# Bezpečná konfigurace přepínačů a směrovačů

## Bezpečnost ICT 2

Lukáš Malina

Vysoké učení technické v Brně
malina@vut.cz
axe.vut.cz

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

2022

Informační bezpečnost

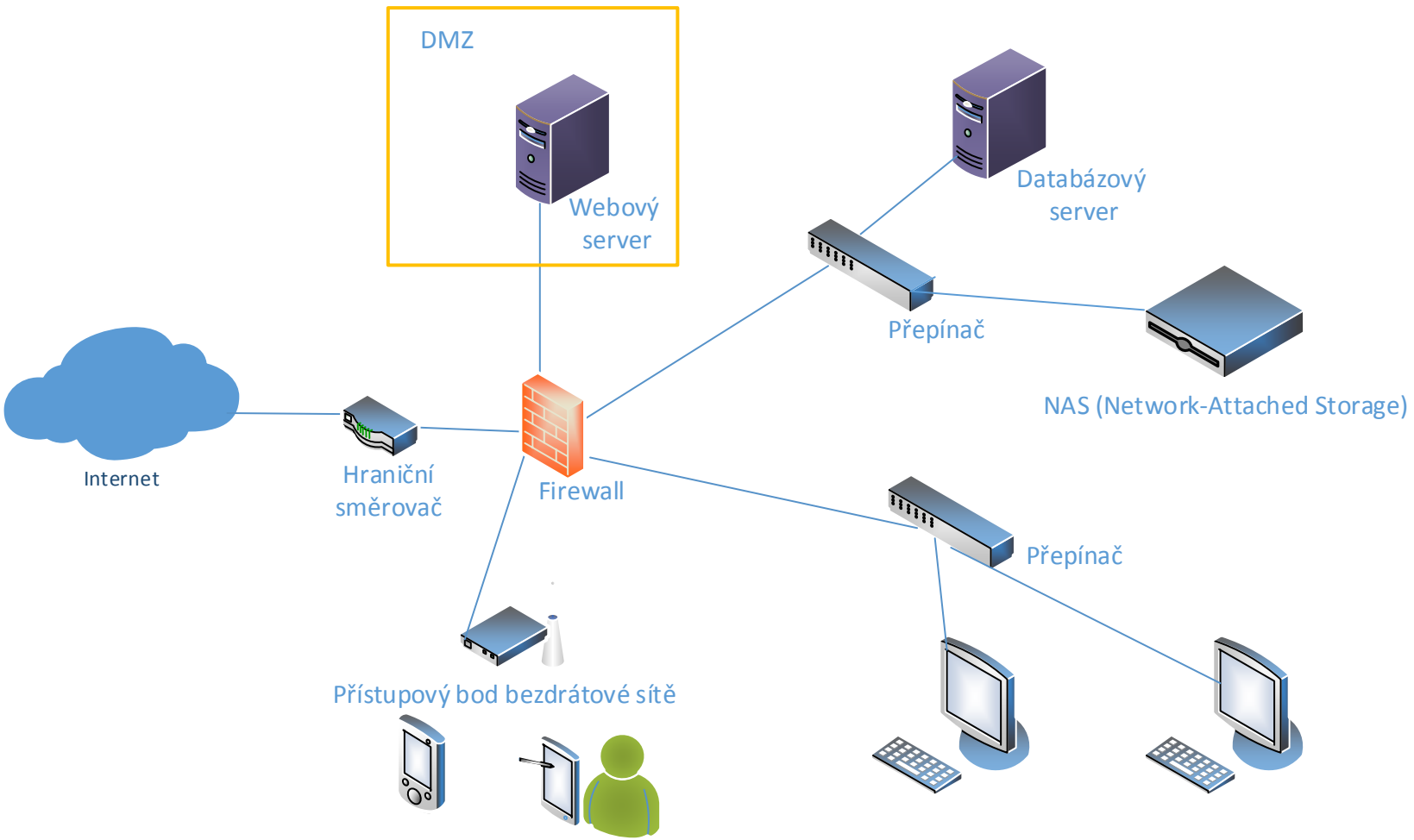
# Bezpečnost sítě

- Dnešní sítě jsou heterogenní (různé typy koncových stanic) a bez pevně daných hranic díky možnosti vzdálenému připojení a zvýšené konektivitě.
- Nebezpečí v sítích: odposlech dat, jejich modifikace, neoprávněný přístup, (D)DoS, zneužití pro (D)DoS, útoky malware, atd.
- Cíle bezpečnosti sítí: ochrana dat (provozu), ochrana koncových stanic a ochrana síťových služeb a protokolů.
- Zabezpečení sítě probíhá obvykle na vrstvách 2 až 7 ISO/OSI.

# Typy síťových prvků

- L1 ISO/OSI: rozbočovač (hub), opakovač (repeater).
- L2 ISO/OSI: most (bridge), přepínač (switch).
- L3 ISO/OSI: směrovač (router), brána (gateway), L3 přepínač (L3 Switch), virtuální switch (Open vSwitch), virtuální router (OpenWrt), paketový firewall, síťové úložiště (Network-Attached Storage (NAS)), ...
- L4 - L7 ISO/OSI: IPS sonda, IDS sonda, VPN brána, honeypot, anti-DDoS, anti malware zařízení, stavový FW, FW nové generace (NGFW), proxy servery, přístupový bod (access point), servery, stanice, ...

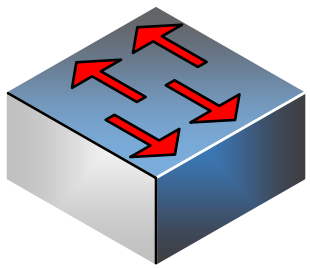
# Bezpečnost sítě - příklad malé sítě

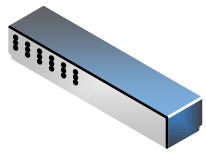


# Bezpečná konfigurace přepínače

# Bezpečná konfigurace přepínače

- Přepínač (Switch) - **pracuje na 2.vrstvě ISO/OSI**, přeposílá data uvnitř sítě (LAN) již po odfiltrování provozu firewallem/hraničním směrovačem.
- **Zabezpečení LAN** je stejně důležité jako zabezpečení perimetru (hraničním směrovačem/firewallem) sítě.
- **L3 přepínače (pracují i se 3.vrstvou OSI).**
- Borderless network - přístup do sítě s více lokalit, zanikají pevné hranice sítě.

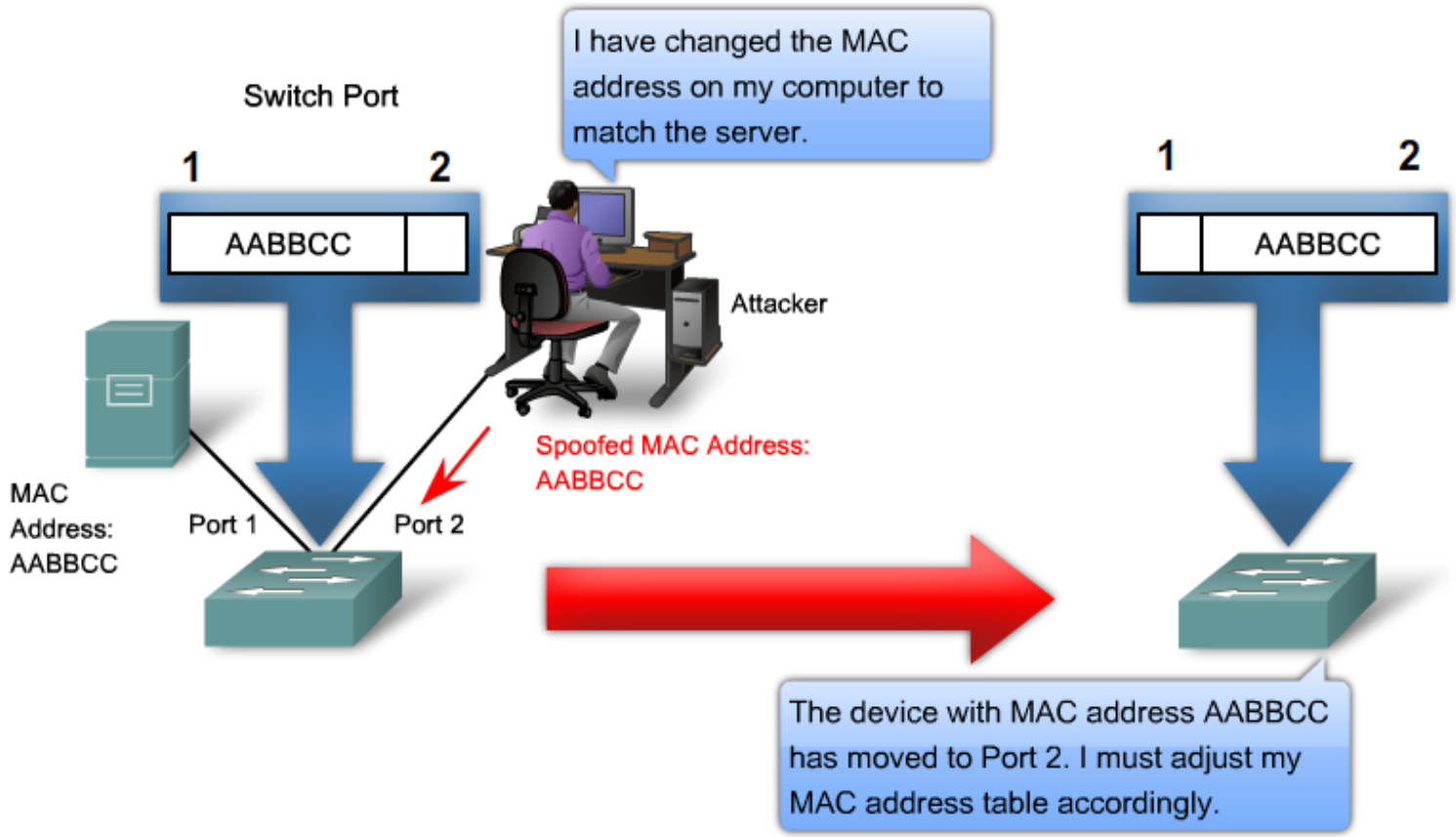




# Bezpečná konfigurace přepínače - útoky uvnitř sítě I.

- **MAC address spoofing** útoky (neautorizovaný příjem cizích dat zpráv pomocí nelegitimní změny zdrojové adresy MAC na přepínači).
- **ARP poisoning** útoky (úprava cache ARP na dvou portech vede k útoku mužem uprostřed MitM, kdy je komunikace vedená přes útočníka).
- **Rogue DHCP Server/spoofing** (útočník řídí falešný DHCP server a odpoví rychleji na DHCP request klientům - může podvrhnout bránu(jako MitM), DNS server nebo přiřadí neroutovatelnou IP adresou - DoS).
- **DHCP starvation** útoky (útočník zaplaví DHCP server velkým počtem DHCP request (nové MAC) a snaží se vyčerpat IP adresy, které lze přiřadit).

# MAC/ARP spoofing



# Bezpečná konfigurace přepínače - útoky uvnitř sítě II.

- **STP (Spanning Tree Protocol) manipulation** útoky (útočník se nastaví jako root bridge pro příjem provozu v síti), STP je určeno k odstranění smyček a nalezení nejvhodnější cesty v redundantních sítích.
- **MAC address table overflow**/address flooding útok (záplava falešnými zprávami o MAC adresách vede k vyčerpání tabulky adres MAC na přepínači a přepínač pak vše přeposílá všemi porty - degraduje na HUB).
- **LAN storm** útoky (přepínače přeposílají broadcast všemi porty - to vede k degradaci sítě LAN záplavou paketů - CPU přepínače až na 100 % - odepření služeb DoS).
- **VLAN útoky** (např. VLAN hopping pomocí spoofingu DTP zpráv, Double-Tagging VLAN pomocí vnoření další hlavičky do VLAN dat).

# Bezpečná konfigurace přepínače - základní postup

- **Zabezpečení fyzického přístupu k přepínači**.
- **Nastavení bezpečného lokálního přístupu** na přepínač pro jednotlivé uživatele včetně odlišení privilegií.
- **Nastavení bezpečného vzdáleného přístupu** na přepínač, tj. SSH s klíči RSA 2048b, případně HTTPS.
- **Vypnutí nepotřebných služeb a portů**.
- **Zapnutí dalších bezpečnostních funkcí** na přepínači (dhcp snooping, port security, ...).
- **Zajištění záloh konfigurace**.
- **Kontrola konfigurace, testování, ověřování**.

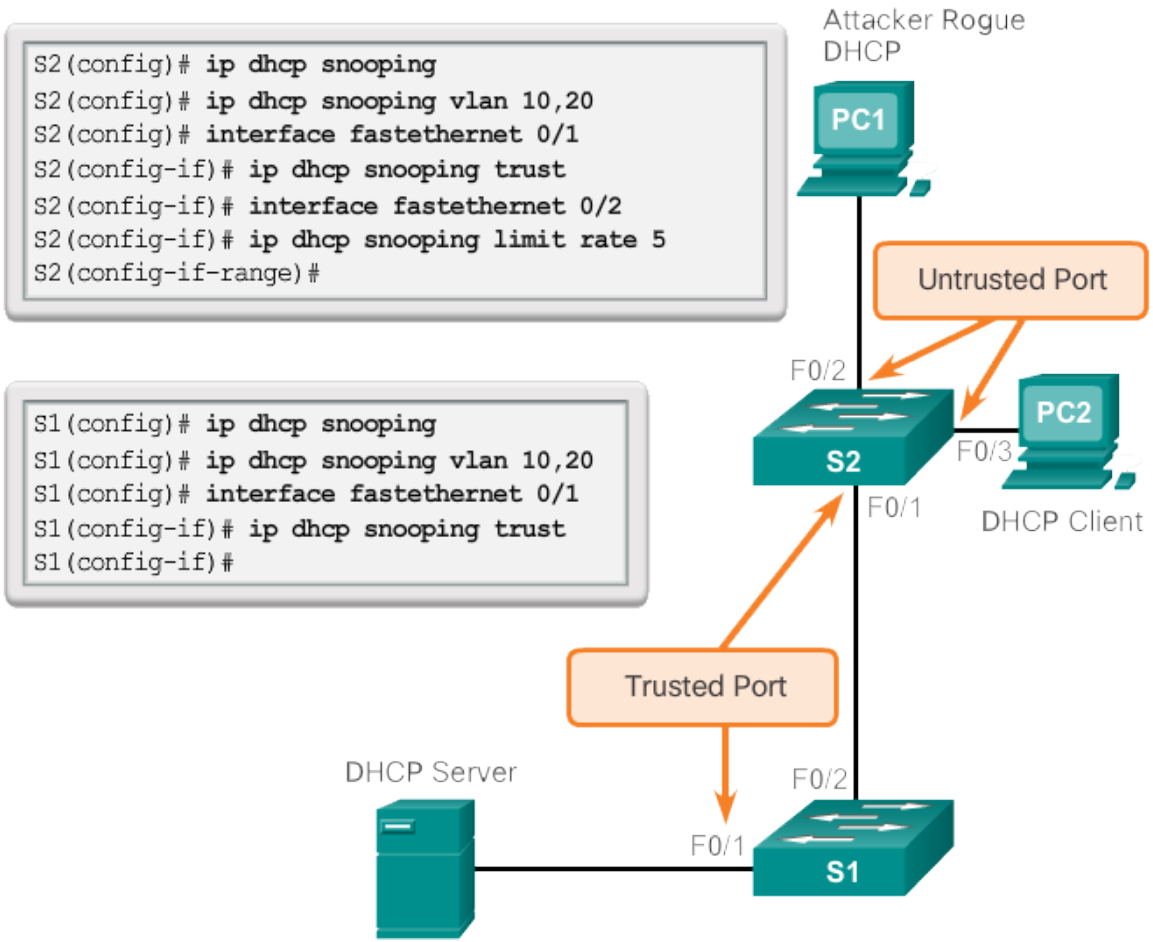
# Bezpečná konfigurace přepínače Cisco - metody obrany

- Zmírnění útoků na ARP - konfigurace Dynamic ARP Inspection (DAI), používá informace z tabulky pro DHCP Snooping.
- Zmírnění útoků na MAC adresy - konfigurace bezpečnosti portů na přepínači, omezení počtu MAC adres na port **Port Security**.
- Zmírnění útoků na DHCP - funkce **DHCP snooping**(omezuje Rogue DHCP útoky) a port security (omezuje DHCP Starvation).
- Zmírnění útoků na STP - metody **PortFast, Root guard a BPDU guard**.
- Zmírnění útoků LAN storm - metoda **Storm control**.
- Zmírnění útoků VLAN - např. VLAN hopping lze zmírnit pomocí vypnutí trunkingu na portech, které jej nepotřebují, nepoužívat VLAN 1 pro všechno.

# Bezpečná konfigurace přepínače Cisco - DHCP snooping

```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10,20
S2(config)# interface fastethernet 0/1
S2(config-if)# ip dhcp snooping trust
S2(config-if)# interface fastethernet 0/2
S2(config-if)# ip dhcp snooping limit rate 5
S2(config-if-range)#
```

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)#
```



# Bezpečná konfigurace přepínače Cisco - konfigurace I.

- Metoda **Port Security** poskytuje ochranu před útoky MAC (spoofing, table overflows).
- Zdrojové MAC mohou být konfigurovány manuálně nebo automaticky naučeny.
- Port security aging - nastaví dobu užití (v minutách) pro statickou nebo dynamickou adresu na portu.
- Příkazy: `switchport mode access`, `switchport port-security`, `switchport port-security maximum` *`value`*.

# Bezpečná konfigurace přepínače Cisco - konfigurace II.

- **PortFast** - nastaví port na forwarding state ihned po zapojení (obchází STP učení), je vhodné jen při připojení stanic a serverů.
- Příkaz pro nastavení PortFast na portech: `spanning-tree portfast default`.
- **BPDU Guard** - chrání síť před zasláním BPDU zpráv na porty, kde by neměli chodit (BPDU může chodit jen od SW, nikoliv od PC/útočníků na access portech).
- Příkaz pro nastavení BPDU guard : `spanning-tree portfast bpduguard default`.

# Bezpečná konfigurace přepínače Cisco - konfigurace III.

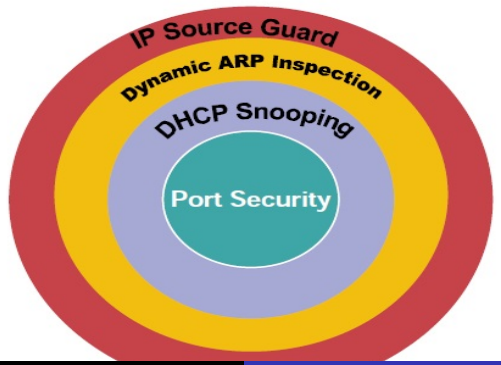
- **Root Guard** - posiluje umístění root bridge v síti díky limitaci portů. Pokud útočník pošle spoofovanou zprávu BPDU, aby se stal root bridge, přepínač tyto pokusy ignoruje a daný port nastaví na stav *root-inconsistent*.
- `storm-control` - jedná se o příkaz, který slouží pro nastavení prahových hodnot (práh nad sledovaný pkts/s) na provoz (uni/multi/broadcast) a tím zmírňuje útoky LAN/traffic storm.
- **Private VLAN** (PVLAN Edge) funkce - izolace portů v rámci VLAN. Datový provoz lze pak přeposlat jen přes L3 zařízení.
- **SPAN** - **Switched Port Analyzer** zrcadlí provoz např. pro sondy IPS, pomáhá při dohledu nad provozem.

# Bezpečná konfigurace přepínače Cisco - shrnutí I.

- Povolit pouze bezpečný přístup ke konfiguraci přepínače (přes **SSH**, out-of-band management, ACLs, etc.).
- Používat **Port Security**, kde je možné.
- Nastavit všechny uživatelské porty na non-trunking: `switchport mode access`
- Nakonfigurovat **PortFast** na všechny non-trunking porty.
- Nakonfigurovat **BPDU guard** na všechny non-trunking porty.
- Nakonfigurovat root guard na STP root porty.
- Manuálně nastavit všechny trunk porty a zakázat DTP na těchto portech.
- Nakonfigurovat **DHCP snooping**.

# Bezpečná konfigurace přepínače Cisco - shrnutí II.

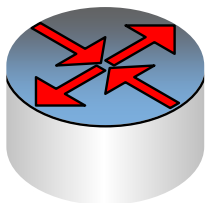
- Používat CDP (Cisco Discovery Protocol) pouze kde je to nutné.
- Užívat nadefinované VLAN namísto defaultní VLAN 1.
- Zakázat všechny nepoužívané porty a zařadit je do nepoužívané VLAN.
- Nakonfigurovat PVLAN Edge, kde je nutné.
- Používat vyšší verze SNMP (v3), používat autentizaci u VTP.
- Zabezpečit ARP/MAC/IP (Dynamic ARP Inspection, IP Source Guard).

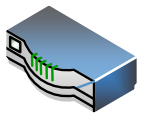


# Bezpečná konfigurace směrovače

# Směrovače

- Směrovač (Router) - **pracuje na 3.vrstvě ISO/OSI**, síťové zařízení pro přeposílání dat a jejich směrování mezi sítěmi.
- Spojuje dvě a více datových linek různých sítí.
- Různé velikosti (domácí, střední sítě, páteřní sítě).
- Hraniční směrovače pro připojení do vnější sítě.
- Směrovač s paketovou filtrací.





# Směrovače v sítích a typy

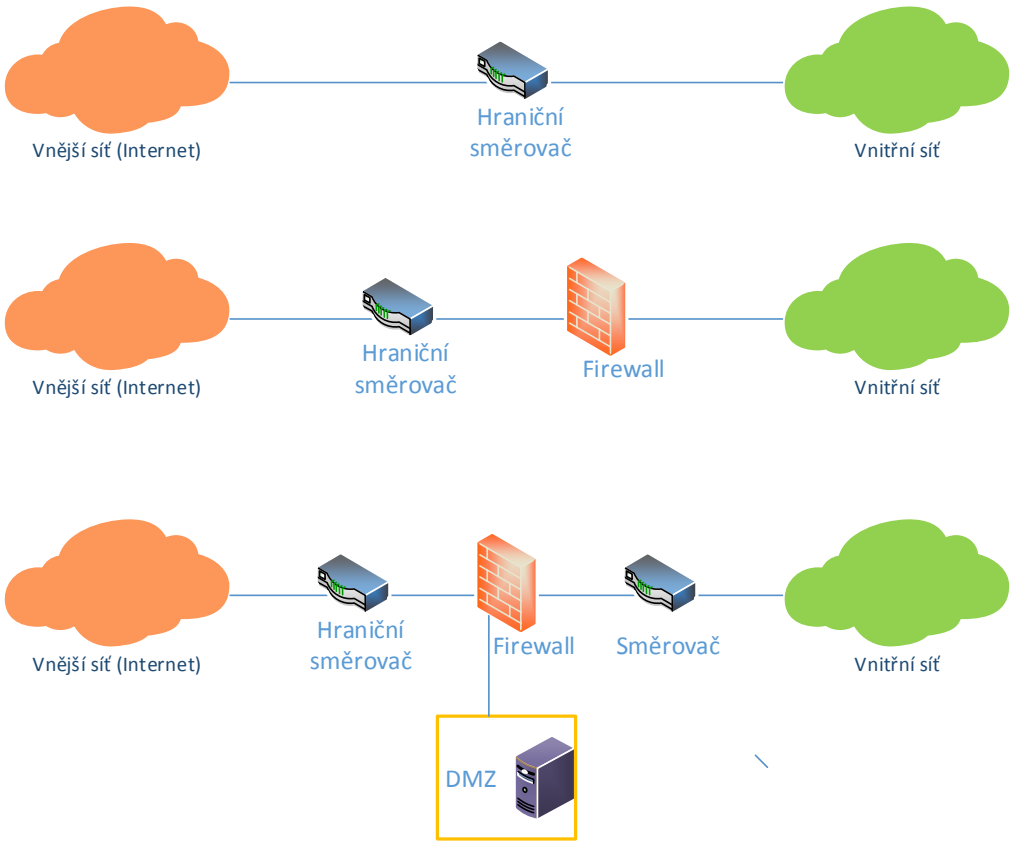
- Směrovače v síti.
- Hraniční směrovače.
- Směrovače s paketovou filtrací a bezpečnostními funkcemi.
- Malé směrovače (domácí).

# Hraniční směrovač

- Hraniční směrovač (Edge Router).
- Poslední směrovač **mezi vnitřní a nedůvěryhodnou sítí** (vnější).
- Většinou s paketovou filtrací pro zajištění bezpečnostních pravidel.
- Je třeba zajistit **fyzickou bezpečnost** (zabezpečit jeho uložení, Uninterruptible Power Supply - **UPS**), bezpečnost OS směrovače (aktualizace, patche, záloha conf) a bezpečnou konfiguraci směrovače tzv. **router hardening** (bezpečná administrace, zakázat nepoužívané porty a rozhraní, zakázat nepotřebné služby, logovat události).
- **Zabezpečení sítě** pomocí funkcí směrovače a **filtrování** provozu.

# Hraniční směrovač - typy zapojení s FW

Single Router zapojení, zapojení R+FW, DMZ (demilitarizovaná zóna) zapojení



# Útoky na směrovače

- **Pokus o průnik do nastavení na směrovači** - zneužití defaultních hesel (např. cisco/cisco atp.).
- **Routing table poisoning** - vyvolání nežádoucí změny ve směrovací tabulce pomocí spoofování routovacích protokolů.
- **Hit-and-Run attack** - posílání škodlivých paketů do směrovače v náhodných intervalech.
- **DoS/DDoS attack** – útok zaplavením množství paketů a vytížení CPU/RAM, logické útoky (Xmas attack atd.).
- **Packet mistreating attack** – implementace škodlivého kódu a špatné zpracování paketů, tvoření smyček, DoS atp.

# Bezpečná konfigurace směrovače - základní body postupu

- **1. zabezpečit směrovač (router hardening, fyzická bezpečnost, aktualizace, patch)**,
- **2. zabezpečit směrovačem síť** (např. nastavit ACL, konfigurace NAT, konfigurace bezpečného směrování),
- **3. konfigurovat další bezpečnostní funkce podporující bezpečnost sítě** (modul firewall, brána VPN, podpora AAA, IPS, monitoring, load balancing).

# Bezpečná konfigurace směrovače - router hardening I.

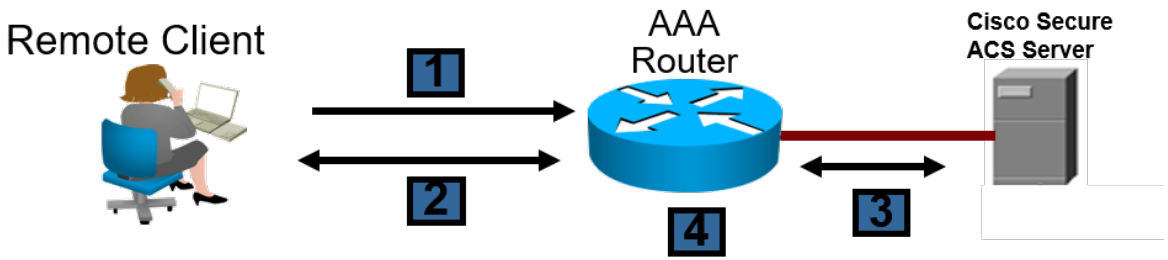
- **Zabezpečit administrativní přístup** podle rozhraní (změnit defaultní heslo na silné heslo, blokovat a zpožďovat pokusy, detekce útoku na hesla).
- **Zobrazit upozornění**/notifikaci pro neautorizované uživatele (banner).
- **Konfigurace SSH** (unikátní hostname, korektní doménové jméno routeru, nastavení autentizace ...).
- **Konfigurace privilegií** pro uživatele.
- **Vypnutí nepoužitých rozhraní**.

# Bezpečná konfigurace směrovače - router hardening II.

- **Zrušení nepotřebných služeb** a **zákaz skenů** (např. blokace ICMP žádostí).
- Zakázat HTTP konfiguraci směrovače.
- Zakázat gratuitous a proxy ARP.
- Zakázat IP broadcasting (kvůli Smurf DoS útoku) a IP zdrojové směrování (IP source routing, např. obcházení FW).
- **Definovat** paketovou **filtraci** / tzv. **Access Control List** (ACL) a ustanovit odchozí a příchozí politiku filtrování adres.
- **Zapnout** dostupné **bezpečnostní funkce** a **protokoly** (AAA, IPS, VPN, ...).
- **Nastavení bezpečného management sítě** (restrikce SNMP, používat verzi 3 se šifrováním a autentizací).
- **Monitorovat, logovat** a kontrolovat bezpečnostní **logy** (Syslog).

# Bezpečný přístup na směrovač pro administraci

- **Lokální** přístup na směrovač - **konzole**, zavádět bezp. hesla (změnit defaultní), chránit i vyšší úrovně nastavení (privilegovaný režim).
- **Vzdálený** přístup na směrovač - přes klienta **SSH** (např. 2048-b RSA), telnet nepoužívat - nešifrováno!.
- Autentizace uživatelů pomocí AAA serverů (TACACS+, RADIUS).



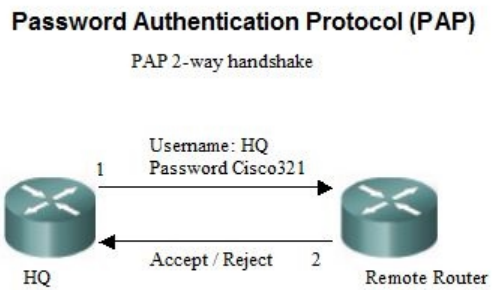
# AAA protokoly RADIUS a TACACS+

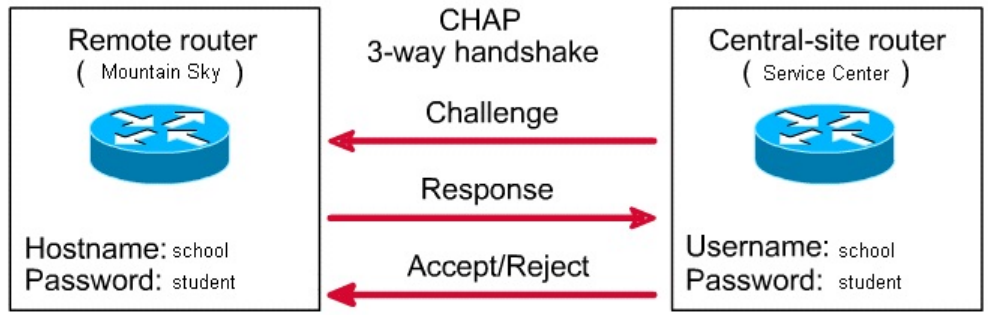
Tabulka : Porovnání AAA protokolů TACACS+, RADIUS

| | **TACACS+** | **RADIUS** |
|---|---|---|
| Funkcionalita | Odděluje služby AAA, dobrá modularita. | Kombinuje autentizaci a authorizaci, ale odděluje accounting/učtování, menší flexibilita než u TACACS+ |
| Standard | Cisco proprietary, IETF | Open/RFC standard (2865/6158) |
| Transportní protokol/port | TCP/49 | UDP/1812,1813,1645,1646 |
| CHAP | Obousměrný výzva/odpověď (challenge/response) - Challenge Handshake Authentication Protocol (CHAP) | Jednosměrná výzva a odpověď od serveru Radius ke klientovi. |
| Podpora protokolů | Multiprotocol support | Ne ARA, ne NetBEUI |
| Důvěrnost a šifrování | Celý paket šifrován | Šifrování hesel |
| Další funkce | Poskytuje autorizaci příkazů směrovače (per-user, per-group). | Neposkytuje autorizaci příkazů podle uživatele/skupin. |

# Autentizační protokoly PAP, CHAP a EAP

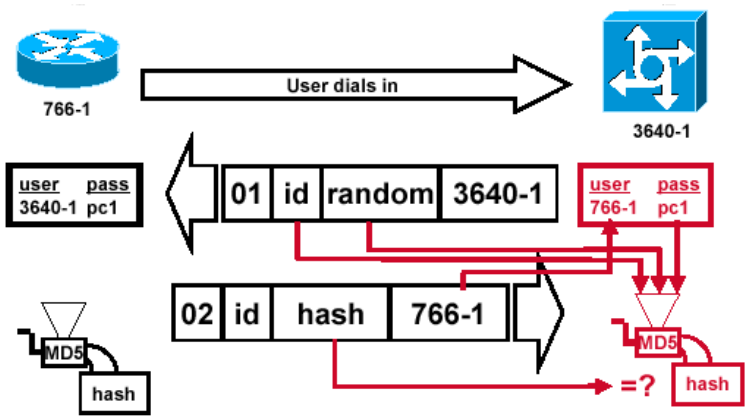
- **Password Authentication Protocol (PAP)** - slabá bezpečnost, **pouze sdílené heslo.**
- **Challenge-Handshake Authentication Protocol (CHAP)** - ochrana proti útokům opakování, **náhodná výzva**, opět sdílené heslo, RFC 1994.
- **Extensible Authentication Protocol (EAP)** - **autentizační framework**, EAP-TLS, EAP-MD5 (zranitelné na slovníkové a MitM útoky), EAP-IKEv2, EAP-PSK (sdílené heslo, 4 zprávy) a mnoho dalších verzí, RFC 5247.
- V rámci EAP je nutné zvolit bezpečnou a aktuální verzi (ne EAP-MD5).



# Bezpečný přístup na směrovač pro protokoly a ostatní zařízení

- Autentizace device-to-device pro servery a služby (EAP).
- Nastavit bezpečnou autentizaci pro přenos Point-to-Point Protocol PPP, např. CHAP/EAP.
- Autentizace routovacích protokolů (např. MD5 otisk dat při sdíleném heslu mezi směrovači s OSPF, sdílené heslo v RIPv2).
- Autentizace SNMP (verze 3) a NTP (verze 3).



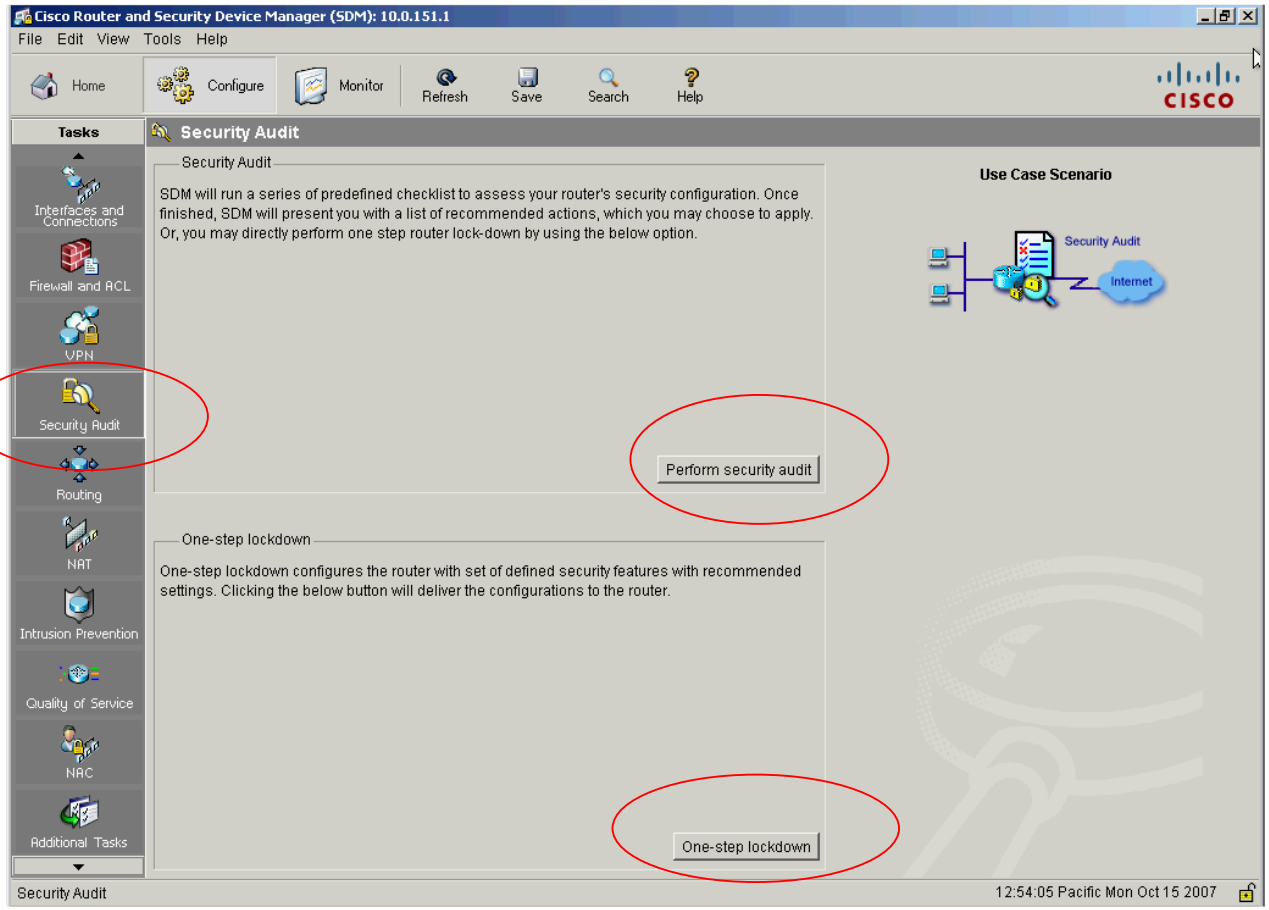
# Další kroky ...

- Implementace filtrace -**standardní a rozšířené ACL u Cisca, Mikrotik - iptables**.
- **Zálohovat** konfigurace/image OS směrovače - zabránit jejich smazání škodlivým uživatelem.
- Pravidelný audit a kontrola nastavení směrovače.
- **Testování a skenování** služeb a nastavení, odolnost vůči pentestům.

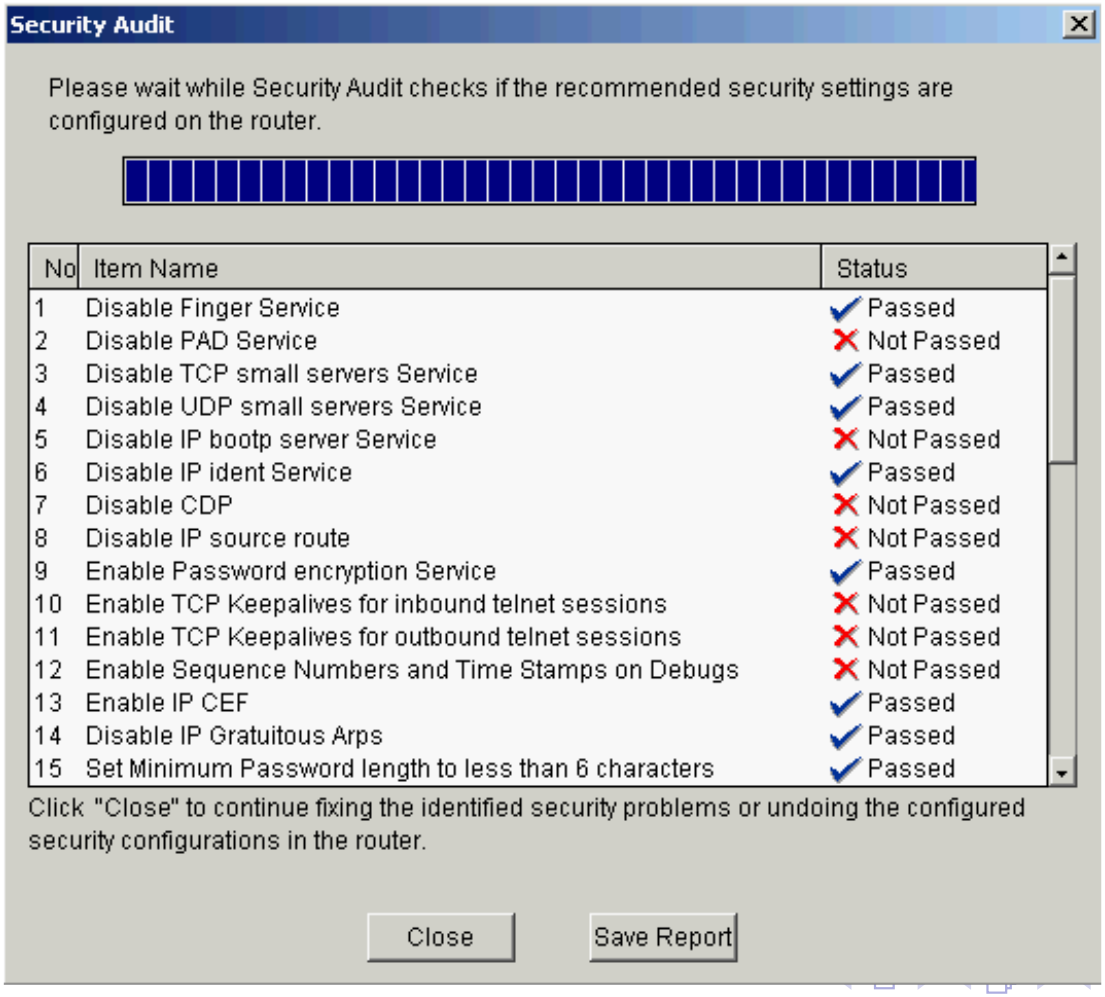
# Bezpečná konfigurace směrovačů Cisco

- Konfigurace zabezpečení pomocí command line rozhraní (CLI) nebo pomocí GUI - SDM Security Device Manager.
- Jednoduché a základní zabezpečení směrovače pomocí automatizovaných procedur: Security Audit Wizard, **AutoSecure** a **One-step Lockdown**.
- Lze nastavit i pomocí jednotlivých příkazů.
- Postup:
  - 1. zabezpečit směrovač (router hardening),
  - 2. zabezpečit směrovačem síť (např. nastavit ACL, konfigurace NAT, konfigurace bezpečného směrování),
  - 3. přidat další bezpečnostní funkce (firewall, VPN, AAA, IPS).
- Cisco Discovery Protocol (CDP) by se měl vypnout u hraničních směrovačů.

# Bezpečná konfigurace směrovačů Cisco v SDM Security Device Manager



# Kontrola zabezpečení směrovače Cisco pomocí Security Audit



# Bezpečná konfigurace směrovačů Cisco - AutoSecure

Procedura CLI **AutoSecure**:

- Od verzí IOS 12.3.
- Nastavení na základní (minimální) úroveň zabezpečení směrovače Cisco.
- Zakáže nepotřebné globální služby (Finger, PAD, BOOTP, IDENT, NTP, ...) a služby na rozhraních, které mohou být zneužity (např. Proxy-arp, ICMP Unreachables).
- V rámci managementu povolí užitečné globální bezpečnostní funkce (např. service password-encryption), logování incidentů a bezpečnostní přístup ke směrovači (banner zprávu, login a heslo).
- Příkaz: `auto secure`

# Bezpečná konfigurace směrovačů Cisco - AutoSecure

Procedura CLI `auto secure` u směrování povoluje nebo se pokusí aktivovat (pokud je služba dostupná na směrovači):

- Cisco Express Forwarding (CEF) - pro lepší zvládnutí DoS SYN-flood útoků.
- TCP přerušení - časové omezení spojení.
- Unicast Reverse Path Forwarding (uRPF) - proti IP spoofingu.
- Context-Based Access Control (CBAC) - v případě služeb firewallu na směrovači.

# Bezpečná konfigurace směrovačů Cisco - One-step Lockdown

Procedura **One-step Lockdown**:

- Konfigurace pomocí GUI u Security Device Manager (SDM).
- Nastavuje se sada definovaných bezpečnostních vlastností a bezpečná konfigurace doporučeného nastavení pomocí jednoho kliknutí.
- Kolem 59 příkazů je odesláno na směrovač.

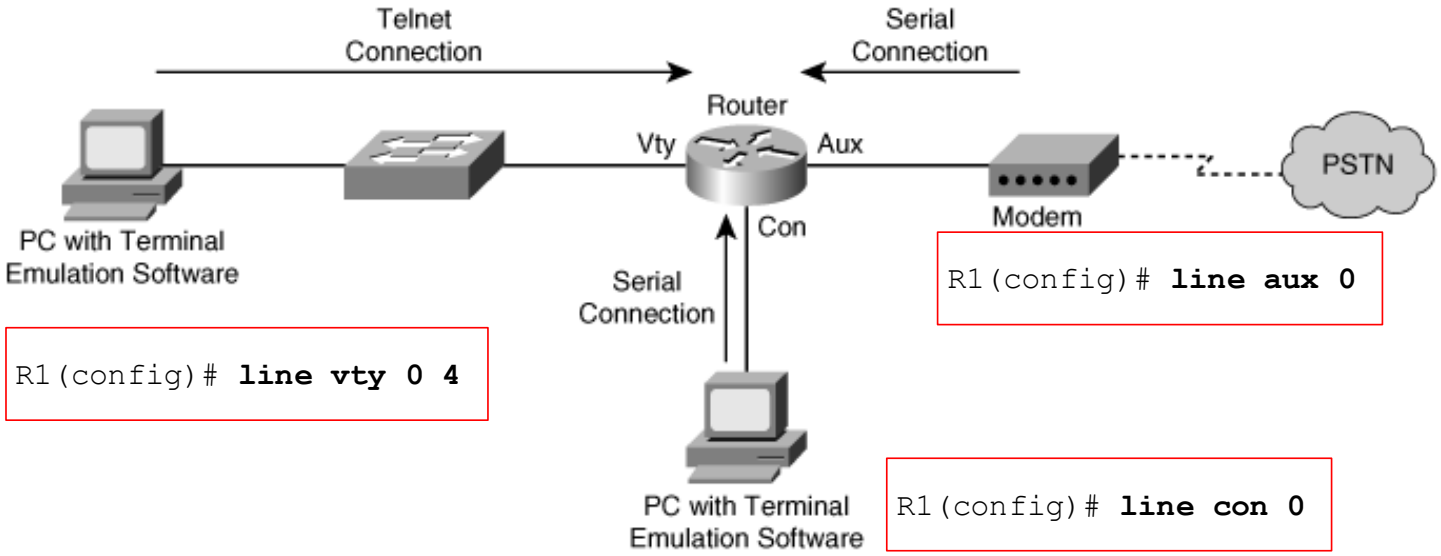
# Rozdíly mezi AutoSecure a One-step Lockdown

AutoSecure narozdíl od One-Step Lockdown:

- Vypne NTP.
- Konfiguruje TCP přerušení.
- Konfiguruje AAA.
- Konfiguruje ACL anti-spoofing na vnějších rozhraních.
- Podporuje konfiguraci SNMPv3.

# Bezpečná konfigurace směrovačů Cisco - přístup

- Lokální přístup (console port).
- Vzdálený přístup (SSH, SNMP, Telnet).




```
R1(config)# line vty 0 4
```

```
R1(config)# line aux 0
```

```
R1(config)# line con 0
```

```
R1(config-line)# password cisco
R1(config-line)# login
```

# Bezpečná konfigurace směrovačů Cisco - přístup

## Implementing Logon Security Enhancements

1. `Router(config)#login block-for <seconds> attempts <attempts> within <seconds>`
2. `Router(config)#login quiet-mode access-class <acl>`
3. `Router(config)#login delay <seconds>`
4. `Router(config)#login on-failure log <every #>`
5. `Router(config)#login on-success log <every #>`
6. `Router(config)#security password min-length <number>`
7. `Router(config-line)#exec-timeout`
8. `Router(config)#service password-encryption`

# Bezpečná konfigurace směrovačů Cisco - AAA

- Metody autentizace - bez autentizace (none), s heslem (line, local), Kerberos 5 (krb5), Radius (`group radius`), Tacacs+ (`group tacacs+`).
- Autorizace a Accounting (trakování, logování a shromažďování dat) - pomocí serveru.
- Např. `Router(config)# aaa authentication login default group radius local`.

# Bezpečná konfigurace směrovačů Cisco - ACL

- Access Control Lists (ACLs) - přístupové kontrolní listy zmírňují síťové útoky a umožňují kontrolovat provoz v síti.
- ACL nastavují parametry jako IPv4/v6, TCP a UDP porty.
- Příkaz:
  `ip access-list [standard | extended]` *name_of_ACL*.
- Např. provoz z podsítě 172.16.5.0 musí být zakázán, zbývající provoz je povolen na rozhraní FE 0/0:

```
R1(config)# access-list 1 deny 172.16.4.0 0.0.0.255
R1(config)# access-list 1 permit any
R1(config)# interface FastEthernet 0/0
R1(config-if)# ip access-group 1 out
```

# Bezpečná konfigurace směrovačů Cisco - ACL

- Zobrazení ACL pomocí příkazu: `show access-lists`
- Inbound provoz - provoz, který přichází do směrovače a je před zpracováním ACL.
- Outbound provoz - provoz, který odchází ze směrovače na správné rozhraní (směrování) po zpracování ACL.
- **Standardní ACL - co nejblíže k cílovému uzlu**. Založeno jen na **zdrojových adresách**.
- **Rozšířené ACL - co nejblíže ke zdroji, který je filtrován**. Umístění daleko od zdroje je neefektivní.

# Bezpečná konfigurace směrovačů Cisco - Mitigace DDoS a spoofingu

- ACL umožňuje mitigaci hrozeb jako je spoofing IP adres, DoS TCP SYN útoků, DoS smurf útoků.
- ACL taky umí filtrovat ICMP zprávy, tracerouty apod.
- Povolit nezbytné služby DNS, SMTP a FTP na vybrané sítě a hosty.

# Bezpečná konfigurace směrovačů Cisco - ACL u IPv6

- IPv6 ACL je podobné jako IPv4 ACL.
- Příkaz: `ipv6 access-list` *access-list-name*
- Aplikováno na rozhraní, kde je `ipv6 traffic-filter` *access-list-name* `in|out`

# Bezpečná konfigurace směrovačů Cisco s firewallem

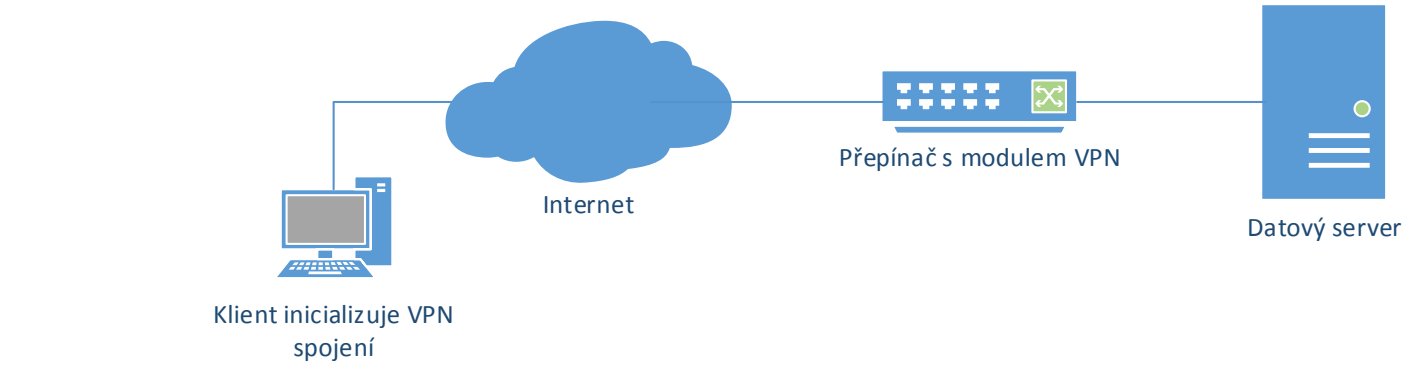
- Hraniční směrovač s modulem Firewall, např. ASR1001-X Cisco Router.
- Best practices: zakázat vše, povolit potřebné.
- Nastavení zón s různou úrovní zabezpečení.
- Firewall wizard.

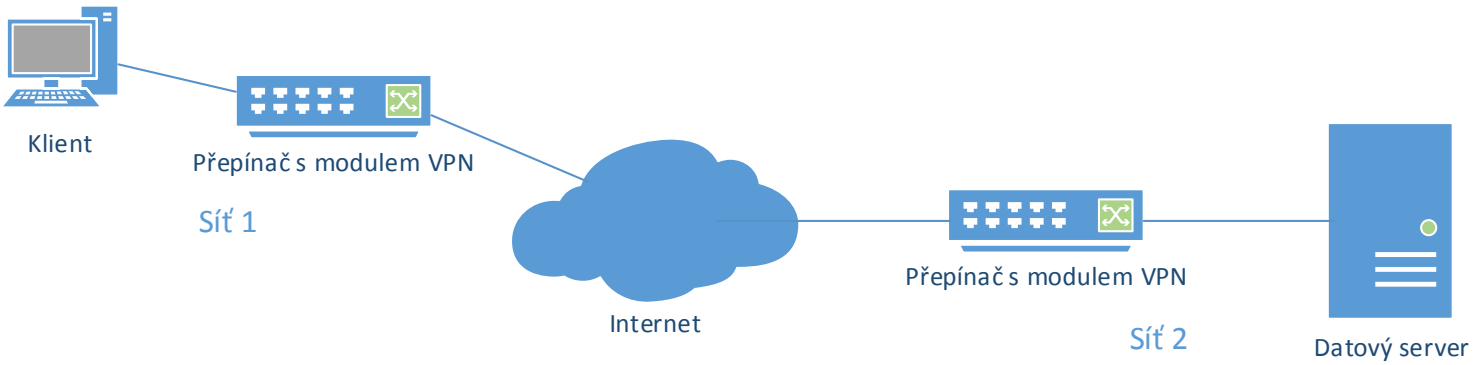
# Bezpečná konfigurace směrovačů Cisco - VPN

- Virtual Private Network (VPN) - soukromá síť vzniklá tunelováním přes veřejnou síť.
- VPN spojení jsou integrovány ve směrovačích Cisco (VPN Advanced Integration Module).
- VPN může být dvojbodové (spojení dvou vzdálených sítí, vzdálené připojení do sítě, atd.).

# Bezpečná konfigurace směrovačů Cisco - typy VPN

- Spojení dvou sítí (Site-to-Site VPN).
- Spojení vzdáleného klienta (Remote-Access VPN).



# Bezpečná konfigurace směrovačů Cisco - VPN metody

- Cisco IOS **SSL** VPN - technologie poskytující spojení přes webový prohlížeč a jeho nativní SSL modul.
- **Generic Routing Encapsulation** (GRE) - zapouzdřuje spojení přes IP, podpora více protokolů (IP, non-IP traffic, směrovací protokoly, multicast), vhodné pro Site-to-Site VPN. **Bez šifrování** (potřeba přidat IPsec).
- Internet Protocol Security (IPsec) - tunelující protokol nad protokolem IP poskytující šifrování dat a autentizaci stran.

# Bezpečnost na Mikrotik směrovačích

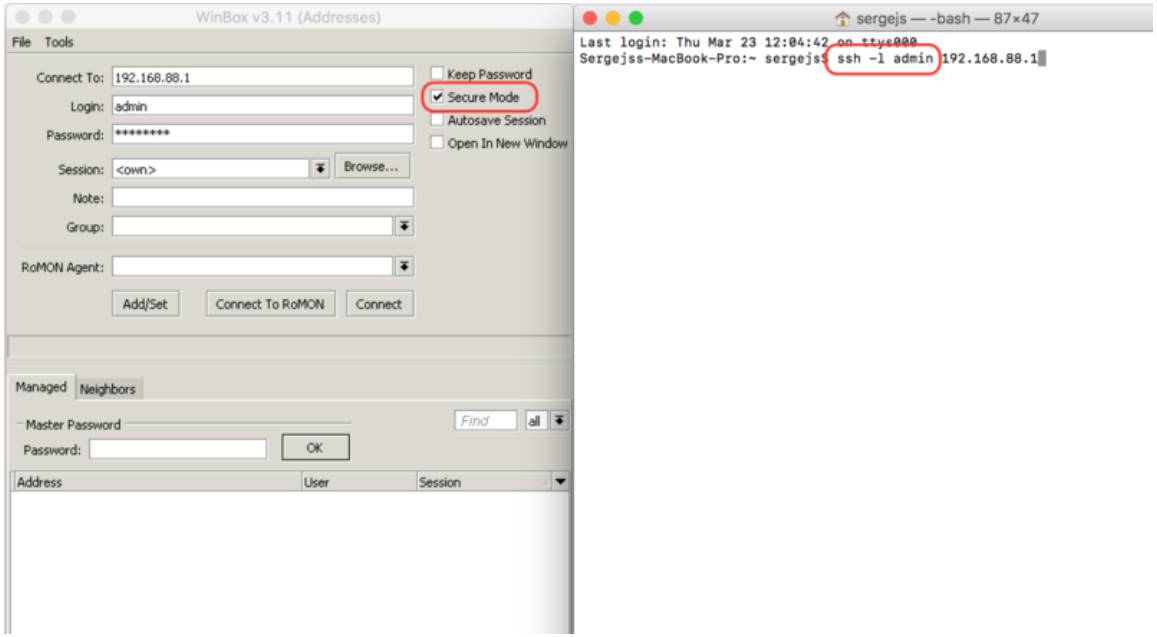

- Mikrotik - 1995, Lotyšsko.
- Mikrotik router - MikroTik RouterOS (Linux).
- MikroTik RouterOS, přístup přes **GUI** - **Winbox**, SSH, Telnet, konzole, Mac-Telnet (přes linkový protokol bez IP adres).
- Mikrotik router funkce - FW, VPN brána (včetně IPSec), routing, Proxy, Bridge, Hotspot, Syslog, TrafficMonitor Server.
- Levné řešení, více viz Mikrotik akademie.

# Bezpečná konfigurace směrovačů MikroTik - Přístup

- Změna username z admin na jiné: `/user set 0 name=MojeNoveJmeno`
- Nastavení hesla: `/user set 0 password=BezpecneHeslo2017`
- Změna username z admin na jiné: `/user set 0 name=MojeNoveJmeno`
- **Omezení přístupu** podle **IP adresy**: `/user set 0 allowed-address=x.x.x.x/yy`

# Bezpečná konfigurace směrovačů MikroTik - Přístup SSH

- SSH: `/ip ssh set strong-crypto=yes`
- Mitigace SSH bruteforce útoku pomocí změny portu SSH (obscurity): `/ip service set ssh port=2200`
- Vymezení IP adres pro službu: `/ip service set winbox allowed-address=192.168.88.0/24`



# Bezpečná konfigurace směrovačů MikroTik - Služby a rozhraní

- Deaktivace všech nepotřebných síťových rozhraní, např. pro 4 a 5 je příkaz: `/interface set 4,5 disabled=yes`
- Kontrolní výpis rozhraní příkazem: `/interface print`
- Deaktivace všech nepotřebných služeb, např: `/ip service disable telnet,ftp,www,api,api-ssl`
- Skrytí před sousedy (Neighbor Discovery Protocol nebo Cisco Discovery Protocol): `/ip neighbor discovery settings set default=no default-for-dynamic=no`
- (pro interface ether1) `/ip neighbor discovery set ether1 discover=no`
- (pro IPv6) `/ipv6 nd set [find] disabled=yes`
- Vypnutí dalších služeb: `/tool bandwidth-server set enabled=no /tool mac-server set [find] disabled=yes /tool mac-server mac-winbox set [find] disabled=yes /tool mac-server ping set enabled=no`

# Bezpečná konfigurace směrovačů MikroTik - Firewall

- Doporučuje se ponechat defaultní nastavení firewallu s mírnými úpravami podle best practice (povolit nezbytný provoz a důvěrné externí IP, zakázat vše ostatní).
- Založeno na **linux iptables**.
- Směr provozu chain (input/output/forward), pravidla/action (accept/reject/drop - tzv. tichý reject).
- Příklad konfigurace: /ip firewall filter
  add action=accept chain=input comment="default configuration" connection-state=established,related
  add action=accept chain=input src-address-list=allowed_to_router
  add action=accept chain=input protocol=icmp
  add action=drop chain=input
  /ip firewall address-list add address=192.168.88.2-192.168.88.254 list=allowed_to_router

# Bezpečná konfigurace směrovačů MikroTik - Další konfigurace

- Zapnutí funkce Reverse Path Filtering (RPF), která zahazuje spoofované pakety (mající odlišnou IP adresu) z vnitřní sítě: `/ip settings set rp-filter=strict`
- Zajištění přesného času pomocí známých NTP serverů: `/system ntp client set enabled=yes server-dns-names=0.pool.ntp.org,1.pool.ntp.org, 2.pool.ntp.org,3.pool.ntp.org`
- Zálohování konfigurace: `export compact file=backup_config_router01`
- Nastavení SNMP protokolu.
- Logování, monitoring a Syslog.
- Blokování P2P provozu.
- Segmentace VLAN a další úprava nastavení FW.

# Děkuji za pozornost!
# Prosím Vaše dotazy/připomínky?

malina@vut.cz

# Reference I


Boyles, Tim.
*CCNA Security Study Guide: Exam 640 - 553*.
John Wiley and Sons, 2010.


MCMILLAN, Troy.
*CCNA Security Study Guide: Exam 210 - 260*.
John Wiley and Sons, 2018.


Cheswick, William R., Steven M. Bellovin a Aviel D. Rubin.
*Firewalls and Internet security: repelling the wily hacker*.
Addison-Wesley Longman Publishing Co., Inc., 2003.