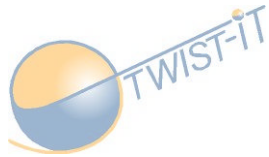


2M05: Sicherheit von IP-Telefonie

Referent:

Christoph Bronold

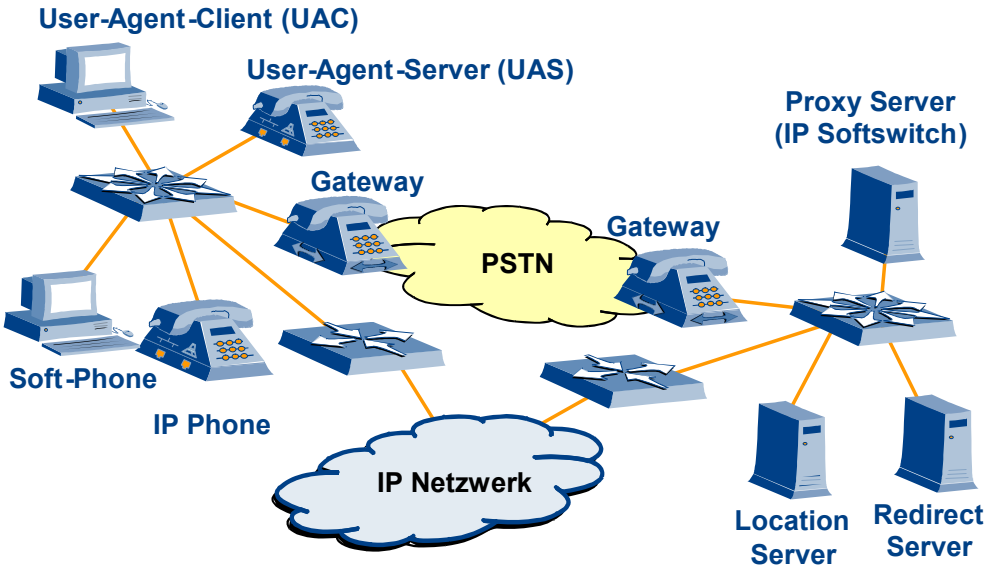
BKM Dienstleistungs GmbH

Agenda

- Bedrohungen und Angriffe auf IP-Telefonie Systeme
- Sicherheitsmaßnahmen für IP-Telefonie Systeme
- Best-Practices
- Designrichtlinien für sichere IP-Telefonie Systeme

TWIST-IT

Bedrohungen und Angriffe auf ein IP-Telefonie System



Viele IP-Telefonie Systeme basieren auf SIP

- **Bedrohungen:**
  - Abhören von IP Telefongesprächen
  - Fälschung der Identität des Anrufers
  - Fälschung der Identität des Angerufenen
  - Veränderung des Status von Endgeräten
  - „Lahm legen“ des IP Telefons
  - Kostenlos oder auf Kosten anderer telefonieren
  - SPIT (Spam over Internet Telephony) Anrufe
- **Angriffe:**
  - Manipulation der Zugangsdaten
  - DoS Attacken auf IP Telefon oder PC mit Soft-Phone
  - Auslesen der Netzwerk-Konfiguration vom IP Telefon
  - Exploits gegen die IP Telefonieapplikation

Bedrohungen und Angriffe: IP Telefon

- **Bedrohungen:**
  - „Lahm legen“ der IP Telefonanlage
  - Ausspionieren von Zugangsdaten und Abrechnungsdaten
  - Manipulation der Eingangzeitpunkt von Nachrichten (Voice Mail etc.)
  - Manipulation von Registrierungs- und Lokalisierungsinformationen
  - Änderung des Status eines Rufes
- **Angriffe:**
  - Manipulation der Signalisierungsdaten
  - DoS Attacken gegen das Betriebssystem (Windows/Linux)
  - Exploits gegen die IP Telefonieapplikation
  - Viren oder Trojaner auf den Server einschleusen

Angriffsziel: IP Telefonanlage

- **Bedrohungen:**
  - Hacker möchte Datenpakete von fremden Stationen mit abhören und/oder manipulieren (Man-in-the-Middle Attack)
  - „Lahm legen“ des Netzwerks
- **Angriffe:**
  - CAM Table Overflow
  - VLAN Hopping (Switch Spoofing, Double Tagging)
  - Spanning-Tree Protocol (STP) Manipulation/Attacken
  - MAC Spoofing/ARP Spoofing
  - Private VLAN Attacks

Bedrohungen und Angriffe: Layer 2 Netzwerk

- **Bedrohungen:**
  - Hacker möchte das Netzwerk zu seinem Gunsten manipulieren
  - Einschleusung von eigenen Systemen
- **Angriffe:**
  - DHCP Starvation/Rogue DHCP Server
  - Routing Protocol Attack/Manipulation/Route Injection
  - HSRP- und VRRP Angriffe
  - ICMP Redirect
  - IRDP Spoofing
  - IP Spoofing

Bedrohungen und Angriffe: Layer 3 Netzwerk

Bedrohungen und Angriffe: Layer 4 - 7 Netzwerk

- **Bedrohungen:**
  - Hacker möchte das Netzwerk zu seinem Gunsten manipulieren
  - Einschleusung von eigenen Systemen
  - "lahm legen" von IP-Telefonie Systemen und Netzwerken
- **Angriffe:**
  - SYN Flood
  - Ping Flood
  - Malware Angriffe (Viren, Würmer, Trojaner etc.)
  - Exploits
  - DNS Spoofing
  - Password Sniffing

Sicherheitsmaßnahmen für IP-Telefonie Systeme

Sicherheitsmaßnahmen für SIP-basierte Telefonie

- **Authentisierung von SIP Nachrichten:**
  - HTTP Digest (RFC 2617/RFC 3261)
- **Verschlüsselung von SIP Nachrichten:**
  - S/MINE (RFC 3851 Version 3.1)
    - Nur SDP Body (= Inhalt einer SIP Nachricht)

  - TLS 1.0 (RFC 2246)
    - Sicherheit auf der Transportschicht

  - IPsec (RFC 2401 ff.)
    - Sicherheit auf der Netzwerkschicht

Sicherheitsmaßnahme für Spracheübertragung

- **The Secure Real-time Transport Protocol (SRTP) (RFC 3711):**
  - Schlüsselmanagement
    - z.B. Multimedia Internet Keying (MIKEY)
  - Verschlüsselung
    - AES-CTR (128 Bit Blöcke)
    - AES-f8
  - Authentifikation und Integrität
    - HMAC-SHA1 (nur 80 Bits von 160 Bits verwendet)


TWIST-IT
Best-Practices
© 2006 BKM Dienstleistungs GmbH


Verschlüsselung der Gespräche
Authentifizierung
Primäre Authentifizierung erfolgt über MAC Adresse
MAC Adressen können gespooft sein
Einige IP Telefone haben Basis-Authentifizierung durch anmelden am Telefon (nur 4-stellige PIN)
Jeder Benutzer benötigt einen Usernamen und Passwort
PC-basierte IP Telefonie-Software ist unsicher
PC ist immer verletzbar (OS, Applikationen, Softphone)
Keine VLAN-Trennung von Sprache und Daten möglich
Getrennte VLANs für Sprache und Daten
Best-Practices: IP Phones
14

- **Automatische Registration von unbekannten IP Telefonen abschalten**
- **Aktivierung einer Firewall:**
  - Nur bekannte VoIP Stationen (IP Hard-/Soft-Phone, Gateways, etc.) zulassen
  - Anzahl der Management Stationen einschränken und Zugriff nur über SSH/HTTP/IPsec erlauben
- **Immer alle Security-Patches einspielen**
- **Alle unnötigen Services im Server ausschalten**
- **Installation von HIDS und Security Agents auf den Servern**
- **Redundante Systeme**

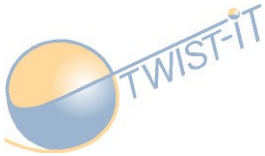
Best-Practices: IP Softswitch

- **Separates VLAN für Daten und Sprache**
  - Private VLAN optional für Sprache
  - Separate VLANs für IP Telefone und Gatekeeper und Voice-Mail System
  - Deaktivierung von nicht benutzten Ports an den Ethernet Switches
- **Authentifizierung der Stationen mittels IEEE 802.1x**
- **Implemenation von Quality of Service:**
  - DiffServ
  - Call Admission Control (Bandbreitenüberwachung mit RSVP)
- **NIDS/NIPS zur Erkennung und Abwehr von Angriffen**
- **IPsec für die sichere Übertragung über das LAN**
- **Redundante System (Switch, Router, etc.)**

Best-Practices: Netzwerk

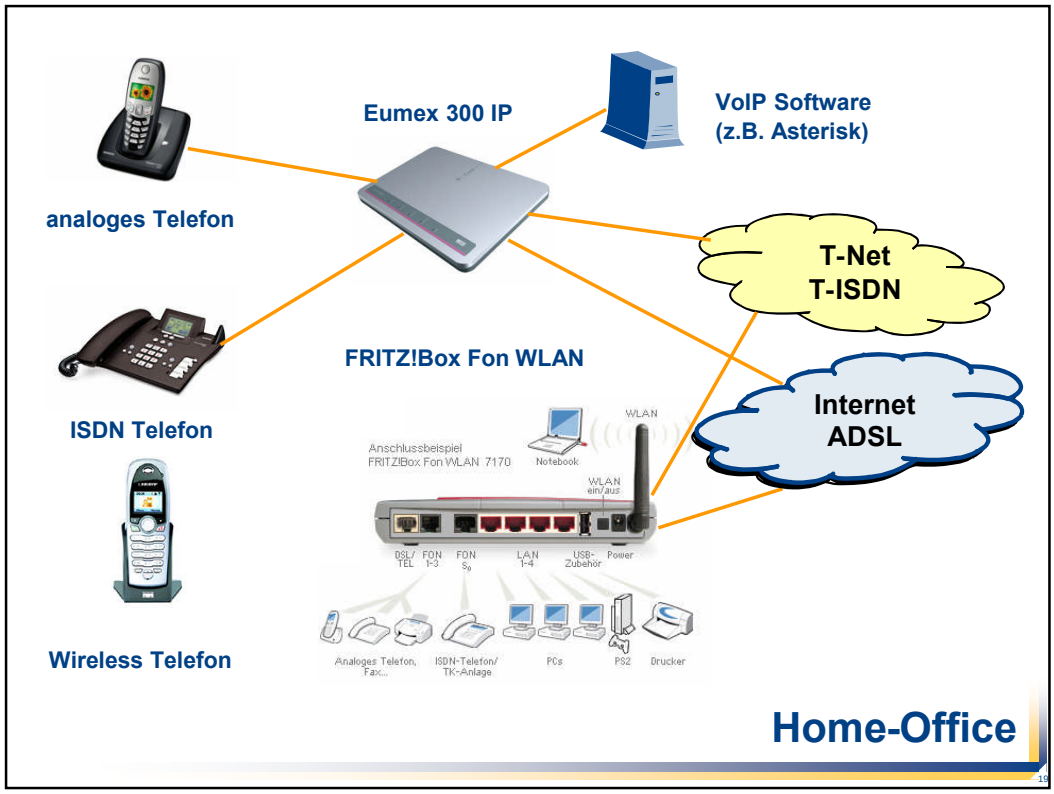
- **Firewall trennt IP Telefone vom IP Softswitch ab**
  - Jeder Voice Traffic soll durch die Firewall gehen (zwischen IP Telefon und IP Softswitch)
  - Filterung des Traffics zum Voice-Mail System
- **Firewall muss stateful Filterung von Voice Traffic unterstützen:**
  - RTP benutzt UDP mit einem großem Portnummernbereich, der bei einer stateless Firewall freigegeben werden muss
- **Application Level Gateway (ALG)**
  - Parser für H.323, SIP, MGCP, SDP etc.

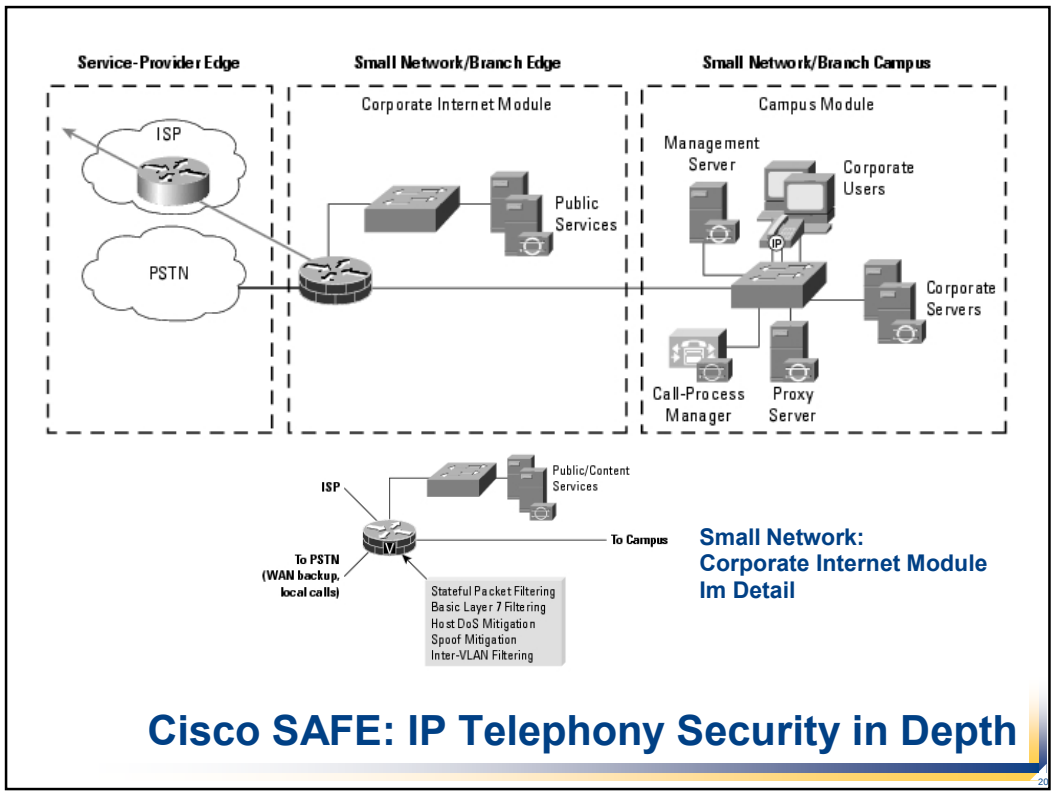
Best-Practices: Firewall

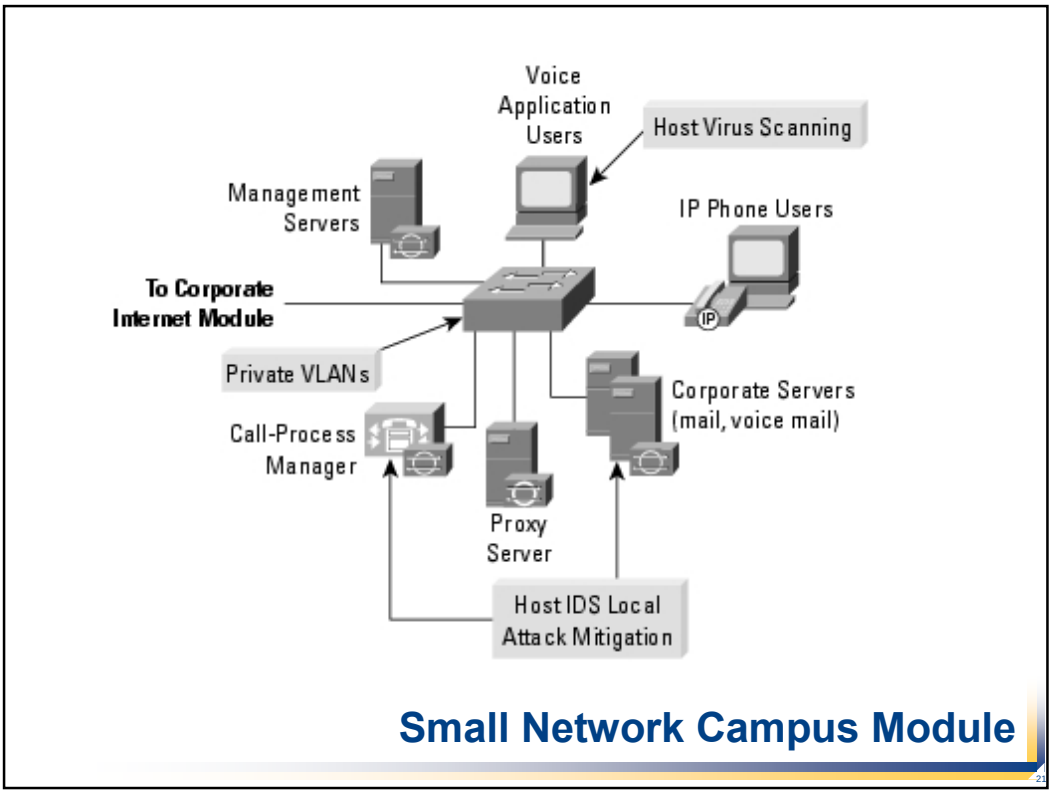


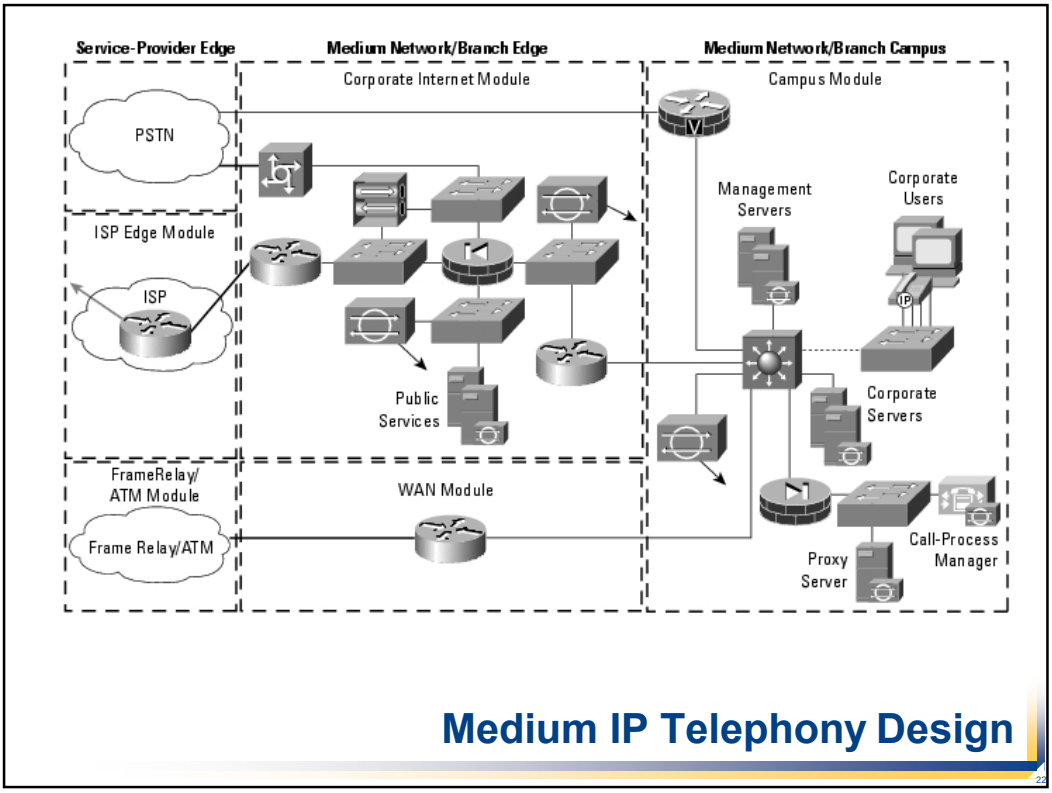
Designrichtlinien für sichere IP-Telefonie Systeme

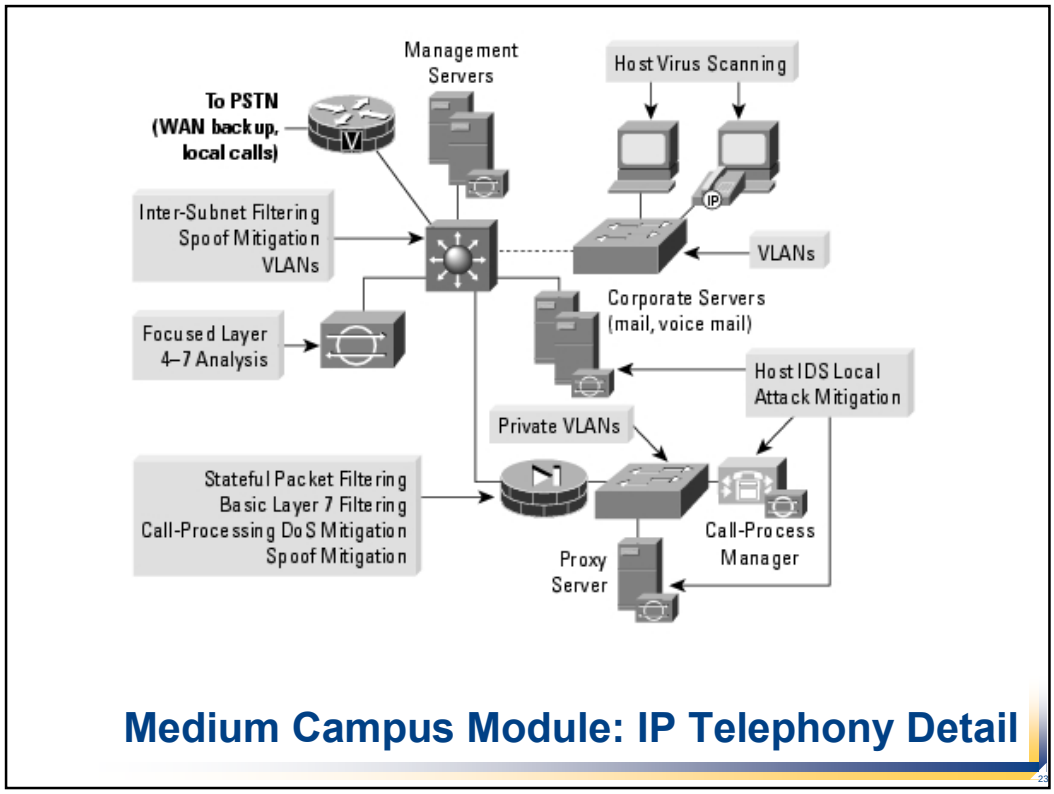
- **Home-Office (Heimarbeitsplatz/Privat)**
- **Small-Business (Kleine + mittlere Unternehmen)**
- **Large Enterprise (Große Unternehmen)**

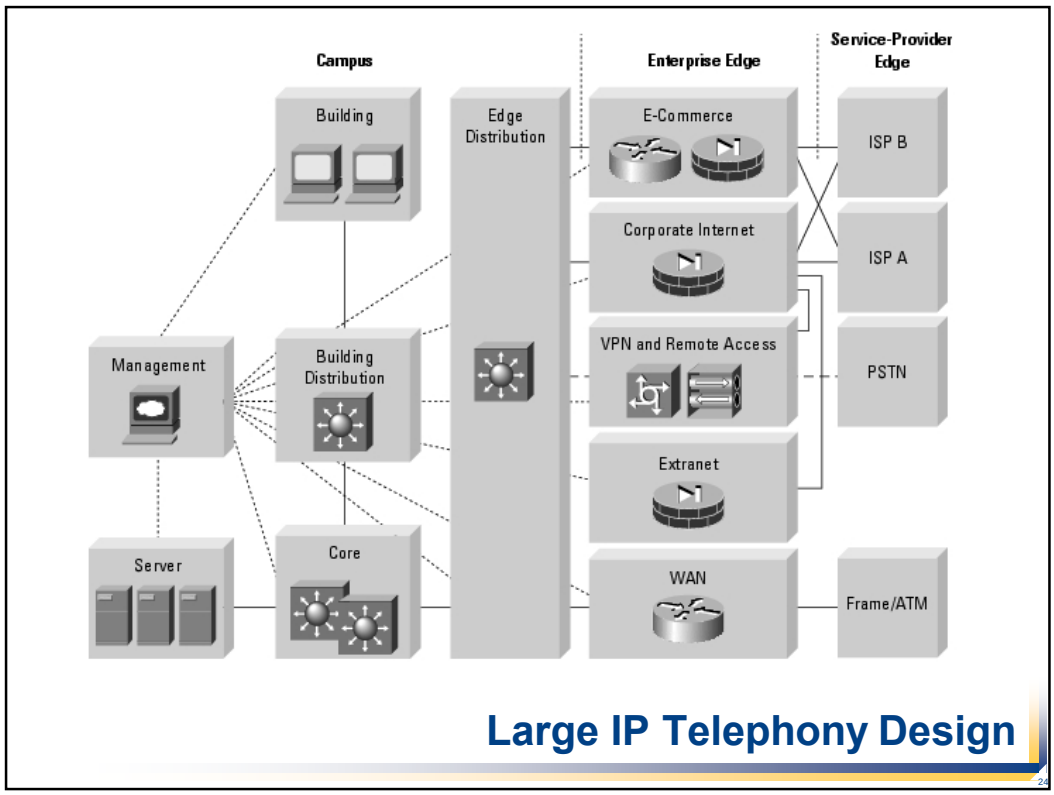

Eumex 300 IP
VoIP Software
(z.B. Asterisk)
analoges Telefon
T-Net
T-ISDN
FRITZ!Box Fon WLAN
ISDN Telefon
Internet
ADSL
Wireless Telefon
Home-Office

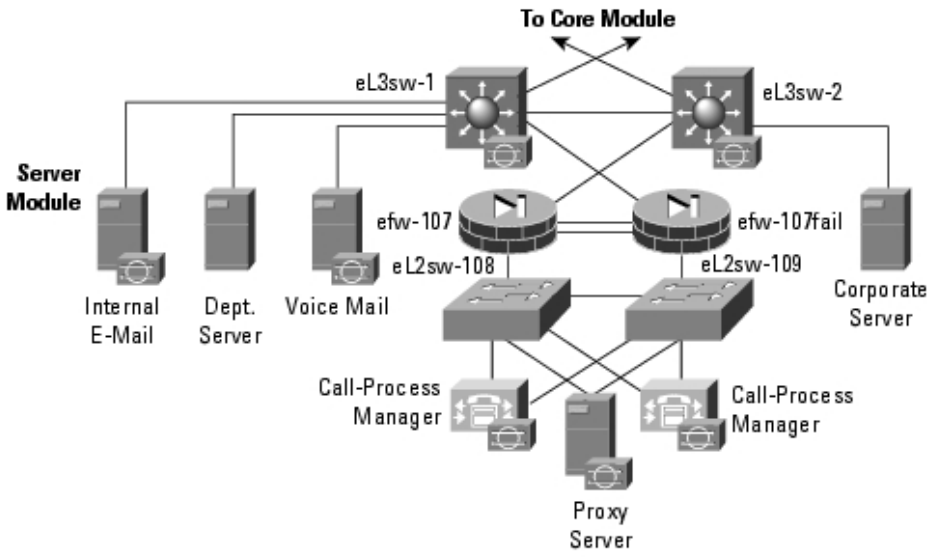

Service-Provider Edge
Small Network/Branch Edge
Small Network/Branch Campus
Corporate Internet Module
Campus Module
ISP
PSTN
Public
Services
Management
Server
Corporate
Users
Corporate
Servers
Call-Process
Manager
Proxy
Server
Public/Content
Services
To Campus
To PSTN
(WAN backup,
local calls)
Stateful Packet Filtering
Basic Layer 7 Filtering
Host DoS Mitigation
Spoof Mitigation
Inter-VLAN Filtering
Small Network:
Corporate Internet Module
Im Detail
Cisco SAFE: IP Telephony Security in Depth


Voice
Application
Users
Host Virus Scanning
Management
Servers
IP Phone Users
To Corporate
Internet Module
Private VLANs
Corporate Servers
(mail, voice mail)
Call-Process
Manager
Proxy
Server
Host IDS Local
Attack Mitigation
Small Network Campus Module


Service-Provider Edge
Medium Network/Branch Edge
Medium Network/Branch Campus
Corporate Internet Module
Campus Module
PSTN
ISP Edge Module
ISP
Management
Servers
Corporate
Users
Public
Services
Corporate
Servers
FrameRelay/
ATM Module
WAN Module
Frame Relay/ATM
Call-Process
Manager
Proxy
Server
Medium IP Telephony Design


Management Servers
Host Virus Scanning
To PSTN (WAN backup, local calls)
Inter-Subnet Filtering Spoof Mitigation VLANs
VLANs
Corporate Servers (mail, voice mail)
Focused Layer 4–7 Analysis
Host IDS Local Attack Mitigation
Private VLANs
Stateful Packet Filtering Basic Layer 7 Filtering Call-Processing DoS Mitigation Spoof Mitigation
Call-Process Manager
Proxy Server
Medium Campus Module: IP Telephony Detail


Campus
Enterprise Edge
Service-Provider Edge
Building
Edge Distribution
E-Commerce
ISP B
Corporate Internet
ISP A
Management
Building Distribution
VPN and Remote Access
PSTN
Extranet
Server
Core
WAN
Frame/ATM
Large IP Telephony Design



Enterprise Server Module

- Bundesamt für Sicherheit in der Informations-technik (BSI): VoIPSEC - Studie zur Sicherheit von Voice over Internet Protocol http://www.bsi.de/literat/studien/VoIP/index.htm
- Cisco SAFE: IP Telephony Security in Depth: http://www.cisco.com/go/safe
- Breaking through IP telephony: http://www.nwfusion.com/reviews/2004/0524voipsecurity.html
- VoIP Security Alliance http://www.voipsa.org/

Referenzen/Links


TWIST-IT ®
Christoph Bronold
Christoph.Bronold@bkm-gmbh.com
BKM Dienstleistungs GmbH
Hauptstrasse 5
D-83607 Holzkirchen
www.bkm-gmbh.com