Young

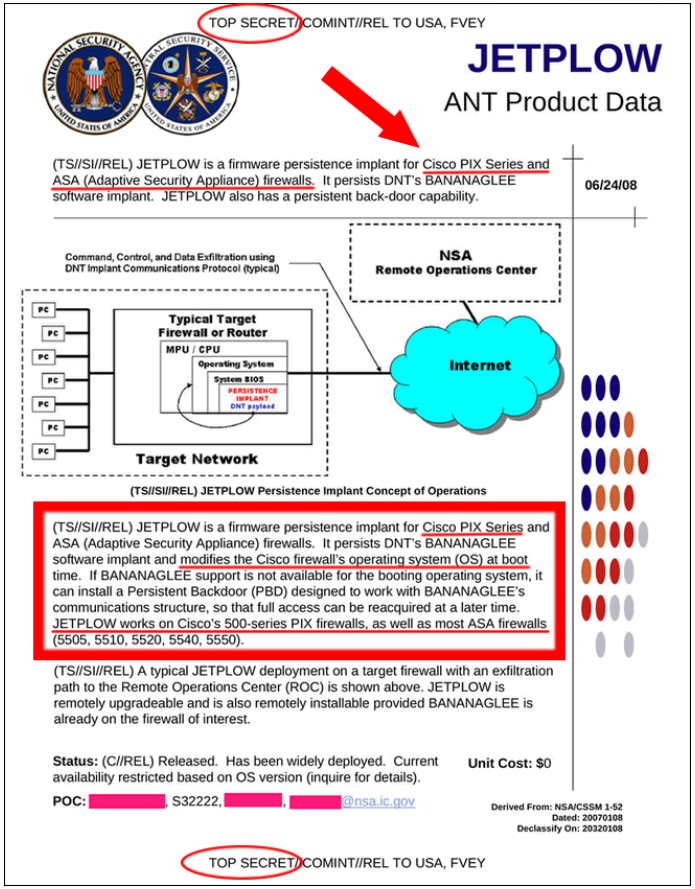
Kommunikációs rendszerekben gondolkodunk

Adatvédelem a VoIP hálózatban

Tűzfalak mögött... biztonságban?

A biztonságról…

„ a lánc erősségét a leggyengébb láncszem határozza meg!”



TOP SECRET//COMINT//REL TO USA, FVEY

JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details).

Unit Cost: $0

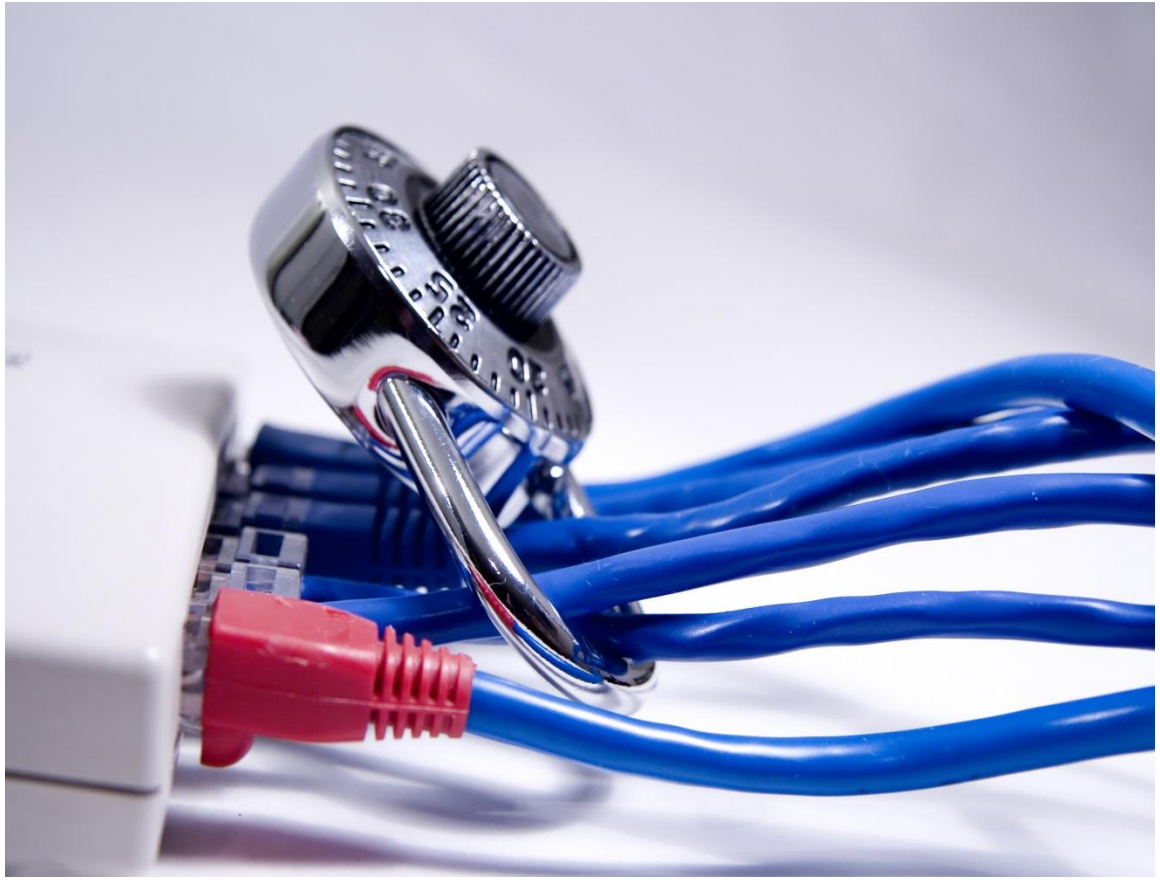
POC: [redacted], S32222, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Young

Tényleg biztonságban vagyunk?



Young

Kockázati forrás is lehet

- IP telefonok megjelenése
- **Előny:**
  - Strukturált kábelezésen keresztül használható
  - Zöldmezős beruházásnál rentábilisabb
  - Telephelyek ingyenes összeköttetése a meglévő IP-s kapcsolaton keresztül
- **Hátrány:** Biztonsági kockázat!

Young

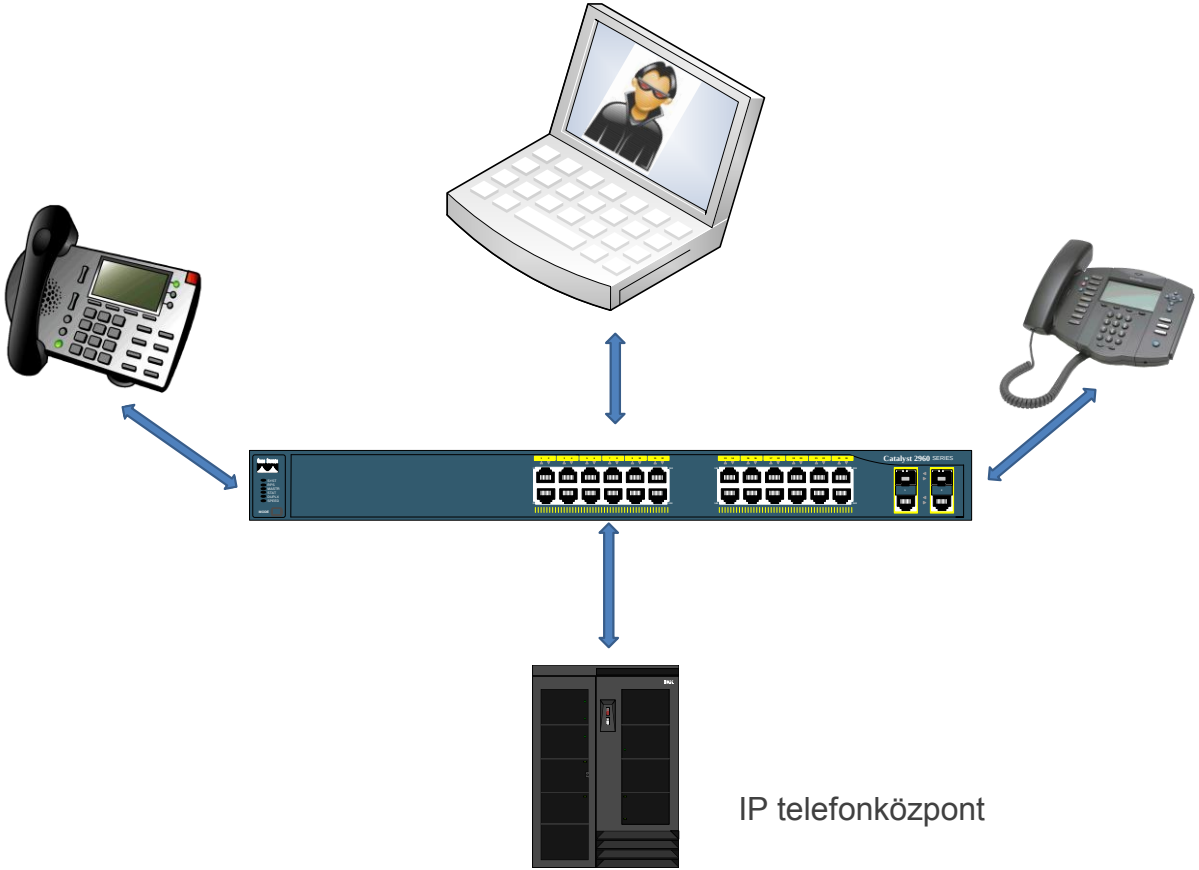
LAN kockázatok

- A hálózati eszközök nem menedzselhetőek
- Biztonsági beállítások hiánya
- A telefonközpont közvetlenül az internetre kapcsolódik, és elfogad direkt IP hívásokat
- Az IP telefonok egy hálózaton a számítógépekkel
- Titkosítás hiánya

Eredmény:

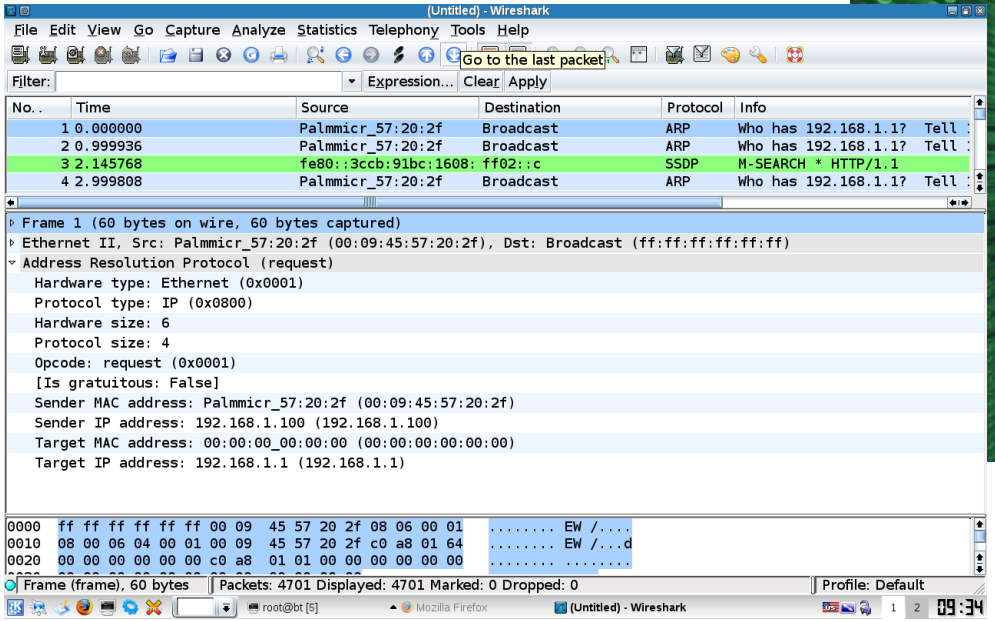
Lehallgathatóvá válnak a telefonbeszélgetések!

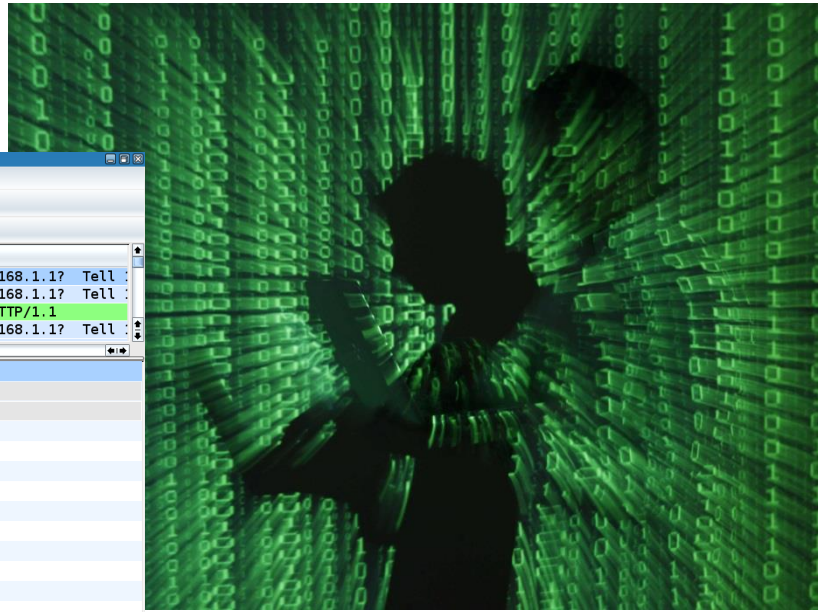
Demó hálózat felépítése



Előkészítő lépések – 1.

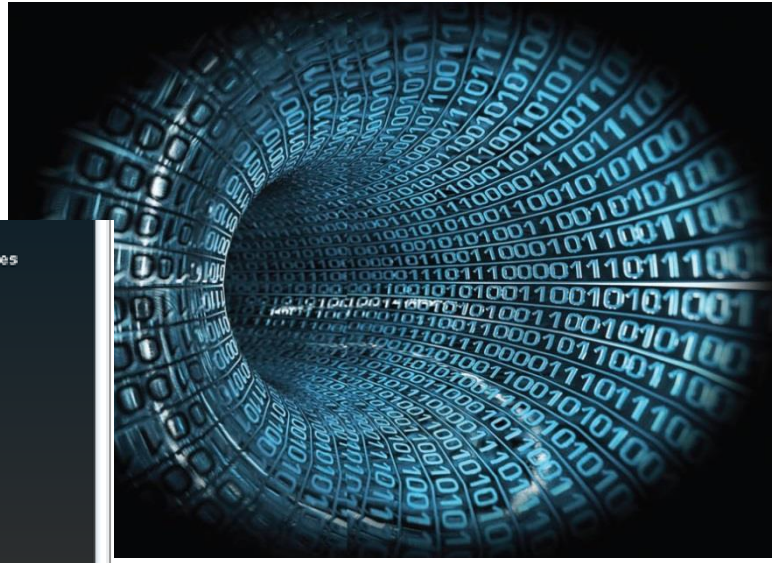
#1 Monitorozás





Előkészítő lépések – 2.

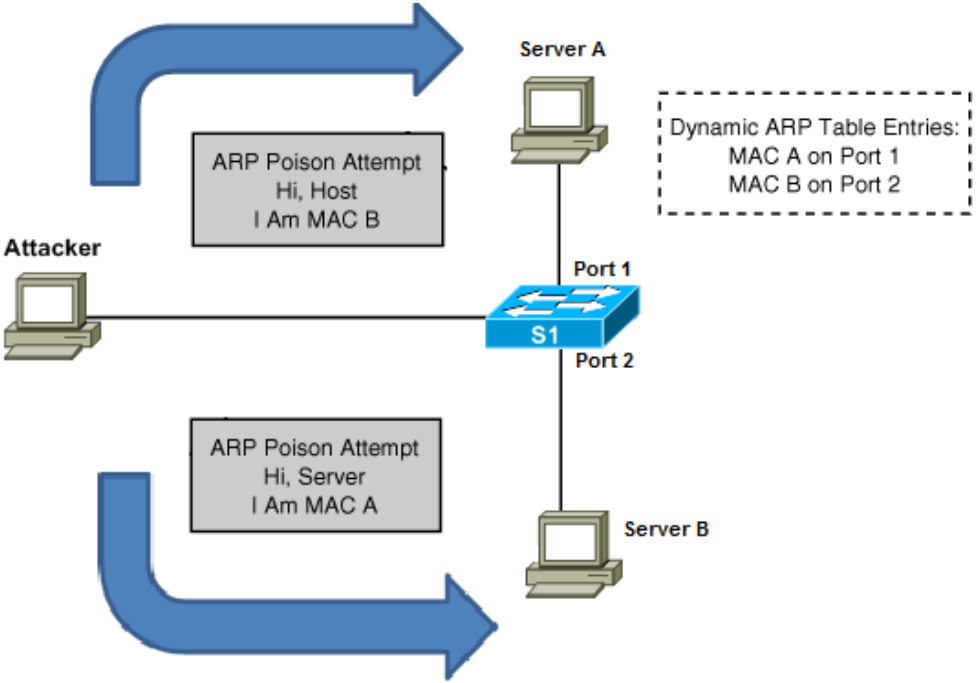
#2 Nyitott portok keresése



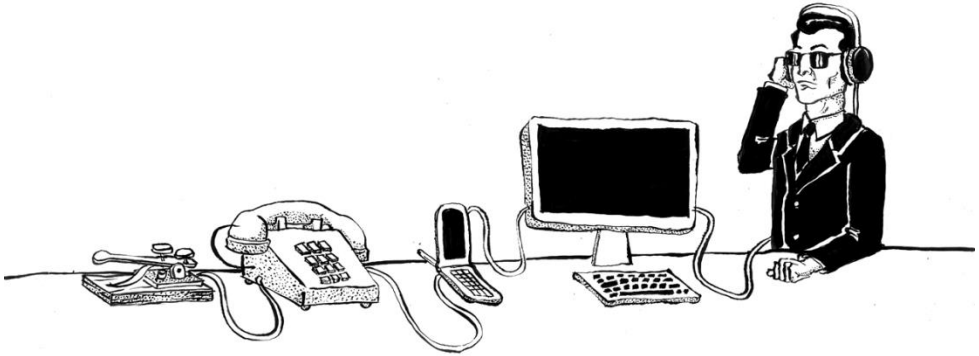
```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-09-07 10:02 EDT
Failed to resolve given hostname/IP: sn.  Note that you can't use '/mask' AND '1-4,7,100-' style IP ranges
Initiating ARP Ping Scan at 10:02
Scanning 192.168.1.101 [1 port]
Completed ARP Ping Scan at 10:02, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:02
Completed Parallel DNS resolution of 1 host. at 10:02, 13.00s elapsed
Initiating SYN Stealth Scan at 10:02
Scanning 192.168.1.101 [1000 ports]
Discovered open port 23/tcp on 192.168.1.101
Discovered open port 80/tcp on 192.168.1.101
Discovered open port 5060/tcp on 192.168.1.101
Completed SYN Stealth Scan at 10:02, 1.39s elapsed (1000 total ports)
Nmap scan report for 192.168.1.101
Host is up (0.013s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
5060/tcp open  sip
MAC Address: 00:09:45:57:9F:BC (Palmmicro Communications)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
           Raw packets sent: 1008 (44.336KB) | Rcvd: 1001 (40.040KB)
root@bt:~#
```

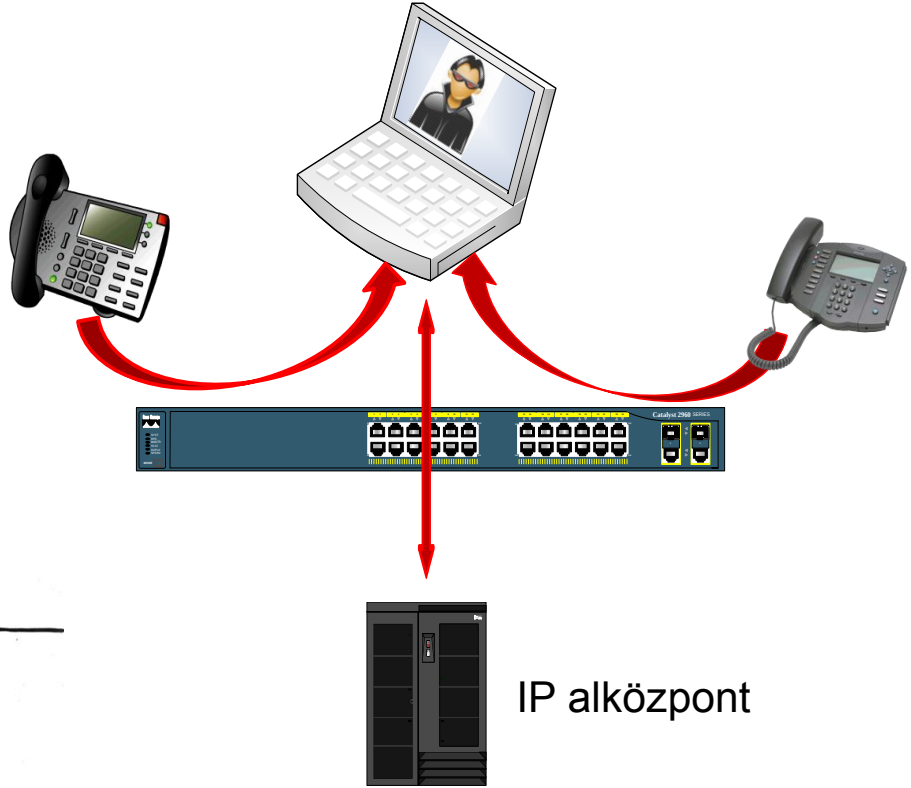
Shell

#3 ARP poisoning



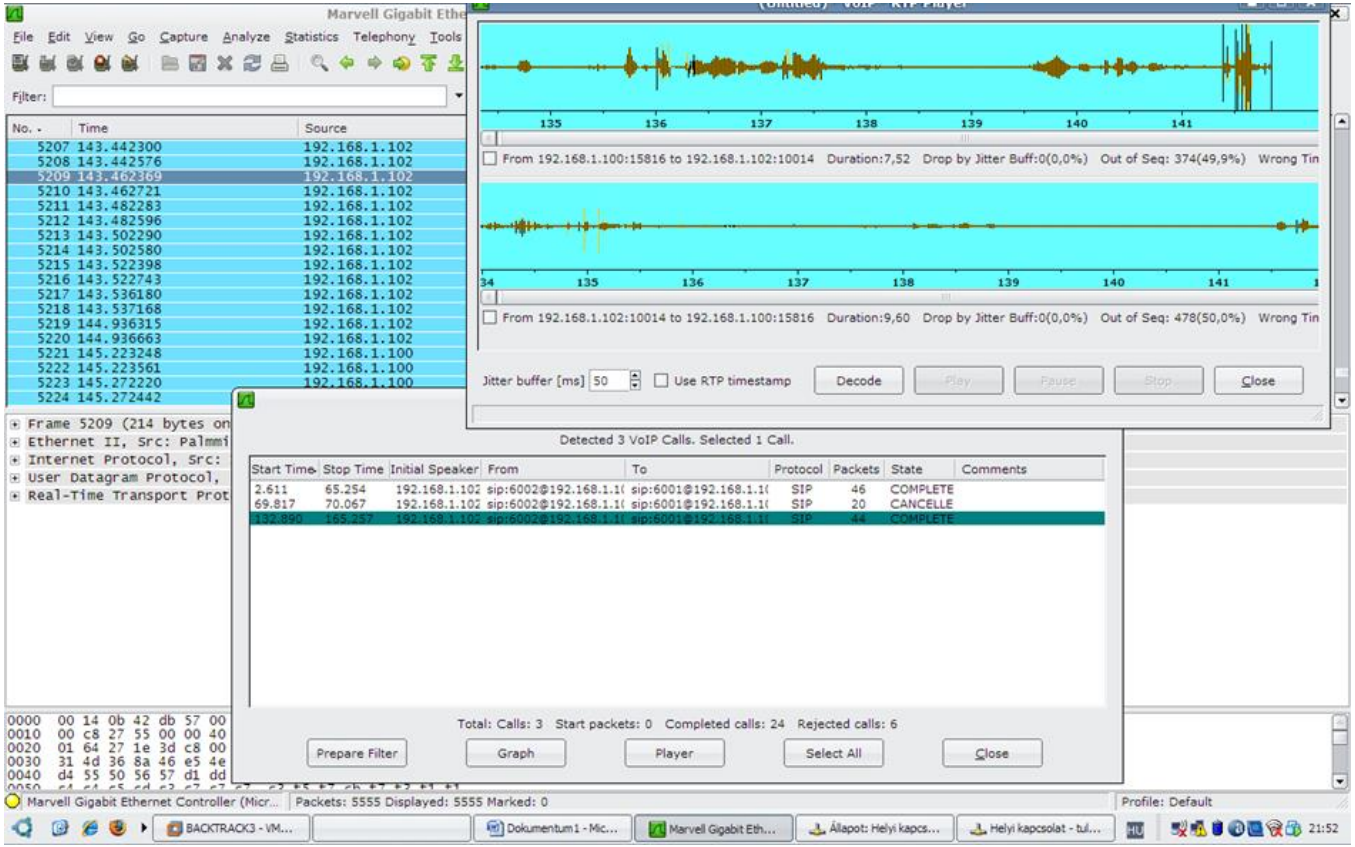
Sikeres támadás



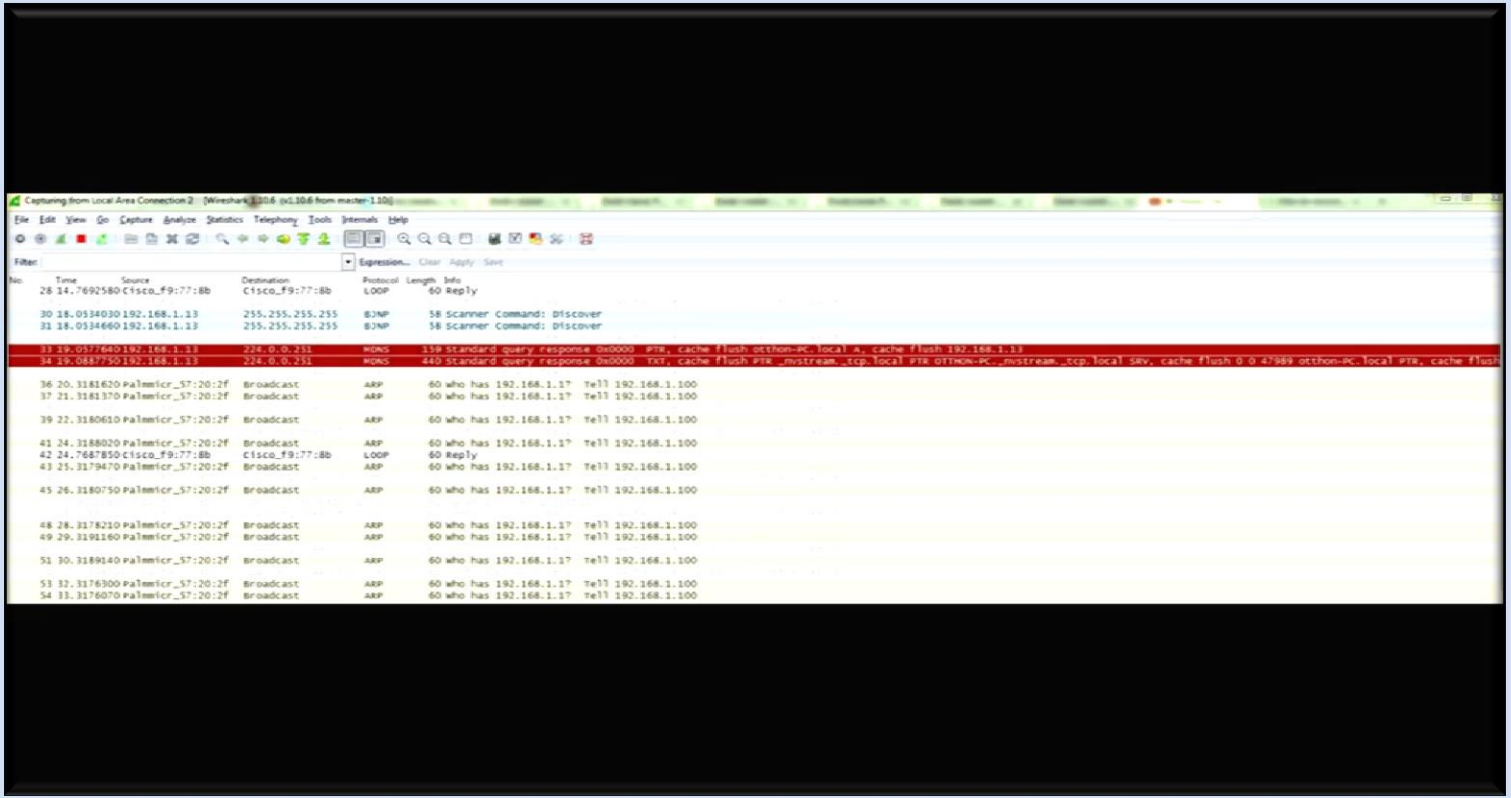


Young

Lehallgatás, dekódolás



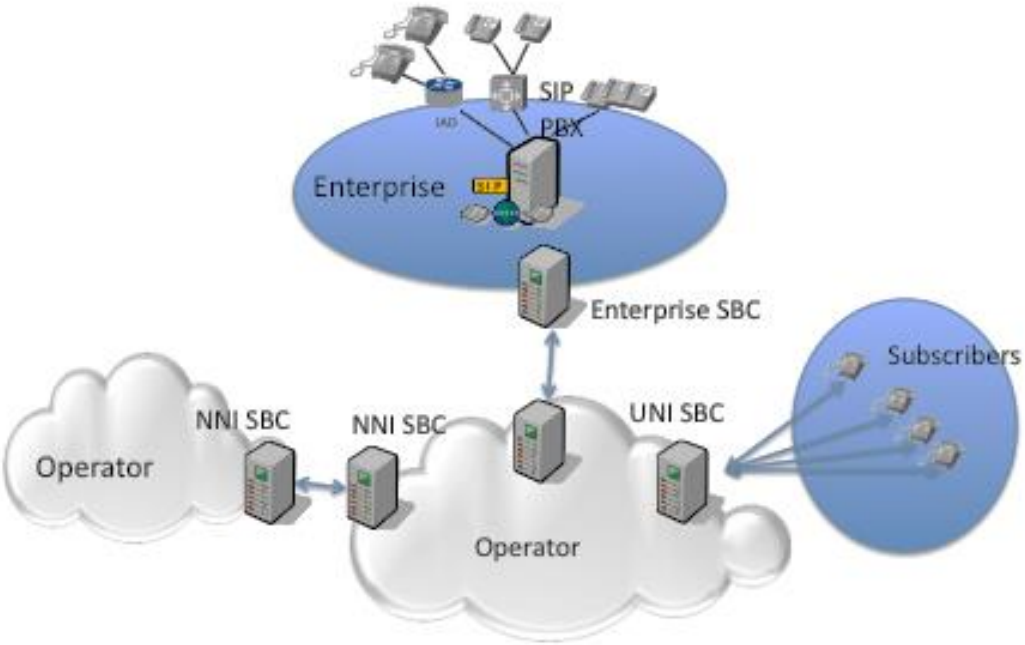
ARP poisoning



Hogyan védekezzünk

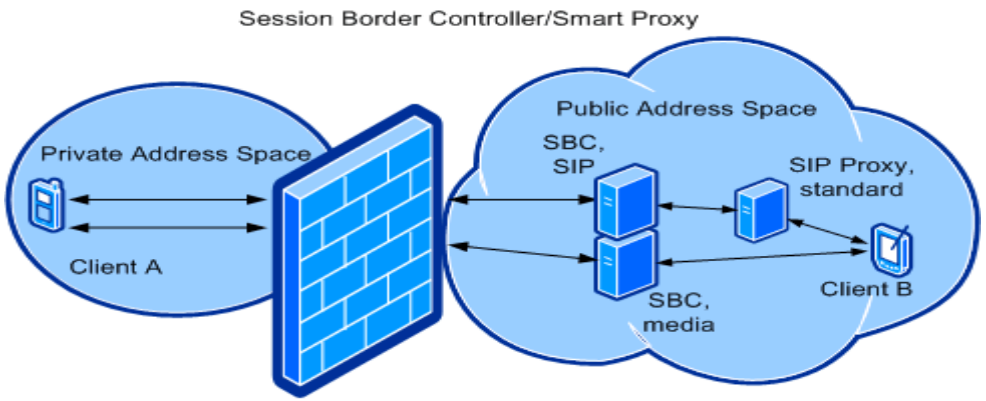
- Az IP telefonok forgalmát különítsük el a belső hálózattól
- Az IP alközpontot tűzfal mögé telepítsük!
- SIP TLS és SRTP támogatott eszközök használata
- Folyamatosan figyeljük a hálózatunkat
- Védjük meg a hálózatunkat!

Session Border Controller



Az SBC felhasználása I.

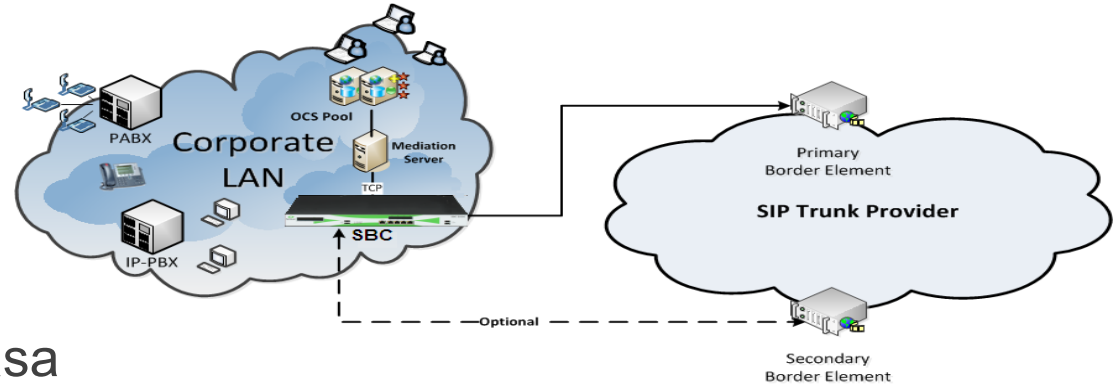
1. **Biztonság**
   - DoS védelem
   - Topológia elrejtése
   - Védelem módosított csomagokkal szemben
   - Titkosítás
2. **Kapcsolat**
   - NAT is helyettesíthető
   - SIP normalizálása
   - VPN kapcsolat
   - Protokoll transzláció



Az SBC felhasználása II.

3. QoS

- Forgalom szabályozása
- Erőforrás allokáció
- CAC – SIP erőforrás foglalás



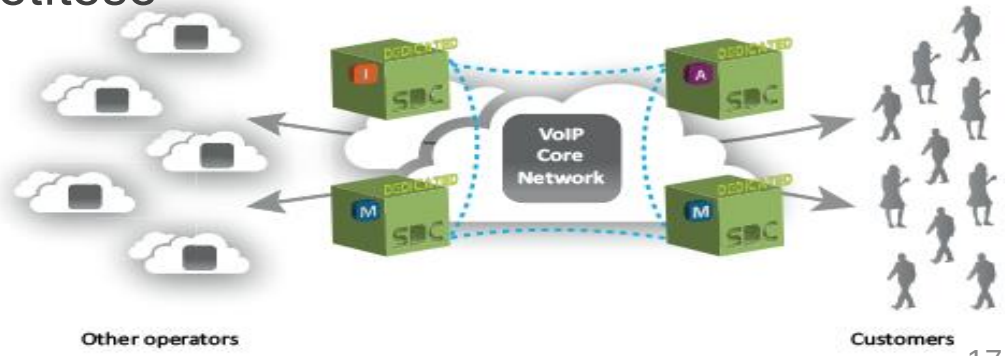
4. Szabályozás

- Vészhívás biztosítása
- Törvényes adatmentés

Az SBC felhasználása III.

5. Szolgáltatások

- DTMF átvitel biztosítása a hálózatok közt
- Média transzkódolás elvégzése
- Hangok és hangbemondások bejátszása
- Adat- és faxátvitel „közvetítése”
- Hang- és videóhívások támogatása



Patton SmartNode 5480 - SBC

64 egyidejű VoIP beszédcsatorna

- VoIP transzkódolás
- SIPv2 jelzésváltás
- H.323v4

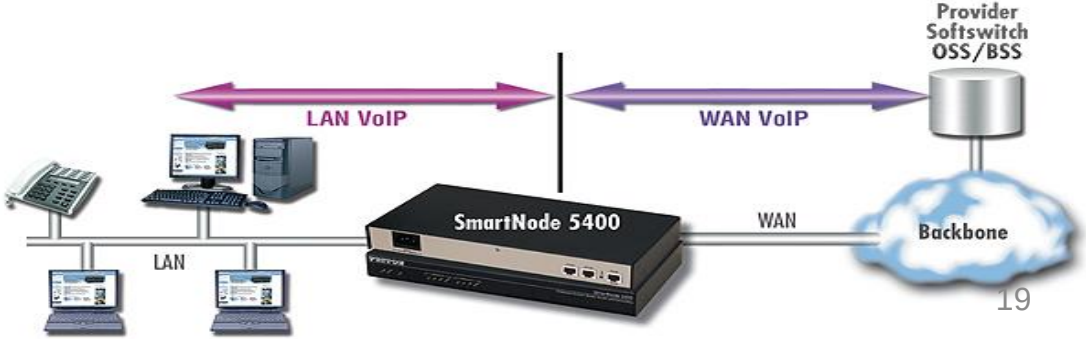
IP access router / routing

- DHCP kliens és szerver
- RIP v1/v2
- BGP
- Tűzfal
- NAT / NAPT
- Access Control List
- VRRP
- Policy Based Routing
- DMZ
- IP Sec VPN

Young

Patton SmartNode 5480 - SBC

- **QoS**
  - Hang priorizálása
  - Traffic management
    - Shaping
    - Policing
  - VLAN tagek módosítása
  - IEEE 802.1p
  - IEEE 802.1Q
  - DownStreamQoS™
  - ToS
  - Diffserv



Young

Köszönöm a figyelmet!

Young

KOMMUNIKÁCIÓS RENDSZEREKBEN GONDOLKODUNK