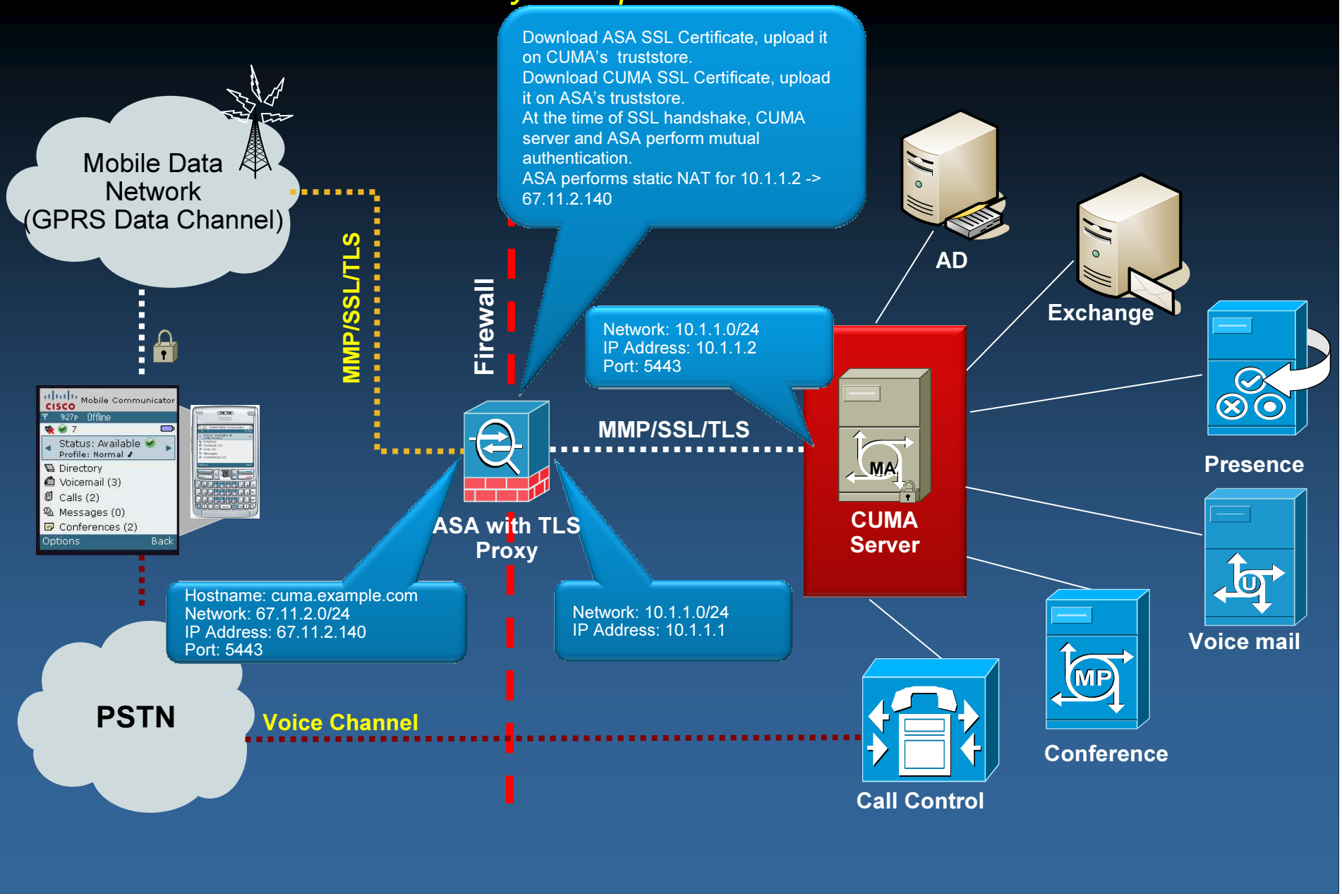
Die Cisco ASA bietet Sicherheit für “Presence” Kommunikation über Firmengrenzen hinweg

- **Firmen mit Cisco Presence Servern können sicher mit Cisco oder Microsoft Presence Servern kommunizieren**
- **Presence Informationen können zwischen Firmen ausgetauscht werden**
- **Alle Cisco UC-Sicherheitsmerkmale werden auf die Presence Informationen angewendet**

ASA Mobility Proxy

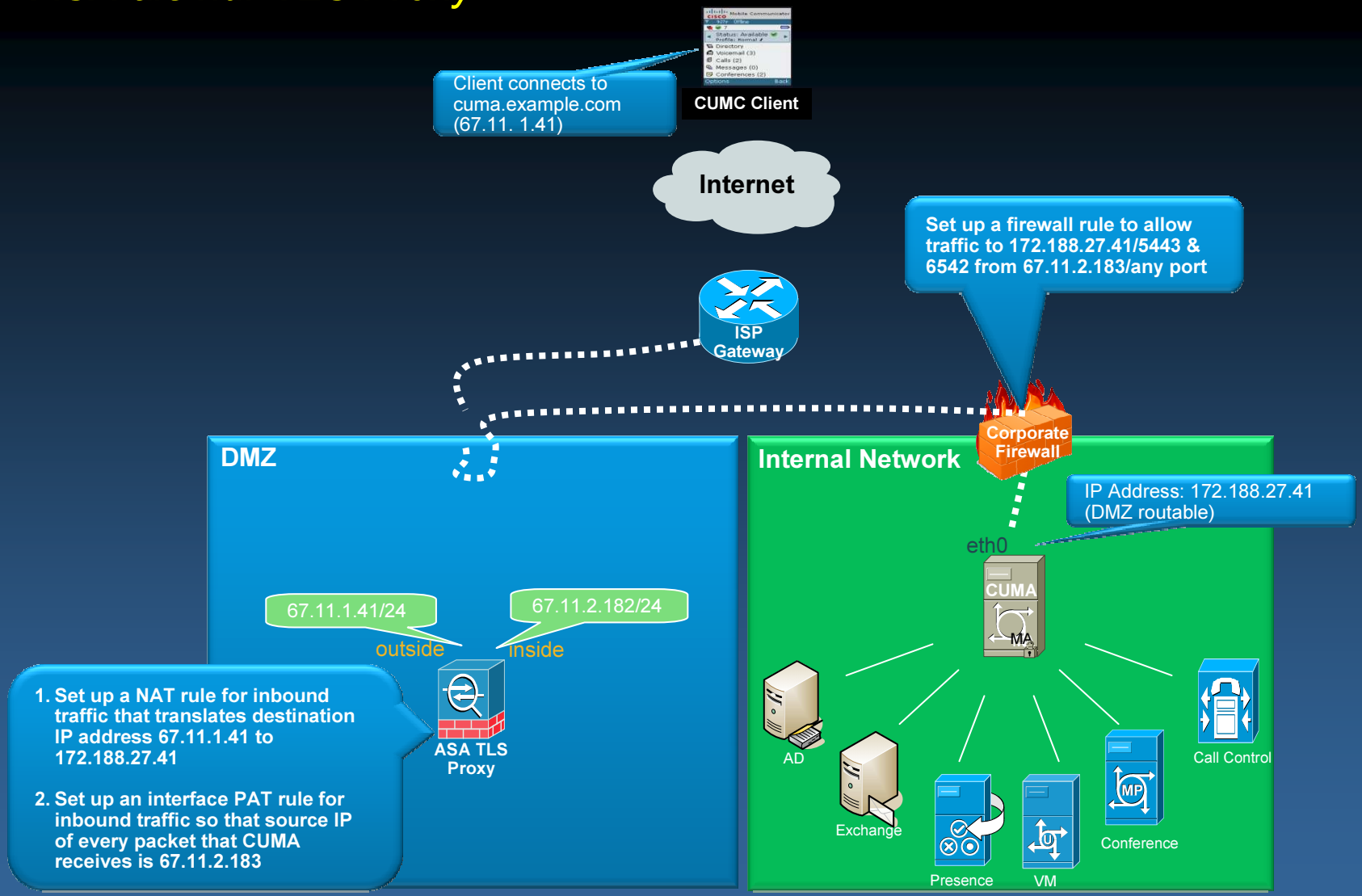
CUMC/CUMA Architektur - Szenario 1

ASA als Firewall & TLS Proxy - Empfohlen



CUMC/CUMA Architektur - Szenario 2

ASA als nur TLS Proxy



Zusammenfassung

- Aus dem Technologiewechsel hin zu IP ergeben sich auch neue Bedrohungen für die Telefonie.
- Daher: Security muss fester Bestandteil des UC Designs sein.
- UC Security erstreckt sich auf mehrere Bausteine.
- Die Cisco ASA 5500 bietet eine Reihe neuer UC spezifischer Leistungsmerkmale:
  - TLS Proxy
  - Phone Proxy
  - Mobility Proxy
  - Presence Federation
- Insbesondere Phone Proxy & Presence Federation ermöglichen völlig neue Designs bzw. Geschäftsmodelle.

Weitere Informationen

- http://www.cisco.com/go/secureuc