# Zabezpečení aktivních prvků Cisco

Filip Soviš

Bakalářská práce
2017



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Filip Soviš** |
| Osobní číslo: | **A13669** |
| Studijní program: | **B3902 Inženýrská informatika** |
| Studijní obor: | **Informační a řídicí technologie** |
| Forma studia: | **prezenční** |
| Téma práce: | **Zabezpečení aktivních prvků Cisco** |
| Téma anglicky: | **Securing Cisco Active Components** |

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Sestavte přehledný souhrn možností zabezpečení aktivních prvků Cisco.**
3. **Navrhněte běžné zabezpečení Cisco SW směrovače.**
4. **Navrhněte běžné zabezpečení Cisco L2 a L3 přepínače.**
5. **Navržené zabezpečení ověřte na Cisco Packet Traceru.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:


1. **ODOM, Wendell. a Rick. MCDONALD. Routers and routing basics: CCNA 2 companion guide. Vyd. 2. Indianapolis: Cisco Press, 2007. ISBN 978-1-58713-166-0.**
2. **EMPSON, Scott. CCNA kompletní přehled příkazů: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2009. ISBN 978-80-251-2286-0.**
3. **ODOM, Wendell, Rus HEALY a Naren MEHTA. Směrování a přepínání sítí: autorizovaný výukový průvodce. Vyd. 3. Brno: Computer Press, 2009. ISBN 978-80-251-2520-5.**
4. **KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Vyd. 1. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.**
5. **LAMMLE, Todd. CCNA: výukový průvodce. Vyd. 1. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.**


Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **24. února 2017**

Termín odevzdání bakalářské práce: **24. května 2017**

Ve Zlíně dne 24. února 2017

doc. Mgr. Milan Adámek, Ph.D.
*děkan*

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
*ředitel ústavu*

**Filip, Soviš:**

**Zabezpečení aktivních prvků Cisco**

**Prohlašuji, že**

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spolu autor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 20.5.2017

.....
podpis diplomanta

## ABSTRAKT

Cílem práce bylo sepsat, navrhnout a vyzkoušet zabezpečení aktivních zařízení firmy Cisco. Zabezpečení se týká 2 a 3 vrstvy OSI/ISO a je zaměřeno na přepínače a směrovače. Záměrně nebyly využity hardwarové bezpečnostní prvky. První část práce rozebírá možnosti zabezpečení a také běžné typy síťových útoků. V následující části je demonstrativní návrh sítě, který slouží pro představu rozložení firemní sítě. Je zde předvedena konfigurace VLAN, přístupových listů ACL, technologie AAA, dynamické ARP inspekce a bezpečnostní funkce jako Port Security. Konfigurace je provedena v programu Cisco Packet Tracer.



Klíčová slova: ACL, AAA, DAI, síťové útoky, zabezpečení sítě.



## ABSTRACT

The aim of this work was to write, design and proof security active devices of the company Cisco. It deals with the securing of the second and third layer OSI/ISO and it was aimed to switches and routers. This paper deliberately doesnt use hardwares securing elements. In the first part of this work are security options and most common network attacks analyzed. In the next part is designed a network, which provides demonstrative picture of company network layout. Furthermore, there are demonstrated configurations VLAN, access list ACL, technology AAA, dynamic ARP inspection and securing function like Port Security. The configuration is demonstrated in the programme named Cisco Packet Tracer.



Keywords: ACL, AAA, DAI, network attacks, securing network.

Rád bych na tomto místě poděkoval vedoucímu práce Ing. Miroslavu Matýskovi, PhD., za vedení, připomínky, rady a trpělivost, kterou mi věnoval.

# OBSAH

# ÚVOD

V dnešní době jsou počítačové sítě neodmyslitelnou součástí života a to jak běžného, tak i firemního. Kvůli jejímu neustálému rozšiřování a využívání se počítačová síť stává pro mnoho lidí bezpečnostním rizikem, obzvláště pro firmy. Počítačové sítě nejsou už jen pouhou infrastrukturou. Stává se z nich spolehlivá platforma poskytování služeb 21. století. Rostoucí množství těchto služeb a úloh prováděných on-line, mezi které patří i telefonování, způsobuje prudký nárůst počtu zařízení připojených k síti. V roce 2013 bylo připojeno k internetu až 1 bilion zařízení. Tím se taky zvyšuje množství útoků a škůdců ve všech formách.

Tyto útoky se provádí z různých důvodů. Na firmy směřující útok má většinou nějakým způsobem uškodit firmě, ať už vyřadit z provozu, nebo prolomit zabezpečení a dostat se k citlivým datům. Další útoky můžou být prováděny jen pro pocit, že útočník někomu uškodil. Důvodů a způsobů je mnoho, a proto se tato práce zabývá zabezpečením sítí se specializací na přepínače a směrovače od firmy Cisco. Firma tak nemusí investovat velké peníze do infrastruktury a stále bude mít kvalitní zabezpečení. Zabezpečení bylo otestováno v simulačním programu Cisco Packet Tracer.

# I. TEORETICKÁ ČÁST

# 1 PROFIL SPOLEČNOSTI CISCO

Společnost Cisco je největším světovým poskytovatelem síťových řešení, která mění způsob, jakým se komunikuje, připojuje a spolupracuje mezi sebou. Cisco nabízí řešení pro firemní komunikaci velkých i malých podniků, zařízení a aplikace pro multimédia, datové sklady, směrovače, přepínače, servery a řadu dalších. Nabízí široké spektrum technologií v oblasti přenosu dat, hlasu a obrazu a v oblasti pevných a bezdrátových sítích. Do portfolia společnosti Cisco patří i nástroje pro efektivní týmovou spolupráci a jednání na dálku, jako je TelePresence nebo WebEx.

V České republice působí organizace Cisco již od roku 1995. Společnost Cisco vnímá Českou republiku jako jeden z klíčových trhů nejen v regionu střední a východní Evropy, ale i mezi všemi světovými trhy. Cílem společnosti na našem trhu je pomáhat velkým i malým organizacím a středním firmám dosáhnout větší efektivity a lepších obchodních výsledků s využitím moderních technologií. Dále se společnost zaměřuje na podporu těch, kteří mohou prostřednictvím technologií zvýšit kvalitu svého života.

Například pro Sdružení Linka bezpečí pomohlo Cisco vybudovat nové call centrum založené na IP telefonii, které tak snížilo náklady na provoz a omezilo i možnost opakovaného zneužití linky. Cisco pomáhá v České republice řešit situaci v oblasti vzdělávání ICT specialistů. Například díky stipendijnímu programu CCIE Inkubátor pro studenty vysokých škol nebo projektu Cisco Networking Academy Program, jehož cílem je vzdělávat a vychovávat nové české odborníky v oblasti síťových technologií [1].

Společnost Cisco byla založena v roce 1984 počítačovými vědci Lenen Bosackem a Sandym Lernerem z univerzity v kalifornském Stanfordu. Od počátků hráli technici a inženýři společnosti vedoucí úlohu ve vývoji síťových technologií založených na protokolu IP. Společnost dnes na celém světě zaměstnává okolo 74 tisíc lidí a za poslední fiskální rok dosáhla tržeb ve výši 49 miliard dolarů, což představuje 4 % nárůst oproti minulému roku. Ročně vydá společnost Cisco cca 5 miliard dolarů na výzkum a vývoj, čímž se řadí na špičku mezi ostatními společnostmi [2].

# 2 ZÁKLADNÍ ZABEZPEČENÍ

## 2.1 Rozhraní příkazového řádku

Uživatelský režim slouží především k zobrazení statistik. Lze v něm používat příkazy ***ping***, ***show, traceroute***. Zabezpečení uživatelského režimu lze nastavit v privilegovaném režimu, do kterého se dostaneme pomocí příkazu ***enable***. Zde vstoupíme do konfiguračního módu příkazem ***configure terminal*** a nastavíme heslo pro přístup k uživatelskému režimu následovně. ***Line console 0*** k možnosti nastavení konzole, ***password <heslo>*** pro zadání hesla a ***login***, aby bylo heslo vynucené při spuštění rozhraní příkazového řádku. Problém spočívá v tom, že příkaz ***password*** heslo nezašifruje a je tedy uloženo tak, jak ho napíšeme, a proto využijeme příkaz ***service password-encryption***, který heslo zašifruje. V okamžiku zadání tohoto příkazu, se ihned zašifrují veškerá hesla, která jsou ve formátu běžně psaného textu. Šifrování se změní, ale na to aby se projevilo ve spouštěcí konfiguraci, se musí uložit konfigurace pomocí ***copy running-config startup-config***. Po zadání příkazu na vypnutí šifrování ***no service password-encryption*** se hesla automaticky nedešifrují, ale jsou uložena zašifrovaná, dokud heslo není změněno. Nové heslo pak bude bez šifrování. Toto šifrování však není nejsilnější a postačí pouze proti běžným uživatelům, kteří nemají mít přístup do příkazového řádku.

Privilegovaný režim, který slouží ke konfiguraci zařízení, musí být chráněn proti útokům. Lze ho zabezpečit podobně jako uživatelský režim. Použije se příkaz ***enable password <heslo>,*** kde je heslo opět nezabezpečené a ukládá se jako běžně psaný text. Pro zašifrování bude použit příkaz ***service password-encryption***. Toto heslo je velmi slabé, a proto se využije místo příkazu ***enable password <heslo>*** příkaz ***enable secret <heslo>***. Pokud jsou zadány oba příkazy, použije se automaticky příkaz ***enable secret <heslo>***. Zmíněný příkaz není pro běžné šifrování, ale heslo se ukládá jako hodnota haše MD5, která je na prolomení velmi obtížná. ***Service password-encryption*** na tento příkaz nemá žádný vliv. Dále může být použit příkaz ***username <jmeno> password <heslo>*** ke kterému je potřebný příkaz ***service password-encryption*** pro zašifrování. Příkaz ***username <jmeno> secret <heslo>*** využívá na heslo haše MD5 a zvyšuje tak zabezpečení.

Dále je vhodné zabezpečit vzdálený přístup přes virtuální terminál „protokol Telnet“. Jakmile je nastavena IP (Internet Protocol) adresa zařízení, můžeme se připojit pomocí

Telnetu. Zadáním příkazu ***line vty 0 2*** budou nakonfigurována Telnetová spojení s ID 0-2. Nastaví se heslo pomocí příkazu ***password <heslo>*** a ***login*** pro vyžadování hesla. Dále bude omezen přístup pro ostatní ID příkazy ***line vty 3 15*** a ***transport input none***. Aby zde bylo heslo šifrované, musí se využít příkazu ***service password-encryption***. Telnet se dá bohužel lehce odposlouchávat. Z tohoto důvodu není příliš vhodný pro použití, a proto se nabízí protokol SSH (Secure shell). Pro nastavení bezpečnosti protokolu SSH se musí provést série příkazů, počínaje nastavením názvu zařízení ***hostname <jmeno>***, nastavení doménového názvu ***ip domain-name <jmeno>*** dále jméno a heslo pro přihlášení ***username <jmeno> password <heslo>***. Nyní se přihlašovací údaje zašifrují příkazem ***crypto key generate rsa*** *a* povolením protokolu SSH v zařízení ***ip ssh version 2***. Protokol je nastaven a k zabezpečení virtuálního terminálu protokolem SSH postačí příkaz ***transport input ssh*** [3].

## 2.2 Autentizace, Autorizace a účtování

Autentizace, autorizace, účtování (AAA) je okruh společných bezpečnostních funkcí, které pro lepší pochopení lze vysvětlit na jednoduchém příkladu vchodových dveří.

Autentizace – je opatření, které zajistí, že osoba, která se pokouší o přístup ke dveřím, je skutečně ta osoba, kterou tvrdí, že je. Proto by byl nejjednodušším mechanismem ověření snímač otisků prstů, jelikož otisky prstů jsou jedinečné. V tomto zařízení se však běžně využívá ověřování heslem, protože pouze jeden člověk by měl znát své heslo. Zadáním správného hesla by mělo být prokázáno, že jsi ten, o kterém tvrdíš, že jsi.

Autorizace – je další krok v procesu. Zahrnuje kontrolu, zda máte k těmto dveřím přístup. Jste sice ověřen, ale máte přístup pouze k určitým dveřím. Například ve firmě je vedoucí a zaměstnanec. Zaměstnanec se může k přístroji připojit, ale nemůže měnit konfiguraci, nebo má přístup jen k omezeným příkazům, kdežto vedoucí může měnit úplně vše.

Účtování – je samostatný krok. Slouží ke zjištění, kdo se pokouší o přístup ke dveřím a jestli byl, nebo nebyl úspěšný. Zařízení tímto může zaznamenat každého uživatele, který se pokouší o připojení, stejně tak může zaznamenávat každý příkaz, který uživatel spouští. Toto je důležité k určení možných bezpečnostních hrozeb a pomoci při narušení bezpečnosti.

Technologie AAA je implementována pomocí serverů RADIUS (Remote Authentication Dial In User Service) a TACACS+ (Terminal Access Controller Access-Control System). Tato technologie se využívá k připojení pomocí TELNETu či SSH [4].

### 2.2.1 Autentizační server TACACS+

Systém řízení přístupu k ovladači terminálového přístupu (TACACS+) je sada protokolů vytvořena a určená pro řízení přístupu k terminálům. Společnost Cisco vytvořila protokol TACACS+, který byl vydán jako ověřený standard. TACACS+ se využívá hlavně pro administraci zařízení AAA a je možné jej využít pro síťový přístup AAA.

TACACS+ používá protokol TCP (Transmission Control Protocol) s portem 49 pro komunikaci mezi klientem TACACS+ a serverem TACACS+. Jedním z klíčových rozdílů mezi serverem RADIUS a TACACS+ je schopnost serveru TACACS+ oddělit autentizaci, autorizaci a účtování jako nezávislé funkce. Proto je TACACS+ běžně využíván pro správu zařízení, i když RADIUS je stále schopen poskytovat správu zařízení AAA.

Správa serveru může být velmi interaktivní. Je nutné provést jednorázově autentizaci, ale autorizace musí být provedena vícekrát během jedné relace v příkazovém řádku. Služba TACACS+ je navržena pro správu zařízení AAA, aby ověřovala a autorizovala uživatele terminálů nebo konzol. TACACS+ používá pro komunikaci mezi klientem a serverem různé typy zpráv v závislosti na funkci. TACACS+ komunikace šifruje celý paket [5].

### 2.2.2 Autentizační server RADIUS

Dálkově přístupná vytáčecí uživatelská služba (RADIUS) je standardem IETF (Internet Engineering Task Force) pro AAA. Stejně jako u TACACS+ jde o model klient/server, kde klient iniciuje požadavek na server. RADIUS je protokol volby pro síťový přístup k AAA. Pokud se pravidelně připojujete k zabezpečené bezdrátové síti, s největší pravděpodobností je zde použit RADIUS mezi bezdrátovým zařízením a serverem AAA. RADIUS je totiž transportní protokol pro EAP (Extensible authentication protocol) protokol spolu s mnoha dalšími ověřovacími protokoly.

Původně byl RADIUS určen k rozšíření autentizace protokolů PPP (Point to Point Protocol) druhé vrstvy používaných mezi koncovým uživatelem a serverem pro síťový přístup NAS (Network Access Server) a přenášení této ověřovací komunikace z NAS na

server AAA. To umožnilo rozšířit ověřovací protokol druhé vrstvy v rámci hranic třetí vrstvy na centralizovaný ověřovací server. Dnes je stále používán stejným způsobem tak, aby nesl přenos autentizace ze síťového zařízení na autentizační server. S protokolem IEEE (Institute of Electrical and Electronics Engineers) 802.1X se RADIUS používá k rozšíření protokolu EAP od koncového uživatele na ověřovací server. Když je žádost o ověření odeslána na server AAA, klient AAA očekává, že výsledek autorizace bude vrácen zpět [5].

Výměna mezi klientem a serverem je ověřována pomocí sdíleného tajemství, které se nikdy neposílá přes internet. Všechny uživatelské hesla se posílají zašifrované mezi klientem a RADIUS serverem. To eliminuje možnost, odposloucháváním na nezabezpečené síti zjistit heslo uživatele. Ovšem ostatní informace, jako je uživatelské jméno, můžou být zachyceny, což patří mezi nevýhody tohoto protokolu. Další nevýhodou RADIUSu je neumožnění určit, které příkazy jsou či nejsou na zařízení povoleny, a proto není vhodný pro správu síťových zařízení nebo pro terminálové služby [6].

## 2.3 PPP

Při zabezpečení protokolu PPP může být využito protokolů PAP (Password Authentication Protocol) a CHAP (Challenge Handshake Authentication Protocol), které se využívají především u vytáčených aplikací. Podle výchozí autentizační metody se protokoly PAP a CHAP opírají o lokálně zadanou množinu příkazů ***username <jmeno> password <heslo>***.

Podpora autentizace AAA v protokolu PPP je stejná v obecných příkazech jako u přihlašovací autentizace. Tuto konfiguraci lze provést následovně. Nejprve se zapne autentizace AAA stejně jako u přihlašovací autentizace a to příkazem ***aaa new-model***. Servery RADIUS nebo TACACS+ jsou zadány stejným způsobem jako v předchozí kapitole, stejným postupem a stejnými příkazy jako u autentizace pro běžné přihlášení a oprávněný režim. Podobně bude stanoveno, že protokol PPP bude používat výchozí množinu autentizačních metod, a to příkazem ***aaa authentication ppp default***. Mohou být také vytvořeny pojmenované skupiny metod, ty je pak možné používat namísto výchozí množiny, a to k přihlašovací autentizaci příkazem ***aaa authentication ppp <název-seznamu metoda1>***. Pro skupinu autentizačních metod může být namísto výchozí množiny použit příkaz ***ppp authentiction <protokol1 protokol2> název-seznamu***. Například zápis

***ppp authentication chap fred*** odkazuje na autentizační metody v příkazu ***aaa authentication ppp fred*** [3].

# 3 ZABEZPEČENÍ VRSTVY 2

## 3.1 Zabezpečení nevyužitých uživatelských portů

Zabezpečení nevyužitých a uživatelských portů se ve většině případů zakládá na doporučení přímo od firmy Cisco. Tato doporučení jsou závislá na jednom ze tří obecně charakterizovaných typů portů. Jsou to nevyužité porty, uživatelské porty a důvěryhodné porty nebo trunkové porty. Nevyužité porty jsou porty přepínače, které nejsou dosud připojeny k žádnému zařízení. Jedním z nich jsou například porty připojené k zásuvce v prázdné kanceláři. Uživatelské porty jsou připojené k zařízením koncových uživatelů, nebo vedené do jakéhokoliv fyzicky nechráněného prostoru. Důvěryhodné nebo trunkové porty jsou připojeny k plně důvěryhodným zařízením, jako jsou další přepínače, umístěné v prostorách s dobrým fyzickým zabezpečením.

Následující výčet shrnuje přehled doporučených postupů pro nevyužité a uživatelské porty, ke kterým je snadné se připojit. Jelikož stačí zlomyslné osobě dostat se dovnitř budovy a nepotřebuje ani další přístup do rozvodné skříně nebo datového centra.

- Vypnout nepotřebné dynamické protokoly jako jsou CDP (Cisco Discovery Protocol) a DTP (Dynamic Trunking Protocol).
- Vypnout trunking a prohlásit tyto porty za přístupové.
- Zapnout ochranné mechanismy BPDU (Bridge Protocol Data Units) Guard a Root Guard, které brání v útocích na protokol STP (Spanning-Tree Protocol) a posilují stabilitu kostry sítě STP.
- Využití funkce DAI (Dynamic ARP Inspection) nebo privátní sítě VLAN (Virtual Local Area Network) pro ochranu před odposlechem.
- Zapnout zabezpečení portů a omezení připojení na konkrétní adresy MAC (Media Access Control).
- Zapnout autentizaci uživatelů 802.1X.
- Pro obranu před útoky (DoS a man in the middle), zapnout mechanismy odposlouchávání DHCP(odposlouchávání) a IP Source Guard.
- Zapnout globálně autentizaci VTP (VLAN Trunking Protocol).
- Vypnout a přesunout nepoužité porty přepínačů do nevyužité sítě VLAN.
- Nepoužívat VLAN 1.

- U trunků nepoužívat nativní VLAN.

Vypnutí protokolů CDP a DTP se provede použitím příkazů ***cdp run*** pro globální zapnutí (některé porty ho můžou potřebovat). Poté bude zvolen port ***int fa0/1*** a vypne se na tomto portu protokol CDP příkazem ***no cdp enable***. Díky příkazům ***switchport mode access*** *a* ***switchport nonegotiate*** *se* zabrání trunkingu nad portem a bude zakázáno odesílání a zpracování jakýchkoliv zpráv DTP. Další příkazy zapínají nad portem mechanismy Root Guard neboli BPDU Guard. Jsou to příkazy ***spanning-tree guard root*** a ***spanning-tree bpduguard enable***.

Při zabezpečení portů přepínače bude omezen okruh MAC adres spojených s tímto portem v přepínací tabulce druhé vrstvy. Nejlepším řešením je zavedení přísnějšího opatření, které umožnuje dosáhnout přes port jen konkrétní adresy MAC. Pro implementaci zabezpečení portů musí přepínač rozšířit svou normální logiku zkoumání příchozích rámců. Místo automatického přidání položky z přepínací tabulky druhé vrstvy přepínač zkontroluje konfiguraci zabezpečení portu a zjistí, je-li tato položka povolena. Zabrání li se takto v přidávání MAC adres do přepínací tabulky, může být díky zabezpečení portu zabráněno i v rozesílání rámců do těchto MAC adres.

Pomocí zabezpečení portů se může předejít některým útokům, jelikož bude omezen počet povolených MAC adres a i konkrétní MAC adresy pro dané porty. Konfigurace zabezpečení portu není složitá. Nezbytné jsou dva příkazy ***switchport mode <access | trunk>*** statické nastavení portu jako přístupový nebo trunking a ***switchport port-security maximum<cislo>*** pro zapnutí zabezpečení portu nad daným rozhraním a volitelné definování počtu MAC adres na portu s výchozí hodnotou 1. Po zadání těchto příkazů bude port používat první zjištěnou adresu, ale už žádnou jinou. Jakmile je adresa odstraněna z paměti CAM (Content Addressable Memory) jako nejstarší, je možné zjistit novou adresu pro tento port, v daném okamžiku ale může platit pouze jedna MAC adresa.

Následující příkazy umožňují definici MAC adres. První z nich je ***switchport port-security mac-address <adresa-mac> vlan <id-vlan|access|voice>*** pro statickou definici povolené MAC adresy pro konkrétní síť VLAN, a to pro běžný přístup nebo hlasovou VLAN. Druhý příkaz nařizuje přepínači si pevně zapamatovat dynamicky zjištěné MAC adresy příkazem ***switchport port-security mac-address sticky***. Poslední příkaz pro toto zabezpečení portů

***switchport port-security aging violation <protect|restrict|shutdown>*** definuje časovač „stárnutí“ Aging a operace prováděné při narušení pravidel pro zabezpečení portů [3].

## 3.2 ARP

Pomocí mechanismu DAI neboli Dynamické inspekce protokolu ARP (Address Resolution Protocol), může přepínač zabránit určitým typům útoků, které zneužívají zprávy protokolu IP ARP. Pro představu jak útok probíhá, je nutné blíže definovat ARP zprávu. Když jeden počítač zjišťuje adresu MAC druhého počítače, tak samotná zpráva ARP neobsahuje IP hlavičku. Obsahuje však čtyři adresové pole, které jsou velmi důležité, a to zdrojovou MAC adresu a zdrojovou adresu IP odesílatele zprávy a MAC adresu s adresou IP hledaného cíle. Políčko pro MAC adresu hledaného cíle je však prázdné. V požadavku ARP je tak uvedena jen IP adresa a k ní je zapotřebí zjistit MAC adresu cíle. V odpovědi ARP se hodnota adresy MAC odvozuje z pole zdrojové adresy MAC. Například cílový počítač zapisuje do zdrojových adres své adresy. To znamená, že když se zpráva dostane do cílového počítače, tak cílový počítač zapíše do zprávy ARP své adresy MAC i IP do zdrojových polí a do cílových polí zapíše adresy prvního počítače, ze kterého zpráva přišla.

Útočník je schopen vyvolat útok „men in middle“ s mužem uprostřed. Takový útok je možné vyvolat pomocí bezdůvodné zprávy ARP. To znamená, že hostitel sám odešle ARP odpověď bez jakéhokoliv požadavku ARP, jejíž cílovou adresou je všesměrová MAC adresa. Odpověď ARP je jednosměrná, a tak se příslušnou ARP položku dozví jen hostitel, který odeslal požadavek. Při odeslání bezdůvodné ARP zprávy se ale ARP položku dozvědí všichni hostitelé v síti. Bezdůvodnou ARP zprávu lze využít i k dobrým účelům, stejně tak ji ale může zneužít i útočník. Stačí, aby útočník odeslal bezdůvodnou ARP zprávu, ve které uvede IP adresu právoplatného hostitele. Následně si všichni hostitelé v dané podsíti (včetně směrovačů a přepínačů) aktualizují své tabulky ARP a do nich si zapíší odkaz na MAC adresu útočníka. Namísto správného hostitele pak budou zasílat rámce útočníkovi.

Příklad - Útočník odešle všesměrově bezdůvodnou zprávu ARP, kde zdrojovou adresou IP je IP adresa druhého počítače, ale zdrojová MAC adresa je útočníka. První počítač si tak na základě zprávy ARP aktualizuje tabulku ARP a přiřadí k IP adrese druhého počítače MAC

adresu útočníka. Poté první počítač odešle rámec na adresu IP druhého počítače, kterou ale převede na MAC adresu útočníka. Přepínač tak odešle rámec na MAC adresu útočníka.

Jakmile je útok úspěšně proveden, budou ostatní hostitelé posílat rámce určené druhému počítači na adresu útočníka. Ten poté odešle kopii každého rámce druhému počítači tedy již správnému příjemci. Stává se tak mužem uprostřed a uživatel si toho ani nemusí všimnout, zatímco útočník se dostává k velkému množství dat. Proti útokům na protokol ARP se přepínače brání mechanismem DAI, který prověřuje přijaté ARP zprávy a nepřípustné filtruje. DAI považuje každý port za nedůvěryhodný nebo za důvěryhodný. Filtrování DAI pak probíhá jen nad nedůvěryhodnými porty. Důvěryhodné porty se musí nastavit. Při své činnosti filtruje každý požadavek a odpověď ARP a rozhodne, zda je přípustný či nikoliv. Přípustnost ARP zpráv pak DAI stanovuje podle této logiky:

1. „Pokud je v odpovědi ARP uvedena zdrojová IP adresa, která nebyla protokolem DHCP přiřazena k zařízení připojenému na tomto portu, DAI ji odfiltruje.
2. Dále spustí DAI podobnou logiku jako v kroku 1, ale provádí porovnání se seznamem staticky definovaných kombinací adres IP a MAC.
3. U přijaté odpovědi ARP porovnává DAI zdrojovou adresu MAC v ethernetové hlavičce se zdrojovou adresou MAC ve vlastní zprávě ARP. Tyto adresy MAC se v normální odpovědi ARP musí shodovat. Při neshodě DAI zprávu odfiltruje.
4. Podobně jako v kroku 3 provede DAI porovnání cílové ethernetové adresy MAC a adresy cíle MAC v těle zprávy ARP.
5. Nakonec DAI kontroluje ve zprávě ARP neočekávané IP adresy jako je 0.0.0.0, 255.255.255.255.“ [3]

Příkazy sloužící pro zapnutí mechanismu DAI, jsou uvedeny níže. DAI je přitom nutné zapnout nejprve globálně. Po zapnutí jsou všechny porty považovány za nedůvěryhodné, musí se proto nakonfigurovat některé porty za důvěryhodné. Jsou to zejména porty připojené k zařízením v bezpečných oblastech. Poté se zapnou za pomoci konfiguračních příkazů různé logické varianty. Například odposlouchávání DHCP, které poslouží k využití vazební databáze. Další možnost je konfigurace statických IP adres a provádění kontrol neboli validace.

Globální příkaz ***ip arp inspection vlan <interval-vlan>***, který zapíná pro zadané sítě VLAN mechanismus DAI. ***Ip arp inspection trust*** je dílčí příkaz, který zapíná a vypíná

inspekci DAI nad rozhraním. Při zápisu ***ip arp inspection*** je příkaz ve výchozím stavu zapnutý. Další globální příkaz ***ip arp inspection filter <název-arp-acl> vlan <interval-vlan>*** definuje statické adresy IP/MAC, kontrolované inspekcí DAI pro danou VLAN. Pro zapnutí doplňkové kontroly ARP zpráv, podle kroků 3-5 viz výše, je příkaz ***ip arp inspection validace <src-mac dst-mac ip>***. Jelikož inspekční mechanismus DAI znamená pro zařízení větší výpočetní zátěž, může se útočník pokusit o útok s odepřením služeb proti zařízení, kdy odešle velké množství ARP zpráv. Proti tomuto riziku DAI automaticky nastavuje limit ARP zpráv na 15 za sekundu na jednom portu. Pokud je nutné nastavení změnit, je to možné pomocí příkazu ***ip arp inspection limit rate <pps> burst interval <sekund>*** [3].

## 3.3 DHCP

Odposlouchávání DHCP (Dynamic Host Configuration Protocol snooping) je mechanismus, který zabraňuje poškození vznikajícímu při útocích proti protokolu DHCP. Tento mechanismus vytváří tabulku mapování IP adres a portů. Sestavuje ji z platných zpráv DHCP a nazývá se vazební tabulka odposlouchávání DHCP. Využívají ji mechanismy DAI a IP Source Guard.

Jako příklad poslouží útok s mužem uprostřed, při kterém je zneužit protokol DHCP. DHCP server je umístěn v hlavní síti a útočník je připojen k místní síti, kde se stává falešným serverem DHCP. Jakmile si počítač vyžádá přidělení IP adresy protokolem DHCP, odpoví mu na tuto zprávu útočník. Přiřadí mu tak správnou IP adresu a masku, ale jako výchozí bránu mu přidělí vlastní IP adresu. Proto rámce určené pro bránu z počítače jdou k útočníkovi a až útočník odesílá kopie této zprávy na bránu.

Takovéto útoky může mechanismus odposlouchávání DHCP odrazit, pokud porty považuje za nedůvěryhodné. Průchod všech zpráv povoluje jen u důvěryhodných portů, ale z nedůvěryhodných portů zprávy filtruje. K nedůvěryhodným portům by měli být připojeni jen klienti DHCP, tudíž příchozí zprávy DHCP, které mají pocházet jen od serverů, zde přepínač filtruje. Je proto vhodné nevyužité porty konfigurovat pro odposlouchávání DHCP jako nedůvěryhodné. Jiné útoky mohou být vedeny prostřednictvím klientské zprávy DHCP z nedůvěryhodných portů. Identifikace klientů probíhá pomocí klientské hardwarové adresy, uvedené v požadavku DHCP. Jediné zařízení může odeslat několik

opakovaných požadavků DHCP a do každého zapsat jinou klientskou MAC adresu, díky tomu se na venek může tvářit jako několik různých zařízení. Právoplatný server DHCP se domnívá, že je každé zařízení jiné a každému přiřadí jinou IP adresu. Nakonec se tak vypotřebují všechny IP adresy a na uživatele žádná nezůstane.

Filtrování nedůvěryhodných portů odposlouchávaním DHCP :

1. „Filtruje veškeré zprávy, které mají normálně pocházet výhradně od serverů DHCP.
2. Zprávy DHCP o uvolnění a odmítnutí (relase a decline) kontroluje přepínač vůči vazební tabulce odposlouchávaním DHCP, jestliže IP adresa v těchto zprávách není v tabulce uvedena u příslušného portu, odfiltruje ji.
3. Volitelně porovnává také klientskou hardwarovou adresu v požadavku DHCP se zdrojovou adresou MAC zapsanou v ethernetovém rámci.“

První bod je odpověď na muže uprostřed s falešným serverem DHCP. Druhé opatření slouží k tomu, aby útočník nemohl hostiteli uvolnit zápůjčku DHCP a poté si okamžitě vyžádat a přidělit stejnou IP adresu. Poslední opatření zabraňuje útoku (DoS - Denial of Service), kdy se útočník pokusí alokovat veškeré IP adresy, které by měl server DHCP jinak pro celou síť.

K nastavení směrovače slouží následující příkazy. ***Ip dhcp snooping vlan <interval-vlan>*** je globální příkaz pro zapnutí DHCP odposlouchávání pro interval sítí VLAN. Příkaz rozhraní ***ip dhcp snooping trust*** zapíná nebo vypíná důvěryhodný režim rozhraní. Příkaz pro přidávání statických položek do vazební databáze je ***ip dhcp snooping binding <mac-adresa> vlan <id-vlan ip-adresa> interface <id-rozhraní> expiry <sekund>***. Přidání volitelné kontroly zdrojové adresy MAC, která má být shodná s ID požadavku DHCP, zajišťuje ***ip dhcp snooping verify mac-address***. A ***ip dhcp snooping limit rate <rychlost>*** definuje maximální počet DHCP zpráv za minutu [3].

### 3.3.1 IP Source Guard

Ip Source Guard je kontrolou navíc k logice odposlouchávání DHCP. Při zapnutí kontroluje zdrojovou IP adresu a porovnává ji s vazební databází odposlouchávání DHCP, případně s touto databází ještě kontroluje zdrojovou IP adresu i adresu MAC. Pokud položky nesouhlasí, rámec se odfiltruje. Tento mechanismus zapínáme pomocí dílčích příkazů rozhraní. Při zadání příkazu ***ip verify source*** se kontrolují jen zdrojové IP adresy.

S příkazem ***ip verify source port-security*** zapneme kontrolu IP adres i MAC adres. ***Ip source binding <adresa-mac> vlan <id-vlan ip-adresa> interface <id-rozhraní>*** vytváří statické položky, které se budou používat zároveň s vazební databází odposlouchávání DHCP [3].

## 3.4 802.1x

Další způsob autentizace je pomocí standartu IEEE 802.1X. Uživatel musí pro autentizaci zadat uživatelské jméno a heslo, které ověřuje server RADIUS. Poté může přepínač teprve povolit průchod portu pro normálního uživatele. Útočník tak nemůže zneužít cizí počítač díky požadavku na zadání jména a hesla. Musel by nejprve prolomit autentizační jméno a heslo podle 802.1X. Standart IEEE 802.1X používá jako podkladový autentizační protokol standart EAP. Ve standartu EAP jsou zprávy, které vypíší uživateli výzvu k zadání hesla, a také toky pro jednorázová hesla.

Konfigurace autentizace 802.1X v přepínači připomíná konfiguraci AAA metod. Podobně jako u nich se zapne mechanismus AAA příkazem ***aaa new-model***. Poté se zapne server RADIUS, nadefinujeme IP adresu a příslušné šifrovací klíče pomocí příkazů ***radius-server host*** a ***radius-server key***. Autentizační metoda 802.1X se definuje příkazem ***aaa authentication dot1x default***, nebo pro případ více skupin ***aaa authentication dot1x group <název>***. Příkaz ***dot1x system auth-control*** zapne globálně mechanismus 802.1X. U každého rozhraní pomocí příslušného příkazu se zapne jedno ze tří možných nastavení příkazem ***port-control auto|force-authorized|force-unauthorized***. ***Auto*** pro autentizaci 802.1X, ***force-authorized*** nepoužívat 802.1X, ale rozhraní bude automaticky autorizováno a ***force-unauthorized*** nepoužívat 802.1X, ale rozhraní bude automaticky neautorizováno [3].

## 3.5 Řízení broadcast bouří

Příkaz ***storm-control*** slouží na druhé vrstvě k omezení rychlosti provozu. Pro tři typy provozu nad portem mohou být v tomto mechanismu stanoveny vzestupné i sestupné prahové hodnoty, jednosměrový, víceměrový a všesměrový provoz. Na každém portu je možné stanovit všechny rychlostní limity. Díky řízení bouří je možné kontrolovat typy provozu podle absolutní rychlosti rámců, nebo podle procenta dostupné šířky pásma

rozhraní. Pokud jsou vzestupné i sestupné prahové hodnoty rozlišné, vypíná port provoz po překročení vzestupného prahu a zapíná jej opět až po poklesu provozu pod sestupný práh. Jestliže jsou prahy stejné, nebo není zadán sestupný práh, zapíná provoz portu ihned po návratu provozu pod hodnotu vzestupného prahu.

Po dosažení prahových hodnot provozu může přepínač využít některé ze tří dodatečných akcí, která se dá nastavit pro každý port zvlášť. Výchozí akcí je, že po omezení rychlosti nadměrný provoz zahodí. Další akce port vyřadí z provozu a poslední odešle zachycenou zprávu SNMP (Simple Network Management Protocol) [3].

# 4 ZABEZPEČENÍ VRSTVY 3

## 4.1 Přístupové seznamy

Přístupový seznam (ACL - Access Control List) je na aktivních zařízeních Cisco vlastností IOS (Internetwork Operating System). ACL slouží pro řízení síťového provozu, tedy pro filtrování paketů. Je to soubor pravidel určující postup paketů. Nejčastěji se ACL využívá pro filtrování nežádoucích paketů. Správnou kombinací přístupových seznamů mohou správci sítí zajistit bezpečnou privátní síť a eliminovat většinu síťových hrozeb. Přístupový seznam se ukládá do zařízení, ve kterém je nutné tento seznam pro jeho funkčnost aplikovat na rozhraní daného zařízení. To následně analyzuje veškeré pakety procházející přes toto rozhraní v určeném směru. Tento směr se uvádí do seznamu. Pokud je nalezena shoda, provede se nadefinovaná akce. V následujícím seznamu jsou uvedena pravidla pro porovnávání paketů.

- Paket se vždy porovnává se všemi řádky přístupového seznamu, počínaje prvním řádkem až po poslední řádek v pevném pořadí.
- Paket se porovnává s řádky přístupového seznamu jen tak dlouho, dokud není nalezena shoda. Jakmile je nalezena shoda, další řádky už se neporovnávají.
- Na konci každého přístupového seznamu je implicitní příkaz ***deny any***. Ten zaručí zahození paketu, pokud nevyhovuje žádné z uvedených podmínek.

Pro jedno rozhraní je možné aplikovat pouze jeden přístupový seznam na příchozí provoz a jeden přístupový seznam na odchozí provoz. Je důležité odlišit provoz a pečlivě nastavit přístupový seznam pro příchozí i odchozí provoz, jelikož jsou většinou odlišné. Přístupové seznamy se dělí na dva hlavní a jeden rozšiřující typ.

Standardní přístupové seznamy – testovací podmínkou těchto seznamů je pouze zdrojová IP adresa v paketu IP. Všechna rozhodnutí jsou založena na zdrojové IP adrese, kde standardní přístupové seznamy povolují nebo zakazují celé sady protokolů. Nerozlišují se tedy typy protokolů jako http (Hypertext Transfer Protocol), TELNET (Telecommunication Network), UDP (User Datagram Protocol), TCP atd. Syntax příkazů je následující: ***access-list <číslo> permit 0.0.0.0 1.1.1.1*** pro vytvoření pravidla *a* ***ip access-group <číslo pravidla> [in|out]*** pro aplikaci na vstup nebo výstup portu.

Rozšířené přístupové seznamy – tyto seznamy mohou vyhodnocovat mnohem více informací v hlavičkách vrstvy 3 a 4 paketu IP. Může se porovnávat zdrojová a cílová IP adresa, číslo portu a typ protokolu. Díky rozšířeným seznamům se tak můžou vytvořit přesnější pravidla pro příchozí i odchozí provoz. Syntax příkazů je následující: ***access-list 180 deny tcp any host 0.0.0.0 eq telnet*** vytvoření pravidla a ***ip access-group 180 [in|out]***aplikace seznamu.

Pojmenované přístupové seznamy – technicky se jedná o předchozí dva typy přístupových seznamů, ale jejich konfigurace probíhá odlišně. Můžou se pojmenovávat, tedy mohou být využity názvy místo čísel, čímž poskytují pojmenované přístupové seznamy lepší přehled a orientaci správcům sítě ve vytvořených seznamech. Syntax příkazů je: ***ip access-list standard IT_ONLY*** vytvoření přístupového seznamu, ***permit host 192.168.0.25*** vytvoření pravidla a ***ip access-group IT_ONLY in*** pro aplikaci seznamu.

Privátní síť tak může být pomocí přístupových seznamů chráněna před bezpečnostními hrozbami.

- Falšování IP adres, příchozí, odchozí.
- Útoky DoS a DDos (Distributed Denial Of Service), odepření přístupu.
- Útok se záplavou paketů SYN (Synchronization).
- Smurf Attack, útok se záplavou paketů ICMP (Internet Control Message Protocol) [7].

## 4.2 Smurf attack

Smurf attack znamená, že útočník odešle velké množství požadavků ICMP Echo request s atypickou IP adresou. Adresa cíle je všesměrová adresa v podsíti, tzv. řízeného všesměrového vysílán neboli directed broadcast address. Pakety pak směrovače rozesílají podle normální shody se směrovací IP tabulkou. Jakmile paket dorazí do směrovače připojeného k cílové podsíti, tak poslední směrovač odešle do LAN sítě paket jako všesměrové vysílání. V paketu zaslaném od útočníka, je podstrčena IP adresa oběti. Všichni hostitelé pak odpovědí zprávou ICMP Echo reply a pošlou ji na adresu oběti. Útok se pak násobí s počtem hostitelů ve zneužité síti, to vyvolá obrovské množství paketů směřujících k oběti. Tím dochází k zahlcení dostupné šířky pásma a napadený systém může být vyřazen z provozu [8].

Řešení smurf attack je několik. V Cisco IOS je software pro každé rozhraní ve výchozím nastavení příkaz ***no ip directed-broadcast***, který zakazuje rozesílat všesměrové pakety do lokální LAN sítě. Dalším řešením je dílčí příkaz rozhraní ***ip verify unicast source reachable-via rx|any [allow-default] [allow-self-ping]***, který zapíná kontrolu nad zasíláním po zpětné cestě RPF (Reverse Path Forwarding). Díky tomuto příkazu systém kontroluje zdrojové adresy IP paketů nad daným rozhraním. Můžou se provádět následující dva typy kontroly.

1. Striktní kontrola RPF. Zadáním slova ***rx*** směrovač kontroluje, zda je odchozím rozhraním právě to rozhraní, na kterém byl paket přijat. V opačném případě je paket zahozen.
2. Volná kontrola RPF. Slovo ***any*** pak znamená kontrolu jakékoliv cesty, přes kterou je možné dosáhnout zdrojové IP adresy.

Při kontrole může příkaz ignorovat výchozí cesty, nebo je může naopak používat. Příkaz může spustit i dotaz ping pro ověření konektivity. To se však nedoporučuje. Poslední možností je omezení množiny adres, pro které se kontrola RPF provádí. To je možné odkazem na vhodný přístupový seznam ACL. Dalším útokem může být útok tříštivých bomb, které mají podobnou logiku jako smurf attack, ale používají místo protokolu ICMP aplikaci UDP Echo. Útok tříštivých bomb se dá odrazit stejnou technikou jako smufr attack [3].

## 4.3 Nevhodné IP adresy

Kromě již zmíněných útoků existují ještě další možné typy a spadají pod pojem „nevhodné“ IP adresy. Jestliže si útočník zapíše nevhodnou IP adresu, zůstává sám skrytý a může vyvolat spolupráci s jinými hostiteli na vedení DDoS.

Prvním z postupů pro zabezpečení vrstvy 3 je filtrování paketů s nevhodnou IP adresou pomocí ACL. V předchozích útocích byla do paketů zapsána sice správná zdrojová adresa, ale tyto pakety by se vůbec do autonomního systému neměly dostat z vnějšího Internetu. Sdružení IANA (Internet Assigned Numbers Authority) řídí přiřazování intervalů prefixů IP adres. Ve směrovači poté můžeme definovat přístupové seznamy, které zabraňují vstupu paketů dle známých přiřazených i nepřiřazených intervalů. Směrovač podnikové sítě by neměl nikdy do Internetu zasílat paket, jehož zdrojová IP adresa je z prefixu IP adres, který

je registrován pro jinou organizaci. Takový přístupový seznam by v případě smurf attack zabránil ve vstupu byť i prvního paketu do autonomního systému.

Směrovač by měl také filtrovat pakety, které mají falešnou nebo nevhodnou IP adresu. Normální paket by totiž nikdy neměl mít jako zdrojovou vícesměrovou nebo všesměrovou IP adresu. Podle dokumentu RFC 1918 by podnikový směrovač neměl od poskytovatele dostat paket se zdrojovou adresou privátní sítě. Směrovač by neměl ani přijmout pakety, jejichž zdrojové IP adresy jsou v nepřiřazených intervalech. Vytvoření přístupového seznamu pro zachycení falešných IP adres není obtížné, musí se ale poté přístupový seznam aktualizovat podle změn v prefixech přiřazených sdružením IANA. Pomocí freeware nástroje RAT (Router Audit Tool) je možné provést zabezpečení směrovače včetně přístupových seznamů pro vadné pakety. Dále se dá využít funkce přístupná přímo v Cisco IOS, a to AutoSecure, jehož konfigurace potřebná pro přístupové seznamy vadných IP adres se provádí automaticky [3].

## 4.4 Záplava paketů TCP SYN

Záplava paketů TCP SYN (Transmission Control Protocol Synchronization) je útok vedený proti serverům. Útočník v tomto útoku zahájí velké množství spojení TCP, ale nedokončí je. Útočník tedy zdánlivě navazuje spojení s příznakem TCP SYN a server mu jako obvykle odpoví. Pro úplné spojení je potřeba 3 zpráv. Ale útočník po tom, co mu server odpoví, už nereaguje. Tím se třícestné spojení komunikace v TCP nezavrší. Server tak mezitím čeká na vypršení časového limitu, aby mohl tato nedokončená spojení vymazat. Dokud se tak nestane, má obsazeno velké množství paměti i prostředků. Díky tomu může server odmítat další spojení TCP.

Útokům se dá zabránit pomocí stavového firewallu. Může být k tomu využit Cisco PIX Firewall, nebo Cisco IOS Firewall. TCP SYN útoky je možné oslabit nebo úplně potlačit i jinými nástroji. Jednou z možností je filtrování paketů, které mají v hlavičce TCP nastaven pouze příznak SYN. V hodně případech nemá směrovač proč povolovat navazování spojení TCP. Od klientů na jedné straně po server na druhé straně může být útokům SYN zabráněno pomocí filtrování počátečního segmentu TCP.

Přístupový seznam v Cisco IOS přímo nedokáže kontrolovat příznak TCP SYN. V položce ACE (Application Control Engine) může být zapsáno klíčové slovo ***established***, jež se

shoduje se segmentem TCP a nastaví příznak ACK (Acknowledge). Kromě prvního segmentu nového spojení je toto klíčové slovo shodující se všemi segmenty TCP. Pokud klienti vně naší sítě nemají dovoleno navazovat TCP spojení dovnitř sítě, tak přístupové seznamy budou plnit svoji funkci. Pokud ale některá spojení TCP budou povolena, stejný přístupový seznam dále nebude fungovat. Proto bude využita další funkce systému Cisco IOS a to zadržení komunikace TCP, která umožňuje vstup spojení TCP do sítě a sleduje v nich možné útoky TCP SYN.

Mechanismus zadržení komunikace TCP pracuje ve dvou režimech. První je režim sledování, který udržuje stavové o spojeních TCP, které odpovídají definovanému přístupovému seznamu. Jakmile se nedokončí v daném intervalu třícestné spojení TCP, odešle zádržný mechanismus na server signál TCP reset a spojení zruší. Zároveň mechanismus sleduje počet pokusů o spojení, pokud jich bude více jak nastavené množství za 1 sekundu, tak je směrovač začne filtrovat a tím zabrání útoku SYN.

Druhý režim je režim zadržení, kde směrovač spojení neodesílá ihned na server, ale odpovídá sám na požadavky spojení TCP. Pokud se třícestné spojení dokončí, vytvoří teprve směrovač spojení sama sebe k serveru a dokončená spojení propojí. Tento režim je náročnější jak na výkon tak nastavení, ale zato mnohem bezpečnější pro servery [3].

## 4.5 Kontextově závislé řízení přístupu CBAC

Mechanismus CBAC (Context-Based Access Control) je součást firewallové množiny funkcí Cisco IOS. Díky tomuto mechanismu se dostává filtrování přístupových seznamů o několik úrovní výše, protože provádí dynamickou inspekci provozu přímo při průchodu firewallovým směrovačem. CBAC provádí takové kontroly dle skutečných příkazů vlastního protokolu. Například příkazem ***get*** v FTP (File Transfer Protocol) protokolu se podle místa daného provozu pak CBAC rozhodne, jestli průchod firewallem povolí. Pokud je relace zahájena v důvěryhodné síti pro daný protokol, ale podle jiných metod by byla filtrována, vytvoří CBAC ve firewallu dočasné průchody, které povolí vstup i odpovědi příchozího provozu z nedůvěryhodné sítě. Tak povolí jen konkrétní provoz, ale neotvírá firewall veškerému provozu. Mechanismus CBAC obsluhuje provoz protokolů TCP, UDP a navíc podporuje i další protokoly jako je FTP, kde je vyžadována činnost více současných relací či spojení. Pomocí CBAC tak chráníme většinou vnitřní sít před

hrozbami z venku a nakonfigurujeme příslušné protokoly k inspekci příchozího provozu z venkovního světa. V CBAC můžeme konkrétně nakonfigurovat, které protokoly podléhají inspekci, nad kterými rozhraními se bude inspekce provádět a v jakém směru se bude inspekce provádět [3].

### 4.5.1 CBAC V PROTOKOLU TCP A UDP

U protokolu TCP jsou jasně ohraničená spojení, tudíž je CBAC snadno zvládá. CBAC pracuje na hlubší úrovni než jen na protokolech a číslech portů. Dokáže rozpoznat a kontrolovat konkrétní příkazy řídícího kanálu FTP a podle nich stanovit, kdy otevřít a zase uzavřít průchody firewallem. UDP je oproti TCP nespojovaný, a proto je obsluha obtížnější. U komunikace UDP se CBAC snaží odhadovat různé faktory. Například zdali jsou zdrojové a cílové adresy v rámcích UDP stejné jako nedávno přijaté, stejně tak je to u čísel portů. Dále kontroluje, v jakém časovém rozestupu byly přijaty. Může být nakonfigurován limit nečinnosti, dle které CBAC určuje, zdali určitý rámec už dorazil v daném čase, aby jej mohl považovat za součást stejného datového toku [3].

### 4.5.2 PODPORA PROTOKOLŮ V CBAC

„Mechanismus CBAC dokáže provádět inspekci následujících protokolů:

- Libovolná generická relace TCP bez ohledu na konkrétní protokol aplikační vrstvy.
- Všechny relace UDP.
- FTP.
- SMTP (Simple Mail Transfer Protocol).
- TFTP (Trivial File Transfer Protocol).
- H.323 (NetMeeting, ProShare apod.).
- Java.
- CU-SeeMe.
- Unixové příkazy „R“ (Regin, rexec, rsh atd.).
- Real Audio.
- Sun RPC.
- SQL*Net.
- StreamWorks.

- VDOLive.“ [3]

### 4.5.3 NÁSTRAHY MECHANISMU CBAC

I když je mechanismus CBAC velmi silný, má i své hranice. Kontroly CBAC jsou spuštěny až tehdy, kdy jsou nad danými rozhraními aplikovány filtry přístupových seznamů. Pokud přístupový seznam některý z provozů zablokuje, inspekce CBAC se k tomuto provozu vůbec nedostane a tento provoz bude bez náhrady zamítnut. CBAC chrání pouze před útoky zvenčí, nikoliv před útoky zevnitř sítě. Pracuje také jen nad protokoly, které jsou mu určeny. Ostatní filtrování přenechává přístupovým seznamům nebo jiným metodám filtrování. CBAC také nekontroluje veškerý provoz, pouze ten, co prochází přes firewall [3].

### 4.5.4 POSTUP KONFIGURACE CBAC

Konfigurace mechanismu CBAC je snadná. V prvním kroku bude zvoleno vnější nebo vnitřní rozhraní. Nadefinuje se na toto rozhraní přístupový seznam IP adres. Dále budou nakonfigurovány pomocí příkazu ***ip inspect*** globální časové limity a prahové hodnoty. Příkazem ***ip inspect name <název protokol>*** bude nadefinováno inspekční pravidlo a volitelná hodnota časového limitu pro toto pravidlo. Přiklad celého příkazu ***ip inspect actionjackson ftp time 360.*** Toto pravidlo musí být aktivováno nad rozhraním. Je nutné zadat příkaz v režimu konfigurace ***ip inspect actionjackson in*** [3].

## 4.6 Dynamické sítě v DMVPN

Mechanismus dynamických multiportů VPN (DMVPN - Dynamic Multiport Virtual Private Network) využívá technologie IPSec, tunelů GRE (Generic Routing Encapsulation) a protokolu NHRP (Next Hop Resolution Protokol). Ve hvězdicové topologii sítě dosahuje IPSec lepší škálovatelnosti. Sítě DMVPN podporují jak VRF (virtuální směrování a přesměrování), tak segmentaci provozu mezi jednotlivé VPN. Výhody DMVPN ve srovnání s hvězdicovou sítí VPN, která je postavena na IPSec jsou následující:

- Jednoduchá konfigurace, stačí jedno tunelové rozhraní vícebodového GRE, jeden profil IPSec a nejsou potřeba přístupové seznamy.

- Není nutné nastavovat centrální směrovač po připojení nových vedlejších směrovačů.
- Automaticky zapínané šifrování IPSec, které zajišťuje protokol NHRP.
- Dynamické adresování vedlejších směrovačů. Centrální směrovač zjistí adresy poboček v okamžiku jejich registrace do sítě.
- Dynamicky vytvářené tunely přímo mezi pobočkami. Díky protokolu NHRP se o sobě dozví pobočné směrovače, takže mezi sebou mohou vytvořit tunely a nemusí vzájemný provoz šifrovat a dešifrovat v centrálním směrovači.
- Integrování virtuálního směrování VRF pro prostředí MPLS

Mezi centrálním a vedlejším směrovačem musí pracovat dynamický směrovací protokol. Například EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), RIP (Routing Information Protocol) nebo ODR (On-Demand Routing). Doporučený je protokol EIGRP s vektorem vzdáleností pro rozsáhlé sítě. Tak se dozví vedlejší směrovače o sítích v ostatních pobočkách. IP adresa dalšího přeskoku vedlejší sítě je v prostředí DMVPN adresa tunelového rozhraní příslušné pobočky [3].

# II. PRAKTICKÁ ČÁST

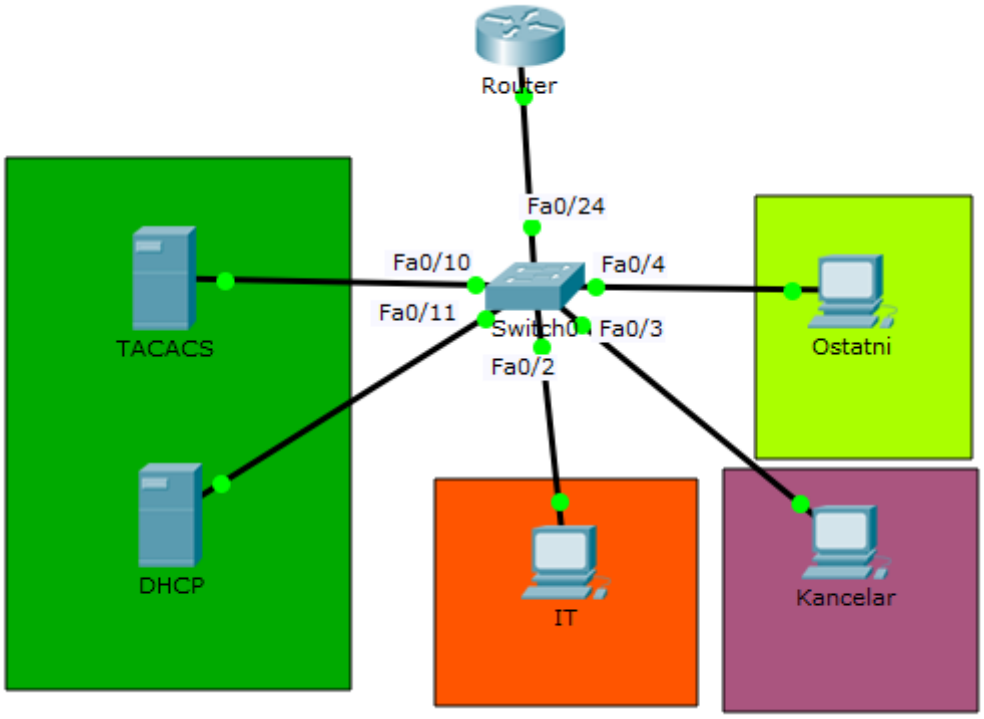
# 5 NÁVRH ZABEZPEČENÍ

Pro návrh zabezpečení aktivních zařízení firmy Cisco byly vybrány pouze směrovače a přepínače. Bezpečnostní zařízení jako jsou firewally, sondy IPS a IDS nebudou využity. Veškeré zabezpečení proběhlo pomocí směrovačů a přepínačů. Firmám se tak podstatně sníží náklady na IT infrastrukturu.

Simulace návrhu zabezpečení proběhla v programu Cisco Packet Tracer, ve kterém jsou však některé služby a příkazy omezeny. Tyto nefunkční příkazy, které budou nastaveny na simulovanou síť a označeny jako nefunkční pro program Cisco Packet Tracer, budou označeny symbolem „//“ a pro reálnou síť mohou být využity. Nejprve musí být rozmysleno, jaká síť se bude zabezpečovat. V tomto případě byla zvolena čistě demonstrativní síť, která poslouží pro ukázku a pochopení nastavení. V síti tak bude pouze jeden směrovač, jeden přepínač, 2 servery a 3 počítače. To bude pro demonstrativní účely stačit.

## 5.1 Cisco Packet Tracer

Cisco Packet Tracer je simulační program, který umožňuje virtuální simulaci nastavení sítě. Je to integrovaná součást komplexního vzdělávacího programu Networking Academy [9]. Cisco Packet Tracer nabízí již zmíněnou simulaci, vizualizaci, tvorbu, testování a usnadňuje i výuku či učení složitých technologických konceptů. Packet Tracer je vybaven různými zařízeními a jeho výhoda spočívá v tom, že umožňuje vytvářet síť s téměř neomezeným počtem zařízení. Simulační software je však bezplatně k dispozici pouze instruktorům, studentům a absolventům Network Academy či správcům registrovaným v Academy Connection.




Obr. 1. *Topologie sítě.*

Určí se adresový prostor pro demonstrativní účely. Pro tuto demonstrativní síť byl zvolen následující rozsah určitých adres a rozdělení do VLAN. VLAN 90 slouží pro zařazení nevyužitých portů a jejich zabezpečení.

Tab. 1. *Rozdělení adresního prostoru.*

| Síť | Adresa sítě | Rozsah adres | Broadcast | Maska sítě |
|---|---|---|---|---|
| VLAN 10 | 192.168.1.0/24 | 192.168.1.1 - 254 | 192.168.1.255 | 255.255.255.0 |
| VLAN 20 | 192.168.2.0/24 | 192.168.2. 1 - 254 | 192.168.2.255 | 255.255.255.0 |
| VLAN 30 | 192.168.3.0/24 | 192.168.3. 1 - 254 | 192.168.3.255 | 255.255.255.0 |
| VLAN 60 | 192.168.4.0/24 | 192.168.4. 1 - 254 | 192.168.4.255 | 255.255.255.0 |
| VLAN 90 | - | - | - | - |

.

# 6 NÁVRH BĚŽNÉHO ZABEZPEČENÍ

Nejprve bude nastaveno běžné nastavení směrovačů a přepínačů, kde se začne pojmenováním zařízení. Následuje využití hesel pro přístup do zařízení, jak pro uživatelský režim, tak i pro privilegovaný režim. Nastavení virtuálních linek, které se využívají pro připojení přes TELNET či SSH. Nastaví se zprávy dne, pro informování v rozhraní příkazového řádku.

| | |
|---|---|
| Switch> | Uživatelský režim. |
| Switch>en | Příkaz pro přepnutí do privilegovaného režimu. |
| Switch# | Privilegovaný režim. |
| Switch#configure terminal | Příkaz pro vstup do konfiguračního režimu. |
| Switch(config)# | Konfigurační režim. |
| Switch(config)#hostname S1 | Nastavení názvu přepínače. |
| S1(config)#no ip domain-lookup | Vypnutí překladu nerozpoznaných příkazů na IP adresy. |
| S1(config)#enable secret sovis | Nastavení šifrovacího hesla „sovis“ pro vstup do privilegovaného režimu. |
| S1(config)#username Admin privilege 15 secret sovis | Nastavení přihlašovacích údajů „Admin“ a „sovis“ úrovně oprávnění 15, s uložením do lokální databáze. |
| S1(config)#line console 0 | Vstup do režimu nastavení přístupu přes konzoli. |
| S1(config-line)#logging synchronous | Synchronní logování. |
| S1(config-line)#password sovis | Nastavení hesla. |
| S1(config-line)#login | Zapnutí přihlášení. |
| S1(config-line)#service password-encryption | Zašifrování hesla. |
| S1(config)#line vty 0 1 | Vstup do režimu pro vzdálený přístup. |
| S1(config-line)#login local | Přístup pomocí přihlašovacích údajů z lokální databáze. |

| | |
|---|---|
| S1(config-line)#line vty 2 15 | Vstup do režimu pro vzdálený přístup na virtuálních linkách 2-15. |
| S1(config-line)#transport input none | Zakázat jakýkoliv přístup na tyto linky. |
| S1(config-line)#transport output none | Zakázat jakékoliv odchozí spojení přes tyto linky. |
| S1(config-line)#no login | Bez přihlášení. |
| S1(config)#banner motd # Unauthorized acces to this device is prohibited! # | Vytvoření MOTD (message-of-the-day). Oznámení pro narušitele. |
| S1(config)#banner login # Please enter your username and password! # | Vytvoření přihlašovací zprávy, která upozorní na přihlášení k zařízení. |
| S1#copy running-config startup-config | Uložení konfigurace do NVRAM. Používáme na konci každé konfigurace. |

Poté budou vypnuty nepotřebné porty a nevyužívané funkce. Nastaví se PortFast, aby koncové zařízení mohlo komunikovat ihned. Využijí se funkce BPDU Guard pro zabránění předávání informací pomocí datových zpráv portům nakonfigurovaných jako PortFast. Root Guard zabrání přepínači, aby se stal Root Bridgem a budou zabezpečeny porty dynamickým zjištěním MAC adresy a stárnutí.

| | |
|---|---|
| S1(config)#interface Fa0/1 | Přístup do konfiguračního režimu daného rozhraní. |
| S1(config)#spanning-tree portfast default | Zapnutí funkce PortFast pro všechny access porty mimo trunk. |
| S1(config-if)#spanning-tree bpduguard enable | Zapnout funkci BPDU Guard pro daná rozhraní. |
| S1(config-if)#spanning-tree guard root | Zapnout funkci Guard Root pro daná rozhraní. |
| S1(config)#interface fa0/2 | Přístup do konfiguračního režimu daného rozhraní. |
| S1(config-if)#switchport port-security mac-address sticky | Zapnutí ukládání dynamických Mac adres do tabulkyMac adres přepínače. |
| S1(config-if)#switchport port-security aging | Zapnutí stárnutí Mac adres v tabulce. |

| | |
|---|---|
| violation protect | |

Následuje vypínání všech nepotřebných funkcí. Funkce Auto Secure automaticky vypne / zakáže různé typy služeb, a ty se pak podle potřeby můžou zapnout. Pro simulaci vypnutí služeb jsou zde uvedeny příkazy, těch však většina není podporována v programu v Cisco Packet Traceru.

| | |
|---|---|
| Router#auto secure | Spuštění procesu CLI AutoSecure, dotazuje se uživatele na povolení či zakázání služeb a bezpečnostních prvků. |
| Router(config)# no service udp-small-server | // Zakázání malé služby protokolu UDP. |
| Router(config)# no service finger | // Zakázání služby Finger, využívána pro zachování zpětné komptability. |
| Router(config)# no service pad | //Zakázat službu Packet Assembler/Disassembler. |
| Router(config)# no service config | //Zabránění v pokusu o lokalizaci konfiguračního souboru v síti s TFTP serverem. |
| Router(config)# no snmp-server | //Zakázat službu SNMP, využívanou pro monitorování a správu sítě. |
| Router(config)# no lldp run | //Vypnutí LLDP. |
| Router(config)# no ip bootp server | //Zakázat Bootstrap. |
| Router(config)# ip dhcp bootp ignore | // Zakázat Bootstrap bez DHCP. |
| Router(config)# no ip http server | //Zakázat přístup přes webové rozhraní. |
| Router(config)# no ip http secure-server | //Zakázat přístup přes šifrované webové rozhraní. |
| Router(config)# no ip finger | //Zakázat službu IP Finger. |
| Route(config)r#no ip source-route | //Zakázat zdrojové směrování. |
| Router(config)# no ip gratuitos-arps | //Zakázat bezdůvodné odesílání ARP |

| | |
|---|---|
| Router(config)# secure boot-image<br>Router(config)# secure boot-config | požadavků.<br>Zabrání odstranění running-config souboru.<br>Archivuje running-config soubor. |

Musí se zde ovšem dát pozor, aby nebyla vypnuta služba, kterou využívá jiná bezpečnostní technologie. Avšak díky vypnutí či zakázání funkcí, které nejsou využité, se zvýší bezpečnost a omezí možnost některých útoků.

Nastavení, které se vytvořilo, je téměř shodné jak pro směrovač, tak i pro přepínač, tudíž se podle toho nastaví i druhé zařízení.

Dále bude nastaveno rozdělení VLAN. Nejprve se všechny porty vypnou a poté se začnou nastavovat. Vytvoří se potřebné VLAN, nastaví se jména, nastaví se rozhraní do přístupového módu a vypne vyjednávání pro trunk port protokolem DTP. Nakonec nevyužité porty budou zařazeny do VLAN 90 a vypnou se.

| | |
|---|---|
| S1#configure terminal | Vstup do konfiguračního režimu. |
| S1(config)#interface range Fa0/1-24 Gi0/1-2 | Vstup do nastavení v daném rozmezí rozhraní. |
| S1(config-if-range)#shutdown | Vypnutí portů. |
| S1(config-if-range)#exit | Navrácení o jedno výše. |
| S1(config)# vlan 10 | Vytvoření VLAN 10. |
| S1(config-vlan)#name Servers | Nastavení názvu pro VLAN 10. |
| S1(config-vlan)#vlan 20 | Vytvoření VLAN 20. |
| S1(config-vlan)#name Others | Nastavení názvu pro VLAN 20. |
| S1(config-vlan)#vlan 30 | Vytvoření VLAN 30. |
| S1(config-vlan)#name Offices | Nastavení názvu pro VLAN 30. |
| S1(config)#vlan 60 | Vytvoření VLAN 60. |
| S1(config-vlan)#name IT | Nastavení názvu pro VLAN 60. |
| S1(config-vlan)#vlan 90 | Vytvoření VLAN 90. |
| S1(config-vlan)#name Unused | Nastavení názvu pro VLAN 90. |

| | |
|---|---|
| S1(config-vlan)#exit | Navrácení o úroveň. |
| S1(config)#interface Fa0/4 | Vstup do konfigurace rozhraní. |
| S1(config-if)#switchport mode access | Nastavení daného rozhraní do přístupového módu. |
| S1(config-if)#switchport access vlan 20 | Zařazení rozhraní do VLAN 20 Others. |
| S1(config-if)#switchport nonegotiate | Vypnout jednávání trunk portu nad protokolem DTP. |
| S1(config-if)#no shutdown | Zapnutí rozhraní. |
| S1(config-if)#interface Fa0/3 | Vstup do konfigurace rozhraní. |
| S1(config-if)#switchport mode access | Nastavení daného rozhraní do přístupového módu. |
| S1(config-if)#switchport access vlan 30 | Zařazení rozhraní do VLAN 30 Offices. |
| S1(config-if)#switchport nonegotiate | Vypnout jednávání trunk portu nad protokolem DTP. |
| S1(config-if)#no shutdown | Zapnutí rozhraní. |
| S1(config-if)#interface Fa0/2 | Vstup do konfigurace rozhraní. |
| S1(config-if)#switchport mode access | Nastavení daného rozhraní do přístupového módu. |
| S1(config-if)#switchport access vlan 60 | Zařazení rozhraní do VLAN 60 IT. |
| S1(config-if)#switchport nonegotiate | Vypnout jednávání trunk portu nad protokolem DTP. |
| S1(config-if)#no shutdown | Zapnutí rozhraní. |
| S1(config-if)#interface range Fa0/10-11 | Vstup do konfigurace rozmezí rozhraní. |
| S1(config-if-range)#switchport mode access | Nastavení daného rozhraní do přístupového módu. |
| S1(config-if-range)#switchport access vlan 10 | Zařazení rozhraní do VLAN 10 Servers. |
| S1(config-if-range)#switchport nonegotiate | Vypnout jednávání trunk portu nad protokolem |

| | |
|---|---|
| | DTP. |
| S1(config-if-range)#no shutdown | Zapnutí rozhraní. |
| S1(config-if-range)#exit | Navrácení o úroveň. |
| S1(config)#interface range Fa0/1, Fa0/5-9, Fa0/12-23, Gi0/1-2 | Vstup do konfigurace rozmezí rozhraní. |
| S1(config-if-range)#switchport mode access | Nastavení daného rozhraní do přístupového módu. |
| S1(config-if-range)#switchport access vlan 90 | Zařazení rozhraní do VLAN 90 Unused. |
| S1(config-if-range)#switchport nonegotiate | Vypnout jednávání trunk portu nad protokolem DTP. |
| S1(config-if-range)#shutdown | Vypnutí rozhraní. |

Nyní dojde k nastavení směrovače pro směrování a komunikaci. Bude popsán daný subinterface, přiřadí se subinterface do trunk módu s využitím IEEE 802.1Q protokolu. Nastaví se IP adresa pro subinterface.

| | |
|---|---|
| Router#configure terminal | Vstup do konfiguračního režimu. |
| Router(config)#interface Gi0/0.10 | Vytvoření subinterface. |
| Router(config-subif)#description Pripojeni k VLAN 10 - Servers | Nastavení popisu pro daný interface. |
| Router(config-subif)#encapsulation dot1Q 10 | Přiřazení subinterface do trunk módu a nastavení využití protokolu IEEE 802.1q pro VLAN 10. |
| Router(config-subif)#ip address 192.168.1.1 255.255.255.0 | Konfigurace IP adresy pro VLAN 10. Brána této VLAN. |
| Router(config-subif)#no shutdown | Zapnutí rozhraní. |
| Router(config-subif)#interface Gi0/0.20 | Vytvoření subinterface. |
| Router(config-subif)#description Pripojeni k VLAN 20 - Others | Nastavení popisu pro daný interface. |
| | Přiřazení subinterface do trunk módu a |

| | |
|---|---|
| Router(config-subif)#encapsulation dot1Q 20 | nastavení využití protokolu IEEE 802.1q pro VLAN 20. |
| Router(config-subif)#ip address 192.168.4.1 255.255.255.0 | Konfigurace IP adresy pro VLAN 20. Brána této VLAN. |
| Router(config-subif)#no shutdown | Zapnutí rozhraní. |
| Router(config-subif)#interface Gi0/0.30 | Vytvoření subinterface. |
| Router(config-subif)#description Pripojeni k VLAN 30 - Offices | Nastavení popisu pro daný interface. |
| Router(config-subif)#encapsulation dot1Q 30 | Přiřazení subinterface do trunk módu a nastavení využití protokolu IEEE 802.1q pro VLAN 30. |
| Router(config-subif)#ip address 192.168.3.1 255.255.255.0 | Konfigurace IP adresy pro VLAN 30. Brána této VLAN. |
| Router(config-subif)#no shutdown | Zapnutí rozhraní. |
| Router(config-subif)#interface Gi0/0.60 | Vytvoření subinterface. |
| Router(config-subif)#description Pripojeni k VLAN 60 - IT | Nastavení popisu pro daný interface. |
| Router(config-subif)#encapsulation dot1Q 60 | Přiřazení subinterface do trunk módu a nastavení využití protokolu IEEE 802.1q pro VLAN 60. |
| Router(config-subif)#ip address 192.168.2.1 255.255.255.0 | Konfigurace IP adresy pro VLAN 30. Brána této VLAN. |
| Router(config-subif)#no shutdown | Zapnutí rozhraní. |
| Router(config-subif)#interface Gi0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#no description | Žádný popisek. |
| | Žádná IP adresa |

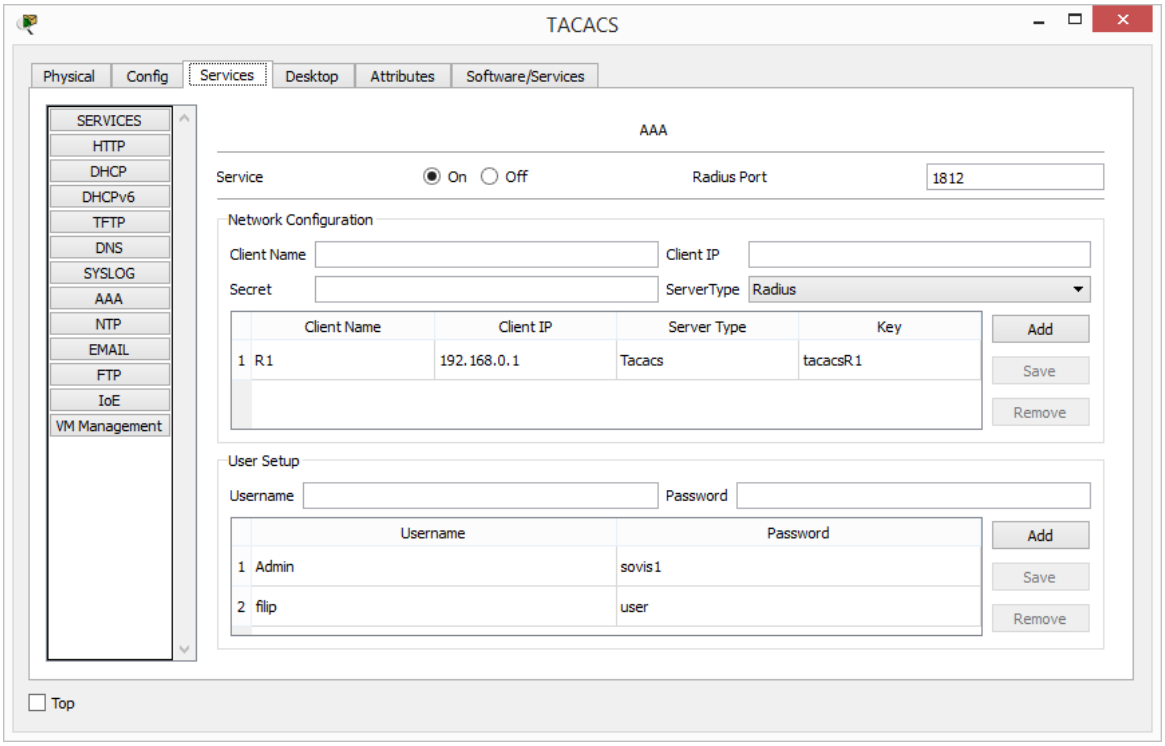
| | |
|---|---|
| Router(config-if)#no ip address<br><br>Router(config-if)#no shutdown | Zapnutí rozhraní. |

Donastaví se přepínač pro komunikaci se směrovačem. Nastaví se trunk port s protokolem IEEE 802.1Q, vypne vyjednávání pro trunk port protokolem DTP a bude zapnut port.

| | |
|---|---|
| S1(config)#interface Fa0/24 | Vstup do konfigurace rozhraní. |
| S1(config-if)#shutdown | Vypnutí rozhraní. |
| S1(config-if)#switchport mode trunk | Nastavení rozhraní do trunk módu. |
| S1(config-if)#switchport trunk encapsulation dot1Q | // Využití protokolu IEEE 802.1q. |
| S1(config-if)#switchport trunk allowed vlan 10,20,30,60 | Přenést přes linku pouze VLAN 10,20,30 a 60. |
| S1(config-if)#switchport nonegotiate | Vypnutí vyjednávání trunku portu nad protokolem DTP. |
| S1(config-if)#no shutdown | Zapnutí rozhraní. |

V konfiguraci technologie AAA se pro tuto síť více hodí řešení pro správu síťových zařízení, a proto byl vybrán protokol TACACS+. Tím se tedy bude řídit a kontrolovat přístup ke konzole směrovače. Pro přepínače toto řízení a kontrolu nepodporuje program Cisco Packet Tracer, ale u reálného zařízení se nakonfiguruje autentizace AAA i u přepínačů.

Nejdříve bude nastaven server TACACS+. Po otevření tohoto serveru se v záložce Config nastaví defaultní brána. V tomto případě se jedná o ip adresu dané VLAN, která je 192.168.1.1. Dále se otevře desktop, IP configuration a nastaví se statická IP adresa z rozsahu pro tuto VLAN například 192.168.1.10. Následně otevřeme záložku Services, kde všechny služby budou vypnuty, a nechá se jen služba AAA zapnuta. Dále bude nakonfigurován server v záložce Services/AAA podle obrázku [2].




Obr. 2. *Nastavení serveru TACACS+.*

Pro funkčnost autentizace pomocí serveru TACACS+ na směrovači je nutné směrovač ještě nastavit. Nastaví se jméno a tajné zašifrované heslo v lokální databázi, nakonfiguruje IP adresa a bezpečnostní klíč serveru TACACS+. Poté bude vytvořen pojmenovaný seznam autentizačních metod. Nastaví se autentizace na přístup přes konzolu a pro přístup přes pomocnou linku.

| | |
|---|---|
| Router(config)#interface Gi0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#ip address 192.168.0.1 255.255.255.0 | Přiřazení IP adresy. |
| Router(config-if)#no shutdown | Zapnutí rozhraní. |
| Router(config-if)#exit | Návrat o úroveň. |
| Router(config)#username Admin privilege 15 secret sovis1 | Nastavení přihlašovacích údajů „Admin“ a „sovis1“ úrovně oprávnění 15, s uložením do lokální databáze. |

| | |
|---|---|
| Router(config)#tacacs-server host 192.168.1.10 | Konfigurace IP adresy serveru TACACS+. |
| Router(config)#tacacs-server key tacacsR1 | Konfigurace klíče serveru TACACS+. |
| Router(config)#aaa new-model | Zapnout technologii AAA. |
| Router(config)#aaa authentication login TACACS_A group tacacs+ local | Vytvoří pojmenovaný seznam autentizačních metod s názvem TACACS_A |
| Router(config)#line console 0 | Vstup do konfigurace přístupu přes konzolu. |
| Router(config-line)#login authentication TACACS_A | Aplikování vytvořeného seznamu na přístup přes konzolu. |
| Router(config-line)#exit | Návrat o úroveň. |
| Router(config)#line aux 0 | Vstup do konfiguračního režimu přístupu přes pomocnou linku. |
| Router(config-line)#login authentication TACACS_A | Aplikování vytvořeného seznamu na přístup přes konzolu. |
| Router(config)#end | Návrat do privilegovaného režimu. |

Dále je možné nastavit autorizaci a účtování pomocí serveru TACACS+, ale jen v reálné síti. Simulační program Cisco Packet Tracer toto nastavení nepodporuje. Uvedou se zde příkazy jako příklad pro konfiguraci, které lze využít pro reálné zařízení.

| | |
|---|---|
| Router(config)#aaa authentication enable default group tacacs+ local | Vytvoří defaultní seznam autentizačních metod. |
| Router(config)#aaa authorization exec TACACS_A group tacacs+ local | Vytvoření seznamu autorizačních metod pro uživatelský režim. |
| Router(config)#aaa authorization config-commands | //Autorizace příkazů v konfiguračním režimu |
| Router(config)#aaa authorization commands 15 TACACS_A group tacacs+ local | //Autorizace příkazů s nejvyšší úrovní. |
| Router(config)#aaa accounting exec TACACS_AC start-stop group tacacs+ | //Zaznamenání příkazů v uživatelském režimu. |

| | |
|---|---|
| Router(config)#aaa accounting commands 15 TACACS_AC start-stop group tacacs+ | //Zaznamenání příkazů v privilegovaném režimu. |
| Router(config)#aaa accounting connection TACACS_AC start-stop group tacacs+ | //Zaznamenání všech odchozích spojení. |
| Router(config)#aaa accounting network TACACS_AC start-stop group tacacs+ | //Zaznamenání všech požadavků na síťové služby. |
| Router(config)#aaa accounting system TACACS_AC start-stop group tacacs+ | //Zaznamenání systémových událostí. |
| Router(config)#line console 0 | Vstup do režimu přístupu přes konzolu. |
| Router(config-line)#authorization exec TACACS_A | //Aplikování seznamu pro autorizaci v uživatelském režimu. |
| Router(config-line)#authorization commands 15 TACACS_A | //Aplikování seznamu pro příkazy s nevyšší úrovní. |
| Router(config-line)#accounting exec TACACS_AC | .//Aplikování účtování v uživatelském režimu. |
| Router(config-line)#accounting commands 15 TACACS_AC | //Aplikování účtování příkazů s nejvyšší úrovní. |

Tyto příkazy byly čerpány z [10]. Dalším bodem návrhu pro zabezpečení je PPP protokol. Jelikož je změna zapouzdření umožněna pouze pro sériová rozhraní, bylo nutno přidat dva směrovače mimo simulovanou síť pro simulaci zabezpečení PPP. Využije se tedy následovné nastavení.

| | |
|---|---|
| Router(config)#interface s0/0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#encapsulation ppp | Zapnout zapouzdření PPP. |
| Router(config-if)#username Router1 password ppp | Nastavení účtu s heslem pro CHAP autentizaci. Jméno se musí shodovat s hostname protilehlého směrovače. Heslo musí být stejné. |
| Router(config)# interface s0/0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#ppp authentication chap | Zapnutí CHAP autentizace. |

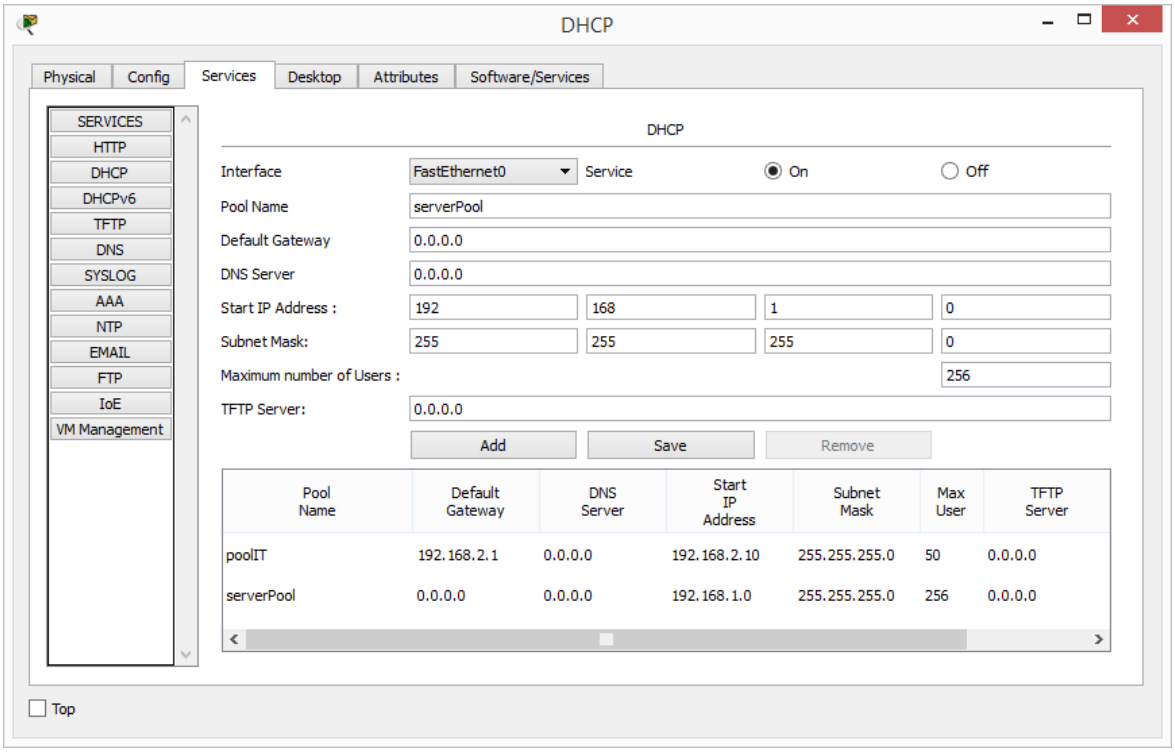
| | |
|---|---|
| Router1(config)# interface s0/1/1 | Vstup do konfigurace rozhraní. |
| Router1(config-if)#encapsulation ppp | Zapnout zapouzdření PPP. |
| Router1(config-if)#username Router password ppp | Nastavení účtu s heslem pro CHAP autentizaci. Jméno se musí shodovat s hostname protilehlého směrovače. Heslo musí být stejné. |
| Router1(config)#interface s0/1/1 | Vstup do konfigurace rozhraní. |
| Router1(config-if)#ppp authentication chap | Zapnutí CHAP autentizace. |

# 7 NÁVRH ZABEZPEČENÍ VRSTVY 2

Dynamic ARP Inspection zabraňuje útokům Man in the middle. Proto bude ukázáno demonstrativní nastavení této dynamické inspekce. Toto nastavení program Cisco Packet Tracer nepodporuje, ale na reálných zařízeních může být využito. Nejprve se spustí inspekce pro dané VLAN, nastaví se důvěryhodnost portů a inspekci pomocí MAC access-list. Dále bude nastaveno, že do VLAN 10, tedy k serverům má přístup pouze IT oddělení, tím, že bude povolena pouze Mac adresa dané VLAN a zbytek zahodíme. Nakonec může být nastavena inspekce podle zdrojové, cílové MAC adresy nebo IP adresy.

| | |
|---|---|
| S1(config)# ip arp inspection vlan 10,20,30,60 | //Zapnutí funkce DAI pro dané VLAN. |
| S1(config)# interface fa0/24 | Vstup do konfigurace rozhraní. |
| S1(config-if)# ip arp inspection trust | //Nastavení daného rozhraní jako důvěryhodné. |
| S1(config)#mac access-list extended mac1 | //Vytvoření Mac přístupového seznamu. |
| S1(config-ext-macl)#permit host 0000.1111.2222 any | Vytvoření pravidla, tato Mac adresa je povolena. |
| S1(config-ext-macl)#deny any any | Vytvoření pravidla nic jiného nemůže vstoupit. |
| S1(config-ext-macl)#exit | Návrat o úroveň. |
| S1(config)#interface Fa0/10 | Vstup do konfigurace rozhraní. |
| S1(config-if)#mac access-group mac1 in | //Aplikace vytvořeného přístupového seznamu. |
| S1(config)# ip arp inspection filter mac1 vlan 10 static | //Aplikace přístupového seznamu pro VLAN 10. |
| S1(config)#ip arp inspection validace src-mac [src-mac\|dst-mac\|ip] | //Porovnávání zdrojové adresy v rámci se zdrojovými MAC adresami v ARP odpovědi. DST-MAC – cílová MAC adresa s cílovými MAC adresami. IP- IP adresa s cílovou IP adresou. |

Nastaví se dále DHCP server a DHCP odposlouchávání. Bude spuštěn server, vypnou se nepoužívané služby a nastaví se rozsah IP adres pro přidělování podle následujícího obrázku.




Obr. 3. *Nastavení DHCP serveru*.

Dále bude nastaven přepínač a směrovač. Začne se tedy přepínačem, kde se zapne DHCP snooping pro dané VLAN a budou nastaveny některé porty za důvěryhodné. Dále se tak může nastavit snooping pro ověřování konkrétních MAC adres a limit maximálního počtu DHCP zpráv za minutu.

| | |
|---|---|
| S1(config)#ip dhcp snooping vlan 10,20,30,60 | Zapnutí DHCP odposlouchávání na daných VLAN. |
| S1(config)#interface fa0/11 | Vstup do konfigurace rozhraní. |
| S1(config-if)#ip dhcp snooping trust | Nastavení daného rozhraní za důvěryhodné. |
| S1(config-if)#exit | Návrat o úroveň. |
| S1(config)#interface fa0/2 | Vstup do konfigurace rozhraní. |

| | |
|---|---|
| S1(config-if)#ip dhcp snooping trust | Nastavení daného rozhraní za důvěryhodné. |
| S1(config)#ip dhcp snooping verify mac-address | Přidání kontroly zdrojové MAC adresy. |
| S1(config)#ip dhcp snooping limit rate 60 | Definice maximálního počtu DHCP zpráv za minutu. |

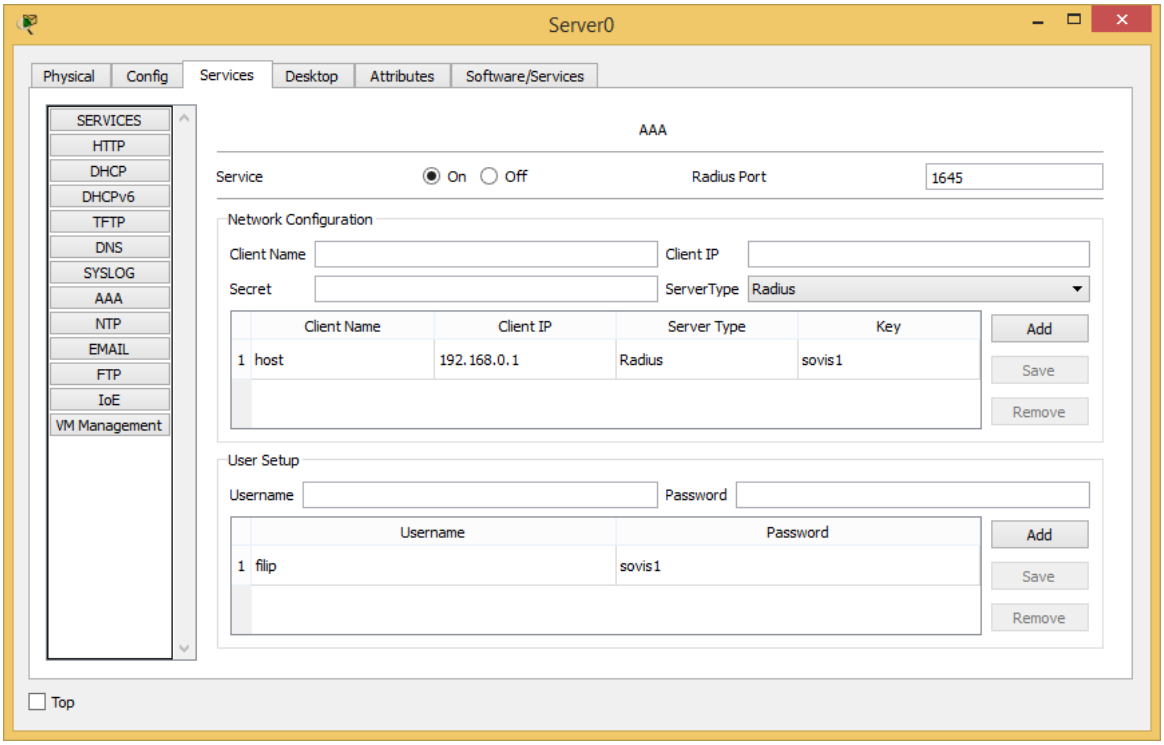
Nastaví se směrovač, aby využil pomocné adresy DHCP serveru a mohl tak žádost přeposlat.

| | |
|---|---|
| Router#config terminal | Zapnutí konfiguračního režimu. |
| Router(config)#interface Gi0/0.60 | Vstup do subinterface. |
| Router(config-subif)#ip helper-address 192.168.1.2 | Využití IP adresy DHCP serveru. |

Dále bude k odposlouchávání DHCP nastaven IP Source Guard. Toto nastavení program Cisco Packet Traceru nepodporuje, ale v reálné síti lze běžně nastavit. Zapne se tedy kontrola IP i MAC adres, nebo se mohou vytvořit statické položky.

| | |
|---|---|
| S1(config)#interface range Fa0/1-24, Gi0/1-2 | Vstup do nastavení rozmezí rozhraní. |
| S1(config-if-range)#ip verify source | //Zapnout funkci IP Source Guard s prověřením zdrojové IP adresy. |
| S1(config-if-range)#ip verify source port-security | // Zapnout funkci s prověřením zdrojové IP i MAC adresy. |
| S1(config-if-range)#Ip source binding ip source binding 0000.1111.2222 vlan 30 192.168.3.1 interface Fa0/5 | // Pro zařízení se statickou IP je možné vložit záznat manuálně. |

Následuje zabezpečení 802.1x, které ale na přepínači v programu Cisco Packet Tracer není podporováno. Ukáže se ale nastavení, které na reálných zařízeních funguje. Nejdříve bude nastaven server RADIUS podle obrázku (Obr. 4). Dále se vypnou všechny služby, které nejsou potřebné.




Obr. 4. *Nastavení serveru RADIUS.*

Nejdříve se pak na přepínači nastaví nové připojení k serveru, nastavení autentizace případně nastavení autentizace pro skupinu. Nakonec bude vybrán port a zvolí se možnost kontroly na portu.

| | |
|---|---|
| S1(config)#aaa new-model | //Zapnout technologii AAA. |
| S1(config)#radius-server host 192.168.1.15 | //Konfigurace IP adresy serveru RADIUS. |
| S1(config)#radius-server key sovis1 | //Konfigurace klíče serveru RADIUS. |

| | |
|---|---|
| S1(config)#aaa authentication dot1x default | //Definování autentizační metody. |
| S1(config)#aaa authentication dot1x group skupina | //Definování autentizační metody pro skupinu. |
| S1(config)#dot1x system auth-control | //Globální zapnutí mechanismu 802.1x |
| S1(config)#interface Fa0/15 | Vstup do konfigurace rozhraní. |
| S1(config-if)#port-control auto | //Autentizace 802.1x na daném rozhraní. |
| S1(config-if)#port-control force-authorized | //Nepoužívat 802.1x, ale rozhraní bude autorizováno |
| S1(config-if)#port-control force-unauthorized | //Nepoužívat 802.1x, neautorizovat. |

Pro nastavení řízení broadcast bouří bude stačit pouze jeden příkaz. Nastavení provedeme pro dané rozhraní.

| | |
|---|---|
| S1(config)#interface Fa0/3 | Vstup do konfigurace rozhraní. |
| S1(config-if)#storm-control broadcast level 50 | Spuštění storm-control na daném rozhraní po dosažení hodnoty 50. |

# 8 NÁVRH ZABEZPEČENÍ VRSTVY 3

Konfigurace přístupových listů. Nejprve se ukáže na standardní přístupové listy, které se umisťují co nejblíže k jejich cíli.

| | |
|---|---|
| [1-99 \| 1300-1999] | Rozlišení pomocí čísel. |
| [permit \| deny \| remark] | Zvolí vykonávanou akci, povolit, zakázat, komentář. |
| [A.B.C.D \| any \| host] | Zvolí se adresa sítě, libovolný uživatel nebo konkrétní uživatel. |
| Router(config)#access-list 30 permit 192.168.1.0 0.0.0.255 | Povolení provozu z dané adresy sítě, zadává se s wildcard maskou. |

Aplikace standardního přístupového listu na daný interface.

| | |
|---|---|
| Router(config)#interface Gi0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#ip access-group 30 [in\|out] | Aplikace vytvořeného seznamu na dané rozhraní na vstup nebo výstup. |

Rozšířené přístupové listy pracují s mnoha informacemi v hlavičkách paketů 3. a 4. vrstvy modelu TCP/IP. Může se tak porovnávat cílová či zdrojová IP adresa, číslo portu a typ protokolu. Dají se tak vytvořit přesná pravidla pro příchozí i odchozí provoz. Jejich aplikace je stejná jako u standardních.

| | |
|---|---|
| [100-199 \| 2000-2699] | Rozlišení pomocí čísel. |
| [permit \| deny \| remark \| dynamic] | Zvolení vykonávané akce povolit, zakázat, komentář nebo dynamický seznam. |
| [protokol ] | Po zvolení akce vybereme protokol. |
| [A.B.C.D \| any \| host] | Zadání zdrojové IP adresy, adresa sítě, libovolný uživatel nebo konkrétní uživatel. |
| [A.B.C.D \| any \| host \| služby ] | Cílová ip adresa, adresa sítě, libovolný uživatel, |

| | |
|---|---|
| [služby ]<br>[protokoly a aplikace ]<br>Router(config)#access-list 180 deny tcp any host 192.168.1.15 eq telnet | konkrétní uživatel, další nabídka.<br>Zvolí se služba.<br>Číslo portu, název aplikace či protokolu.<br>Ukázka celého příkazu, který zakazuje připojení přes TELNET s touto adresou. |

Tato konfigurace rozšířeného přístupového seznamu zakazuje všem uživatelům přístup k zařízení s adresou 192.168.1.15 přes protokol TELNET.

Pojmenované přístupové seznamy, jedná se buď o standardní, nebo rozšířené přístupové seznamy, ale jejich konfigurace a aplikace probíhá odlišně. Umožňují používat názvy místo čísel a poskytují tak správcům sítě lepší orientaci ve vytvořených přístupových seznamech.

| | |
|---|---|
| Router(config)#ip access-list standard IT_ONLY<br>[standard \| extended \| logging]<br>[1–99 \| WORD]<br>Router(config-std-nacl)#permit host 192.168.0.25<br>Router(config)#interface Gi0/0<br>Router(config-if)#ip access-group IT_ONLY in | Vytvoření pojmenovaného přístupového seznamu.<br>Zvolím si, který přístupový seznam chci.<br>Označení seznamu.<br>Pravidlo přístupového senamu.<br>Vstup do konfigurace rozhraní.<br>Aplikace pojmenovaného přístupového seznamu na vstup. |

Pro přehled při nastavování je dobré využívat znak „?“, díky kterému se zobrazí všechny možné pokračování příkazu.

Následně se nakonfigurují přístupové seznamy v simulované síti. Jsou jistá doporučení, která by se měla dodržovat [11]. Tak budou předvedeny na simulovaném směrovači.

| | |
|---|---|
| Router(config)#access-list 80 deny ip 10.0.0.0 0.255.255.255 any | Zakázat všechny adresy z rozsahu třídy A. |
| Router(config)#access-list 80 deny ip 172.16.0.0 0.15.255.255 any | Zakázat všechny adresy z rozsahu třídy B. |
| Router(config)#access-list 80 deny ip 192.168.0.0 0.0.255.255 any | Zakázat všechny adresy z rozsahu třídy C. |
| Router(config)#access-list 80 deny ip 127.0.0.0 0.255.255.255 any | Zakázat všechny adresy smyček. |
| Router(config)#access-list 80 deny ip 224.0.0.0 15.255.255.255 any | Zakázat adresy pro multicast vysílání. |
| Router(config)#access-list 80 deny ip 0.0.0.0 0.255.255.255 any | Zakázat síťové adresy. |
| Router(config)#access-list 80 deny ip host 255.255.255.255 any | Zakázat broadcast adresu. |
| Router(config)#access-list 80 permit icmp any host 188.246.111.254 unreachable | Povolit ICMP zprávu Unreachable z Internetu na veřejnou IP adresu. |
| Router(config)#access-list 80 permit icmp any host 188.246.111.254 source-quench | //Povolit ICMP source-quench z Internetu na veřejnou IP adresu. |
| Router(config)#access-list 80 permit icmp any host 188.246.111.254 echo-reply | Povolit ICMP zprávu echo-reply z Internetu na veřejnou IP adresu. |
| Router(config)#access-list 80 deny icmp any any | Zakázat ostatní zprávy ICMP z Internetu na jakoukoliv zdrojovou IP adresu. |
| Router(config)#interface Gi0/1 | Vstup do konfigurace rozhraní. |
| Router(config-if)#ip access-group 80 in | Aplikace rozšířeného přístupového seznamu v příchozím směru. |

Další zabezpečení je proti smurff attack, program Cisco Packet Tracer toto nastavení ale nepodporuje. Bude tak ukázáno nastavení, které funguje v reálné síti [12].

| | |
|---|---|
| Router(config)#interface Gi0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)# no ip directed-broadcast | //Zakázat všesměrové vysílání. |
| Router(config-if)# ip verify unicast source reachable-via rx allow-default | //Kontrola odchozího rozhraní s rozhraním, na které byl paket přijat a využívá výchozí cesty. |

Následuje zabezpečení TCP Synchronizace, nastaví se IP přístupový seznam a dále bude nastaveno pravidlo s klíčovým slovem „established“, které má nastavený příznak ACK. Tento seznam se pak aplikuje na dané rozhraní a zapne režim sledování s upraveným časem pro čekání na dokončení spojení.

| | |
|---|---|
| Router(config)#ip access-list extended prevent | Vytvoření rozšířeného přístupového seznamu. |
| Router(config-ext-nacl)#permit tcp any 1.0.0.0 0.255.255.255 established | Vytvoření pravidla rozšířeného seznamu. |
| Router(config-ext-nacl)#exit | Návrat o úroveň. |
| Router(config)#interface Gi0/0 | Vstup do konfigurace rozhraní. |
| Router(config-if)#ip access-group prevent in | Aplikace přístupového seznamu na vstup daného rozhraní. |
| Router(config)#ip tcp intercept mode watch | Nastavení sledování. |
| Router(config)#ip intercept watch-timeout 20 | Nastavení sledování na 20 vteřin. |

Pro nastavení mechanismu CBAC je nutné zvolit rozhraní, na toto rozhraní definovat přístupový seznam IP a poté konfigurovat hodnoty. Jelikož tento mechanismus nepodporuje program Cisco Packet Tracer, budou příkazy alespoň pro představu jak zapnout tento mechanismus, vypsány.

| | |
|---|---|
| Router(config)#ip inspect name test ftp timeout 3600 | //Zapnutí mechanismu CBAC. |
| Router(config)#interface Gi0/0 | Vstup do konfigurace rozhraní. |

| | |
|---|---|
| Router(config-if)#ip inspect test in | Aplikace inspekce s daným názvem na vstupu. |

Ještě bude zabezpečen přístup ke směrovači přes protokol SSH, aby mohl být směrovač na dálku spravován [13].

| | |
|---|---|
| Router(config)#ip ssh time-out 10 | Nastavení časového intervalu pro SSH. |
| Router(config)#ip ssh authentication-retries 3 | Počet pokusů o přihlášení 3. |
| Router(config)#ip ssh version 2 | Verze protokolu SSH. |
| Router(config)#ip domain-name sovis.cz | Přiřazení názvu domény pro přístup přes SSH. |
| Router(config)#crypto key generate rsa | Vygenerování RSA klíče, pro SSH(1024 bitů). |
| Router (config)#aaa authentication login SSH group tacacs+ local | //Vytvoření pojmenovaného seznamu autentizačních metod. |
| Router (config)#ip access-list standard IT | Vytvoření přístupového seznamu. |
| Router (config-std-nacl)#permit 192.168.2.0 0.0.0.255 | Pravidlo pro povolený přístup pouze IT oddělení. |
| Router (config-std-nacl)#exit | Návrat o úroveň. |
| Router (config)#line vty 0 1 | Vstup do konfigurace vzdáleného přístupu. |
| Router (config-line)#login authentication SSH | //Aplikace vytvořeného seznamu. |
| Router (config-line)#transport input ssh | Povolí připojení pouze protokolem SSH. |
| Router (config-line)#transport output none | Zakázat jakékoliv odchozí spojení. |
| Router (config-line)#access-class IT in | Aplikace vytvořeného přístupového listu. |
| Router (config-line)#exit | Návrat o úroveň. |

Na konec budou vypsány důležité příkazy pro výpisy informací.

| | |
|---|---|
| Router #show running-config | Výpis běžící konfigurace. |
| Router #show startup-config | Výpis startovací konfigurace. |
| Router #show interfaces | Výpis rozhraní. |
| Router #show ip interface | Výpis informací o daném rozhraní. |
| Router #show ip interface brief | Stručný seznam všech rozhraní. |
| Router #show privilege | Úroveň oprávnění. |

| | |
|---|---|
| Router #show users | Vypíše informace o přihlášených uživatelích. |
| Router #show version | Vypíše informace o zařízení. |
| Router #show ip protocols | Výpis použitého směrovacího protokolu. |
| Router #show ip route | Výpis směrovací tabulky. |
| Router #show access-list | Zobrazení všech přístupových seznamů. |
| S1#show vlan | Informace a VLAN. |
| S1#show interface trunk | Informace o trunk rozhraní. |
| S1#show ip interface brief | Informace o všech rozhraních na zařízení. |
| S1#show mac address-table | Zobrazí tabulku MAC adres. |
| S1#show port-security | Informace o Port Security. |
| S1#show ip arp inspection | Informace funkce DAI. |
| S1#show spanning-tree | Informace o STP pro každou VLAN. |

# ZÁVĚR

Cílem této práce bylo navržení a otestování běžného zabezpečení aktivních prvků firmy Cisco. Nejprve byla zpracována literární část a seznámení se síťovými hrozbami a zabezpečením. Poté následovalo seznámení se s nastavením směrovačů a přepínačů. Pro návrh zabezpečení byla vytvořena demonstrativní topologie firemní sítě. Po přidělení adresních prostor se rozdělili VLAN a bylo zahájeno testování. Práce probíhala od navržení až po testování v simulačním programu Cisco Packet Tracer verze 7.0.0.0306. Program však nepodporuje řadu příkazů a tak jsou některé pasáže sepsány pouze pro reálná zařízení.

Výsledkem této práce je celistvý materiál, který lze využít pro výuku či zabezpečení přivátní sítě s využitím aktivních prvků firmy Cisco. Díky tomuto materiálu je možné zabezpečit síť proti běžným útokům a škodolibým pokusům o penetraci do sítě. Pokud by byl vznesen požadavek na dokonalejší zabezpečení, lze jej taktéž dosáhnout pomocí přístupových seznamů, avšak v podstatně větším rozsahu, než byl použit v této práci.

## SEZNAM POUŽITÉ LITERATURY


[1] *Cisco Systems (Czech Republic), s.r.o.: Profil společnosti Cisco.* [online]. [cit. 2017-05-01]. Dostupné z: http://www.czechict.cz/clenstvi/aktuality-o-clenech/cisco-systems-czech-republic-sro.htm

[2] *2015 Letter to Shareholders*. [online]. 2015 [cit. 2017-05-01]. Dostupné z: http://www.cisco.com/c/en/us/about/annual-reports/annual-report-2015/letter.html

[3] LAMMLE, Todd. *CCNA: výukový průvodce*. Vyd. 1. Brno: Computer Press, 2015. ISBN 978-80-251-4602-6.

[4] SEAN WILKINS, Sean. *TACACS+ vs. RADIUS: Similarities and Differences*. [online]. 2015 [cit. 2017-05-01]. Dostupné z: http://www.pearsonitcertification.com/articles/article.aspx?p=2449614

[5] WOLAND, Aaron. *RADIUS versus TACACS+: An explanation and comparison of RADIUS and TACACS+ for Authentication, Authorization and Accounting (AAA)*. [online]. 2014 [cit. 2017-05-01]. Dostupné z: http://www.networkworld.com/article/2838882/radius-versus-tacacs.htm

[6] *TACACS+ and RADIUS Comparison*. [online]. 2008 [cit. 2017-05-01]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

[7] LAMMLE,T. *CCNA: Výukový průvodce přípravou na zkoušku 640–802*. Vyd. 1. Brno: Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.

[8] WENSTROM, M. *Zabezpečení sítí Cisco*. Autorizovaný výukový průvodce. Vyd. 1 Brno: Computer Press, 2003. 753 s. Cisco Systems. ISBN 80-722-6952-6.

[9] *Cisco Networking Academy* [online]. [cit. 2017-05-15]. Dostupné z: https://www.netacad.com

[10] VACHON, Bob. *CCNA security portable command guide*. Second edition. Cisco press, 2016, 322 s. ISBN 1587205750.

[11] ODOM, Wendell. a Rick. MCDONALD. *Routers and routing basics: CCNA 2 companion guide.* Vyd. 2. Indianapolis: Cisco Press, 2007. ISBN 978-1-58713-166-0.

[12] *Unicast reverse path forwarding*. [online]. [cit. 2017-05-15]. Dostupné z: http://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

[13] EMPSON, Scott. *CCNA kompletní přehled příkazů: autorizovaný výukový průvodce.* Vyd. 1. Brno: Computer Press, 2009. ISBN 978-80-251-2286-0.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| ACE | Application Control Engine |
| ACK | Acknowledge |
| ACL | Access Control List |
| ACS | Access Control System |
| ARP | Address Resolution Protocol |
| BGP | Border Gateway Protocol |
| BPDU | Bridge Protocol Data Units |
| CAM | Content Addressable Memory |
| CBAC | Context-Based Access Control |
| CDP | Cisco Discovery Protocol |
| DAI | Dynamic ARP Inspection |
| DDoS | Distributed Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |
| DMVPN | Dynamic Multiport VPN |
| DTP | Dynamic Trunking Protocol |
| EAP | Extensible Authentication Protocol |
| EIGRP | Enhanced Interior Gateway Routing Protocol |
| FTP | File Transfer Protocol |
| GRE | Generic Routing Encapsulation |
| HTTP | Hypertext Transfer Protocol |
| CHAP | Challenge Handshake Authentication Protocol |
| IANA | Internet Assigned Numbers Authority |
| ICMP | Internet Control Message Protocol |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IOS | Internetwork Operating System |
| IP | Internet Protocol |
| MAC | Media Access Control |
| NAS | Network Access Server |

| | |
|---|---|
| NHRP | Next Hop Resolution Protocol |
| ODR | On-Demand Routing |
| OSPF | Open Shortest Path First |
| PAP | Password Authentication Protocol |
| PPP | Point to Point Protocol |
| RADIUS | Remote Authentication Dial In User Service |
| Rat | Router audit tool |
| RFP | Reverse Path Forwarding |
| RIP | Routing Information Protocol |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| STP | Spanning-Tree Protocol |
| SYN | Synchronization |
| TACACS | Terminal Access Controller Access-Control System |
| TCP | Transmission Control Protocol |
| TELNET | Telecommunication Network |
| TFTP | Trivial File Transfer Protocol |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| VTP | VLAN Trunking Protocol |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK