Mendelova univerzita v Brně
Provozně ekonomická fakulta

Návrh univerzitního firewallu na platformě Cisco

Diplomová práce

Vedoucí práce:
Ing. Martin Pokorný, Ph.D.

Bc. Jan Burian

Brno 2016

Rád bych poděkoval svému vedoucímu, panu Ing. Martinovi Pokornému, Ph.D., za odborné rady a trpělivost v průběhu zpracování této práce. Poděkování patří také mé rodině za celkovou podporu a především bych chtěl poděkovat mé přítelkyni Ing. Lence Navrátilové, za to, že mi v tomto období byla nesmírnou oporou.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Návrh univerzitního firewallu na platformě Cisco**
vypracoval samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*
Jsem si vědom, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.
Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 4. ledna 2017 .....

Abstract

Burian, J. The desing of university firewall on Cisco platform. Diploma thesis. Brno, 2016.

The diploma thesis focuses on design of university firewall on Cisco platform. The design deals with important functionalities, which are used in the current solution. These include routing, network address translation, access control lists, VPN. The thesis furher deals with dynamic insertion rules, which are generated based on traffic analysis by Flowmon probe and its ADS module. The new design is implemented in a testing environment and its funcionality is verified. The thesis will serve like feasibility study for final implementation in the production MENDELU network.

Keywords
firewall, iptables, Cisco ASA, NAT, VPN, routing, ACL, Flowmon, ADS

Abstrakt

Burian, J. Návrh univerzitního firewallu na platformě Cisco. Diplomová práce. Brno, 2016.

Tato diplomová práce se zaměřuje na návrh univerzitního firewallu na platformě Cisco ASA. Návrh obsahuje důležité funkcionality, které jsou využívány na aktuálním řešení. Patří mezi ně směrování, překlad adres, přístupová pravidla, VPN. Práce se dále věnuje dynamicky vkládaným pravidlům, které jsou generovány na základě analýzy provozu na Flowmon sondě a jeho ADS modulu. Nový návrh je implementován v testovacím prostředí a jeho funkčnost ověřena. Práce bude sloužit jako studie proveditelnosti pro finální implementaci v produkční síti MENDELU.

Klíčová slova
firewall, iptables, Cisco ASA, NAT, VPN, routing, ACL, Flowmon, ADS

Obsah

1 Úvod

Otázka bezpečnosti, nejen síťové infrastruktury, ale celkové kybernetické bezpečnosti, je stále zásadnější a při návrhu řešení hraje velkou roli. Je tedy důležité tuto část nepodcenit, aby infrastruktura byla schopná čelit neustále narůstajícímu počtu kybernetických útoků, ať se již jedná o automatizované útoky, kterých je na Internetu nepřeberné množství, či cílené útoky za účelem získat požadované informace nebo pouze znemožnit přístup legitimním uživatelům.

Základní prvek, který by měl pomáhat s bezpečností počítačové sítě, je firewall. Právě tento prvek je nasazován na perimetru sítě a on je stavěn do pozice, kdy se musí vypořádat s největším množstvím legitimního či zákeřného provozu, který přichází z vnější sítě. Díky němu je povolen přístup uživatelům ke zdrojům, ke kterým skutečně mají mít přístup. Firewall nám také poskytuje další užitečné funkcionality, jako např. vzdálený přístup pro uživatele, bezpečné propojení vzdálených lokalit, prevence před vniknutím do sítě nebo možnost kontroly provozu i proti virům.

Role firewallu v počítačové síti se zvyšuje s počtem uživatelů, kteří využívají služeb v této síti, a také podle zajímavosti informací, které mohou být získány. V univerzitní síti MENDELU momentálně studuje přes 10 500 studentů a pracuje zde přes 1 500 zaměstnanců. Tito lidé každý den využívají různé služby, které jsou na univerzitě k dispozici (přístup k univerzitnímu informačnímu systému, Wi-Fi připojení, stravování, dohledový systém a další). Z tohoto důvodu musí být firewall spolehlivý, aby byl dostupný po celou dobu (vysoká dostupnost). Výkonný, aby zvládal odbavit velké množství různých požadavků. A samozřejmě bezpečný a aktualizovaný, aby neobsahoval známé zranitelnosti. Samozřejmě je vhodné znát možnosti, které jsou s ohledem na bezpečnostní řešení v počítačové síti nabízeny. A jelikož Mendelova univerzita v Brně má k dispozici platformu Cisco ASA, bude vypracována alternativa k univerzitnímu firewallu na tomto zařízení.

Téma ohledně firewallů a Cisco ASA platformy jsem si vybral z důvodu, že problematika bezpečnosti počítačových sítí mne zajímá a mám zájem se v této oblasti více rozvíjet. O to více bylo zajímavé řešit tuto problematiku pro takovou velkou síť, kde má firewall velice důležitou roli, a poodkrýt komplexnost takovéto sítě.

2 Cíl práce

Primárním cílem této práce je navrhnout a implementovat nové řešení firewallu na platformě Cisco ASA. Pro dosažení tohoto primárního cíle je potřeba splnit dílčí cíle mezi které patří obeznámení se s problematikou firewallů na platformě Linux a Cisco. Dále analýzy stávajícího řešení firewallu v počítačové síti Mendelovy univerzity v Brně včetně uživatelských požadavků na řešení nové. A zaměřit se zejména na technologie routingu, firewallu, dynamicky vkládaných pravidel, VPN a NAT. Po této analýze již navrhnout řešení nové na platformě Cisco ASA, provést implementaci nového řešení a také ověřit funkčnost tohoto řešení. A celkové řešení ekonomicky zhodnotit.

3 Analýza uživatelských požadavků

V této kapitole bude zaměřeno na body, které jsou požadovány v rámci této práce. Tyto požadavky byly navrženy a diskutovány se zaměstnanci Ústavu informačních technologií.

3.1 Migrace současné konfigurace na platformu Cisco ASA

Mezi základní požadavky patří migrace konfigurace z aktuálního řešení na řešení nové, které bude postaveno na platformě Cisco ASA. Při migraci je zapotřebí zachovat nynější funkcionalitu a především nesmí být snížena bezpečnost Mendelovy univerzity na novém řešení, a proto nastavení bude nutné ověřit v testovacím prostředí. Migrace se bude týkat základního nastavení, směrování, ACL pravidel, VPN a NAT.

3.2 Virtual Private Network

Site-to-Site VPN Tauferovy koleje

Na novém řešení bude potřeba provést implementaci Site-to-Site VPN, která využívá technologii IPSec a spojuje univerzitní síť se vzdálenou sítí Tauferových kolejí. Přes tento tunel prochází provoz uživatelů, kteří jsou ubytování na těchto kolejích, zaměstnanců a komerčních subjektů.

Remote Access VPN

Z důvodu již zastaralé technologie VPN koncentrátoru, který již nesplňuje požadavky uživatelů Mendelovy univerzity a omezené funkčnosti technologie na novějších operačních systémech Windows, je zapotřebí provést inovaci.

Proběhne analýza možných řešení Remote Access VPN technologií, které se dají využít na platformě Cisco ASA. Analýza proběhne jak z pohledu uživatelské přívětivosti, tak i finační náročnosti.

3.3 Směrování

Na univerzitním firewallu se využívá především statický routing. Dynamický routing zde využíván v této chvíli není. Ale je zde nakonfigurován Policy Based Routing, u kterého je možnost definovat cestu paketů na základě zdrojové adresy/sítě. Protože v síti MENDELU jsou různé druhy provozu, které jsou určeny pro jiné poskytovatele internetového připojení, je důležité tuto funkcionalitu zachovat a naimplementovat na platformě Cisco ASA.

3.4 Network Address Translation

Univerzitní firewall se také stará o překlad adres pomocí řetězců PREROUTING a POSTROUTING, které jsou dostupné na iptables. Samozřejmě tato funkcionalita musí být implementována i na platformě Cisco ASA. Je zde např. řešen překlad zdrojových a cílových adres, když uživatel nemá mít přístup k Internetu, nebo přesměrování provozu na jiné servery na základě portu.

3.5 Přístupová pravidla

Momentálně jsou pravidla na univerzitním firewallu naimplementována v podobě iptables. Bude tedy potřeba tyto pravidla přemigrovat do podoby pro platformu Cisco ASA. A také provést návrh týkající se dynamicky vkládaných pravidel pomocí propojení FlowMon sondy a Cisco ASA zařízení (viz níže).

3.6 Monitoring sítě

V síti Mendelovy univerzity je nasazena FlowMon sonda, která je určena pro monitoring a analýzu provozu v počítačové síti a upozorňuje na různé incidenty, útoky a abnormality. Pro zvýšení bezpečnosti sítě Mendelovy univerzity se nabízí propojení tohoto řešení s platformou Cisco ASA, aby reakce na incidenty byly flexibilnější.

3.7 Anonymizace citlivých údajů

Tato práce se věnuje citlivému tématu z oblasti bezpečnosti. Jelikož bude veřejná, je zapotřebí provést anonymizaci citlivých údajů, aby např. potencionální útočník neměl zjednodušenou práci. Mezi hlavní údaje, které bude nutné anonymizovat, jsou IP adresy a VLAN ID.

Také je potřeba anonymizovat informace ohledně přístupových pravidel. Především pravidla, která povolují průchozí provoz. Budou zde použita pouze modelová pravidla.

4 Metodika

Pro úspěšné splnění cílů, které jsou definovány pro tuto diplomovou práci, bude zapotřebí se řídit těmito kroky:

1. Seznámit se podrobně s problematikou firewallů a technologiemi, které se využívají v této souvislosti. Pro splnění tohoto kroku bude zapotřebí nastudovat literaturu, která se danou problematikou zabývá. Mezi tuto literaturu patří především RFC dokumetace a ostatní odborná literatura. Bude se jednat zejména o technologie routingu, překladu síťových adres (NAT), virtuální privátní sítě (VPN), firewallů a možnosti dynamicky vkládaných pravidel. Poznatky, které budou nabyty studiem literatury, poté budou sepsány do jedné z následujících kapitol.

2. Zmapovat aktuální stav řešení v počítačové síti MENDELU, aby bylo možné správně navrhnout řešení nové. Analyzovat potřebné uživatelské požadavky pro uplatnění v novém řešení. Tato analýza proběhne ve spolupráci se zaměstnanci Ústavu informačních technologií na MENDELU.

3. Poté proběhne analýza již existujících bakalářských prací, diplomových prací a také oficiálních publikací, které jsou zaměřeny na stejné či podobné téma. Podklady budou vyhledány na základě definovaných klíčových slov na specializovaném serveru pro závěrečné práce a také v rámci Internetu. Díky této analýze budou získány nové poznatky a budou moci být využity v této diplomové práci.

4. Pomocí získaných poznatků z předchozího studia závěrečných prací a odborné literatury bude dalším krokem navrhnout nové řešení firewallu pro počítačovou síť MENDELU, které bude postavené na platformě Cisco ASA, a to včetně technologií, které k univerzitnímu firewallu patří (NAT, VPN, ACL).

5. Bude následovat implementace navrženého řešení v podmínkách síťové laboratoře ÚI PEF MENDELU, případně v síťovém simulátoru GNS3. Z tohoto kroku poté vyplyne studie proveditelnosti, která bude sloužit pro finální implementaci v produkční síti MENDELU.

6. U implementovaného řešení v síťové laboratoři proběhne otestování hlavních funkcionalit pro zjištění, zda je model správně naimplementován a může být použit v produkční síti MENDELU.

7. Součástí této diplomové práce bude i ekonomické zhodnocení řešení.

5 Popis technologického aparátu

5.1 Základní pojmy

V této kapitole bude uveden teoretický základ, který je potřebný pro pochopení problematiky bezpečnosti na perimetru sítě. Budou uvedeny technologie, které jsou na bezpečnostním prvku zde na univerzitě. Následně budou popsány prerekvizity pro úspěšné nakonfigurování a nasazení prvku do produkčního prostředí.

Internet Protocol (IP)

Dle RFC 791 (1981) byl tento protokol navržen pro propojení počítačových systémů a možnost mezi sebou komunikovat. Pracuje na třetí vrstvě modelu ISO/OSI. Dnes jsou nejznámější protokoly IPv4 a IPv6. IPv4 se týká zmíněný dokument RFC 791 (1981) a IPv6 je popsán v RFC 2460 (1998). Oba protokoly byly i aktualizovány a v rámci aktualizací vznikly i navazující RFC dokumentace, ale pro tuto práci nejsou podstatné.

V rámci této práce jsou nejvíce zajímavé informace z paketu týkající se zdrojové a cílové adresy IP paketu. Díky těmto informacím je možnost filtrovat pakety mezi jednotlivými sítěmi.

Transmission Control Protocol (TCP)

Tento protokol je popsán v RFC 793 (1981) a stará se o navázání spojení mezi dvěma hosty a pracuje nad vrstvou IP, tedy na čtvrté vrstvě ISO/OSI modelu. Jedná se o spojově orientovaný a spolehlivý protokol, který se využívá pro přenos dat, u kterých je vyžadována spolehlivost. Mezi aplikace, které využívají TCP patří např. e-mailová komunikace, HTTP/S přenos, přenos souborů, SSH a další.

Na firewallu k filtrování provozu jsou využity informace o zdrojovém a cílovém portu. Stavové firewally jsou pomocí příznaků schopny určit, zda se jedná o nové spojení nebo již existující.

User Datagram Protocol (UDP)

Specifikace tohoto protokolu je popsána v RFC 768 (1980). Protokol UDP je jako TCP protokol určen pro přenos dat, ale oproti TCP nenavazuje spojení předem a označuje se jako nespolehlivý. Datagramy mohou dorazit v jiném pořadí či vůbec nedorazit. Tento protokol je vhodný pro streamování videa či zvuku. U UDP se pro potřeby filtrování využivá pouze zdrojový a cílový port.

Virtual Local Area Network (VLAN)

Bouška (2007a) uvádí, že VLAN je technologie, která umožňuje logicky rozdělit síť bez ohledu na její fyzické propojení. Díky VLAN je možnost snížit velikost broadcast domén rozdělením na menší broadcast domény, dále umožňuje zjednodušení správy

sítě, zvýšení bezpečnosti a také oddělení speciálního provozu od zbytku sítě (např. management sítě). VLAN jsou v dnešních sítích vysoce rozšířené a vznikl standard IEEE 802.1q.

Směrování

Směrování se využívá pro spojení jednotlivých sítí. Se směrováním je možnost se setkat na L3 přepínačích, směrovačích i firewallech.

Mezi nejzákladnější typ směrování patří statické směrování, kde se manuálně určí, jaké cílové sítě se budou směrovat přes daný next-hop (např. adresa sousedního směrovače, ke kterému je potřeba zaslat pakety). Speciálním záznamem ve směrovací tabulce je default route. Tento záznam se použije, když není definovaná specifičtější cesta.

Dále existuje dynamické směrování, které na základě algoritmů přepočítává cesty, kudy pakety potečou. Reaguje na změny v síti. Protokolům dynamického směrování se v této práci věnovat nebude, jelikož zde nebudou využity. (Bouška 2007b)

Co naopak bude využito, tak je směrování na základě politik (Policy Based Routing - PBR). RFC 1104 (1989) uvádí, že se jedná o směrování, které nemusí být podmíněno pouze na základě cílové sítě, ale i např. zdrojové sítě, zdrojového portu či cílového portu.

VRF (Virtual Routing and Forwarding)

Cisco.com (2014a) uvádí, že se jedná o IP technologii, která umožňuje mít více instancí směrovací tabulky na stejném směrovači ve stejný okamžik. Jelikož jsou směrovací instance nezávislé, mohou být v těchto tabulkách stejné nebo překrývající se IP adresy, aniž by zde vznikl nějaký konflikt.

Network Address Translation (NAT)

Funkce NAT vznikla v důsledku blížícího se vyčerpání IPv4 adres. Zavádí privátní rozsahy adres, tzv. třídy, které se nemohou objevit na veřejném Internetu.

Díky NATu také mírně roste bezpečnost, protože IP adresa počítače není přímo viditelná. Mezi nevýhody patří to, že některé aplikace mohou mít problém při komunikaci se stroji, které jsou přístupné za NATem.

Tato funkce se konfiguruje na zařízeních, která se nachází na perimetru sítě, jako jsou směrovače či firewally. Existují různé typy této technologie. NAT je možné rozdělit podle adresy, která se bude překládat:

- SNAT (Source NAT): tato varianta je více využívána. Dochází zde k překladu zdrojové adresy paketu.
- DNAT (Destination NAT): tento typ se používá, když je paket cílen do sítě s privátním adresním rozsahem. (Mikrotik.com 2016)

Dále je možné NAT rozdělit podle způsobu mapování adres při překladu:

- Statický NAT: mapuje IP adresy na bázi jedna ku jedné. Využívá se u zařízení, která potřebují být přístupná z vnější sítě.
- Dynamický NAT: mapuje IP adresy z definované skupiny IP adres.
- Port Address Translation (PAT): nejčastější forma NATu v dnešních sítích. Dochází zde k překladu mnoha privátních adres na jednu veřejnou, ale v tabulce překladů si zařízení udržuje čísla portů k adrese a díky tomu pozná, ke komu se provoz váže. Tento typ se také nazývá NAT *overload*. (Tyson 2001)

Virtual Private Network (VPN)

Technologie VPN se dělí na dvě hlavní skupiny: Site-to-Site a Remote-Access. První zmíněná slouží pro propojení jednotlivých vzdálených lokalit mezi sebou. Druhá zmíněná slouží pro připojení jednotlivých uživatelů do firemní sítě, aby mohli využívat firemní zdroje. Obě varianty mají více protokolů a možností, jak nadefinovat a naimplementovat spojení. (Frahim 2014)

VPN typu site-to-site slouží k propojení dvou vzdálených sítí, mezi kterými je potřeba provádět bezpečný přenos informací. Typický příklad je hlavní pobočka (centrála) a k ní se pomocí privátního tunelu připojí jednotlivé pobočky.

K dispozici je několik protokolů, které mohou být využity pro propojení dvou sítí. Mezi nejpoužívanější patří IPSec (Internet Protocol Security). Tento protokol se pro větší bezpečnost využívá i v kombinaci s některými staršími technologiemi. (Frahim 2014)

Mezi výhody těchto typů VPN patří pořizovací cena a jednoduchost nasazení. Nicméně existují i další možnosti, jak vzdálené lokality propojit. Jedná se o propojení na úrovni poskytovatele internetového připojení. Tato technologie se nazývá MPLS (MultiProtocol Label Switching) a existují tři způsoby, které je možné pro spojení využít:

- L3 VPN: tato VPN pracuje na třetí vrstvě referenčního modelu ISO/OSI, využívají se zde dynamické směrovací protokoly jako jsou BGP a OSPF a poskytovatel připojení zde propaguje IP prefixy sítí mezi routery zákazníka. Tyto VPN jsou zajímavé pro zákazníky, kteří chtějí přenechat břemeno ohledně Site-to-Site routingu na poskytovateli připojení.
- L2 VPN: poskytovatel připojení propojuje sítě zákazníka skrz L2 technologii. Příkladem jsou ATM, Frame Relay nebo Ethernet.
- VPLS (Virtual Private LAN Service): u této technologie vypadá síť internetového poskytovatele jako jeden switch. A zákazník díky tomu může mít svoji vzdálenou lokalitu připojenou jako kdyby se nacházela ve stejné lokalitě.

K výhodám MPLS VPN patří, že o nastavení se postará poskytovatel připojení, dále možnost propojit různé protokoly a jednoduchost jeho požívání. Nevýhodou mohou být cenové podmínky. (Doyle 2008)

VPN typu Remote Access slouží pro připojení uživatelů do firemní sítě a existuje celá řada VPN protokolů, které se dají využít:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Layer 2 Forwarding (L2F) Protocol
- IPsec
- L2TP over IPsec
- Secure Sockets Layer (SSL) VPN

Platforma Cisco ASA podporuje tyto čtyři typy:

- IPsec
- L2TP over IPsec
- Bezklientní Remote-Access SSL VPN
- Klientský Remote-Access SSL VPN (Frahim 2014)

IPsec (Internet Protocol Security)

IPsec je rozšíření pro zabezpečení IP datagramů. Nejedná se o standard, ale o sadu protokolů, které mohou být použity, aby provoz byl ochráněn např. před odposlechem či změnou dat. IPsec je popsán ve starším RFC 2411 a v novějším RFC 6071. V těchto RFC se nachází přehled možných protokolů, jejich kratší popis a hlavně odkazy na další RFC, které se zabývají daným protokolem více do hloubky. (RFC 6071)

Při návrhu implementace IPsec jsou zajímavé především tyto body:

- Protokol: mezi dva hlavní protokoly IPsec patří AH (Authentication Header) a ESP (Encapsulating Security Payload). AH se stará pouze o ověření paketů a ESP o ověření a šifrování paketů.
- Transportní mód: k dispozici dva transportní módy a liší se tím, co bude v paketu zašifrováno. Transportní mód se stará pouze o šifrování obsahu IP paketu, ale ne jeho hlavičky. Tunelovací mód zašifruje celý paket a přidá novou hlavičku. Z paketu nelze zjistit původní odesílatel a příjemce. Druhý uvedený mód je využíván u tradičních VPN.
- Algoritmus autentizace a šifrování: zde je na výběr větší počet možností. Např. MD5, SHA-1, DES, 3DES, AES. Autentizace se stará o výpočet kontrolního

součtu paketu. Obě strany mají dohodnutý způsob výpočtu kontrolního součtu a ověřují, zda paket nebyl po cestě poškozen či úmyslně změněn. Šifrování je nasazeno z důvodu zachování důvěrnosti dat během přenosu.

- Výměna klíčů: mezi stranami, které spolu chtějí komunikovat bezpečně, je potřeba předat tajné hodnoty, které jsou použity pro hashovací funkci nebo pro šifrovací algoritmy. Jedna z možností je výměna klíčů manuálně, která vyžaduje zadání klíče na obou stranách. Druhou možností je použít IKE (Internet Key Exchange). Jedná se o mechanismus automatické výměny klíče. (Friedl 2005)

PPTP (Point-to-Point Tunneling Protocol)

Tento protokol už je poměrně starý (byl integrován již do operačního systému Windows 95). Mezi jeho výhody patří snadná konfigurace a také jeho integrace do mnoha operačních systémů. Již ovšem není považován za bezpečný protokol z důvodu přítomnosti několika známých bezpečnostních zranitelností. Je pravděpodobné, že některé bezpečnostní agentury dokáží provoz s využitím tohoto protokolu odposlouchávat a dešifrovat. Je tedy doporučeno se nasazení tohoto protokolu vyhnout. (Hoffman 2015)

L2TP (Layer 2 Tunneling Protocol)

L2TP je tunelovací protokol, který sám o sobě nenabízí možnosti šifrování komunikace. Z tohoto důvodu je nejčastěji implementován se šifrováním pomocí sady protokolů IPsec. Uvádí se také název L2TP over IPsec. Díky integraci v moderních operačních systémech, které jsou určeny pro osobní počítače nebo i mobilní zařízení, je nasazení tohoto protokolu snadné. Ale jelikož využívá UDP port 500, je snadné ho blokovat na firewallech a uživatelé mohou mít problémy s navázáním tohoto tunelu. (Hoffman 2015)

Bezklientní Remote-Access SSL VPN

Tento typ VPN se stává stále více nasazovaným typem VPN pro uživatele, kteří se potřebují připojit vzdáleně k některým firemním zdrojům a je zapotřebí, aby toto spojení bylo bezpečné. Tento typ VPN využivá Secure Socket Layer (SSL) protokol a pro větší bezpečnost také jeho následovníka, Transport Layer Security (TLS) protokol. Velkou výhodou tohoto řešení je, že uživatel nepotřebuje instalovat žádný speciální program pro navázání spojení, ale postačí mu pouze webový prohlížeč, přes který se přihlásí ke speciální doméně, kde se nachází firemní portál, a po přihlášení má k dispozici zdroje určené danému uživateli. (Cisco.com 2016e)

Klientský Remote-Access SSL VPN

Předchozí zmíněný typ VPN neumožňuje uživateli poskytnout plnohodnotné připojení do počítačové sítě ze vzdáleného stroje a využívat tak veškeré firemní sítě,

jako kdyby byl přímo připojen do sítě na pobočce. Z tohoto důvodu byl zaveden i klientský Remote-Access SSL VPN typ. Využívá se zde protokolů SSL/TLS a je již potřeba speciální program, který si uživatel nainstaluje na svém koncovém zařízení. Po správné autentizaci se uživatelovo zařízení chová jako přímo připojené na pobočce do firemní sítě. Mezi takovýto program může být řazen např. proprietární program AnyConnect Secure Mobility Client od firmy Cisco. (Frahim 2014)

GRE (General Routing Encapsulation)

Umožňuje navázat spojení (tunel) mezi dvěma prvky přes veřejnou síť (Internet). Pro vyšší zabezpečení se užívá kombinace s IPsec. Kde se nejdříve vezme původní paket, zabalí se do GRE enkapsulace a poté je ještě zabalen pomocí IPsec. Výhodou tohoto řešení je, že přes tunel se může zasílat i provoz směrovacích protokolů. Nevýhodou je, že další hlavička paketu přidává režii. (Juniper.net 2014)

5.2 Firewall

Firewall je zařízení, které se stará o kontrolu přístupu mezi jednotlivými zónami počítačové sítě. Zamezuje či povoluje přístup k dané části sítě za daných podmínek (např. dle zdrojové nebo cílové IP adresy, zdrojového nebo cílového portu a dalších parametrů). Hlavní rozdělení zón je na důvěryhodnou a nedůvěryhodnou část, kde za důvěryhodnou zónu je považována interní síť a za nedůvěryhodnou zónu je zpravidla považován Internet. Zóny se také mohou označovat jako inside (interní síť) a outside (Internet). Základem při modelování sítí je i přidání třetí zóny (při správné segmentaci může být zón i více) tzv. demilitarizované zóny. Tato zóna se přidává pro servery (služby) v síti, které mají být přístupné i z Internetu (např. e-mailový server, webový server a další), v případě, že není žádoucí povolovat přístup z Internetu přímo do interní sítě, kde se nacházejí klientské stanice.

Firewall ve většině případů poskytuje více možností a funkcí než pouhé filtrování provozu. Mezi nejrozšířenější funkce patří Network Address Translation (NAT), Virtual Private Network (VPN) a Intrusion Prevention System (IPS). Hlavní typy síťových firewallů:

- Paketové filtry: tyto firewally patří mezi nejstarší typ firewallů, které řídí filtrování na základě některých síťových a transportních informací jednotlivých paketů. Např. zdrojová IP adresa, cílová IP adresa, zdrojový TCP/UDP port a další. Jedná se o bezstavové firewally, protože svoje filtrační pravidla aplikují na jednotlivé pakety, i když se jedná o totožné spojení.
- Stavové firewally: dochází zde k chápání toku paketů jako spojení a může být konrolován i stav paketů. Využívá informace z TCP hlaviček, se kterými může dále pracovat (např. příznaky SYN, ACK, sekvenční čísla). Narozdíl od paketových filtrů pracuje firewall s celým tokem a ne s každým paketem zvlášť.

- Aplikační brány: tento typ bran pracuje na sedmé vrstvě OSI modelu a rozumí příkazům aplikačního protokolu, pro který brána poskytuje služby. Je tu vyžadován specifický software na straně klienta. Typickým příkladem je webový prohlížeč na klientském stroji a protokol HTTP. (Moraes 2011)

5.3 Iptables

Iptables spadá pod framework netfilter.org, který se stará o filtraci paketů. Tento framework se usídlil v linuxovém jádře od verze 2.4.x a je nástupcem ipchains (Linux 2.2.x) a ipfwadm (Linux 2.0.x). Iptables má strukturu tabulky (filtrovací tabulka), ve které se definují jednotlivá pravidla.

Pomocí iptables je možnost vytvářet bezstavové a stavové filtrování, překlad adres (NAT) a to jak na IPv4, tak i pro IPv6. S využitím API je možnost přidat funkcionalitu o rozšíření třetích stran. (Welte a Ayuso, 2014)

Filtrovací tabulka obsahuje řetězce, přes které prochází jednotlivé pakety. Existuje 5 typů řetězců, které je možné v iptables nadefinovat:

- INPUT: vstupní řetězec, pakety určené pro lokální stroj.
- FORWARD: řetězec pro procházející provoz, zařízení musí být nastaveno jako router.
- OUTPUT: výstupní řetězec, pakety vygenerované lokálním strojem.
- PREROUTING: řetězec určený pro zpracování paketů před routováním.
- POSTROUTING: řetězec určený pro zpracování odchozích paketů. (Petříček 2001)

Pomocí iptables je také možnost nakonfigurovat stavový firewall. Tedy firewall, který si vede tabulku spojení a díky tomu je schopen lépe provádět filtraci. Existují tyto stavy:

- NEW: datagram otevírá novou komunikaci.
- ESTABLISHED, RELATED: datagram je součástí již navázaného spojení nebo s ním nějakým způsobem souvisí.
- INVALID: datagram není součástí žádného spojení nebo se jej nepodařilo identifikovat. (Petříček 2002)

Konfigurace pravidel probíhá pomocí příkazové řádky. Použití není složité a syntaxe je srozumitelná. Viz příklad níže:

```
iptables -A FORWARD -s 10.0.0.0/24 -d 10.0.1.0/24 -p tcp --dport
443 -j ACCEPT
```

Je použit příkaz iptables a pomocí přepínáčů se definuje dané pravidlo. V uvedeném příkladu se nachází přepínač -A, který provede přidání pravidla na konec politiky. Klíčové slovo FORWARD označuje název politiky. Dále tu jsou přepínače

-s a -d, které definují zdrojovou a cílovou síť. Také existuje možnost pomocí přepínače -p určit protokol a definovat specifický cílový port s přepínačem –dport. A jako poslední přepínač je uveden přepínač -j, který definuje akci, kterou má provést. Definice a možnosti iptables lze nalézt přímo v man stránce na linuxovém stroji nebo na stránce projektu. (Eychenne 2015)

5.4 Cisco ASA (Adaptive Security Appliance)

Jedná se o bezpečnostní zařízení od firmy Cisco, které chrání podnikové sítě a datová centra všech velikostí. Po celém světě je nasazeno více než jeden milion těchto zařízení. Je možnost toto zařízení nasadit v síti jako samostatné zařízení, blade nebo jako virtuální stroj. Cisco ASA přináší více variant použití než pouze jako klasický firewall, ale pro vyšší zabezpečení lze využít i IPS (Intrusion Prevention System) a VPN. Zařízení klade důraz na vysokou propustnost a díky mnoha modelovým řadám si můžeme vybrat, která bude nejvíce sedět našim potřebám. Samozřejmě zde nesmí chybět i vysoká dostupnost řešení. (Cisco.com 2014c)

5.5 Flowmon

Flowmon Networks a.s. je brněnská firma, která se zaměřuje na sledování toků v síti na bázi NetFlow a IPFIX. Díky tomu dokáží vyhotovit komlexní přehled provozu v síti, diagnostikovat ho a vyhodnocovat. Díky výsledkům vyhodnocení umožňují podnikům lépe nahlížet na problematiku toků v síti, zvyšovat výkonnost aplikací a chránit síť i proti moderním kybernetickým hrozbám.

V rámci této práce budou popsány tři produkty z portfolia. Jedná se o Flowmon sondu, Flowmon kolektor a Flowmon ADS.

Flowmon sonda je zařízení, které se zapojí do počítačové sítě a monitoruje provoz, který se v síti odehrává. Poté se získané informace mohou zaslat pro analýzu na Flowmon kolektor nebo jakýkoliv kolektor, který podporuje NetFlow/IPFIX standard. Sondy mohou sledovat IP toky a zde informace, mezi kým komunikace probíhala, jak dlouho, jakým protokolem, kolik se přeneslo dat a další informace. Lze monitorovat a analyzovat i vrstvy L5 - L7 dle relačního modelu ISO/OSI. Např. informace z HTTP, DNS, VoIP a další. (Flowmon.com 2016a)

Flowmon kolektor se stará o základní analýzu provozu a poskytuje přehled o provozu v síti. Kolektor se stará o sběr, zobrazení, analýzu a uložení statistik o provozu a pomáhá detekovat a řešit problémy, které se mohou v síti objevit. Problémy mohou být výkonnostní či např. bezpečnostní. (Flowmon.com 2016b)

Flowmon ADS (Anomaly Detection System) slouží pro detekci anomálií v síti. Tento systém se dá využít pro odhalování kybernetických útoků, síťových anomálií, chybných konfigurací, zneužívání dat. Flowmon ADS využívá technologii pro detekci anomálií a analýzu chování v síti (NBAD - Network Behavior Anomaly Detection) a díky tomuto může detekovat i neznámé hrozby a reagovat na ně. (Flowmon.com 2016c)

6 Literární rešerše

Tato kapitola bude zaměřena na analýzu bakalářských a diplomových prací, které se zabývaly stejným či podobným tématem. Také bude proveden průzkum publikací, které byly zveřejněny na Internetu. Pro vyhledání akademických prací bude využit server theses.cz. Do tohoto projektu je momentálně zapojeno 44 vysokých škol. V seznamu vysokých škol nicméně chybí dvě výzmnamné vysoké školy, které mají fakulty zaměřené na informační technologie. Je to univerzita České vysoké učení technické v Praze a Vysoké učení technické v Brně. Tyto dvě univerzity mají vlastní portál pro vyhledávání závěrečných prací, kterých také bude využito.

Bude zaměřeno na práce a publikace, které byly vydány v posledních pěti letech. Pro vyhledání příbuzných prací bude využito těchto klíčových slov: Cisco ASA, firewall, VPN, Flowmon.

6.1 Akademické práce

BP Generátor základních filtrovacích pravidel pro konfiguraci firewallů na síťových zařízeních

Tato bakalářská práce se zaměřuje na vývoj aplikace pro mobilní platformu Android, která má pomoci generovat základní filtrovací pravidla pro firewally a jejich aplikování přímo na firewallu.

Vyhnánek (2013) implementoval řešení generování pravidel pro platformu Cisco ASA a jejich ACL, linuxové iptables a pro platformu RouterOS od MikroTiku. V práci se zmiňuje i o omezeních aplikace. Omezení se týkají hlavně parametrů filtrů, které se moc nevyužívají a uživatel se ve většině případů bez nich obejde.

Autor se dále zabývá tím, jak tyto vygenerovaná pravidla aplikovat na cílové zařízení. Jelikož všechny tyto platformy mají přístup přes SSH, řešením bylo využít některý z již hotových SSH klientů dostupných na platformě Android a implementovat ho do vlastní aplikace.

Implementace byla úspěšná a výsledek této práce lze stáhnout z Google Play pod názvem Firewall Builder.

Nejzajímavější částí bakalářské práce je, že se zde autor zabývá vzdáleným přístupem k zařízení a jeho řešením. Tuto problematiku bude nutno vyřešit kvůli dynamicky vkládaným pravidlům i v této diplomové práci.

BP Propojení firemních poboček pomocí virtuální privátní sítě

Kozák (2012) se v práci Propojení firemních poboček pomocí virtuální privátní sítě v první části věnuje popisu typů VPN, jejich výhodám a nevýhodám, technologiím využívaným při implementaci VPN. Zabývá se zde popisem šifrování a tunelování. Zmiňuje i použití VPN s protokolem IPv6.

Autor se v praktické části věnuje VPN sítím typu site-to-site, kde řešení aplikuje pro tři pobočky. Součástí řešení je i ověření přenosu dat mezi pobočkami a zejména ověření přenosu dat z účetního systému z dílčích databází do centrální databáze.

Samotné řešení bylo provedeno pomocí simulátoru GNS3 z důvodu, že se nepodařilo práci reálně vypracovat v dané firmě z důvodu chybějících financí a také kvůli tomu, že prvky v síťové laboratoři neměly potřebné parametry pro konfiguraci VPN spojení.

V této práci se autor primárně zaměřuje na implementaci VPN site-to-site, což poskytuje možnost inspirovat se v oblasti využití a následného porovnání jednotlivých konfigurací.

BP Monitoring a správa sítě pomocí Cisco ASA firewallu

Bakalářská práce Monitoring a správa sítě pomocí Cisco ASA firewall se zabývá především monitoringem v síti za pomocí protokolu NetFlow. Dále se autor v práci věnuje stavové a hloubkové inspekci paketů a popisuje možnosti a rozdíly systémů IPS a IDS.

Dostal (2015) uvádí výhody využití NetFlow protokolu, např. když někdo provádí DOS útok, okamžitě se dozvíme jeho IP adresu. Problém nastává u DDOS útoku, kde je situace složitější. Pro otestování inspekce paketů použil protokol HTTP, kde pomocí regulárního výrazu zakazoval danou adresu. Pro kontrolu HTTPS komunikace je vyžadován ASA CX modul, který nebyl v laboratoři dostupný. Dále se autor zmiňuje o modulu AIP-SSM-10, který je zapotřebí pro využití IPS/IDS služeb na ASA firewallu. I tento modul v laboratoři chyběl a práce se tedy touto problematikou zabývá pouze po teoretické stránce.

Autor se zde zabývá inspekcí paketů, která by se eventuálně dala využít i v této diplomové práci.

BP Zabezpečení datové komunikace pomocí bezpečnostní brány firewall ASA

Práce Zabezpečení datové komunikace pomocí bezpečnostní brány firewall ASA nejprve obecně popisuje problematiku firewallů, pojmy s touto problematikou spojené a také typy útoků, se kterými se můžeme setkat.

Laš (2012) pro implementaci využívá zařízení Cisco ASA 5505. Věnuje se základní konfiguraci zařízení (VLAN, rozhraní), překladu adres (NAT) a vybraným ACL pravidlům (povolení služeb http, ftp, smtp, ssh a telnet). V práci je zmíněn i grafický nástroj ASDM určený pro konfiguraci Cisco ASA zařízení, ale je využito především příkazové řádky. Dané konfigurace jsou ověřeny pomocí nástrojů Hping2, Wireshark a Packet Tracer.

Tato práce se zabývá základní konfigurací zařízení Cisco ASA, kterou bude potřeba naimplemenovat i v této práci. Lze ji tedy využít jako zdroj pro toto nastavení.

BP Srovnání platforem pro zabezpečení počítačových sítí

Tato bakalářská práce se zaměřuje na porovnání konkurenčních firewallů. Jsou zde popsány technologie IPS, SSL VPN a varianty šifrované komunikace. Broulík (2015) se v práci zaměřil na firewall Cisco ASA, Juniper SRX a Fortigate. Autor provedl nakonfigurování zmíněných technologií a poté provedl testy, které měly zjistit jejich propustnost. Dále také otestoval úspěšnost odhalení útoků, a to i okrajového otestování antivirových modulů. Pro tuto diplomovou práci by byly nejzajímavější konfigurace Remote Access SSL VPN, ale bohužel zde žádné konfigurace nebyly uvedeny. Přínosný je tedy pouze teoretický popis této technologie. Pravidla IPS při testování byly ponechány v defaultním stavu a výsledky pro Cisco ASA nebyly příliš příznivé. Celkový počet útoků byl 136 a Cisco ASA zachytila pouze 22 útoků. Oproti tomu Fortigate zachytil 83 útoků.

Shrnutí analýzy akademických prací

Po analýze akademických prací jsem došel k závěru, že žádná z prací neřeší popsanou problematiku v síti MENDELU a bude zapotřebí se řešením zabývat více do hloubky.

Práce se věnují implementaci některých technologií na platformě Cisco ASA, ale ve většině případů pouze základním konfiguracím. V této práci se bude také zabývat i základní konfiguraci a uvedené práce mohou pomoci při implementaci. Bohužel informace pro stěžejní část této práce, dynamicky vkládaná pravidla na základě výstupů z Flowmon modulu ADS, z uvedených akademických prací nebude možné získat.

6.2 Oficiální publikace

Po analýze bakalářských a diplomových prací bude následovat další krok, kterým je analýza oficiálních publikací či vědeckých článků.

RFC

Pro správné pochopení problematiky je zapotřebí mít přehled o základních protokolech a síťových pojmech. Informace můžeme získat z Request for Comments (RFC). Jedná se o dokumenty, které popisují především internetové protokoly. Mezi základní znalosti patří přehled o Internet Protocol (IP), který je popsán v RFC 791, RFC 1349, RFC 2474 a RFC 6864. Dále je nutná znalost protokolů TCP a UDP, které jsou popsány v RFC 793 a RFC 768.

VLAN Interfaces

Další důležitou technologií, bez které by moderní sítě nemohly existovat, je VLAN (Virtual Local Area Network) technologie. V Cisco.com (2016a) jsou uvedeny obecné základní informace o VLAN, licencování VLAN na platformě Cisco ASA, informace vztahující se ke konfiguraci. Jsou zde i ukázky konfigurací.

Routing Overview

Zapotřebí je i znalost směrování, pro tuto práci především statické směrování a PBR (Policy Based Routing). Ve zdroji Cisco.com (2016b) jsou uvedeny všeobecné informace týkající se směrování. Dále zdroj uvádí, jaké typy směrování jsou podporovány na platformě Cisco ASA, jejich srovnání a jak se směrování na platformě Cisco ASA chová. Dozvíme se zde, jaké jsou podporované směrovací protokoly. V poslední řadě informuje o směrovací tabulce, např. jak je směrovací tabulka naplněna záznamy, administrativní vzdálenosti pro jednotlivé typy směrovacích záznamů a další. Popsaná problematika je doplněna i různými schématy.

Static and Default Routes

Po všeobecném seznámení se směrováním se zaměříme na statické směrování. Pro prostudování této problematiky více do hloubky slouží zdroj Cisco.com (2016c). Ohledně statických a defaultních směrovacích záznamů jsou zde k nalezení všechny potřebné informace. Jsou tu samozřejmě i uvedeny příklady, které na platformě Cisco ASA mohou být využity.

Policy Based Routing

Poslední z oblastí směrování, které bude věnována pozornost, je oblast směrování založeném na politice. Policy Based Routing nebyl na platformě Cisco ASA dlouhou dobu přítomen. Do operačního systému byl nasazen až ve verzi 9.4(1) (verze vydána v březnu 2015). Dokument Cisco.com (2016d) popisuje technologii PBR obecně a jsou zde uvedeny příklady použití, ukázky konfigurací a názorná schémata pro lepší pochopení problematiky.

Configuring IPSec and ISAKMP

Článek Cisco.com (2014b) popisuje možnosti konfigurace IPsec (Internet Protocol Security) a ISAKMP (Internet Association and Key Management Protocol) pro vytvoření VPN spojení.

Jsou zde obecné informace o tunelování, IPsec a ISAKMP. Dále informace o licencování pro VPN Remote Access dle jednotlivých modelů Cisco ASA. Především obsahuje popisy jednotlivých příkazů, které se využijí při konfiguraci VPN spojení. Také udává příklady použití příkazů.

Access Control List

Cisco (2016g) zde uvádí do problematiky přístupových pravidel na platformě Cisco. Kromě základních obecných informací, které je potřeba znát pro tvorbu ACL záznamů, se věnuje i běžným příkladům možných pravidel, a to včetně grafického znázornění i s příklady konfigurace.

V dalším článku Cisco (2013) popisuje rozšířené ACL záznamy pro platformu Cisco ASA, jejich využití, popis a také příklady konfigurací.

NAT Examples and Reference

V článku Cisco.com (2016f) se nachází potřebné informace pro pochopení a implementaci technologie NAT (Network Address Translation) na platformě Cisco ASA. Jsou zde vysvětleny různé druhy NAT typů (statický NAT, dynamický NAT, Port Address Translation). Ke každému případu je uvedeno schéma a jsou popsány jednotlivé kroky konfigurace.

Cisco ASA - All-in-One Next Generation Firewall, IPS, and VPN Services (Third Edition)

Publikace Frahim (2014) patří mezi důležitý zdroj informací, který bude k vypracování této práce využit. Věnuje se základním i pokročilým tématům, na která narazím při řešení této práce. Patří mezi ně základní konfigurace, směrování, NAT, přístupová pravidla, VPN a další. Publikace obsahuje i ukázky konfigurací určené přímo pro zařízení Cisco ASA. Je to i vhodný pramen informací pro pokročilejší problematiku, jako je IPS, aplikační inspekce, virtualizace, vysoká dostupnost a další.

FlowMon - Uživatelská příručka

Pro seznámení se s FlowMon sondou a FlowMon kolektorem bude využita oficiální uživatelská příručka Flowmon.com (2016d). Díky této publikaci bude prozkoumáno řešení na analýzu datových toků od firmy InveaTech. Bude zjištěno, jaké možnosti a funkcionalitu toto řešení nabízí, a budou prozkoumány možnosti propojení FlowMon sondy a Cisco ASA zařízení.

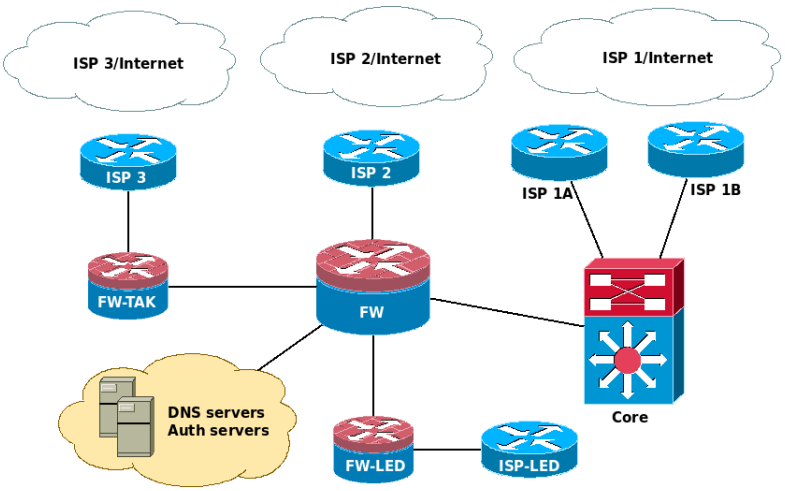
Bude zde zaměřena pozornost i na modul ADS (Anomaly Detection System), který se specializuje na detekci anomálií v datových tocích. Pro prostudování této problematiky bude použita uživalská příručka Flowmon.cz (2016e) pro ADS modul. Na základě výstupů z tohoto modulu budou vytvářena dynamická pravidla na zařízení Cisco ASA pro lepší zabezpečení sítě vůči novým hrozbám.

Skriptování

Pro potřeby dynamického vkládání pravidel z FlowMon sondy bude zapotřebí naprogramovat skript, který se o tuto úlohu postará. Bude využit skriptovací jazyk Expect, který je užíván pro vytváření automatizovaných a interaktivních skriptů. Pro seznámení s tímto skriptovacím jazykem bude použito manuálních stránek programu Expect.

7 Analýza aktuálního stavu

Tato kapitola bude zaměřena na popis a analýzu aktuálního stavu v počítačové síti Mendelovy univerzity v Brně. Pozornost bude věnována jednotlivým částem počítačové sítě, které je zapotřebí znát, mít o nich povědomí a díky tomu navrhnout nové řešení. Pro pochopení celé problematiky sítě byl vytvořen zaměstnanci Ústavu informačních technologií MENDELU (J. Passinger, M. Pokorný) model sítě, ze kterého práce vychází. Nejprve bude uveden zjednodušený model pro lepší pochopení problematiky počítačové sítě MENDELU (obr. 1) a poté bude každá část sítě zvlášť podrobněji popsána. Modely sítě obsahují náhodné rozsahy sítí a identifikátory VLAN z důvodu zachování anonymity modelu pro potencionální záškodníky. Po konzultaci s vedoucím pracovníkem oddělení infrastruktury univerzitní sítě MENDELU, panem J. Passingerem, bylo dohodnuto, že budou upraveny další citlivé informace, které byly poskytnuty v rámci této práce, aby nebyly zveřejněny detaily, které by mohly snížit bezpečnost univerzitní sítě. Jednotlivé případy budou popsány dále v textu.



Obr. 1: Zjednodušený model počítačové sítě MENDELU. Zdroj: autor

Středem počítačové sítě je univerzitní firewall (FW), který se stará o propojení s ostatními sítěmi. Hlavní spoj je mezi univerzitním firewallem a jádrem sítě (Core), kudy prochází provoz určený pro univerzitní servery, demilitarizovanou zónu a provoz směrem z a do Internetu. Toto jádro sítě má připojenou hlavní univerzitní konektivitu (ISP 1A) a také je zde napojena záložní konektivita od stejného poskytovatele (ISP 1B) pro případ, že by hlavní konektivita byla přerušena.

Univerzitní firewall také propojuje vzdálenou lokalitu, která se nachází v Lednici (FW-LED). Jedná se o Zahradnickou fakultu MENDELU. Tato vzdálená síť využívá pro přístup k Internetu lokální připojení (ISP-LED). Spojení s univerzitním firewallem je využíváno pouze pro provoz určený serverům MENDELU.

Další vzdálenou lokalitou jsou Koleje Josefa Taufera (FW-TAK), které jsou propojeny pomocí šifrovaného VPN tunelu s univezitním firewallem. Připojení zde

nevyužívají pouze studenti ubytovaní na těchto kolejích, ale i zaměstnanci Ústavu tělesné výchovy a zaměstnanci Správy kolejí a menz a také komerční subjekty. Koleje Josefa Taufera mají k dispozici svého poskytovatele internetové konektivity (ISP 3), která slouží studentům. Ale z důvodu, že tímto spojem nesmí procházet komerční provoz, je nutné tento komerční provoz tunelovat směrem na univerzitní firewall a využít jiného poskytovatele internetu (ISP 2). Přes VPN tunel je směrován i studentský provoz, který cílí na univerzitní servery.

Ve zjednodušeném modelu je znázorněna i další síť. V této síti jsou umístěny servery, především DNS servery, které se starají o překlad IP adres, a také autentizační servery, které se využívají pro autentizaci uživatele. Tím se též určí, jaká přístupová práva uživatel má v rámci sítě.

Tento model obsahuje upravené rozsahy podsítí a identifikátory VLAN z důvodu zachování anonymity modelu pro potencionální záškodníky.

Univerzitní firewall

Univerzitní firewall je v současné době provozován jako linuxový stroj ve virtuálním prostředí. Jedná se o centrální prvek, který se stará o logiku celé sítě MENDELU.

Jelikož se jedná o linuxový firewall, tak pro přístupová pravidla jsou využívány iptables, která povolují a omezují přístup do jednotlivých částí sítě. Pomocí iptables je řešen i překlad adres a přesměrování provozu podle portů. Také se zde řeší případy, kdy má učebna vypnutý přístup k Internetu, aby pokus o přístup k Internetu byl zablokován.

Dále jsou zde ukončovány VPN ze vzdálených lokalit. Mezi ně patří vzdálená lokalita Lednice a vzdálená lokalita Koleje Josefa Taufera.

Firewall se také stará o statické směrování mezi jednotlivými sítěmi a přístupem do Internetu. Policy Based Routing je nastaven pro směrování provozu ze vzdálené lokality Koleje Josefa Taufera na základě zdrojové adresy sítě k jinému poskytovateli internetu a ne jako zbytek provozu z interní sítě. Podrobnější informace k jednotlivým částem a funkcionality sítě budou popsány dále v této kapitole.

Jádro sítě

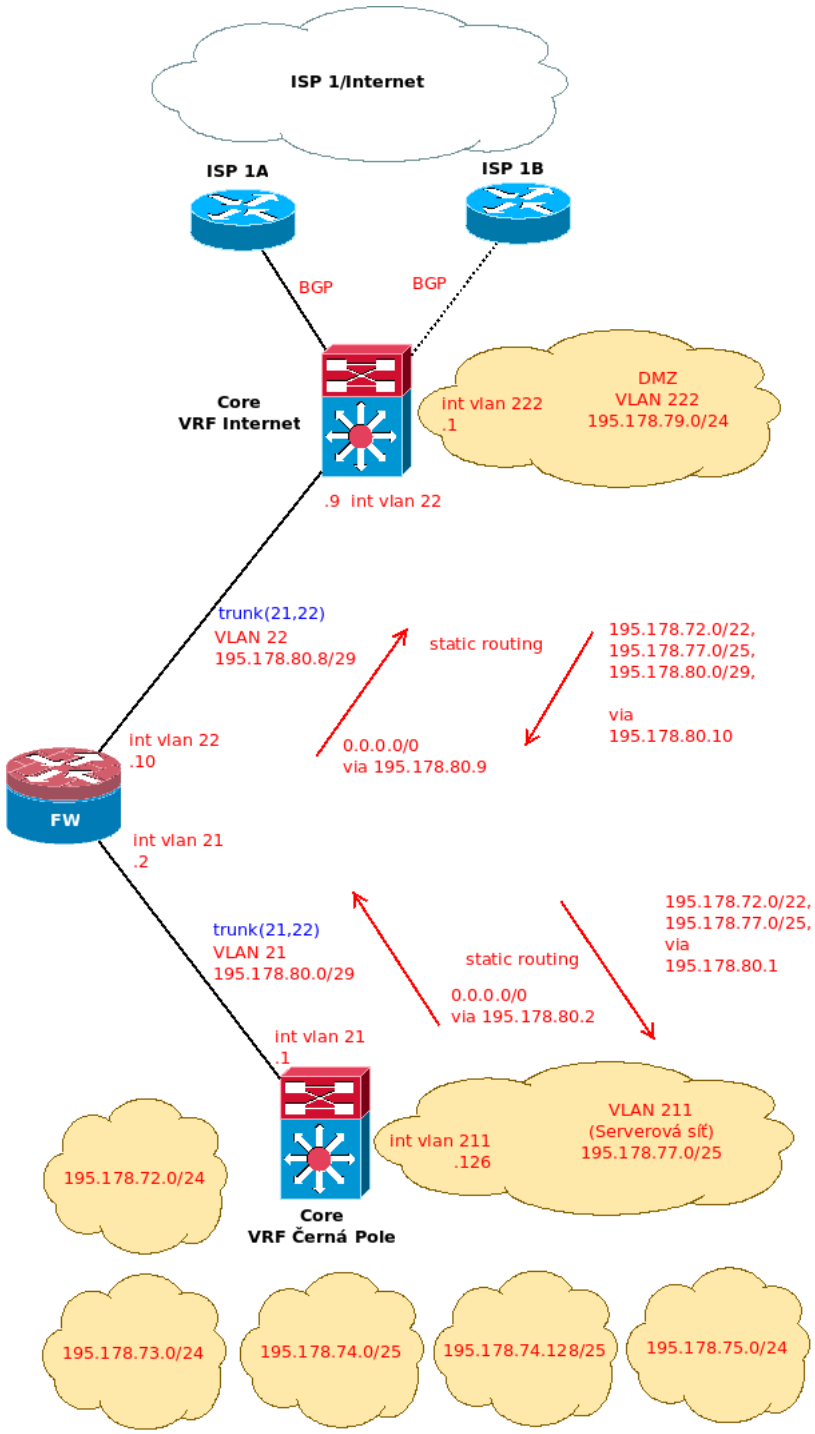
Ústředními prvky Mendelovy univerzity jsou dva L3 přepínáče Catalyst 6500 Series od firmy Cisco. Tyto prvky jsou spolu propojeny technologií VSS (Virtual Switching Systems), kdy se tyto prvky chovají jako prvek jeden. Díky této technologii se zajišťuje redundance.

Dále je na tomto *Core* prvku využita technologie VRF (Virtual Routing and Forwarding). Nachází se zde více instancí směrovacích tabulek, ale pro tuto práci budou stěžejní pouze dvě instance. Instance VRF Černá Pole a VRF Internet. Tyto instance jsou spojeny s univerzitním firewallem pomocí VLAN:

- VRF Černá Pole: VLAN 21 s rozsahem 195.178.80.0/29
- VRF Internet: VLAN 22 s rozsahem 195.178.80.8/29

Instance VRF Černá Pole se stará o směrování k serverové části, která má VLAN identifikátor 211 a podsíť 195.178.77.0/25. Dále se zde nachází další rozsahy veřejných adres. Směrování z této sítě je tvořeno defaultním záznamem na rozhraní VLAN 21 na firewallu.

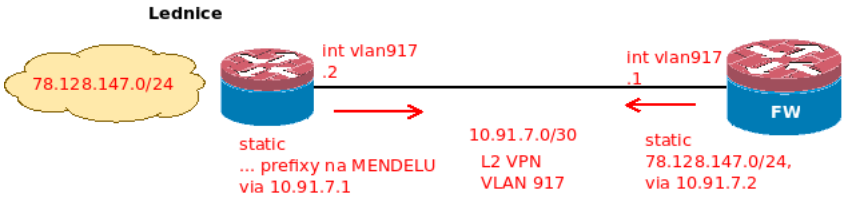
Instance VRF Internet je připojena do Internetu dvěma spoji od jednoho poskytovatele připojení. V jeden moment se využívá pouze jedna konektivita, druhá slouží pouze jako záložní. Primární i záložní konektivita je propojena pomocí dynamického směrovacího protokolu BGP (Border Gateway Protocol). Také se zde nachází demilitarizovaná zóna, která má VLAN identifikátor 222 a slouží pro servery, které musí být vystaveny do Internetu, aby k nim měli uživatelé přístup zvenčí, ale nepřipojovali se do interní sítě. Směrovací tabulka obsahuje záznamy, které směřují na servery připojené k VRF instanci Černá Pole a na servery, které se nacházejí na kolejích Josefa Taufera. Tyto záznamy směřují na rozhraní VLAN 22 univerzitního firewallu. V opačném směru, tedy z univerzitního firewallu, je jeden defaultní statický záznam.



Obr. 2: Model propojení Core Switch a univerzitního firewallu. Zdroj: autor

Vzdálená lokalita - Lednice

Pobočka Lednice, kde se nachází Zahradnická fakulta Mendelovy univerzity v Brně, je propojena s hlavním univerzitním firewallem pomocí technologie L2 VPN. Tento spoj mohl být implementován tímto způsobem díky tomu, že se jedná o propojení sítí v rámci jednoho internetového poskytovatele. Tento spoj spravuje sdružení CESNET. Na pobočce v Lednici se nachází rozsah adres 78.128.147.0/24. Ve směrovací tabulce jsou uvedeny statické záznamy, které jsou obsaženy v síti MENDELU. Provoz, který není určen pro síť MENDELU, je směrován přes defaultní statický záznam přímo do Internetu přes lokálního poskytovatele připojení. Z hlavního firewallu směřuje jeden statický záznam na již zmíněný rozsah adres v Lednici. Na tomto spoji je definována VLAN s identifikátorem 917.



Obr. 3: Model propojení Lednice a univerzitního firewallu. Zdroj: autor

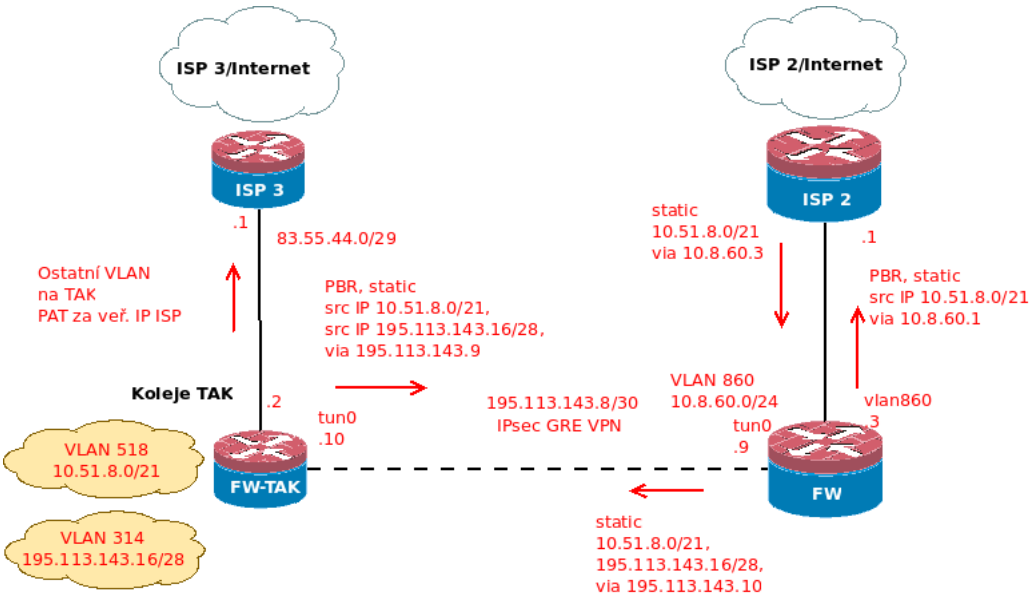
Koleje Josefa Taufera

Firewall na této pobočce se stará o propojení s univerzitním firewallem, připojení studentů na kolejích k Internetu a univerzitní síti a také o připojení komerčních zákazníků do Internetu.

Komerční subjekty se nachází v síti 10.51.8.0/21. Tato síť patří do VLAN s identifikátorem 518. Pod VLAN 314 se nachází servery s veřejnými adresami v rozsahu 195.113.143.16/28. I když tento firewall má přímé napojení na ISP, tak komerční subjekty ve VLAN 518 nemohou využívat tohoto ISP a tím pádem musí být směrovány přes IPSec tunel směrem k univerzitnímu firewallu pomocí Policy Based Routingu na základě zdrojové adresy sítě. Tímto způsobem je směrována i VLAN 314. Dále se na univerzitním firewallu rozhoduje, kudy bude provoz směrován. Komerční provoz bude směrován k ISP 2. Provoz přes tohoto poskytovatele půjde zpátky na univerzitní firewall a na firewall na kolejích Josefa Taufera. Ostatní provoz je směrován přes statický záznam směrem ke Core VRF Internet.

Studenti využívají přímo připojeného poskytovatele na kolejích, tedy ISP 3 dle obr. 4. Na tento provoz je uplatněn PAT (Port Address Translation) a provádí se překlad na veřejnou adresu poskytovatele připojení.

Kolejní firewall s univerzitním firewallem je propojen pomocí site-to-site IPsec VPN tunelu, který využívá technologii GRE over IPsec.



Obr. 4: Model propojení kolejí TAK a univerzitního firewallu. Zdroj: autor

Přístupová pravidla

Jak už bylo řečeno, pro přístupová pravidla se využívá iptables, které nalezneme na linuxových strojích. Pro tuto práci a testovací implementaci byla připravena anonymizovaná modelová pravidla. O přípravu těchto pravidel se postaral pan J. Balej.

Pro filtraci provozu se zde pracuje se dvěmi řetězci. Jsou to řetězce INPUT a FORWARDING. Pro řetězec OUTPUT je vše povoleno.

INPUT

Řetězec INPUT se stará o provoz, který je určen pro lokální zařízení – univerzitní firewall. Je zde povolen provoz, který je již navázán (ESTABLISHED) nebo se jedná o nové spojení, které se ale vztahuje k některému již existujícímu (RELATED). Povolen je také provoz na loopback rozhraní. Provoz, který se neváže k žádnému navázanému provozu, je rovnou zahazován (INVALID). Dále je na zařízení povolen provoz ICMP, ale pouze některé typy. Jedná se o ICMP typ 0 (Echo Reply), 3 (Destination Unreachable), 8 (Echo), 11 (Time Exceeded). Ostatní ICMP typy jsou blokovány. Pro správu zařízení je povoleno SSH spojení, ale pouze z některých podsítí.

Dále se zde nachází pravidlo pro IPSec provoz mezi univerzitním firewallem a vzdálenou lokalitou Koleje Josefa Taufera. Tento tunel je na univerzitním firewallu ukončen. Na pravidle je tedy povolen protokol ESP a cílový UDP port 500. A mezi poslední pravidla, která povolují provoz na univerzitní firewall, patří ta týkající se monitoringu (SNMP provoz) a komunikace s monitorovacím nástrojem Zabbix.

Ostatní provoz určený pro firewall je zahazován a blokován.

FORWARD

Řetězec FORWARD je určen pro provoz, který prochází skrz univerzitní firewall. Také obsahuje daleko více pravidel než předchozí řetězec. Stejně jako řetězec INPUT jsou zde pravidla, která povolují již navázaný provoz (ESTABLISHED) a nové spojení, které se vztahuje již k existujícímu provozu (RELATED). Je zde také zahazován provoz, který se neváže k žádnému provozu (INVALID).

Jak již bylo uvedeno v úvodu této kapitoly, proběhne úprava pravidel, které byly poskytnuty v rámci této práce. Skutečná pravidla byla nahrazena podobnými příklady z důvodu citlivosti informací. Záznamy i s anonymizovanými IP adresami a identifikátory VLAN by mohly potenciálnímu útočníkovi usnadnit útok. V následující kapitole týkající se návrhu budou uvedena pouze modelová pravidla pro vysvětlení a ukázku konfigurace ACL pravidel na novém řešení.

NAT

Stejně jako přístupová pravidla, tak i pravidla pro překlad síťových adres se na aktuálním řešení definují s využitím iptables. Používají se tabulky PREROUTING a POSTROUTING. Jedná se o ekvivalenty k DNAT a SNAT.

V tabulce PREROUTING dochází především ke změně cílové adresy na základě cílového portu, kam provoz směřuje. Byly zde změněny informace o cílových portech, aby nebylo možné identifikovat služby, kterých se provoz týká. Podstata problematiky bude zachována, pouze se změní číslování portů a název objektů.

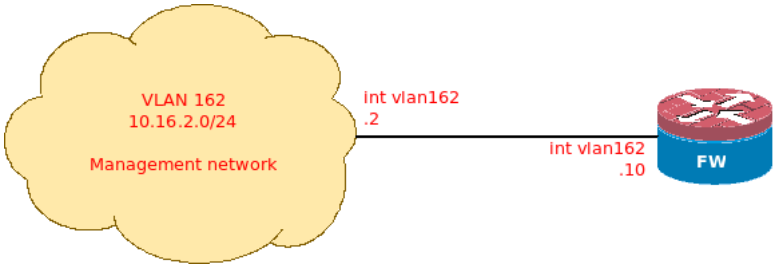
Pokud provoz cílí na cílové porty TCP/800 a TCP/900 na IP adresu 195.178.80.11 (jedná se o veřejnou IP adresu definovanou na firewallu), bude provoz přesměrován na server s adresou 10.45.5.90 ve VLAN 455. Pokud provoz na tuto adresu na firewallu bude cílit na port UDP/390, tak cílová adresa bude změněna na adresu 195.178.77.123. Ostatní provoz, který cílil na adresu 195.178.80.11 bude přesměrován na adresu 10.45.5.100.

Další provoz se týká adres, které mají zablokovaný webový přístup (vyučující vypne žákům v učebně Internet). Takové zdrojové IP adresy jsou pomocí skriptu nahrány z informačního systému na univerzitní firewall a pakety z takové adresy jsou označeny příznakem 0x5a a poté je změněna cílová adresa paketu na adresu 10.45.5.9 a port 3658, kde se nachází informační stránka o zablokovaném Internetu.

V tabulce POSTROUTING se provádí SNAT pro provoz, který míří do DNS, ale má zakázaný internet. Proběhne zde překlad zdrojové adresy na adresu, která se nachází na rozhraní VLAN 455 (10.45.5.1) na základě příznaku 0x5a.

Management síť

V síti MENDELU je vytvořená management síť, díky které se odděluje provoz určený pro správu zařízení od ostatního provozu v síti. Jedná se o adresní rozsah 10.16.2.0/24 s VLAN identifikátorem 162.



Obr. 5: Management síť. Zdroj: autor

Vysoká dostupnost

U tak důležitého prvku jako je univerzitní firewall je důležité zachovat vysokou dostupnost. Při výpadku prvku nebudou k dispozici důležité funkce sítě. Vysoká dostupnost aktuálního řešení virtuálního firewallu je nyní zajišťována druhým virtuálním firewallem, který není aktivní současně s primárním prvkem. Probíhá zde monitoring primárního prvku a pokud dojde k nedostupnosti tohoto prvku, tak se spustí druhý prvek se stejnou konfigurací. Dochází zde tedy pouze k dočasnému výpadku v rámci minut.

Remote Access VPN

V síti MENDELU je vzdálený přístup pomocí VPN určen pro několik typů uživatelů, kteří potřebují vzdáleně pracovat s nástroji a službami dostupnými pouze v univerzitní síti nebo s IP adresou univerzity.

Studenti i zaměstnanci také mohou využít připojení pomocí proxy serveru a díky tomu získat přístup k odborným článkům a databázím.

Aktuálně se využívá VPN technologie L2TP over IPSec, která se ukončuje na Cisco ASA zařízení. Dříve se ale využíval i IPSec tunel a uživatelé se připojovali pomocí Cisco klienta. Tento tunel byl ukončován na Cisco VPN koncentrátoru. Bohužel Cisco podporu tohoto klienta ukončilo a tento klient měl na novějších verzích operačního systému Windows problémy se spuštěním. Proto se od této varianty upustilo. Výhodou L2TP VPN je, že většina operačních systémů již obsahuje nativního klienta pro připojení ke vzdálené síti. Na současné technologii L2TP over IPSec se identifikují čtyři typy uživatelů:

- Administrátoři
- Zaměstnanci

- Studenti
- Externí subjekty

Každé z těchto skupin jsou samozřejmě vymezena jiná přístupová práva. Tedy každému uživateli se zpřístupní pouze ta část sítě, do které má mít přístup. Po autentizaci do VPN dostane uživatel dle své nastavené skupiny IP adresu z rozsahu, který náleží dané skupině. Na základě toho je pak prováděna filtrace přístupů v síti. Na různé skupiny uživatelů se také uplatňují jiná NAT pravidla.

Momentálně univerzitě chybí moderní vzdálený přístup pro uživatele do univerzitní sítě. Tímto přístupem je myšlen Remote Access SSL VPN, kdy se např. jen za pomoci webového prohlížeče uživatel dostane ke zdrojům, které jsou přístupné pouze v univerzitní síti. Je velice pravděpodobné, že tento typ připojení ke vzdálené síti v budoucnu bude vyžadován.

8 Návrh univerzitního firewallu na platformě Cisco ASA

Jak už bylo uvedeno v zadání této diplomové práce, návrh a implementace nového řešení pro univerzitní firewall bude vypracován na platformě Cisco ASA. Platforma Cisco ASA byla vybrána z toho důvodu, že toto zařízení je již ve vlastnictví univerzity.

V první řadě se bude jednat o migraci základních funkcionalit, které jsou dány aktuálně nasazeným řešením v prostředí univerzity. Proběhne zjištění a ověření, zda všechny funkcionality, které jsou momentálně implementovány, bude možné implementovat i na novém řešení. Mezi tyto základní funkcionality patří především směrování, pravidla pro kontrolu přístupu, VPN mezi jednotlivými pobočkami univerzity, NAT.

Další částí práce je implementace dynamicky vkládaných pravidel na univerzitní firewall, aby byl schopný reagovat na aktuální podezřelé či zákeřné chování. Pro dosažení tohoto stavu bude využito FlowMon sondy, která je již v univerzitní síti nasazena a sbírá informace z toků v síti v reálném čase. Tyto sesbírané toky předává pro analýzu FlowMon ADS modulu, který vyhodnocuje toky a upozorňuje na podezřelé chování.

Proběhne zde i analýza možností pro vzdálený přístup pro uživatele a implementace Remote Access SSL VPN.

8.1 Základní konfigurace

Tato podkapitola bude zaměřena na základní, ale důležitou konfiguraci pro univerzitní firewall na platformě Cisco ASA.

Název zařízení

Pro jednodušší orientaci, na kterém zařízení se administrátor zrovna nachází (může mít otevřeno více příkazových řádek na různá zařízení), je vhodné nastavit název zařízení, které bude dané zařízení identifikovat. Název zařízení bude nastaven na hodnotu *FW*.

Rozhraní

Na platformě Cisco ASA je možné se setkat s těmito fyzickými rozhraními: Fast Ethernet, Gigabit Ethernet a 10-Gigabit Ethernet. V testovacím modelu budou na zařízení k dispozici Gigabit Ethernet porty. Při implementaci se využijí jak samotná fyzická rozhraní, tak i definice virtuálních rozhraní (*subinterfaces*) – i více virtuálních rozhraní na jednom fyzickém rozhraní, která se využijí pro segmentaci sítě pomocí VLAN.

Na zařízení se také nadefinuje management rozhraní. Testovací zařízení nemá k dispozici dedikovaný management port určený pro *out-of-band-management*, ale je zde možnost definice jednoho klasického portu jako management portu. Pro management provoz je vhodné využívat dedikovaný port a oddělit provoz od zbytku sítě. Je to bezpečnější řešení v případě, že je správa zařízení možná pouze přes management port.

U každého rozhraní proběhne konfigurace názvu rozhraní, které se později využije u dalších příkazů (např. směrování a přístupová pravidla). Také je zapotřebí nakonfigurovat bezpečnostní úroveň (*security-level*) na škále od 0 do 100. Defaultní chování je, že rozhraní s vyšší bezpečnostní úrovní může přistupovat na rozhraní s nižší bezpečnostní úrovní, ale ne naopak. Nicméně, toto chování se bude upravovat pomocí přístupových pravidel.

Posledním nastavením na rozhraní bude přiřazení IP adresy a aktivace rozhraní. Také ne nutným, ale žádaným krokem je nastavení popisu rozhraní pro lepší orientaci v konfiguraci.

Atributy pro jednotlivá rozhraní budou postupně popsány, definovány a názorně zobrazeny na obr. 6.

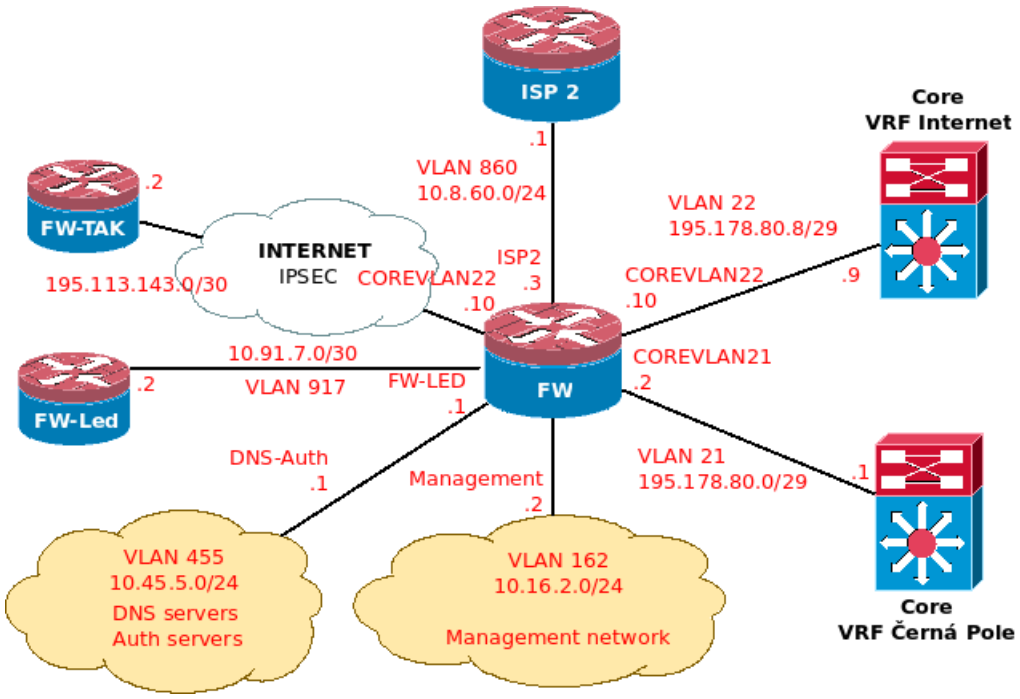
Mezi první rozhraní bude patřit propojení s jádrem sítě, tedy Core routerem. Na tomto fyzickém rozhraní jsou dvě virtuální rozhraní pro VLAN 21 a pro VLAN 22. Budou zde tedy nastaveny dva subinterfaces a rozhraní budou přidána do příslušných VLAN. Pro rozhraní na VLAN 21 bude zadán název rozhraní COREVLAN21 a bezpečnostní úroveň 100. Z této sítě je počítáno s bezpečným provozem. Pro VLAN 22 se nastaví název COREVLAN22 a bezpečnostní úroveň 0, jelikož toto rozhraní je připojeno směrem k Internetu a může se zde objevit jakýkoliv provoz. IP adresy budou nastaveny dle modelu a pro rozhraní COREVLAN21 připadne adresa 195.178.80.2/29 a na rozhraní COREVLAN22 bude nastavena adresa 195.178.80.10/29. Na rozhraní COREVLAN 22 také bude ukončen IPsec tunel, který spojuje univerzitní firewall se vzdálenou sítí Tauferových kolejí.

Spojení do vzdálené sítě Zahradnické fakulty v Lednici bude probíhat přes rozhraní s názvem FW-LED, které bude náležet do VLAN 917. Úroveň bezpečnosti tohoto rozhraní bude nastavena na hodnotu 100, protože by zde měl probíhat provoz určený pouze pro servery v MENDELU síti. IP adresa na tomto rozhraní bude 10.91.7.1/30.

V pořadí třetí rozhraní bude určeno pro spojení s poskytovatelem internetu pro soukromé subjekty v MENDELU síti. Tomuto rozhraní bude přiřazen název ISP2. Provoz zde prochází do VLAN 860. Toto rozhraní také bude připojeno do Internetu, tak jeho bezpečnostní úroveň bude nastavena na hodnotu 0 jako v předchozím případě. IP adresa rozhraní bude 10.8.60.3/24.

Rozhraní Management bude připojeno do Management sítě a zde bude probíhat správa zařízení přes SSH a ASDM. Komunikace v této síti probíhá ve VLAN 162. Bude zde probíhat bezpečný provoz a bezpečnostní úroveň tedy bude 100. IP adresa Management rozhraní bude 10.16.2.2/24 a toto rozhraní bude označeno pouze pro management provoz.

Poslední rozhraní bude určeno pro komunikaci s DNS a autentizačními servery. Bude nastaven název DNS-Auth a VLAN 455. Bezpečnostní úroveň se nastaví také na hodnotu 100 a IP adresa na hodnotu 10.45.5.1/24. Přes tuto síť také bude probíhat komunikace do interní testovací sítě, kde bude k dispozici testovací FlowMon sonda a FreeRadius server.



Obr. 6: Popis rozhraní a jejich atributů. Zdroj: autor

SSH přístup

SSH přístup je velice rozšířeným způsobem, jak spravovat zařízení. Oproti protokolu Telnet je SSH bezpečný, jelikož využívá šifrovaného přenosu. Pro povolení přístupu přes SSH k zařízení je zapotřebí nejdříve vygenerovat privátní a veřejný klíč. Správa zařízení bude nastavena pro rozhraní Management a na SSH bude možné se přihlásit z management sítě a tedy z rozsahu 10.45.5.0/24.

Čas

Nastavení času patří mezi důležité kroky při inicializačním nastavování zařízení. Na zařízení je vhodné mít přesný čas a nejlépe stejně synchronizovaný napříč celou sítí. Je to důležité při vyhodnocování bezpečnostních incidentů a logů, kde čas hraje zásadní roli. Při konfiguraci bude použit NTP server, který se nachází na adrese 195.178.77.123. Ještě zde bude potřeba definovat odchozí rozhraní a tím bude COREVLAN21.

ASDM (Adaptive Security Device Manager)

Pokud je požadavek na správu zařízení přes webové grafické rozhraní, je možnost využít ASDM. Nejdříve je potřeba zkontrolovat, zda se binární soubor ASDM nachází na zařízení. Pokud ne, je potřeba ho nahrát. Pro nahrání se dá využít příkaz *copy* z Cisco ASA zařízení nebo příkaz *scp* z Unix/Linux systémů (pro kopírování pomocí příkazu *scp* je zapotřebí mít aplikován příkaz *ssh scopy enable*).

Když se soubor pro ASDM na zařízení nachází, specifikujeme umístění tohoto souboru pomocí příkazu *asdm*. Poté je potřeba spustit webový server na zařízení pomocí příkazu *http server enable* a povolit přístup na tento server pomocí příkazu *http*.

Grafické rozhraní poté bude dostupné na adrese https://10.16.2.1/admin, kde se nabídne ke stáhnutí Java aplikace.

Zabezpečení přístupu

Je velice žádoucí, aby se přístup k zařízení opatřil hesly a tím útočníkovi znemožnil (či alespoň znesnadnil) neautorizovaný přístup k zařízení. V návrhu řešení bude věnována pozornost několika možnostem, jak omezit neoprávněný přístup na zařízení. Pro přístup k zařízení se dá nastavit účet v lokální databázi nebo využít autentizace pomocí autentizačního serveru. Budou uvedeny kombinace těchto možností.

První heslo bude nastaveno pro přístup k zařízení přes konzolový port. Zde se využije lokální účet. Jako první tedy bude vytvořen lokální uživatel *admin* s heslem *admin123* (jedná se pouze o ukázkové heslo a je zapotřebí zvolit nějaké bezpečnější). Poté se nadefinuje lokální autentizace pro sériovou konzoli.

Druhé nastavení se týká SSH přístupu. Zde bude nastavena autentizace nejdříve pomocí Radius server. Pokud tento server nebude dostupný, proběhne ověření přístupu vůči lokální databázi. Bude zde tedy nakonfigurován autentizační server s názvem *FreeRadius*, který bude na adrese 192.168.0.36 (jedná se o adresu v testovacím prostředí).

Poslední heslo, které se bude konfigurovat, je přístup do privilegovaného módu. Toto heslo je defaultně prázdné, takže je vhodné ho pro větší bezpečnost nastavit. Zde bude nastaveno heslo *enable123*.

Výhodou je, že všechna hesla, která se nastaví v lokální databázi, jsou v šifrované podobě a při výpisu konfigurace nejsou zobrazena v prostém textu. Není tedy zapotřebí nastavovat další volbu.

8.2 Routing

Na univerzitním firewallu se řeší dva typy routingu. Prvním typem je statický routing, který slouží ke spojení jednotlivých sítí. Na platformě Cisco ASA je tento typ směrování bez problémů podporován, a tudíž s implementací nebudou žádné problémy.

Defaultní statický záznam ve tvaru 0.0.0.0/0, který se postará o směrování provozu bez specifické shody, bude nadefinován na rozhraní COREVLAN22 a jeho *next-hop* adresa bude IP adresa 195.178.80.9 směrem do Internetu či do demilitarizované zóny.

Na rozhraní COREVLAN21 bude definován routovací záznam pro cílové adresy 195.178.72.0/22 a 195.178.77.0/25 na rozhraní s IP adresou 195.178.80.1.

Pro komunikaci do vzdálené lokality Lednice bude nakonfigurován statický záznam na rozhraní FW-LED. Bude se jednat o podsíť 78.128.147.0/24 a pakety budou směrovány na adresu 10.91.7.2.

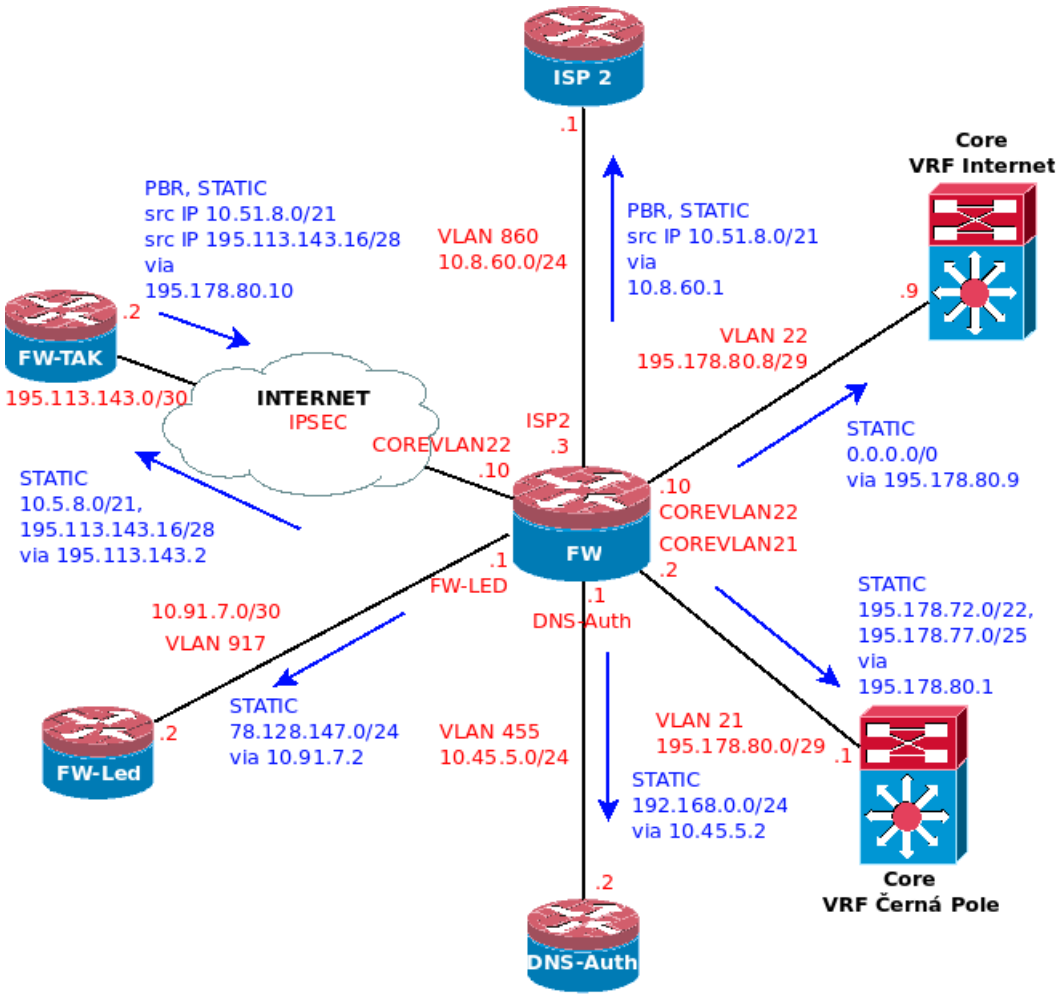
Bude zde zapotřebí nakonfigurovat i routovací záznam pro provoz do interní testovací sítě, kde bude k dispozici FreeRadius server pro autentizaci a také FlowMon sonda. Budou se nacházet v adresním rozsahu 192.168.0.0/24 a budou dostupné přes rozhraní DNS-Auth.

Mezi poslední klasický statický záznam bude ještě patřit provoz, který bude směřovat do IPsec tunelu pro vzdálenou lokalitu Tauferovy koleje. Zde se bude šifrovaně posílat provoz pro adresní rozsahy 10.5.8.0/21 a 195.113.143.16/28. *Next-hop* adresa bude adresa 195.113.143.10, která je nastavena na druhém konci IPsec tunelu směřem k ISP 3 na Tauferových kolejích.

Po statickém routingu následuje Policy Based Routing. Na univerzitní firewall přes IPsec tunel z Tauferových kolejí dorazí provoz z adresních prostorů 10.51.8.0/21 a 195.113.143.16/28. První adresní rozsah je komerční provoz určen pro ISP2. Univerzitní firewall tedy na základě zdrojové adresy určí, že provoz má jít na rozhraní ISP2 a provoz bude směrován na adresu 10.8.60.1. Pro určení, na které rozhraní má být provoz přesměrován, je potřeba nadefinovat ACL záznam. Proběhne konfigurace rozšířeného ACL záznamu s názvem NetFromTAKPBR, ve kterém bude definována síť 10.51.8.0/21. Tento ACL záznam bude využit v routovací mapě, která bude nazvána TOISP2 s prioritou 10. V routovací mapě bude dále nastavena *next-hop* adresa 10.8.60.1. Posledním krokem se aplikuje routovací mapa na rozhraní FW-TAK.

Druhý adresní rozsah (195.113.143.16/28) bude určen pro univerzitní síť a o zpracování tohoto provozu se již postarají ostatní statické záznamy. Již se zde nebudou aplikovat PBR pravidla.

Pro lepší orientaci a přehled je na obr. 7 uveden model, ve kterém jsou obsaženy jednotlivé směrovací záznamy a jejich směry.



Obr. 7: Přehled směrování na univerzitním firewallu. Zdroj: autor

Objekty

V této části budou uvedeny objekty, které se nadefinují pro využití v ACL pravidlech. Pro definici NATu je také využito objektů, ale definice je více spjata s těmito objekty, budou tedy uvedeny přímo v kapitole Network Address Translation. Jak bylo již řečeno dříve, budou vytvořena pouze modelová pravidla, z důvodu nezveřejnění citlivých informací.

Budou vytvořeny následující objekty určené pro služby:

- ICMP-TYPE-ALLOWED: skupina objektů pro povolení ICMP zpráv.
- SNMP-SERVICE: UDP port 161 pro SNMP provoz.
- ZABBIX-SERVICE: UDP port 10050 pro monitorovací provoz.

- WEB-SERVICES: skupina objektů, která bude obsahovat webové služby (porty TCP/80 a TCP/443).
- MAIL-SERVICES: skupina objektů, která bude obsahovat mailové služby (porty TCP/25 a TCP/465).
- MGMT-SERVICES: skupina objektů, která bude obsahovat služby pro vzdálenou správu (porty TCP/22 a TCP/3389).

A síťové objekty:

- SNMP-SERVER: IP adresa SNMP serveru (10.16.2.10).
- ZABBIX-SERVER: IP adresa Zabbix serveru (195.178.77.125).
- MAIL-SERVERS: zde se definují dva mailové servery (IP adresa 195.178.77.25 a 195.178.77.26).
- SERVERS-SUBNET: serverová podsíť 195.178.77.0/25.
- MANAGEMENT-SUBNET: management síť 10.16.2.0/24.
- UCEBNY-SUBNET: PC v učebnách v síti 195.178.72.0/24.

8.3 Access Control Lists

Politika pravidel bude taková, že provoz, který není vysloveně povolen, bude zakázán.

INPUT

Pravidla, která zde budou uvedena, budou ekvivalentní INPUT pravidlům, která byla uvedena v analýze aktuálního stavu. Bude vytvořena skupina objektů týkající se ICMP zpráv s názvem *ICMP-TYPE-ALLOWED*, které jsou na zařízení povoleny (ICMP typ 0 (Echo Reply), typ 3 (Destination Unreachable), typ 8 (Echo), typ 11 (Time Exceeded).

Povolení SSH přístupu je již uvedeno dříve v této kapitole.

Povolení provozu týkajícího se IPsec tunelu bude uvedeno v této kapitole v návrhu Site-to-Site VPN.

Poslední příchozí pravidla se budou týkat monitoringu. Vytvoří se objekt *SNMP-SERVICE*, který bude obsahovat UDP port 161 a objekt *SNMP-SERVER* s IP adresou 10.16.2.10. Dále se vytvoří objekt pro server, na kterém se nachází Zabbix. Bude se nazývat *ZABBIX-SERVER* a bude obsahovat IP adresu 195.178.77.125. Pro definici portu se vytvoří objekt *ZABBIX-SERVICE* s UDP portem 10050.

V pravidle INPUT se také řeší jednotlivé stavy ESTABLISHED, RELATED, INVALID. Cisco ASA je stavový firewall a kontroluje i tyto stavy spojení. Tyto kontroly provádí defaultně a není nutné toto zvlášť konfigurovat.

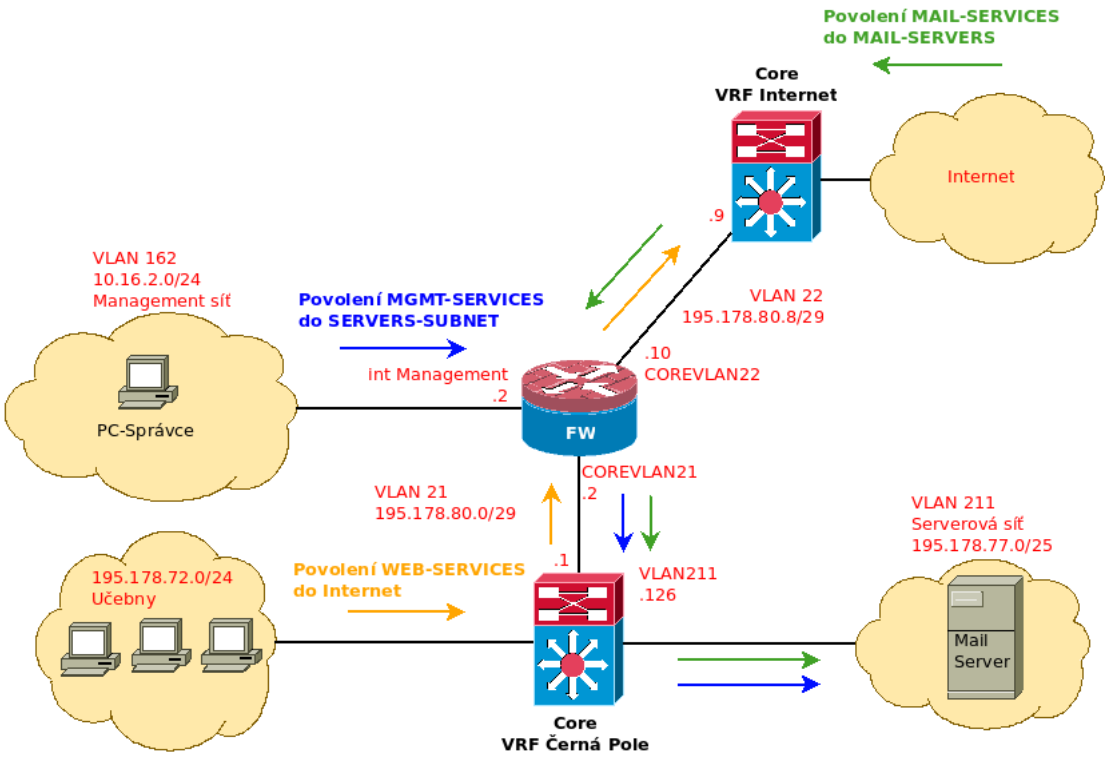
FORWARD

Na obr. 8 jsou uvedeny jednotlivé příklady odlišené různou barvou.

Jako první bude nastaveno pravidlo povolující e-mailovou komunikaci z Internetu směrem na e-mailové servery (MAIL-SERVERS) na TCP portech 25 a 465. Pro SMTP a SMTP over TLS (MAIL-SERVICES). Toto rozšířené ACL pravidlo bude aplikováno na rozhraní COREVLAN22 s názvem TRAFFIC-FROM-OUTSIDE. Na obr. 8 je tento provoz zobrazen zelenou barvou.

Druhý případ bude povolovat správu zařízení, která se nacházejí v serverové síti (SERVERS-SUBNET). Tato správa bude povolena pouze z management sítě (MANAGEMENT-SUBNET). Mezi povolené služby pro správu bude patřit SSH a RDP (Remote Desktop Protocol), tedy TCP porty 22 a 3389 (MGMT-SERVICES). Na obr. 8 vyznačeno modrou barvou. Pravidlo se bude nazývat TRAFFIC-FROM-MANAGEMENT a bude aplikováno na rozhraní Management.

Poslední modelové pravidlo bude povolovat webový provoz (WEB-SERVICES) na TCP portech 80 a 443. Tento provoz bude povolen ze sítě učeben (UCEBNY-SUBNET) do Internetu a na obr. 8 je vyznačen oranžovou barvou. Pravidlo TRAFFIC-FROM-CORE-CERNA-POLE bude aplikováno na rozhraní COREVLAN21.



Obr. 8: Přehled ACL pravidel. Zdroj: autor

8.4 Network Address Translation

Pro implementaci a otestování překladu adres opět bude využito připravených modelových pravidel pro anonymizovaný model sítě. Ve verzi Cisco ASA Softwaru 8.3 a novějších se překlad adres definuje přímo pod objekty.

Nejdříve proběhne návrh pro DNAT. V tabulce PREROUTING se nachází záznam, který určuje, že pokud bude provoz cílit na sekundární adresu 195.178.80.11 a TCP porty 800 nebo 900, tak se provede přesměrování na IP adresu serveru 10.45.0.90. Dále pokud provoz cílí na UDP port 390, bude provoz přesměrován na IP adresu 195.178.77.123. Pokud provoz cílí na jiný port, dojde k přesměrování na IP adresu 10.45.0.100.

Jelikož zařízení Cisco ASA neumožňuje definici více adres na jednom rozhraní klasickou metodou a na rozhraní VLAN22 je sekundární adresa zapotřebí, musí se postupovat následujícími kroky. Nejdříve je potřeba zjistit MAC adresu fyzického rozhraní, na kterém se nachází VLAN22 (0000.AB16.DC00), tuto adresu nastavit na fyzickém rozhraní a pro rozhraní VLAN22 vytvořit ARP statický záznam pro IP adresu 195.178.80.11 a MAC adresu 0000.AB16.DC00 a označit tento záznam jako alias.

Dále již lze definovat jednotlivá pravidla pro NAT. Vytvoří se jednotlivé síťové objekty s názvy:

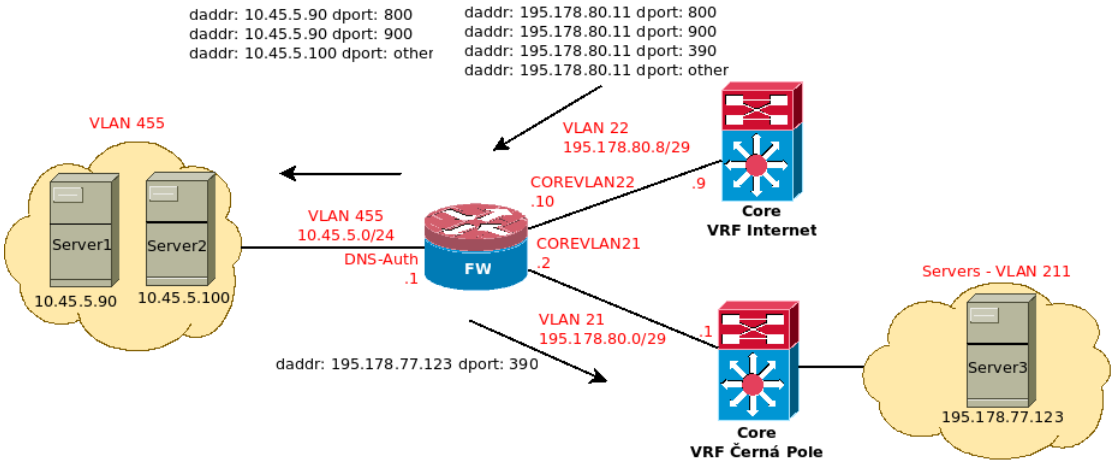
- SERVER_10.45.5.90: server s adresou 10.45.5.90
- SERVER_195.178.77.123: server s adresou 195.178.77.123
- SECONDARY-EXTERNAL-ADDRESS: sekundární adresa 195.178.80.11 na rozhraní VLAN22
- OTHER-TRAFFIC-SECONDARY-ADDRESS: server 10.45.5.100, kam se bude směřovat ostatní provoz cílený na adresu 195.178.80.11.
- SERVER-SERVICES: skupina služeb určených pro server 10.45.5.90. TCP porty 800 a 900.

V těchto objektech (vyjma SERVER-SERVICES) bude definován i překlad adres. Pro objekt SERVER_10.45.5.90 se definuje interní rozhraní DNS-Auth a externí VLAN22. Zde bude očekáván provoz, který bude zapotřebí NATovat. Bude zde zvolena statická metoda překladu a pro provoz, který míří na sekundární adresu na rozhraní VLAN22 (SECONDARY-EXTERNAL-ADDRESS) a určí se, pro které porty se překlad má provádět (SERVER-SERVICES). Jakmile je nastaven NAT, musí být ještě nastaven ACL záznam, který nám tento provoz povolí. Bude vytvořen záznam s názvem DNAT a povolí se zde SERVER-SERVICES pro SERVER_10.45.5.90. Dále je nutné tento ACL záznam aplikovat na rozhraní VLAN22.

NAT pro objekt SERVER_195.178.77.123 bude nastaven obdobně. Bude se lišit adresa, na kterou bude UDP port 390 přesměrován. A také, kterých rozhraní se tento

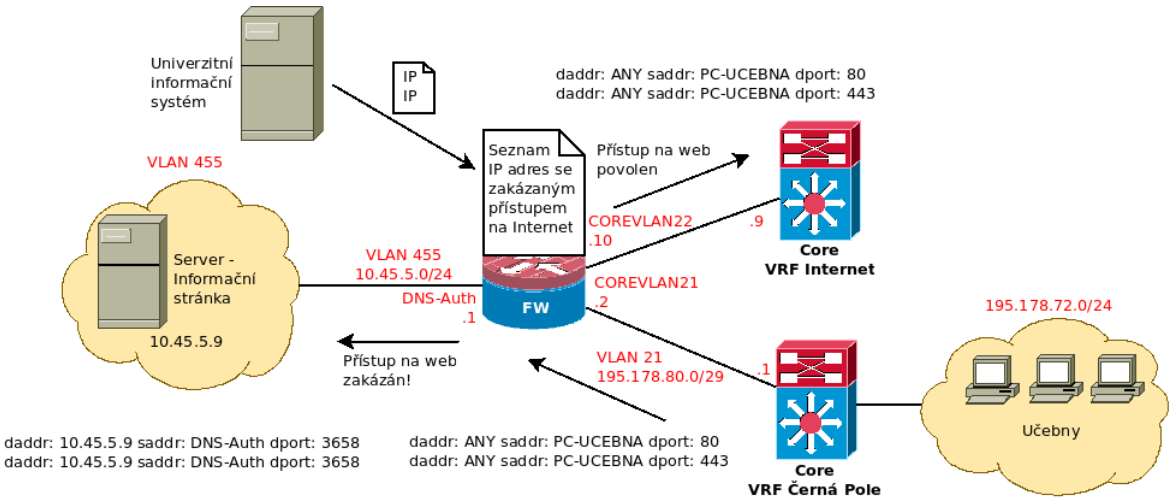
provoz bude týkat. Interní bude VLAN21 a externí VLAN22. ACL pravidlo bude pod stejným názvem jako předchozí záznam, tedy pod DNAT.

V případě, že provoz půjde na jiný port, využije se objektu OTHER-TRAFFIC-SECONDARY-ADDRESS, kde se nastaví interní rozhraní DNS-Auth a externí VLAN22. Tedy stejně jako v prvním případě. Provoz se přesměruje na adresu 10.45.5.100.



Obr. 9: Destination NAT pro služby na serverech. Zdroj: autor

Poslední NAT případ se bude týkat provozu, který má zakázán přístup na webové stránky (porty TCP/80 a TCP/443). Na platformě Cisco ASA není možné provádět označování paketů jako pomocí iptables. Provoz, který má zakázaný internet, tedy není možné opatřit příznakem 0x5a. Bude zapotřebí pracovat pouze se seznamem adres, které mají tento přístup omezen. Provoz bude pomocí *port forwardingu* přesměrován na port 3658 na server s IP adresou 10.45.5.9. Bude zde provedena změna zdrojové IP adresy za adresu rozhraní DNS-Auth.



Obr. 10: Destination NAT a source NAT pro IP adresy s omezeným přístupem k webu. Zdroj: autor

Nejdříve budou vytvořeny potřebné objekty:

- ZAKAZANE-IP-ADRESY-WEB: IP adresy, které budou nahrány z UIS na zařízení z důvodu zákazu přístupu k webu.
- INFORMACNI-STRANKA: IP adresa webového serveru, kde se nachází informační stránka o zablokovaném přístupu k webu.
- OBJECT-WWW: v NAT pravidle bohužel nejde použít nadefinovanou skupinu objektů a je zapotřebí zvlášť definovat jednotlivé porty. Zde se jedná o port TCP/80.
- OBJECT-HTTPS: objekt pro port TCP/443.
- INFORMACNI-STRANKA-PORT: port, na který se má provoz přesměrovat pro zobrazení hlášení o zablokovaném Internetu.

Dále se již nadefinuje pravidlo pro překlad adres. Bude se jednat o provoz, který bude směrován na portu COREVLAN21 směrem do Internetu. A využijí se dříve definované objekty.

8.5 Virtual Private Network

Tato část bude zaměřena na návrh virtuální privátní sítě, mezi které bude patřit bezpečné propojení vzdálených sítí, ale také bezpečné vzdálené připojení uživatelů do univerzitní sítě MENDELU.

IPSec VPN

Jak již bylo popsáno v kapitole Analýza aktuálního stavu, v síti MENDELU jsou dvě významnější vzdálené lokality (Koleje Josefa Taufera a Zahradnická fakulta v Lednici). Jelikož u vzdálené lokality do Lednice se jedná pouze o klasický L2 propoj v rámci jednoho poskytovatele připojení, bude pozornost zaměřena na propojení mezi univerzitním firewallem a kolejemi Josefa Taufera.

Na tomto propoji bude tedy zapotřebí nakonfigurovat protokol IPsec. IPsec provoz je momentálně ještě zaobalen do GRE tunelu, ale ten není na zařízení Cisco ASA implementován. Tento protokol momentálně není nezbytný pro správné fungování tohoto tunelu, takže v návrhu bude pouze varianta s IPsec tunelem. Bezpečnost přenosu dat nebude snížena, protože GRE tunel žádné šifrování nenabízí.

Kdyby vyvstala potřeba mít zde nakonfigurován i GRE tunel, dal by se problém řešit např. routerem, který GRE tunel podporuje, a na tomto zařízení by se GRE tunel ukončoval a poté by se provoz směřoval na univerzitní firewall, kde by se prováděla filtrace. Samozřejmě toto řešení vyžaduje zdroje v podobě dalšího zařízení, případně nějakého stávajícího zařízení, ale s potřebou mít volné porty pro tuto implementaci. Jelikož GRE tunel není podporován, není možné nakonfigurovat *tunnel* rozhraní na prvku. Z tohoto důvodu bude tunel ukončen na rozhraní COREVLAN22 a bude použita i adresa tohoto rozhraní. Ve vzdálené lokalitě na Tauferových kolejí bude zapotřebí také překonfigurovat prvek pro použití tunelu bez *tunnel* rozhraní.

Samotná implementace IPsec tunelu bude rozdělena do pěti základních kroků:

1. Povolení ISAKMP
2. Definice ISAKMP politiky
3. Nastavení typu tunelu
4. Definice IPsec politiky
5. Definice crypto mapy

Povolení ISAKMP

Jako první krok je potřeba povolit ISAKMP protokol, který se stará o výměnu klíčů při navozování IPsec tunelu. Je možnost volby IKEv1 a IKEv2. Druhý zmíněný je novější a bezpečnější varianta, a proto v konfiguraci bude použita tato volba. Tunel se bude terminovat na rozhraní, které směřuje do Internetu, tedy na rozhraní *COREVLAN22*.

Definice ISAKMP politiky

V dalším kroku se vytvoří ISAKMP politika, která bude definovat parametry, které se využijí při navazování tunelu v první fázi. Této politice nejdříve nadefinujeme prioritu, zvolíme prioritu 1. Pro vyšší bezpečnost zvolíme šifrování AES s klíčem 256 bitů. Jedná se o nejvyšší hodnotu, která se může na zařízení nastavit. Dalším bodem bude konfigurace hashovacího algoritmu, kterým bude zvolen SHA. Pro výměnu klíčů bude zvolena Diffie-Hellman skupina č. 5. Jedná se o nejlepší skupinu,

kterou Cisco ASA v testovacím prostředí nabízí. Na novějším softwaru a výkonnějším zařízení bude možné využít pro větší bezpečnost lepší D-H skupinu. A posledním parametrem bude doba platnosti sady ISAKMP klíčů, která bude nastavena na 86 400 sekund.

Nastavení typu tunelu

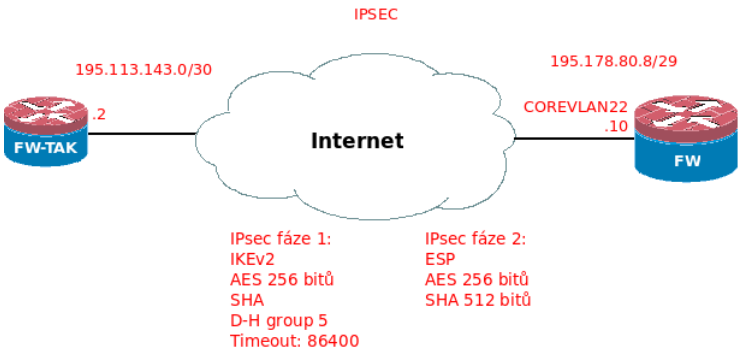
V definici atributů určené pro samotný tunel se nejprve určí IP adresa druhého konce tunelu (*peer*). V tomto případě to bude adresa firewallu na Tauferových kolejích a tou je IP adresa 195.113.143.2. Definuje se typ tunelu, kterým je IPsec Site-to-Site. Dále se nastaví sdílené heslo, které se použije pro vzdálenou a lokální autentizaci. Bude zde definováno heslo *password*.

Definice IPsec politiky

Dalším krokem je nadefinovat IPsec množinu pro přenos dat v tunelu (*transform set*). Tato množina bude mít název IPSEC-TS-TAK a bude zde nastaven protokol ESP. Šifrování pro data bude zvoleno AES s velikostí klíče 256 bitů a pro integritu dat se využije protokolu SHA s klíčem 512 bitů. Mohl by zde vzniknout problém, že šifrování by bylo náročné a zařízení by nezvládalo obsloužit provoz, který by přes tunel procházel. Pokud by se vyskytlo toto omezení, bylo by zapotřebí zvolit nižší šifru.

Definice crypto mapy

Posledním nutným krokem je definice crypto mapy, která se postará o aplikaci dříve nakonfigurovaných kroků a vytvoření IPsec tunelu. Nejdříve je potřeba nastavit ACL pravidlo pro určení, které sítě či adresy mají být šifrovány a posílány pomocí IPsec tunelu. Bude se tedy jednat o sítě 10.51.8.0/21 a 195.113.143.16/28. Tento seznam bude definován v rozšířeném ACL s názvem IPSEC-SITES. Název pro crypto mapu bude zvolen FW-TAK-CRYPTOMAP s prioritou 1. V této crypto mapě bude použit dříve nakonfigurovaný ACL záznam. Dále bude nastavena IP adresa druhého konce tunelu (195.113.143.2) a dříve definovaná transportní množina IPSEC-TS-TAK. Posledním atributem je rozhraní, na kterém se crypto mapa má využívat. Jedná se o rozhraní IPsec tunelu směrem k Tauferovým kolejím, tedy rozhraní COREVLAN22. Po této akci již bude provoz mezi univerzitním firewallem a Tauferovými kolejemi šifrovaný a bezpečný.



Obr. 11: Parametry IPsec fáze 1 a 2. Zdroj: autor

RemoteAccess VPN

V rámci této práce proběhl i průzkum, který měl za úkol zhodnotit možnosti, které univerzita má při přechodu z původní Remote-Access VPN technologie na novou, z pohledu nasazení i z pohledu finanční stránky.

Tento požadavek vzešel od vedoucího Ústavu informačních technologií z důvodu již nedostatečného a problematického řešení. Řešení bylo postavené na protokolu IPsec, který se ukončoval na Cisco VPN koncetrátoru. Uživatelé pro vzdálené spojení do sítě využívali proprietární software Cisco VPN klient, u kterého byl bohužel oznámen konec podpory. Na novějších operačních systémech Windows již ani nebyl podporován a byly komplikace s jeho spuštěním. Bylo zde řešení, které dokázalo zprovoznit tento VPN klient i pod novějším operačním systémem, ale toto řešení vyžadovalo zásah do registrů operačního systému, což není pro uživatele příliš přívětivé. Navíc tento klient již nepodporoval novější a bezpečnější protokol pro výměnu klíčů – IKEv2. Byla tedy řešena alternativa, kde se nejvíce nabízela varianta využití volně dostupného klienta i pro firemní zákazníky od firmy Shrew Soft Inc., která stojí za VPN klientem Shrew. Ale i zde nastal problém. Při navazování tunelu si nedokázal převzít všechny potřebné atributy, které byly důležité, a také již delší dobu není vyvíjen.

Dalším testovaným klientem byl opět proprietární klient od firmy Cisco. Jedná se o Cisco AnyConnect, který je následníkem zastaralého Cisco VPN klienta. Podporuje SSL VPN i IKEv2. Nevýhodou je, že sice zvládá vzdálené spojení pomocí IPsec, ale odečítá licence, které jsou určeny pro SSL VPN. Tyto licence se pro využívání klienta musí dokoupit. K dispozici na zařízení jsou pouze dvě licence pro účely testování. Cisco AnyConnect by byl vhodným řešením z pohledu jednoduchého použití a bezpečnosti, ale bohužel z hlediska finančního není možné v tuto chvíli toto řešení nasadit.

Nakonec bylo rozhodnuto pro jinou Remote-Access VPN technologii. Byla vybrána varianta L2TP over IPsec, která byla i implementována a již běží v síti MENDELU. Tato implementace není v rámci této diplomové práce zahrnuta. Výhodou tohoto řešení je, že uživatelé nemusí instalovat další software, protože je obsažen již ve většině různých operačních systémů. Nevýhodou je, že nepodporuje IKEv2 a jeho bezpečnost může být snížena.

Licence Cisco pro SSL VPN

Problematika licencování pro Remote-Access VPN na platformě Cisco ASA byla telefonicky diskutována s panem F. Pávkem ze společnosti ALEF NULA a.s., hovor proběhl dne 30. 11. 2015.

Licencování určené pro Remote-Access prošlo změnami. Dříve byly k dispozici čtyři varianty licencí. Byly to:

- AnyConnect Essentials
- AnyConnect Premium Peers

- AnyConnect for Mobile
- Shared Premium Licensing

Dnes jsou k dispozici tři typy licencí. První dvě licence AnyConnect Plus a AnyConnect Apex, které nabízejí více služeb k VPN spojení. Změnil se i způsob licencování uživatelů. Dříve se licencoval počet uživatelů, který mohl využívat služeb Remote-Access současně. U těchto licencí je zapotřebí licencovat celkový potenciální počet uživatelů, kteří mohou služby využívat. Licence se dají zakoupit na čtyři různá období platnosti. Na jeden rok, tři roky, pět let. U licence AnyConnect Plus je i možnost neomezené doby platnosti. Dále se licence dělí podle počtu uživatelů. Mohou být objednány licence od 25 až po 250 000 uživatelů.

Licence se dělí podle typu připojení, které uživatelé používají, a také podle služeb, které mohou v rámci licence využívat.

Licence AnyConnect Plus poskytuje tyto služby:

- VPN funkcionalitu pro PC a mobilní platformy, Cisco phone VPN, IKEv2 VPN klienty třetích stran
- Basic device context collection
- IEEE 802.1X Windows supplicant
- Cisco Cloud Web Security agent pro platformy Windows a Mac OS X
- Cisco Advanced Malware Protection pro koncové uzly
- Norma FIPS (Federal Information Processing Standards) (Frahim 2014)

Licence AnyConnect Apex poskytuje tyto služby:

- Využití webového prohlížeče pro terminaci VPN spojení na Cisco ASA zařízení
- Vynucení VPN politik a posture agent ve spojení s Cisco ASA
- Vynucení jednotných politik a posture agent ve spojení s Cisco Identity Services Engine (ISE) 1.3 a novější
- Využití Suite B šifrování s AnyConnect a IKEv2 VPN klienty třetích stran
- Network Visibility module
- Všechny služby licence AnyConnect Plus popsané výše (Frahim 2014)

Během druhého čtvrtletí roku 2016 byl představen nový typ licencí s názvem *VPN Only*. Tato licence slouží pro sestavení SSL/IPsec IKEv2 VPN pomocí Cisco AnyConnect klienta. Výhodou je, že se licence objednávají pro souběžná spojení. Nejmenší počet souběžných spojení, který lze na jednu licenci zakoupit, je 25, největší počet je 10 000 souběžných spojení. Při potřebě většího počtu souběžných spojení se dá koupit licencí více. Licence jsou dostupné pouze jako časově neomezené. (Cisco.com 2016h)

Clientless Remote-Access SSL VPN

Z důvodu udržení kroku s novými technologiemi a snahou poskytnout uživatelům jednoduchý a přívětivý způsob připojení do vzdálené sítě a zpřístupnění zdrojů dostupných pouze v této vzdálené síti, proběhne i návrh a implementace pro stále oblíbenější a rozšířenější Remote-Access SSL VPN, kde pro připojení postačuje pouze webový prohlížeč.

Pro zprovoznění VPN tohoto typu je potřeba nakonfigurovat Group Policy, která určuje, do které skupiny bude patřit uživatel a jaká pravidla a nastavení se budou na tohoto uživatele uplatňovat. Jedná se např. o povolení URL adres, souborových serverů, ke kterým uživatel bude mít přístup, jaký typ VPN se definuje a další atributy. Pro testovací účely se vytvoří Group Policy s názvem MENDELU-RA-GroupPolicy, která bude interní. Mezi atributy se nastaví typ VPN, kterým bude webová VPN. Dále je zapotřebí nakonfigurovat Tunnel Group, kde se nastaví typ VPN a Group Policy, která byla vytvořena v předchozím kroku.

Důležitým krokem je nastavení, jakým způsobem bude prováděna autentizace. Je možnost vytvořit lokální databázi, ale to je velice nepraktické při tisících uživatelích. Proto bude použita autentizace přes autentizační server FreeRadius. V MENDELU síti se využívá propojení FreeRadius s LDAP serverem, ale v této práci bude řešena autentizace pouze přes FreeRadius. Propojení s LDAP serverem je již v síti vyřešeno, tak není zapotřebí toto implementovat. Pro využití autentizace přes FreeRadius server se musí nastavit atributy pro daný server. Tedy IP adresa, na které Radius server naslouchá (192.168.0.36), rozhraní Management a tajný sdílený klíč (cisco).

Ze základních kroků zbývá již pouze povolit tuto VPN na rozhraní. V tomto případě na rozhraní COREVLAN22.

8.6 Vysoká dostupnost

Cisco ASA pro vysokou dostupnost podporuje možnost zapojení prvků do clusteru. Prvky zapojené do clusteru se poté v síti jeví jako jeden logický prvek. Od verze Cisco ASA Software 9.2(1) u modelu ASA 5585-X lze propojit až 16 prvků. Výhodou tohoto řešení je minimalizace doby výpadku při vypadnutí jednoho fyzického prvku. Aktivní prvek také udržuje záložní stavovou tabulku spojení na jiném fyzickém prvku a tedy když aktivní prvek přestane fungovat, nedojde ke ztrátě navázaných spojení. Další výhodou je centralizovaná správa těchto prvků a nulová doba výpadku při provádění upgradu na novou verzi softwaru. Pro vytvoření clusteru je zapotřebí cluster licence, ale o tuto licenci stačí u firmy Cisco pouze zažádat. Tedy na tuto licenci nevznikají další náklady.

Pro spojení prvků do clusteru je zapotřebí dodržet tyto podmínky:

- Stejný model zařízení. Včetně počtu SSP (Security Services Processor).
- Shodné přídavné moduly (např. IPS).

- Shodné nainstalované karty pro rozhraní.
- Shodná licence ohledně šifrování.
- Base nebo Security Plus licence stejná na všech prvcích v clusteru. Ne kombinaci těchto licencí. Z důvodu funkcionality 10GE I/O.

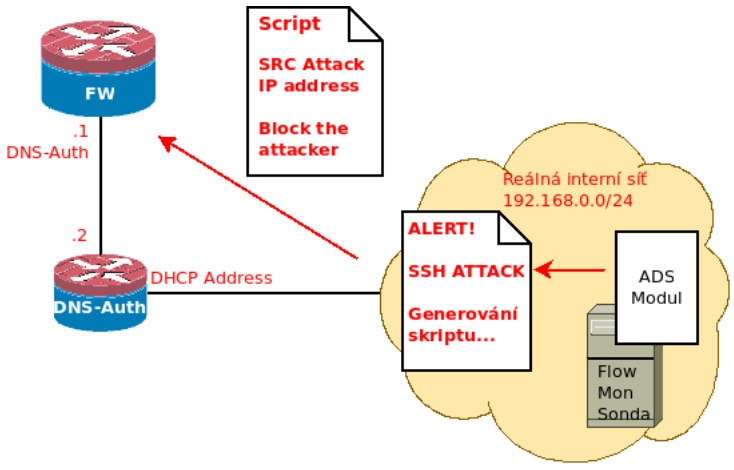
Z důvodu nedostačující verze Cisco ASA software v testovacím prostředí a absence licence pro clustering nebude tato část implementována.

8.7 Dynamicky vkládaná pravidla

Problematika dynamicky vkládaných pravidel bude řešena pomocí FlowMon sondy, která je již v síti MENDELU nasazena. Tato sonda monitoruje a vyhodnocuje provoz, který probíhá v síti. Pro analýzu tohoto provozu je použit ADS modul, který má několik desítek předdefinovaných událostí a každé této události je možnost přiřadit nějakou akci, jako je např. odeslání e-mailu, nahrávání provozu nebo spuštění uživatelsky definovaného skriptu.

V této práci bude zaměřena pozornost právě na uživatelsky definovaný skript. Pro definici skriptu se dá využít bash, perl, python, C a další. Pro potřeby práce se využije skript, který převezme hodnoty od vygenerované události (IP adresu) a definuje pro tuto IP adresu blokovací pravidlo na Cisco ASA. U tohoto pravidla bude ze začátku nastavena časově neomezená blokace a postupem času se ukáže, zda toto řešení je dostačující nebo je zapotřebí politiku upravit.

Pro připojení k zařízení Cisco ASA bude využit protokol SSH z FlowMon sondy. Další variantou, jak propojit Cisco ASA firewall a FlowMon sondu by bylo pomocí RestAPI rozhraní na Cisco ASA, ale bohužel se RestAPI dodává jako přídavný modul pro zařízení, které není volně k dispozici. Další překážkou bylo, že RestAPI je podporované až od novějších verzí Cisco ASA software (9.3(x)), který v testovacím prostředí bohužel nebyl dostupný.



Obr. 12: Komunikace ADS modulu s firewallem. Zdroj: autor

FlowMon sonda bude umístěna v reálné interní síti, kde bude vyhodnocován provoz a případné zákeřné IP adresy přeneseny pomocí skriptu na univerzitní firewall. Pro tvorbu skriptu bude využito skriptovacích jazyků Bash a Expect a vzorové šablony, která je k dispozici ke stáhnutí na ADS modulu.

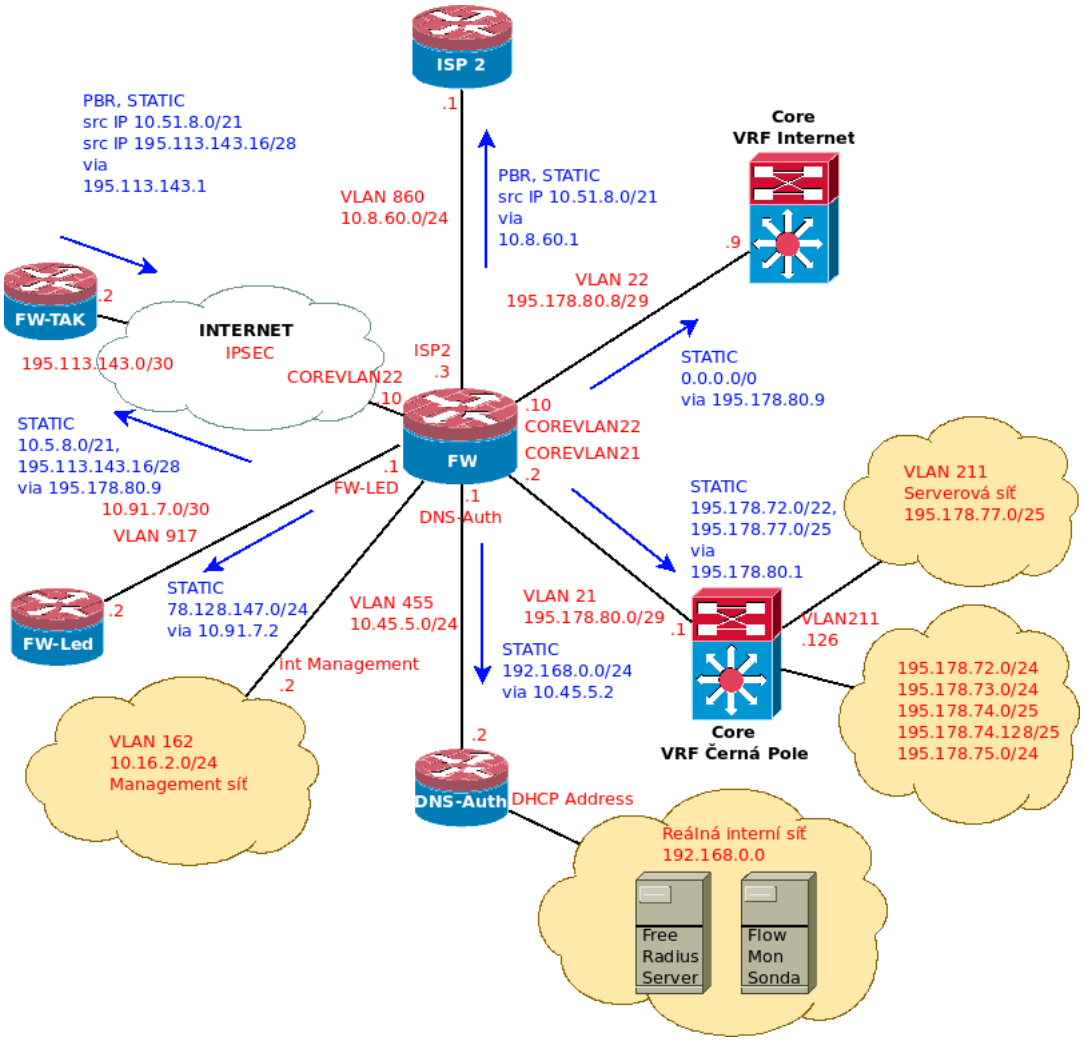
Při výskytu incidentu bude spuštěn skript, kterému bude předán parametr, kterým bude IP adresa útočníka. Dále se pomocí skriptu vykoná přihlášení na univerzitní firewall a zde se do předpřipraveného pravidla s názvem AdresyZeSondyBlok vloží IP adresa útočníka. Skript se opět odhlásí a ukončí SSH spojení.

Nevýhodou tohoto řešení je, že ve skriptu bude v čitelné formě heslo k uživatelskému účtu, který má právo se připojit na SSH a vykonat tuto akci. Řešením by bylo místo autentizace heslem využít autentizace pomocí certifikátu. Ale tato možnost je na platformě Cisco ASA podporována až od verze 8.4(4), která bohužel není v testovacím prostředí dostupná. Uživatel pro přihlášení na Cisco ASA zařízení bude nakonfigurován lokálně s uživatelským jménem *flowmonuser* se stejným heslem.

Pro ukázku funkčnosti bude využita metoda *SSH attack*, pro kterou se nastaví speciální perspektiva s názvem *SSHDICT-Perspective*. Při incidentu, kdy dojde k většímu počtu pokusů připojení ke stroji pomocí SSH a budou končit neúspěšně se aktivuje zmíněná metoda a spustí nadefinovaný skript, který přidá IP adresu do přístupového pravidla na Cisco ASA a adresa bude blokována.

9 Implementace návrhu

Implementace návrhu řešení probíhala především v simulačním programu GNS3. Tento postup byl zvolen z důvodu omezených časových možností pro přístup do laboratoře síťových technologií ÚI PEF MENDELU (probíhá zde výuka a také je zapotřebí přístup do laboratoře pouze s oprávněnou osobou). Prvotní seznámení s prvky probíhalo na fyzických prvcích v laboratoři, ale celková implementace návrhu probíhala v simulačním programu GNS3. Na obr. 13 je zobrazen implementační model.



Obr. 13: Model implementované sítě. Zdroj: autor

9.1 Technikcé vybavení

Pro implementaci návrhu a otestování funkcí firewallu bylo využito následujících zařízení a nástrojů:

- Cisco ASA 5510 Firewall Edition (verze software 8.0(4))
- Cisco ASA 5585-X (verze software 9.5(2))
- Síťový simulátor GNS3 (verze Cisco ASA software 8.4(2))
- Invea FlowMon Probe 4000 (Comguard a.s.)
- Flowmon ADS 8.01.02 (Comguard a.s.)

Flommon sonda a Flowmon ADS modul byly využity v testovacím prostředí společnosti Comguard a.s.

9.2 Základní konfigurace

Název zařízení

Nastavení názvu zařízení pomocí příkazu *hostname*:

- `ciscoasa(config)# hostname FW`
- `FW(config)#`

Rozhraní

Konfigurace rozhraní COREVLAN21 na fyzickém rozhraní Gi0:

```
interface GigabitEthernet0.21
 description Spojeni do Core VLAN 21 - serverova a uzivatelska
 cast
 vlan 21
 nameif COREVLAN21
 security-level 100
 ip address 195.178.80.2 255.255.255.248
```

Konfigurace rozhraní COREVLAN22 na fyzickém rozhraní Gi0:

```
interface GigabitEthernet0.22
 description Spojeni do Core VLAN22 - DMZ a Internet
 vlan 22
 nameif COREVLAN22
 security-level 0
 ip address 195.178.80.10 255.255.255.248
```

Konfigurace rozhraní FW-LED na fyzickém rozhraní Gi1:

```
interface GigabitEthernet1.917
 description Spojeni do vzdalene site Lednice
 vlan 917
 nameif FW-LED
```

```
 security-level 100
 ip address 10.91.7.1 255.255.255.252
```

Konfigurace rozhraní ISP2 na fyzickém rozhraní Gi3:

```
interface GigabitEthernet3.860
 description Spojeni k poskytovateli internetu ISP2
 vlan 860
 nameif ISP2
 security-level 0
 ip address 10.8.60.3 255.255.255.0
```

Konfigurace rozhraní Management na fyzickém rozhraní Gi4:

```
interface GigabitEthernet4.162
 description Management sit
 vlan 162
 nameif Management
 security-level 100
 ip address 10.16.2.1 255.255.255.0
```

Konfigurace rozhraní DNS-Auth na fyzickém rozhraní Gi4:

```
interface GigabitEthernet4.455
 description DNS a autentizacni servery
 vlan 455
 nameif DNS-Auth
 security-level 100
 ip address 10.45.5.1 255.255.255.0
```

Konfigurace sekundární adresy na rozhraní COREVLAN22:

```
interface GigabitEthernet0.22
 mac-address 0000.ab16.dc00
arp VLAN22 195.178.80.11 0000.ab16.dc00 alias
```

SSH přístup

Konfigurace SSH přístupu z management sítě:

```
crypto key generate rsa
ssh 10.45.5.0 255.255.255.0 Management
```

Čas

Konfigurace NTP serveru:

```
ntp server 195.178.77.123 prefer source COREVLAN21
```

ASDM (Adaptive Security Device Manager

Zpřístupnění grafického rozhraní zařízení Cisco ASA:

```
asdm image disk0:/asdm-641.bin
http server enable
http 10.16.2.0 255.255.255.0 Management
```

Zabezpečení přístupu

Konfigurace lokálního uživatele:

```
username admin password admin123
```

Konfigurace zabezpečeného přístupu ke konzoli pomocí lokálního účtu:

```
aaa authentication serial console LOCAL
```

Konfigurace zabezpečeného přístupu k SSH pomocí Radius serveru a lokálního účtu:

```
aaa authentication ssh console Radius LOCAL
```

Konfigurace zabezpečeného přístupu do privilegovaného módu:

```
enable password enable123
```

9.3 Routing

Konfigurace statických routovacích záznamů:

```
route COREVLAN22 0.0.0.0 0.0.0.0 195.178.80.9
route COREVLAN21 195.178.72.0 255.255.252.0 195.178.80.1
route COREVLAN21 195.178.77.0 255.255.255.128 195.178.80.1
route COREVLAN22 10.51.8.0 255.255.248.0 195.178.80.9
route FW-LED 78.128.147.0 255.255.255.0 10.91.7.2
route DNS-Auth 192.168.0.0 255.255.255.0 10.45.5.2
route COREVLAN22 195.113.143.16 255.255.255.240 195.178.80.9
```

Konfigurace Policy Based Routingu:

```
access-list NetFromTAKPBR extended permit ip 10.51.8.0 255.255.248.0
any
route-map TOISP2 permit 10
  match ip address NetFromTAKPBR
  set ip next-hop 10.8.60.1
interface gi2
  policy-route route-map TOISP2
```

9.4 Objekty

Konfigurace objektů, které se využijí v ACL pravidlech. Jako první jsou uvedeny objekty týkajících se služeb. ICMP povolených typů, SNMP, Zabbix, webové služby, služby pro e-mailovou komunikaci a služby určené pro správu zařízení.

```
object-group service ICMP-TYPE-ALLOWED
  service-object icmp echo-reply
  service-object icmp echo
  service-object icmp unreachable
  service-object icmp time-exceeded

object service SNMP-SERVICE
  service udp destination eq snmp

object service ZABBIX-SERVICE
  service udp destination eq 10050

object-group service WEB-SERVICES
  service-object tcp destination eq www
  service-object tcp destination eq https

object-group service MAIL-SERVICES
  service-object tcp destination eq smtp
  service-object tcp destination eq 465

object-group service MGMT-SERVICES
  service-object tcp destination eq ssh
  service-object tcp destination eq 3389
```

Další objekty se týkají síťových objektů. SNMP server, Zabbix, mailové servery, podsíť se servery, management síť a podsíť s počítači v učebnách.

```
object network SNMP-SERVER
  host 10.16.2.10

object network ZABBIX-SERVER
  host 195.178.77.125

object-group network MAIL-SERVERS
  network-object host 195.178.77.25
  network-object host 195.178.77.26

object network SERVERS-SUBNET
```

```
  subnet 195.178.77.0 255.255.255.128

object network MANAGEMENT-SUBNET
  subnet 10.16.2.0 255.255.255.0

object network UCEBNY-SUBNET
  subnet 195.178.72.0 255.255.255.0
```

9.5 Access Control Lists

Konfigurace INPUT pravidel:

```
access-list GLOBAL extended permit object-group ICMP-TYPE-ALLOWED
any any

access-list TRAFFIC-FROM-MANAGEMENT extended permit object
SNMP-SERVICE object SNMP-SERVER interface Management

access-list TRAFFIC-FROM-CORE-CERNA-POLE extended permit object
ZABBIX-SERVICE object ZABBIX-SERVER interface COREVLAN21
```

Dle návrhu zde bude uvedena konfigurace tří modelových FORWARD pravidel:

```
access-list TRAFFIC-FROM-OUTSIDE extended permit object-group
MAIL-SERVICES any object-group MAIL-SERVERS

access-list TRAFFIC-FROM-MANAGEMENT extended permit object-group
MGMT-SERVICES object MANAGEMENT-SUBNET object SERVERS-SUBNET

access-list TRAFFIC-FROM-CORE-CERNA-POLE extended permit object-group
WEB-SERVICES object UCEBNY-SUBNET any
```

A jejich aplikování na rozhraní:

```
access-group TRAFFIC-FROM-CORE-CERNA-POLE in interface COREVLAN21
access-group TRAFFIC-FROM-OUTSIDE in interface COREVLAN22
access-group TRAFFIC-FROM-MANAGEMENT in interface Management
```

9.6 Network Address Translation

Nejprve proběhne konfigurace jednotlivých objektů a definice pravidel pro překlad adres a poté budou definovány jednotlivá přístupová pravidla pro povolení průchodu tohoto provozu.
Konfigurace skupiny objektů služeb pro server 10.45.5.90:

```
object-group service SERVER-SERVICES
```

```
 service-object tcp destination eq 800
 service-object tcp destination eq 900
```

Konfigurace objektu pro sekundární externí adresu na firewallu:

```
object network SECONDARY-EXTERNAL-ADDRESS
 host 195.178.80.11
```

Konfigurace objektu pro IP adresu serveru 10.45.5.90:

```
object network SERVER_10.45.5.90_800
 host 10.45.5.90
 nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS
 service tcp 800 800

object network SERVER_10.45.5.90_900
 host 10.45.5.90
 nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS
 service tcp 900 900
```

Konfigurace objektu pro IP adresu serveru 195.178.77.123:

```
object network SERVER_195.178.77.123
 host 195.178.77.123
 nat (COREVLAN21,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS
 service udp 390 390
```

Konfigurace objektu pro IP adresu serveru, kam směřuje provoz, který není určen pro SERVER_10.45.5.90 nebo SERVER_195.178.77.123:

```
object network OSTATNI-PROVOZ-SECONDARY-ADDRESS
 host 10.45.5.100
 nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS
```

Dále je zapotřebí nakonfigurovat jednotlivá ACL pravidla:

```
access-list TRAFFIC-FROM-OUTSIDE extended permit object-group
SERVER-SERVICES any object SERVER_10.45.5.90

access-list TRAFFIC-FROM-OUTSIDE extended permit udp any object
SERVER_195.178.77.123 eq 390

access-list TRAFFIC-FROM-OUTSIDE extended permit tcp any object
OSTATNI-PROVOZ-SECONDARY-ADDRESS
```

A aplikování na správném rozhraní:

```
access-group TRAFFIC-FROM-OUTSIDE in interface COREVLAN22
```

Poslední pravidlo pro překlad adres omezující přístup k webu a potřebné defince objektů:

```
object network ZAKAZANE-IP-ADRESY-WEB
 host 195.178.80.1

object network INFORMACNI-STRANKA
 host 10.45.5.9

object service OBJECT-WWW
 service tcp destination eq www

object service OBJECT-HTTPS
 service tcp destination eq https

object service INFORMACNI-STRANKA-PORT
 service tcp destination eq 3658

nat (COREVLAN21,DNS-Auth) source static ZAKAZANE-IP-ADRESY-WEB
interface destination static interface INFORMACNI-STRANKA
service OBJECT-WWW INFORMACNI-STRANKA-PORT

nat (COREVLAN21,DNS-Auth) source static ZAKAZANE-IP-ADRESY-WEB
interface destination static interface INFORMACNI-STRANKA
service OBJECT-HTTPS INFORMACNI-STRANKA-PORT
```

9.7 Virtual Private Network

V této části bude provedena implementace dvou typů VPN. První se bude týkat Site-to-Site tunelu mezi univerzitním firewallem a vzdálenou sítí Tauferových kolejí. V druhém případě proběhne implementace Remote-Access SSL VPN pro připojení ke zdrojům univerzity pouze pomocí prohlížeče.

Site-to-Site VPN

Konfigurace Site-to-Site VPN mezi univerzitním firewallem a Tauferovými kolejemi bude rozdělena do 5 kroků:

1. **Povolení ISAKMP**: povolení protokolu pro výměnu klíčů:
   `crypto ikev2 enable VLAN22`
2. **Definice ISAKMP politiky**: v této politice proběhne definice priority politiky, typ šifrování, hashovací algoritmus, Diffie-Hellman skupinu pro odvození klíče a dobu platnosti sady ISAKMP klíčů:

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5
 lifetime seconds 86400
```

3. **Nastavení typu tunelu**: v dalším kroku bude nadefinován typ tunelu, IP adresa vzdálené strany tunelu a sdílené heslo pro autentizaci tunelu:
```
tunnel-group 195.113.143.2 type ipsec-l2l
tunnel-group 195.113.143.2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Cisco123
 ikev2 local-authentication pre-shared-key Cisco123
```

4. **Definice IPsec politiky**: v tomto kroku proběhne definice IPsec politiky, která určí, jaký protokol, šifrování a hashování bude využit pro data v tunelu:
```
crypto ipsec ikev2 ipsec-proposal IPSEC-TS-TAK
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

5. **Definice crypto mapy**: posledním krokem bude definice rozsahu adres, pro které se využije šifrovaný provoz přes tunel, a definice crypto mapy, která bude obsahovat informace, které se nadefinovaly dříve – rozsah adres pro šifrovaný provoz (sítě na vzdálené pobočce Tauferových kolejí), informace o použitém šifrovaní pro IPsec tunel, adresa druhé strany tunelu a rozhraní, na kterém se tato crypto mapa bude aplikovat:
```
access-list FW-TAK-NET extended permit ip any 10.51.8.0
255.255.248.0
access-list FW-TAK-NET extended permit ip any 195.113.143.16
255.255.255.240
crypto map FW-TAK-CRYPTOMAP 1 match address FW-TAK-NET
crypto map FW-TAK-CRYPTOMAP 1 set peer 195.113.143.2
crypto map FW-TAK-CRYPTOMAP 1 set ikev2 ipsec-proposal IPSEC-TS-TAK
crypto map FW-TAK-CRYPTOMAP interface VLAN22
```

Clientless Remote-Access SSL VPN

Konfigurace Group Policy pro SSL VPN s názvem MENDELU-RA-GroupPolicy:
```
group-policy MENDELU-RA-GroupPolicy internal
group-policy MENDELU-RA-GroupPolicy attributes
 vpn-tunnel-protocol ssl-clientless
```

Konfigurace Tunnel Policy pro SSL VPN s názvem MENDELU-RA-TunnelPolicy:
```
tunnel-group MENDELU-RA-TunnelGroup type remote-access
tunnel-group MENDELU-RA-TunnelGroup general-attributes
```

```
 authentication-server-group FreeRadius
 default-group-policy MENDELU-RA-GroupPolicy
```

Nastavení autentizace přes FreeRadius:

```
aaa-server FreeRadius protocol radius
aaa-server FreeRadius (Management) host 192.168.0.36
 key cisco
```

A povolení SSL VPN na rozhraní:

```
webvpn
 enable COREVLAN22
```

9.8 Dynamicky vkládaná pravidla

Veškerá nastavení se budou provádět ve webovém prostředí Flowmon ADS modulu. Pro potřeby skriptu bude nejdříve vytvořena nová perspektiva s názvem *SSHDICT-Perspective*. Na záložce Zpracování -> Perspektivy vytvoříme zmíněnou perspektivu. V perspektivě se vybere priorita *HIGH* a zde se vybere metoda *SSHDICT*. Perspektiva se uloží. Dále je potřeba nahrát uživatelský skript. Na záložce Nastavení -> Uživatelské skripty se přidá nový skript s názvem *skript-flowmon.sh* a vybere se typ *1x pro každou událost*. Poté stačí nahrát skript z lokální stanice. Parametry není zapotřebí nastavovat.

A nastaví se reportování události. Na záložce Zpracování -> Reportování událostí -> Uživatelské skripty se vytvoří nová definice akce. Této akci se přiřadí název, vybere se skript, perspektiva, případně upraví další parametry a akce se aktivuje. Nyní když bude vygenerována SSHDICT událost, spustí se definovaný skript.

Původně byl zamýšlen jeden skript, ve kterém se budou kombinovat skriptovací jazyky Bash a Expect. Tahle kombinace bohužel nefungovala podle představ a skript byl rozdělen do dvou souborů. První, který využívá Bash, se stará o získání IP adresy z Flowmon ADS modulu. Tento skript, s názvem *skript-flowmon.sh*, byl nahrán na Flowmon ADS a bude se spouštět, když nastane daná událost. V tomto skriptu také bude cesta k druhému skriptu, který se jmenuje *skript-asa.sh* a bude mu parametrem předána informace o zdrojové IP adrese. Tento skript bude nahrán na Flowmon sondě, vykoná přihlášení na Cisco ASA zařízení a vytvoří záznam s danou IP adresou. Skripty jsou uvedeny níže.

Skript pro získání zdrojové IP adresy z události ADS modulu (skript-flowmon.sh):

```
#!/bin/bash
LINE_NUM=1
while read line
do
 LINE_NUM=$((LINE_NUM+1))
```

```
  IFS=$''
  WORD_NUM=1
  for WORD in $line
  do
  [ $WORD_NUM -eq 11 ] && {
    ADDRESS=$WORD
  }
    WORD_NUM=$((WORD_NUM+1))
  done
done < /dev/stdin
/home/flowmon/skript-asa.sh $ADDRESS
```

A druhý skript týkající se přihlášení na zařízení Cisco ASA a vložení pravidla (skript-asa.sh):

```
#!/usr/bin/expect -f
set address [lindex $argv 0]
spawn ssh flowmon10.45.5.1
expect "assword:"
send "flowmon"
expect "FW>"
send ""
send "enable"
send ""
send "configure terminal"
send "access-list AdresyZeSondyBlock extended deny ip $address"
255.255.255.255 any"
send "end"
send "exit"
interact
```

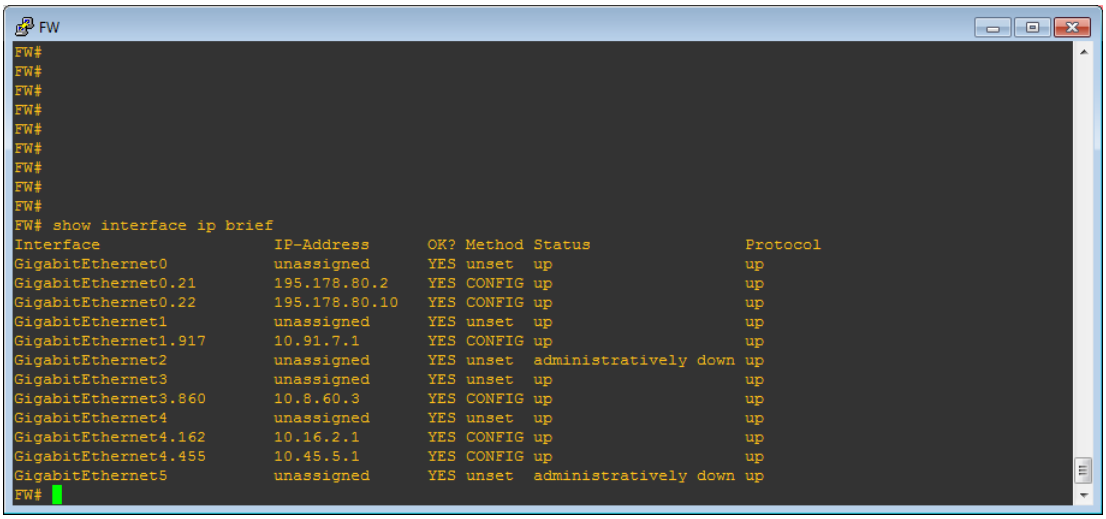
10 Verifikace návrhu řešení

V této kapitole bude ověřeno a otestováno nastavení, které proběhlo v předchozí kapitole týkající se implementace. Budou zde uvedeny výpisy příkazů *show* a v některých případech testy i s ukázkou komunikace pomocí programu *wireshark*, který je určen pro odchyt komunikace.

10.1 Základní ověření

Rozhraní

Kontrola konfigurace rozhraní a jejich stavu příkzem *show interface ip brief*:

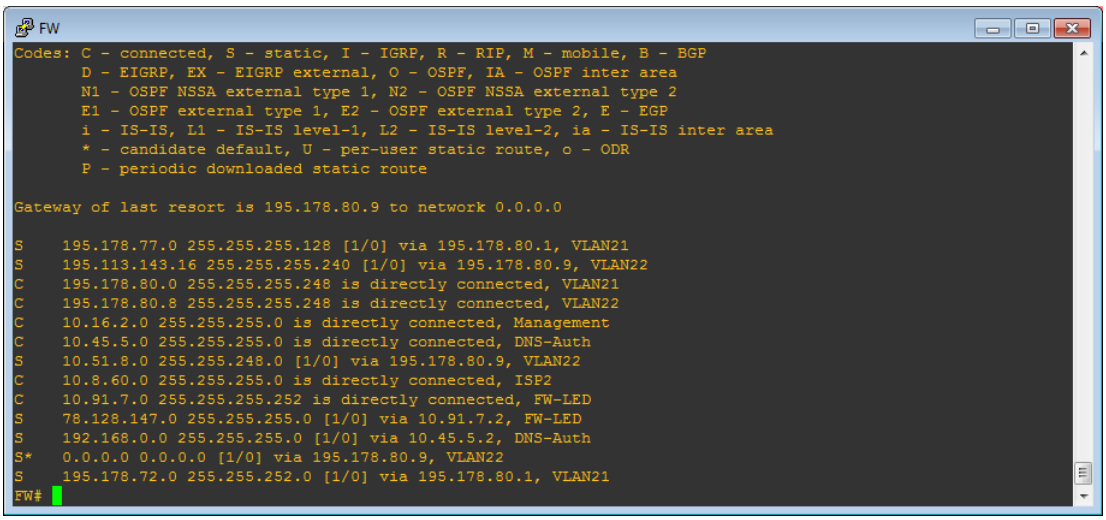


Obr. 14: Kontrola stavu rozhraní. Zdroj: autor

U rozhraní musí být status a protokol ve stavu *up*. Rozhraní *Gi2* a *Gi5* nejsou v návrhu použita, a tedy všechna potřebná rozhraní jsou v pořádku.

Routing

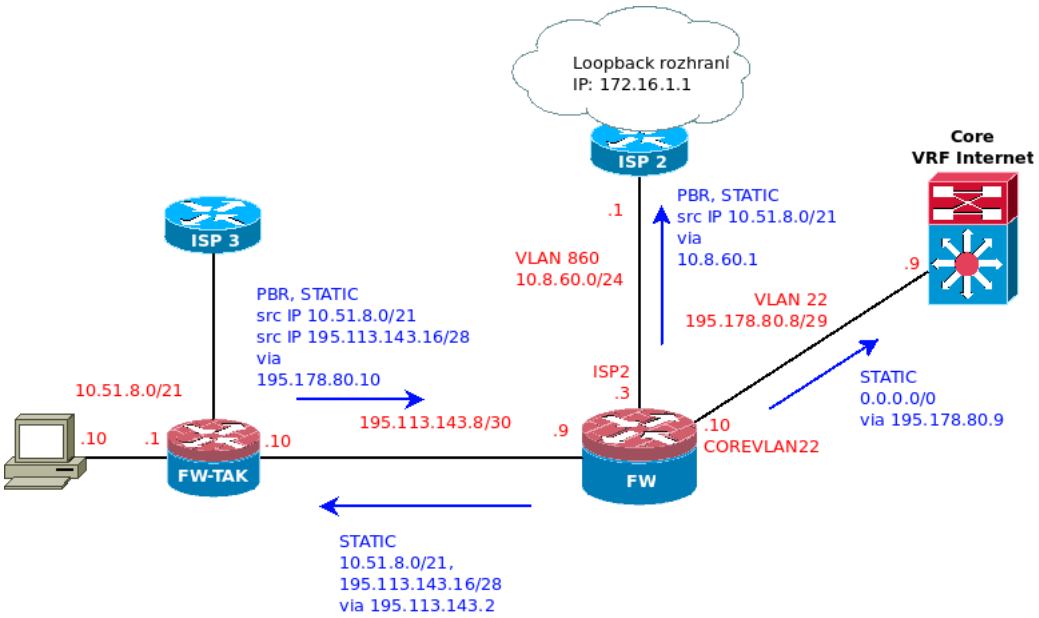
Další výpis se bude týkat směrování. Budou zde všechny přímo připojené sítě a manuální statické záznamy.



Obr. 15: Kontrola směrovacích záznamů. Zdroj: autor

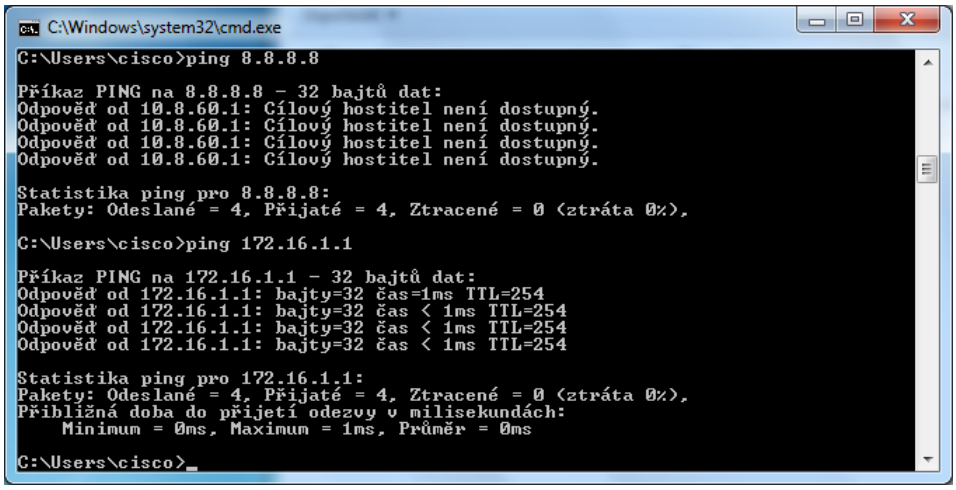
Nachází se zde všechny potřebné směrovací záznamy, které byly zapotřebí nakonfigurovat pro správné fungování testovacího modelu.

Nyní proběhne otestování fungování *Policy Based Routingu*. Tento proces byl proveden přímo na platformě Cisco ASA, která je určena pro produkční prostředí z důvodu přítomnosti novější verze Cisco ASA Software, který podporuje PBR. Testovaní probíhalo pomocí příkazu *ping*, kdy se provedl test se zapnutým a poté s vypnutým PBR na rozhraní. Při tomto testu nebyl implementován IPsec tunel mezi univerzitním firewallem a firewallem na Tauferových kolejích.



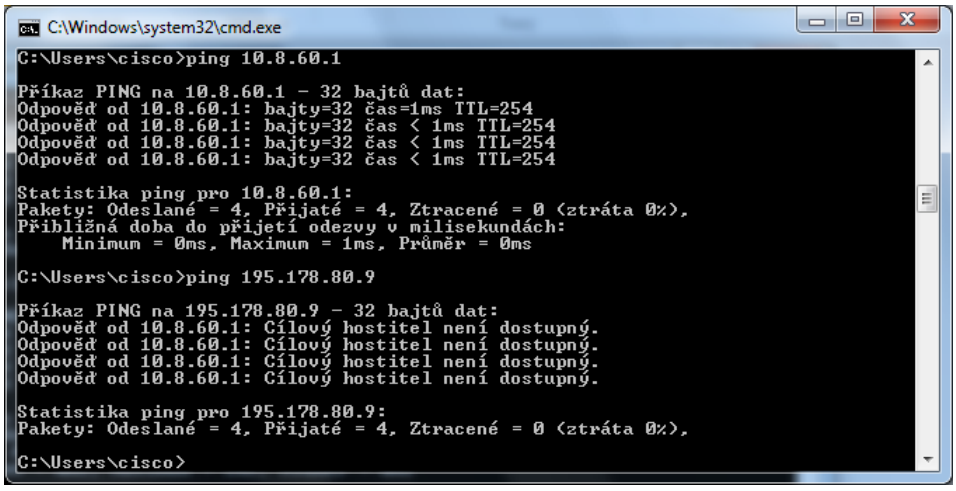
Obr. 16: Model pro otestování *Policy Based Routing*. Zdroj: autor

Na firewall Tauferovy koleje bylo připojeno PC do sítě 10.51.8.0/21 reprezentující komerční síť. Na routeru ISP2 bylo nakonfigurováno *loopback* rozhraní s IP adresou 172.16.1.1, které reprezentuje server v Internetu. Jako první byl vyzkoušen příkaz ping na adresu 8.8.8.8, kde správně odpověděl router ISP2, že cílový hostitel není dostupný. Poté byl proveden ping na adresu *loopback* rozhraní 172.16.1.1, který proběhl v pořádku.



Obr. 17: Úspěšný ping do univerzitní sítě z FW-TAK. Zdroj: autor

Byl ověřen i ping na adresu 195.178.80.9 (*next-hop* adresa defaultního záznamu na univerzitním firewallu), který se opět zachoval správně a odpověď byla obdržena od routeru ISP2.



Obr. 18: Neúspěšný ping IP adresy 195.178.80.9 z FW-TAK. Zdroj: autor

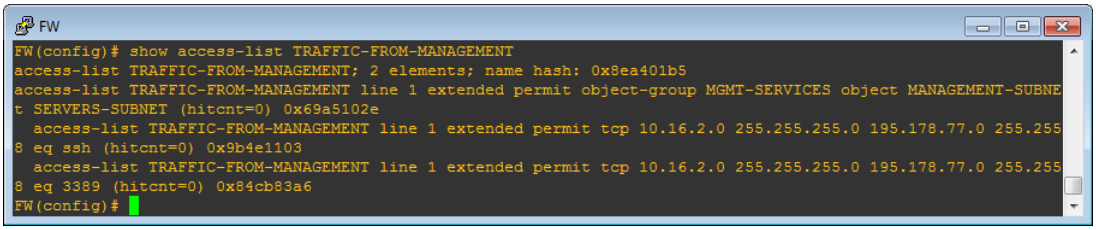
Verifikační test dopadl v pořádku a Policy Based Routing je správně nakonfigurován. Komunikace byla vždy správně přesměrována směrem k ISP2, který slouží

pro komerční subjekty, a správně se nepodařilo spojit s IP adresou 195.178.80.9, která je ve vnitřní síti, ale záznam k této adrese existuje.

10.2 Access Control Lists

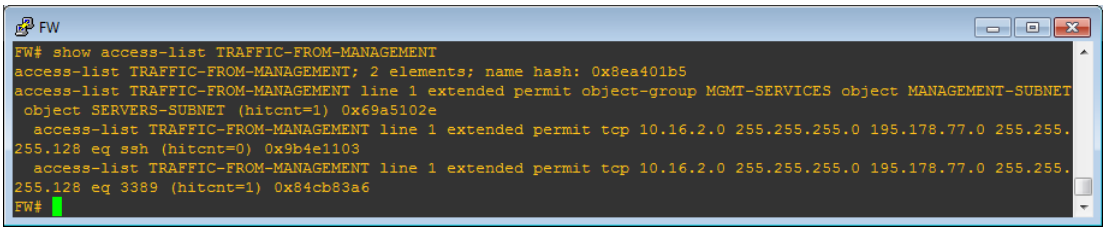
Zde bude verifikační test věnován pravidlu, který se stará o provoz, který míří z Management sítě. Otestuje se zde provoz z routeru s IP adresou 10.16.2.2, který bude směřovat do serverové sítě na adresu 195.178.77.87. Komunikace bude ověřena na portu TCP/3389 pomocí programu *telnet*.

Na obr. 19 lze vidět, že počítadla jsou vynulována.



Obr. 19: Vynulovaná počítadla u pravidla pro management provoz. Zdroj: autor

Spustí se komunikace z routeru v Management síti na port TCP/3389 a do serverové sítě. Nyní na výpisu lze vidět, že pravidlo se shodlo s pravidlem, který se týká této komunikace (viz obr. 20).



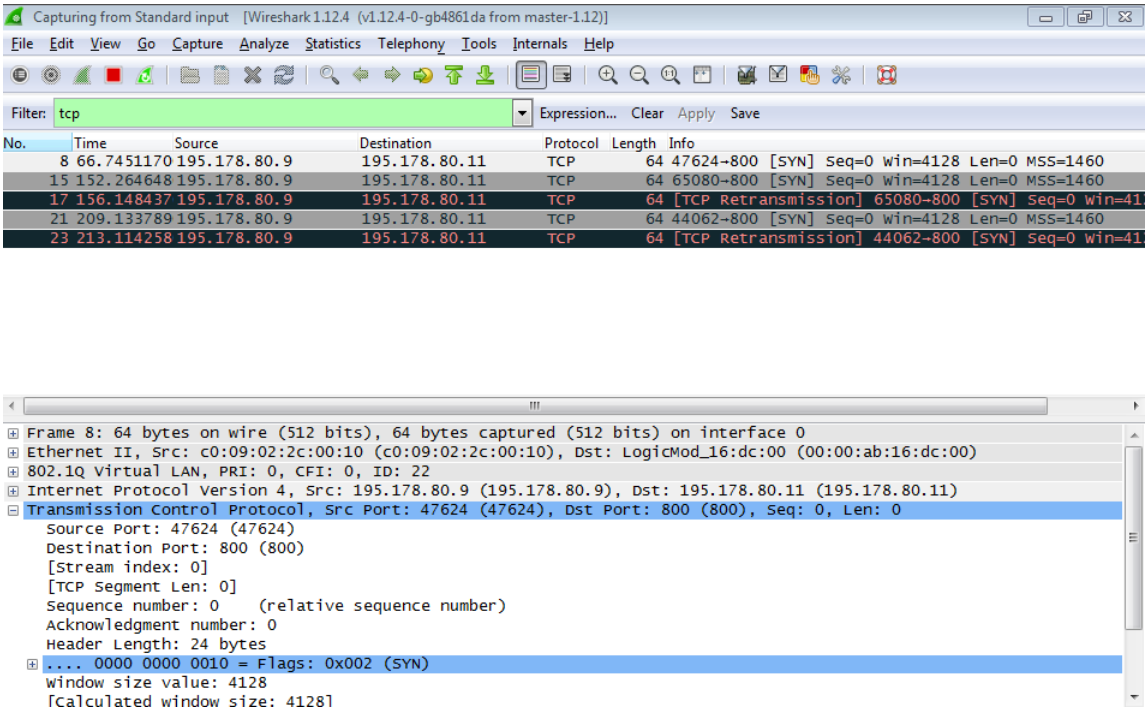
Obr. 20: Zvýšené počítadlo u pravidla pro TCP/3389. Zdroj: autor

10.3 Network Address Translation

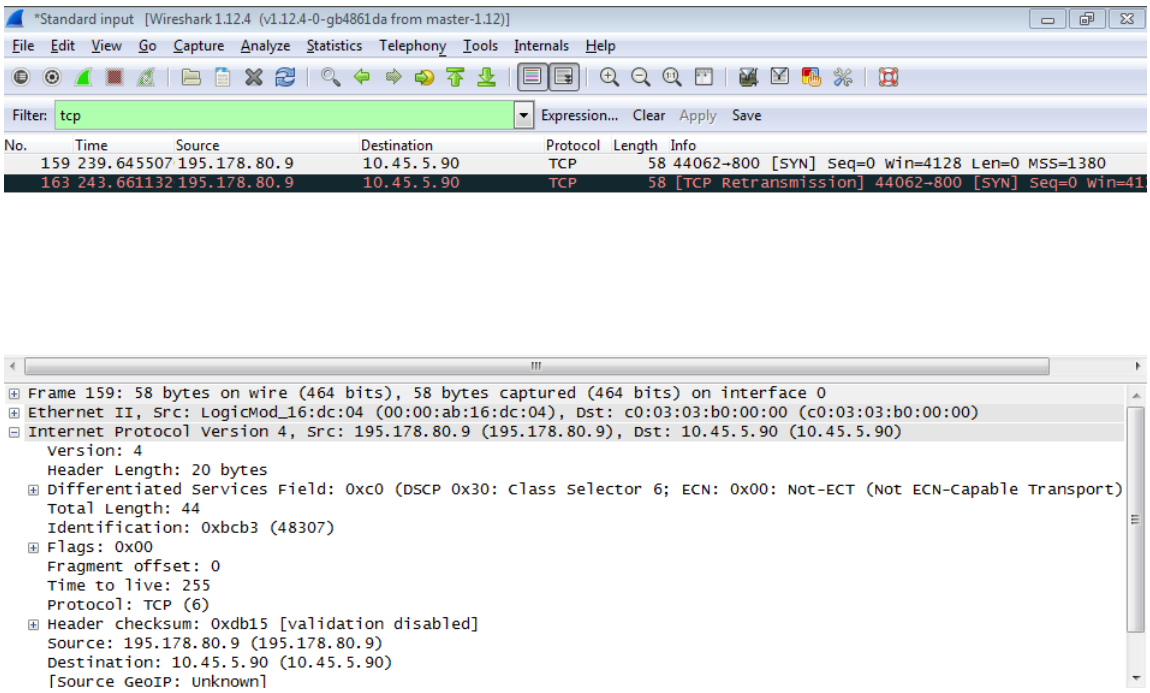
V této kapitole bude otestován překlad adres u provozu, který bude mířit na sekundární externí IP adresu 195.178.80.11 a na port TCP/800. Test bude proveden z *Core* prvku z rozhraní *COREVLAN22*. Pro test se využije nástroj *telnet*, kterému bude změněn defaultní TCP port 23 na port TCP/800. Bude se muset ještě definovat VRF instance, kterou bude *COREVLAN22*. Celý příkaz bude mít následující podobu:

```
CORE#telnet 195.178.80.11 800 /vrf COREVLAN22
```

Zároveň bude spuštěn odchyt na spoji mezi Core prvkem a univerzitním firewallem a mezi univerzitním firewallem a routerem ve VLAN 455, který bude mít na rozhraní IP adresu 10.45.5.90. Výsledky jsou na obrázcích níže:



Obr. 21: Odchyt provozu mezi univerzitním FW a Core prvkem. Zdroj: autor



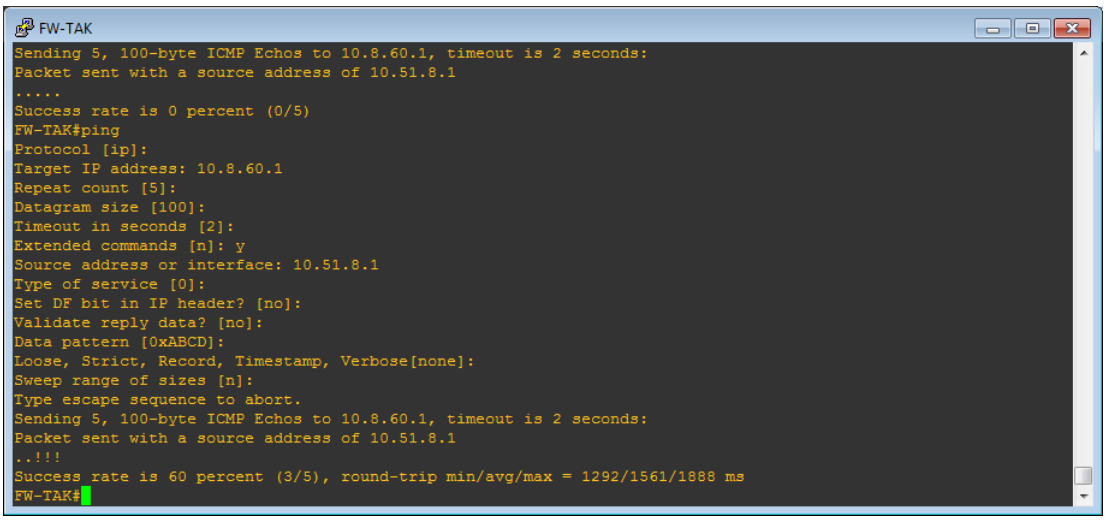
Obr. 22: Odchyt provozu mezi univerzitním FW a DNS-Auth sítí. Zdroj: autor

Na obr. 21 obrázku lze vidět, že komunikace probíhá z IP adresy Core routeru 195.178.80.9 na IP sekundární adresu univerzitního firewallu na portu TCP/800. Na obr. 22 lze pozorovat změnu cílové adresy na IP adresu 10.45.5.90. Zdrojová IP adresa a TCP port jsou zachovány. Není zde žádná odpověď, protože na routeru s IP adresou 10.45.5.90 neběží žádná služba na portu TCP/800.

Překlad adres zde probíhá v pořádku.

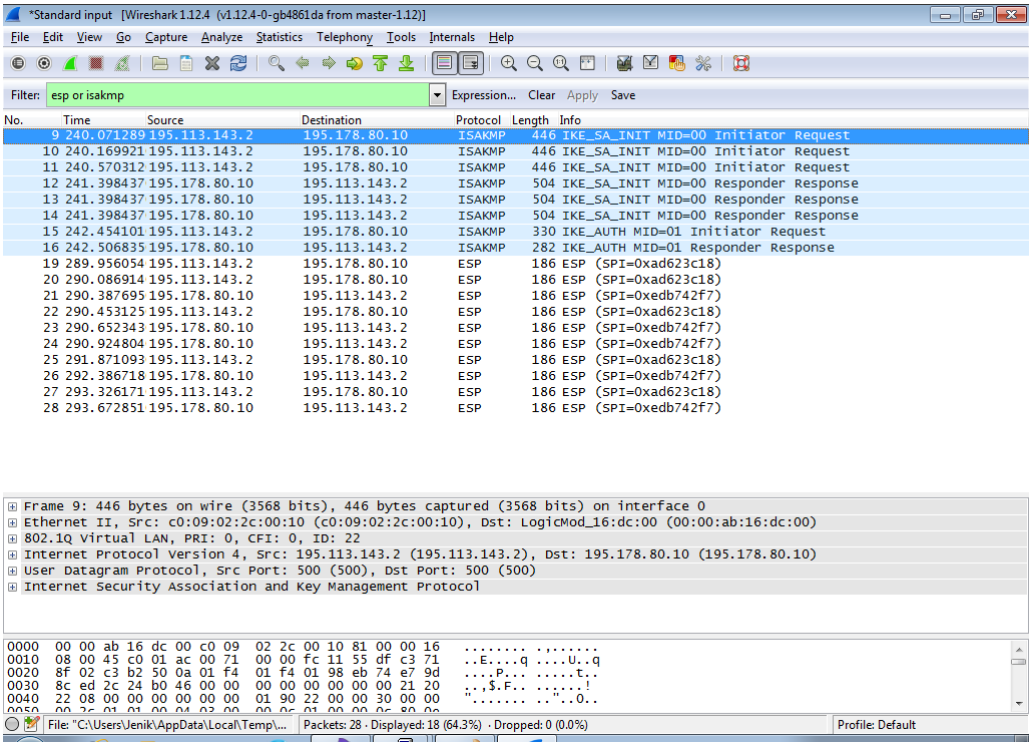
10.4 Site-to-Site VPN

Nyní proběhne ověření navázání Site-to-Site IPsec tunelu mezi univerzitním firewallem a firewallem vzdálené lokality Tauferových kolejí. Test bude vykonán opět pomocí příkazu ping z firewallu Tauferových kolejí se zdrojovou IP adresou 10.51.8.1 na cílovou IP adresu, která se nachází na ISP2 (10.8.60.1).



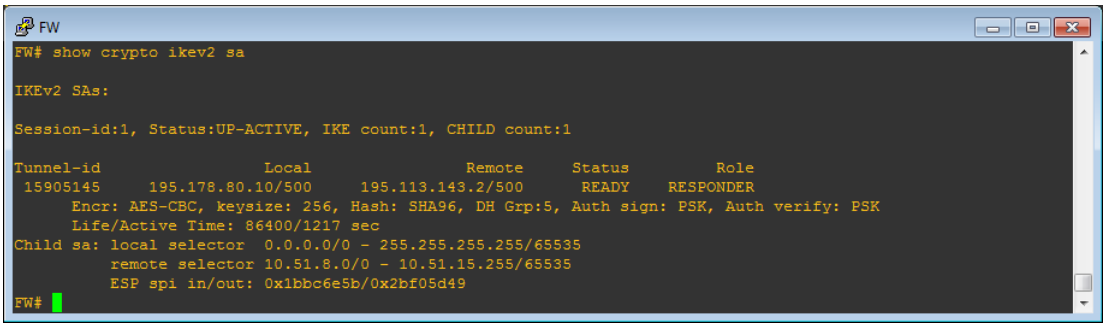
Obr. 23: Ping z FW-TAK přes IPsec tunel. Zdroj: autor

Nejprve proběhne navázání tunelu pomocí protokolu ISAKMP, kde se firewally domluví na klíči pro spojení, a poté probíhá komunikace (ping) v šifrované podobě na protokolu ESP. Viz ukázka odchytu komunikace v programu Wireshark na obr. 24.



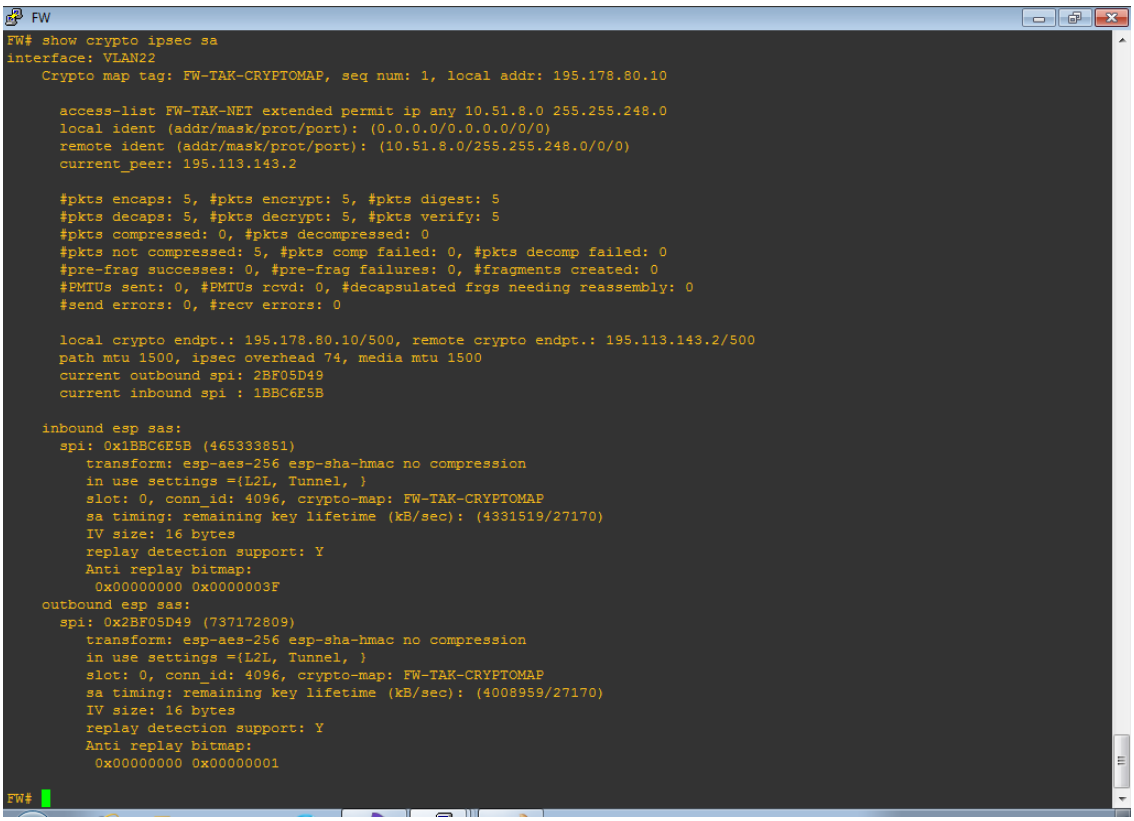
Obr. 24: Odchyt ISAKMP a ESP komunikace - IPsec tunel. Zdroj: autor

Nejdříve je zde vidět komunikace na protokolu ISAKMP, který se stará o výměnu klíčů a informací. Poté, co v pořádku proběhne tato prvotní komunikace a tunel se naváže, jsou již samotné ICMP zprávy přenášeny šifrovaně protokolem ESP. Následně se ještě příkazem *show crypto ikev2 sa* zkontroluje, že tunel je navázán (obr. 25). Jsou zde informace o lokálním a vzdáleném uzlu (IP adresa), status (tunel navázán) a typ šifrování a hashe.



Obr. 25: Zobrazení *security associations* pro protokol IKEv2. Zdroj: autor

Příkazem show crypto ipsec sa se zobrazí detailnější informace o navázaném tunelu (obr. 26). V tomto výpise se dají zjistit další informace. Např. kterého rozhraní se IPsec tunel týká (COREVLAN22), jaká crypto mapa byla použita (FW-TAK-CRYPTOMAP), které přístupové pravidlo (FW-TAK-NET).



Obr. 26: Zobrazení *security associations* pro protokol IPsec. Zdroj: autor

Pro kontrolu, zda při navazování tunelu nenastala nějaká chyba, bude využit příkaz *debug crypto ipsec 150*. Výstup tohoto příkazu je obsažen v příloze A.

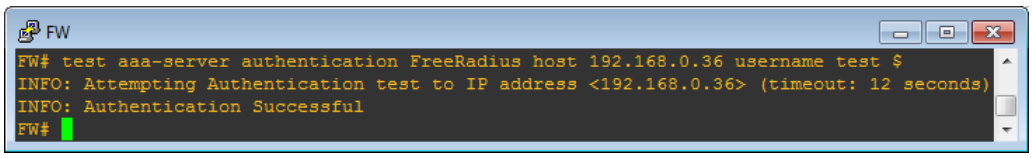
Ve výpisu nebyla objevena žádná chyba. Tunel se mezi univerzitním firewallem a firewallem na Tauferových kolejích v pořádku navazuje. A v pořádku také šifruje provoz pro tunel určený.

10.5 Clientless Remote-Access SSL VPN

U Remote-Access SSL VPN bude otestován přístup na webový portál a otestováno přihlášení pomocí FreeRadius serveru. Pro otestování komunikace s FreeRadius serverem a zjištění funkčnosti přihlašovacích údajů lze využít následující příkaz:

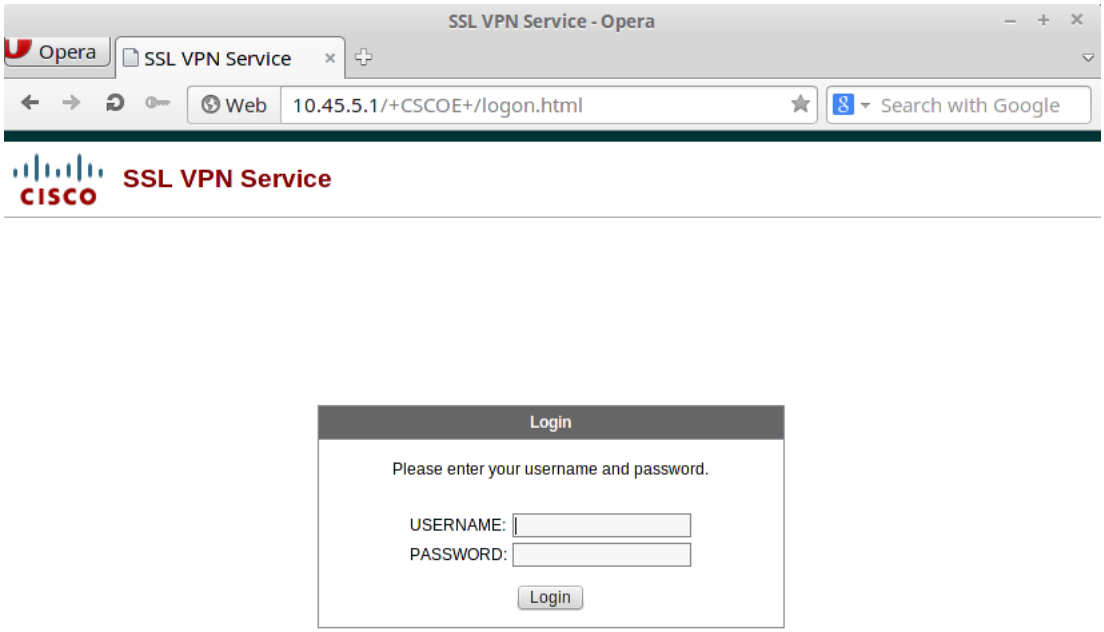
```
FW# test aaa-server authentication FreeRadius host 192.168.0.36
username test password test
```

Volba FreeRadius určuje, která definice autentizačního serveru bude použita. Volbou *host* se určí IP adresa autentizačního serveru a zvolí uživatelské jméno a heslo. V tomto případě test/test. Tyto údaje jsou nastaveny na FreeRadius serveru.



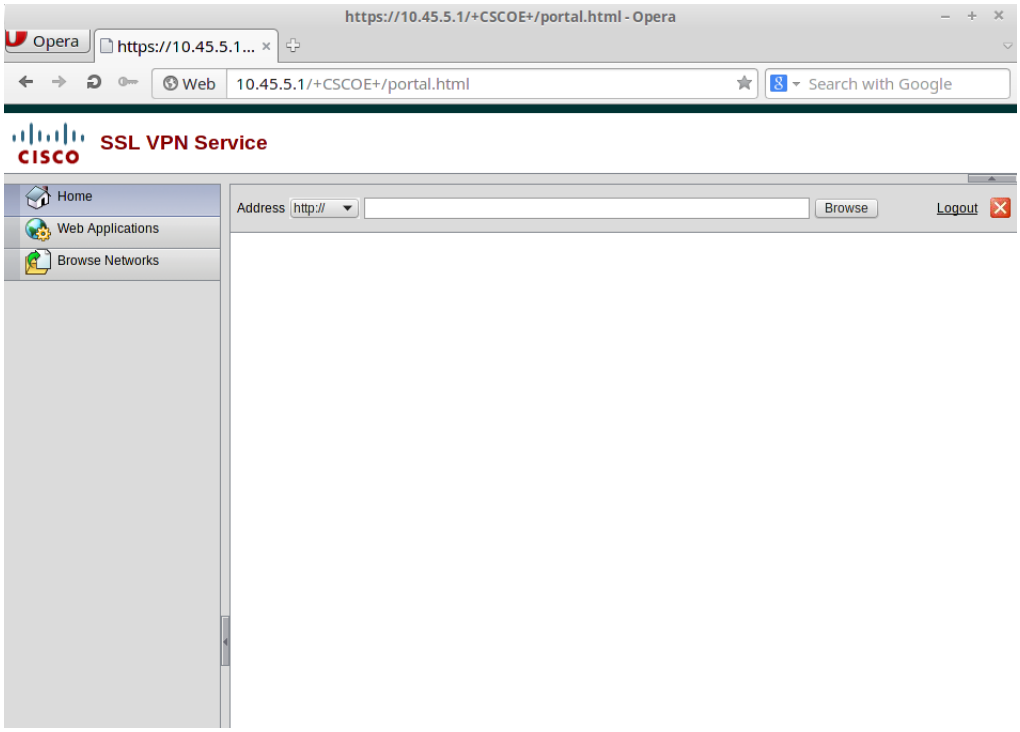
Obr. 27: Test autentizace vůči FreeRadius serveru. Zdroj: autor

Zmíněný příkaz vrátil *Authentication Successful*. Znamená to tedy, že autentizační server ve spojení s Cisco ASA pracuje v pořádku. Po přístupu na adresu https://10.45.5.1 se zobrazí přihlašovací stránka SSL VPN portálu.



Obr. 28: SSL VPN portál. Zdroj: autor

A na obr. 29 je vidět portál po úspěšném přihlášení:



Obr. 29: SSL VPN portál po přihlášení. Zdroj: autor

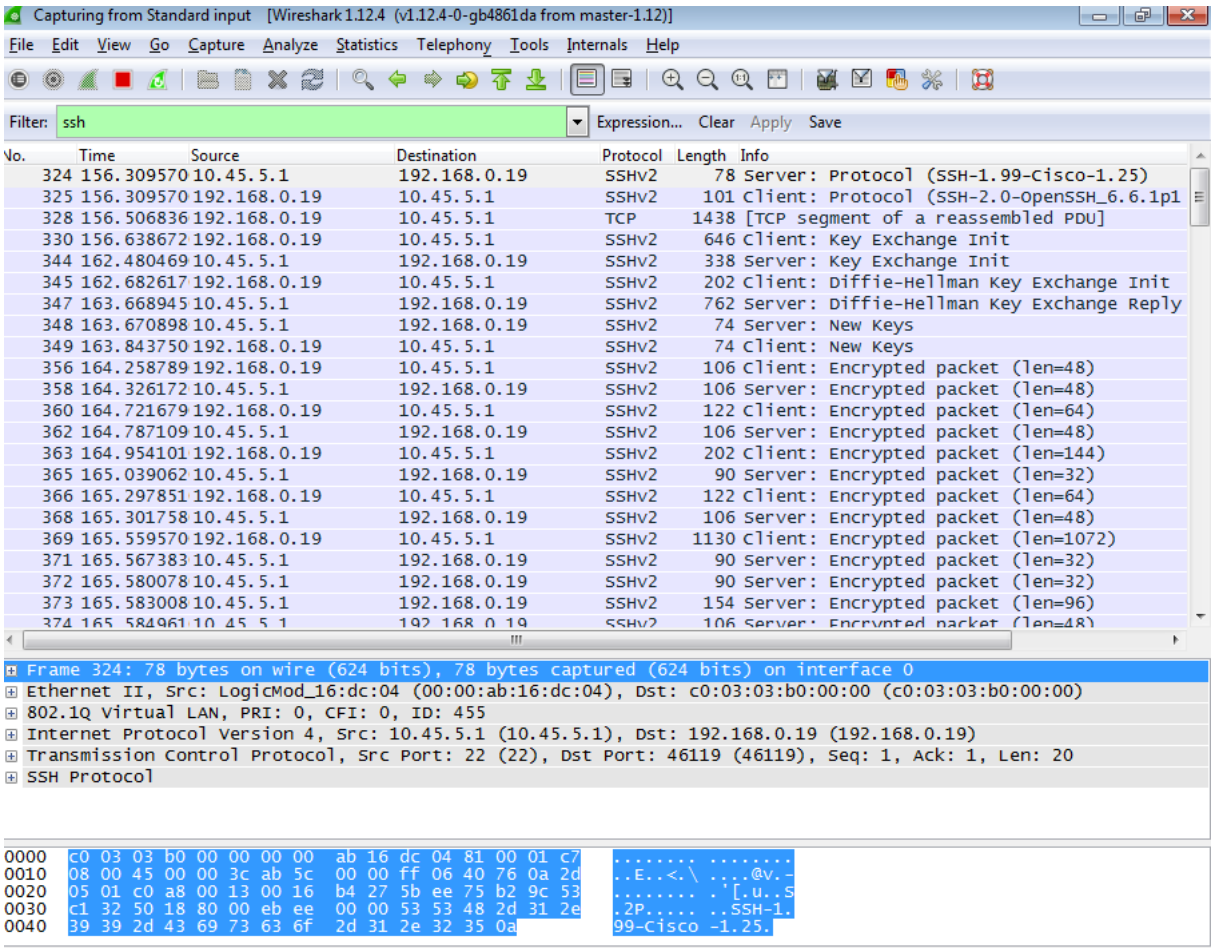
10.6 Dynamické vkládání pravidel

Z důvodu docela častých SSH útoků na externí IP adresy byla verifikace provedena na ostrém provozu. Byl tedy nastaven skript dle uvedených kroků v kapitole implementace. Spustil se odchyt provozu na spoji v testovacím prostředí vedoucímu k zařízení Cisco ASA a vyčkávalo se, až Flowmon ADS modul vytvoří SSHDICT událost a spustí skript. Na obr. 30 je záznam z ADS modulu takového SSH útoku (je zde vymazána externí IP adresa společnosti Comguard a.s.). Útočná adresa je 221.194.47.224.

221.194.47.224	SSHDICT	End of attack (unsuccessful), summary: Total count of targets: 1, maximum transferred: 2.23 KiB, total count of attempts: 24, duration of attack: 379.85 seconds (6m 20s). Part of distributed attack.	2017-01-02 17:30:00	Default	

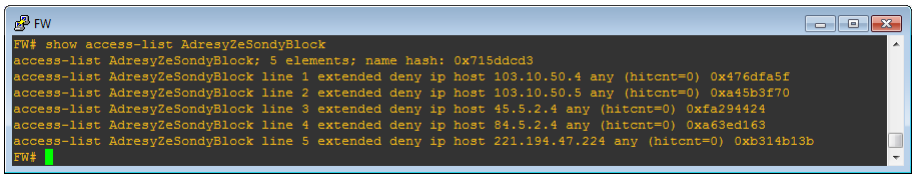
Obr. 30: Událost z Flowmon ADS modulu. Zdroj: autor

Na obr. 31 je vidět inicializace SSH spojení z Flowmon sondy (IP adresa 192.168.0.19) na IP adresu rozhraní DNS-Auth (10.45.5.1).



Obr. 31: Událost z Flowmon ADS modulu. Zdroj: autor

A na obr. 32 se nachází výpis přístupového pravidla *AdresyZeSondyBlock*. Nachází se zde více adres z dřívějšího testování, ale jako poslední je IP adresa, která se týká vygenerované události na Flowmon ADS modulu.



Obr. 32: Zobrazení seznamu adres z Flowmon sondy. Zdroj: autor

Dynamické vkládání pravidel pomocí skriptu z Flowmon sondy je tedy funkční.

11 Ekonomické zhodnocení řešení

V této kapitole proběhne ekonomické zhodnocení provedeného návrhu řešení. Budou zde zahrnuty náklady na pořízení hardwaru, licencí a náklady na implementaci. Pro výpočet nákladů na HW a licence budou použity ceny uvedené v oficiálním ceníku. U HW bude započítán pouze prvek navíc pro potřeby vysoké dostupnosti. První prvek již univerzita vlastní. Prvek má kód ASA5585-S20-K9 a cena je 59 995,- dolarů.

Další položkou budou licence na provozování SSL Remote-Access VPN. Bude zde počítáno s licencemi typu VPN Only, které neaktivují žádné dodatečné funkcionality, ale pouze umožní uživatelům využívat VPN připojení. Do celkových nákladů bude uvedena cena pro 100 souběžných spojení. Produkt má označení L-AC-VPNO-100= a uvedená cena je 13 995,- dolarů.

Doba celkové implementace by mohla být zhruba 60 člověkodní (1 člověkoden = 8 hodin) s cenou 1 000,- Kč za jednu člověkohodinu.

Tab. 1: Ekonomické zhodnocení řešení

Produkt	**Popis**	**Cena v Kč**
ASA5585-S20-K9	HW	Cca 1 500 000,-
L-AC-VPNO-100=	SSL VPN licence	Cca 360 000,-
Práce technika	60 člověkodní	480 000,-
Cena celkem:		**2 340 000,-**

Dle tab. 1 jsou celkové náklady na migraci ve formě vysoké dostupnosti vypočteny na 2 340 000,- Kč.

12 Závěr

Cílem této diplomové práce bylo navrhnout nové řešení univerzitního firewallu na platformě Cisco ASA včetně jeho implementace. Po obeznámení se s novou platformou proběhla analýza uživatelských požadavků a také analýza aktuálního stavu se zástupci Ústavu informačních technologií. Po analýze byl vypracován návrh řešení na platformě Cisco ASA, který obsahoval řešení technologií routingu, přístupových pravidel, dynamicky vkládaných pravidel, VPN a NAT.

Po návrhu následovala implementace řešení, která byla provedena v prostředí síťového simulátoru GNS3. Implementaci se nepodařilo provést 1:1 k současnému řešení, ale tyto nedostatky nejsou zásadní a nijak nesnižují zabezpečení univerzitní sítě. Jedná se především implementaci GRE tunelu, který na platformě Cisco ASA není podporován. Také není možné na této platformě označovat pakety příznaky, které byly využity pro filtraci provozu z učeben, které měly vypnutý přístup k Internetu. Ostatní funkcionality se podařilo zachovat a implementovat.

Práce se také věnovala vzdálenému přístupu uživatelů do sítě pomocí Remote-Access SSL VPN pouze přes webový prohlížeč. Samotná implementace byla provedena a bylo ověřeno i přihlašování pomocí FreeRadius serveru. Bohužel z časových důvodů se nepodařilo VPN naimplementovat detailněji. V rámci práce byly také zjišťovány požadavky pro SSL VPN z pohledu licencí, jelikož u základní licence je poskytován přístup pouze dvěma uživatelům pro testování této VPN. Výhodou je, že během roku 2016 byl představen nový typ licencí, který je určen pouze pro přístup na VPN (bez dodatečných funkcionalit). Tento typ licencí by mohl být pro univerzitu zajímavý a byl zahrnut také do ekonomického zhodnocení řešení.

Pro zvýšení bezpečnosti univerzitní sítě byla navrhnuta a implementována dynamicky vkládaná pravidla na základě výstupů analýzy provozu Flowmon sondy, která je již v síti nasazena. Byl napsán skript, který se postará o vytvoření blokačního pravidla na firewallu na základě zdrojové adresy získané ze sondy.

Nevýhodou přechodu na nové řešení je, že je momentálně k dispozici pouze jedno zařízení. Pokud by nastal výpadek tohoto prvku, systémy by byly nedostupné. Bylo by tedy zapotřebí pořídit sekundární prvek pro zachování dostupnosti i v případě výpadku jednoho prvku. Další nevýhodou tohoto řešení je celková cena na pořízení nového řešení (sekundární prvek, implementační práce, licence pro SSL VPN), která byla v rámci ekonomického zhodnocení vyčíslena přibližně na 2 340 000,- Kč. Na druhou stranu by univerzita získala moderní bezpečnostní řešení s velkým výkonem, vysokou propustností a užitečnými funkcionalitami. Mezi tyto funkcionality patří již zmíněná SSL VPN, která podporuje vysokou bezpečnost. Existuje také možnost bezpečnost dále zvyšovat zakoupením rozšiřujících modulů (např. IPS modulu).

13 Literatura

BOUŠKA Petr. *TCP/IP - Routing - směrování*. 2007b Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/.

BOUŠKA Petr. *VLAN - Virtual Local Area Network*. 2007a Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

BROULÍK, Jiří. *Srovnání platforem pro zabezpečení počítačových sítí*. Hradec Králové, 2015. Bakalářská práce.

Chris Hoffman. *Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP*. 2015 Dostupné z: http://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpipsec-vs.-sstp/.

Cisco.com. *Adding an Extended Access List*. 2013 Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/acl_extended.html.

Cisco.com. *Cisco Adaptive Security Appliance (ASA) Software*. 2014c Dostupné z: http://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html.

Cisco.com. *Cisco AnyConnect*. 2016h Dostupné z: http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf.

Cisco.com. *Configure Clientless SSL VPN (WebVPN) on the ASA*. 2016e Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html.

Cisco.com. *Configure Commonly Used IP ACLs*. 2016g Dostupné z: http://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html.

Cisco.com. *Configuring IPSec and ISAKMP*. 2014b Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_ike.html.

Cisco.com. *NAT Examples and Reference*. 2016f Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/firewall/asa-95-firewall-config/nat-reference.html.

Cisco.com. *Policy Based Routing*. 2016d Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/general/asa-94-general-config/route-policy-based.html.

Cisco.com. *Routing Overview*. 2016b Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-general-config/route-overview.html.

Cisco.com. *Static and Default Routes*. 2016c Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-general-config/route-static.html.

Cisco.com. *Virtual Routing and Forwarding*. 2014a Dostupné z: http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37/vrf.html.

Cisco.com. *VLAN Interfaces*. 2016a Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/general/asa-95-general-config/interface-vlan.html.

DOSTAL, Jakub. *Monitoring a správa sítě pomocí Cisco ASA firewallu*. Ostrava, 2015. Bakalářská práce.

FILLA, Milan. *Realizace firemního firewallu s použitím Cisco technologií*. Brno, 2010. Bakalářská práce.

Flowmon.com. *Flowmon Sonda*. 2016a Dostupné z: https://www.flowmon.com/getattachment/fd92a24b-17ca-4dbb-bd0f-aa65981a9275/Flowmon-Probe-Product-Brief.aspx.

Flowmon.com. *Výkonný NetFlow/IPFIX kolektor pro detailní přehled o dění v síti*. 2016b Dostupné z: https://www.flowmon.com/cs/products/flowmon/netflow-collector.

Flowmon.com. *Vypořádejte se s bezpečnostními hrozbami a provozními problémy ve vaší síti*. 2016c Dostupné z: https://www.flowmon.com/cs/products/flowmon/anomaly-detection-system.

Flowmon.com. *Vypořádejte se s bezpečnostními hrozbami a provozními problémy ve vaší síti*. 2016d Dostupné z: https://flowmon.invea.com/doc/flowmon_userguide_cz.pdf.

Flowmon.com. *Vypořádejte se s bezpečnostními hrozbami a provozními problémy ve vaší síti*. 2016e Dostupné z: https://flowmon.invea.com/doc/flowmon_ads_business_userguide_cz.pdf.

FRAHIM, Jazib. *Cisco Asa: all-in-one next-generation firewall, IPS, and VPN services. 3rd Ed*. Indianapolis, IN: Cisco Press, 2014 ISBN 9781587143076.

Harald Welte, Pablo Neira Ayuso. *Netfilter/iptables project*. 2014 Dostupné z: http://www.netfilter.org/.

HERVE EYCHENNE. *Man page of IPTABLES*. 2015 Dostupné z: http://ipset.netfilter.org/iptables.man.html.

IETF. *RFC 1104*. Dostupné z: https://tools.ietf.org/html/rfc1104.

IETF. *RFC 1349*. Dostupné z: https://tools.ietf.org/html/rfc1349.

IETF. *RFC 2474*. Dostupné z: https://tools.ietf.org/html/rfc2474.

IETF. *RFC 6864*. Dostupné z: https://tools.ietf.org/html/rfc6864.

IETF. *RFC 768*. Dostupné z: https://tools.ietf.org/html/rfc768.

IETF. *RFC 791*. 1981 Dostupné z: https://tools.ietf.org/html/rfc791.

IETF. *RFC 793*. Dostupné z: https://tools.ietf.org/html/rfc793.

JEFF DOYLE. *Understanding MPLS VPNs, Part I*. 2008 Dostupné z: http://www.networkworld.com/article/2350732/cisco-subnet/understanding-mpls-vpns–part-i.html.

JUNIPER.NET. *Understanding Generic Routing Encapsulation*. 2014 Dostupné z: https://www.juniper.net/documentation/en_US/junos13.3/topics/concept/gre-tunnel-services.html.

KOZÁK, MARTIN. *Propojení firemních poboček pomocí virtuální privátní sítě*. Zlín, 2012. Bakalářská práce.

LAŠ, JAROSLAV. *Zabezpečení datové komunikace pomocí bezpečnostní brány firewall ASA*. Ostrava, 2012. Bakalářská práce.

MIKROTIK.COM. *Manual:IP/Firewall/NAT*. 2016 Dostupné z: http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT.

PETŘÍČEK, MIROSLAV. *Stavíme firewall (1)* Dostupné z: https://www.root.cz/clanky/stavime-firewall-1/.

PETŘÍČEK, MIROSLAV. *Stavíme firewall (3)* Dostupné z: https://www.root.cz/clanky/stavime-firewall-3/.

STEVE FRIEDL. *An Illustrated Guide to IPsec*. 2005 Dostupné z: http://www.unixwiz.net/techtips/iguide-ipsec.html.

TYSON, JEFF. *How Network Address Translation Works*. 2001 Dostupné z: http://computer.howstuffworks.com/nat1.htm.

VYHNÁNEK, JAN. *Generátor základních filtrovacích pravidel pro konfiguraci firewallů na síťových zařízeních*. Brno, 2013. Bakalářská práce.

Přílohy

A Výstup debug příkazu (IPsec)

```
FW# IPSEC: New embryonic SA created  0xb65bc440,
      SCB: 0xBCB85B90,
      Direction: inbound
      SPI : 0x74C64097
      Session ID: 0x00003000
      VPIF num : 0x00000003
      Tunnel type: l2l
      Protocol : esp
      Lifetime : 240 seconds
      IPSEC: New embryonic SA created  0xbcb843a8,
      SCB: 0xBCB85308,
      Direction: outbound
      SPI : 0xB663BFA9
      Session ID: 0x00003000
      VPIF num : 0x00000003
      Tunnel type: l2l
      Protocol : esp
      Lifetime : 240 seconds
      IPSEC: Completed host OBSA update, SPI 0xB663BFA9
      IPSEC: Creating outbound VPN context, SPI 0xB663BFA9
      Flags: 0x00000005
      SA : 0xbcb843a8
      SPI : 0xB663BFA9
      MTU : 1500 bytes
      VCID : 0x00000000
      Peer : 0x00000000
      SCB : 0x000D9D47
      Channel: 0xb62afa00
      IPSEC: Completed outbound VPN context, SPI 0xB663BFA9
      VPN handle: 0x0000bf84
      IPSEC: New outbound encrypt rule, SPI 0xB663BFA9
      Src addr: 0.0.0.0
      Src mask: 0.0.0.0
      Dst addr: 10.51.8.0
      Dst mask: 255.255.248.0
      Src ports
      Upper: 0
      Lower: 0
      Op : ignore
      Dst ports
      Upper: 0
      Lower: 0
      Op : ignore
      Protocol: 0
      Use protocol: false
      SPI: 0x00000000
      Use SPI: false
      IPSEC: Completed outbound encrypt rule, SPI 0xB663BFA9
      Rule ID: 0xb65bb1b8
      IPSEC: New outbound permit rule, SPI 0xB663BFA9
      Src addr: 195.178.80.10
      Src mask: 255.255.255.255
      Dst addr: 195.113.143.2
      Dst mask: 255.255.255.255
      Src ports
      Upper: 0
      Lower: 0
      Op : ignore
      Dst ports
      Upper: 0
      Lower: 0
      Op : ignore
      Protocol: 50
```

```
Use protocol: true
SPI: 0xB663BFA9
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB663BFA9
Rule ID: 0xbcb84ae0
IPSEC: Completed host IBSA update, SPI 0x74C64097
IPSEC: Creating inbound VPN context, SPI 0x74C64097
Flags: 0x00000006
SA : 0xb65bc440
SPI : 0x74C64097
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000BF84
SCB : 0x000D6087
Channel: 0xb62afa00
IPSEC: Completed inbound VPN context, SPI 0x74C64097
VPN handle: 0x0000ca64
IPSEC: Updating outbound VPN context 0x0000BF84, SPI 0xB663BFA9
Flags: 0x00000005
SA : 0xbcb843a8
SPI : 0xB663BFA9
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x0000CA64
SCB : 0x000D9D47
Channel: 0xb62afa00
IPSEC: Completed outbound VPN context, SPI 0xB663BFA9
VPN handle: 0x0000bf84
IPSEC: Completed outbound inner rule, SPI 0xB663BFA9
Rule ID: 0xb65bb1b8
IPSEC: Completed outbound outer SPD rule, SPI 0xB663BFA9
Rule ID: 0xbcb84ae0
IPSEC: New inbound tunnel flow rule, SPI 0x74C64097
Src addr: 10.51.8.0
Src mask: 255.255.248.0
Dst addr: 0.0.0.0
Dst mask: 0.0.0.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x74C64097
Rule ID: 0xbbd749c8
IPSEC: New inbound decrypt rule, SPI 0x74C64097
Src addr: 195.113.143.2
Src mask: 255.255.255.255
Dst addr: 195.178.80.10
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
```

Use protocol: true
SPI: 0x74C64097
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x74C64097
Rule ID: 0xbbd74a60
IPSEC: New inbound permit rule, SPI 0x74C64097
Src addr: 195.113.143.2
Src mask: 255.255.255.255
Dst addr: 195.178.80.10
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x74C64097
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x74C64097
Rule ID: 0xbbd74dc8

B Konfigurace Cisco ASA

```
FW(config)# show run
        : Saved
        :
        ASA Version 8.4(2)
        !
        hostname FW
        enable password 8Ry2YjIyt7RRXU24 encrypted
        passwd 2KFQnbNIdI.2KYOU encrypted
        names
        !
        interface GigabitEthernet0
        no nameif
        no security-level
        no ip address
        !
        interface GigabitEthernet0.21
        description Spojeni do Core VLAN 21 - serverova cast
        vlan 21
        nameif COREVLAN21
        security-level 100
        ip address 195.178.80.2 255.255.255.248
        !
        interface GigabitEthernet0.22
        description Spojeni do Core VLAN22 - DMZ a Internet
        mac-address 0000.ab16.dc00
        vlan 22
        nameif COREVLAN22
        security-level 0
        ip address 195.178.80.10 255.255.255.248
        !
        interface GigabitEthernet1
        no nameif
        no security-level
        no ip address
        !
        interface GigabitEthernet1.917
        description Spojeni do vzdalene site Lednice
        vlan 917
        nameif FW-LED
        security-level 100
        ip address 10.91.7.1 255.255.255.252
        !
        interface GigabitEthernet2
        shutdown
        no nameif
        no security-level
        no ip address
        !
        interface GigabitEthernet3
        no nameif
        no security-level
        no ip address
        !
        interface GigabitEthernet3.860
        description Spojeni k poskytovateli internetu ISP2
        vlan 860
        nameif ISP2
        security-level 0
        ip address 10.8.60.3 255.255.255.0
        !
        interface GigabitEthernet4
        no nameif
        no security-level
```

```
no ip address
!
interface GigabitEthernet4.162
description Management sit
vlan 162
nameif Management
security-level 100
ip address 10.16.2.1 255.255.255.0
!
interface GigabitEthernet4.455
vlan 455
nameif DNS-Auth
security-level 100
ip address 10.45.5.1 255.255.255.0
!
interface GigabitEthernet5
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network SERVER_10.45.5.90_800
host 10.45.5.90
object network SERVER_195.178.77.123
host 195.178.77.123
object network SERVER_10.45.5.90_900
host 10.45.5.90
object network SECONDARY-EXTERNAL-ADDRESS
host 195.178.80.11
object network OSTATNI-PROVOZ-SECONDARY-ADDRESS
host 10.45.5.100
object network INFORMACNI-STRANKA
host 10.45.5.9
object service INFORMACNI-STRANKA-PORT
service tcp destination eq 3658
object network ZAKAZANE-IP-ADRESY-WEB
host 195.178.80.1
object network DNS-Auth-int
host 10.45.5.1
object network SERVERS-SUBNET
subnet 195.178.77.0 255.255.255.128
object network MANAGEMENT-SUBNET
subnet 10.16.2.0 255.255.255.0
object network UCEBNY-SUBNET
subnet 195.178.72.0 255.255.255.0
object service OBJECT-WWW
service tcp destination eq www
object network SERVER_10.45.5.90_800
host 10.45.5.90
object service SNMP-SERVICE
service udp destination eq snmp
object service ZABBIX-SERVICE
service udp destination eq 10050
object network SNMP-SERVER
host 10.16.2.10
object network ZABBIX-SERVER
host 195.178.77.125
object-group network MAIL-SERVERS
network-object host 195.178.77.25
network-object host 195.178.77.26
object-group service WEB-SERVICES
service-object tcp destination eq www
```

service-object tcp destination eq https
object-group service MAIL-SERVICES
service-object tcp destination eq smtp
service-object tcp destination eq 465
object-group service MGMT-SERVICES
service-object tcp destination eq ssh
service-object tcp destination eq 3389
object-group service ICMP-TYPE-ALLOWED
service-object icmp echo-reply
service-object icmp echo
service-object icmp unreachable
service-object icmp time-exceeded
object-group service SERVER-SERVICES
service-object tcp destination eq 800
service-object tcp destination eq 900
access-list TRAFFIC-FROM-OUTSIDE extended permit udp any object SERVER_195.178.77.123
access-list TRAFFIC-FROM-OUTSIDE extended permit tcp any object OSTATNI-PROVOZ-SECONDARY-ADDRESS
access-list TRAFFIC-FROM-OUTSIDE extended permit object-group SERVER-SERVICES any host 10.45.5.90
access-list FW-TAK-NET extended permit ip any 10.51.8.0 255.255.248.0
access-list FW-TAK-NET extended permit ip any 195.113.143.16 255.255.255.240
access-list TRAFFIC-FROM-OUTSIDE extended permit object-group MAIL-SERVICES any object-group MAIL-SERVERS
access-list TRAFFIC-FROM-MANAGEMENT extended permit object-group MGMT-SERVICES object MANAGEMENT-SUBNET object SERVERS-SUBNET
access-list TRAFFIC-FROM-MANAGEMENT extended permit object SNMP-SERVICE object SNMP-SERVER interface Management
access-list TRAFFIC-FROM-CORE-CERNA-POLE extended permit object ZABBIX-SERVICE object ZABBIX-SERVER interface COREVLAN21
access-list TRAFFIC-FROM-CORE-CERNA-POLE extended permit object-group WEB-SERVICES object UCEBNY-SUBNET any
access-list GLOBAL extended permit object-group ICMP-TYPE-ALLOWED any any
access-list TRAFFIC-FROM-MANAGEMENT extended permit udp object-group ICMP-TYPE-ALLOWED any any
access-list AdresyZeSondyBlock extended deny ip host 103.10.50.4 any
access-list AdresyZeSondyBlock extended deny ip host 103.10.50.5 any
access-list AdresyZeSondyBlock extended deny ip host 45.5.2.4 any
access-list AdresyZeSondyBlock extended deny ip host 84.5.2.4 any
access-list AdresyZeSondyBlock extended deny ip host 221.194.47.224 any
!
pager lines 24
mtu COREVLAN21 1500
mtu COREVLAN22 1500
mtu FW-LED 1500
mtu FW-TAK 1500
mtu ISP2 1500
mtu Management 1500
mtu DNS-Auth 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any COREVLAN21
icmp permit any COREVLAN22
no asdm history enable
arp COREVLAN22 195.178.80.11 0000.ab16.dc00 alias
arp timeout 14400
nat (COREVLAN21,DNS-Auth) source static ZAKAZANE-IP-ADRESY-WEB interface destination static interface INFORMACNI-STRANKA service OBJECT-WWW INFORMACNI-STRANKA-PORT
!
object network SERVER_10.45.5.90_800
nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS service tcp 800 800
object network SERVER_195.178.77.123
nat (COREVLAN21,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS service udp 390 390
object network SERVER_10.45.5.90_900
nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS service tcp 900 900
object network OSTATNI-PROVOZ-SECONDARY-ADDRESS

```
    nat (DNS-Auth,COREVLAN22) static SECONDARY-EXTERNAL-ADDRESS
    nat (COREVLAN21,DNS-Auth) source static ZAKAZANE-IP-ADRESY-WEB interface destination static
interface INFORMACNI-STRANKA service OBJECT-WWW INFORMACNI-STRANKA-PORT
    nat (COREVLAN21,DNS-Auth) source static ZAKAZANE-IP-ADRESY-WEB interface destination static
interface INFORMACNI-STRANKA service OBJECT-HTTPS INFORMACNI-STRANKA-PORT
    access-group TRAFFIC-FROM-CORE-CERNA-POLE in interface COREVLAN21
    access-group TRAFFIC-FROM-OUTSIDE in interface COREVLAN22
    access-group TRAFFIC-FROM-MANAGEMENT in interface Management
    access-group AdresyZeSondyBlock global
    route COREVLAN22 0.0.0.0 0.0.0.0 195.178.80.9 1
    route COREVLAN22 10.51.8.0 255.255.248.0 195.178.80.9 1
    route FW-LED 78.128.147.0 255.255.255.0 10.91.7.2 1
    route DNS-Auth 192.168.0.0 255.255.255.0 10.45.5.2 1
    route COREVLAN22 195.113.143.16 255.255.255.240 195.178.80.9 1
    route COREVLAN21 195.178.72.0 255.255.252.0 195.178.80.1 1
    route COREVLAN21 195.178.77.0 255.255.255.128 195.178.80.1 1
    timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
    timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
    timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
    timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
    timeout tcp-proxy-reassembly 0:01:00
    timeout floating-conn 0:00:00
    dynamic-access-policy-record DfltAccessPolicy
    aaa-server FreeRadius protocol radius
    aaa-server FreeRadius (DNS-Auth) host 192.168.0.36
    key *****
    authentication-port 1812
    user-identity default-domain LOCAL
    aaa authentication ssh console LOCAL
    http server enable
    no snmp-server location
    no snmp-server contact
    snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
    crypto ipsec ikev2 ipsec-proposal IPSEC-TS-TAK
    protocol esp encryption aes-256
    protocol esp integrity sha-1
    crypto map FW-TAK-CRYPTOMAP 1 match address FW-TAK-NET
    crypto map FW-TAK-CRYPTOMAP 1 set peer 195.113.143.2
    crypto map FW-TAK-CRYPTOMAP 1 set ikev2 ipsec-proposal IPSEC-TS-TAK
    crypto map FW-TAK-CRYPTOMAP interface COREVLAN22
    crypto ikev2 policy 1
    encryption aes-256
    integrity sha
    group 5
    prf sha
    lifetime seconds 86400
    crypto ikev2 enable COREVLAN22
    telnet timeout 5
    ssh 10.45.5.0 255.255.255.0 DNS-Auth
    ssh 192.168.0.0 255.255.255.0 DNS-Auth
    ssh timeout 5
    console timeout 0
    threat-detection basic-threat
    threat-detection statistics access-list
    no threat-detection statistics tcp-intercept
    ntp server 195.178.77.123 source VLAN21 prefer
    webvpn
    enable COREVLAN22
    enable DNS-Auth
    group-policy MENDELU-RA-GroupPolicy internal
    group-policy MENDELU-RA-GroupPolicy attributes
    vpn-tunnel-protocol ssl-clientless
    username test password P4ttSyrm33SV8TYp encrypted
    username flowmon password SQkGlkCVb/l.Ajgs encrypted privilege 15
```

```
tunnel-group 195.113.143.10 type ipsec-l2l
tunnel-group 195.113.143.10 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
tunnel-group MENDELU-RA-TunnelGroup type remote-access
tunnel-group MENDELU-RA-TunnelGroup general-attributes
authentication-server-group FreeRadius
default-group-policy MENDELU-RA-GroupPolicy
tunnel-group 195.113.143.2 type ipsec-l2l
tunnel-group 195.113.143.2 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
!
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhomecisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
crashinfo save disable
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```