12. téma

Bezpečnost IP telefonie

Obsah

1. Taxonomie slabin a útoků
2. Řešení Cisco
3. Útoku na IP telefonii v LAN

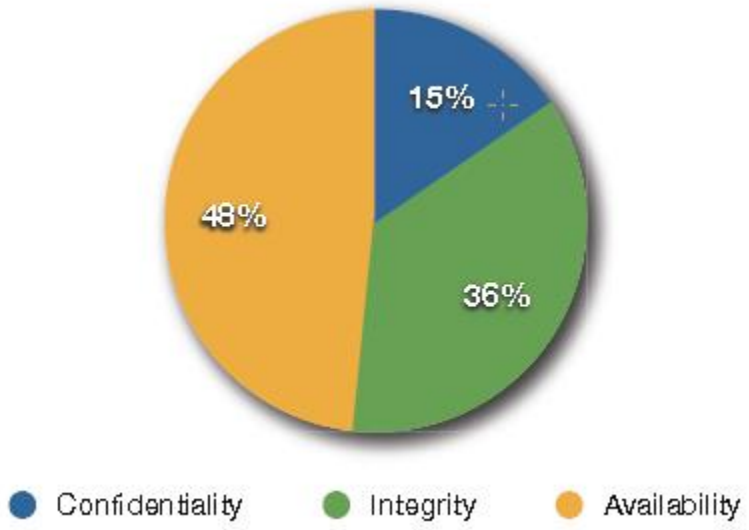
1. Taxonomie slabin a útoků

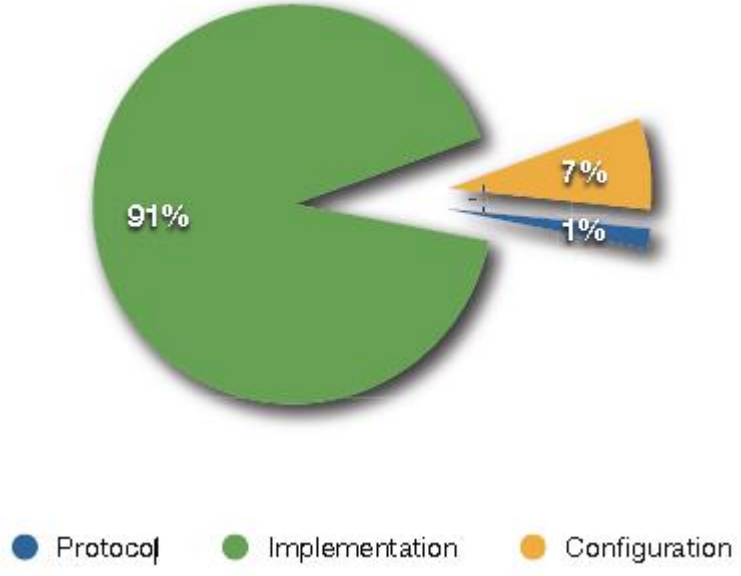
Jak to vlastně je

- Voice/VoIP systémy jsou zranitelné:
  - platformy, sítě, protokoly, aplikace – vše je zranitelné
  - k dispozici je množství nástrojů
  - výrobci posilují bezpečnost svých produktů
  - ale během jejich vývoje bezpečnost není hlavní kritérium
- Naštěstí to není tak strašné, protože
  - IP telefonie je převážně používána uvnitř kampusů
  - omezené stimuly pro útoky
  - Přístup do veřejných sítí je stále založen na tradičních truncích
  - Hlavní zdroj útoků jsou aplikace
- SIP trunking a UC mohou hrozby navyšovat (TDoS, harrasment, vishing…)

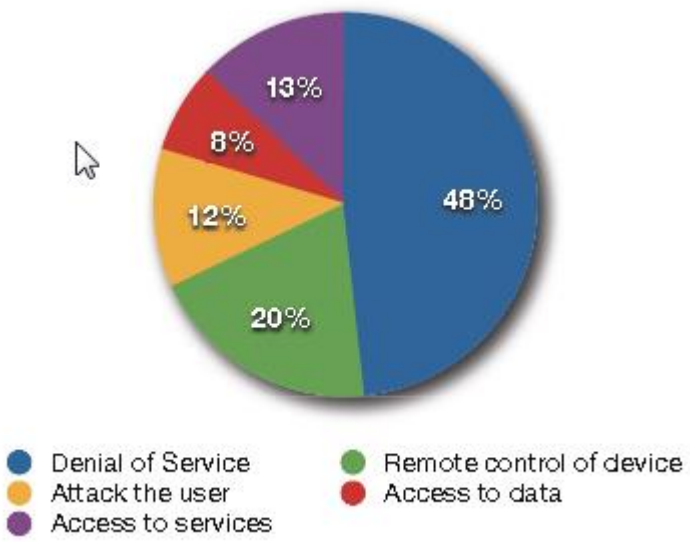
Kategorie útoků

(https://gforge.inria.fr/docman/view.php/1766/6771/d1.1-full.pdf)

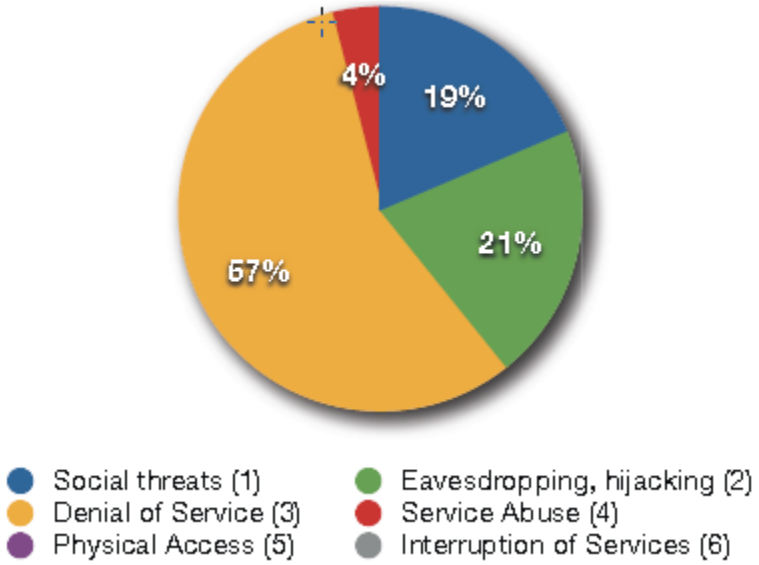




Slabiny měřené podle odlišných metodik



Taxonomie zdroje z předchozího slajdu



Taxonomie VoIPSA

Jaké porty můžeme skenovat?

- SIP používá UDP/TCP ports 5060 and 5061
- H.323 devices use multiple ports, including TCP 1720, UDP 1719
  - H.245 – dynamická TCP
  - H.225.0 – Q.931 – Call Setup – TCP 1720 a RAS – UDP 1719
  - Audio Call Control – TCP 1731
  - RTCP – a RTP dynamické UDP
- SCCP telefony (Cisco) používají porty UDP/TCP 2000-2001
- Unistim (Nortel) používají UDP/TCP 5000
- MGCP zařízení používají UDP 2427

Flooding (záplava, zahlcení)

- Slabá místa
  - redukovaný hardware
  - neautentizované a neautorizované funkce
- Útok
  - záplava pakety (SIP INVITE, OPTIONS…)
  - falešné pakety RTP
  - záplava běžných paketů (TCP SYN, ICMP…)
- Účinek
  - degradace QoS
  - výpadek zařízení
- Nástroje
  - Scapy, InviteFlood, IAXFlood, UDPFlood, RTPFlood, Sivus
- Opatření
  - ochrana zařízení jádra sítě před externími útoky
  - omezení provozu VoIP ve vybraných místech sítě

Flood Amplification (zesílení záplavy)

- Slabá místa
  - protokoly poskytující funkčnost bez autentizace
  - protokoly bez navazování spojení (UDP)
- Útok
  - použití zdrojové adresy paketu oběti
  - v rámci dané funkčnosti poskytování více dat než je třeba
- Účinek
  - zesilování záplav
- Nástroje
  - Scapy, NetSamhain, Nemesis
- Opatření
  - použití spojově orientovaných přenosů
  - autentizace zpráv
  - omezení provozu VoIP ve vybraných místech sítě

Fuzzing
(z Fuzz – US , polda, chlupatý)

- Slabá místa
  - nezralé či slabé implementace protokolového zásobníku
- Útok
  - posílání znetvořených zpráv na vstup zařízení
- Účinek
  - výpadek koncových zařízení, někdy i jádra sítě
  - efektivní metoda pro identifikaci softwarových chyb
- Nástroje
  - Sulley Fuzzer, ohrwurm (RTP)
  - PROTOS Suite (SIP, HTTP, SNMP)
  - NastySIP, Protos suite, Asteroid, Fuzzy Packet…
- Opatření
  - používat odolná a otestovaná zařízení

Termín byl poprve použit v roce1988 prof. Millerem z University of Wisconsin

Call Teardown
(násilné přerušení spojení)

- Slabá místa
  - většina realizací protokolů používá nešifrované přenosy
  - pakety jsou nešifrované
  - lze monitorovat signalizační kanály
- Útok
  - vkládání zpráv pro rozpojení: BYE (SIP), HANGUP (IAX)
- Účinek
  - rozpojení
- Nástroje
  - SIP: Teardown, sip-kill, sip-proxykill
  - IAX: IAXHangup
- Opatření
  - šifrování přenosů hlasu
  - autentizace signalizace

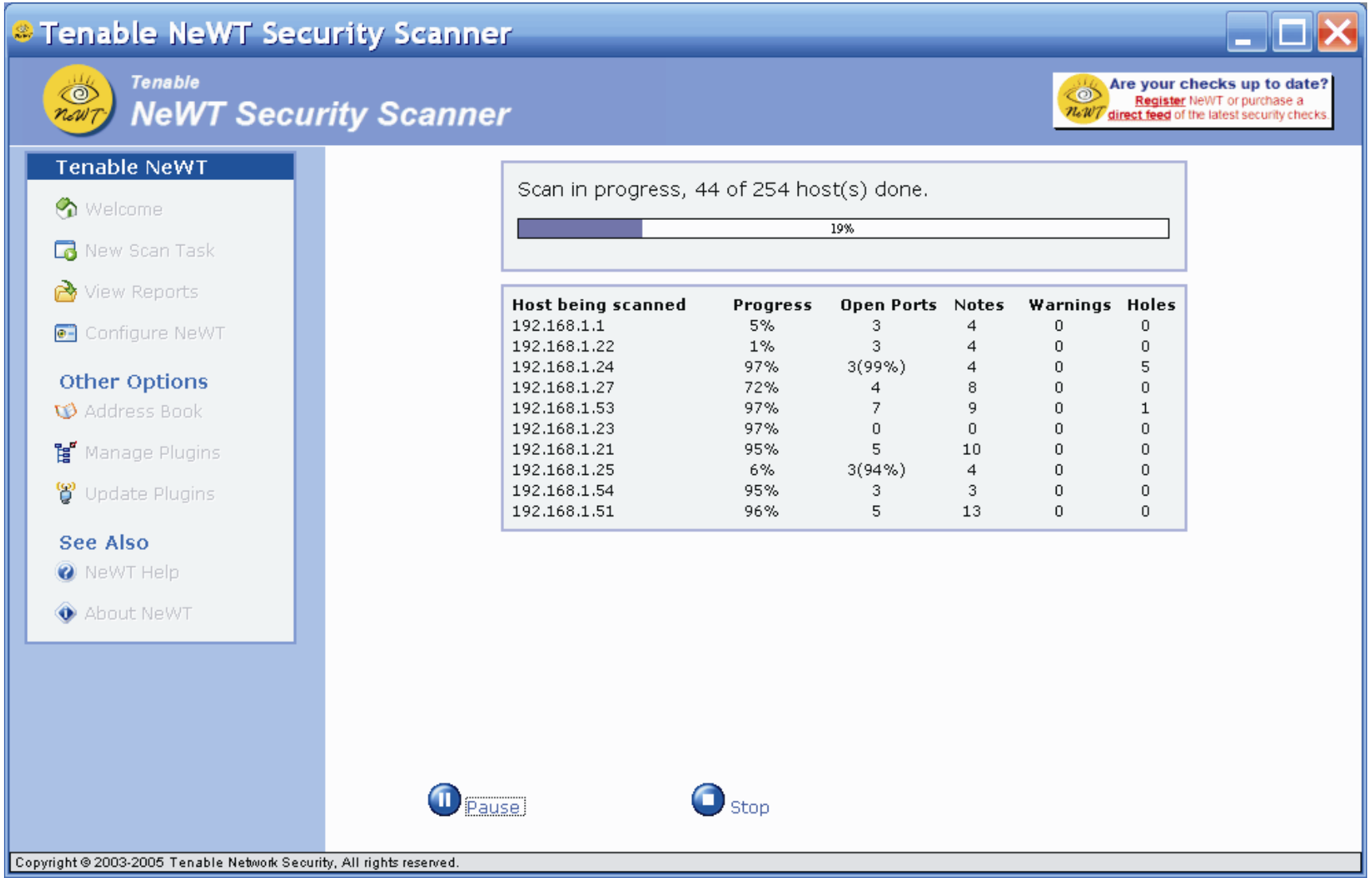
Pomocí SCAPY hledám základ pro BYE

```
>>> sip[7].show() ###[ Ethernet ]###
dst= 00:0e:08:dd:la:bd src= 00:01:02:la:8d:ab type= 0x800 ###[ IP ]###
version= 4L ihl= 5L tos= 0x0 len= 764 id= 0 flags= DF frag= OL ttl= 54 proto= udp
chksum= 0x880e src= 86.64.162.35 dst= 192.168.0.215 options= '' ###[ UDP ]###
sport= 5060 dport= 5060 len= 744 chksum= Oxbcdc ###[ Raw ]###
load= 'SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP 192.168 . 0 . 215 : 5060;b
ranch=z9hG4bK-82 6b4f7;rport=50 60\r\nRecord-Route: <sip:8 160.216.1.3;ftag=
e3bfc272 9667 92 8fo0;lr=on>\r\nFrom: "unob" <sip: jarda@unob.cz>;tag=e3 bfc272
9667 92 8fo0\r\nTo: <sip:50 0@unob.cz>;tag=as48e6f2f4\r\nCall-ID: 92 3cae6e-
7b8136c3@192.168.0.215\r\nCSeq: 102 INVITE\r\nUser-Agent: UNOB.CZ\r\nAllow:
INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY\r \nContact:
<sip:500086.160.216.3:50 8 0>\r\nContent-Type: application/sdp\r \nContent-
Length: 240\r\n\r\nv=0\r\no=root 9126 9126 IN IP4 86 . 64.162.35\
r\ns=session\r\nc=IN IP4 86.64.162.35\r\nt=0 0\r\nm=audio 19064 RTP/AVP 0
97 101\r\na=rtpmap:0 PCMU/8000\r\na=rtpmap:97 iLBC/8000\r\na=rtpmap:101
telephone-event/8000\r\na=fmtp:101 0-16\r\na=silenceSupp:off - - - -\r\n' >>>
bye=sip[7] >>> raw=bye.getlayer(Raw)
»> raw.load="BYE sip: ferda@unob.cz SIP/2.0" + raw.load[14:] >»
packet=IP(src="86.64.162.35", dst="192.168.0.215") / UDP(sport=5060, dport=5060)
/ raw >>> send(packet)
```

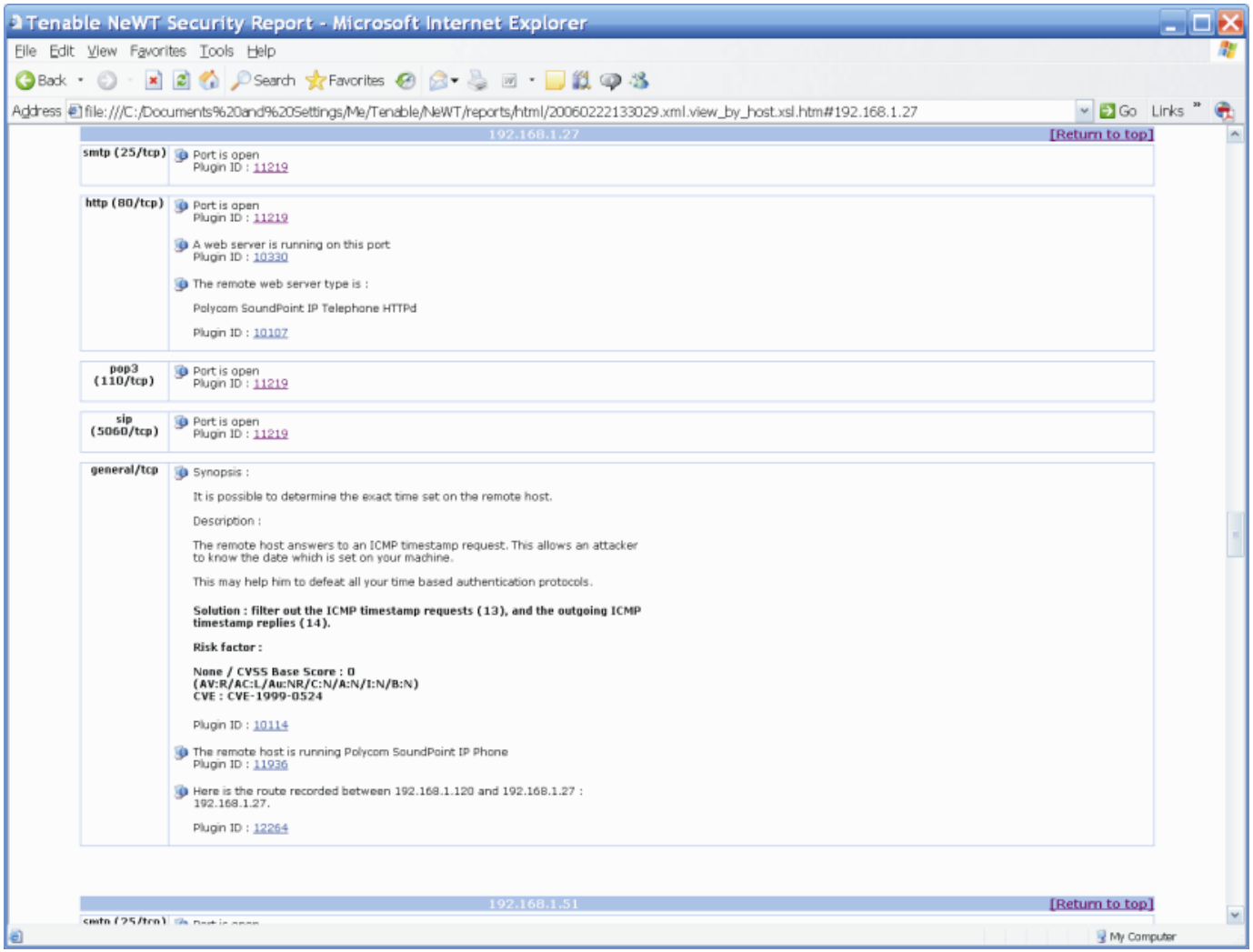
Directory Enumeration (inventarizace adresáře)

- Slabá místa
  - neautorizované funkčnosti
  - protokol odpovídá jinak na platná a neplatná usernames
  - nezašifrované přenosy
- Útok
  - aktivní: speciální zprávy
  - pasivní: odchyt zpráv registračního procesu
- Účinek
  - prozrazení jmen uživatelů
- Nástroje
  - SIPCrack, enumIAX, SIPSCAN, NeWT Security Scanner, Retina Network Security Scanner, SAINT
- Opatření
  - šifrování signalizace
  - protokoly nesmí jinak odpovídat na platná a jinak na neplatná usernames

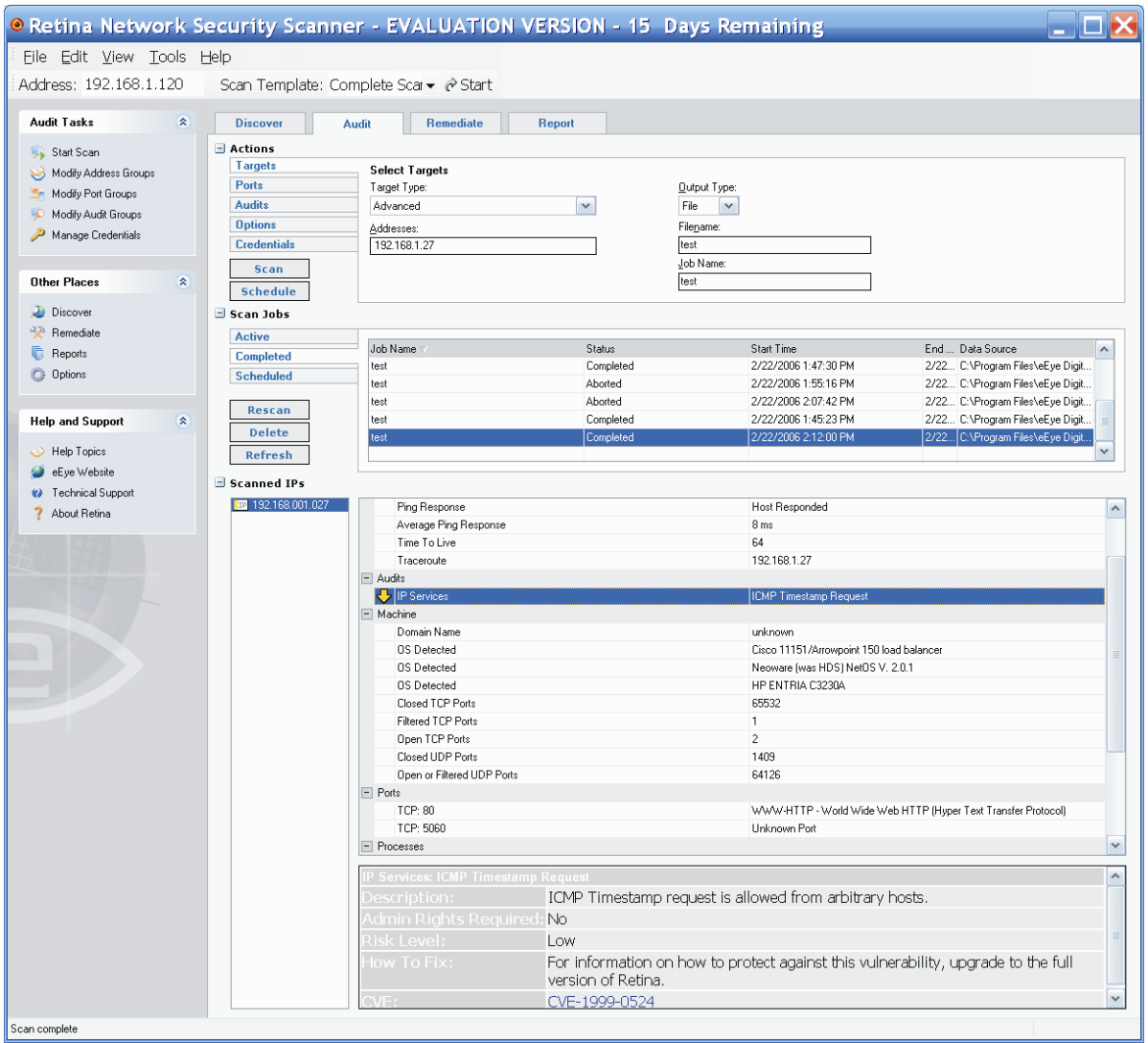
Skenovací nástroje – NeWT Security Scanner



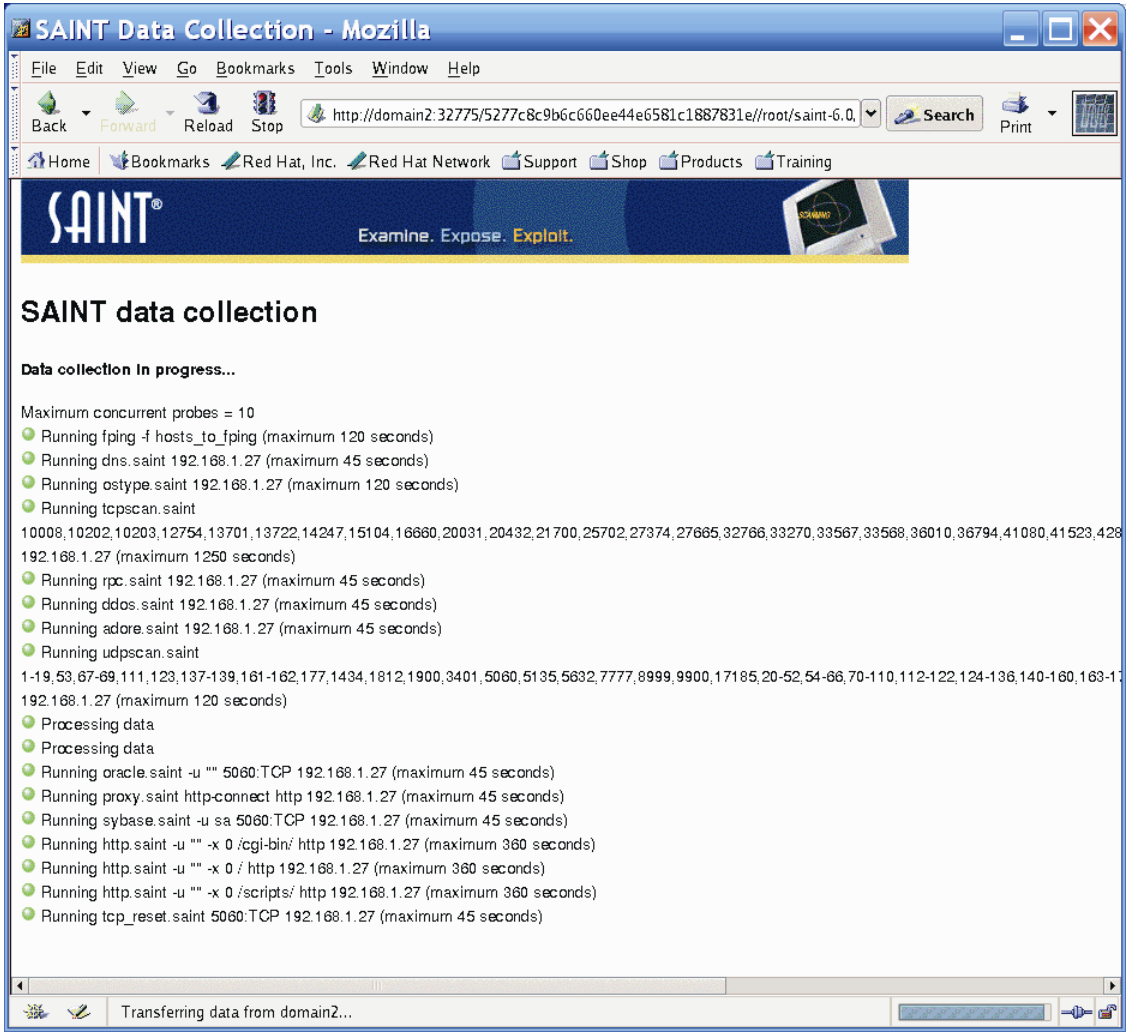
Skenovací nástroje – Tenable NeWT Security Report



Skenovací nástroje – Retina Network Security Scanner

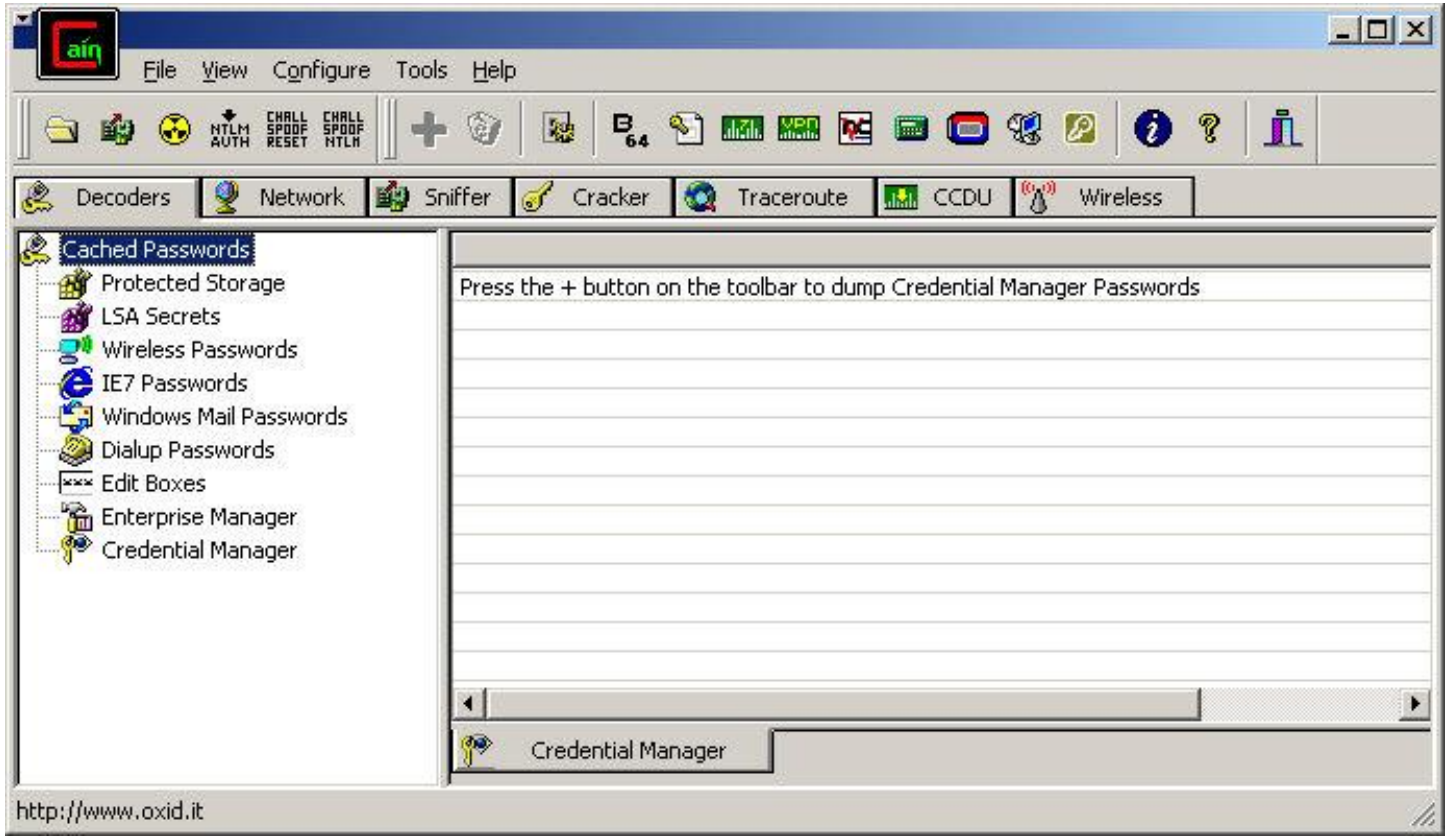


Skenovací nástroje – SAINT



Cain Abel: Sniffer, Password cracker

http://www.oxid.it/ca_um/



G711 uLaw, G771 aLaw, ADPCM, DVI4, LPC, GSM610, Microsoft GSM, L16, G729, Speex, iLB and my understanding is that it is

Caller-ID Name Disclosure (získání jména volajícího)

- Slabá místa
  - přístup k Caller-ID

Útok
  - falešná identifikace volajícího

Účinek
  - prozrazení jména volajícího

- Nástroje
  - www.fakecaller.com, www.iax.cc, www.spoofcard.com
- Opatření
  - kontrola, jaké jméno je s číslem asociováno

Configuration Disclosure: Device (odhaleni zařízení)

- Slabá místa
  - řiditelné rozhraní hardphonů
  - debugging

Útok
  - port 80, SNMP, debugger

Účinek
  - zjištění

- Nástroje
  - tcpkill
- Opatření
  - raději obnovu relace než reboot

Configuration Disclosure: Infrastructure (odhaleni infrastruktury)

- Slabá místa
  - - většina hardphonů používá pro bootování FTP nebo TFTP
  - - FTP není bezpečný a TFTP je na tom ještě hůře

Útok

- - rekonstrukce konfigurace

Účinek

- - odhalení citlivé informace (jméno uživatele, heslo, služby, server, brána, registrační server
- Nástroje
  - - Wireshark, TFTP-Bruteforce, dedukce…
- Opatření
  - - nepoužívat TFTP, FTP je lepší, ale ne zase tak o tolik ☺
  - - nepoužívat defaultní jména souborů

Web Management Interface XSS

- Slabá místa
  - zařízení nechrání web s jeho slabinami
  - lze si zobrazit jeho logy

Útok
- vložený XSS kód

Účinek
- vykonání kódu Cross-Side-Scripting

Nástroje
- jakýkoliv zařízení VoIP s uživatelsky konfigurovatelným zobrazováním polí

- Opatření
  - pokud není potřebné, je třeba webové rozhraní vypnout

A řada dalších…

- odchyt zpráv na médiu
- falešná komunikace (RTPInsetSound, RTPMixSound, RTPInject)
- změna komunikace (SteganRTP atd.)
- ……

IP phone reboot

- Slabá místa

  - SCCP běží na TCP, který je citlivý na reset, telefon pak dělá plný reboot

Útok

- vložení paketu RST do signalizačního kanálu

Účinek

- služba je během rebootu nedostupná
- telefon rebootuje i po záplatě od Cisco

- Nástroje

  - tcpkill

- Opatření

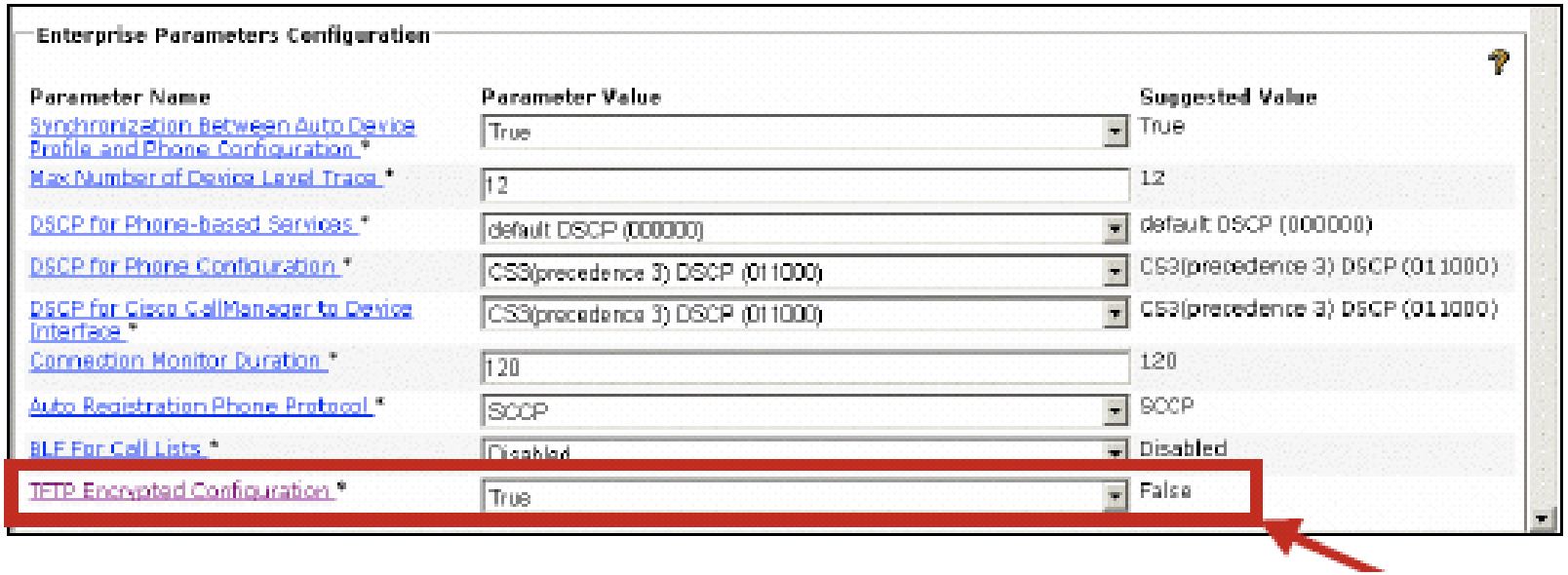
  - raději obnovu relace než reboot

2. Řešení Cisco

Vývoj Cisco Unified CallManagera

- 1998, akvizice mladé společnosti Selsius Systems
- 2000 verze 3.0
- 2001 verze 3.1
- 2004 verze 4.0 a 4.1
- 2006 verze 4.2 (Unified) a 5.0
- 2007 verze 4.3 (Windows) a 5.0 (Linux)
- 2007 verzi 6.0 (Linux)
- 2008 verze 7.0
- 2010 verze 8.0.1

Šifrování hlasu od verze 4.0, od verze 5.0 i konfigurační soubory



šifrovaný konfigurační soubo

Kvalitní algoritmus: AEC-128-CBC

Autentizací proti hrozbám

- modifikace signalizace mezi telefonem a CCM
- útoky typu MITM
- útoky na identitu zařízení a serverů

Kvalitní algoritmus: HMAC-SHA-1

- podpis obrazů firmware od CCM 3.3(3)
- podpis konfiguračních souborů od CCM 4.0

Certifikáty

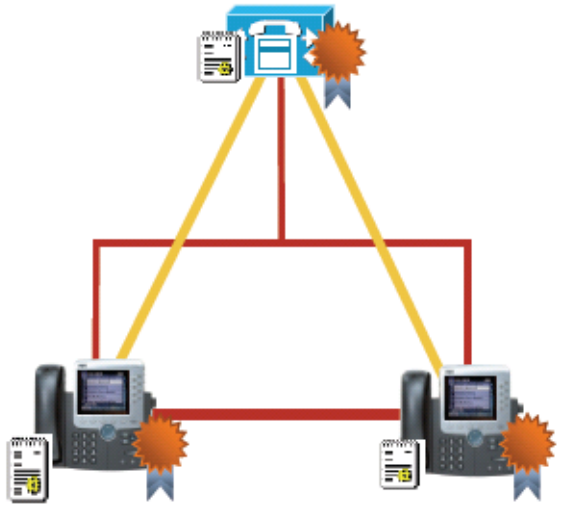
- nesmazatelné tovární certifikáty telefonů
- lokálně významné certifikáty
- certifikáty telefonů jako proxy funkce – vytváří seznamy CTL
- certifikát HTTPS zajišťující autentizaci mezi IIS a prohlížečem klienta
- sebou podepisovaný certifikát CCM; součást identifikace serveru
- certifikát bezpečného řešení náhrady výpadku spojení mezi telefonem a CCM

Kvalitní algoritmus pro podpis: RSA

Použité kryptografické algoritmy

TLS (Transport Layer Security) mezi CCM a IP telefony:

- RSA pro podpisy
- HMAC-SHA-1 pro autentizaci
- AES-128-CBC pro šifrování



SRTP (Secure RTP) mezi IP telefony:

- HMAC-SHA-1 pro autentizaci
- AES-128-CM pro šifrování

Co není zapotřebí – je třeba vypnout

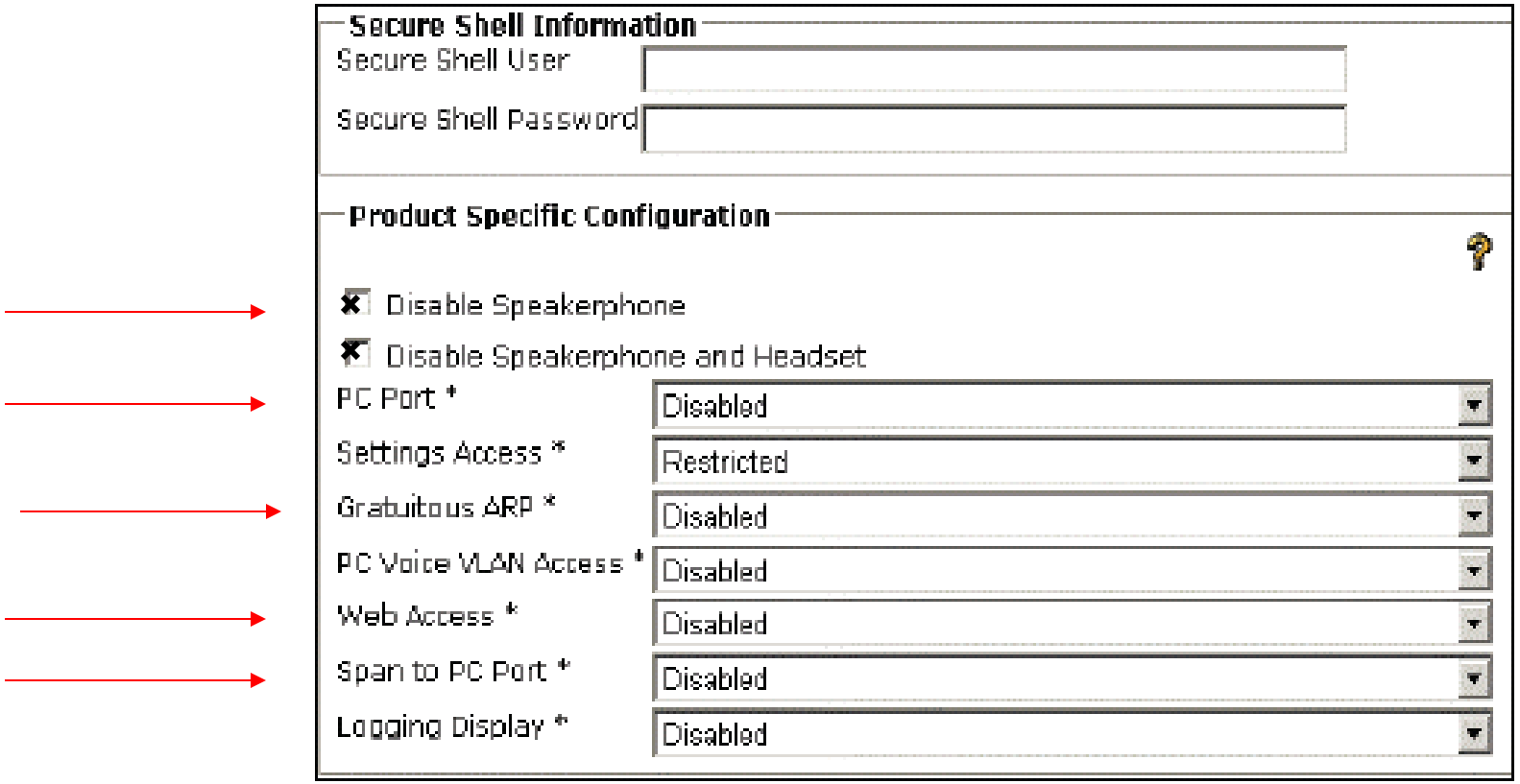
- vypnutí nastavení přístupu
- vypnutí nastavení PC Portu
- vypnutí přístupu k PC Voice VLAN
- vypnutí nastavení gratuitous ARP
- falešné ARP odpovědi, generuje je např. ettercap či dsniff
- vypnutí webového přístupu

Zodolnění sítě pro hlasovou službu

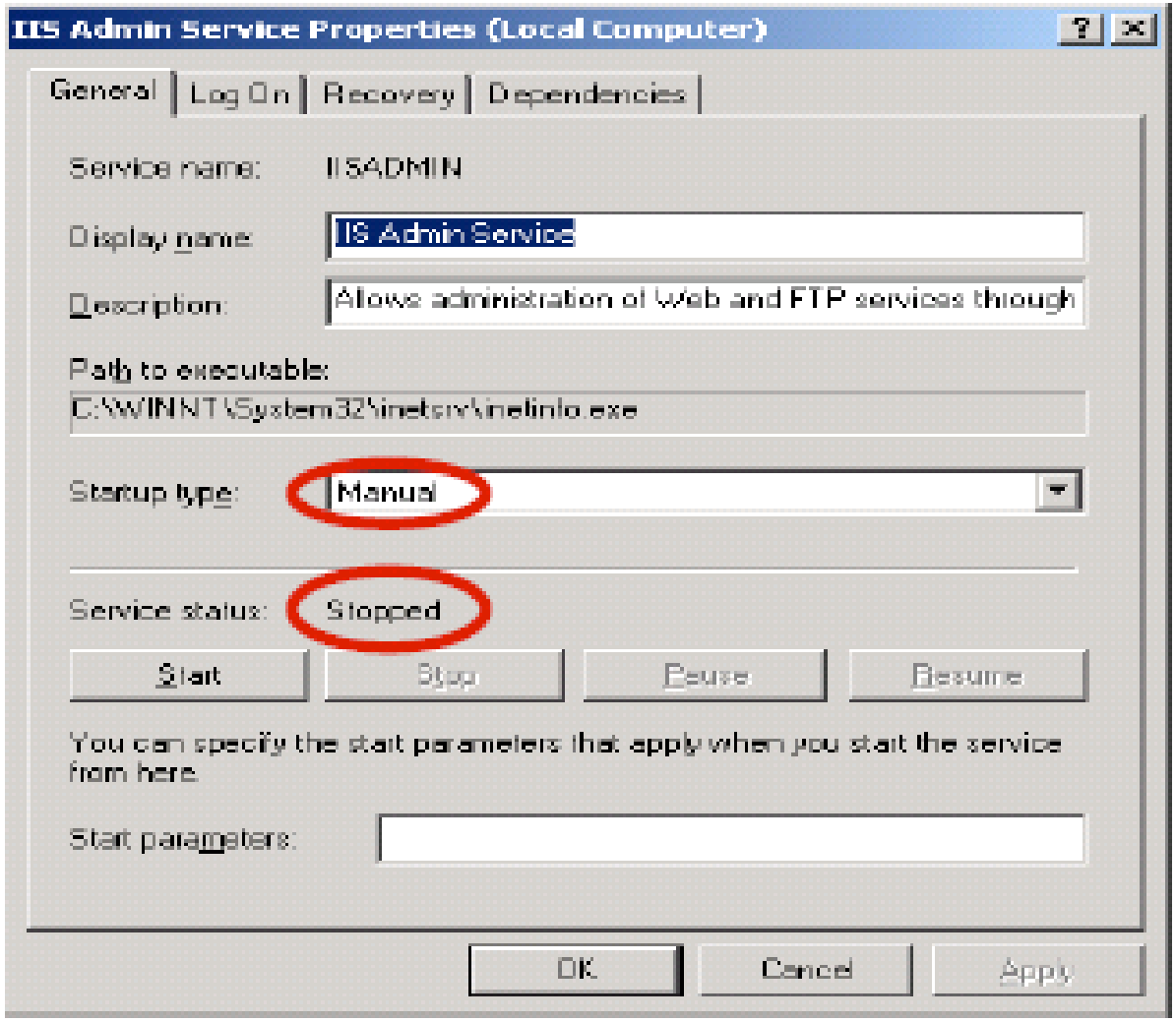
- Oddělení hlasových a datových VLAN a nastavení ACL pro každou VLAN
- Ochrana jednotlivých portů povolením MAC adres před tzv. IP a MAC spoofingem
- Ochrana před P2P provozem a hrami pomocí tzv. scavenger-class provozu (mapuje se do DSCP CS1)
- Ochrana před útokem MITM neautorizovanými DHCP odpověďmi (DHCP Snooping)
- Ochrana před útokem MITM falešnými ARP odpověďmi

Zodolnění IP telefonu

Podepsané konfigurační soubory a firmware, vypnutí všeho zbytného

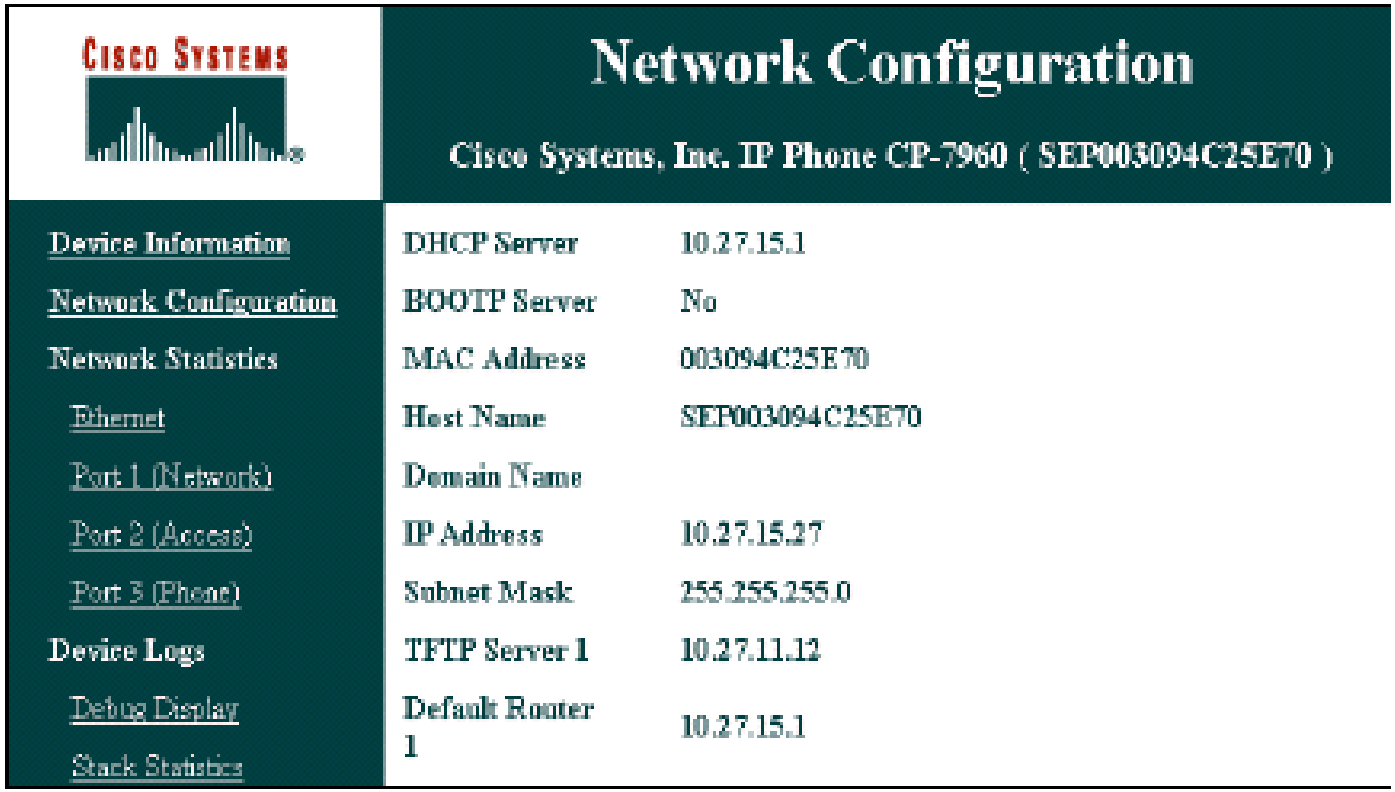


Windows: 80 % útoků vede přes IIS (verze 4.3)



Problém web přístupu k IP telefonu

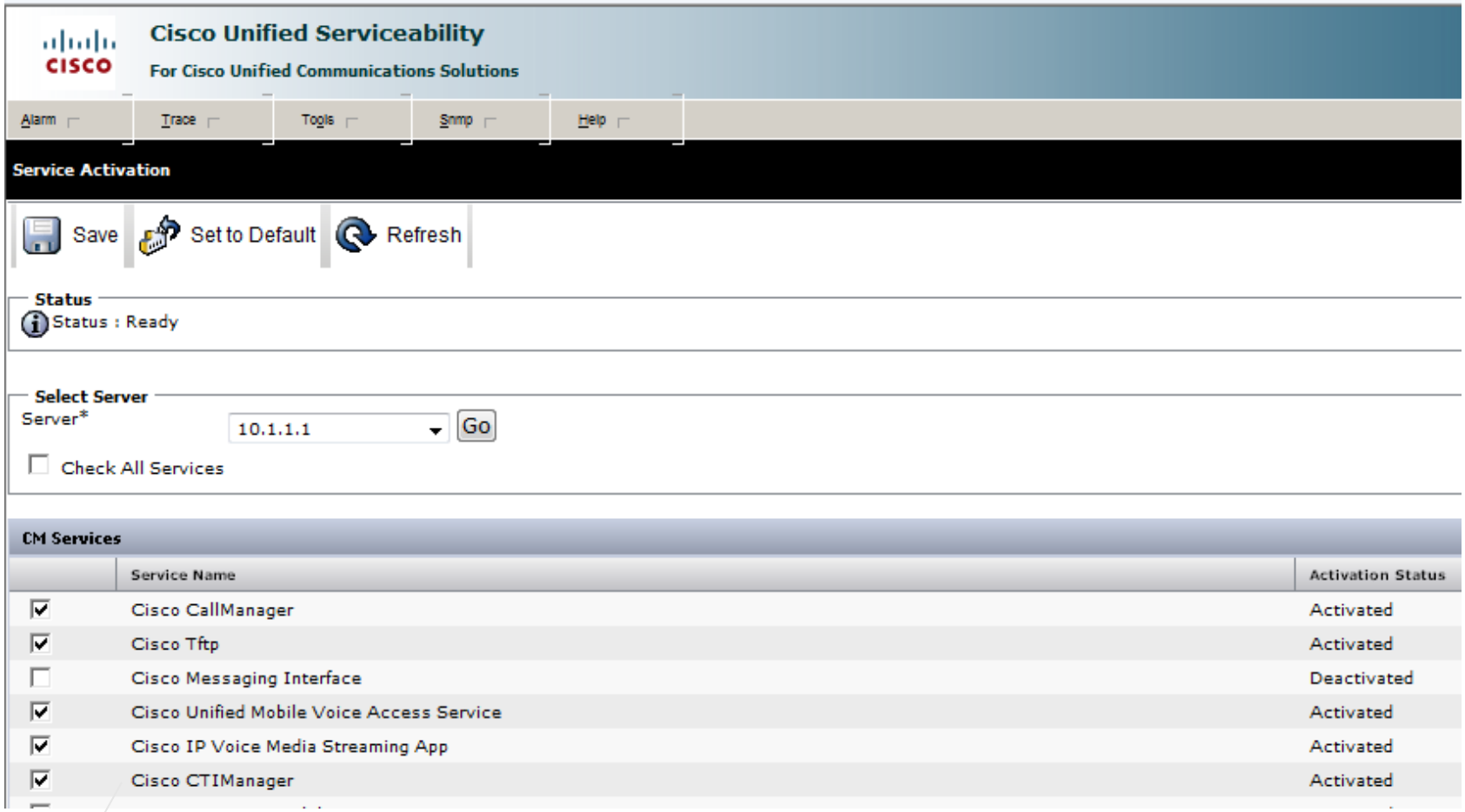
Mnoho cenných informací a vypnout to jen tak nejde (ztráta aplikací na bázi XML)



Řešení:

ACL umožňující komunikaci mezi IP telefonem a serverem pouze přes port 80.

Aktivace potřebných služeb (verze 5.0)



Komunikace s aplikacemi přes CTI, TAPI, JTAPI – šifrovaná a autentizovaná za pomocí certifikátu

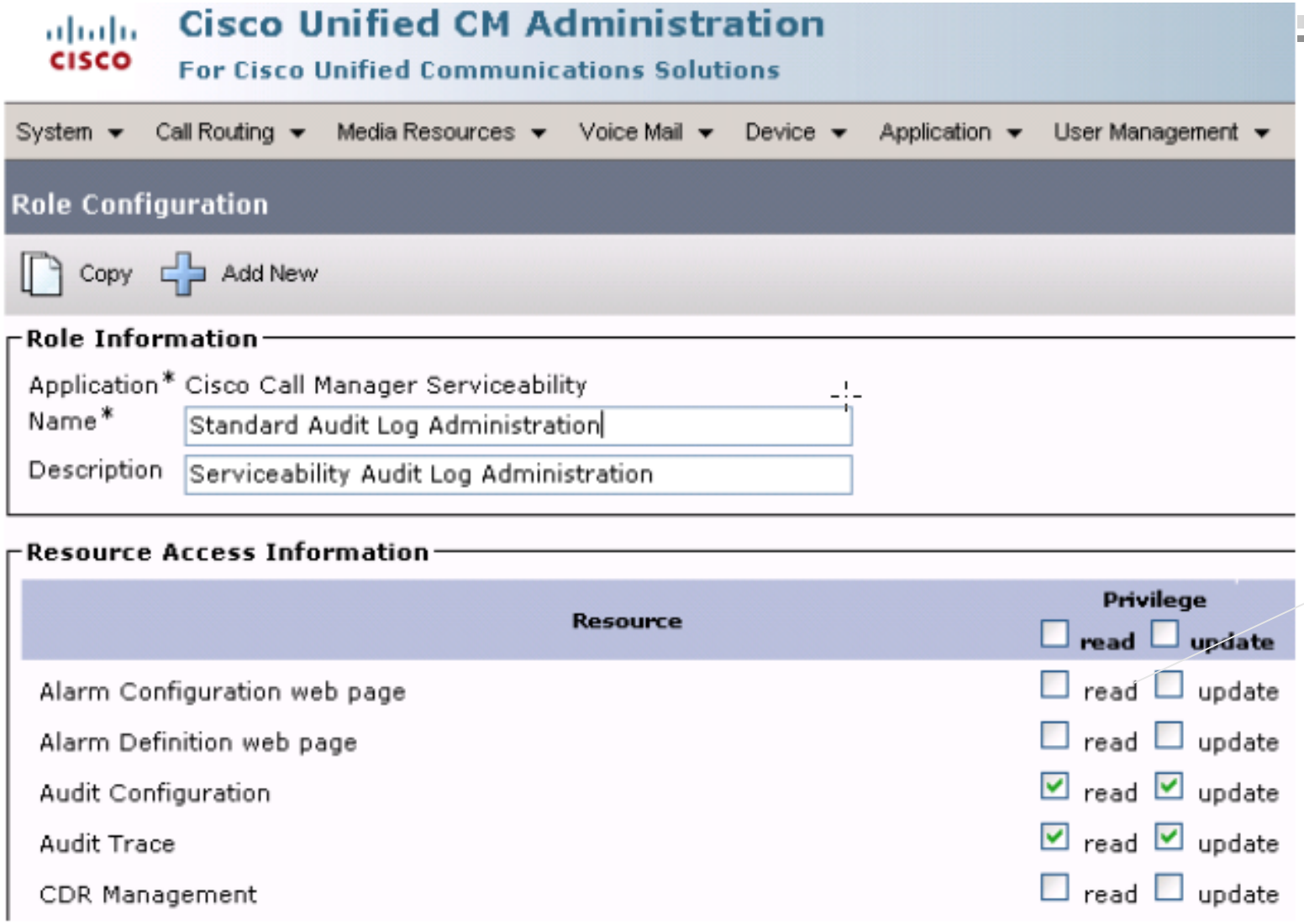
Nové bezpečnostní vlastnosti Call Manageru 5.0 (r. 2006)

- TLS pro autentizaci a šifrování přenosu s SIP telefony
- SRTP pro komunikaci mezi SIP telefony a s bránou MGCP
- IPSec pro tunelování k branám s IOSem
- SSL pro dotazy na adresář LDAP
- HTTPS rozhraní místo HTTP; možnost generovat a rušit certifikáty
- hostující firewall
- Automaticky instalovaný Cisco Security Agent
- rychlé resety hesla (rychlý – bez obtěžování admina, bezpečný – bez přerušení služeb)
- bezpečnostní profily telefonu s protokolem SIP, SCCP či trunkem
- příjem datumu a času od NTP serveru a jejich další výdej
- rozdělení uživatelů do základní a pokročilé skupiny
- různé administrátorské účty zaručující pružnost řízení přístupu
- vypnutí po třiceti minutách pasivity

Klíčové nové či vylepšené bezpečnostní vlastnosti verze 7.1(2)

- auditní logy
- H.235
  (např. MIKEY pro klíčový management SRTP)
- 802.1x EAP-FAST/TLS (RFC 4851)
  místo EAP-MD5 (RFC 3847)
- Trusted Relay Point

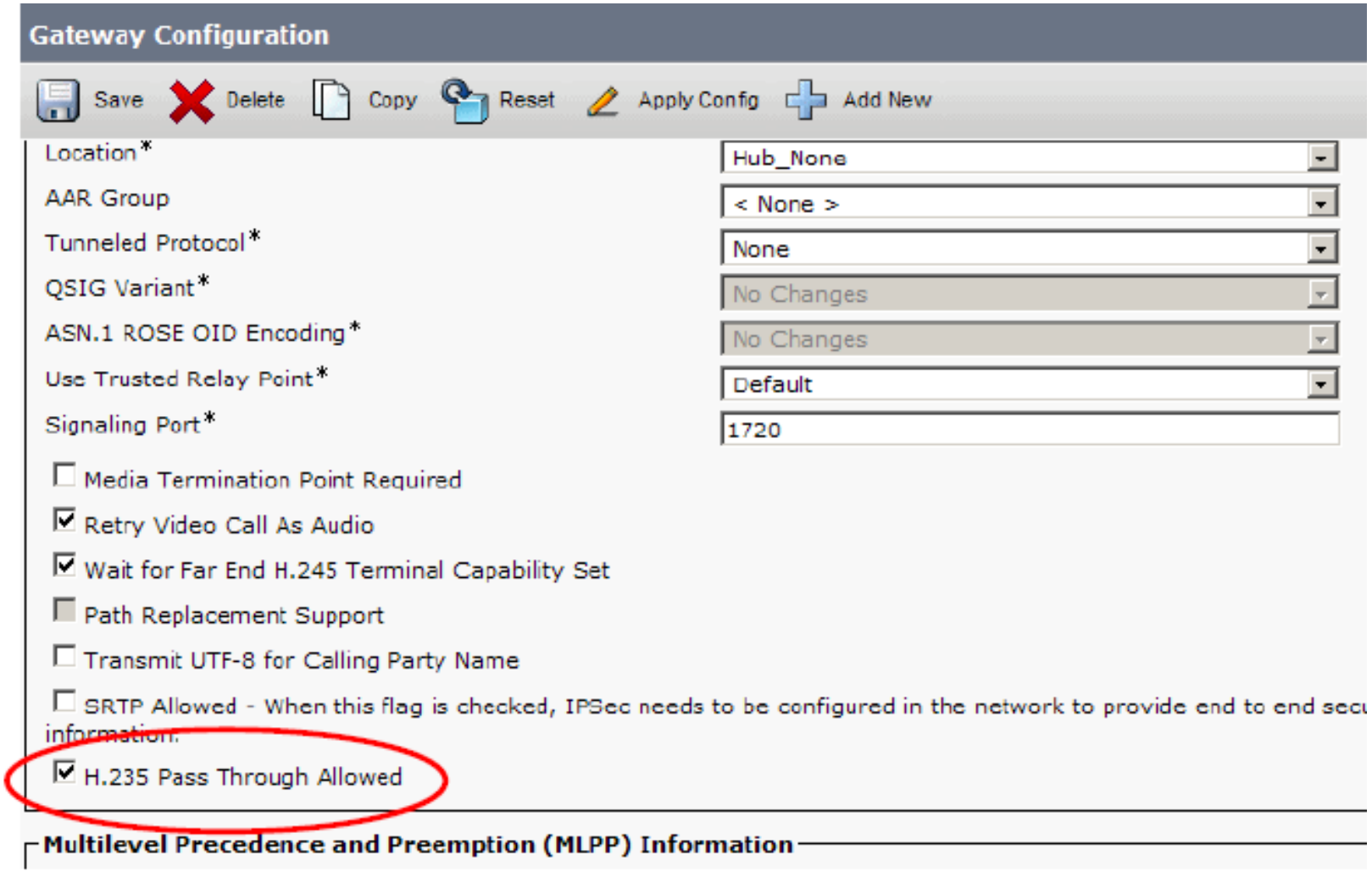
Auditní logy



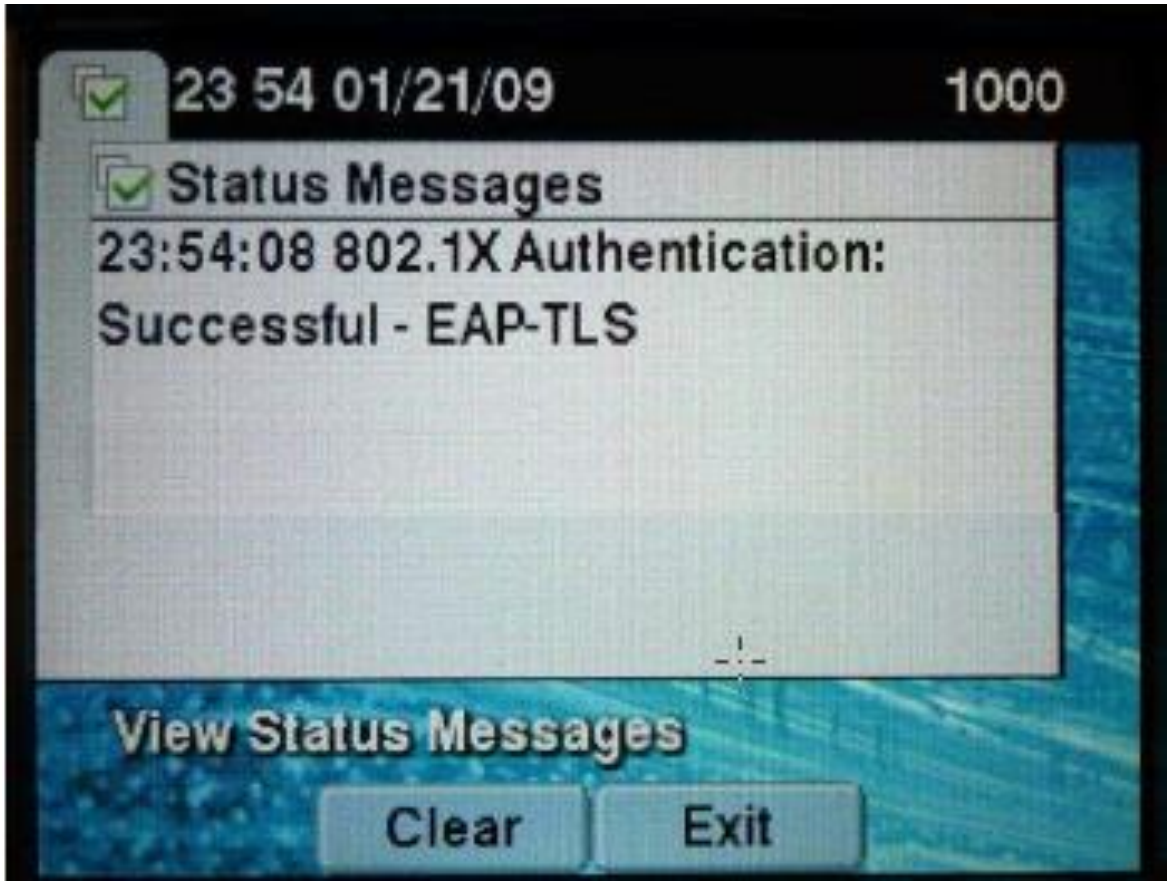
novinka pro externisty

H.235

(CUCM se dá nastavit jako pass-through)

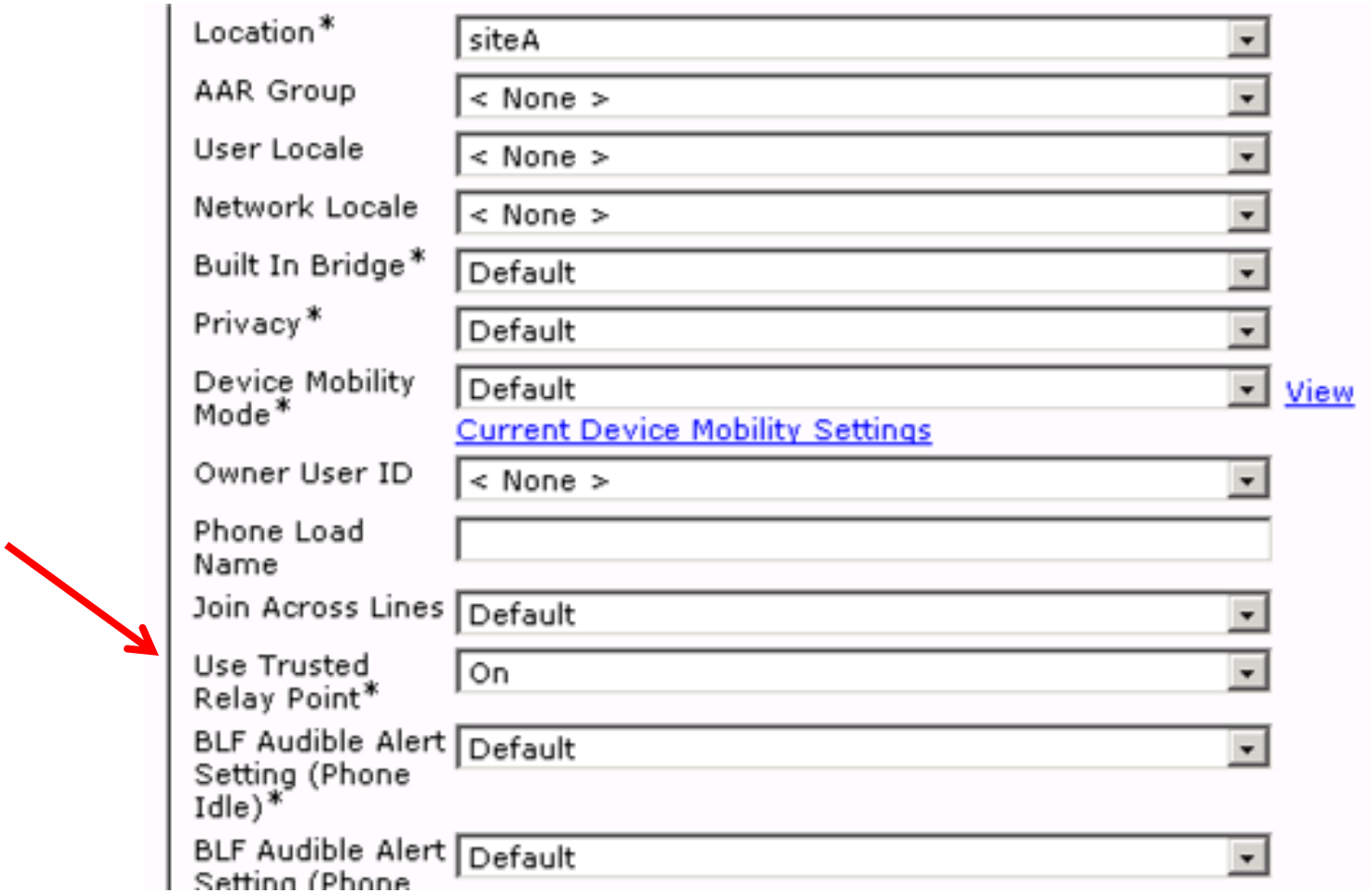


802.1x EAP-FAST/TLS

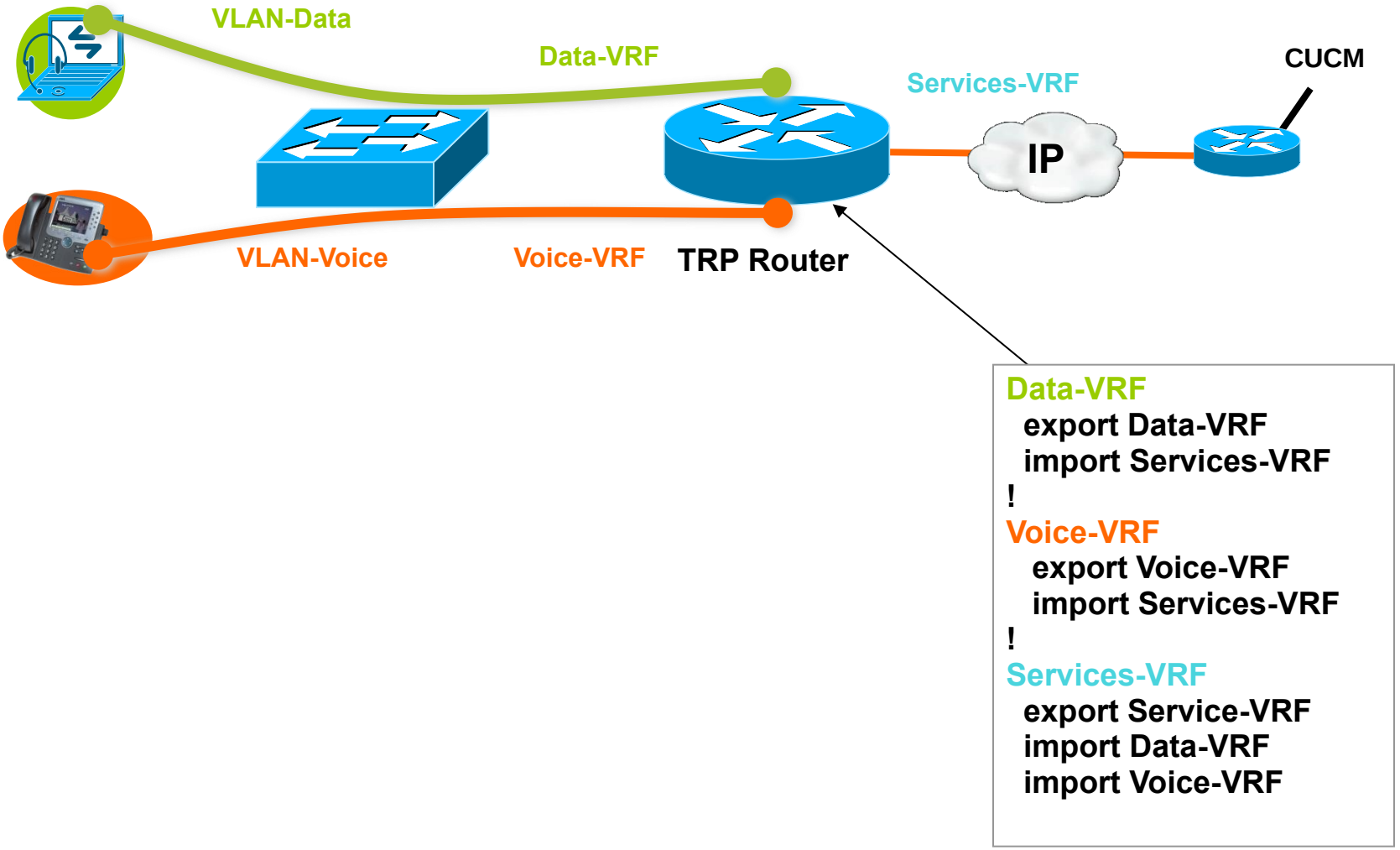


TLS zabezpečuje šifrování, autentizaci a kompresi, autentizace může být i vzájemná, nejen klienta vůči serveru

Trusted Relay Point
(trusted VLAN traversal)



Virtuální směrovače propojují datovou a hlasovou VLAN



Nové či vylepšené bezpečnostní vlastnosti verze 8.0.1

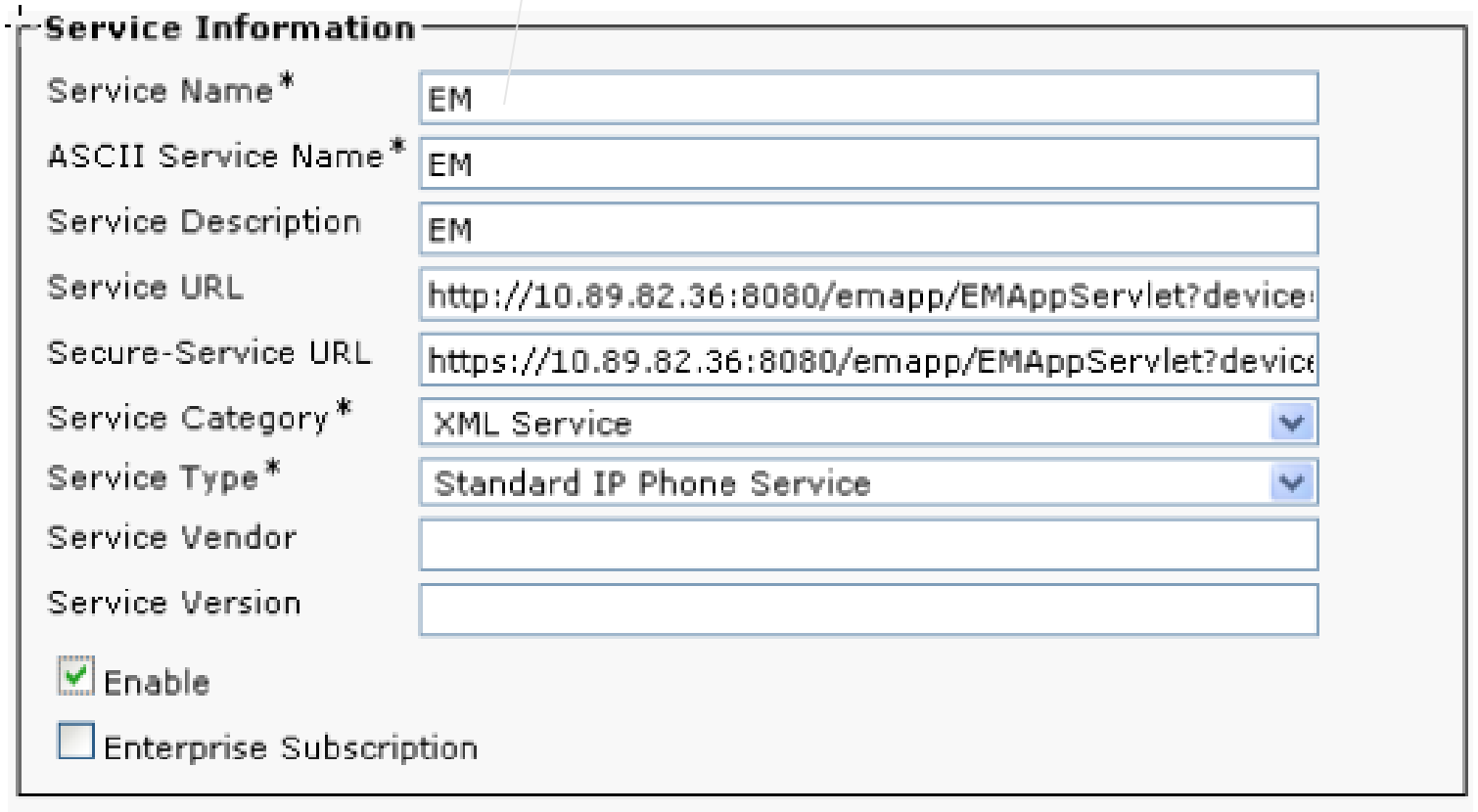
- bezpečnostní monitoring a záznamy
- podpora HTTPS pro telefonní služby
- vylepšení kreditních služeb
- VPN klienti pro IP telefony
- bezpečnost ve výchozím nastavení (Security by Default)

Bezpečnostní monitoring a záznamy

- příposlechy
- problémy se šifrováním, zvláště u více proudů
- použití Trusted Relay Pointu

Podpora HTTPS

Extension Mobility a to nově i mezi klastry



Vylepšení kreditních služeb

VPN klienti pro IP telefony - tři způsoby

- směrovač – směrovač doma

  je ho třeba konfigurovat a spravovat

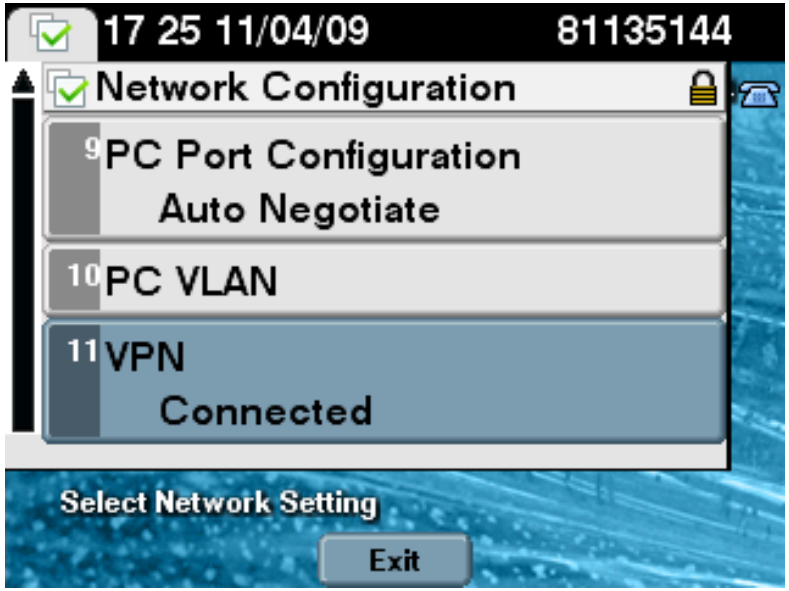
- telefon doma s TLS + SRTP– ASA

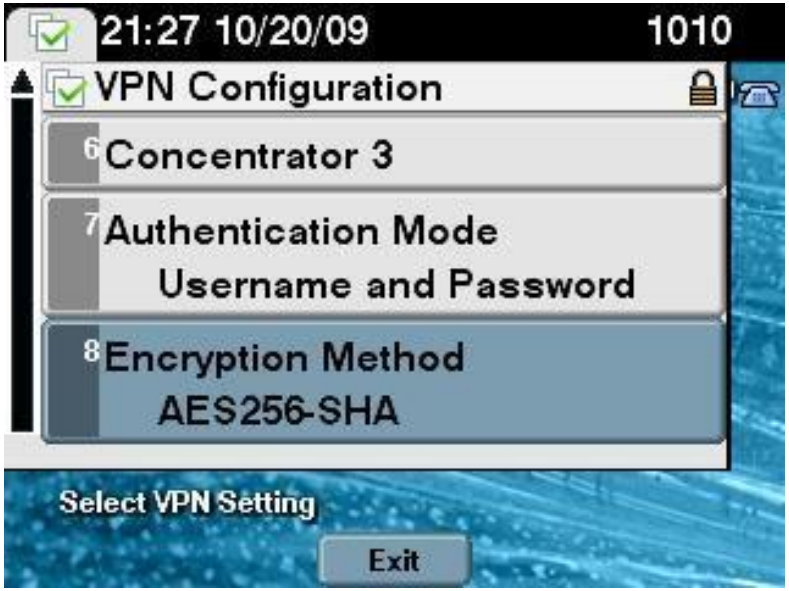
  phone-proxy – mohu jen telefonovat

- SSL VPN (nové)

  mohu volat z domu a užívat si všech služeb bez omezení

Nastavení SSL VPN na telefonu





Nastaveni parametrů SSL VPN na CUCM

VPN Parameters

Parameter Name	Parameter Value	Suggested Value
Enable Auto Network Detect *	False	False
MTU *	1290	1290
Keep Alive *	60	60
Fail to Connect *	30	30
Client Authentication Method *	User And Password	User And Password
Enable Password Persistence *	False	False
Enable Host ID Check *	True	True

Security by Default

Oddělení certifikátů pro podepisování/šifrování a podporu HTTPS, pro interní a externí použití atd.

Otázka

Jaký je základní princip ochrany sítě vybavené IP telefony?

Řešení: komplexní ochrana

	Telefon	Přepínač	Směrovač	Síť	CUCM	Server
Odposlech	X	X	X	X	X	X
Zahlcení	X	X	X	X	X	X
Vložení	X	X	X	X	X	X
Útok na aplikace	X	X	X	X	X	X
Útok na Soft klienta	X	X	X	X	X	X
Krádeže	X	X	X	X	X	X

3. Útoku na IP telefonii v LAN

Příklady útoků na IP telefonii v sítích Cisco

- Přeplnění tabulky CAM u Cisco sítí
- Útok vygenerováním falešných BPDU
- Útok pomocí odchycené MAC adresy
- Neautorizované DHCP a ARP odpovědi

Tabulka CAM

Jak se s tabulkou CAM (Content-Addressable Memory) pracuje ukazuje následující slajd.

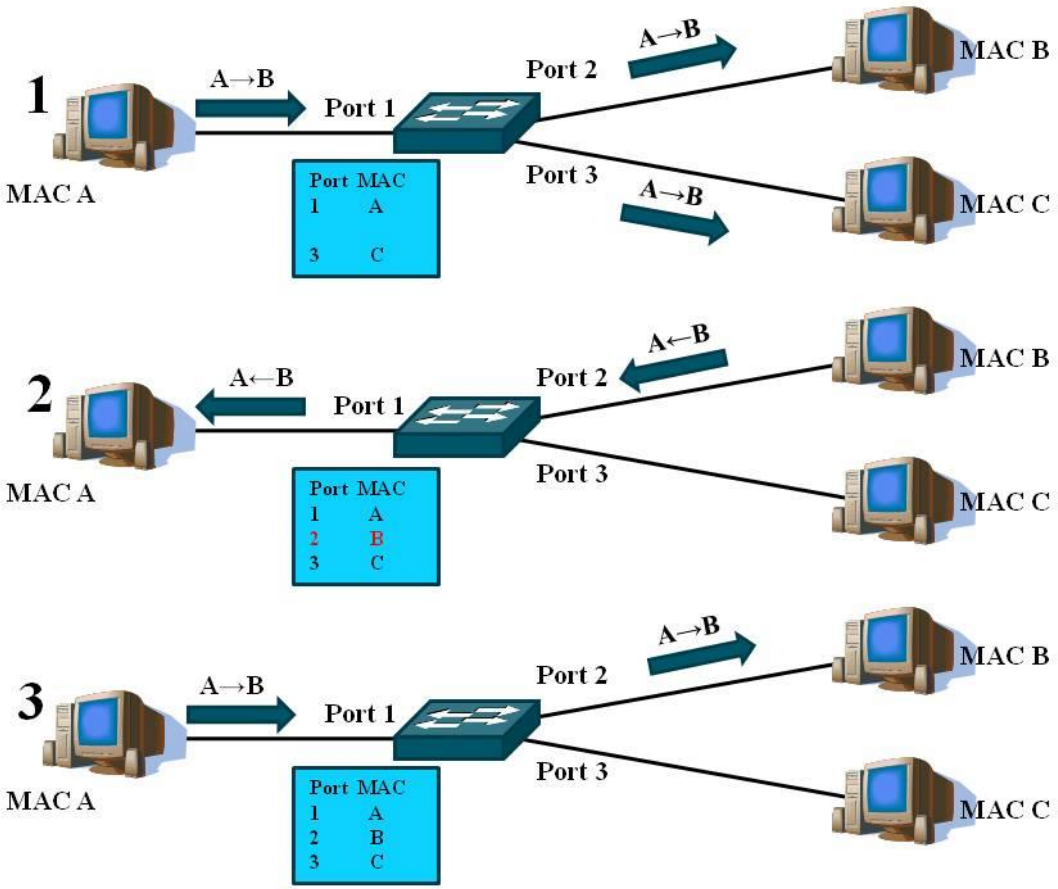
Tabulka CAM registruje MAC adresy přiřazené ke konkrétním portům.
PC s MAC adresou A a C jsou registrovány v tabulce CAM, PC s MAC B ne.

Pokud posílá PC A rámec PC B, je rozeslán všem koncovým stanicím připojeným k přepínači (1).

Pokud ale přijde první rámec z cílové stanice B, je tato zaznamenána do tabulky CAM (2). Od této doby jsou rámce pro stanici B posílány přímo na ni. Pokud ale začne útočník generovat jeden rámec za druhým s vymyšlenými MAC adresami odesilatele, je schopen brzy z tabulky CAM vytlačit relevantní údaje a pak se rámce rozhlašují způsobem 1.

Je zřejmé, **že tabulka CAM je nejslabším místem přístupových sítí**.

Přeplnění tabulky CAM u Cisco sítí



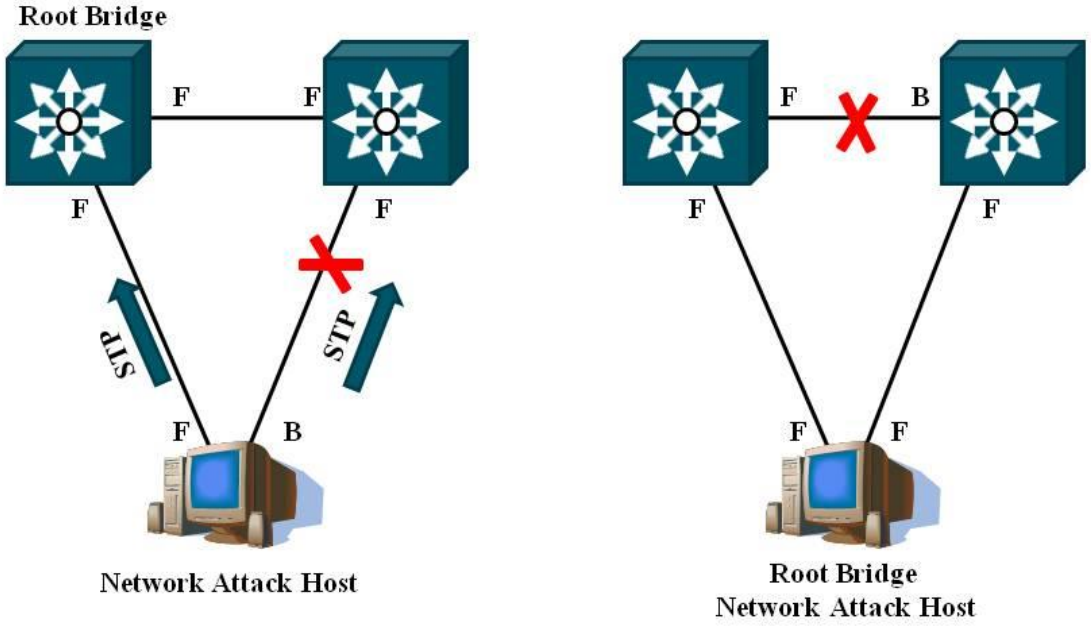
Falešný kořen stromu

Pro volbu falešného kořene stromu (topologicky kostra grafu) stačí vygenerovat rámec BPDU s nejmenší hodnotou priority v síti a tím přinutit ostatní přepínače k tomu, aby zvolily ten, u kterého je připojen útočník, za kořen stromu.

Obrana je jednoduchá – zakázat takové BPDU na jiných portech než k relevantním přepínačům či definovat kořen:

```
S1(config)#spanning-tree vlan 1-1000 root primary
```

Útok vygenerováním falešných BPDU

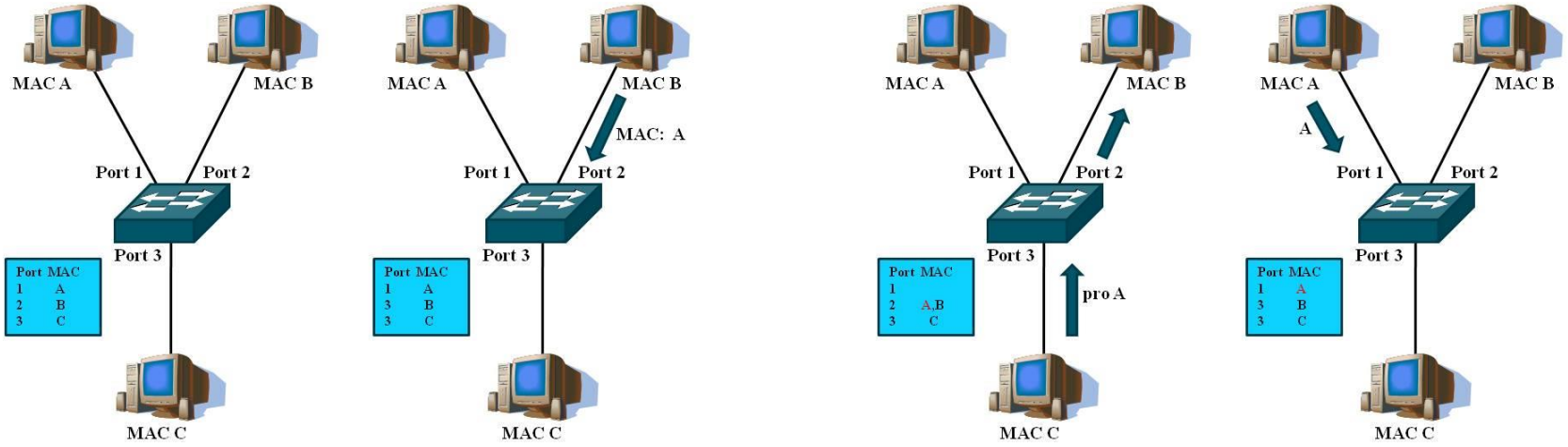


Útok s využitím falešné MAC adresy

(1) Přepínač má přehled o koncových stanicích.
(2) PC s MAC B se ohlašuje s falešnou adresou A jako adresou odesilatele.
(3) Rámce určené pro PC A tečou k PC B.
(4) Rámec odesílaný uzlem A vše napravuje, možná jen dočasně.

Jak se tomuto útoku bránit? Definovat bezpečnost na portu pomocí příkazu je u rozsáhlejších LAN problematické a tak je vhodnější použití složitějšího prostředku a to VLAN.

Útok pomocí odchycené MAC adresy



DHCP snooping binding

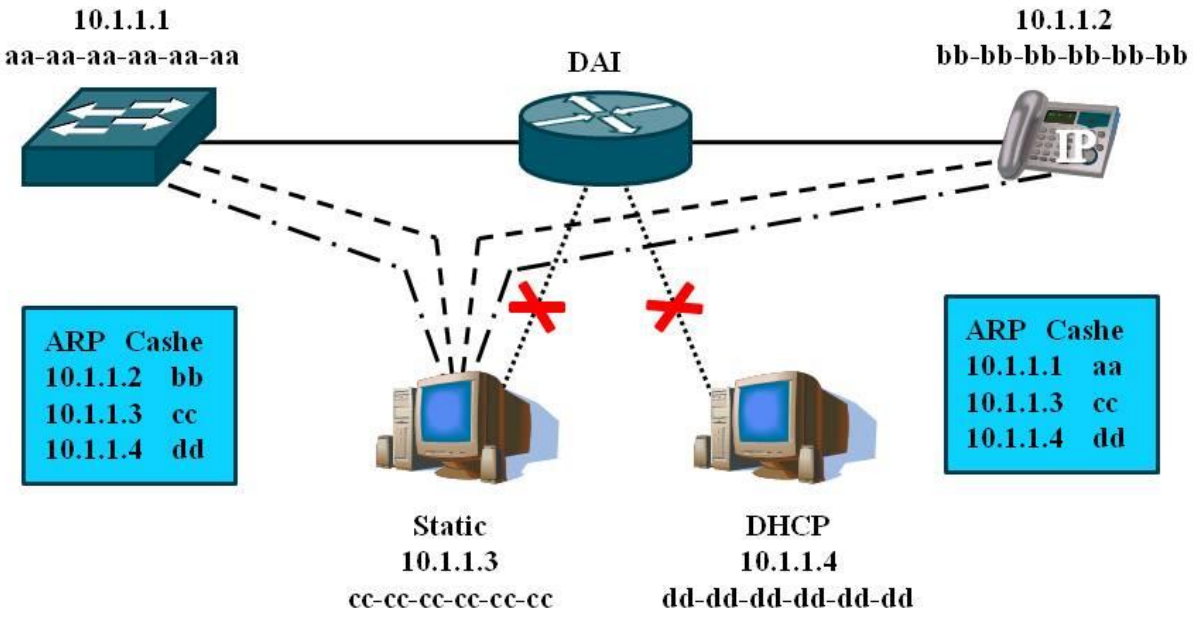
Je třeba zajistit, aby DHCP odpovědi (DHCPOffer, DHCPAck nebo DHCPNak) přicházely pouze od relevantního DHCP serveru. To je zajištěno pomocí tzv. **DHCP snooping binding** tabulky obsahující MAC adresu, IP adresu, lease time, binding type, číslo VLAN a specifikace nechráněného rozhraní.

Dynamic ARP Inspection (DAI, také ARP poisoning, ARP Poison Routing) je zase bezpečnostní vlastnost, která má pod dohledem výskyt ARP paketů v síti. DAI umožňuje správci sítě logovat a rušit ARP pakety s neoprávněnou MAC adresou. Cílem je zabránit útoku typu „man-in-the-middle“ (MitM). Útok typu MitM je založen na používání tzv. „nevyžádaných“ ARP paketů zvaných **gratuitous ARP packets**. Jedná o pakety, kterými stanice oznamuje vazbu mezi IP a MAC adresou (ARP Reply), aniž by obdržela požadavek na vyslání takové informace (ARP Request).

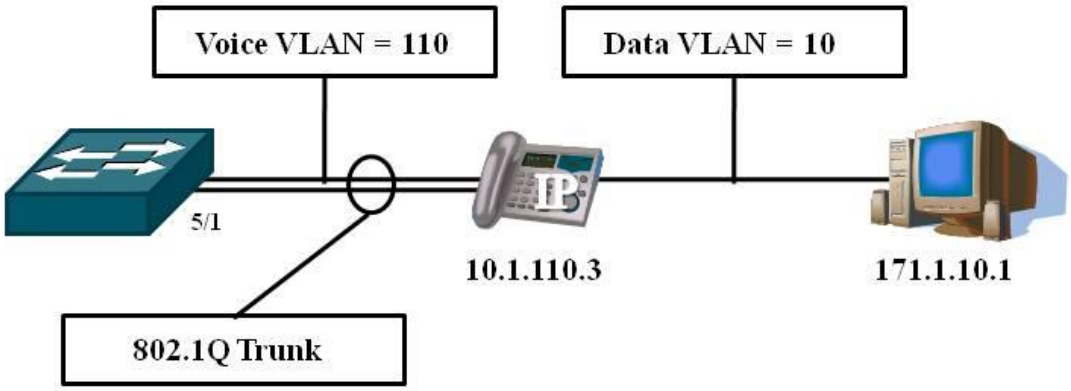
Stanice většinou nevyžádaný ARP paket přijme a informace z něj si zapíše do ARP cache a používá je. Útočník může například pomocí gratuitous ARP podstrčit stanicím svou MAC adresu místo MAC adresy síťové brány. Stanice pak posílají data do jiných podsítí přes počítač útočníka, který je odposlouchává. Obranou je **Dynamic ARP Inspection** (DAI), které využívá tabulku, vybudovanou při DHCP Snoopingu.

Neboli pokud počítač s MAC adresou dd-dd-dd-dd-dd-dd začne posílat falešné DHCP odpovědi, přepínač je nepřijme, protože nejde o důvěryhodný zdroj DHCP informace. Navíc si buduje tabulku DAI, pomocí které kontroluje ARP odpovědi. Pokud útočník z počítače s MAC adresou cc-cc-cc-cc-cc-cc začne posílat ARP odpovědi, nebude mu věřeno.

Neautorizované DHCP a ARP odpovědi



Oddělení hlasových a datových VLAN



Pokyny ke zkoušce

Pozor na http://www.voiptroubleshooter.com/diagnosis/