

Firewally v počítačových sítích

Libor Horák

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Libor Horák
Osobní číslo: A21599
Studijní program: B0613A140020 Softwarové inženýrství
Forma studia: Kombinovaná
Téma práce: Firewally v počítačových sítích
Téma práce anglicky: Firewalls in Computer Networks

Zásady pro vypracování

- Provedte rešerši na téma firewallů.
- Popište princip činnosti firewallu a jeho úlohu v bezpečnosti počítačových sítí.
- Srovnajte různé druhy firewallů a jejich využití v počítačových sítích.
- Popište funkcionality firewallu Cisco ASA 5508-X.
- Provedte základní konfiguraci Cisco ASA v jednoduché počítačové síti.

Seznam doporučené literatury:

1. SANTOS, Omar; KAMPANAKIS, Panos a WOLAND, Aaron T. Cisco next-generation security solutions: all-in-one Cisco ASA FirePOWER services, NGIPS, and AMP. Indianapolis: Cisco Press, [2017]. ISBN 9781587144462.
2. CRAWLEY, Don R. Cisco ASA for accidental administrators: an illustrated step-by-step Cisco ASA learning and configuration guide. Version 1.1. The accidental administrator series. Seattle, Washington: Soundtraining.net, [2015]. ISBN 9780983660750.
3. CRAWLEY, Don R. Cisco ASA security appliance training: student exercise manual edition 2.1d. The accidental administrator series. Seattle, Washington: Soundtraining.net, [2016]. ISBN 9780983660781.
4. SANTOS, Omar; STUPPI John. CCNA Security 210-260 official cert guide. Indianapolis: Cisco Press, [2015]. ISBN 9781587205668.
5. VACHON, Bob. CCNA security portable command guide. Indianapolis: Cisco Press, [2016]. ISBN 9781587205750.
6. WOLAND, Aaron T.; SANTUKA, Vivek; HARRIS, Mason a SANBOWER, Jamie. Integrated security technologies and solutions: Cisco security solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security. Indianapolis: Cisco Press, [2018]. ISBN 9781587147067.

Vedoucí bakalářské práce:

Ing. Jiří Korbelt, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: 27. října 2024

Termín odevzdání bakalářské práce: 2. června 2025



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem řádně citoval; v případě publikace výsledků budu uveden jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.
- jsem při tvorbě bakalářské práce použil nástroj generativního modelu AI Perplexity; <https://www.perplexity.ai> za účelem kvalitnější formulace textu. Po použití tohoto nástroje jsem provedl kontrolu obsahu a přebírám za něj plnou zodpovědnost.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Cílem práce je přiblížení problematiky bezpečnosti počítačových sítí. V teoretické části jsou diskutovány kybernetická bezpečnost spolu s nejčastějšími typy útoků, se kterými se lze setkat. Dále jsou popsány druhy firewallů a způsoby filtrace síťového provozu. Poslední kapitola teoretické části je věnována zařízení Cisco ASA (Adaptive Security Appliance) 5508-X a charakteristice funkcí tohoto zařízení.

V praktické části práce je představena navržená topologie sítě, do které bylo zařízení Cisco ASA zapojeno. Tato topologie byla implementována v Cisco laboratoři FAI. V této části práce je popsána základní konfigurace jednotlivých zařízení (např. nastavení jména, zabezpečení přístupu do zařízení nebo nastavení směrování) s důrazem na detailnější popis konfigurace Cisco ASA. Představené nastavení síťových zařízení je možné použít jako startovací bod pro reálné nasazení Cisco ASA v prostředí malých nebo středních firem.

Klíčová slova: firewall, Cisco ASA, počítačová síť, kybernetická bezpečnost

ABSTRACT

The goal of this thesis is to present the issue of computer network security. The theoretical part discusses cyber security along with the most common types of attacks that can be encountered. Furthermore, types of firewalls and methods of filtering network traffic are described. The last chapter of the theoretical part is devoted to Cisco ASA (Adaptive Security Appliance) 5508-X and the characteristics of its functions.

In the practical part of the thesis, the proposed network topology, in which the Cisco ASA device was connected, is presented. This topology has been implemented in the Cisco FAI lab. In this part of the thesis, the basic configuration of each device (e.g., name settings, device access security, or routing settings) is described, with emphasis on a more detailed description of the Cisco ASA configuration. The network device setup presented can be used as a starting point for real deployments of Cisco ASA in a small or medium-sized business environment.

Keywords: firewall, Cisco ASA, computer network, cyber security

Rád bych poděkoval Ing. Jiřímu Korbelovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích. Dále mé partnerce Veronice, mým rodičům a přátelům za podporu a trpělivost, díky nimž mohla být tato práce sepsána.

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 BEZPEČNOST POČÍTAČOVÝCH SÍTÍ	13
1.1 BEZPEČNOSTNÍ RIZIKA	14
2 FIREWALL	18
2.1 STATELESS FIREWALL	19
2.2 STATEFUL INSPECTION FIREWALL	20
2.3 APLIKAČNÍ FIREWALL	21
2.4 NGFW FIREWALL	21
2.5 SOFTWAREOVÝ FIREWALL	23
2.6 HARDWAROVÝ FIREWALL	25
3 CISCO ASA 5508-X	26
3.1 OPERAČNÍ REŽIMY	27
3.2 POROVNÁNÍ MODELŮ ŘADY CISCO ASA 5500-X	27
3.3 LICENCE FIREPOWER	29
3.4 CISCO ADAPTIVE SECURITY DEVICE MANAGER	30
3.5 CISCO ASA SECURITY LEVELS	32
II PRAKTICKÁ ČÁST	33
4 TOPOLOGIE SÍTĚ	34
4.1 ZÁKLADNÍ KONFIGURACE ZAŘÍZENÍ	35
4.2 KONFIGURACE ASA	38
4.2.1 Základní konfigurace	38
4.2.2 Nastavení rozhraní	39
4.2.3 Konfigurace OSPF	41
4.2.4 Nastavení DHCP	42
4.2.5 Konfigurace NTP pomocí ASDM	43
4.2.6 NAT	45

4.2.7	Konfigurace ACL	48
4.2.8	Nastavení SSH a AAA	49
ZÁVĚR.....		50
SEZNAM POUŽITÉ LITERATURY		51
SEZNAM OBRÁZKŮ		54
SEZNAM TABULEK		55
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK		56
SEZNAM PŘÍLOH.....		59

ÚVOD

V dnešním stále více propojeném světě se kybernetická bezpečnost stala klíčovým pilířem pro ochranu soukromí osob i stabilitu a odolnost provozu organizací ve všech odvětvích. Exponenciální nárůst zařízení připojených k internetu a šíření sofistikovaných kybernetických hrozeb, od malwaru přes ransomware až po DDoS útoky, zdůraznily naléhavou potřebu robustních a adaptivních obranných mechanismů. Mezi klíčové prvky zabezpečení dnešních počítačových sítí patří firewall. Tato technologie se za poslední desítky let vyvinula z jednoduchých paketových filtrů v komplexní vícevrstvé systémy, které jsou schopny čelit i velmi pokročilým útokům.

Tato práce si klade za cíl podat úvod do oblasti kybernetické bezpečnosti se zvláštním zaměřením na technologie firewallů. Větší pozornost bude věnována konkrétnímu modelu firewallu Cisco ASA 5508-X, vysvětlení jeho funkcionalit a možnosti zapojení takového zařízení do jednoduché počítačové sítě.

V teoretické části práce jsou nejdříve definovány a vysvětleny základní pojmy bezpečnosti počítačových sítí a jsou prezentovány nejčastější typy hrozeb a útoků, kterým dnes v této oblasti čelíme. V další kapitole je vysvětlen pojem firewallu a představeny jednotlivé typy podle principu zpracování paketů. V poslední kapitole teoretické části je blíže představeno zařízení Cisco ASA 5508-X. Jsou popsány jeho operační režimy, uvedena komparace technických aspektů s ostatními zařízeními z řady 5500-X a v neposlední řadě jsou popsány licence, které mohou pro toto zařízení být zakoupeny.

V praktické části práce je zařízení Cisco ASA 5508-X zapojeno, spolu s dalšími síťovými prvky, do jednoduché počítačové sítě a nakonfigurováno.

I TEORETICKÁ ČÁST

1 BEZPEČNOST POČÍTAČOVÝCH SÍTÍ

Úvodem je na místě se krátce zastavit nad základními principy bezpečnosti v počítačových sítích. Typickým příkladem komunikace je zaslání zprávy z jednoho bodu do jiného v dané komunikační síti. Principiálně nezáleží na tom, jestli se jedná o pozdrav kamarádovi v instant messaging aplikaci, o komunikaci mezi e-mailovým serverem a klientem nebo třeba o výměnu směrovacích informací dvou routerů. Aby aktéři mohli komunikaci považovat za bezpečnou, měly by být zachovány tři základní aspekty, které jsou někdy označovány jako CIA triáda [1]. Tyto tři principy nemají nic společného se zpravodajskou službou USA, ale jedná se o akronym sestávající z počátečních písmen anglických slov, která je vyjadřují – Confidentiality, Integrity a Availability.

Účastníci komunikace tedy mohou obecně komunikaci považovat za bezpečnou, bude-li zajištěno, že si zprávu mohou přečíst pouze oni nebo jimi pověřený uživatelé, jinými slovy bude zajištěna důvěrnost (confidentiality). Dále pokud bude zajištěno, že se zprávou nebylo manipulováno a byla tak zachována její integrita (integrity). A konečně je také velmi důležitá samotná dostupnost (availability) komunikačních zdrojů jako takových, aby bylo vůbec možné komunikaci uskutečnit.

Důvěrnost zajišťuje, aby data byla přístupná pouze těm, kteří k nim mají příslušná oprávnění. V případě síťové komunikace se zprávy před odesláním typicky šifrují a přístup k nim mají tedy pouze držitelé příslušných klíčů.

Integrita představuje pro účastníky komunikace záruku, že odeslaná zpráva nebyla pozměněna a to jak ve smyslu útočníka, tedy záměrné změny, tak ve smyslu nezáměrné změny (např. chyba při přenosu). Typickými mechanismy k zajištění integrity jsou elektronické podpisy nebo kontrolní součty.

Dostupnost je pro počítačovou síť a její prvky klíčová. Pokud komunikace není možná např. kvůli poruše nebo DoS (Denial of Service) útoku, přínosnost počítačové sítě pro uživatele klesá k nule, protože ji zkrátka nemohou použít. Různým typům rizik a útoků bude věnován následující text práce. Jednou z možností, jak útokům čelit, je nasazení firewallu [2].

1.1 Bezpečnostní rizika

V současnosti představují bezpečnostní hrozby v počítačových sítích stále závažnější téma. Téměř všechny oblasti lidské činnosti se buď částečně nebo zcela přesunuly do on-line světa a prakticky všechny organizace (banky, nadnárodní korporace, univerzity a další) musí velmi vážně řešit bezpečnost svých komunikačních sítí. S rozšiřující se dostupností hotových nástrojů na internetu se navíc řady potenciálních útočníků rozšiřují i o uživatele bez větších technických znalostí.

Ať už si útočníci vyberou jednodušší necílený útok, kupříkladu mapování sítě např. pomocí programu nmap, který nachází dostupná zařízení v dané síti pomocí tzv. ping sweep, tedy postupným rozesíláním ICMP (Internet Control Message Protocol) echo request paketů na adresy z rozsahu daného subnetu. Nebo zvolí cílený útok třeba v podobě DDoS (Distributed Denial of Service), tedy už sofistikovanější typ útoku, jehož cílem je znepřístupnit nějakou službu uživatelům tím, že danou službu (např. webový server) útočník zahltlíví obrovským počtem de facto legitimních požadavků. Je nutné na tyto a jiné hrozby myslet při návrhu a správě komunikačních sítí, aby se pokud možno potenciálním škodám zabránilo úplně nebo aby se alespoň co nejvíce minimalizovaly dopady útoků. Velmi často používaným zařízením v oblasti bezpečnosti počítačových sítí je firewall. Než bude popsán, bude ještě krátce popsáno několik nejčastějších typů bezpečnostních hrozeb a útoků, kterým dnes čelíme [1].

Útočníci využívají ke svým aktivitám různé přístupy, každý z nich využívá jiné zranitelnosti ať v technologii, procesech nebo lidském chování. Jednou z nejrozšířenějších hrozeb využívající technologické zranitelnosti stále zůstává malware. Jedná se o souhrnné označení pro škodlivý software, jehož účelem je narušit, poškodit nebo zneužít počítačové systémy, síť nebo data, případně k nim získat neautorizovaný přístup. Malwaru je mnoho typů od počítačových virů přes spyware (sledující činnost uživatele např. sledování klávesnice – keylogging), adware (zobrazující nevyžádanou reklamu, případně sbírající uživatelská data pro reklamní účely), po trojské koně a v posledních letech stále populárnější ransomware. V této kapitole jsou blíže popsány pouze některé z nejrozšířenějších druhů malwaru.

Počítačový virus je asi nejznámější typ malwaru. Šíří se vkládáním svého kódu do jiných spustitelných souborů, dokumentů nebo systémových oblastí (např. boot sektor). Charakteristickým rysem je závislost na hostiteli – vir vyžaduje aktivaci infikovaného souboru nebo procesu uživatelem, aby mohl provést replikaci a spustit svůj škodlivý kód. V současnosti je spíše na ústupu a je nahrazován sofistikovanějšími formami malwaru (např. ransomwarem). Poměrně účinnou obranou je antivirový software [3].

Červ (worm) je typ samostatně se šířícího malwaru, který se šíří sítí bez závislosti na hostitelském souboru nebo aktivaci uživatelem. Na rozdíl od virů nepotřebuje infikovat jiné programy – replikuje se autonomně, k čemuž využívá síťové služby, operační systém nebo aplikační zranitelnosti. Existuje několik typů červů, např. e-mailoví červi, kteří se šíří pomocí podvodných e-mailů s přílohami či odkazy nebo třeba mobilní červi, kteří cílí na mobilní zařízení (např. červ CommWarrior šířící se přes MMS). Obrana je složitější než v případě počítačových virů a kromě pravidelných aktualizací a blokování nepotřebných síťových portů zahrnuje i IDS (Intrusion Detection System), který bude blíže rozebrán v druhé kapitole této práce [4].

Trójský kůň je typ malwaru, který se tváří jako legitimní software nebo soubor, ale obsahuje nějakou skrytou funkci. Na rozdíl od červů se nereplikuje autonomně – ke své aktivaci vyžaduje akci uživatele (např. spuštění souboru). Za účelem oklamání uživatele se často prezentuje jako software zdarma, např. hra nebo antivirový software apod. [5].

Ransomware je malware, jehož primárním cílem je zašifrovat data oběti a následně požadovat finanční výkupné za jejich obnovení (výkupné - anglicky ransom). Od ostatních druhů malwaru se odlišuje přímou ekonomickou motivací a kombinací kryptografických technik s psychologickým nátlakem. Příkladem velmi rozšířeného ransomwaru je např. WannaCry z roku 2017, který nakazil stovky tisíc počítačů. Nejúčinnější obranou je záloha dat s pravidelnou verzovací kontrolou, důsledná aktualizace operačního systému nebo také segmentace sítě, která omezí šíření ransomwaru v rámci LAN [6].

Zatímco s malwarem se dá poměrně účinně bojovat pomocí antivirového softwaru a pravidelnými aktualizacemi, zejména operačního systému, existuje oblast hrozeb, proti které se

brání technickými prostředky jen velmi obtížně. Důvodem je, že tato hrozba využívá zranitelnosti v podobě lidského chování samotného. Jedná se o nejčastější metodu tzv. sociálního inženýrství v oblasti kybernetické bezpečnosti - phishing.

Phishing je označení pro útok, jehož cílem je přimět oběť, aby sama útočnickovi předala citlivé údaje (např. přihlašovací jméno a heslo, informace o platební kartě apod.) nebo provedla jinou akci ve prospěch útočníka, například nainstalovala malware. Phishingový útok se obvykle maskuje jako legitimní komunikace od důvěryhodného zdroje – např. banky, univerzity nebo kolegy z práce. Hlavním motivem je zneužití důvěry a lidského faktoru, nikoliv technické zranitelnosti. V základní podobě se objevil již v 90. letech 20. století v prostředí e-mailové komunikace. V současnosti je již mnohem sofistikovanější a využívá personalizace i další komunikační kanály (např. SMS, sociální sítě nebo instant messaging). Klasický phishing využívá velkého množství rozesílaných zpráv bez konkrétního zacílení. Poměrně nízká úspěšnost je kompenzována velkým počtem oslovených. Naproti tomu cílený útok na vybraného jednotlivce nebo organizaci se nazývá **spear phishing**. Útočník investuje čas do sběru informací o oběti, což zvyšuje důvěryhodnost podvržené zprávy a tím i úspěšnost útoku. Existuje ještě specifická forma spear phishingu, která cílí na vysoce postavené osoby (např. management) a ta je někdy označována jako whaling. Obrana proti phishingu technickými prostředky je velmi obtížná, za nejefektivnější je považováno pravidelná školení o rozpoznávání phishingu, případně simulované phishingové kampaně. Ale částečně efektivní mohou do určité míry být i antispamové filtry nebo detekce phishingových webů [7], [8].

Posledním typem bezpečnostních rizik, kterým bude věnována pozornost, jsou kyberbezpečnostní rizika spojená se síťovým provozem. Využívají nedostatky v komunikaci mezi zařízeními, servery nebo uživateli. Jedním z nejzávažnějších rizik je Man-in-the-Middle útok.

Man-in-the-Middle je typ kybernetického útoku, při kterém je komunikace mezi dvěma subjekty (např. serverem a uživatelem) tajně zachytávána, analyzována nebo modifikována útočníkem. Cílem je získat citlivé informace nebo manipulovat přenášená data bez vědomí obětí. Klíčovým rysem je nelegitimní pozice útočníka v komunikačním kanálu, který se vydává za důvěryhodnou stranu. Existuje několik základních typů tohoto druhu útoku, např.

ARP spoofing - falešné ARP (Address Resolution Protocol) zprávy, které přesměrují síťový provoz přes útočnickův stroj nebo DNS spoofing - podvržení DNS odpovědí, aby se oběť připojila k falešné IP adrese. Obranou je použití DNSSEC jako ochranu proti podvržení DNS záznamů, šifrování komunikace nebo monitorování ARP tabulek a následná detekce duplicitních ARP odpovědí [1], [9].

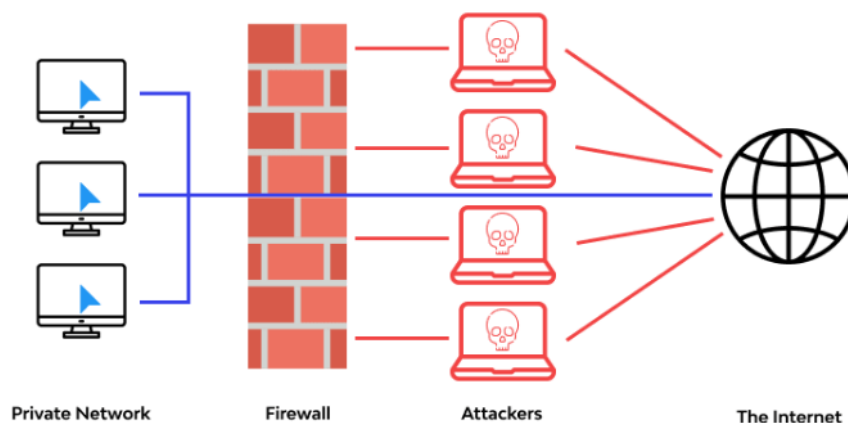
Extrémním typem síťového útoku jsou potom DoS a DDoS. V případě, že je útok úspěšný, celá jedna složka CIA triády - dostupnost je narušena.

DoS (Denial of Service) je druh kyberútoku, jehož cílem je znemožnit běžným uživatelům přístup ke konkrétní službě, serveru nebo síťovému zdroji. Útočník přetíží cílový systém takovým množstvím požadavků nebo škodlivých dat, že už systém nedokáže obsloužit legitimní uživatele. Konkrétním příkladem může být tzv. SYN flood - útočník zahájí mnoho TCP spojení, ale nikdy je nedokončí, čímž vyčerpá kapacitu serveru pro navazování nových spojení. Pokud je útok veden z jednoho stroje nebo menšího počtu strojů, dá se pomocí monitorování a detekce anomálií v síťovém provozu zakročit a útok ukončit např. zákazem komunikace s konkrétními IP adresami. Existuje ale ještě sofistikovanější verze tohoto typu útoku - tzv. DDoS (Distributed Denial of Service). Cílem je opět znepřístupnit nějakou službu uživatelům tím, že danou službu útočník zahltlí obrovským počtem požadavků, tyto požadavky však přicházejí z mnoha stran a adresních rozsahů od útočníkem ovládaného botnetu, tedy velkého počtu (řádově desítek tisíc) infikovaných strojů, které útočník ovládá. Obrana proti tomuto typu útoku je velmi obtížná. Zahrnuje filtrování provozu ať už za pomoci firewallu, rate-limitingu (omezení počtu požadavků během určitého časového intervalu od jednoho zdroje např. IP adresy) nebo geo-blokace [10], [11].

2 FIREWALL

Firewall je bezpečnostní prvek realizovaný jako fyzické zařízení nebo software, který je typicky umístěný mezi spravovanou sítí (vnitřní síť dané organizace např. univerzity) a nespravovanou sítí, kterou je v dnešní době ve většině případů internet. Jeho hlavním cílem je monitorování a filtrování příchozího a odchozího síťového provozu na základě bezpečnostních pravidel [1].

Termín firewall se v počítačových sítích objevil v 80. letech 20. století, kdy se začaly objevovat první nástroje na filtrování síťového provozu v reakci na rostoucí propojení počítačových sítí a potřebu chránit je před neoprávněným přístupem. Termín jako takový byl pravděpodobně převzat z oboru stavebnictví, kde představoval speciálně upravenou zeď mezi sousedícími domy, jejíž účel byl zabránit šíření požáru mezi soudními budovami. Metaforicky byl tedy pojem firewallu použit v oblasti informatiky jako bariéra bránící vnitřní síť před nežádoucím provozem ze sítě vnější.



Obrázek 2.1 Firewall

(zdroj: 12)

Prvním typem firewallu byl tzv. nestavový (stateless) firewall, který analyzoval základní informace v síťových paketech a na základě předem daných pravidel povoloval nebo blokoval jejich průchod. S postupem času, a s nárůstem složitosti útoků, se objevila potřeba sofistikovanější ochrany, což vedlo k vývoji stavových (stateful) firewallů, které byly schopny sledovat stav síťových spojení a lépe rozlišovat legitimní a podezřelý provoz. Dalším milníkem bylo zavedení aplikačních firewallů, které dokázaly analyzovat provoz na úrovni konkrétních aplikací a tím poskytnout ještě detailnější kontrolu. V současnosti se staly standardem firewally nové generace (NGFW - Next-Generation Firewall), které kromě tradičního filtro-

vání a stavové kontroly nabízejí i DPI (Deep Packet Inspection), kontrolu aplikací, prevenci průniků a další pokročilé funkce s podporou cloudových technologií [13]. Jednotlivým druhům firewallů je věnována následující část práce.

2.1 Stateless Firewall

Stateless firewall, někdy označovaný jako paketový filtr, je základním typem firewallu, který analyzuje a filtruje síťový provoz na základě předem definovaných pravidel. Klíčovým mechanismem pro tuto filtraci je ACL (Access Control List). Každý příchozí či odchozí paket je vyhodnocován samostatně, typicky podle informací v jeho hlavičce. Jsou analyzovány IP adresy odesílatele a příjemce, číslo portu nebo typ protokolu. Pokud paket nesplňuje stanovené podmínky, je zablokován. Stateless firewallly neuchovávají žádné informace o předchozích paketech ani o stavu navázaných spojení. To znamená, že není nerozlišováno, jestli paket patří k již existujícímu spojení nebo zda se jedná o nový či potenciálně rizikový pokus o komunikaci. Dnes jsou ACL často implementovány i na routerech nebo L3 switchích, aby byla umožněna základní filtrace provozu i na těchto zařízeních [1].

Výhody

- jednoduchá implementace
- rychlejší oproti jiným firewallům (vykonáváno méně funkcí)
- nízká latence díky nižším nárokům na systémové prostředky

Nevýhody

- nedostatečná ochrana proti složitějším útokům (sledují pakety pouze na základě základních údajů v hlavičce např. IP adresa nebo port)
- neschopnost rozhodovat podle vyšších vrstev (není možné rozpoznat protokoly např. na aplikační vrstvě)
- nutnost složitějších pravidel (pro dosažení vyšší úrovně bezpečnosti je nutné vytvářet rozsáhlé a komplikované sady pravidel, což zvyšuje riziko chyb a snižuje přehlednost)

2.2 Stateful Inspection Firewall

Stateful firewall pracuje na třetí a čtvrté vrstvě modelu OSI (Open Systems Interconnection), kde sleduje například TCP/UDP relace, jejich stav a kontext. Firewall si vede tzv. stavovou tabulku, kde uchovává informace o všech navázaných spojeních, včetně zdrojových a cílových IP adres, portů a aktuálního stavu spojení. Na základě těchto informací je rozhodováno, které pakety budou zablokovány. Každý nový paket je porovnáván s touto tabulkou, a pokud odpovídá existujícímu spojení, je povolen. To umožňuje efektivněji chránit síť před neoprávněným přístupem a složitějšími útoky, protože firewall má přehled o celém průběhu spojení, ne jen o jednotlivých paketech.

Výhody

- vyšší úroveň bezpečnosti
- kontextová analýza (díky sledování celého průběhu komunikace je zvýšena přesnost filtrování)
- podpora složitějších protokolů (možnost pracovat s dynamickými protokoly (např. FTP, VoIP), kde se porty mění za běhu, protože související provoz může být spojen do jednoho spojení)

Nevýhody

- vyšší nároky na výkon (sledování stavu všech spojení a analýza obsahu paketů vyžaduje více paměti i výpočetního výkonu)
- složitější konfigurace a správa (nastavení a správa pravidel je komplexnější, což klade větší nároky na znalosti správce)
- omezená inspekce šifrovaného provozu [1]

2.3 Aplikační firewall

Aplikační firewally, často označované jako WAF (Web Application Firewall), byly představeny jako další generace firewallů, která reagovala na omezení předchozích generací. Aplikační firewally analyzují celý obsah komunikace mezi uživatelem a aplikací, včetně HTTP a HTTPS požadavků i odpovědí [1].

Výhody

- ochrana před útoky na aplikační vrstvě (které nejsou odhalitelné z pohledu třetí a čtvrté vrstvy OSI modelu)
- možnost detailního nastavení a přizpůsobení (bezpečnostní pravidla a politiky pro konkrétní aplikace, včetně whitelistingu a blacklistingu specifických HTTP hlaviček)

Nevýhody

- složitější správa a konfigurace
- vyšší výkonové nároky

2.4 NGFW firewall

NGFW (Next-Generation Firewall) je v současnosti nejpoužívanější typ firewallu. Představuje zásadní evoluční krok v oblasti síťové bezpečnosti, překonává totiž omezení tradičních firewallů. Umožňuje inspekci paketů až na úrovni aplikační vrstvy OSI modelu a zároveň hlubší analýzu síťového provozu za pomoci technologie DPI (Deep Packet Inspection), která umožňuje analýzu až na úroveň obsahu samotných datových paketů. Tato technologie je základem systémů detekce a prevence průniků do sítě. Dále tento typ firewallu umožňuje realizovat ochranu proti malwaru prostřednictvím AMP (Advanced Malware Protection) [13]. Tyto pokročilé funkcionality jsou přiblíženy níže.

IDS (Intrusion Detection System) je systém určený pro monitorování síťového provozu nebo aktivit na jednotlivých zařízeních s cílem detekovat podezřelé nebo škodlivé činnosti, které mohou naznačovat probíhající kybernetický útok nebo narušení bezpečnosti. Pokud je

podezřelá aktivita identifikována, generuje upozornění pro správce sítě, kteří mohou na incident adekvátně reagovat. IDS nezasahuje do síťového provozu, ale slouží především jako nástroj včasné detekce a analýzy bezpečnostních incidentů.

IPS (Intrusion Prevention System) je aktivní systém, který monitoruje síťový provoz v reálném čase a automaticky blokuje nebo upravuje podezřelé či škodlivé aktivity, čímž zabraňuje průnikům a útokům na síťovou infrastrukturu. Na rozdíl od IDS zasahuje přímo do datového toku např. tím, že zahazuje škodlivé pakety, ukončuje spojení, blokuje podezřelé IP adresy nebo přenastavuje firewall pro prevenci opakovaných útoků. Využívá různé metody detekce, včetně analýzy signatur známých útoků (Signature-based), detekce anomálií v síťovém chování (Anomaly-based) a politik založených na bezpečnostních pravidlech (Policy-based) [14].

AMP (Advanced Malware Protection) je pokročilý bezpečnostní systém navržený k prevenci, detekci a odstraňování malwaru. Kromě klasické detekce podle signatur využívá i detekci na základě reputace (Reputation-based filtering). Ta funguje v rámci AMP tak, že při analýze souboru nebo síťového provozu ověřuje jeho reputaci v globálních databázích (např. podle hashe souboru, IP adresy nebo URL). Pokud je soubor nebo zdroj již známý a je označen jako škodlivý, je okamžitě zablokován; pokud není známý, může být dále analyzován například v sandboxu a jeho reputace je následně aktualizována. Tento přístup umožňuje rychle zastavit známé hrozby ještě před jejich vstupem do sítě a zároveň průběžně reagovat na nově vznikající rizika [13].

Výhody

- funkce firewallu jsou rozšířeny o pokročilý systém detekování hrozeb (DPI, IDS, IPS) včetně detekce malwaru
- schopnost monitorovat síťovou komunikaci téměř na všech vrstvách OSI modelu od vrstvy datových spojů (vrstva 2) až po aplikační vrstvu (7)
- správa bezpečnostních pravidel z jednoho místa a centralizovaná konfigurace (úspora času)

Nevýhody

- vyšší pořizovací a provozní náklady, náročná implementace
- možný negativní dopad na výkon sítě (DPI, analýza šifrovaného provozu a další bezpečnostní kontroly mohou způsobit zpoždění a snížit propustnost sítě)
- riziko centralizace v podobě single point of failure (v případě selhání NGFW může být výpadkem ohrožena celá infrastruktura za firewallem)

2.5 Softwarový firewall

Softwarové firewally jsou implementovány jako programy běžící přímo na serverech nebo koncových stanicích. Poskytují ochranu na úrovni jednotlivého zařízení, kde monitorují a filtrují příchozí i odchozí síťový provoz podle předem definovaných pravidel. Mohou být součástí operačního systému nebo nainstalovány jako samostatná aplikace. Umožňují uživateli detailně nastavit, které aplikace nebo služby mohou komunikovat se sítí a jaký provoz bude povolen či blokován. Výhodou je snadná instalace a konfigurace, kterou zvládne i běžný uživatel, a možnost rychlé aktualizace pravidel podle aktuálních hrozeb. Nevýhodou naopak je, že softwarový firewall zatěžuje systémové prostředky chráněného zařízení [15].

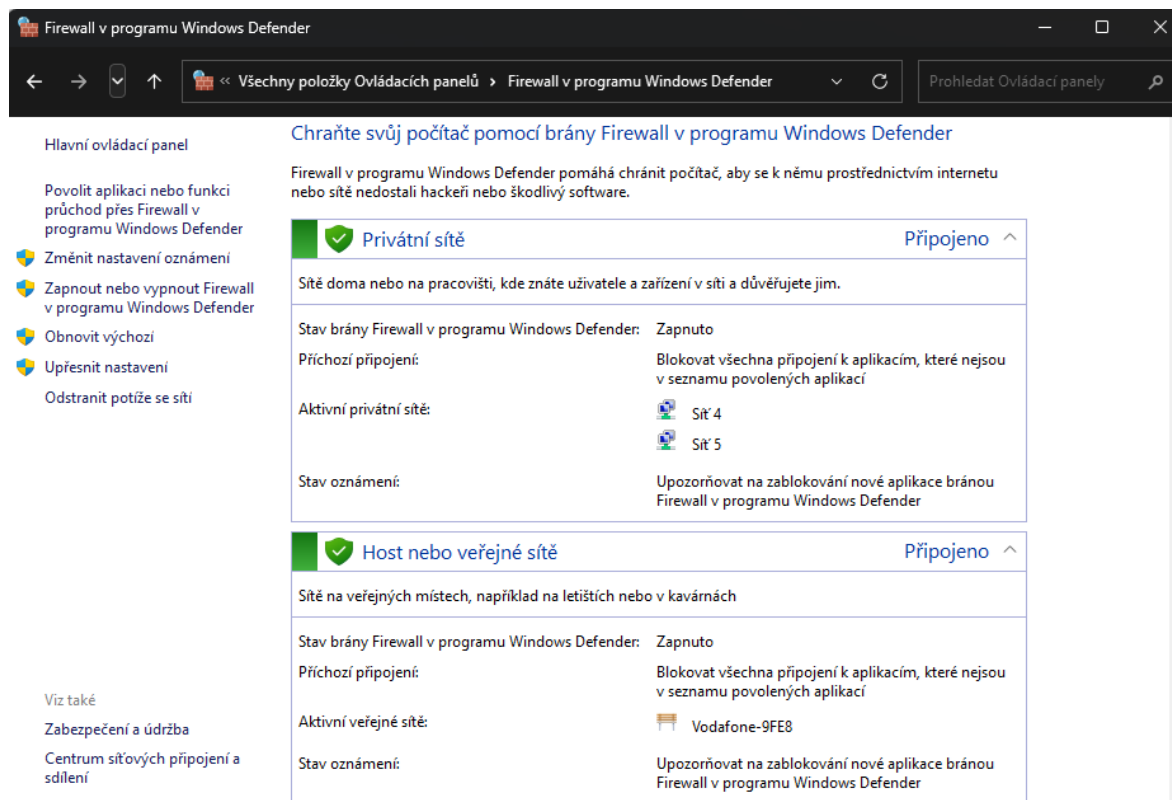
Výhody

- snadná instalace a flexibilita
- výrazně levnější oproti hardwarovému firewallu

Nevýhody

- zátěž na systémové prostředky hostitelského zařízení
- ochrana pouze konkrétního zařízení, na kterém je nainstalován

V některých operačních systémech je softwarový firewall již přímo implementován (např. Windows 11 nebo MAC OS). Na obrázku 2.2 je screenshot softwarového firewallu, který je součástí operačního systému Windows 11.



Obrázek 2.2 Firewall v operačním systému Windows 11

(zdroj: vlastní)

S rozšiřující se prací na dálku a rychlým rozvojem cloudových technologií, nabývá v současnosti na popularitě pronájem služeb od externích společností. Tento model je vhodný zejména pro organizace s více pobočkami nebo vzdálenými uživateli. **FWaaS (Firewall as a Service)** je cloudová bezpečnostní služba, která poskytuje firewallové funkce formou předplatného, bez nutnosti nasazení a správy hardwaru v síti společnosti. Odpadá tak nutnost netriviální finanční investice do potřebných zařízení a jejich správy. Hlavní výhodou je škálovatelnost a flexibilita. Služba se snadno přizpůsobí aktuálním potřebám firmy, umožňuje centralizovanou správu politik a nabízí pokročilé funkce známé z NGFW, jako je IPS, ochrana proti malwaru či podpora šifrovaného provozu. Nevýhodou naopak může být závislost na poskytovateli služby, možné zvýšení latence při směrování provozu přes cloudovou infrastrukturu a otázky ochrany soukromí. Mezi společnostmi nabízející FWaaS patří např. Cloudflare, Fortinet nebo Palo Alto Networks [16].

2.6 Hardwarový firewall

Hardwarový firewall je fyzické zařízení, které je umístěno mezi interní sítí a vnějším světem, obvykle na hranici mezi lokální sítí a internetem. Na rozdíl od softwarových firewallů, které chrání pouze konkrétní zařízení, poskytuje hardwarový firewall ochranu celé sítě, aniž by zatěžoval výkon jednotlivých počítačů nebo serverů. Hardwarové firewally filtrují příchozí i odchozí síťový provoz na základě předem definovaných bezpečnostních pravidel, nabízejí pokročilé funkce, jako je detekce útoků (IDS, IPS), filtrování obsahu nebo možnost vytváření bezpečných VPN spojení [1].

Výhody

- rychlost (poskytují vysoký výkon pro zajištění analýzy a zpracování dat a dosažení minimální latence)
- zabezpečení celé sítě (ne jen jednoho zařízení)
- vyšší úroveň zabezpečení

Nevýhody

- vyšší pořizovací cena (představují výrazně vyšší investici než softwarová řešení)
- náročnost instalace, nastavení a správy
- možné omezení výkonu sítě (při špatné konfiguraci nebo nedostatečné kapacitě může firewall představovat úzké hrdlo a zpomalovat síťový provoz)

Na obrázku 2.3 je příklad hardwarového firewallu od společnosti Juniper Networks, konkrétně model SRX300, přímý konkurent zařízení Cisco ASA 5508-X, jehož konfiguraci je věnována kapitola 4.



Obrázek 2.3 Juniper Networks SRX300 Services Gateway

(zdroj: 17)

3 CISCO ASA 5508-X

Cisco ASA 5508-X je moderní bezpečnostní zařízení ze série Cisco ASA 5500-X, určené především pro malé a střední podniky, případně pobočky větších firem, které vyžadují spolehlivou a komplexní ochranu své sítě. Tento model představuje vstupní úroveň tzv. NGFW (Next-Generation Firewall) s podporou pokročilých bezpečnostních funkcí díky integraci služby Cisco FirePOWER Services. Zařízení kombinuje tradiční firewall s možnostmi detekce a prevence průniků (IDS a IPS), kontrolou aplikací, filtrováním webových stránek, ochranou proti malwaru a dalšími funkcemi, které budou popsány v této kapitole.

Zařízení nabízí osm gigabitových ethernetových portů pro datový provoz, jeden dedikovaný management port a konzolový port. Je vybaveno 80GB SSD diskem pro ukládání logů, aktualizací a provozních dat, má 8 GB operační paměti i flash paměti a podporuje až 50 virtuálních rozhraní (VLAN) a 2 (maximálně 5) bezpečnostních kontextů, což umožňuje segmentaci sítě a oddělení různých provozních částí. [18]. Správa a konfigurace probíhá buď přes CLI, webové rozhraní ASDM, nebo centrálně pomocí Cisco Security Manager, což umožňuje efektivní dohled a správu více zařízení najednou.

Díky kombinaci vysokého výkonu, široké škály bezpečnostních funkcí a jednoduché správy představuje Cisco ASA 5508-X ideální volbu pro firmy, které hledají spolehlivou ochranu před moderními síťovými hrozbami a zároveň potřebují zařízení, které lze snadno integrovat do stávající infrastruktury.

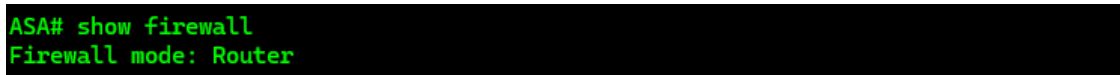


Obrázek 3.1 Cisco ASA 5508-X

(zdroj: 19)

3.1 Operační režimy

Cisco ASA může pracovat ve dvou různých režimech: router a transparent. Režim router je výchozí a zároveň nejčastější režim, ve kterém je zařízení nasazováno. To souvisí i s tradičním umístěním firewallu mezi vnitřní a vnější síť, kde monitoruje a filtruje příchozí a odchozí provoz. V tomto režimu ASA vystupuje jako další směrovací prvek v síti, pracuje tedy na třetí vrstvě OSI modelu. Každé rozhraní je v jiné podsíti a zařízení směruje provoz na základě směrovací tabulky. ASA v tomto režimu často vystupuje v roli výchozí brány pro zařízení připojená k danému rozhraní. Může také přidělovat adresy pomocí DHCP (Dynamic Host Configuration Protocol) nebo provádět překlady adres pomocí NAT (Network address translation) [20]. Operační mód může být snadno ověřen příkazem "show firewall", jak je vidět na obrázku 3.2.



```
ASA# show firewall
Firewall mode: Router
```

Obrázek 3.2 Ověření operačního režimu Cisco ASA

(zdroj: vlastní)

Druhou možností je režim transparent. V tomto módu zařízení pracuje na druhé vrstvě modelu OSI a neprovádí tedy směrování. Pouze přemostí uje (bridging) provoz mezi rozhraními, která jsou seskupena do tzv. bridge-group. Ostatní zařízení nevnímají firewall jako další síťový prvek, proto je ASA v tomto režimu označováno jako „neviditelný“ firewall. Přesto je možné detailně řídit a filtrovat síťový provoz pomocí access-listů a dalších bezpečnostních pravidel. Tento režim je vhodný například v případech, kdy je požadováno dodatečné zvýšení bezpečnosti v existující síti, bez nutnosti změn v adresaci nebo směrování. Konfigurace ASA v transparentním režimu je jednoduchá, slouží k ní příkaz "firewall transparent". Je důležité zmínit, že tímto úkonem dojde k vymazání aktuální konfigurace. Je proto důležité mít zálohu nebo tímto příkazem začít při počáteční konfiguraci [20].

3.2 Porovnání modelů řady Cisco ASA 5500-X

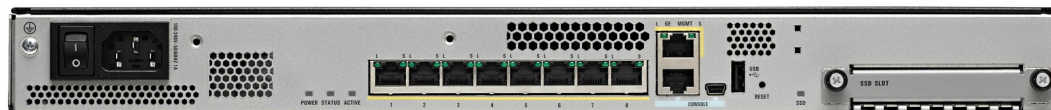
V modelové řadě Cisco ASA 5500-X jsou dostupná zařízení o různých výkonech a velikostech, aby bylo možné uspokojit různé požadavky zákazníků. Všechny modely podporují pokročilé bezpečnostní funkce a nabízejí možnost rozšíření o moduly FirePOWER, které

budou rozebrány níže v rámci této kapitoly. V tabulce 3.1 je porovnání jednotlivých modelů této produktové řady. Zařízení jsou určena pro malé a střední podniky, ale Cisco nabízí i výkonnější varianty (např. 5585-X), které jsou určeny pro ISP (Internet Service Provider) nebo do datových center. Tito zákazníci mimo jiné ocení velké možnosti škálování pomocí tzv. clusteringu, který umožňuje propojit až 16 firewallů do jednoho logického celku a výrazně tak zvýšit propustnost bezpečnostní infrastruktury [18].

Tabulka 3.1 Porovnání modelů řady Cisco ASA 5500-X

Model Cisco ASA	5506-X	5508-X	5516-X	5525-X	5545-X	5555-X
Stateful firewall throughput	300 Mbps	500 Mbps	900 Mbps	1 Gbps	1.5 Gbps	2 Gbps
Maximální počet souběžných spojení	50K	100K	250K	500K	750K	1 milion
Nová spojení za sekundu	5000	10 000	20 000	20 000	30 000	50 000
Maximální počet souběžných VPN spojení	50	100	250	750	2500	5000
IPsec VPN throughput	100 Mbps	175 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps
Orientační cena v \$	800	1 200	2 250	3 000	7 000	10 000

(zdroj: [18])



Obrázek 3.3 Cisco ASA 5508-X (zadní strana)

(zdroj: [21])

3.3 Licence FirePOWER

FirePOWER licence jsou důležitým prvkem k využití pokročilých bezpečnostních funkcí na zařízeních Cisco ASA. Základní provoz zařízení je možný i bez speciálních licencí, avšak pro většinu funkcí nové generace, např. detekci a prevenci průniků (IDS a IPS), kontrolu aplikací, filtrování webových adres nebo ochranu proti malwaru, je nutné zakoupit a aktivovat odpovídající licenci. Licencování FirePOWER je navrženo modulárně, což znamená, že zákazník si může vybrat přesně ty bezpečnostní služby, které potřebuje. FirePOWER licence jsou dostupné jako časově omezené předplatné (například na 1, 3 nebo 5 let). Základní (base) licence neexpiruje [22].

Licence Protection

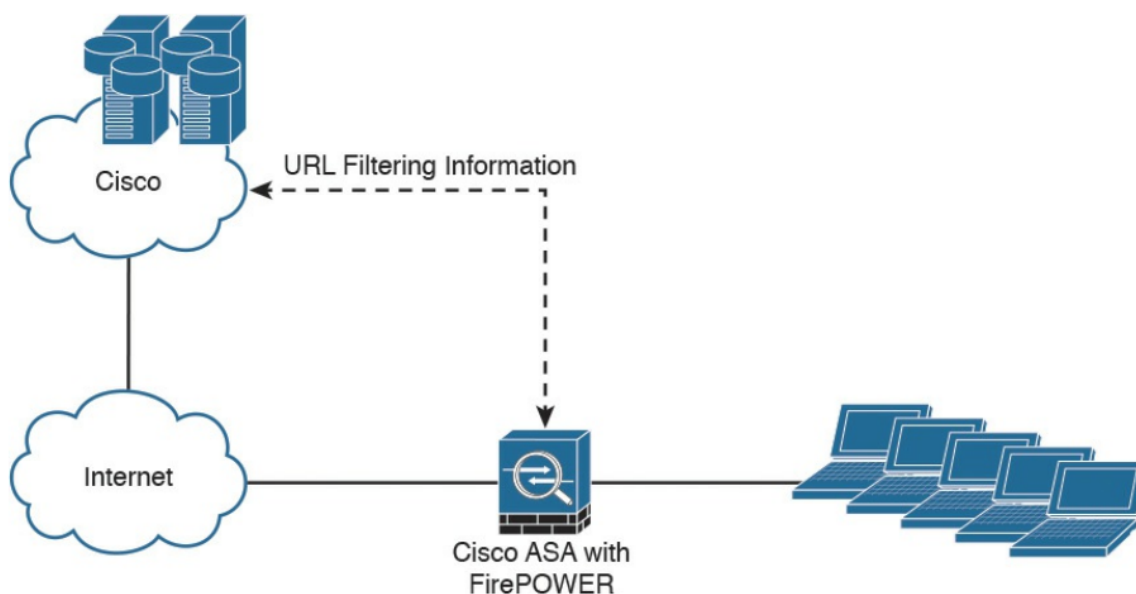
Licence Protection umožňuje správcům provádět detekci a prevenci průniku (IDS a IPS), kontrolu souborů a filtrování komunikace. Díky této licenci může zařízení analyzovat síťový provoz v reálném čase, rozpoznávat známé útoky, zranitelnosti a podezřelé aktivity a aktivně je blokovat nebo upozorňovat správce. Kontrola souborů umožňuje správcům sítě detekovat a blokovat odesílání nebo přijímání souborů určitých typů přes specifické aplikační protokoly. Licence Protection je vyžadována pro všechny ostatní licence (Control, Malware i URL Filtering). Pokud je tato licence odstraněna, má to přímý vliv na všechny ostatní nainstalované licence [13].

Licence Control

Licence Control umožňuje implementaci kontroly nad jednotlivými aplikacemi a uživateli. Této kontroly je dosaženo prostřednictvím ACL. Stejně jako u Protection licence je možné přidat podmínky pravidel ACL bez vlastnictví licence, ale před jejich aplikováním je nutné licenci nainstalovat.

Licence URL Filtering

URL Filtering licence umožňuje nasazení pravidel, které rozhodují o tom, jaká komunikace bude zakázána a jaká povolena na základě URL žádostí od koncových stanic. ASA získává informace o těchto URL ze Cisco cloudu, jak je vidět na obrázku 3.4. Jedná se o data z reputační databáze [13].



Obrázek 3.4 Obdržena informace o URL filtrování ze Cisco cloudu

(zdroj: 13)

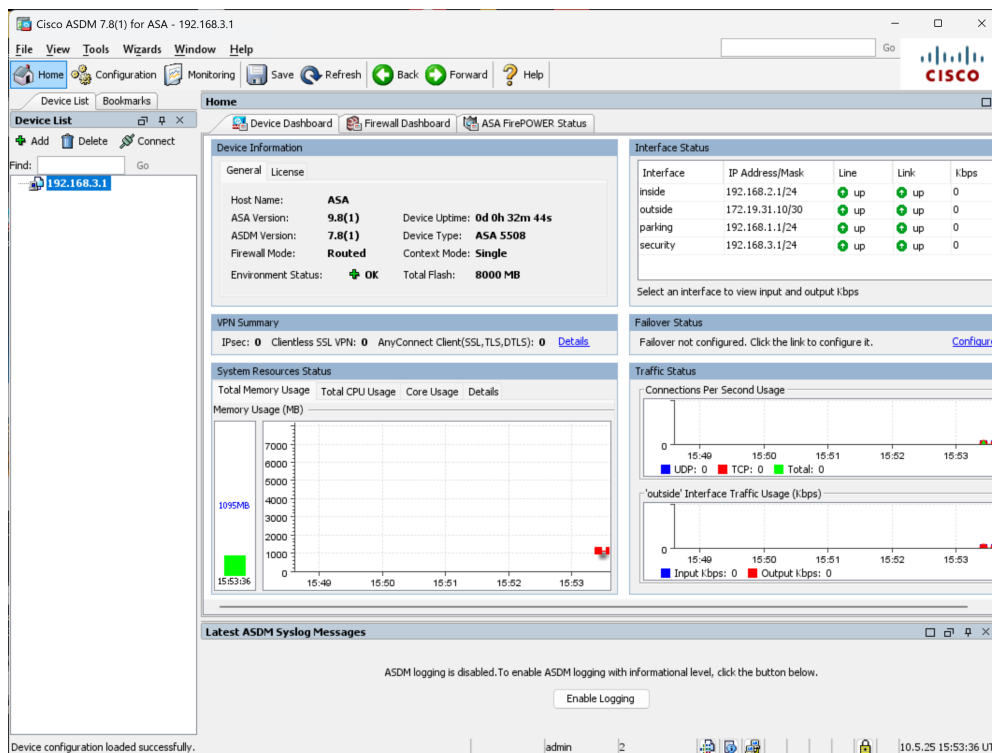
Licence Malware

Touto licencí je aktivováno AMP (Advanced Malware Protection), což zařízení umožní detekovat, analyzovat a blokovat malware, který prochází sítí. Konfigurace ochrany před malwarem je součástí souborové politiky, která je pak přidělena ke konkrétnímu ACL [13].

3.4 Cisco Adaptive Security Device Manager

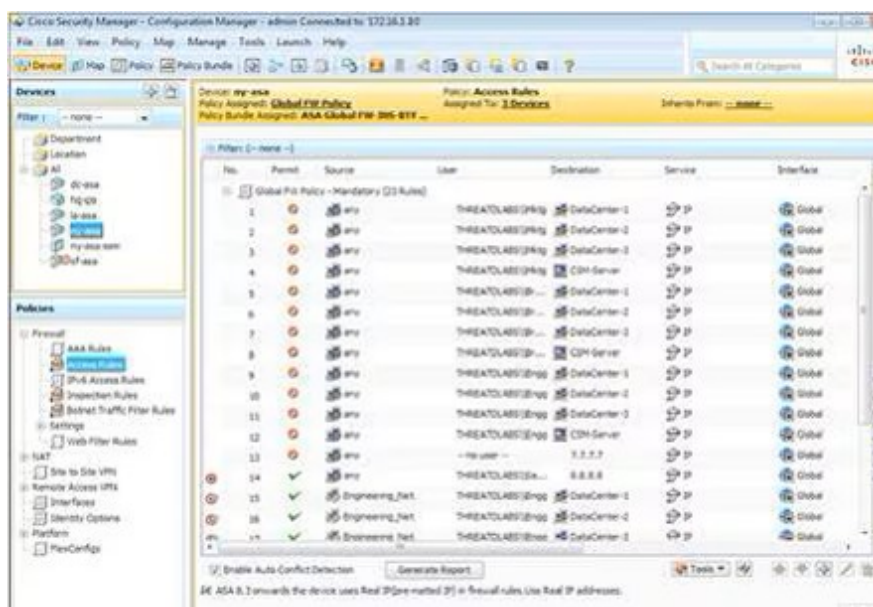
Cisco Adaptive Security Device Manager je grafické uživatelské prostředí, které slouží ke správě, konfiguraci a monitorování firewallů řady Cisco ASA. Umožňuje administrátorům pohodlně a rychle nastavovat bezpečnostní politiky, pravidla firewallu, NAT, VPN i další pokročilé funkce prostřednictvím přehledného webového rozhraní. Nabízí také pokročilé nástroje pro monitoring a troubleshooting např. real-time logování, sledování síťového provozu, zobrazení stavu zařízení nebo analýzu bezpečnostních událostí [23]. Grafické rozhraní ASDM je na obrázku 3.5 níže. Existuje ještě další grafické prostředí pro konfiguraci zařízení ASA a tím je CSM (Cisco Security Manager). To ale slouží pro správu velkého počtu zařízení ve větších společnostech. Ukázka tohoto grafického rozhraní je na obrázku 3.6.

Pro úplnost by mělo být zmíněno, že zařízení ASA je možné konfigurovat také pomocí CLI (Command-line Interface) ať už in-band přes SSH nebo out-of-band pomocí konzolového portu.



Obrázek 3.5 Adaptive Security Device Manager

(zdroj: vlastní)



Obrázek 3.6 Cisco Security Manager

(zdroj: 24)

Před použitím ASDM je nutná jeho předchozí instalace. Grafické rozhraní je možné stáhnout ze stránek výrobce nebo přímo ze zařízení ASA. Pokud je zařízení v továrním nastavení, je možné připojit počítač na management port, nastavit na síťové kartě počítače adresu z rozsahu 192.168.1.0/24 (např. 192.168.1.2) a do prohlížeče zadat adresu "https://192.168.1.1". Po úspěšné instalaci je již možné se připojit na ASA pomocí ASDM a to na zmíněné adrese 192.168.1.1 (v továrním nastavení nejsou uživatelské jméno a heslo nastavena) [23].

3.5 Cisco ASA security levels

Cisco ASA firewally využívají koncept tzv. „security levels“ (úrovně důvěryhodnosti), který určuje, jak moc je dané síťové rozhraní důvěryhodné ve srovnání s ostatními. Každé rozhraní na zařízení ASA má přiřazené číslo v rozsahu 0 až 100, přičemž vyšší číslo znamená vyšší míru důvěry. Pokud security level není při konfiguraci rozhraní uveden, aplikuje se implicitní hodnota 0 s jednou výjimkou, kterou je rozhraní pojmenované "inside". Takovému rozhraní je naopak implicitně přidělen security level 100, protože se předpokládá, že se jedná o vnitřní síť dané společnosti [20].

Zásadní vlastností security levelů je, že určují směr toku síťového provozu bez nutnosti explicitního nastavení pravidel. Provoz z rozhraní s vyšší úrovní důvěry na rozhraní s nižší úrovní je povolen automaticky – například uživatelé z vnitřní sítě mohou bez omezení komunikovat s internetem. Opačný směr, tedy z nižší úrovně na vyšší, je však ve výchozím stavu blokován a je nutné jej povolit pomocí ACL. To znamená, že například server v DMZ, s úrovní důvěry 40, nemůže sám od sebe navazovat spojení do vnitřní sítě, pokud toto není správcem explicitně povoleno.

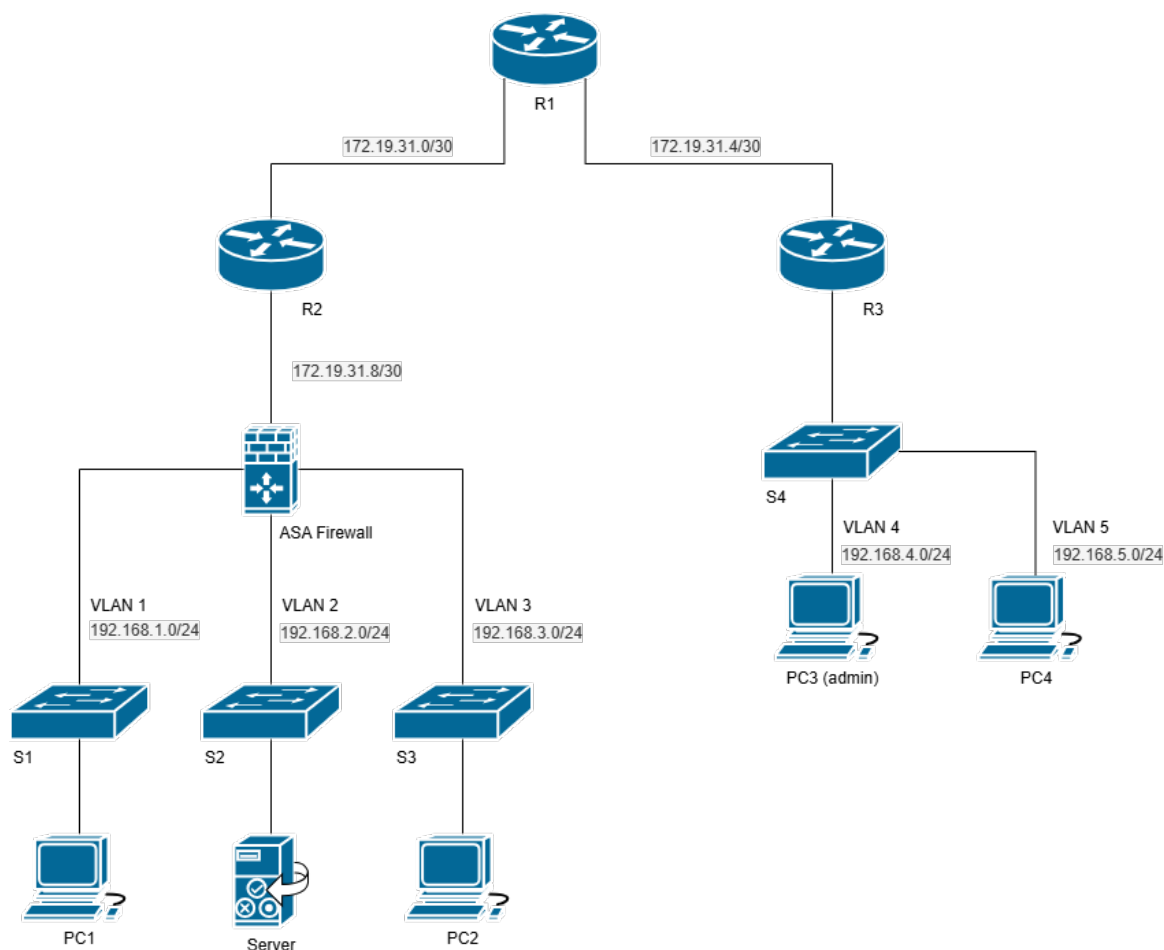
Security levels tak umožňují jednoduchou a přehlednou segmentaci sítě do bezpečnostních zón podle důvěryhodnosti. Ještě však existuje jedna možnost, která nebyla diskutována. A to je chování síťového provozu, pokud mají dvě rozhraní stejný security level. Ve výchozí konfiguraci je tento provoz blokován. Toto chování může být změněno pomocí příkazu "same-security-traffic permit inter-interface". Tento příkaz povolí provoz mezi všemi rozhraními se stejnou úrovní security levelu. Toto ale nemusí být vždy žádoucí. Není možné tuto konfiguraci provést selektivně, jen pro konkrétní rozhraní, a proto se tento příkaz používá spíše při troubleshootingu, než v produkční konfiguraci [20].

II PRAKTICKÁ ČÁST

4 TOPOLOGIE SÍTĚ

Tato část práce se zabývá zapojením a konfigurací zařízení Cisco ASA do jednoduché počítačové sítě. Za tímto účelem byla navržena jednoduchá topologie sítě, která je na obrázku 4.1 níže. V uvažované topologii jsou použity pouze adresy z rozsahu podle RFC 1918 [25], tedy privátní adresy, které nejsou směrovány v rámci internetu. Při implementaci v reálném nasazení by se příslušné rozsahy adres na routerech jednoduše zaměnily za přidělený rozsah veřejných IP adres.

Směrování je zajištěno dynamicky pomocí OSPF a koncovým zařízením jsou přidělovány adresy pomocí DHCP, konkrétně u VLAN 1-3 za použití DHCP serveru běžícího na ASA a pro VLAN 4-5 prostřednictvím DHCP serveru běžícího na routeru R3. Na zmíněných zařízeních (ASA, R3) je také použit NAT, tedy překlad adres z VLAN rozsahů (192.168.x.0/24) na adresu odchozího rozhraní.



Obrázek 4.1 Topologie sítě

(zdroj: vlastní)

4.1 Základní konfigurace zařízení

V tabulce 4.1 se nachází IP adresace pro uvažovanou topologii sítě, ze které bylo v konfiguraci jednotlivých zařízení vycházeno.

Tabulka 4.1 IP adresování v topologii sítě

Zařízení	Interface	IP adresa	Maska	VLAN	Gateway
R1	G0/0	172.19.31.1	255.255.255.252		
R1	G0/1	172.19.31.5	255.255.255.252		
R2	G0/0	172.19.31.2	255.255.255.252		
R2	G0/1	172.19.31.9	255.255.255.248		
R3	G0/0	172.19.31.6	255.255.255.252		
S1	Vlan 1	192.168.1.2	255.255.255.0		192.168.1.1
S2	Vlan 2	192.168.2.2	255.255.255.0		192.168.2.1
S3	Vlan 3	192.168.3.2	255.255.255.0		192.168.3.1
S4	Vlan 4	192.168.4.2	255.255.255.0		192.168.4.1
ASA	G1/1	172.19.31.10	255.255.255.248		
ASA	G1/2	192.168.1.1	255.255.255.0		
ASA	G1/3	192.168.2.1	255.255.255.0		
ASA	G1/4	192.168.3.1	255.255.255.0		
Server	NIC	ASA DHCP	ASA DHCP	2	ASA DHCP
PC1	NIC	ASA DHCP	ASA DHCP	1	ASA DHCP
PC2	NIC	ASA DHCP	ASA DHCP	3	ASA DHCP
PC3	NIC	R3 DHCP	R3 DHCP	4	R3 DHCP
PC4	NIC	R3 DHCP	R3 DHCP	5	R3 DHCP

(zdroj: vlastní)

Cílem této práce je popsat zejména konfiguraci Cisco ASA, ale pro funkčnost uvažované topologie je samozřejmě nutná i konfigurace ostatních síťových zařízení - tedy routerů a switchů. V následujícím textu budou krátce diskutovány určité části konfigurace těchto zařízení. Pozornost si zaslouží hlavně konfigurace SSH, konkrétně délka použitého RSA klíče. V konfiguraci je použita délka klíče 1024 bitů, která dnes již není považována za bezpečnou. V současnosti je doporučována nejmenší délka klíče 3072 bitů [26]. Hodnota 1024 je tedy zvolena pouze jako příklad a to i z toho důvodu, že model routeru dostupný v síťové laboratoři FAI (Cisco 1941) délku klíče 3072 nepodporuje.

Na výpisu 4.1 níže jsou všechny příkazy použité pro konfiguraci routeru R1. Konfigurační příkazy pro ostatní zařízení jsou k dispozici v přílohách 1 - 6 .

```
en
conf t
no ip domain lookup
hostname R1
enable secret failab
service password-encryption
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
line vty 0 4
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
int g0/0
ip address 172.19.31.1 255.255.255.252
description R2 connection
no shut
int g0/1
ip address 172.19.31.5 255.255.255.252
description R3 connection
no shut
!
router ospf 1
router-id 3.3.3.3
network 172.19.31.0 0.0.0.3 area 0
network 172.19.31.4 0.0.0.3 area 0
auto-cost reference-bandwidth 1000
!
end
write
```

Výpis 4.1 Příkazy použité pro konfiguraci routeru R1 (zdroj: vlastní)

Jak je vidět, jedná se o velmi jednoduchou konfiguraci, která sestává, kromě základního za-

bezpečení přístupu do zařízení, z nastavení IP adres na příslušná rozhraní a nastavení OSPF pro zajištění dynamického směrování.

U konfigurace switchů je pak nastavena IP adresa z příslušného rozsahu na virtuální rozhraní, které slouží jako management adresa pro účely ustanovení SSH spojení pro umožnění vzdálené správy. Porty k jednotlivým koncovým zařízením jsou přiřazeny do příslušných VLAN a propojení do routeru je pak realizováno pomocí trunku, který zajišťuje bezproblémový průchod provozu ze všech potřebných VLAN ke směrování. Je dobrou praxí všechny nepoužívané porty vypnout.

Správná konfigurace může být ověřena např. pomocí nástroje ping. Na obrázku 4.2 je vidět, že PC3 byla úspěšně přidělena adresa a byly doručeny odezvy od routeru R1 i R2.

```
C:\Users\Cisco>ipconfig

Windows IP Configuration

Ethernet adapter CISCO:

    Connection-specific DNS Suffix  . : engineers.failab.cz
    Link-local IPv6 Address . . . . . : fe80::cb24:781c:ac6b:a02d%10
    IPv4 Address. . . . . : 192.168.4.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.4.1

C:\Users\Cisco>ping 172.19.31.1

Pinging 172.19.31.1 with 32 bytes of data:
Reply from 172.19.31.1: bytes=32 time<1ms TTL=254
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254
Reply from 172.19.31.1: bytes=32 time<1ms TTL=254

Ping statistics for 172.19.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ping 172.19.31.9

Pinging 172.19.31.9 with 32 bytes of data:
Reply from 172.19.31.9: bytes=32 time<1ms TTL=253
Reply from 172.19.31.9: bytes=32 time=1ms TTL=253
Reply from 172.19.31.9: bytes=32 time=1ms TTL=253
Reply from 172.19.31.9: bytes=32 time=1ms TTL=253

Ping statistics for 172.19.31.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Obrázek 4.2 Ověření konektivity PC3

(zdroj: vlastní)

4.2 Konfigurace ASA

Následující část práce je věnována popisu konfigurace zařízení Cisco ASA. V jednotlivých podkapitolách je postupně rozebrána konfigurace zařízení pro uvažovanou topologii sítě a to od základního nastavení zařízení, přes konfiguraci rozhraní, až po nastavení směrování, DHCP serveru, ACL nebo překladu adres.

Jak bylo zmíněno v kapitole 3, konfigurace zařízení Cisco ASA je možná pomocí CLI (Command Line Interface) nebo lze využít ASDM (Adaptive Security Device Manager) a konfiguraci provést za pomoci grafického rozhraní. CLI nabízí možnost detailně přizpůsobit konfiguraci a je mnohdy rychlejší než použití grafického rozhraní, proto je často preferováno administrátory. I většina konfigurace pro účely této práce byla provedena za pomoci CLI, ale pro úplnost byla zařazena i krátká ukázka konfigurace pomocí ASDM.

4.2.1 Základní konfigurace

Konfiguraci je vhodné začít názvem zařízení, pod kterým bude v síti vystupovat, doménovým jménem a heslem pro privilegovaný mód zabezpečujícím přístup do zařízení. V globálním konfiguračním módu tedy byly zadány tři příkazy na výpisu 4.2.

```
hostname ASA
domain-name failab.cz
enable password failab
```

Výpis 4.2 Konfigurace názvu, doménového jména a hesla pro privileg. mód (zdroj: vlastní)

Dalším krokem velmi často bývá nastavení přesného času, který je důležitý pro správné logování událostí, synchronizaci s ostatními síťovými zařízeními nebo pro SSL/TLS certifikáty. Příslušný příkaz je vidět na výpisu 4.3.

```
clock set 14:15:00 march 21 2025
```

Výpis 4.3 Konfigurace data a času (zdroj: vlastní)

Přestože se dá datum a čas nastavit tímto jednoduchým příkazem, frekventovaným řešením je nastavení synchronizace času pomocí NTP (Network Time Protocol). Právě nastavení NTP synchronizace bylo zvoleno pro ukázku konfigurace ASA pomocí ASDM. Aby však bylo možné se do ASDM přihlásit, je nutné nejprve nastavit rozhraní a HTTP server.

4.2.2 Nastavení rozhraní

Při konfiguraci rozhraní bylo vycházeno z tabulky 4.1, kde se nacházejí veškeré potřebné IP adresy včetně masek podsítí. Na výpisu 4.4 jsou uvedeny příkazy použité ke konfiguraci jednotlivých rozhraní.

```
int g1/1
description R2 connection
nameif outside
ip address 172.19.31.10 255.255.255.248
no shut
int g1/2
description S1 connection
nameif parking
ip address 192.168.1.1 255.255.255.0
security-level 50
no shut
int g1/3
description S2 connection
nameif inside
ip address 192.168.2.1 255.255.255.0
security-level 70
no shut
int g1/4
description S3 connection
nameif security
ip address 192.168.3.1 255.255.255.0
security-level 100
no shut
```

Výpis 4.4 Konfigurace rozhraní (zdroj: vlastní)

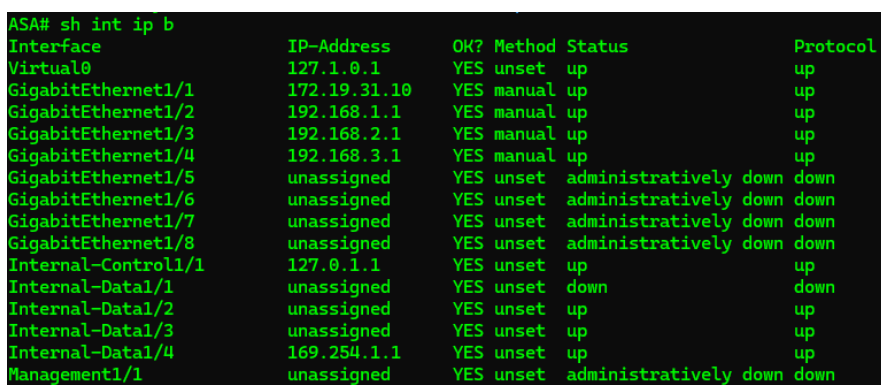
Dobrou praxí je začít popisem daného rozhraní pro lepší přehlednost a orientaci příkazem "description". Z popisu by mělo být zřejmé, jaké zařízení je k danému rozhraní připojeno.

U zařízení ASA je oproti Cisco routerům a switchům specifický příkaz "nameif", který slouží k přiřazení logického jména danému rozhraní. Toto jméno je klíčové pro další konfiguraci, protože se následně používá v pravidlech firewallu, ACL (Access Control List), směrování a dalších nastaveních. Bez přiřazeného nameif rozhraní na ASA nemůže propouštět provoz a nebude funkční.

Dále již byly podle tabulky 4.1 přiděleny jednotlivým rozhraním jejich IP adresy. Dalším specifickým příkazem oproti jiným Cisco zařízením je "security-level". Při konfiguraci rozhraní na zařízení Cisco ASA je určována úroveň jejich důvěryhodnosti (Security Level). Nastavuje se hodnota v rozsahu 0 až 100 s tím, že nejvyšší hodnota představuje nejvyšší důvěru. Pokud při konfiguraci security-level není uveden, nastaví se hodnota automaticky

na 0. Existuje však jedna výjimka a to pro "nameif inside", která má automaticky hodnotu 100, protože se předpokládá, jak název napovídá, že se jedná o vnitřní síť. Jak bylo zmíněno v kapitole 3, rozhraní s vyšší úrovní důvěryhodnosti může komunikovat s nižší úrovní bez omezení, ale opačný směr je blokován, pokud není explicitně povolen pomocí ACL.

Příkazem "no shut" pak byla rozhraní již jen aktivována. Stejně jako u ostatních prvků v síti, byla nepoužívaná rozhraní vypnuta pomocí příkazu "shut". Konfiguraci je snadno ověřitelná využitím příkazu "show interface ip brief", jehož výstup je na obrázku 4.3.



```
ASA# sh int ip b
```

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	172.19.31.10	YES	manual	up	up
GigabitEthernet1/2	192.168.1.1	YES	manual	up	up
GigabitEthernet1/3	192.168.2.1	YES	manual	up	up
GigabitEthernet1/4	192.168.3.1	YES	manual	up	up
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	down	down
Internal-Data1/2	unassigned	YES	unset	up	up
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	administratively down	down

Obrázek 4.3 Kontrola nastavení rozhraní ASA

(zdroj: vlastní)

Po dokončení nastavení rozhraní bylo přistoupeno ke konfiguraci HTTP serveru pro ASDM. I když je v příkazu "http", komunikace neprobíhá na portu 80, ale na portu 443, tedy přes HTTPS. Na tuto skutečnost je tedy nutné později myslet při zadávání adresy do adresního řádku prohlížeče. Na výpisu 4.5 jsou vidět dva příkazy. Pomocí prvního byl HTTP server na ASA povolen a díky druhému byl umožněn přístup zařízením z podsítě 192.168.3.0/24 připojeným na rozhraní security.

```
http server enable
http 192.168.3.0 255.255.255.0 security
```

Výpis 4.5 Konfigurace HTTP serveru (zdroj: vlastní)

4.2.3 Konfigurace OSPF

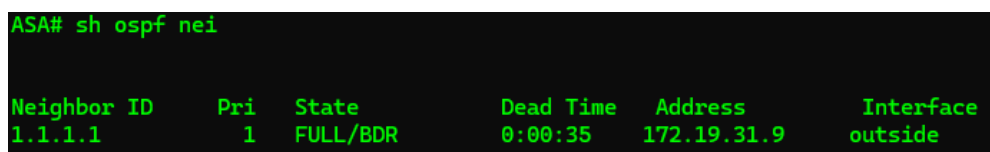
Aby se ASA bylo schopno spojit s NTP serverem, musí znát cestu k jeho adrese. V našem případě k adrese na routeru R2. V uvažované topologii je použito dynamické směrování pomocí OSPF. Směrování bylo nastaveno s využitím příkazů ve výpisu 4.6.

```
router ospf 1
router-id 1.1.1.2
network 172.19.31.8 0.0.0.7 area 0
```

Výpis 4.6 Konfigurace směrování pomocí OSPF (zdroj: vlastní)

Prvním příkazem byl aktivován OSPF proces s ID 1. Druhým bylo nastaveno statické OSPF Router ID, které slouží k jeho identifikaci v síti, při výpočtech směrování a hraje důležitou roli při výběru DR (Designated Router) a BDR (Backup Designated Router). Poslední příkaz umožňuje routeru propagovat síť 172.19.31.8/29 do směrovací tabulky a sdílet ji s ostatními OSPF sousedy v oblasti 0.

K ověření správného fungování OSPF byl využit příkaz "show ospf neighbor", byly zobrazeny informace o OSPF sousedech, se kterými má zařízení navázanou komunikaci (viz. obrázek 4.4). Případně je možné použít "show route" k zobrazení směrovací tabulky a ověřit, jestli v ní jsou přítomny cesty například k sítím na R3 a vyzkoušet ping jednoho z rozhraní na tomto routeru.



```
ASA# sh ospf nei
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	0:00:35	172.19.31.9	outside

Obrázek 4.4 Verifikace OSPF konfigurace na ASA
(zdroj: vlastní)

4.2.4 Nastavení DHCP

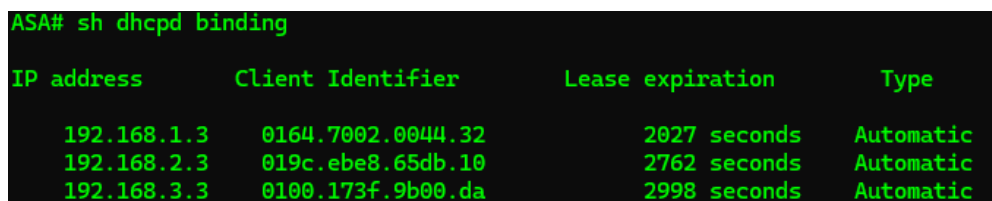
Aby bylo možné se na HTTP server na ASA připojit, musí mít počítač adresu z rozsahu 192.168.3.0/24. V této podsíti se budou adresy přidělovat dynamicky pomocí DHCP (Dynamic Host Configuration Protocol). Je tedy třeba nejprve nakonfigurovat DHCP server. Na výpisu 4.7 jsou příkazy, které byly použity pro nastavení DHCP serveru.

```
dhcpd address 192.168.1.3-192.168.1.253 parking
dhcpd address 192.168.2.3-192.168.2.253 inside
dhcpd address 192.168.3.3-192.168.3.253 security
dhcpd option 3 ip 192.168.1.1 interface parking
dhcpd option 3 ip 192.168.2.1 interface inside
dhcpd option 3 ip 192.168.3.1 interface security
dhcpd enable parking
dhcpd enable inside
dhcpd enable security
```

Výpis 4.7 Konfigurace DHCP serveru (zdroj: vlastní)

Nejprve pro každé rozhraní parking, inside a security byly nastaveny rozsahy přidělovaných adres, každý z těchto rozsahů koresponduje s příslušnou podsítí podle tabulky 4.1. Příkazem "dhcpd option 3 ip" byla nastavena výchozí brána pro každý uvažovaný subnet. Jedná se vždy o adresu ASA rozhraní, na které je daná podsít' připojena. Nakonec již jen bylo DHCP pro jednotlivá rozhraní spuštěno.

Je namístě ověřit, jestli počítače dostávají přidělené adresy pomocí "show dhcpd binding". Na obrázku 4.5 je vidět, že DHCP server přidělil všem připojeným počítačům adresu ze zadaných rozsahů.



The screenshot shows the command 'ASA# sh dhcpd binding' and its output. The output is a table with four columns: IP address, Client Identifier, Lease expiration, and Type. It lists three active DHCP leases for the subnets 192.168.1.3, 192.168.2.3, and 192.168.3.3.

IP address	Client Identifier	Lease expiration	Type
192.168.1.3	0164.7002.0044.32	2027 seconds	Automatic
192.168.2.3	019c.ebe8.65db.10	2762 seconds	Automatic
192.168.3.3	0100.173f.9b00.da	2998 seconds	Automatic

Obrázek 4.5 Verifikace DHCP konfigurace na ASA
(zdroj: vlastní)

4.2.5 Konfigurace NTP pomocí ASDM

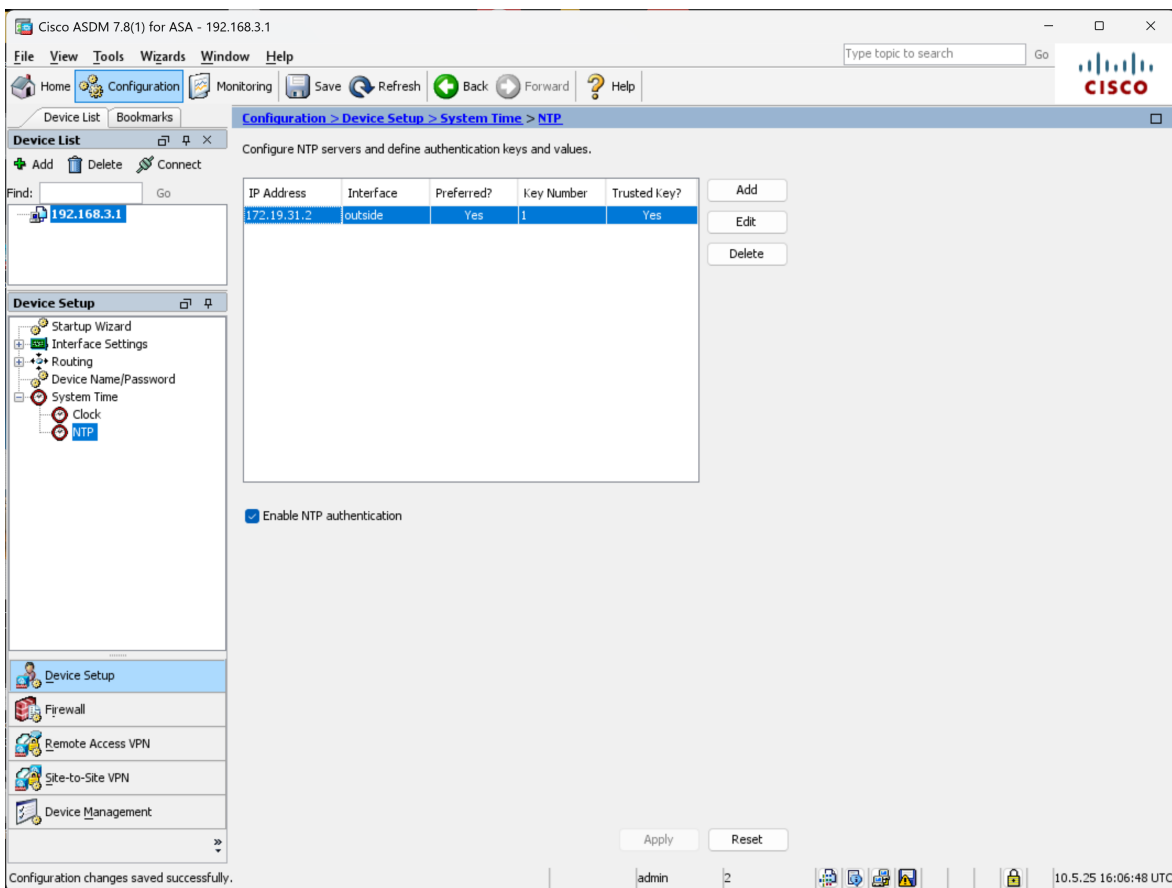
Po úspěšném nastavení rozhraní, povolení HTTP serveru a nastavení DHCP a směrování, bylo přistoupeno ke konfiguraci NTP pomocí ASDM. Aplikace ASDM Launcher je ke stažení přímo ze zařízení ASA nebo na stránkách výrobce [27].

Pro stažení aplikace přímo z ASA byla zadána do prohlížeče na počítači PC2, který je ve správné podsíti, adresa "https://192.168.3.1". Následně se zobrazila webová stránka s možností instalace aplikace na obrázku 4.6



Obrázek 4.6 Webová stránka ASDM Launcher
(zdroj: vlastní)

Po instalaci aplikace již bylo přistoupeno k ASA pomocí ASDM po zadání výše zmíněné adresy 192.168.3.1. Přihlašovací údaje zatím nebyly nastaveny, takže bylo přihlašovací jméno i heslo ponecháno prázdné. V sekci "Configure -> System Time -> NTP" byla přidána adresa NTP serveru 172.19.31.2, tedy adresa routeru R2, na kterém byl NTP server nastaven. Po vyplnění autentizačních údajů byl před aplikováním změn zaškrtnut check-box "enable NTP authentication", jak je vidět na obrázku 4.7.



Obrázek 4.7 Konfigurace NTP pomocí ASDM
(zdroj: vlastní)

Správná funkčnost byla potom ověřena pomocí "show ntp status" a "show ntp associations", jejichž výstupy jsou na obrázku 4.8. Je vidět, že došlo k úspěšné synchronizaci a firewall bude pravidelně získávat přesný čas od routeru R2.

```
ASA# sh ntp status
Clock is synchronized, stratum 3, reference is 172.19.31.2
nominal freq is 99.9984 Hz, actual freq is 99.9984 Hz, precision is 2**6
reference time is ebc9f856.51256219 (16:07:50.316 UTC Sat May 10 2025)
clock offset is -1.1866 msec, root delay is 0.50 msec
root dispersion is 15892.06 msec, peer dispersion is 15890.63 msec

ASA# sh ntp associations
      address      ref clock      st  when poll reach delay offset  disp
*~172.19.31.2      127.127.1.1    2   18   64   1    0.5  -1.19 15890.
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
```

Obrázek 4.8 Verifikace NTP konfigurace na ASA
(zdroj: vlastní)

4.2.6 NAT

NAT (Network Address Translation) je technologie používaná k překladu IP adres mezi interní a externí sítí. Původně byl navržen jako nástroj, který měl napomoci překonat nedostatek veřejných IPv4 adres. Umožňuje totiž zařízením v soukromé síti komunikovat s veřejným internetem tím, že překládá jejich privátní IP adresy na veřejnou IP adresu. Má však i rozměr v oblasti bezpečnosti, protože skryje skutečné IP adresy zařízení před externími hrozbami. Existují tři různé typy NAT: statický NAT, který mapuje jednu IP adresu na jinou pevně definovanou, dynamický NAT, který umožňuje překlad více interních adres na jednu nebo více veřejných adres, a PAT (Port Address Translation), který umožňuje sdílení jedné veřejné IP adresy mezi více zařízeními pomocí různých portů [2].

```
object network parking_nat
subnet 192.168.1.0 255.255.255.0
nat (parking,outside) dynamic interface
exit
object network server_nat
host 192.168.2.3
nat (inside,outside) static 172.19.31.11
exit
object network security_nat
subnet 192.168.3.0 255.255.255.0
nat (security,outside) dynamic interface
```

Výpis 4.8 Konfigurace překladu adres (zdroj: vlastní)

Jak je vidět na výpisu 4.8, nastavení bylo provedeno pomocí příkazu "object network", za kterým následuje název. Na dalším řádku bylo specifikováno, jaké adresy se mají překládat a poslední třetí příkaz definuje, na jakou adresu/adresy se mají překládat. Podsítě 192.168.1.0/24 a 192.168.3.0/24 reprezentují PAT, kdy se všechny adresy z daného rozsahu překládají na adresu outside rozhraní. Příkladem statického NAT je překlad adresy 192.168.2.3, tedy adresy serveru, na adresu 172.19.31.11.

Nyní by bylo vhodné konfiguraci ověřit např. pomocí pingu. Ve výchozí konfiguraci ASA jsou však ICMP pakety filtrovány, aby bylo možné použít ping k ověření komunikace např. PC2 s routerem R3, je nutné na ASA nastavit, aby se ICMP pakety zpracovávaly. Příkazy, které toto realizují, následují ve výpisu 4.9. Než budou příkazy diskutovány, je vhodné se ještě krátce zastavit u konceptu MPF (Modular Policy Framework), který je používán.

MPF (Modular Policy Framework) je flexibilní způsob konfigurace bezpečnostních funkcí na Cisco ASA. Umožňuje definovat bezpečnostní politiky pro různé typy provozu (např. inspekci protokolů, QoS). MPF tvoří tři základní komponenty:

- policy map - definuje akce, které se mají provést na identifikovaném provozu.
- class map - identifikuje provoz, na který se mají aplikovat bezpečnostní politiky
- service policy - určuje, kde bude definovaná akce aplikována: na konkrétní rozhraní nebo globálně na celý firewall

```
policy-map global_policy
class inspection_default
inspect icmp
```

Výpis 4.9 Konfigurace zpracování ICMP paketů (zdroj: vlastní)

Pomocí prvního řádku, na výpisu 4.9, byla zvolena globální bezpečnostní politika, která se aplikuje na veškerý provoz, pokud není specifikováno jinak. Mapa global_policy je přítomna v základní konfiguraci, nebyla tedy vytvořena nová, ale byla upravena již existující.

Druhý řádek odkazuje na třídu provozu inspection_default, která je v základní konfiguraci součástí policy mapy global_policy. Zahrnuje běžné protokoly jako FTP (File Transfer Protocol) nebo RTSP (Real-Time Streaming Protocol).

A konečně za pomoci příkazu na třetím řádku byla aktivována inspekce ICMP provozu, což znamená, že firewall bude analyzovat ICMP pakety [20].

Po provedení konfigurace výše byla ověřena konektivita PC2, na obrázku 4.9 je vidět, že je z počítače dostupný jak router R1, tak i router R3.

Na firewallu potom bylo verifikováno, jestli překlad adres probíhá korektně. Na obrázku 4.10 jsou vidět výstupy příkazů "show xlate" a "show nat". Na výstupu prvního je vidět, že se adresa PC2 překládá na adresu rozhraní outside a výstup druhého zobrazuje osm překladů, což odpovídá osmi uskutečněným pingům z tohoto počítače. Translate_hits odpovídá paketům echo request, tedy provozu zevnitř sítě ven a untranslate_hits reprezentuje echo reply a směr komunikace z vnější sítě do té vnitřní.

```
C:\Users\Cisco>ipconfig

Windows IP Configuration

Ethernet adapter CISCO:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8:acad::10
    Link-local IPv6 Address . . . . . : fe80::6359:37f2:7de7:1da9%16
    IPv4 Address. . . . . : 192.168.3.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%16
                                192.168.3.1

C:\Users\Cisco>
C:\Users\Cisco>ping 172.19.31.1

Pinging 172.19.31.1 with 32 bytes of data:
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254
Reply from 172.19.31.1: bytes=32 time=1ms TTL=254

Ping statistics for 172.19.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Cisco>ping 172.19.31.6

Pinging 172.19.31.6 with 32 bytes of data:
Reply from 172.19.31.6: bytes=32 time=1ms TTL=253
Reply from 172.19.31.6: bytes=32 time=1ms TTL=253
Reply from 172.19.31.6: bytes=32 time=1ms TTL=253
Reply from 172.19.31.6: bytes=32 time=1ms TTL=253

Ping statistics for 172.19.31.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Obrázek 4.9 Ověření konektivity PC2

(zdroj: vlastní)

```
ASA# sh xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from security:192.168.3.3/1 to outside:172.19.31.10/1 flags ri idle 0:00:10 timeout 0:00:30
ASA#
ASA# sh nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static server_nat 172.19.31.11
   translate_hits = 0, untranslate_hits = 0
2 (parking) to (outside) source dynamic parking_nat interface
   translate_hits = 0, untranslate_hits = 0
3 (security) to (outside) source dynamic security_nat interface
   translate_hits = 8, untranslate_hits = 8
```

Obrázek 4.10 Ověření překladu adres

(zdroj: vlastní)

4.2.7 Konfigurace ACL

Access Control Listy jsou, jak bylo zmíněno v kapitole 2, klíčovým nástrojem pro řízení bezpečnosti v síti s širokým využitím nejen na Cisco ASA firewallech. Na výpisu 4.10 jsou příkazy, kterými byly povoleny HTTP požadavky z vnější sítě na server připojený ke switchi S2. Tuto komunikaci je nutné explicitně povolit, protože se jedná o komunikaci ze směru rozhraní s nižší úrovní důvěry (rozhraní outside má security level 0) na rozhraní s vyšší úrovní důvěry (rozhraní inside má nastavenou hodnotu security level na 70).

```
access-list internet_to_server extended permit icmp any host
192.168.2.3
access-list internet_to_server extended permit tcp any host
192.168.2.3 eq www
access-group internet_to_server in interface outside
```

Výpis 4.10 Konfigurace ACL pro zpracování HTTP paketů pro web server (zdroj: vlastní)

Nejprve byly na prvním řádku povoleny ICMP pakety, aby byla umožněna klientům serveru jednoduchá verifikace připojení. Na druhém řádku již byl povolen TCP provoz na portu 80 směřující na server. Nakonec byl ACL aplikován na rozhraní outside ve směru in (inbound) [28].

HTTP provoz je podobně jako v případě ICMP ve výchozí konfiguraci filtrován, je tedy nutné na firewallu nastavit, aby byly HTTP pakety zpracovávány. Příkazy, které toto zabezpečí, následují ve výpisu 4.11.

```
policy-map global_policy
class inspection_default
inspect http
```

Výpis 4.11 Konfigurace zpracování HTTP paketů (zdroj: vlastní)

Na obrázku 4.11 je potom vidět úspěšné načtení webové stránky v prohlížeči na počítači PC4.



Obrázek 4.11 Ověření připojení k webovému serveru
(zdroj: vlastní)

4.2.8 Nastavení SSH a AAA

Nakonec bylo nastaveno SSH pro umožnění vzdálené správy. Při konfiguraci SSH je nezbytné povolit AAA (Authentication, Authorization, Accounting) autentizaci, aby bylo uživatelům umožněno přihlašovat se pomocí definovaných účtů. V této práci byla využita lokální databáze uživatelů, ale ověření uživatele je možné nastavit i vůči externímu AAA serveru, jako je RADIUS nebo TACACS+ [29].

```
username admin password cisco
aaa authentication ssh console LOCAL
crypto key generate rsa modulus 1024
ssh version 2
ssh 192.168.3.0 255.255.255.0 security
ssh 192.168.4.0 255.255.255.0 outside
```

Výpis 4.12 Konfigurace SSH (zdroj: vlastní)

Na výpisu 4.12 jsou vidět postupné kroky ke konfiguraci SSH. Nejprve bylo definováno uživatelské jméno a heslo. Následně byla nastavena AAA autentizace pro SSH pomocí lokální databáze. Dále byl vygenerován RSA klíč a byla nastavena používaná verze SSH. Navázání spojení bylo potom omezeno na dvě podsítě (192.168.3.0/24 přes rozhraní security a 192.168.4.0/24 přes rozhraní outside).

Závěrem je třeba zmínit, že přihlašovací údaje z lokální databáze výše budou použity i pro přístup do konfigurace pomocí ASDM.

Úplná konfigurace zařízení Cisco ASA je k dispozici v příloze 7.

ZÁVĚR

Cílem této bakalářské práce bylo na úvod seznámit čtenáře s bezpečností v oblasti počítačových sítí. Bylo prezentováno, že bezpečnost v komunikačních sítích stojí na třech základních pilířích tzv. CIA triády. A to na důvěrnosti (confidentiality), integritě zasílaných zpráv (integrity) a dostupnosti (availability). Dále byly diskutovány nejčastější typy hrozeb a útoků, se kterými je možné se v současných počítačových sítích setkat, včetně návrhů protiopatření minimalizujících jejich dopady.

Druhá kapitola byla zaměřena na klíčový prvek bezpečnosti počítačových sítí - firewall. Byl popsán jejich vývoj, funkcionality a charakteristiky jednotlivých kategorií. Dále byly vysvětleny rozdíly mezi stateless a stateful firewally a v neposlední řadě byly prezentovány hlavní typy firewallů včetně jejich výhod a nevýhod. Poslední kapitola teoretické části byla věnována firewallu od společnosti Cisco, konkrétně ASA 5508-X. Postupně bylo zařízení představeno a byly vysvětleny jeho operační režimy. Dále byla provedena komparace s ostatními modely dané produktové řady. Byly popsány licence FirePOWER, možnosti správy zařízení včetně Adaptive Security Device Manager. V závěru kapitoly byly potom vysvětleny úrovně důvěryhodnosti rozhraní tzv. security levels.

V praktické části práce byla navržena, zapojena a nakonfigurována ukázková topologie sítě v Cisco laboratoři FAI. Nedílnou součástí této topologie bylo i zařízení Cisco ASA 5508-X. Postupně byla prezentována konfigurace jednotlivých síťových zařízení v uvažované topologii od základní konfigurace v podobě nastavení jména jednotlivých prvků v síti, zabezpečení přístupu do zařízení přes nastavení IP adres na jednotlivých rozhraních až po konfiguraci dynamického směrování zabezpečeného pomocí OSPF. Detailní pozornost byla věnována konfiguraci zařízení Cisco ASA. Postupně bylo popsáno nastavení DHCP serveru (zajištění přidělování adres počítačům v připojených podsítích), NAT (překlad privátních adres z připojených podsítí), ACL (povolení určitého typu provozu), SSH (zajištění vzdálené správy pomocí CLI). Dále byla demonstrována konfigurace zařízení pomocí ASDM. V závěru práce bylo nastavení ověřeno pomocí pingů a navázání spojení s webovým serverem nacházejícím se za Cisco ASA. Výsledky této práce mohou sloužit jako podklady pro zajištění kybernetické bezpečnosti jak pro domácí síť, tak pro sítě malých a středních podniků.

SEZNAM POUŽITÉ LITERATURY

- [1] SANTOS, Omar a STUPPI, John, 2015. *CCNA Security 210-260: Official Cert Guide*. Indianapolis: Cisco Press. 3. vyd. ISBN 978-1-587-20566-8.
- [2] VACHON, Bob, 2016. *CCNA security portable command guide*. Indianapolis: Cisco Press. 1. vyd. ISBN 978-1-587-20575-0.
- [3] ESET, 2025. *Co je počítačový virus + druhy virů*. Online. Dostupné z: <https://www.eset.com/cz/virus/>. [cit. 2025-04-25].
- [4] AVAST, 2025. *What Is a Computer Worm?* Online. Dostupné z: <https://www.avast.com/c-computer-worm>. [cit. 2025-04-25].
- [5] AVG, 2025. *What is a Trojan Horse?* Online. Dostupné z: <https://www.avg.com/en/signal/what-is-a-trojan>. [cit. 2025-04-25].
- [6] KASPERSKY LAB, 2025. *What is Ransomware?* Online. Dostupné z: <https://www.kaspersky.com/resource-center/threats/ransomware>. [cit. 2025-04-25].
- [7] MCAFEE, 2025. *What Is Phishing?* Online. Dostupné z: <https://www.mcafee.com/learn/what-is-phishing/>. [cit. 2025-04-25].
- [8] KASPERSKY LAB, 2025. *What is a Whaling Attack?* Online. Dostupné z: <https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack>. [cit. 2025-04-25].
- [9] NORTON, 2025. *What is a man-in-the-middle attack?* Online. Dostupné z: <https://us.norton.com/blog/wifi/what-is-a-man-in-the-middle-attack>. [cit. 2025-04-25].
- [10] AKAMAI, 2025. *What Is a DDoS Attack?* Online. Dostupné z: <https://www.akamai.com/glossary/what-is-ddos>. [cit. 2025-04-25].
- [11] CLOUDFLARE, 2025. *SYN flood DDoS attack*. Online. Dostupné z: <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/>. [cit. 2025-04-25].

- [12] BESCHOKOV, Mukhadin, 2025. *What is a Firewall and How does it Work?* Online. Dostupné z: <https://www.wallarm.com/what/the-concept-of-a-firewall>. [cit. 2025-05-02].
- [13] SANTOS, Omar; KAMPANAKIS, Panos a WOLAND, Aaron T., 2017. *Cisco next-generation security solutions: all-in-one Cisco ASA FirePOWER services, NGIPS, and AMP*. Indianapolis: Cisco Press. 2. vyd. ISBN 978-1-587-14446-2.
- [14] PALO ALTO NETWORKS, 2025. *What is an Intrusion Prevention System?* Online. Dostupné z: <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>. [cit. 2025-05-07].
- [15] PALO ALTO NETWORKS, 2025. *What is a Software Firewall?* Online. Dostupné z: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-software-firewall>. [cit. 2025-04-25].
- [16] PALO ALTO NETWORKS, 2025. *What Is Firewall as a Service (FWaaS)? | FWaaS Defined & Explained*. Online. Dostupné z: <https://www.paloaltonetworks.com/cyberpedia/what-is-firewall-as-a-service>. [cit. 2025-05-10].
- [17] JUNIPER NETWORKS, 2025. *Juniper Networks SRX300 Services Gateway*. Online. Dostupné z: <https://www.networkscreen.com/SRX300.asp>. [cit. 2025-05-05].
- [18] CISCO, 2020. *Cisco ASA 5500 Series Data Sheet*. Online. Dostupné z: <https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html>. [cit. 2025-05-15].
- [19] CISCO, 2025. *Cisco ASA 5500-X with FirePOWER Services*. Online. Dostupné z: <https://www.cisco.com/c/en/us/support/security/asa-firepower-services/series.html>. [cit. 2025-04-30].
- [20] WOLAND, Aaron T.; SANTUKA, Vivek; HARRIS, Mason a SANBOWER, Jamie, 2018. *Integrated security technologies and solutions: Cisco security solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security*. Indianapolis: Cisco Press. 1. vyd. ISBN 978-1-587-14706-7.

- [21] SHI GOVERNMENT SOLUTIONS, 2025. *Cisco ASA 5508-X with FirePOWER Services*. Online. Dostupné z: <https://texas.gs.shi.com/product/30083334/Cisco-ASA-5508-X-with-FirePOWER-Services>. [cit. 2025-04-30].
- [22] CISCO, 2025. *Smart Software Licensing*. Online. Dostupné z: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa923/configuration/general/asa-923-general-config/intro-license-smart.html>. [cit. 2025-05-07].
- [23] CRAWLEY, Don R., 2015. *Cisco ASA for accidental administrators: an illustrated step-by-step Cisco ASA learning and configuration guide. Version 1.1. The accidental administrator series*. Seattle, Washington: Soundtraining.net. 1. vyd. ISBN 978-0-983-66075-0.
- [24] CISCO, 2018. *Cisco Security Manager Data Sheet*. Online. Dostupné z: <https://www.cisco.com/c/en/us/products/collateral/security/security-manager/datasheet-C78-737182.html>. [cit. 2025-05-23].
- [25] REKHTER, Y.; MOSKOWITZ, B.; KARREBERG, D.; GROOT, G. J. a LEAR, E., 1996. *RFC 1918: Address Allocation for Private Internets*. Online. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc1918>. [cit. 2025-03-02].
- [26] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2025. *Minimální požadavky na kryptografické algoritmy: doporučení v oblasti kryptografické bezpečnosti*. Online. Dostupné z: https://nukib.gov.cz/download/uredni_deska/Minimalni_pozadavky_v4_FINAL.pdf. [cit. 2025-03-02].
- [27] CISCO SYSTEMS, 2025. *Software Download*. Online. Dostupné z: <https://software.cisco.com/download/home/279513399/type>. [cit. 2025-04-29].
- [28] CRAWLEY, Don R., 2016. *Cisco ASA security appliance training: student exercise manual edition 2.1d. The accidental administrator series*. Seattle, Washington: Soundtraining.net. 2. vyd. ISBN 978-0-983-66078-1.
- [29] CISCO, 2025. *Configuring TACACS+ Servers for AAA*. Online. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_tacacs.html. [cit. 2025-04-30].

SEZNAM OBRÁZKŮ

Obrázek 2.1	Firewall	18
Obrázek 2.2	Firewall v operačním systému Windows 11	24
Obrázek 2.3	Juniper Networks SRX300 Services Gateway	25
Obrázek 3.1	Cisco ASA 5508-X.....	26
Obrázek 3.2	Ověření operačního režimu Cisco ASA	27
Obrázek 3.3	Cisco ASA 5508-X zadní strana	28
Obrázek 3.4	Obdržena informace o URL filtrování ze Cisco cloudu	30
Obrázek 3.5	Adaptive Security Device Manager.....	31
Obrázek 3.6	Cisco Security Manager.....	31
Obrázek 4.1	Topologie sítě.....	34
Obrázek 4.2	Ověření konektivity PC3	37
Obrázek 4.3	Kontrola nastavení rozhraní ASA	40
Obrázek 4.4	Verifikace OSPF konfigurace na ASA	41
Obrázek 4.5	Verifikace DHCP konfigurace na ASA	42
Obrázek 4.6	Webová stránka ASDM Launcher	43
Obrázek 4.7	Konfigurace NTP pomocí ASDM.....	44
Obrázek 4.8	Verifikace NTP konfigurace na ASA	44
Obrázek 4.9	Ověření konektivity PC2	47
Obrázek 4.10	Ověření překladu adres	47
Obrázek 4.11	Ověření připojení k webovému serveru.....	49

SEZNAM TABULEK

Tabulka 3.1	Porovnání modelů řady Cisco ASA 5500-X	28
Tabulka 4.1	IP adresování v topologii sítě	35

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA Authentication, Authorization, Accounting

ACL Access Control List

AMP Advanced Malware Protection

ARP Address Resolution Protocol

ASA Adaptive Security Appliance

ASDM Adaptive Security Device Manager

BDR Backup Designated Router

CLI Command-line Interface

CSM Cisco Security Manager

DDoS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

DoS Denial of Service

DPI Deep Packet Inspection

DR Designated Router

FAI	Fakulta aplikované informatiky
FTP	File Transfer Protocol
FWaaS	Firewall as a Service
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IDS	Intrusion Detection System
ISP	Internet Service Provider
IPS	Intrusion Prevention System
LAN	Local Area Network
MMS	Multimedia Messaging Service
MPF	Modular Policy Framework
NAT	Network address translation
NGFW	Next-Generation Firewall
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PAT	Port Address Translation
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman
RTSP	Real-Time Streaming Protocol
SMS	Short Message Service
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall

SEZNAM PŘÍLOH

PŘÍLOHA P I:	Konfigurace routeru R2
PŘÍLOHA P II:	Konfigurace routeru R3
PŘÍLOHA P III:	Konfigurace switche S1
PŘÍLOHA P IV:	Konfigurace switche S2
PŘÍLOHA P V:	Konfigurace switche S3
PŘÍLOHA P VI:	Konfigurace switche S4
PŘÍLOHA P VII:	Úplná konfigurace ASA

PŘÍLOHA P I: KONFIGURACE ROUTERU R2

```
en
conf t
hostname R2
enable secret failab
service password-encryption
no ip domain lookup
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
clock set 14:15:00 march 21 2025
ntp master 2
ntp authenticate
ntp authentication-key 1 md5 Tajny.25Time
ntp trusted-key 1
!
line vty 0 4
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
int g0/0
ip address 172.19.31.2 255.255.255.252
description R1 connection
no shut
int g0/1
ip address 172.19.31.9 255.255.255.248
description ASA connection
no shut
!
router ospf 1
router-id 1.1.1.1
network 172.19.31.0 0.0.0.3 area 0
network 172.19.31.8 0.0.0.7 area 0
auto-cost reference-bandwidth 1000
!
end
write
```

Výpis 0.13 Příkazy použité pro konfiguraci routeru R2 (zdroj: vlastní)

PŘÍLOHA P II: KONFIGURACE ROUTERU R3

```
en
conf t
hostname R3
enable secret failab
service password-encryption
no ip domain lookup
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
int g0/0
ip address 172.19.31.6 255.255.255.252
description R1 connection
no shut
int g0/1
description S4 connection
no shut
int g0/1.4
encapsulation dot1Q 4
description Vlan4_Engineers
ip address 192.168.4.1 255.255.255.0
no shut
int g0/1.5
encapsulation dot1Q 5 native
description Vlan5_Sales
ip address 192.168.5.1 255.255.255.0
no shut
exit
router ospf 1
router-id 172.19.31.2
network 172.19.31.4 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
auto-cost reference-bandwidth 1000
passive-interface GigabitEthernet0/1
!
ip dhcp excluded-address 192.168.4.1 192.168.4.2
ip dhcp pool Engineers_Pool
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
domain-name engineers.failab.cz
exit
ip dhcp excluded-address 192.168.5.1 192.168.5.2
ip dhcp pool Sales_Pool
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
domain-name sales.failab.cz
exit
!
access-list 1 permit 192.168.5.0 0.0.0.255
int g0/1.5
ip nat inside
int g0/0
ip nat outside
exit
ip nat inside source list 1 interface g0/1 overload
end
write
```

PŘÍLOHA P III: KONFIGURACE SWITCHE S1

```
en
conf t
no ip domain lookup
hostname S1
enable secret failab
service password-encryption
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
line vty 0 15
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
vlan 1
name Parking
!
interface vlan 1
ip address 192.168.1.2 255.255.255.0
description Management Interface
no shutdown
exit
ip default-gateway 192.168.1.1
!
interface vlan 1
ip address 192.168.1.2 255.255.255.0
description Management Interface
no shutdown
!
int f0/1
description ASA connection
switchport mode access
switchport access vlan 1
no shut
int f0/2
description PC1
switchport mode access
switchport access vlan 1
no shut
interface range f0/3-24
description Unused
shut
int range g0/1-2
description Unused
shut
exit
```

Výpis 0.15 Příkazy použité pro konfiguraci switchu S1 (zdroj: vlastní)

PŘÍLOHA P IV: KONFIGURACE SWITCHE S2

```
en
conf t
no ip domain lookup
hostname S2
enable secret failab
service password-encryption
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
line vty 0 15
password failab
login local
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
vlan 2
name Servers
!
interface vlan 2
ip address 192.168.2.2 255.255.255.0
description Management Interface
no shutdown
exit
ip default-gateway 192.168.2.1
!
!
int f0/1
description ASA connection
switchport mode access
switchport access vlan 2
no shut
!
int f0/2
description Server
switchport mode access
switchport access vlan 2
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security mac-address sticky
no shut
!
interface range f0/3-24
description Unused
shut
!
int range g0/1-2
description Unused
shut
exit
```

Výpis 0.16 Příkazy použité pro konfiguraci switchu S2 (zdroj: vlastní)

PŘÍLOHA P V: KONFIGURACE SWITCHE S3

```
en
conf t
no ip domain lookup
hostname S3
enable secret failab
service password-encryption
line con 0
password failab
logging synchronous
login
!
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
line vty 0 15
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
vlan 3
name Security
!
interface vlan 3
ip address 192.168.3.2 255.255.255.0
description Management Interface
no shutdown
exit
ip default-gateway 192.168.3.1
!
int f0/1
description ASA connection
switchport mode access
switchport access vlan 3
no shut
int f0/2
description PC2
switchport mode access
switchport access vlan 3
no shut
interface range f0/3-24
description Unused
shut
int range g0/1-2
description Unused
shut
end
```

Výpis 0.17 Příkazy použité pro konfiguraci switchu S3 (zdroj: vlastní)

PŘÍLOHA P VI: KONFIGURACE SWITCHE S4

```
en
conf t
no ip domain lookup
hostname S4
enable secret failab
service password-encryption
line con 0
password failab
logging synchronous
login
username admin secret thesis
ip domain name failab.cz
crypto key generate rsa modulus 1024
!
ip ssh version 2
!
line vty 0 15
password failab
login local
exec-timeout 15 0
transport input ssh
logging synchronous
!
banner motd "Authorized access only!"
!
vlan 4
name Engineers
vlan 5
name Sales
!
interface vlan 4
ip address 192.168.4.2 255.255.255.0
description Management Interface
no shutdown
!
int f0/1
description PC3
switchport mode access
switchport access vlan 4
switchport port-security
switchport port-security maximum 3
switchport port-security violation shutdown
no shut
int f0/2
description PC4
switchport mode access
switchport access vlan 5
no shut
interface range f0/3-24
description Unused
shut
int g0/1
description R3 connection
switchport mode trunk
switchport trunk native vlan 5
switchport trunk allowed vlan 4,5
no shut
int g0/2
description Unused
shut
end
```

Výpis 0.18 Příkazy použité pro konfiguraci switchu S4 (zdroj: vlastní)

PŘÍLOHA P VII: ÚPLNÁ KONFIGURACE ASA

```
ASA# sh run
: Saved
: Serial Number: JAD2146036K
: Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series
: 2000 MHz, 1 CPU (8 cores)
:
ASA Version 9.8(1)
!
hostname ASA
domain-name failab.cz
enable password $sha512$5000$eth37Bd/k755PgEXebscew==
$XGrV8fe4BTWk7ENDjvA1Rg== pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface GigabitEthernet1/1
description R2 connection
nameif outside
security-level 0
ip address 172.19.31.10 255.255.255.248
!
interface GigabitEthernet1/2
description S1 connection
nameif parking
security-level 50
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/3
description S2 connection
nameif inside
security-level 70
ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet1/4
description S3 connection
nameif security
security-level 100
ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet1/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface Management1/1
management-only
shutdown
no nameif
no security-level
no ip address
!
```

```

ftp mode passive
dns server-group DefaultDNS
domain-name failab.cz
object network parking_nat
subnet 192.168.1.0 255.255.255.0
object network security_nat
subnet 192.168.3.0 255.255.255.0
object network server_nat
host 192.168.2.3
access-list internet_to_server extended permit icmp any host
192.168.2.3
access-list internet_to_server extended permit tcp any host
192.168.2.3 eq www
pager lines 24
mtu outside 1500
mtu parking 1500
mtu inside 1500
mtu security 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network parking_nat
nat (parking,outside) dynamic interface
object network security_nat
nat (security,outside) dynamic interface
object network server_nat
nat (inside,outside) static 172.19.31.11
access-group internet_to_server in interface outside
router ospf 1
router-id 1.1.1.2
network 172.19.31.8 255.255.255.248 area 0
log-adj-changes
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp
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
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
http server enable
http 192.168.3.0 255.255.255.0 security
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.4.0 255.255.255.0 outside
ssh 192.168.3.0 255.255.255.0 security
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.1.3-192.168.1.253 parking
dhcpd option 3 ip 192.168.1.1 interface parking
dhcpd enable parking
!
dhcpd address 192.168.2.3-192.168.2.253 inside
dhcpd option 3 ip 192.168.2.1 interface inside
dhcpd enable inside
!
dhcpd address 192.168.3.3-192.168.3.253 security
dhcpd option 3 ip 192.168.3.1 interface security
dhcpd enable security
!
threat-detection basic-threat

```

```

threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp authentication-key 1 md5 *****
ntp authenticate
ntp trusted-key 1
ntp server 172.19.31.2 key 1 source outside prefer
dynamic-access-policy-record DfltAccessPolicy
username admin password $sha512$5000$/Lc6KEu5PTy0WVprPUkGIw==
$hr3w5yetvP8NJVQzZPWK6g== pbkdf2
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect dns preset_dns_map
    inspect icmp
    inspect http
policy-map type inspect dns migrated_dns_map_2
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
call-home
  profile CiscoTAC-1
    no active
    destination address http https://tools.cisco.com/its/
      service/oddce/services/DDCEService
    destination address email callhome@cisco.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
Cryptochecksum:2db954e2eac9b032c339489bdbae1e3c
: end

```

Výpis 0.19 Výpis konfigurace ASA (zdroj: vlastní)