Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnost síťové infrastruktury na platformě CISCO

Bc. Veteška Jan

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Veteška

Systémové inženýrství a informatika
Informatika

Název práce

Bezpečnost síťové infrastruktury na platformě CISCO

Název anglicky

Computer Network Security on Cisco

Cíle práce

Hlavním cílem práce je ověřit bezpečnost síťové infrastruktury na platformě CISCO. To představuje vlastní návrh, dokumentaci, realizaci, ve které je zahrnuta počítačová síť, zabezpečení sítě a ekonomické zhodnocení.

Dílčí cíle práce:
-charakteristika počítačové sítě
-bezpečnost počítačových sítí
-představení novinek a trendů
-zákon o kybernetické bezpečnosti
-návrh, realizace a testování
-závěr a doporučení

Metodika

Teoretická část obsahuje představení bezpečnostních prvků počítačové sítě a principy síťové bezpečnosti.

V praktické části bude vytvořen návrh počítačové sítě za pomocí výukového softwaru Packet Tracer od společnosti Cisco. Na tomto návrhu budou simulovány a testovány konfigurace, které slouží k zabezpečení sítě. Zabezpečení se týká 2 a 3 vrstvy referenčního modelu ISO/OSI a je zaměřeno na přepínače a směrovače. Pro simulaci v reálném prostředni bude využita počítačová laboratoř, která je vybavena Cisco zařízeními. Pro ověření bezpečnosti bude použito skenování sítě, které slouží k odhalení slabin zabezpečení.

Primárním přínosem práce je poskytnutí informací o nejrůznějších typech zabezpečení, které je možné využívat v rámci bezpečnostní politiky. Formulace závěru a doporučení.

Doporučený rozsah práce
60 – 80 stran

Klíčová slova
Cisco, Packet tracer, zabezpečení sítě, firewall, AAA, VLAN , zákon o kybernetické bezpečnosti

---

Doporučené zdroje informací

CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Brno: Computer Press, 2011. Samostudium. ISBN 978-80-251-2884-8.
CARROLL, Michael Wenstrom. Zabezpečení síti Cisco: autorizovaný výukový průvodce. Brno: Computer Press, 2003. Samostudium. ISBN 80-7226-952-6.
Kolektiv: Online kurikulum CCNA Routing and Switching: Scaling Networks verze 5.0 (aktuální verze je pro registrovené uživatele dostupná na portále netacad.com)
Kolektiv: Online kurikulum CCNA Security: Implementing Network Security 2.0 (aktuální verze je pro registrovené uživatele dostupná na portále netacad.com)
PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

Předběžný termín obhajoby
2019/20 LS – PEF

Vedoucí práce
Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště
Katedra informačních technologií

Konzultant
Ing. Alexandr Vasilenko, Ph.D.

Elektronicky schváleno dne 28. 6. 2019
Ing. Jiří Vaněk, Ph.D.
Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019
Ing. Martin Pelikán, Ph.D.
Děkan

V Praze dne 10. 02. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost síťové infrastruktury na platformě CISCO" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 6.4.2020 _____

Poděkování

Velmi rád bych touto cestou poděkoval panu Ing. Jiřímu Vaňkovi, Ph.D. za odborné rady, trpělivost, postřehy, za možnost psát práci na toto téma a vedení při zpracovaní této diplomové práce. Rád bych poděkoval panu Ing. Alexandru Vasilenkovi, Ph.D za věnování jeho času během testování v laboratoři. Dále bych chtěl poděkovat firmě VUMS DataCom s.r.o za poskytnutí odborných rad a informací v oblasti zabezpečení počítačových sítí. Poslední poděkování patří mé rodině a blízkým za podporu během celé délky mého studia.

Bezpečnost síťové infrastruktury na platformě Cisco

Abstrakt

Tato diplomová práce řeší bezpečnost síťové infrastruktury na platformě Cisco. Cílem bylo ověřit bezpečnost vlastního návrhu počítačové sítě, který byla vytvořena v Packet Traceru. Ověření bezpečnosti návrhu probíhalo ve specializované laboratoři.

Teoretická část obsahuje představení bezpečnostních prvků počítačové sítě a principy síťové bezpečnosti. V praktické části byl vytvořen návrh počítačové sítě s cílem ověření bezpečnosti na počítačové sítě 2. a 3. vrstvy ISO/OSI modelu.

Přínosem této práce je poskytnutí informací o nejrůznějších slabinách zabezpečení v počítačové síti. Finální výstup zahrnuje návrh počítačové sítě v Cisco Packet Traceru a zdrojového kódu, který byl aplikován na každé Cisco zařízení v laboratoři.

Klíčová slova: Cisco, Packet tracer, zabezpečení sítě, firewall, AAA, VLAN , VPN, zákon o kybernetické bezpečnosti, Kali Linux, cena

Security of network infrastructure on the Cisco platform

Summary

This post-graduation thesis is dealing with the security of network infrastructure on the Cisco platform. The main goal is to verify the author's computer network design, which was created in Packet Tracer. Verification of the security design was conducted in specialized laboratory.

The theoretical part contains an introduction to the security features of a computer network and the principles of network security. In the practical part, the author created a design with verifying security on computer networks of the 2nd and 3rd layers of the ISO / OSI model.

This thesis provides information about a variety of faults in the security of the device concerning a computer network. The final output contains the design of a computer network in the Cisco Packet Tracer and its source code, which is applied to each Cisco device in the laboratory.

Keywords: Cisco, Packet tracer, network security, firewall, AAA, VLAN, VPN, Act on cybersecurity, Kali Linux, price

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešní době se počítačové sítě stávají nepostradatelnou součástí našich životů. Slouží k výměně informací a propojení počítačů po celém světě. Stává se z nich spolehlivá platforma 21. století. Rostoucí množství služeb a úloh prováděných on-line způsobuje prudký nárůst počtu zařízení připojených k síti. S tím souvisí i jejich bezpečnost. Každoročně rostou případy počítačové kriminality, které mohou mít fatální dopady na fungování společnosti. Každodenní útoky směřující na firemní zařízení mají za cíl jim škodit, zejména je vyřadit z provozu nebo prolomit zabezpečení a dostat se k datům.

Bezpečná síť má za úkol chránit firemní data a provoz. Zároveň má umožnit to, aby byla odolná vůči útokům jak z vnější, tak z vnitřní sítě.

Důvodů a postupů je mnoho, a proto se tato práce zabývá zabezpečením počítačových sítí na 2 a 3 vrstvě ISO/OSI modelu. Práce je zaměřena na přepínače (switch) a směrovače (router) od společnosti Cisco.

Diplomová práce se zabývá na charakteristiku počítavé bezpečnosti. Teoretická část se zabývá charakteristikou počítačové sítě a bezpečností počítačových sítí. Její nedílnou součástí je i představení novinek a trendů. Pomocí grafů jsou znázorněny nejčastější útoky a náklady na únik dat v roce 2019.

Praktická část ověřuje bezpečnost vlastní navrhnuté topologie v software Cisco Packet Tracer. Pro reálné ověřování byla využita laboratoř síťových a internetových technologií (LSIT) v učebně D326. Poslední část zahrnuje ekonomické zhodnocení využitých zařízení od společnosti Cisco a alternativa od společnosti MikroTik.

V diplomové práci jsou využívány anglické odborné termíny. Součástí práce je slovník použitých termínů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je ověřit bezpečnost síťové infrastruktury na platformě CISCO. To představuje vlastní návrh, dokumentaci a realizaci, ve které je zahrnuta počítačová sít, zabezpečení sítě a ekonomické zhodnocení.

Dílčí cíle práce:

- charakteristika počítačové sítě
- bezpečnost počítačových sítí
- představení novinek a trendů
- zákon o kybernetické bezpečnosti
- návrh, realizace a testování
- závěr a doporučení

2.2 Metodika

Teoretická část obsahuje představení bezpečnostních prvků počítačové sítě a principy síťové bezpečnosti.

V praktické části bude vytvořen návrh počítačové sítě za pomocí výukového softwaru Packet Tracer od společnosti Cisco. Na tomto návrhu budou simulovány a testovány konfigurace, které slouží k zabezpečení sítě. Zabezpečení se týká 2 a 3 vrstvy ISO/OSI a je zaměřeno na přepínače a směrovače. Pro simulaci v reálném prostřední mi bude sloužit počítačová učebna, která je vybavena Cisco zařízeními. Pro ověření bezpečnosti bude použito skenování sítě, která slouží k odhalení slabin zabezpečení.

Primárním přínosem práce je poskytnutí informací o nejrůznějších typech zabezpečení, které je možné využívat v rámci bezpečnostní politiky. Závěr a doporučení.

SLOVNÍK POUŽITÝCH TERMÍNŮ

Admin / Administrátor	Správce, nejčastěji počítačové sítě. Pracovník, který má síť na starosti a stará se o to, aby vše nejenom fungovalo, ale také aby do sítě nevstupoval někdo cizí, kdo do sítě nemá přístup. Správce sítě je občas označuje jako admin.
AAA	Authentication Authorization and Accounting.
Authorization	Oprávnění. Používá se v kontextu autorizace, ověření vaší totožnosti. Slouží pro průstup k datům.
DNS	Doménový jmenný systém. Každý počítač, který je připojený k internetu má svou jedinečnou adresu na světe .DNS je protokol, který překládá slovní formu na IP adresy.
DoS	Denial of service - odepření služby
Firewall	Doslovný překlad z angličtiny se jmenuje „požární zeď“ . Firewall je bezpečnostní zařízení nebo program.
Gateway	Z angličtiny před je brána. Slouží k převodu mezi dvěma různými protokoly.
Hacker	Záškodník, který narušuje počítačové systémy.
Kylogger	Keylogger je software, který snímá stisky jednotlivých kláves
LAN	Lokální počítačová sít. Vzájemné propojení počítačů, kteří si mezi sebou vyměňují data.
Online	Být připojen.
Paket	Blok dat přenášených v síti.
Password	Heslo.
Ping	Testování pojení mezi jednotlivými zařízeními.
Router	Síťové zařízení , které předává datové pakety mezi počítačovými sítěmi. Český překlad je směrovač.
Server	Počítač, který poskytuje různorodé služby od DNS /DHCP / FTP server.
Telnet	Nejstarší protokol pro vzdálenou práci.

SSH	Secure Shell. Zabezpečený komunikační protokol pro vzdálenou práci.
CLI	Představuje uživatelské rozhraní, ve kterém uživatel s programy nebo operačním systémem komunikuje zapisováním příkazů do příkazového řádku.
NAT	Síťový překlad adres. Překlad veřejných IP adres na lokální a naopak.
ACL	Access Control List. Seznam oprávnění.
OSPF	Open Shortest Path First. Směrovací protokol.
DHCP	Dynamic Host Configuration Protocol. Protokol poskytující IP adresy koncovým zařízením.
VLAN	Virtuální LAN.
VTY	Virtual teletype.
DHCP spoofing	Konkrétní druh DHCP útoku.
VPN	Virtual private network - Virtuální privátní síť.
Spaning tree	Zkratka STP. Síťový protokol, který v ethernetových LAN sítích odstraňuje smyčky.
TCP	Transmission Control Protocol.
UDP	User Datagram Protocol.
Switch	Síťový přepínač. Aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie.
MITM	Man in the middle (z angličtiny „člověk uprostřed“). Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem.
Segmentovaná sítě	Počítačové síti je akt nebo postup rozdělení počítačové sítě do podsítí , z nichž každá je segmentem sítě . Výhody takového rozdělení jsou především pro zvýšení výkonu a zvýšení bezpečnosti.

[1] [2] [3] [4] [5] [6]

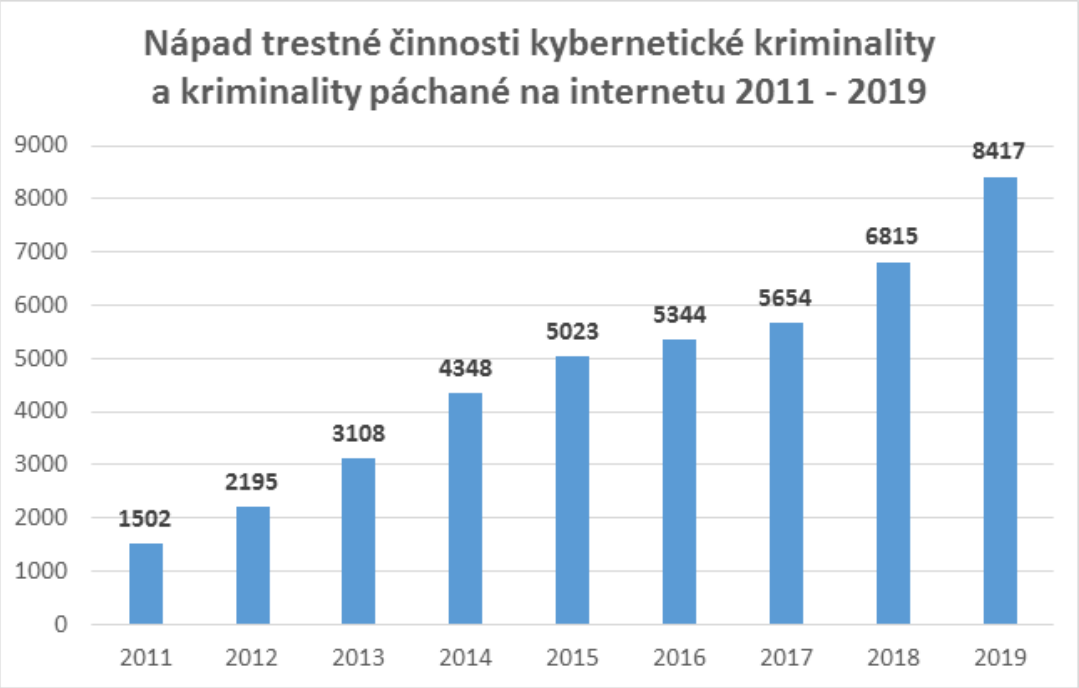
3 Teoretická východiska

Nadcházející část diplomové práce vysvětluje veškeré teoretické podklady potřebné k bezpečnosti počítačové sítě.

3.1 Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

Informační kriminalistika je nejrychleji se rozvíjející forma kriminalit na území České republiky. Hlavní příčinou je že, každý rok celosvětově přibývá počet uživatelů kteří, používají internetové připojení. V roce 2004 bylo k internetu připojeno 750 milionů lidí.

Po deseti letech toto číslo narostlo na neuvěřitelné 3 miliardy. V roce 2014 Policie ČR zaznamenala nárůst této trestné činnosti spáchané v oblasti výpočetní techniky o 50%. Kybernetická kriminalita byla v minulosti značena jako informační kriminalita. Kybernetická kriminalita je podle „Policie ČR“ jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Policie ČR od r. 2011 pozoruje počet trestných činů spáchaných v kyberprostoru. V uvedeném období je pozorován trend stálého nárůstu evidovaných případů kybernetické kriminality (Obrázek 1). Tato data jsou pouze ohlášená, ale počet útoků které, nebyly ohlášeny mohou toto číslo zvětšit i několikrát. [2]



Obrázek 1 - Kyberkriminalita od roku 2011 – 2019 [2]

Od 1. ledna roku 2015 proto přišel v platnost účinný zákon 181/2014 SB. o kybernetické bezpečnosti, jehož cílem je ochrana významných informačních a komunikačních systémů států včetně soukromých subjektů. Lze právě předpokládat že, tyto systémy budou ve velkém případě napadány. Souhrnně řečeno kybernetický zákon o bezpečnosti řeší:

- Definuje pojmy a systémy zajištění kybernetické bezpečností, bezpečnostních opatření v oblasti zabezpečení informačních a komunikačních systémů
- Stanovuje kybernetické nebezpečí a jak na ně mají jednotlivé objekty a subjekty odpovídat.
- Národní úřad pro kybernetickou a informační bezpečnost určuje jak se má kontrolovat, postupovat a popřípadě pokutovat správní delikty.
- Ukládá subjektům celkem pět zákonných povinností, co musí hlásit. Subjekty musí uvádět své kontaktní údaje, detekovat kybernetické bezpečnostní události, hlášení kybernetického útoku, zpracování kybernetické bezpečnostní dokumentace, zavádět bezpečnostní opatření a provádět opatření vydaná Národní úřadem pro kybernetickou a informační bezpečnost.

Autoři zákona deklarují, že zákon je postaven na spolupráci mezi veřejným a soukromým sektorem. Zákon však ukládá mnoho povinností pro subjekty ale, nabízí velmi málo jako protislužbu. Velký důraz autoři kladou na spolupráci v oblasti školení, vzdělávání, řešení problematických kyberútoků nebo simulace.

Zákon o kybernetické bezpečnosti je významný krok směrem k bezpečnějšímu digitálnímu prostředí. Klade velké nároky na zdroje pro povinné osoby, inspiraci i podnikům, které nejsou součástí povinných osob. Pomáhá zvýšit povědomí o kybernetické bezpečnosti a jejích praktikách a také o tom, že bezpečnost není pouhé jednorázové technické řešení problému.

Příkladem z praxe může být nemocnice, která se musí řídit požadavky zákona o kybernetické bezpečnosti. To znamená zavedení systému řízení bezpečnosti informací, včetně provedení analýzy rizik a implementaci příslušných technických a organizačních bezpečnostních opatření, jak je definuje vyhláška o kybernetické bezpečnosti č. 82/2018 Sb. Zároveň nemocnice má povinnost komunikovat a spolupracovat s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a hlásit incidenty týmu vládního CERT. V případě neplnění těchto povinností může být nemocnice sankcionována, horní hranice těchto sankcí činí až 5 mil. Kč. [2] [3] [4] [5]

ZÁKLADNÍ USTANOVENÍ Zákona č. 181/2014 Sb.

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

§ 3

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací1), pokud není orgánem nebo osobou podle písmene b),
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
c) správce a provozovatel informačního systému kritické informační infrastruktury,
d) správce a provozovatel komunikačního systému kritické informační infrastruktury,
e) správce a provozovatel významného informačního systému,
f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
h) poskytovatel digitální služby. [17]

§ 5

(1) Bezpečnostními opatřeními jsou
   a) organizační opatření a
   b) technická opatření.
(2) Organizačními opatřeními jsou
   a) systém řízení bezpečnosti informací,
   b) řízení rizik,
   c) bezpečnostní politika,
   d) organizační bezpečnost,
   e) stanovení bezpečnostních požadavků pro dodavatele,
   f) řízení aktiv,
   g) bezpečnost lidských zdrojů,
   h) řízení provozu a komunikací,
   i) řízení přístupu osob,
   j) akvizice, vývoj a údržba,
   k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
   l) řízení kontinuity činností a
   m) kontrola a audit.

(3) Technickými opatřeními jsou
   a) fyzická bezpečnost,
   b) nástroj pro ochranu integrity komunikačních sítí,
   c) nástroj pro ověřování identity uživatelů,
   d) nástroj pro řízení přístupových oprávnění,
   e) nástroj pro ochranu před škodlivým kódem,
   f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
   g) nástroj pro detekci kybernetických bezpečnostních událostí,
   h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
   i) aplikační bezpečnost,
   j) kryptografické prostředky,
   k) nástroj pro zajišťování úrovně dostupnosti informací a
   l) bezpečnost průmyslových a řídících systémů [17]

3.1.1 **Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti**

Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).[18]

Předmět úpravy vyhlášky o kybernetické bezpečnosti

Tato vyhláška zapracovává příslušný předpis Evropské unie (Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii) a pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby a nebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb, (dále jen „informační a komunikační systém“) upravuje:

a) obsah a strukturu bezpečnostní dokumentace,
b) obsah a rozsah bezpečnostních opatření,
c) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
d) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
e) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
f) vzor oznámení kontaktních údajů a jeho formu a
g) způsob likvidace dat, provozních údajů, informací a jejich kopií. [18]

3.1.1.1 **Vyhláška o kybernetické bezpečnosti - Hodnocení aktiv**

(1) Pro hodnocení důležitosti aktiv jsou v tomto případě použity stupnice o čtyřech úrovních a posuzuje se, jaký dopad by mělo narušení bezpečnosti informací u jednotlivých aktiv. Povinná osoba může používat odlišný počet úrovní pro hodnocení důležitosti aktiv, než jaký je uveden v této příloze, dodrží-li jednoznačné vazby mezi jimi používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv, které jsou uvedeny v této příloze.
(2) Je doporučeno, aby si každá povinná osoba tyto dopadové matice přizpůsobila svým potřebám.

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4.

Obrázek 2 - Stupnice pro hodnocení důvěrnosti [18]

Tab. 2: Stupnice pro hodnocení integrity

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Tab. 3: Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Obrázek 3 - Stupnice pro hodnocení integrity [18]

3.1.1.2 **Vyhláška o kybernetické bezpečnosti - Hodnocení rizik**

h) 1) Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 5.
i) (2) Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.
j) (3) Pro hodnocení rizik lze použít například tuto funkci:
k) Riziko = dopad x hrozba x zranitelnost.
l) (4) Dopad je v tomto případě odvozen z hodnocení aktiv podle přílohy č. 1.
m) (5) V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Tab. 1: Stupnice pro hodnocení hrozeb

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tab. 2: Stupnice pro hodnocení zranitelností

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tab. 3: Stupnice pro hodnocení rizik

Úroveň	Popis
Nízké	Riziko je považováno za akceptovatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Obrázek 4 - Stupnice pro hodnocení hrozeb, zranitelnosti a rizik [18]

3.1.1.3 **Vyhláška o kybernetické bezpečnosti- Zranitelnosti a hrozby**

Obrázek (Obrázek 5) obsahuje jen vybrané kategorie zranitelností a hrozeb. Identifikace konkrétních zranitelností a hrozeb je odpovědností povinné osoby.

Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,

2. zastaralost informačního a komunikačního systému,

3. nedostatečná ochrana vnějšího perimetru,

4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,

5. nedostatečná údržba informačního a komunikačního systému,

6. nevhodné nastavení přístupových oprávnění,

7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,

9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,

10. nedostatečná ochrana aktiv,

11. nevhodná bezpečnostní architektura,

12. nedostatečná míra nezávislé kontroly,

13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,

2. poškození nebo selhání technického anebo programového vybavení,

3. zneužití identity,

4. užívání programového vybavení v rozporu s licenčními podmínkami,

5. škodlivý kód (například viry, spyware, trojské koně),

6. narušení fyzické bezpečnosti,

7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,

8. zneužití nebo neoprávněná modifikace údajů,

9. ztráta, odcizení nebo poškození aktiva,

10. nedodržení smluvního závazku ze strany dodavatele,

11. pochybení ze strany zaměstnanců,

12. zneužití vnitřních prostředků, sabotáž,

13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,

14. nedostatek zaměstnanců s potřebnou odbornou úrovní,

15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,

16. zneužití vyměnitelných technických nosičů dat,

17. napadení elektronické komunikace (odposlech, modifikace).

Obrázek 5 - Zranitelnosti a hrozby [18]

3.1.2 **Národní úřad pro kybernetickou a informační bezpečnost**

NÚKIB vykonává řadu zákonných činností, například: vydává opatření, ukládá příslušné správní sankce, působí jako koordinační orgán ve stavu kybernetického nebezpečí, poskytuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a vybrané oblasti ochrany utajovaných skutečností, analýzy a monitorování kybernetických hrozeb a rizik, působící v oblasti veřejné regulované služby evropského družicového navigačního programu Galileo. Úřad dále provádí odpovídající kontrolu. Mezi působnost NÚKIB patří například:

- Vytvoření strategie kybernetické bezpečnosti
- Příprava zákonů a podzákonných norem v oblasti kybernetické bezpečnosti
- Příprava a koordinace kybernetických cvičení jak v ČR, tak v zahraničí

Ředitel Úřadu se pravidelně účastní jednání Bezpečnostní rady státu a je členem Výboru pro kybernetickou bezpečnost , který je stálým pracovním orgánem Bezpečnostní rady státu pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky. [13]

Obrázek 6 - Národní úřad pro kybernetickou a informační bezpečnost [13]

Z nejvíce zásadních upozornění, které zachytila široká veřejnost je zpráva o společnosti Huawei. Dne 17. prosinec 2018 národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. Používání těchto prostředků představuje bezpečnostní hrozbu. Na základě této zprávy a zákona o kybernetické bezpečnosti musí firmy, které spolupracují s firmou Huawei zavést příslušná opatření.[13]

3.2 Charakteristika produktu od společnosti Cisco

3.2.1 Společnost Cisco

Cisco je jedna z největších světových firem v oblasti síťových řešení, která jejich pomocí změnila a mění způsob, jakým se dnes lidé připojují k internetu, komunikují mezi sebou a spolupracují. Poskytují širokou škálu technologií v oblasti přenosu dat, hlasu, obrazu a v oblasti pevných a bezdrátových sítí. Společnosti patří například nástroje pro efektivní týmovou spolupráci a jednání na dálku, jako je TelePresence nebo WebEx. Cisco předkládá ucelené řešení firemní komunikace jak pro velké i malé podniky, zařízení a aplikace pro routery, switche, multimédia, cloudové řešení a datové sklady. [1][4]

Historie a současnost

Společnost Cisco byla založena v roce 1984 ve Stanfordu. Od samých počátků hráli technici a inženýři společnosti vedoucí úlohu ve vývoji síťových technologií založených na internetovém protokolu (IP). Kvůli tomu téměř veškerá data na internetu proudí přes produkty od společnosti Cisco. Dnes tato společnost po celém světě zaměstnává kolem 76 tisíc lidí a v roce druhém kvartálu 2019dosáhla čistých tržeb ve výši 2,822 miliard dolarů. Cisco vydalo za posledních 10 let meziročně v průměru 6,1 miliard dolarů na výzkum a vývoj. Řadí se mezi nejlepší špičku ve srovnání s ostatními společnostmi. [1][4]

Cisco v České republice

Na českém trhu působí Cisco od roku 1995. Cílem společnosti na našem trhu je pomáhat velkým organizacím a také malým a středním firmám dosáhnout větší efektivity s využitím moderních technologií a také větší efektivity v oblasti bezpečnosti. Pomáhá řešit také situaci v oblasti vzdělávání ICT specialistů v České republice. Příkladem toho může být stipendijní program CCIE pro studenty vysokých škol nebo projektu Cisco Networking Academy Program. Jeho cílem je vzdělávat a vychovávat nové odborníky v oblasti síťových technologií. [1][4]

3.2.2 **Cisco IOS Software**

Všechna koncová zařízení a síťová zařízení vyžadují operační systém. Část operačního systému, která interaguje přímo s počítačovým hardwarem, se nazývá kernel. Část, která je v rozhraní s aplikacemi a uživatelem, se nazývá shell (příkazový procesor). Uživatel může komunikovat s shellem pomocí rozhraní příkazového řádku nebo grafického uživatelského rozhraní.

Při použití CLI uživatel interaguje přímo se systémem v textovém prostředí zadáním příkazů na klávesnici do příkazového řádku. Systém provede příkaz a často poskytuje textový výstup. Provoz CLI vyžaduje jen velmi malou režii. Vyžaduje však, aby uživatel měl znalosti základní struktury, která řídí systém.

Rozhraní GUI, jako jsou Windows, Apple iOS nebo Android, umožňuje uživateli komunikovat se systémem pomocí prostředí grafických ikon, nabídek a oken. Uživatelské rozhraní je přívětivější a vyžaduje méně znalostí základní struktury příkazů, které řídí systém. Z tohoto důvodu se mnoho uživatelů spoléhá na prostředí GUI.

Síťový operační systém používaný na zařízeních Cisco se nazývá operační systém Cisco IOS (Internetwork operationg systém). Cisco IOS je systémové jádro vyvinuté společností Cisco, které poskytuje funkce které sloužící k rotování, směrování, propojení sítí a telekomunikací mezi zařízeními. První verze byla vyvinuta v roce 1986. [4]

Software IOS od společnosti Cisco se stará o nadcházející úkoly

- Přenos sítových protokolů a funkcí
- Propojení vysokorychlostních přenosů mezi zařízeními
- Doplnění bezpečnosti kvůli řízení a přístupu a zamezení neoprávnění použití sítě
- Poskytování škálovatelnost i za účelem usnadnění růstu sítě a zaručení redundance
- Zajištění spolehlivosti sítě při připojovaní k sítovým prostředkům

K systému ISO je možné přistupovat těmito způsoby:

- Pomocí webového prohlížeče
- Pomocí sériové konzole
- Pomocí CLI protokolem Telnet nebo SSH [4]

3.3 Bezpečnost počítačových sítí

Zabezpečení sítě je nedílnou součástí počítačových sítí. Zabezpečení sítě zahrnuje protokoly, technologie, zařízení, nástroje a techniky pro zabezpečení dat a zmírnění útoků. Síťová bezpečnostní řešení se objevila v 60. letech 20. století, ale až do 2000. let se nevytvářel komplexní soubor řešení pro moderní sítě.

Zabezpečení sítě je do značné míry poháněno snahou zůstat o krok napřed před hackery (útočníky). Odborníci v oblasti zabezpečení sítě se pokoušejí zabránit případným útokům a zároveň minimalizují účinky útoků v reálném čase. Kontinuita podnikání je dalším faktorem zabezpečení sítě.

Organizace pro zabezpečení sítě byly vytvořeny, aby vytvořily společenství profesionálů pro zabezpečení sítě. Tyto organizace stanovují standardy, podporují spolupráci a poskytují příležitosti pro rozvoj pracovních sil pro profesionály v oblasti zabezpečení sítě. Odborníci na zabezpečení sítě by si měli být vědomi zdrojů poskytovaných těmito organizacemi

Zásady zabezpečení sítě jsou vytvářeny společnostmi a vládními organizacemi, aby zaměstnancům poskytovaly rámec, který mají dodržovat během své každodenní práce. Za vytvoření a udržování politiky zabezpečení sítě jsou odpovědní odborníci na zabezpečení sítě na úrovni správy sítě. Všechny postupy zabezpečení sítě se vztahují k zásadám zabezpečení sítě a řídí se jimi.

Zabezpečení sítě je rozděleno do domén zabezpečení sítě a síťové útoky jsou organizovány do klasifikací, aby bylo snazší se o nich dozvědět a správně je řešit. Viry, červy a trojské koně jsou specifické typy síťových útoků. Obecněji jsou síťové útoky klasifikovány jako průzkumy, útoky nebo útoky typu DoS. Zmírňování síťových útoků je úkolem administrátora v oblasti zabezpečení sítě. [5]

3.3.1 Sítě jsou cíle

Sítě jsou každodenně pod útokem. Je běžné číst zprávy o další napadené síti. Dostupné internetové vyhledávání „napadená počítačová síť“ odhalí mnoho článků týkajících se síťových útoků, včetně ohrožených organizací, nejnovějších hrozeb pro zabezpečení sítě, nástrojů ke zmírnění útoků a dalších. [5]

Důvody pro zabezpečení sítě

Zabezpečení sítě přímo souvisí s obchodní politikou organizace. Porušení zabezpečení sítě může narušit elektronický obchod, způsobit ztrátu obchodních dat, ohrozit soukromí lidí a ohrozit integritu informací. Tato porušení mohou mít za následek ztrátu příjmů pro společnosti, krádež duševního vlastnictví, soudní spory a mohou dokonce ohrozit veřejnou bezpečnost. Zákon o kybernetické bezpečnosti právě slouží k tomu, aby vůbec k potenciálnímu úkolu nedošlo.

Udržování zabezpečené sítě zajišťuje bezpečnost uživatelů sítě a chrání obchodní zájmy firmy nebo zájmy státu. Pro udržení bezpečnosti v síti je vyžadována ostražitost ze strany odborníků na bezpečnost sítí. Musí si neustále uvědomovat nové a vyvíjející se hrozby a útoky na sítě a zranitelnosti zařízení a aplikací. [5]

Charakteristika síťových útoků

Útočný faktorem je znalost nebo nástroj pomocí nichž může útočník získat přístup k serveru, hostiteli nebo do sítě. Mnoho útočných faktorů pochází z vnější strany podnikové sítě. Útočníci mohou například zacílit na síť prostřednictvím Internetu ve snaze narušit síťové operace a vytvořit útok na odmítnutí služby (DoS).Útočné vektory mohou také pocházet z vnitřku sítě. Interní uživatel, například zaměstnanec, může náhodně nebo úmyslně:

- Ukrást a zkopírovat důvěrná data na vyměnitelná média, e-mail, software pro zasílání zpráv a další média.
- Kompromitovat interní servery nebo zařízení síťové infrastruktury.
- Odpojit kritické síťové připojení a způsobit výpadek sítě.
- Připojit infikovanou jednotku USB k podnikovému počítačovému systému.

Interní hrozby mohou také způsobit větší škody než externí hrozby, protože interní uživatelé mají přímý přístup do budovy a jejích infrastrukturních zařízení. Zaměstnanci mají rovněž znalosti o podnikové síti, jejích zdrojích a důvěrných datech. Odborníci na síťovou bezpečnost musí implementovat nástroje a používat techniky pro zmírnění vnějších i vnitřních hrozeb. [5]

Ztráta dat

Data budou pravděpodobně nejcennější věcí celé firmy. Firemní data mohou zahrnovat údaje o výzkumu a vývoji, o prodeji, financích, lidských zdrojích a právech, o zaměstnancích, o dodavatelích a údaje o zákaznících. V dnešní době jsou data velice cenná věc, které stojí nemalé peníze. Ztráta dat nastává, když jsou data úmyslně nebo neúmyslně ztracena, odcizena nebo pokud uniknou do vnějšího světa. Odborníci na zabezpečení sítě musí chránit data organizace. Musí být zavedeny různé kontroly prevence ztráty dat, aby nedošlo k problémům, které byli zmíněny. Ztráta dat může vést k:

- Poškození značky a ztráta reputace
- Ztrátě konkurenční výhody
- Ztrátě zákazníků
- Ztrátě příjmů
- Soudnímu řízení vedoucímu k pokutám a občanským sankcím [5]

Sítě kampusu

Administrátoři v síti musí implementovat různé techniky zabezpečení sítě, aby chránili data organizace před vnějšími a vnitřními hrozbami. Před dosažením podnikových zdrojů musí být připojení k nedůvěryhodným sítím důkladně zkontrolováno několika vrstvami obrany. [5]

Sítě datových center

Sítě datových center jsou obvykle umístěny v externích zařízeních pro ukládání citlivých nebo vlastnických dat. Tyto weby jsou propojeny s podnikovými weby pomocí technologie VPN se zařízeními ASA a integrovanými switch datových center, jako jsou vysokorychlostní switche. Dnešní datová centra ukládají obrovské množství citlivých, kriticky důležitých informací. Fyzická bezpečnost je proto pro její fungování kritická. Fyzická bezpečnost nejen chrání přístup k areálu, ale také chrání lidi a zařízení. Například jsou zavedeny požární poplachy, serverové stojany a redundantní systémy vytápění, větrání a klimatizace a UPS, které chrání lidi a zařízení.

- Vnější obvodové zabezpečení
    - To může zahrnovat bezpečnostní důstojníky na místě, ploty, brány, nepřetržité video sledování a alarmy narušení bezpečnosti.
- Vnitřní obvodová bezpečnost
    - Může zahrnovat nepřetržité video sledování, elektronické detektory pohybu, bezpečnostní pasti a biometrické snímače vstupu a výstupu. [5]

3.3.2 **Hacker**

Hacker je běžný termín používaný k charakterizuje síťového útočníka. Výraz „hacker“ má však různé významy: [20]

- Chytrý programátor schopný vyvíjet nové programy a kódovat změny stávajících programů, aby byly efektivnější.
- Síťový profesionál, který používá sofistikované programovací dovednosti, aby zajistil, že sítě nebudou náchylné k útoku.
- Osoba, která se snaží získat neoprávněný přístup k zařízením na internetu.
- Jednotlivci, kteří spouští programy, které zabraňují nebo zpomalují přístup k síti velkému počtu uživatelů nebo poškozují nebo vymazávají data na serverech.

Hackerství je důležitým aspektem zabezpečení sítě. Hackerstvím se dá i živit. Aktuálně společnost Apple nabízí 1 milion dolarů člověku za prolomení bezpečnosti jejich mobilního zařízení iPhone nebo jejich software. [5]

Evoluce hackerů

Hacking začal v 60. letech 20. V polovině osmdesátých let byly k připojení počítačů k sítím používány modemy vytáčeného připojení. Hackeři psali programy, které vytočily každé telefonní číslo v dané oblasti při hledání počítačů, systémů vývěsek a faxů. Když bylo nalezeno telefonní číslo, byly k získání přístupu použity programy na prolomení hesla. Od té doby se obecné profily a metody hackerů docela změnily. V dnešní době se ještě dělí na:

- White hat (Bílý klobouk)
- Black hat (Černý klobouk)
- Gray hat (Šedý klobouk)
- Elitní cracker
- Blue Hat (Modrý klobouk)
- Cracktivista [5]

Kybernetičtí zločinci

Kybernetičtí zločinci jsou hackeři s motivem vydělat peníze pomocí jakýchkoli nezbytných prostředků. I když někdy jde o osamělé jedince pracující samostatně, častěji jsou financovány a sponzorovány zločineckými organizacemi. Odhaduje se, že kybernetičtí zločinci na celém světě ukradnou spotřebitelům a podnikům miliardy dolarů ročně.

Kybernetičtí zločinci působí v podzemní ekonomice, kde nakupují, prodávají a obchodují s nástroji pro útoky, služby botnetů (internetový robot), bankovní trojské koně, keyloggery a mnoho dalšího. Kupují a prodávají také soukromé informace a duševní

vlastnictví, které ukradli obětem. Počítačoví zločinci se zaměřují na malé podniky a spotřebitele, jakož i na velké podniky a průmyslová odvětví. [5]

Hacktivisté

Hacktivisté neusilují o zisk, jejich hlavní motivace je strhnout pozornost. Jsou to obvykle politicky nebo sociálně motivovaní kybernetičtí útočníci, kteří využívají sílu internetu k propagaci svých sdělení.

Dva příklady hacktivistických skupin jsou Anonymous a Syrian Electronic Army. Ačkoli většina hacktivistických skupin není extrémně organizovaná, mohou vládám a podnikům způsobit značné problémy. Hacktivisté mají sklon spoléhat se na poměrně základní, volně dostupné nástroje. [5]

Státem podporovaní Hackeři

Státní sponzorovaní počítačoví hackeři jsou nejnovějším typem hackerů. Jedná se o státem financované a řízené útočníky, kteří mají za úkol zahájit operace, které se liší od kybernetické špionáže po krádež duševního vlastnictví. Mnoho hackerů sponzoruje tyto hackery, ale jen velmi málo jich veřejně připouští, že existují. Národy si najímají ty nejlepší talenty, aby vytvořily ty nejpokročilejší a nejzávažnější hrozby. Státem podporovaní hackeři vytvářejí pokročilé, přizpůsobené útočné kódy, často využívající dříve neobjevené zranitelnosti softwaru. Příklad útoku podporovaného státem zahrnuje malware Stuxnet, který byl vytvořen, aby poškodil íránské jaderné odvětví. [5]

Obrázek 7 – Hacker [26]

3.3.3 Typy útoků

Zavedení Attack Tools

Aby útočník mohl zneužít zranitelnost, musí mít techniku nebo nástroj, který lze použít. V průběhu let se útočné nástroje staly sofistikovanějšími a vysoce automatizovanými a vyžadují k jejich použití méně technické znalosti než v minulosti. [5]

Vývoj bezpečnostních nástrojů

Hackování zahrnuje mnoho různých typů nástrojů pro testování a udržování sítě a jejích dat v bezpečí. Pro ověření bezpečnosti sítě a jejích systémů bylo vyvinuto mnoho nástrojů pro testování penetrace sítí. Mnoho z těchto nástrojů však mohou hackeři využít ke skenování. Hackeři také vytvořili různé hackerské nástroje. Tyto nástroje jsou výslovně psány k útočným důvodům. Velké množství těchto nástroju je zdarma. Pomocí jednotných návodů a internetových videí na kanále YouTube je možné tyto nástroje snadno ovládat. [5]

Počítačové viry

Počítačový virus je škodlivý kód, který je připojen ke spustitelným souborům, které jsou často legitimními programy. Většina virů vyžaduje aktivaci koncového uživatele a nečinnost delší dobu a poté se aktivuje v určitý čas nebo datum.

Jednoduchý virus se může nainstalovat do prvního řádku kódu počítače spustitelného souboru. Při aktivaci může virus zkontrolovat disk na jiné spustitelné soubory, aby mohl infikovat všechny soubory, které ještě nebyly infikovány. Viry mohou být neškodné. Například viry, které se zobrazují na obrazovce, nebo mohou být viry destruktivního charakteru, které upravují nebo odstraňují soubory na pevném disku.

Většina virů se nyní šíří paměťovými jednotkami USB, CD, DVD, sdílenými soubory v síti a e-mailem. E-mailové viry jsou nyní nejčastějším typem. Proto často dochází k tomu, že neznalí lidí otevřou email a stáhnou si do svého počítače škodlivý virus. [5]

Trojský kůň

Termín trojský kůň pocházel z řecké mytologie. Trójský kůň je malware, který provádí škodlivé operace pod záminkou požadované funkce. Trójský kůň přichází se skrytým škodlivým kódem. Tento škodlivý kód využívá oprávnění uživatele. Často jsou trojské koně připojeny k hrám, které lidi stahují z různých torrentů nebo webů. Tyto hry jsou většinou kradené a stahují je lidé kteří nechtějí za dané hry platit. Při hraní hry

si uživatel nevšimne problému. V pozadí byl na systému uživatele nainstalován trojský kůň. Škodlivý kód od trojského koně pokračuje v činnosti i po ukončení hry.

Koncept trojského koně je flexibilní. Může způsobit okamžité poškození, poskytnout vzdálený přístup do systému nebo přístup přes zadní dveře. Může také provádět akce podle pokynů na dálku, například odeslat mi soubor s heslem jednou týdně. Trojské koně psané na míru, jako jsou viry se specifickým cílem, je obtížné odhalit. [5]

Červy

Červi se replikují tím, že samostatně zneužívají zranitelnosti v sítích. Červi obvykle zpomalují sítě. Zatímco virus vyžaduje spuštění hostitelského programu, červy mohou běžet samy. Kromě počáteční infekce již nevyžadují účast uživatelů. Po napadení hostitele je červ schopen šířit se po síti velmi rychle. Červi jsou zodpovědní za některé z nejničivějších útoků na internetu. V roce 2001 napadl červ Red Code infikovaných 658 serverů. Během 19 hodin infikoval červ více než 300 000 serverů. Počáteční infekce červa SQL Slammer, známého jako červ, který zamořil internet. SQL Slammer byl útok DoS, který využíval chybu přetečení vyrovnávací paměti na serveru SQL společnosti Microsoft. Na svém vrcholu se každých 8,5 sekund zdvojnásobil. Proto byl schopen nakazit 250 000+ hostitelů do 30 minut. Když byl vydán 25. ledna 2003, narušil internet, finanční instituce, bankomaty a další. Na infikovaných serverech nebyla aktualizovaná oprava použita. Pro mnoho organizací to byla výzva k probuzení, která zavedla bezpečnostní politiku vyžadující včasné aktualizace a opravy.

V roce 2004 by červ MyDoom aktivoval netušící uživatel otevřením přílohy v e-mailu. Příloha uvolnila červa, který byl schopen zjistit všechny dostupné e-mailové adresy v systému. Červ poté zaslal spam všem e-mailům, které objevil. To dramaticky ovlivnilo internet. Ostatní uživatelé otevřeli přílohu od prvního uživatele a cyklus by se opakoval.

Všechny tito červi sdílejí podobné vzorce. Navzdory technikám zmírňování, které se objevily v průběhu let, se červi s internetem vyvíjeli a stále představují hrozbu. Zatímco červi se postupem času stávali sofistikovanějšími, stále mají tendenci vycházet ze zneužívání slabých stránek v softwarových aplikacích. [5]

Většina útoků červů se skládá ze tří složek

- Povolení zranitelnosti
  - Červ se nainstaluje pomocí zranitelného mechanismu, jako je e-mailová příloha, spustitelný soubor nebo trojský kůň, na zranitelný systém.
- Propagační mechanismus
  - Po získání přístupu k zařízení se červ replikuje a lokalizuje nové cíle.
- Zatížení
  - Nejčastěji se používá k vytvoření infikovaného hostitele nebo k útoku DoS, který je nejvíce známý.

Červi jsou samostatné programy, které útočí na systém a zneužívají známou zranitelnost. [5]

Ostatní Malware

Hackeři použili viry, červy a trojské koně k přepravě zatížení systému a z jiných škodlivých důvodů. Malware se neustále vyvíjí Zde je několik příkladů pestro moderních malwarů :

- Ransomware - Tento malware zakazuje přístup k infikovanému počítačovému systému. Ransomware pak požaduje výkupné za omezení, které má být následně odstraněno.
- Spyware - Tento malware se používá ke shromažďování informací o uživateli a zasílání informací bez souhlasu uživatele. Spyware lze klasifikovat jako systémový monitor, trojský kůň, adware, sledování cookies a klíčové loggery.
- Adware - Tento malware obvykle zobrazuje nepříjemná vyskakovací okna, aby generoval příjmy pro svého autora. Malware může analyzovat zájmy uživatelů sledováním navštívených webových stránek. Poté může na tyto weby poslat vyskakovací reklamu relevantní.
- Scareware - Tento malware zahrnuje podvodný software, který pomocí sociálního inženýrství šokuje nebo vyvolává úzkost vytvářením vnímání hrozby. Obecně je zaměřen na nic netušícího uživatele.
- Phishing - Tento malware se pokouší přesvědčit lidi, aby vyzradili citlivé informace. Příkladem může být přijetí e-mailu od banky s požadavkem na vyzrazení účtu a čísla PIN. Častým phishing útokem jsou hesla k účtům na sociální sítě daného uživatele.
- Rootkits - Tento malware je nainstalován na ohroženém systému. Poté, co je nainstalován, nadále skrývá své narušení a udržuje privilegovaný přístup k hackerovi.

Tento seznam se bude s vývojem internetu nadále rozšiřovat. Nový malware bude vždy vyvíjen. Hlavním cílem hackerů je naučit se nový malware. Často je to i otázkou hry daných hackerů a poměřování sil, na základě kterých mezi sebou soutěží, kdo je lepší v hackingu. [5]

Existuje několik typů přístupových útoků

- Útok na heslo - Hackeři se pokoušejí objevit systémová hesla pomocí různých metod,.
- Využití důvěryhodnosti - Hacker používá neautorizovaná oprávnění k získání přístupu k systému, což může ohrozit cíl.
- Přesměrování portů - hacker používá kompromitovaný systém jako základnu pro útoky proti jiným cílům.
- Útok typu Man-in-the-middle - Hacker je umístěn mezi dvěma legitimními zařízeními, aby mohl číst nebo upravovat data, která prochází mezi oběma stranami.
- Přetečení vyrovnávací paměti - to je situace, kdy hacker využívá vyrovnávací paměť a přemůže ji neočekávanými hodnotami. To obvykle způsobí nefunkčnost systému a vytvoří DoS útok. Odhaduje se, že jedna třetina škodlivých útoků je důsledkem přetečení vyrovnávací paměti. Bohužel těmto útokům se moc bránit nedá.
- IP, MAC, DHCP Spoofing - Spoofing útoky jsou útoky, při nichž se jedno zařízení pokouší představovat jako druhé falšováním dat. Existuje několik typů podvodných útoků. Například k falšování MAC adres dochází, když jeden počítač přijímá datové pakety založené na MAC adrese jiného počítače. [5]

Útok přes sociální inženýrství

Sociální inženýrství je přístupový útok, který se snaží manipulovat jednotlivce s prováděním akcí nebo sdělováním důvěrných informací.

Sociální inženýři často spoléhají na ochotu lidí spočívající v pomoci. Oni také kořistí na slabostech lidí. Například hacker může zavolat oprávněnému zaměstnanci s naléhavým problémem, který vyžaduje okamžitý přístup k síti. Hacker většinou spoléhá na chybu lidského faktoru a nedostatku informací daných lidí, kteří systém spravují. K dispozici je mnoho příkladů nástrojů sociálního inženýrství. Mezi konkrétní typy útoků v oblasti sociálního inženýrství patří:

- Pretexting - Toto je situace, kdy hacker volá jednotlivce a lže mu ve snaze získat přístup k privilegovaným datům. Příkladem je útočník, který předstírá, že potřebuje osobní nebo finanční údaje, aby potvrdil totožnost příjemce.
- Phishing - Phishing je situace, kdy strana se špatnými úmysly odešle podvodný e-mail maskovaný jako pocházející z legitimního důvěryhodného zdroje. Záměrem této zprávy je přimět příjemce k instalaci malwaru do zařízení nebo ke sdílení osobních nebo finančních informací.
- Spear phishing - Jedná se o cílený phishingový útok přizpůsobený konkrétní osobě nebo organizaci.
- Spam - Hackeři mohou pomocí spamového e-mailu přimět uživatele ke kliknutí na infikovaný odkaz nebo ke stažení infikovaného souboru. Většinou hackeři uspějí u lidí, kteří nejsou dostatečně proškoleni v rámci bezpečnosti dané firmy.
- Něco za něco- to je situace, kdy hacker požádá o osobní informace od strany výměnou za něco jako dárek zdarma nebo finanční odměnu. [5]

- Návnady - Toto je situace, kdy hacker opustí fyzické zařízení napadené malwarem, například jednotku USB Flash na veřejném místě, jako je podniková toaleta. Zaměstnanec najde zařízení a načte jej do svého počítače, čímž neúmyslně nainstaluje malware. V tomto případě hacker spoléhá na lidskou hloupost a zvědavost daného zaměstnance. [5]

Odepření služby – DOS

Útoky typu DoS (Denial of Service) jsou vysoce propagované síťové útoky. Útok DoS má za následek nějaké přerušení služby uživatelům, zařízením nebo aplikacím. Existují dva hlavní zdroje útoků DoS:

- Škodlivě formátované pakety
    - Jedná se o případ, kdy je paket se špatným formátem předán hostiteli nebo aplikaci a příjemce nemůže zvládnout neočekávaný stav.
- Ohromující množství dat
    - Je situace, kdy síť, hostitel nebo aplikace nedokáže zpracovat obrovské množství dat, což způsobí zhroucení systému nebo jeho extrémní zpomalení.
    - Příkladem je portál ticketportal.cz kdy prodeje vstupenek na mistrovství v hokeji v roce 2015 se webový portál zhroutil. Nebyl připraven na množství dotazů od zákazníků. Nešlo o hackerský útok ale jenom o velkou poptávku, která měla podobný vzorec chování. [5]

Typy útoků DoS

Přestože existuje mnoho metod útoku DoS, jsou z historických důvodů rozlišovány následující tři útoky.Tři současné útoky DoS jsou Ping of Death, Smurf Attack, Protokol TCP, SYN Flood Attack. [5]

DDoS útok

Distribuovaný útok DoS (DDoS). Útoky DDoS také zavádějí nové termíny, jako jsou botnet, handlerové systémy a zombie počítače. Příkladem může být útok DDoS:

Hacker vytváří síť infikovaných počítačů. Síť infikovaných hostitelů se nazývá botnet. Kompromitované počítače se nazývají zombie počítače a jsou ovládány systémy obsluhy. Počítače zombie nadále skenují a infikují více cílů a vytvářejí další zombie. Když je připraven, hacker dá pokyn manipulačním systémům, aby botnickou síť zombie provedly útok DDoS. Tento útok se dá normálně koupit na určitých dostupných webech. [5]

Sítový bezpečnostní profesionálové

Organizace zažívají ztrátu produktivity, když jsou jejich sítě pomalé nebo nereagují. Obchodní cíle a zisky jsou negativně ovlivněny ztrátou dat a poškozením dat. Z obchodního hlediska je tedy nutné minimalizovat dopady hackerů se špatnými úmysly.

Odborníci na síťovou bezpečnost jsou odpovědní za udržování zabezpečení dat v organizaci a zajištění bezpečnosti. Hackerství mělo nezamýšlený účinek, vytvořilo vysokou poptávku po profesionálech v oblasti zabezpečení sítě v důsledku rostoucího zneužití hackerů, sofistikovanosti hackerských nástrojů a kvůli vládní legislativě (Zákon o kybernetické bezpečnosti). Odborníci na bezpečnost musí dbát tyto zásady.

- Musí neustále zlepšovat své dovednosti, aby drželi krok s nejnovějšími hrozbami.
- Musí se účastnit školení a workshopů.
- Musí se přihlásit k odběru zpravodajství o hrozbách v reálném čase.
- Musí si prohlížet webové stránky zabezpečení každý den.
- Musí udržovat důvěrnost s organizacemi pro zabezpečení sítě. Tyto organizace mají často nejnovější informace o hrozbách a zranitelnostech. [5]

Obrázek 8 - Správce sítě [27]

3.3.4 **Obrana sítě**

Neustálá ostražitost a průběžné vzdělávání jsou vyžadovány k obraně sítě před útokem. Doporučené postupy pro zabezpečení sítě jsou následující:

- Písemná bezpečnostní politika společnosti.
- Vzdělání zaměstnanců o rizicích sociálního inženýrství a rozvíjení strategie ověřování totožnosti telefonicky, e-mailem nebo osobně.
- Řízení fyzického přístupu k systémům.
- Silná hesla a často je měnit.
- Šifrovat a chránit citlivá data.
- Implementace bezpečnostního hardwaru a softwaru jako jsou brány firewall, IPS, zařízení virtuální privátní sítě (VPN), antivirový software a filtrování obsahu.
- Zálohování a pravidelné testování zálohovaných dat
- Vypnout nepotřebné služby a porty
- Pravidelné aktualizace daných software
- Provést bezpečnostní audit a otestovat síť. [5]

Zmírňující malware

Malware včetně virů, červů a trojských koní může způsobit vážné problémy v sítích a koncových zařízeních. Správci sítě mají několik způsobů, jak tyto útoky zmírnit.

Primárním prostředkem ke zmírnění útoků virů a trojských koní je antivirový software. Antivirový software pomáhá zabránit hostům v nakažení a šíření škodlivého kódu. Vyčištění infikovaných počítačů vyžaduje mnohem více času než udržování aktuálního antivirového softwaru a definic antivirů na stejných počítačích.

Antivirové produkty mají možnosti automatizace aktualizací, takže nové definice virů a nové aktualizace softwaru lze stahovat automaticky nebo na vyžádání. Tato praxe je nejkritičtějším požadavkem pro udržení sítě bez virů a měla by být formalizována v zásadách zabezpečení sítě. [5]

Zmírňující průzkumné útoky

Průzkumné útoky jsou obvykle předchůdcem dalších útoků se záměrem získat neoprávněný přístup k síti nebo narušit síťové funkce. Odborník v oblasti zabezpečení sítě může zjistit, kdy probíhá průzkumný útok, a to přijímáním oznámení z předem nakonfigurovaných alarmů. Tyto alarmy se spouštějí, když jsou překročeny určité parametry, například počet požadavků ICMP za sekundu. [5]

Zmírnění přístupových útoků

Počet útoků na přístup se provádí pomocí jednoduchého hádání hesel nebo útoků slovníkovými silami proti heslům. Bránit se lze vytvořením a prosazení silné politiky ověřování, která zahrnuje:

- Používáním silných hesel
- Zákaz účtů po zadaném počtu neúspěšných přihlášení - Tento postup pomáhá zabránit neustálým pokusům o heslo.

Síť by také měla být navržena na základě zásady minimální důvěry. To znamená, že systémy by se neměly navzájem zbytečně používat. Kryptografie je kritickou součástí každé moderní zabezpečené sítě. Doporučuje se použít šifrování pro vzdálený přístup k síti. Příkladem šifrované vzdálené komunikace je VPN. Směrovací protokol by měl být také šifrován. Čím více je šifrován provoz, tím méně příležitostí mají hackeři k zachycení dat útoků typu *MITM*. [5]

3.3.5 **Kryptologie**

Kryptografické systémy

Existuje celá řada způsobů, jak zabezpečit síť. Sítě mohou být zabezpečeny prostřednictvím seznamů řízení přístupu, ověřování, autorizace a účetnictví (AAA) (ACL), funkcí brány firewall a implementací systému prevence narušení (IPS).

Kryptologie je věda o vytváření a porušování tajných kódů. Vývoj a použití kódů se nazývá kryptografie a zlomové kódy se nazývají kryptoanalýza. Kryptografie se po staletí používá k ochraně tajných dokumentů. V dnešní době se moderní kryptografické metody používají k zajištění bezpečné komunikace mnoha různými způsoby. [5]

Ověřování, integrita a důvěrnost

Aby byla zajištěna bezpečná komunikace přes veřejnou i soukromou infrastrukturu, je prvním cílem správce sítě zabezpečení síťové infrastruktury, včetně routerů, switchů, serverů a hostitelů. Toho lze dosáhnout například pomocí služeb AAA (Authentication Authorization and Accounting), ACL, firewallů. Zabezpečení komunikace má tři hlavní cíle:

- Ověřování - Zaručuje, že zpráva není padělek a že skutečně pochází, od koho uvádí.
- Integrita - zaručuje, že nikdo zprávu nezachytil a nezměnil; podobné funkci kontrolního součtu v rámci paketu.
- Důvěrnost - Zaručuje, že pokud je zpráva zachycena, nelze ji dešifrovat.[5]

Metody proprolomení kódu

V kryptoanalýze se používá několik metod:

- Brute-force method - Útočník zkouší všechny možné klíče s vědomím, že nakonec jeden z nich bude fungovat.
- Metoda Ciphertext - Útočník má šifrový text několika zašifrovaných zpráv, ale žádnou znalost základního textu v pozadí.
- Metoda Known-Plaintext - Útočník má přístup k šifrovému textu několika zpráv a ví něco o holém textu, z něhož je tento šifrový text považován.
- Metoda Chosen-Plaintext - Útočník si vybere, která data šifrovací zařízení šifruje a sleduje výstup šifrového textu.
- Metoda Chosen-Ciphertext - Útočník si může vybrat jiný šifrovaný text, který má být dešifrován a má přístup k dešifrovanému prostému textu.
- Metoda Meet-in-the-Middle - Útočník zná část prostého textu a odpovídajícího šifrového textu.

Cílem moderních kryptografů je mít dostatečně velký prostor pro klíče (hesla), aby bylo zapotřebí příliš mnoho času a peněz na provedení útoku hrubou silou.[5]

Dvě třídy šifrovacích algoritmů

Existují dva přístupy k zajištění bezpečnosti dat při použití šifrování. Prvním je ochrana algoritmu. Je-li zabezpečení šifrovacího systému založeno na utajení samotného algoritmu, musí být kód algoritmu chráněn. Pokud je algoritmus odhalen, musí každá zúčastněná strana tento algoritmus změnit. Druhým přístupem je ochrana klíčů. Díky moderní kryptografii jsou všechny algoritmy veřejné. Kryptografické klíče zajišťují utajení dat. Kryptografické klíče jsou sekvence bitů, které se vstupují do šifrovacího algoritmu společně s daty, která mají být šifrována. Existují dvě třídy šifrovacích algoritmů:

- Symetrické algoritmy - Tyto algoritmy používají ke šifrování a dešifrování dat stejný předem sdílený klíč, někdy nazývaný tajný klíč. Před sdíleným klíčem je odesílatel a příjemce znám před zahájením šifrované komunikace. Protože obě strany hlídají sdílené tajemství, použité šifrovací algoritmy mohou mít kratší délky klíče. Kratší délka klíče znamená rychlejší provedení.
- Asymetrické algoritmy - Tyto šifrovací algoritmy používají různé klíče k šifrování a dešifrování dat. Zabezpečené zprávy lze vyměňovat, aniž byste museli mít předem sdílený klíč. Protože žádná ze stran nemá sdílené tajemství, je nutné použít velmi dlouhé délky klíčů. Tyto algoritmy jsou náročné na zdroje a provádějí se pomaleji. [5]

3.3.6 **Zabezpečení LAN**

Otevřená a nesegmentovaná síť ,přímo zaznamenává kybernetické útočníky. Jakmile útočník najde a zneužije nejcitlivější přístupový bod, téměř vyhrál. Může snadno přistupovat k datům a smazat v celé síti.

Nesegmentované sítě nejsou ohroženy pouze vnějšími hrozbami. Bez oddělení sítě a omezení představují vysoké hrozby také vnitřní hrozby. Nezáleží na tom, zda se jedná o úmyslné chování nespokojeného zaměstnance nebo selhání lidského faktoru v podobě nežádoucí změny systému. Segmentace sítě by měla být součástí bezpečnostní strategie každé společnosti.

Kvůli segmentaci můžete svou síť rozdělit na několik menších sítí a vytvořit takzvané zóny důvěryhodnosti. To výrazně snižuje bezpečnostní útoky a předchází jim. Data poskytuji jenom tomu, kdo to nezbytně potřebuje. Virtuální sítě LAN nebo VLAN jsou nejčastěji spojovány se segmentací sítě. Jde o vytvoření zabezpečené virtuální sítě v rámci stávající sítě. VLANy mohou zabezpečit zařízení a data dvěma způsoby. Nejprve můžete zabránit zařízením v určitých sítích VLAN v komunikaci s ostatními zařízeními. Pro zabezpečení se využívají routery nebo switche.

Nejčastější metody segmentace patří firewall, ACL, VPN, systém prevence narušení (IPS) a systém detekce narušení (IDS). Mezi nejčastějšími úkoly na VLAN sítě je VLAN hopping. Základní myšlenkou všech hopping útoků na VLAN je, aby hostitelé útočící na VLAN získali přístup ke komunikaci na jiné VLAN, které by za normálních okolností neměly být přístupné. [11]

3.3.7 **Emailové a Webové bezpečnostní brány**

Za posledních 20 let se e-mail se zařadil mezi hlavní komunikační kanály internetu. Především firemní prostředí ho často využívá. Každý den je posláno několik miliard emailů napříč internetem. Zvyšujícím se počtem se úroveň bezpečnosti stává větší prioritou. Hromadné spamové útoky již nejsou jediným problémem. Dnes jsou spam a malware pouze součástí komplexního obrazu, který zahrnuje příchozí hrozby a odchozí rizika. Cisco vyvinula několik nástrojů kterým lze vzdorovat. Cisco Email Security Appliance (ESA) a Cisco Web Security Appliance (WSA).

Cisco WSA je technologie zmírňování webových hrozeb, která pomáhá organizacím řešit rostoucí výzvy zabezpečení a kontroly webového provozu. Poskytuje úplnou kontrolu nad přístupem uživatelů k internetu. Zahrnujeme sem chat, zasílání zpráv,

video a audio. Mohou být povoleny, omezeny časovými a šířkami pásma nebo blokovány podle požadavků organizace. Cisco ESA bojuje proti spamu, virům a kombinovaným hrozbám Vynucuje dodržování předpisů a chrání pověst a majetek firmy, která si tuto službu platí. Snižuje prostoje a zjednodušuje správu podnikových emailových systémů. [5]

3.3.8 **Firewall**

Firewall je určen pro ochranu proti neoprávněným vnějším útočníkům, kteří se snaží proniknout do interní sítě a pro blokaci útoků vedených do této sítě. Dnes existuje mnoho typů firewallů jako je filtrování paketů, stavové, nextgen firewall, aplikační brána, proxy, překlad adres, hostitelské, transparentní a hybridní brány firewall. Na světě je mnoho typů firewallů, ale zároveň mají společné vlastnosti kterými jsou:

- Firewally jsou odolné vůči útokům.
- Firewally jsou jediným tranzitním bodem mezi sítěmi, protože veškerý provoz protéká bránou firewall.
- Brány firewall vynucují zásady kontroly přístupu.

Brány firewall v síti mají několik výhod:

- Zabraňují vystavení citlivých hostitelů, zdrojů a aplikací nedůvěryhodným uživatelům.
- Dezinfikují tok protokolu, který zabraňuje zneužití chyb protokolu.
- Blokují škodlivá data ze serverů a klientů.
- Snižují složitost správy zabezpečení přesunutím většiny řízení přístupu do sítě na několik bran firewall v síti.

Firewally také představují určitá omezení:

- Chybně nakonfigurovaný firewall může mít pro síť závažné důsledky,
- Data z mnoha aplikací nelze bezpečně předávat přes brány firewall.
- Výkon sítě se může zpomalit.
- Neautorizovaný provoz sítě lze tunelem nebo skrýt jako legitimní provoz prostřednictvím brány firewall. [5]

3.3.8.1 **Stavový firewall**

Stavový firewall jsou nejvšestrannější a nejběžnější používané technologie bránami. Stavový firewall poskytují stavové filtrování paketů pomocí informací o připojení udržovaných v tabulce stavu. Stavové filtrování je architektura brány firewall, která je klasifikována na síťové vrstvě. Analyzuje také provoz na vrstvě 4 a vrstvě 5 OSI modelu.

Výhody

- Jsou často používány jako primární prostředek obrany filtrováním nežádoucího, zbytečného nebo nežádoucího provozu.
- Poskytují přísnější kontrolu nad zabezpečením.
- Zlepšují výkon filtrů paketů nebo serverů proxy.
- Brání se před útoky typu spoofing a DoS

Nevýhody

- Nemohou zabránit útokům aplikační vrstvy
- Ne všechny protokoly jsou stavové, například UDP a ICMP
- Nepodporují ověřování uživatelů. [5]

3.3.9 **Next-Generation Firewalls**

Účelem každého podnikového firewallu je ochrana sítě před vetřelci a ochrana systémů a dat, ale ne všechny firewally jsou rovnocenné. Všichni sdílejí stejný cíl, ale specifické rysy, schopnosti a úrovně sofistikovanosti se mohou velmi lišit. Dvě nejzákladnější kategorie firewallů na podnikové úrovni jsou tradiční a nová generace. Brány firewall nové generace (Next-Generation Firewalls - NGFW) jsou vyspělejší a nabízejí nejobsáhlejší ochranu počítačových sítí.Ne všechny hrozby přicházející z internetu vyřeší NGFW. Například volumetrický útok spočívající v zahlcení linky NGFW nevyřeší. Je potřeba zvolit AntiDDoS řešení. [12]

3.3.10 **AAA protokol**

Síť musí být navržena tak, aby určovala, kdo se k ní smí připojit, kdy se k ní smí připojit a co může dělat. Tyto konstrukční specifikace jsou určeny v zásadách zabezpečení sítě. Zásada určuje, jak správci sítě, firemní uživatelé, vzdálení uživatelé, obchodní partneři a klienti přistupují k síťovým prostředkům. Zásady zabezpečení sítě mohou také nařídit implementaci účetního systému, který sleduje, kdo se přihlásil a kdy a co dělal při přihlášení. [2][4]

Ověření bez AAA

Síťoví hackeři mohou potenciálně získat přístup k citlivým síťovým zařízením a službám. Řízení přístupu omezuje, kdo nebo co může použít konkrétní zdroje. Omezuje také služby nebo možnosti, které jsou k dispozici po udělení přístupu. Na zařízení Cisco lze provádět mnoho typů autentizace a každá metoda nabízí různé úrovně zabezpečení.

Nejjednodušší metoda autentizace vzdáleného přístupu je konfigurace kombinace přihlášení a hesla na konzole, VTY linkách a aux portech0. Tuto metodu je nejjednodušší implementovat, ale je také nejslabší a nejméně bezpečná. Tato metoda neposkytuje žádnou odpovědnost. Kdokoli s heslem může získat vstup do zařízení a změnit konfiguraci.

Metoda lokální databáze má některá omezení. Uživatelské účty musí být nakonfigurovány na každém zařízení. Ve velkém podnikovém prostředí, které má více routerů a switchů pro správu, může implementace a změna lokálních databází na každém zařízení trvat nějakou dobu. Konfigurace místní databáze navíc neposkytuje žádnou záložní metodu autentizace. [2][4]

AAA Components

Služby zabezpečení sítě AAA poskytují primární rámec pro nastavení řízení přístupu na síťovém zařízení. AAA je způsob, jak kontrolovat, kdo má povolen přístup k síti. Síťové a administrativní zabezpečení AAA v prostředí Cisco má tři funkční komponenty:

- Ověřování - Uživatelé a administrátoři musí prokázat, že jsou tím, kdo tvrdí, že jsou.
- Autorizace - Po autentizaci uživatele autorizační služby určují, ke kterým prostředkům má uživatel přístup a které operace může uživatel provádět.
- Účetnictví a auditování - Účetnictví zaznamenává, co uživatel dělá, včetně toho, co je přístupné, dále množství času, ke kterému je přístup ke zdroji, a všechny provedené změny. [2][4]

Režim ověření

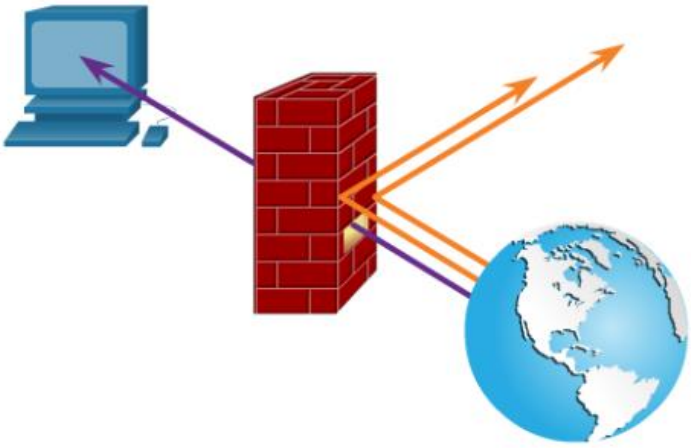
Ověřování AAA lze použít k ověření uživatelů pro administrativní přístup nebo k ověření uživatelů pro vzdálený přístup k síti. Cisco poskytuje dva běžné způsoby implementace služeb AAA:

- Místní ověřování AAA -Místní AAA používá pro autentizaci lokální databázi. Tato metoda je někdy označována jako samostatná autentizace.
- Serverová autentizace AAA - S metodou založenou na serveru routeru přistupuje k centrálnímu serveru AAA. Centrální server AAA obsahuje uživatelská jména a heslo pro všechny uživatelé. [2][4]

3.3.11 **Politika ACL**

Jednou z nejdůležitějších stránek je zabezpečení. Bezpečnostní politika je formální prohlášení o pravidlech, podle kterých se musí lidé, kterým je poskytován přístup k technologickým a informačním aktivům organizace, řídit. Koncepce, vývoj a aplikace bezpečnostní politiky jsou rozhodující pro udržení bezpečnosti firmy. Je úkolem profesionálů v oblasti zabezpečení sítí, aby se ve všech aspektech obchodních operací v rámci organizace zabývali bezpečnostní politikou. Seznam ACL poskytují zabezpečení sítě. V praxi se jedná o seznam podmínek různých služeb (portů, protokolů) které filtrují packety. Udělují jim různé podmínky, které určí sám správce sítě. Mohou být často užitečné, ale občas nastane situace, že administrátor zabrání komunikaci mezi zařízeními a omylem vypne důležitou službu pro fungování firemní sítě. Příkladem je zablokování emailu.

Správci sítí používají brány firewall (Obrázek 9) k ochraně sítí před neoprávněným použitím. Brány firewall jsou hardwarová nebo softwarová řešení (ACL), která vynucují zásady zabezpečení sítě. Na routeru Cisco lze nakonfigurovat jednoduchý firewall, který poskytuje základní funkce filtrování provozu pomocí přístupových seznamů ACL (access list). [2][5]



Obrázek 9 - Schéma firewallu [5]

Cisco Access Control Lists

ACL (Access Control Lists) je seznam oprávnění v CISCO IOS (Obrázek 10). Patří mezi nejčastěji používané funkce softwaru Cisco IOS. ACL je obecný pojem který využívají i jiné operační systémy např. Windows (Obrázek 11). Pokud například podniková politika nepovoluje přenos videa ve firemní síti, je možné nakonfigurovat a použít seznamy ACL, které blokují přenos videa. To by výrazně snížilo zatížení sítě

a zvýšilo výkon sítě. Takový příkladů může být mnoho pro účely toho, aby zaměstnanci netrávili svůj pracovní čas na internetu sledováním videí. Seznam ACL slouží především k zabezpečení počítačové sítě. Seznam určuje, kdo (zařízení) nebo co (zařízení/služba) má povolení přistupovat k objektu a jaké operace s ním může provádět. Ve výchozím nastavení router nemá nakonfigurované ACL. Toto je velice nebezpečném, protože router ve výchozím nastavení nefiltruje žádný provoz. Tím pádem je snadnou obětí pro kybernetický útok a únik firemních dat. [5]

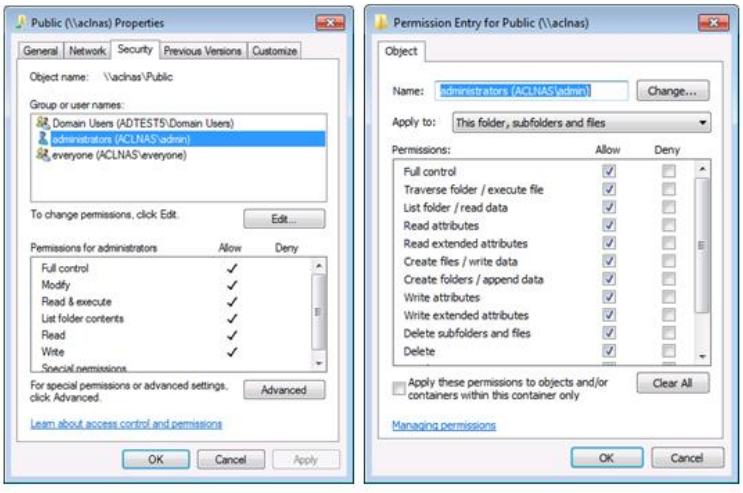
Při porovnávání paket podle ACL platí vždy tři důležitá pravidla

- paket je vždy porovnává s každým řádkem ACL v sekvenčním pořadí. Vždy se začíná od prvního řádku ACL, pak se přejde k řádku 2 a dále.
- Porovnává s řádky AC pouze do té doby než není nalezena shoda. Jakmile je nalezena shoda, packet projde a už k porovnávání nedochází.
- Na konci každého příkazu se nachází příkaz „deny“ , který má za úkol zahazovat pakety zda dané podmínce nevyhoví.

Obecně platí zásada, že ACL seznamy se nijak neprojeví, dokud je správce sítě nebo daného zařízení neaplikuje. Mohou se dělit na aktivní a neaktivní. ACL se dějí na dva typy. Příchozí ACL a odchozí ACL. [2][5]

```
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq telnet
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq ftp
access-list 101 permit tcp 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255 eq http
access-list 101 deny ip 192.168.212.0 0.0.0.255 10.0.0.0 0.255.255.255
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 administratively-prohibited
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 echo-reply
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 packet-too-big
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 time-exceeded
access-list 101 permit icmp any 10.0.0.0 0.255.255.255 unreachable
access-list 101 permit icmp 172.16.20.0 0.0.255.255
access-list 101 deny icmp any any
access-list 101 permit ip 202.33.42.0 0.0.0.255 any
access-list 101 permit ip 202.33.73.0 0.0.0.255 any
access-list 101 permit ip 202.33.48.0 0.0.0.255 any
access-list 101 permit ip 202.33.75.0 0.0.0.255 any
access-list 101 deny ip 202.33.0.0 0.0.255.255 any
access-list 101 deny tcp 210.120.122.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.183.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.114.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.175.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.136.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp 210.120.177.0 0.0.0.255 10.2.2.0 0.255.255.255 eq www
access-list 101 permit tcp any 10.2.2.0 0.255.255.255 eq www
access-list 101 deny tcp any any eq www
access-list 101 permit tcp any any
access-list 101 deny ip 195.10.45.0 0.0.0.255 any
access-list 101 permit ip any any
(access-list 101 deny all) (implicit)
```

Obrázek 10 - Cisco Access Control Lists [30]



Obrázek 11 - Windows Access Control Lists [31]

3.4 Charakteristika počítačové sítě

Tato kapitola se věnuje problematice počítačových sítí. Text charakterizuje základní znalosti o sítích. Sítě a jejich slovo se za posledních dvacet let exponenciálně rozrostly. Přizpůsobují se každodenním požadavkům lidstva. V dnešním světě jsme pomocí sítí spojeni jako nikdy předtím. Lidé s nápady mohou okamžitě komunikovat s ostatními, aby se tyto nápady staly realitou. Zpravodajské události jsou známé po celém světě během několika sekund. Jednotlivci se mohou spojovat a hrát videohry s přáteli mimo kontinenty. Svět se díky sítím zmenšil oproti tomu, jak tomu bylo před pouhými 200 lety. Sítě změnily způsob, jakým se učíme. Přístup k vysoce kvalitnímu vyučování již není omezen. [1][4]

3.4.1 Síť

Termín počítačová síť se týká zejména spojení dvou nebo více počítačů, aby mohly komunikovat mezi sebou a sdílet své zdroje. Nezáleží na tom, zda se jedná o prostředek hardware nebo software.[4]

Koncová zařízení

Síťová zařízení, se kterými jsou lidé nejvíce obeznámeni, se nazývají koncová zařízení. Koncové zařízení je buď zdroj, nebo cíl zprávy přenášené sítí. Nejznámějším příkladem koncového zařízení v posledních letech je počítač, chytrý telefon (smartphone), tablet, tiskárna. [4]

Přenosová zařízení v síti

Zprostředkovatelská zařízení která jsou například router nebo switch, připojují jednotlivá koncová zařízení k síti a mohou propojit více jednotlivých sítí za účelem vytvoření mezinárodní sítě. Tato zprostředkující zařízení zajišťují konektivitu a tok dat přes síť. [4]

Síťová média

Komunikace přes síť probíhá po médiu. Médium poskytuje přenos, přes který data putují od zdroje do cíle. Počítačové sítě používají tři typy médií k propojení zařízení, která zajištují přenos dat.[4]

- Sítový kabel - data jsou přenášena pomocí elektrických impulsů , které fungují na binárním spojení
- Optický kabel - data jsou přenášena pomocí světla
- Bezdrátový přenos - data jsou přenášena pomocí vlnových délek z elektromagnetického spektra

Všechny tyto tři typy přenosových medií mají různé funkce a výhody či nevýhody. Ne všechna síťová média mají stejné vlastnosti, ani nejsou vhodná pro stejný účel. [4]

Typy počítačových sítí

- Local Area Network (LAN) - Síťová infrastruktura, která poskytuje přístup k uživatelům a koncovým zařízením v malé oblasti. Krásným příkladem je podniková infrastruktura.
- Wide Area Network (WAN) - Síťová infrastruktura, která poskytuje přístup k dalším sítím v široké oblasti
- Metropolitní oblastní síť (MAN) - síťová infrastruktura, která zahrnuje fyzickou oblast větší než LAN, ale menší jak WAN
- Wireless LAN (WLAN) - Bezdrátově propojuje uživatele a koncové body [4]

3.4.2 Referenční model ISO/OSI

K hlavním pilířům ISO modelu patří to, že umožnují datové přenosy mezi hostiteli s odlišnými operačními systémy jako jsou například Unix a Windows. Tento model je logický nikoliv fyzický. V zásadě se jedná o takovou kuchařku pro vývojáře, jak mají implementovat aplikace, které budou fungovat v počítačové síti. Poskytuje taky sadu síťových standardů a schémat propojení sítí. [1]

Referenční model ISO/OSI obsahuje sedm vrstev , které se rozdělují do dvou skupin. Tři horní vrstvy charakterizují, jakým způsobem komunikují aplikace na koncových zařízeních s uživatelem. Zbývající čtyři vrstvy charakterizují datový přenos mezi koncovými body. Každá vrstva má svoje charakteristické úkoly a komunikuje jenom se sousedními. V praxi to znamená, že probíhá stabilní a efektivní komunikace. Skládá se z následujících vrstev (Obrázek 12)

- Aplikační vrstva - Poskytuje uživatelské rozhraní
- Prezentační vrstva - Prezentuje data a zajišťuje zpracování typu šifrování
- Relační vrstva - Udržuje oddělená data různých aplikací
- Transportní vrstva - Poskytuje spolehlivé nebo nespolehlivé doručení. Zajišťuje korekci chyb před opakovaným přenosem
- Sítová vrstva - Zajišťuje logické adresování
- Linková vrstva - Poskytuje přístup k médiu pomocí MAC adresy [1]

3.4.3 Sítové protokoly

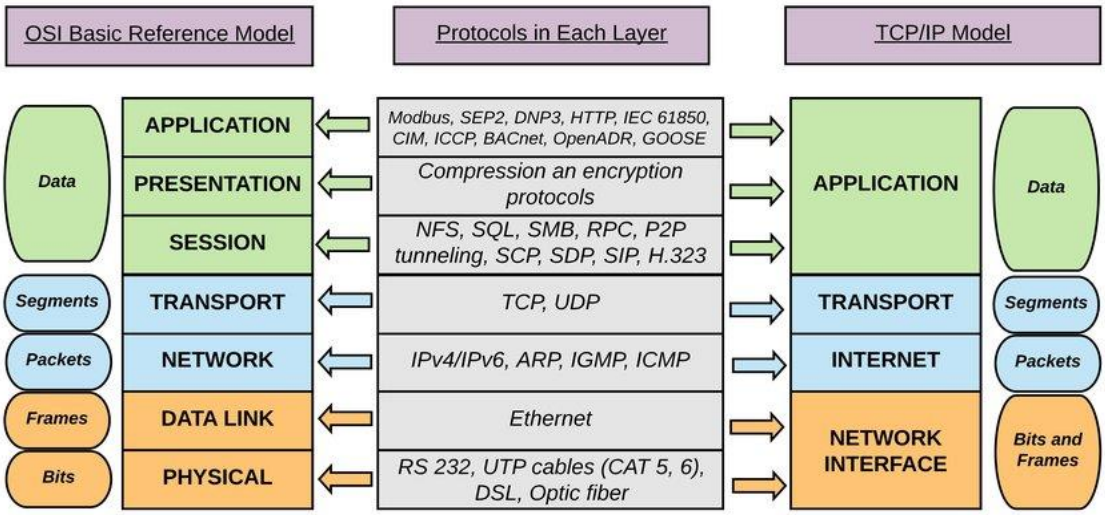
Aby zařízení mohla úspěšně komunikovat, musí sada síťových protokolů charakterizovat přesné požadavky a interakce. Síťové protokoly definují společný formát a sadu pravidel pro výměnu zpráv mezi zařízeními.

- HTTP - je aplikační protokol, který řídí způsob interakce webového serveru a webového klienta..
- TCP - je přenosový protokol, který řídí jednotlivé konverzace.
- IP - odpovídá za převzetí formátovaných segmentů z TCP, jejich zapouzdření do paketů, přiřazení příslušných adres a jejich doručení cílovému hostiteli.
- Ethernet - je síťový přístupový protokol, který charakterizuje dvě primární funkce-komunikaci přes datové spojení a fyzický přenos dat na síťovém médiu. [4]

3.4.4 Síťový model TCP/IP

Protokol TCP/IP byl navržen během studené války v USA. Cílem bylo zajistit bezpečnou komunikaci během tragédie, která mohla nastat. Především bylo nutné zjistit, zda je síť dobře navržena na modelu TCP/IP a zda může být bezpečná, spolehlivá a odolná. Protokol lze charakterizovat jako zlehčenou verzi síťového model OSI, která má místo sedmi vrstev čtyři. Oba dva modely fungují na stejném principu, kterým je zajištění komunikace mezi zařízeními. Síťový model TCP/IP se skládá z následujících vrstev (Obrázek 12):

- Aplikační vrstva – Definuje protokoly pro komunikaci mezi aplikacemi.
- Transportní vrstva – Zajišťuje bezchybné doručení dat, pracuje s pakety.
- Síťová vrstva – Zahrnuje protokoly, které slouží k přenosu paketů v celé síti. Zodpovídá za adresaci hostitelů, jenž uděluje IP adresu a ošetřuje směrování paketů v celé síti.
- Vrstva síťového rozhraní –Dohlíží na hardwarové adresování a definuje protokoly fyzické vrstvy. Velká obliba tohoto modelu právě tkví v tom, že nezahrnuje žádné pevné specifikace v této vrstvě. Právě díky tomu může fungovat v každé existující či budoucí síti.[1]



Obrázek 12 - Rozdíl mezi modelem ISO/OSI a TCP/IP [14]

3.4.4.1 **Protokoly v aplikační vrstvě**

V aplikační vrstvě se nachází mnoho protokolů. Charakteristika bude zaměřena na ty nejčastější.

- Telnet – Uživateli vzdáleného klientského zařízení je umožněno pomocí rozhraní příkazového řádku přístup k jinému počítači. Nevýhoda tohoto protokolu je, že neobsahuje žádnou šifrovací metodu a snadný cíl pro útočníka.
- SSH – Protokol Secure Shell navazuje bezpečnou komunikaci podobnou protokolu Telnet. Všechny operace během komunikace jsou šifrované.
- FTP – Umožnují přenášet soubory a tyto úkony lze provést mezi dvěma počítači
- HTTP - Je internetový protokol určený pro komunikaci s WWW servery.
- HTTPS - protokol umožňující zabezpečenou komunikaci v počítačové síti.
- DNS - hierarchický, decentralizovaný systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace
- DHCP - Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, bránu a DNS. [1]

3.4.4.2 **Protokoly v transportní vrstvě**

V této vrstvé fungují dva protokoly, které se jmenují TCP a UDP. Hlavním úkolem těchto dvou protokolů je odstínit aplikace z aplikační vrstvy do spodních vrstev. [1]

TCP (Transmission Control Protocol)

Přijímá velké bloky dat od aplikací a dělí je na jednotlivé segmenty. Tento protokol je plně duplexní, spojovaný, spolehlivý a přesný. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí, proto se označuje jako spolehlivý. [1]

UDP (User Datagram Protocol)

Je zjednodušenou verzí protokolu TCP, proto se občas označuje tenký nebo nespolehlivý protokol. O protokolu UDP říkáme, že neposkytuje záruky na datové přenosy, které přenáší mezi počítači v síti. Je označován jako nespolehlivý, nemá záruku správného doručení dat. [1]

3.4.4.3 **Protokoly v síťové vrstvě**

Nejvíce známým protokolem v této vrstvě je IP protokol. IP protokol byl navržen jako protokol s nízkou režií. Poskytuje pouze funkce, které jsou nezbytné pro doručování paketu ze zdroje do cíle přes propojený systém sítí. Protokol nebyl navržen ke sledování a správě toku paketů. Tyto funkce, jsou-li vyžadovány, jsou prováděny jinými protokoly v jiných vrstvách. [4]

3.4.5 IP Adresace a podsítě

Navrhování, implementace a správa efektivního plánu adresování IP zajišťuje, že sítě mohou fungovat efektivně. To platí zejména s rostoucím počtem připojení. Důležitou součástí plánování je schéma adresování IP.

V původní adrese IPv4 jsou dvě úrovně hierarchie: síť a hostitel. Tyto dvě úrovně adresování umožňují základní seskupení sítí, které usnadňují směrování paketů do cílové sítě. Router předává pakety na základě síťové části adresy IP. Když je síť lokalizována, hostitelská část adresy umožňuje identifikaci cílového zařízení.

Podsítě (subnetting) snižují celkový síťový provoz a zvyšují výkon sítě. umožňují také správci implementovat zásady zabezpečení, jako jsou podsítě, které mohou nebo nemohou spolu komunikovat.

Existují různé způsoby použití podsítí, které pomáhají spravovat síťová zařízení. Správci sítě mohou seskupovat zařízení a služby do podsítí, které jsou určeny. Například podlahy v budově, typ zařízení.

Aby mohli adresy podsítí komunikovat, musí každý počítač v síti vědět, která část hostitelské adresy se budou používat pro adresy podsítě. Tato podmínka se vyřeší přidělením masky podsítě (subnet mask). Maska je 32 bitová a se skládá z nul a jedniček. IP adresy se dělí na pět částí tříd A,B,C,D,E (Obrázek 13). [1]

Třídy IP adres

Třída	začátek (bin)	1. bajt	standardní maska	bitů sítě	bitů stanice	sítí	stanic v každé síti
A	0	0–127	255.0.0.0	8	24	$2^7 = 128$	$2^{24}-2 = 16\ 777\ 214$
B	10	128–191	255.255.0.0	16	16	$2^{14} = 16384$	$2^{16}-2 = 65\ 534$
C	110	192–223	255.255.255.0	24	8	$2^{21} = 2\ 097\ 152$	$2^8-2 = 254$
D	1110	224–239	*multicast*				
E	1111	240–255	*vyhrazeno jako rezerva*				

Rozsahy IP adres a masky sítě

Třída	1. bajt	minimum	maximum	maska podsítě
A	0–127	0.0.0.0	127.255.255.255	255.0.0.0
B	128–191	128.0.0.0	191.255.255.255	255.255.0.0
C	192–223	192.0.0.0	223.255.255.255	255.255.255.0
D	224–239	224.0.0.0	239.255.255.255	255.255.255.255
E	240–255	240.0.0.0	255.255.255.255	—

Obrázek 13 - Třídy IP adres [15]

3.4.6 **LAN technologie**

Local area network (LAN) je termín používaný pro lokální sítě. Jedná se o stanice propojené do jednoho rovnoměrně adresovaného segmentu.V místní síti mají všechny počítače IP adresu ze stejného rozsahu hodnot. Taková síť může mít různé topologie, obvykle pomocí switchů a bridgů. Síť domácího počítače je příkladem LAN, se kterou většina uživatelů normálně pracuje. Základním aktivním prvkem v tomto případě je router. Má kabel pro připojení k internetu a lze jej připojit přímo k terminálu.

Router poté provádí směrování z adres sítě (NAT) při směrování z místní sítě, což znamená, že veškerá komunikace s vnějším světem probíhá pod veřejnou adresou. Routery a adresy v místní síti nejsou z venku viditelné. Tento přístup se používá ze dvou důvodů. Vyžaduje méně globálně jedinečných IP adres a zajišťuje bezpečnost počítačů v místní síti proti přímým útokům zvenčí. [19]

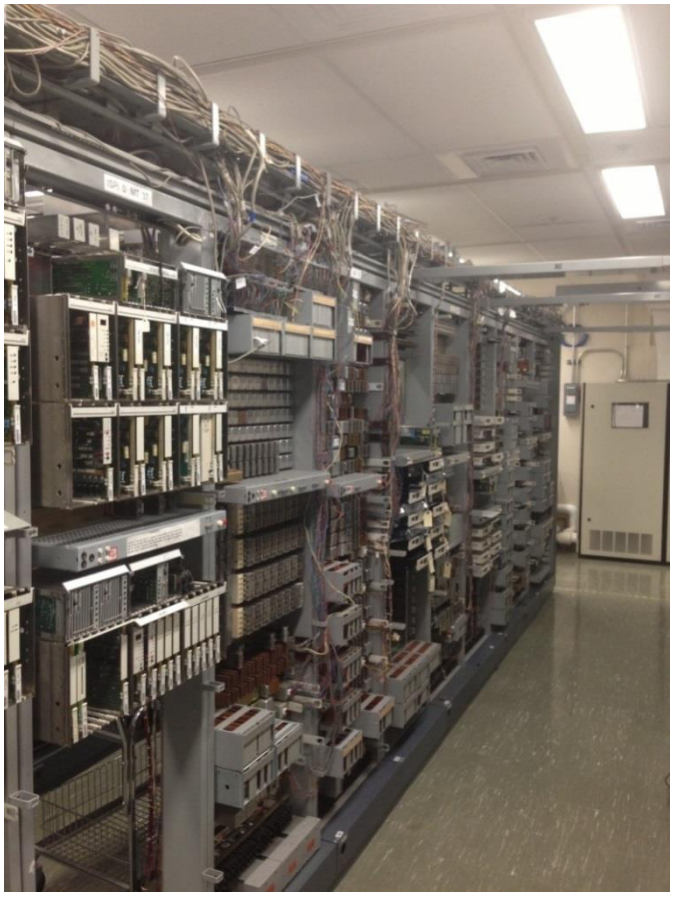
3.4.7 **Switch**

Moderní sítě se každým dnem vyvíjejí, aby udržovaly krok s měnícím se způsobem, jakým organizace provádějí své každodenní činnosti. Uživatelé nyní očekávají okamžitý přístup k firemním prostředkům odkudkoli a kdykoli. Tyto zdroje zahrnují nejen tradiční data, ale také video a hlas. Roste také potřeba technologií pro spolupráci. Tyto technologie umožňují sdílení zdrojů v reálném čase mezi více vzdálenými osobami.

Různá zařízení musí hladce spolupracovat, aby zajistily rychlé, bezpečné a spolehlivé spojení mezi hostiteli. Switch LAN poskytují připojení koncovým uživatelům do podnikové sítě a jsou primárně odpovědné za řízení informací v prostředí LAN. Switche usnadňují pohyb informací mezi sítěmi LAN. Všechny pokročilé služby závisí na dostupnosti robustnosti switchů a routerů v dané infrastruktuře. Tato infrastruktura musí být pečlivě navržena, zabezpečena, rozmístěna a spravována, aby poskytovala stabilní účinnost a funkčnost.

Nové generace sítových zařízení musí podporovat nejen současné požadavky, ale musí být také schopny komunikace se staršími platformami.

Na obrázku (Obrázek 14) je možné vidět starší technologie, které byly používané v minulosti na rozdíl od obrázku (Obrázek 15), kde je prezentovaná novější forma sítových prvků, které pomáhají poskytovat přístup k síti kdykoli, kdekoli a na jakémkoli zařízení. [4]



Obrázek 14 - Telefonní rozbočovač [4]

Obrázek 15 - Cisco Catalyst 2960 [4]

Ve firemních sítích se používají různé typy switchů. Nejčastější obchodní úvahy při výběru switche jsou:

- Cena - bude záviset na počtu a rychlosti rozhraní, podporovaných funkcích a schopnosti rozšíření.
- Hustota portů - Síťové switche musí podporovat příslušný počet zařízení v síti.
- Spolehlivost - Switch by měl poskytovat nepřetržitý přístup k síti.
- Rychlost portu - Rychlost síťového připojení se primárně týká koncových uživatelů.
- Vyrovnávací paměti rámců - Možnost přepínání rámců pro ukládání rámců je důležitá v síti, kde mohou být přetížené porty k serverům nebo jiným oblastem sítě.
- Škálovatelnost - Počet uživatelů v síti obvykle roste v průběhu času. Switch by proto měl poskytnout příležitost pro růst.[4]

Při kupování switchů si musí správce sítě uvědomit, jaký typ bude potřebovat, jelikož, existují switche s pevnou konfigurací nebo modulární. Dalším faktorem je tloušťka switche, která je vyjádřena v počtu regálových jednotek. To je důležité pro switche, které jsou namontovány v stojanu. Je nutné investici zvážit pro vzdálenou budoucnost. [4]

Switche s pevnou konfigurací

Switche s pevnou konfigurací nepodporují funkce nebo možnosti nad rámec těch, které byly původně navrhnuty pro daný switch. Každý takový model předem udává jaké funkce a možnosti poskytuje. Například 12 bitový gigabitový switch nemůže podporovat další gigabitový porty. Typicky existují různé možnosti konfigurace, které se liší v tom, kolik a jaké typy portů jsou součástí konfigurace. [4]

Modulární konfigurační switche

Modulární konfigurační switche nabízejí větší rozmanitost v jejich konfiguraci, které umožňují instalaci různých počtů modulárních linkových karet. Linkové karty skutečně obsahují porty. Čárová karta zapadá do šasi spínače tak, jak se rozšiřující karty vejdou do počítače. Existuje mnoho různých velikostí podvozku. Modulární switch s jedinou 24-portovou linkovou kartou by mohl mít nainstalovanou další 24-portovou linkovou kartu, aby celkový počet portů byl až 48. [4]

Vlastnosti switche

Switch udržuje LAN tabulku, kterou používá k určení způsobu předávání provozu směrování. Jedinou inteligencí switche LAN je jeho schopnost použít svou tabulku k předávání provozu na základě vstupního portu a cílové adresy zprávy. U switche LAN existuje pouze jedna hlavní přepínací tabulka, která sděluje přísné spojení mezi adresami a porty. Switche LAN mají zvláštní vlastnosti, díky nimž jsou účinné při přetížení sítě.

Nejprve umožňují segmentaci LAN do samostatných kolizních domén. Poskytují duplexní komunikaci mezi zařízeními. Plně duplexní připojení může přenášet vysílané i přijímané signály současně. Plně duplexní připojení výrazně zvýšila výkon sítě LAN a je vyžadována pro rychlosti Ethernet 1 Gb / s a vyšší. Následuje několik důležitých charakteristik switchů, které přispívají ke zmírnění přetížení sítě: [4]

- Vysoká hustota portů - Switche mají vysokou hustotu portů. Velké podnikové switche mohou podporovat mnoho stovek portů.
- Velké vyrovnávací paměti snímků - Možnost uložit více přijatých rámců před jejich spuštěním je užitečné, zejména pokud mohou existovat přetížené porty serverů.
- Rychlost portu - V závislosti na nákladech na switch může být možné podporovat kombinaci rychlostí porty 100 Mb / s a 1 nebo 10 Gb.
- Rychlé interní přepínání - Možnost rychlého interního přeposílání umožňuje vysoký výkon.
- Nízké náklady na port - Switche poskytují vysokou hustotu portů při nižších nákladech.[4]

3.4.7.1 **Konfigurace**

Switche se používají k propojení více zařízení ve stejné síti, zejména k propojení koncových zařízení jako je počítač, tiskárna, notebook či router. Ve správně navržené síti jsou switche LAN zodpovědné za směrování a řízení toku dat.

Switche Cisco se konfigurují samy a nejsou nutné žádné další konfigurace, aby fungovaly ihned po vybalení (nové zařízení od výrobce). Z hlediska bezpečnosti se nezapojuje nové zařízení, které není pečlivě kontrolováno ohledně nastavené konfigurace. Jeden switch může pak napáchat mnoho škody v celé počítačové infrastruktuře. Switche Cisco obsahují Cisco IOS.

Switche Cisco lze spravovat lokálně i vzdáleně. Pro vzdálenou správu switche je nutné mít nakonfigurovanou IP adresu a výchozí bránu na daném switchi. Lokální správa se používá na základě konzolového kabelu, který je zapojený ze switche do počítače.

Switche fungují na přístupové vrstvě, kde se zařízení klientských sítí připojují přímo k síti a oddělení IT požadují pro uživatele nekomplikovaný přístup k síti. Je to jedna z nejzranitelnějších oblastí sítě. Switche musí být nakonfigurovány tak, aby odolávaly útokům všech typů, chrání uživatelská data a umožňují vysokorychlostní připojení. Zabezpečení portů je jednou z bezpečnostních funkcí, které poskytují switche spravované společností Cisco.

Secure Shell (SSH) je protokol, který poskytuje bezpečné (šifrované) připojení správy ke vzdálenému zařízení. SSH by měl nahradit Telnet za připojení pro správu. Telnet

je starší protokol, který používá bohužel nezabezpečený prostý přenos autentizace přihlašování (uživatelské jméno a heslo) a dat přenášených mezi komunikujícími zařízeními. Tato data se dají bohužel odposlechnout a získat tak přihlašovací údaje. SSH poskytuje zabezpečení pro vzdálená připojení poskytováním silného šifrování při autentizaci zařízení a také pro přenášená data mezi komunikujícími zařízeními. SSH je přiřazen k portu TCP 22. Telnet je přiřazen k portu TCP 23. Pro povolení SSH na switchi od společnosti Cisco musí switch používat verzi softwaru IOS včetně kryptografických funkcí a schopností. Pro zjištění této funkce existuje příkaz „show version“, který zobrazí jaký IOS na switchi funguje. [4]

3.4.7.2 **Zabezpečení switchů**

Obecná obrana počítačové sítě proti útoku vyžaduje ostražitost a vzdělání. Doporučené faktory pro zabezpečení sítě jsou:

- Vypracování písemné bezpečnostní politiky
- Vypnutí nevyužívaných služeb a portů
- Silná hesla
- Zamezení fyzického přístupu k zařízením
- Nepoužívání nezabezpečené webové stránky HTTP
- Zálohování
- Vzdělávání zaměstnanců v oboru kybernetické bezpečnosti
- Šifrování a ochrana dat
- Firewall
- Pravidelné aktualizace zařízení

Tyto body jsou jenom jedny z mnoha opatření, které mohou zabránit útoku. Firmy musí být neustále připravené na útoky a musí se proti nim neustále bránit. Hrozby se každým dnem vyvíjejí a je nutné na tento fakt brát ohledy. Pomocí různých nástrojů a funkcí je možné těmto útokům předejít. [4]

Zakázat nepoužívané porty

Nejjednodušší metoda, kterou většina správní sítě používá k zabezpečení sítě před neoprávněným přístupem, je deaktivace všech nepoužitých portů na switchi. U Cisco zařízení slouží k vypnutí daného pornu příkaz „shutdown“. Proces povolení a deaktivace portů může být časově náročný, ale zvyšuje bezpečnost v síti a stojí za námahu. [4]

DHCP útoky (DHCP spoofing)

DHCP je protokol, který automaticky přidělí hostiteli platnou IP adresu z DHCP serveru. Proti přepínané síti lze provádět dva typy útoků DHCP. Útoky hladověním DHCP a spoofing DHCP.

Při útocích hladověním DHCP zaplaví útočník server DHCP požadavky DHCP, aby využil všechny dostupné adresy IP, které může server DHCP vydat. Po vydání těchto adres IP server nemůže vydávat žádné další adresy a tato situace způsobí útok typu DoS, protože noví klienti nemohou získat přístup k síti. Útok DoS je jakýkoli útok, který se používá k přetížení konkrétních zařízení a síťových služeb nelegitimním provozem, čímž zabraňuje legitimnímu provozu dosáhnout těchto zdrojů.

Při útocích na spoofing DHCP útočník nakonfiguruje falešný server DHCP v síti tak, aby klientům odesílal adresy DHCP. Normálním důvodem tohoto útoku je nutit klienty, aby používali servery falešných doménových jmen (DNS) a útočníkovu DHCP nebo stroj pod kontrolou útočníka jako jejich výchozí bránu. Hladovění DHCP se často používá před útokem spoofingu DHCP k odepření služby legitimnímu serveru DHCP, což usnadňuje zavedení falešného serveru DHCP do sítě. [5]

Útoky na Telnet

Protokol Telnet je nezabezpečený a útočník jej může použít k získání vzdáleného přístupu k síťovému zařízení Cisco. K dispozici jsou nástroje, které umožňují útočníkovi zahájit útok brutální silou s heslem proti VTY linkám na switche. [5]

Brute Force Password Attack

První fáze útoku heslem s hrubou silou začíná útočníkem pomocí seznamu běžných hesel a programu určeného k pokusu o navázání spojení telnet. Pokud heslo nezjistí první fáze, začne druhá fáze. Ve druhé fázi útoku hrubou silou útočník používá program, který vytváří sekvenční kombinace znaků ve snaze uhodnout heslo. Při dostatečném čase může útok hrubou silou odhalit téměř všechna použitá hesla. Ke zmírnění útoků s hrubou silou se používají silná hesla, která se často mění. Silné heslo by mělo obsahovat kombinaci velkých a malých písmen a mělo by obsahovat číslice a symboly (speciální znaky).Český jazyk má v tomto případě velkou výhodu. Přístup k připojení telnet na dané zařízení lze také omezit pomocí seznamu řízení přístupu pomocí ACL politiky. [5]

Telnet DoS Attack

Telnet lze také použít k zahájení útoku DoS. Při útoku na Telnet útočník využije chybu v softwaru serveru. Služba Telnet není následně dostupná. Z tohoto důvodu je lepší volit nastavení SSH než Telnet. [5]

Zabezpečení přístupu rozhraní

Všechny porty (rozhraní) switchů by měly být zabezpečeny před nasazením switche pro použití do sítě. Jedním ze způsobů, jak zabezpečit porty, je implementace funkce zvané zabezpečení portů. Zabezpečení portu omezuje počet platných MAC adres povolených na portu. Přístup na adresy MAC legitimních zařízení je povolen, zatímco ostatní adresy MAC jsou odepřeny, což znamená ,že koncové zařízení nebude fungovat.

Zabezpečení portů lze nakonfigurovat tak, aby umožňovalo jednu nebo více MAC adres. Pokud je počet MAC adres povolených na portu omezen na jednu, pak se k portu může úspěšně připojit pouze zařízení s touto konkrétní adresou MAC.

Pokud je port nakonfigurován jako zabezpečený port a je dosaženo maximálního počtu MAC adres, jakékoli další pokusy o připojení pomocí neznámých MAC adres způsobí narušení zabezpečení. [5]

Typy zabezpečení na MAC adresu

Existuje mnoho způsobů, jak nakonfigurovat zabezpečení portů. Níže jsou vyjmenované základní typy:

1. Statické zabezpečené adresy MAC
    - adresy MAC, které jsou ručně nakonfigurovány na portu
2. Dynamické bezpečné adresy MAC
    - adresy MAC, které jsou dynamicky naučeny a uloženy pouze v tabulce adres.
3. Sticky zabezpečené MAC adresy
    - MAC adresy, které lze dynamicky naučit nebo ručně nakonfigurovat, poté se přidá do tabulky adres a running konfigurace, která slouží k tomu, že při restartování switche bude neustále daná tabulka MAC adres platná na rozdíl od dynamického zabezpečení. [4]

Port security

Rozhraní portů lze nakonfigurovat pro jeden ze tří režimů narušení a určit akci, která má být provedena, pokud dojde k narušení. Seznam režimů je :

- Protect
  - Tento režim spočívá v tom, že jakmile počet povolených MAC adres dosáhne limitu povoleného na portu, pakety s neznámými zdrojovými adresami jsou vyřazovány, dokud není uvolněn dostatečný počet povolených MAC adres, nebo zvýšen počet maximálních povolených adres. Neexistuje žádné upozornění, že došlo k narušení zabezpečení.
- Restrict
  - Stejný princip jako u režimu protect ,ale tomto režimu je upozornění, že došlo k narušení zabezpečení.
- Shutdown (výchozí režim)
  - V tomto režimu narušení zabezpečení portu způsobí, že se rozhraní okamžitě deaktivuje a vypne příslušný port. Dané porušení je zapsáno v systému a administrátor může zjistit, co to způsobilo. Pro fungování daného rozhraní se musí rozhraní vypnout a zapnout, aby fungovala komunikace. [4]

Ověření bezpečnosti portů

Po nakonfigurování daných portů na switchi je nutné zkontrolovat každý port zvlášť a hlavně, zda je všechno správně nastaveno, než začneme toto zařízení používat v reálném provozu. Toto může být jedna z lidských chyb, kvůli může daná sít narušena. Je nutná kontrola MAC adress tabulky ve switchi, která odpovídá MAC adresám zapojených počítačů v síti.

Narušení portu v režimu shutdown se většinou projeví tak, že LED dioda portu zhasne. Výstup příkazu *show port-security interface* zobrazuje stav portu jako zabezpečené vypnutí. Protože je režim narušení zabezpečení portu nastaven na vypnutí, port s narušení bezpečnosti přejde do stavu deaktivace chyby.

Před opětovným povolením portu by měl správce sítě zjistit, co způsobilo narušení zabezpečení. Pokud je k zabezpečenému portu připojeno neautorizované zařízení, nemělo by být znovu povoleno, dokud nebude eliminována bezpečnostní hrozba. [4]

3.4.8 **VLAN**

VLAN (Virtuální LAN) je logicky samostatná podsíť IP která je virtuální. VLAN umožňují existenci více sítí IP a podsítí ve stejné switch síti. Aby mohly počítače komunikovat ve stejné VLAN, musí mít každý IP adresu a masku podsítě, která je konzistentní pro danou VLAN. Switche musí být nakonfigurován s VLAN a každý port ve VLAN musí být přiřazen k VLAN. Port switche s nakonfigurovanou jedinečnou sítí VLAN se nazývá přístupový port. Například to, že dva počítače jsou fyzicky připojeny ke stejnému switchi, neznamená, že mohou komunikovat. Zařízení ve dvou samostatných sítích a podsítích musí komunikovat prostřednictvím switche, ať už jsou použity sítě VLAN. Používání sítě VLAN má určité výhody.

- Zabezpečení
    - Skupiny, které mají citlivá data, jsou odděleny od zbytku sítě, což snižuje riziko narušení důvěrných informací.
- Snížení nákladů
    - Úspory nákladů vyplývají z menší potřeby drahých upgradů sítě
- Vyšší výkon
    - Rozdělení plochých sítí vrstvy na více logických pracovních skupin snižuje zbytečný provoz v síti a zvyšuje výkon.
- Broadcast storm
    - Rozdělení sítě na sítě VLAN snižuje počet zařízení, která se mohou účastnit broadcast storm.
- Vylepšená efektivita zaměstnanců IT
    - sítě VLAN usnadňují správu sítě, protože uživatelé s podobnými požadavky na síť sdílejí stejnou síť

Porty switche jsou v rozhraní na 2. vrstvě OSI modelu, která je přiřazena k fyzickému portu. Port může patřit do libovolné VLANy. Tento port může být přístupový port nebo trunkový port. Ke komunikaci mezi jednotlivými VLANy slouží trunkový port, který je připojený k routeru. Router musí brát v potaz že se jedná o VLANy. Proto používá speciální routování, které se jmenuje router on a stick. [4]

3.4.9 **Router a routování**

Dnešní počítačové sítě mají velký dopad na způsob komunikace v nynější době. Mění způsob, jakým žijeme, pracujeme a hrajeme počítačové hry. Počítačové sítě respektive internet umožňují lidem komunikovat jak nikdy předtím. Síť využíváme různými způsoby internetové obchodování nebo vzdělávání.

Uprostřed sítě je router. Router připojuje jednu síť k druhé síti. Router je proto zodpovědný za doručování paketů do různých sítí. Cílovým paketem IP může být webový server v jiné části planety nebo e-mailový server v místní síti. Povinností routeru je doručit tyto pakety včas.

Kromě předávání paketů poskytuje router také další služby. Zajistěte dostupnost 24 hodin denně, 7 dní v týdnu. Aby se zajistila dostupnost sítě, router používají alternativní cesty v případě selhání primární cesty. Zařízení komunikující v různých sítích mohou komunikovat pouze kvůli směrování paketů mezi sítěmi.

Primární funkcí routeru je předávat paket směrem k jeho cílové síti, což je cílová IP adresa paketu. Aby to bylo možné provést, musí router vyhledat informace o směrování uložené v jeho směrovací tabulce. Směrovací tabulka je datový soubor v RAM paměti, který se používá k ukládání informací o trase přímo připojených a vzdálených sítí. Směrovací tabulka obsahuje přidružené sítě. Vzdálená síť je síť, která není přímo připojena k routeru. U vzdálené sítě lze zaručit doručení pouze odesláním paketu jinému routeru. Vzdálené sítě jsou doplňovány do směrovací tabulky pomocí dynamického směrovacího protokolu nebo ruční konfigurací statických tras. Dynamické trasy jsou trasy do vzdálených sítí, které se router naučil automaticky pomocí dynamického směrovacího protokolu. Statické trasy jsou trasy do sítí, které správce sítě ručně nakonfiguroval. Mezi dynamické protokoly patří RIPv2,OSPF, EIGRP, BGP. Cisco router se konfiguruje stejně jako Cisco Switch. V kapitole 3.4.7.1 je vylíčeno jak se konfiguruje switch. [4]

3.4.10 **OSPF Routing**

Protokol OSPF (Open Shortest Path First) je směrovací protokol otevřeného standartu, který implementuje mnoho dodavatelů síťových zařízení včetně společnosti Cisco. Právě díky své otevřenosti tento protokol nabízí pružnost a popularitu. Většina správců sítě volí tento protokol, který nejdříve sestaví strom nejkratších cest a poté zaplní směrovací tabulky výslednými nejlepšími trasami. [4]

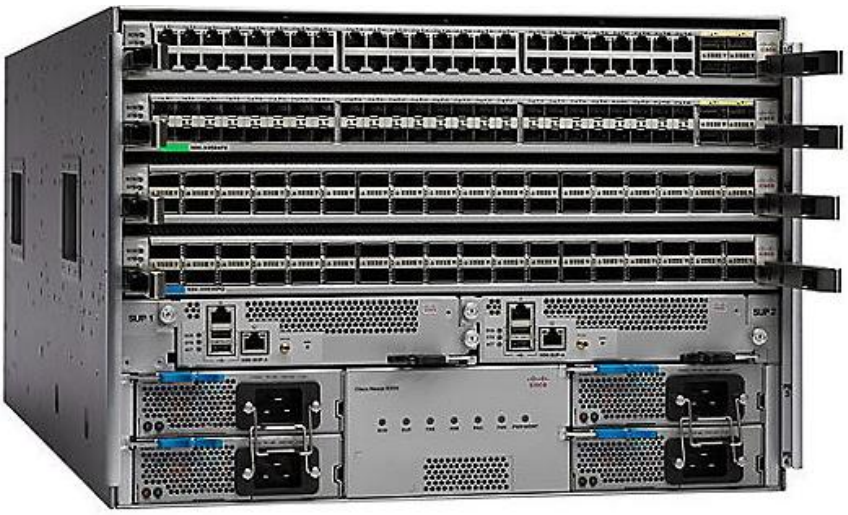
Protokol EIGRP sítě dosahuje mimořádně krátkých časů konvergence, ale protokol OSPF za ním příliš nezaostává. Rychlá konvergence představuje další důvod jeho obliby. Protokol OPSF poskytuje další dvě zásadní výhody. Podporuje více tras se stejnými náklady ke stejnému cíli a podobně protokol EIGRP je také kompatibilní se směrovacími protokoly IP. OSPF pracuje se třemi roubovacími tabulkami:

- Sousední tabulka
    - Obsahuje všechny objevené sousedy OSPF, se kterými budou vyměněny směrovací informace.
- Tabulka topologie
    - Obsahuje celou cestovní mapu sítě se všemi dostupnými OSPF a vypočítané nejlepší a alternativní cesty.
- Směrovací tabulka
    - Obsahuje aktuální pracovní nejlepší cesty, které budou použity pro předávání datového přenosu mezi sousedy.[4]

3.5 Představení novinek a trendů v oblasti bezpečnosti

Cisco ACI

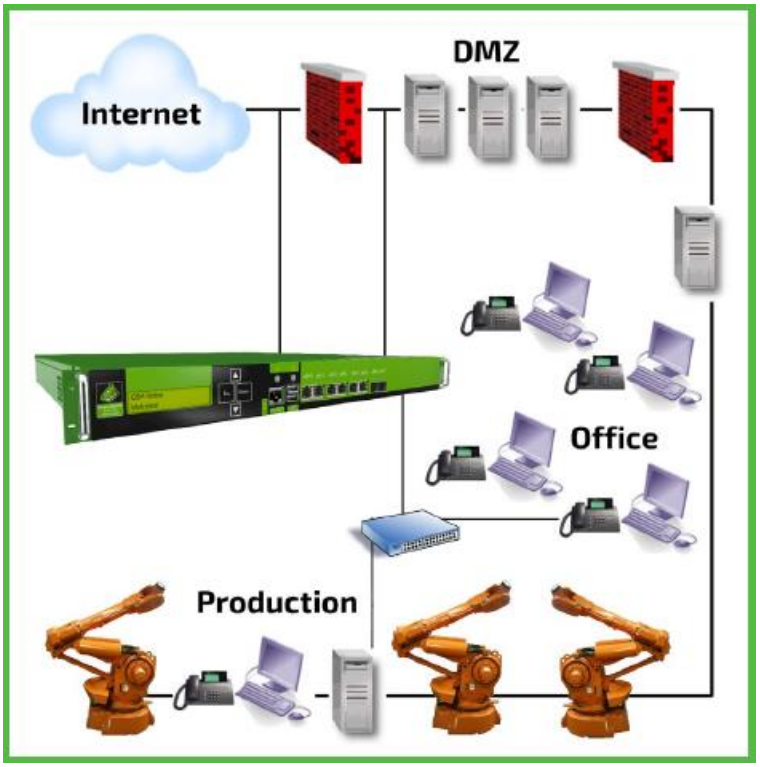
Cisco Application Centric Infrastructure (ACI), je softwarové řešení definované v síti (SDN).Usnadňuje agilitu aplikací a automatizaci datových center. ACI umožňuje škálovatelné multi-cloudové sítě s konzistentním modelem politiky a poskytuje flexibilitu pro bezproblémový přesun aplikací na libovolné místo nebo do jakéhokoli cloudu při zachování bezpečnosti a vysoké dostupnosti. Zaměřuje se na aplikace a poskytuje centralizovanou platformu pro správu aplikačních politik napříč fyzickým i virtuálním pracovním zatížením. Cisco ACI automatizuje pracovní toky a zabezpečení IT, což zákazníkům umožňuje vytvářet agilní a zabezpečená datová centra nové generace. Základní stavební kámen nového řešení Cisco ACI tvoří síťové prvky Nexus 9000 (Obrázek 16). [24]



Obrázek 16 - Cisco Nexus 9000 [24]

Greenbone

Greenbone Security Manager (GSM) je vyhrazené bezpečnostní zařízení pro správu zabezpečení počítačových sítí. Je je to opatření s ohledem na rizika a náklady. Dokáže odhalit zranitelnost dříve, než dojde k útoku. Hlavním pointou je prevence nežádoucích útoků. GSM lze aplikovat z různých perspektiv. Aktivace z vnější perspektivy zahrnuje identifikace špatně nakonfigurovaných firewallů a detekce vysoce bezpečnostních chyb. V rámci vnitřní sítě se jedná o počítačové červy, vnitřní útok, detekce potenciálního poškození a klasifikace podle rizika.



Obrázek 17 - Greenbone [25]

3.5.1 **Očekávané směry vývoje zabezpečení sítě**

Posledních pět let bylo pro zabezpečení dat velmi kritickými. Zpráva od společnosti IBM Security o „nákladech na porušení dat“ z roku 2019 říká, že průměrné náklady na porušení dat dosáhly 3,92 milionu USD. Za únik dat jsou odpovědné velké společnosti. Průzkum Ping identity z října roku 2019 zjistil, že 81% spotřebitelů by přestalo spolupracovat online, kdyby došlo k úniku dat. To by vedlo k porušení reputace společnosti a zvýšení nákladu na bezpečnost dat. Zákony GDPR a CCPA mají za dopad další náklady na bezpečnost dat. U osob, které mají na starosti ochranu dat v dnešním rozsáhlém prostředí hrozeb může dojít ke zvýšené míře vyčerpání a vyhoření. [21] [22]

Pět počítačových rizik, která budou v roce 2020 ohrožovat firemní data

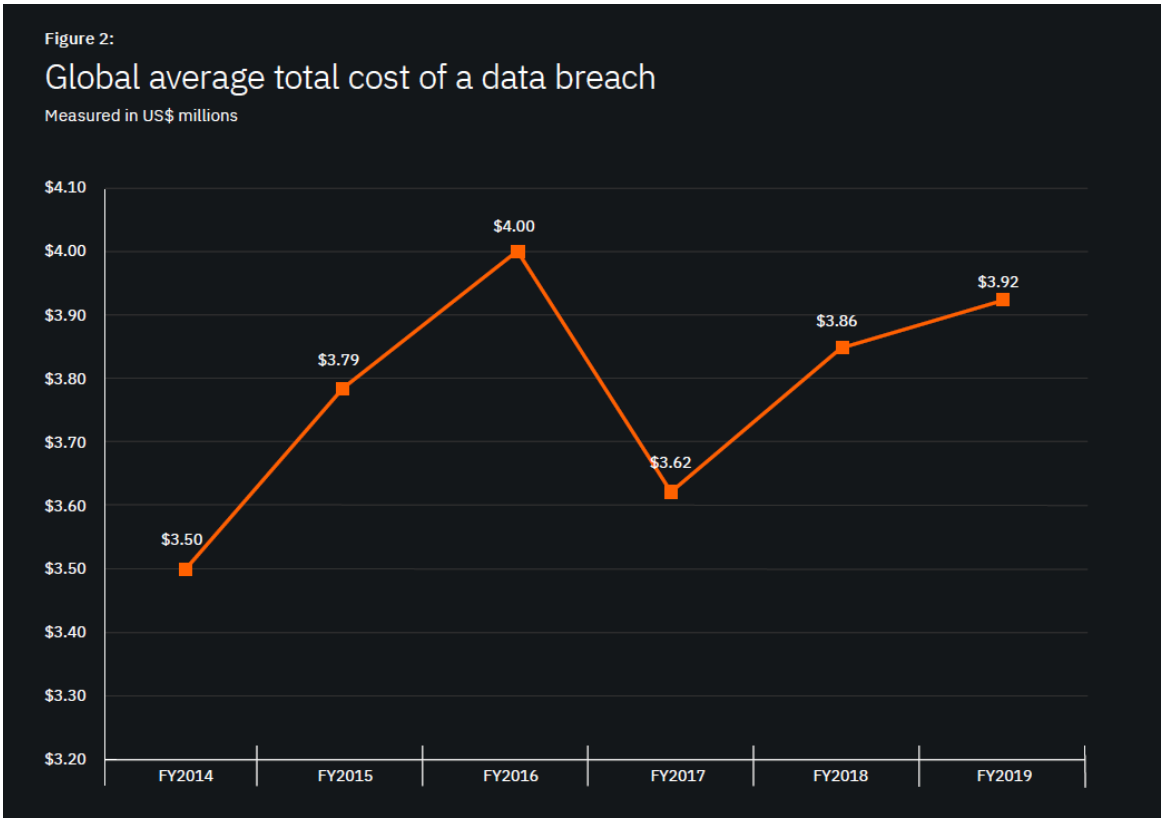
- Člověk zevnitř
  - Zaměstnanci představují významnou hrozbu pro firemní data. Zpráva Verizon's 2019 Insider Threat Report odhaduje, že interní hrozby způsobují více než třetinu všech dat.
- Phishingscam
  - Navzdory jejich nejlepšímu úsilí se phishingové podvody nevyhnutelně dostávají do doručené pošty zaměstnanců, což ohrožuje firemní data.
- Odkryté databáze
  - Cloud computing patří mezi nejnovější trendy pro podniky malé i střední.. Vzhledem k tomu, že převážná většina podniků přesouvá své operace do cloudu, představuje tento přechod příležitost k vystavení dat. Tento technologický dohled může mít závažné důsledky pro bezpečnost dat
- Unavení IT administrátoři
  - Odborníci na kybernetickou bezpečnost čelí neuvěřitelným útokům. I když se každý den brání proti tisícům útoků, počítačoví zločinci a interní špatní aktéři musí být úspěšní pouze jednou, aby společnosti způsobili vážné škody. Výsledkem je, že odborníci na kybernetickou bezpečnost vyhoří a opouštějí povolání. Odhaduje se, že 65% odborníků v oblasti IT zvažuje ukončení své práce a podobný počet je otevřený pro odchod z profese úplně.
- Špatné priority
  - Navzdory ohromným důkazům, že ztráta dat je jednou z největších hrozeb, kterým společnosti v digitálním věku čelí, stále roste důkaz o tom, že vedení společnosti rizika neuznává. Vedení firem se neshodují s manažery informační bezpečnosti, kde se jejich pohledy na bezpečnost rozcházejí. [22]

3.5.2 Náklady na únik dat v roce 2019

Náklady na únik dat Dle statistik IBM a výroční zprávy IBM Security, která v roce 2019 je vydala na 77 stránkách agreguje náklady nahlášené 507 organizacemi, ze 17 průmyslových odvětví, ze 16 regionů: USA, Indie, Velká Británie, Německo, Brazílie, Japonsko, Francie, Střední východ, Kanada, Itálie, Jižní Korea, Austrálie, Turecko, ASEAN, Jižní Afrika a Skandinávie. [23]

Celkové průměrné celkové náklady na narušení dat

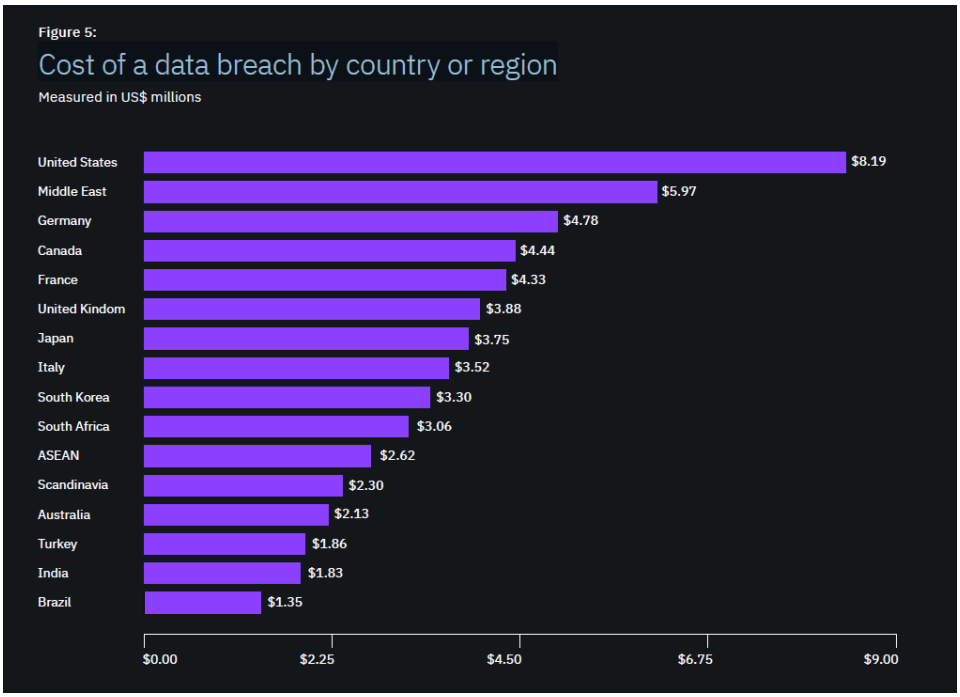
Obrázek (Obrázek 18) demonstruje celkové průměrné celkové náklady na porušení dat během šesti let. Z konsolidovaného průměru je zřejmé, že celkové náklady na porušení v roce 2019 vzrostly o 1,5 procenta oproti roku 2018. Za šest let od roku 2014 průměrné celkové náklady na porušení dat vzrostly o 12 procent z 3,5 milionu dolarů.[23]



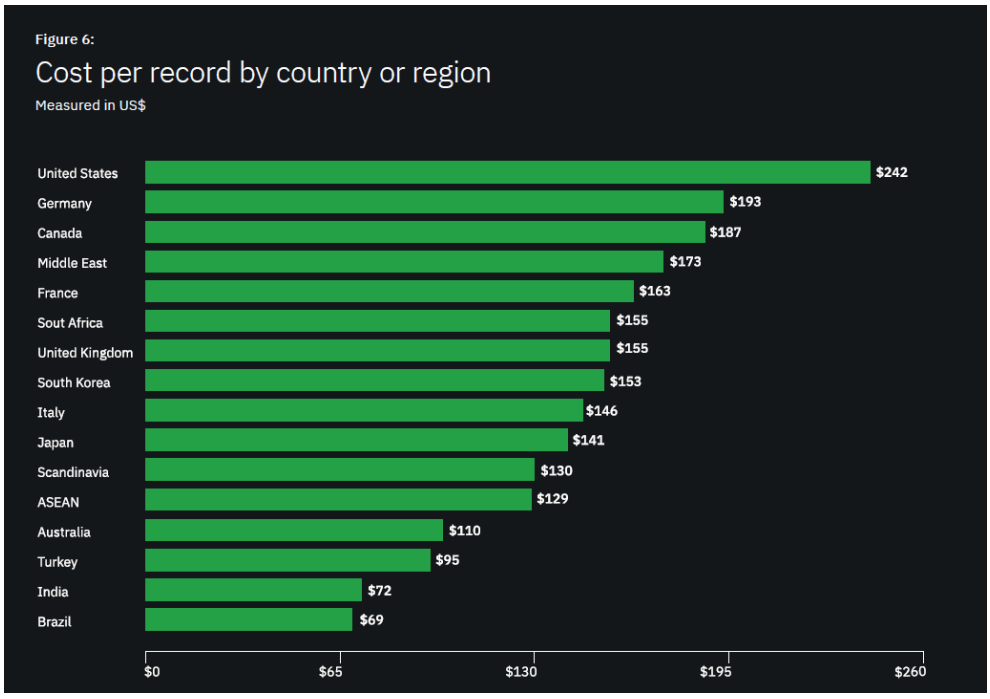
Obrázek 18 - Graf celkových průměrných nákladů na narušení dat [23]

Náklady na porušení dat podle země nebo regionu

V USA stojí narušení dat společnosti v průměru 8,19 milionu USD, což tvoří nárůst ze 7,91 milionu USD v roce 2018 a více než dvojnásobek celosvětového průměru (Obrázek 19). Cena za porušený záznam je 242 $ (Obrázek 20). [23]



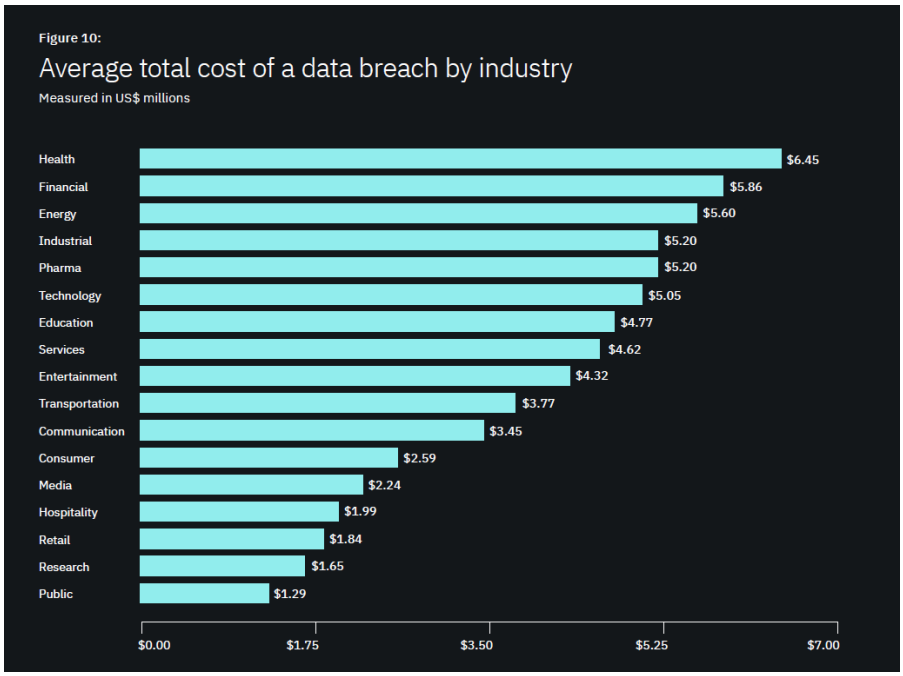
Obrázek 19 - Graf nákladů na porušení dat podle země nebo regionu [23]



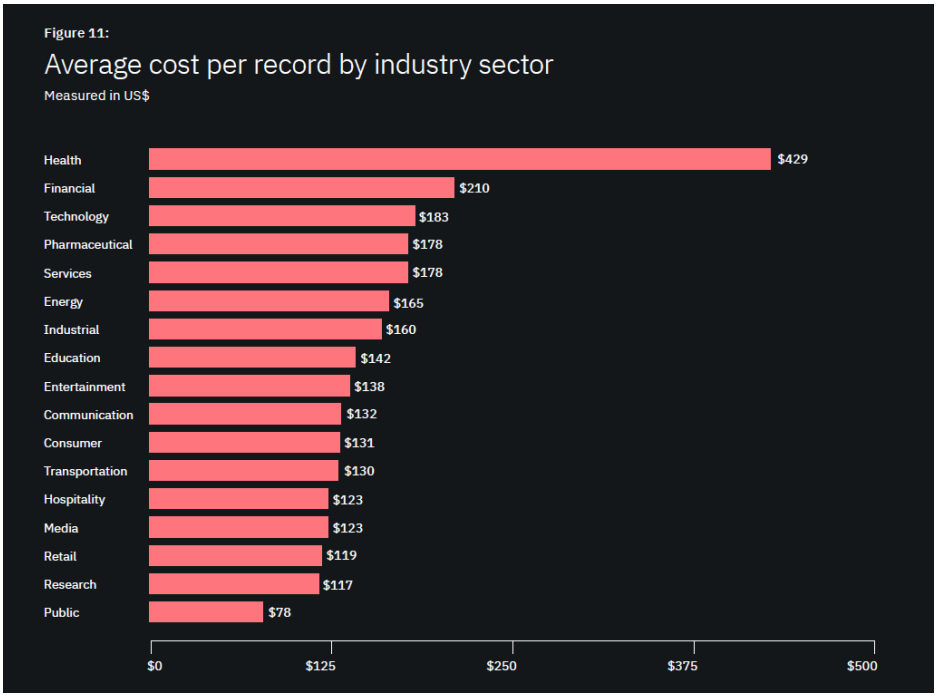
Obrázek 20 - Graf nákladů na porušení dat podle země nebo regionu na jeden záznam [23]

Průměrné celkové náklady na porušení dat podle odvětví

Obrázek (Obrázek 21) demonstruje, že ve zdravotnictví, finančních službách, energetice a farmaceutickém průmyslu došlo k průměrným celkovým nákladům na porušení údajů výrazně vyšším než v méně regulovaných odvětvích, jako jsou média, pohostinství, maloobchod a výzkumné organizace. Organizace veřejného sektoru tradičně měly nižší náklady na narušení dat, protože je nepravděpodobné, že by došlo k významné ztrátě zákazníků v důsledku narušení dat. Zdravotnický průmysl stojí narušení 6,45 milionu USD. Cena za porušený záznam je 429 $ (Obrázek 22). [23]



Obrázek 21 - Graf průměrných celkových nákladů na porušení dat podle odvětví [23]



Obrázek 22 - Graf průměrných celkových nákladů na porušení dat podle odvětví za jeden záznam [23]

4 Praktická část

Praktická část je rozdělena na tři kapitoly. První kapitola je zaměřena na Cisco Packet Tracer, vlastní návrh, IP adresace a dílčí konfigurace . Druhá kapitola představu je reálné řešení a skenování sítě pro odhalení slabin. Třetí kapitola je zaměřena na ekonomické zhodnocení j e obohacena dalšími cenovými nabídkami.

4.1 Packet tracer

Je představeno používání software Cisco Packet Traceru. Následuje vlastní návrh počítačové topologie, adresace zařízení, konfigurace jednotlivých zařízení, nastavení jednotlivých služeb, blokování nebezpečné webové stránky. Tato kapitola je zaměřena na detailnější konfiguraci všech sítových prvků.

Stanové úlohy pro fungování topologie.

- Základní konfigurace pro komunikaci – adresace
- Vytvoření VLAN
- OSPF směrovací protokol
- VPN přenos
- NAT
- Zabezpečení 2 vrstvy
- Zabezpečení 3 vrstvy
    - Zamezený přístup přes pravidla ACL na webový portál www.thepiratebay.org
- Nastavení hesel
    - Konfigurace AAA na routeru R5
    - SSH
    - Zaheslování zařízení v rámci modrého kampusu

4.1.1 Cisco Packet Tracer

Cisco Packet Tracer je výukový software vyvinutý od společnosti Cisco Systems. Jeho hlavním cílem jsou vzdělávací nástroje, které fungují pro účel Networking Academy, během kterého získávají studenti dostupné znalosti. Packet Tracer je neustále vyvíjen a je v souladu s aktuálním vývojem počítačových sítí. Jeho prostředím lze simulovat jakoukoli síť založenou na síťových prvcích Cisco. Konfigurace bude prováděna na verzi 7.3.0.0838. Tento software je bezplatný v rámci členství Cisco Networking Academy, kterým je autor členem od roku 2012.

4.1.2 **Stažení a instalace**

Plnou verzi software Cisco Packet Tracer lze stáhnout na stránkách.
https://www.netacad.com/courses/packet-tracer s minimálními hardwarovými požadavky :

- CPU: Intel Pentium 4, 2.53 GHz
- OS: Microsoft Windows 7, 8.1, 10, Linux Ubuntu 18.04.3 LTS
- RAM: 2 GB
- Disk: 500 MB
- Rozlišení: 1024 x 768
- Poslední grafický ovladače a operační systémový update

Po instalaci je nutné využít přihlašovací účet, který je součástí Cisco Networking Academy (Obrázek 23).

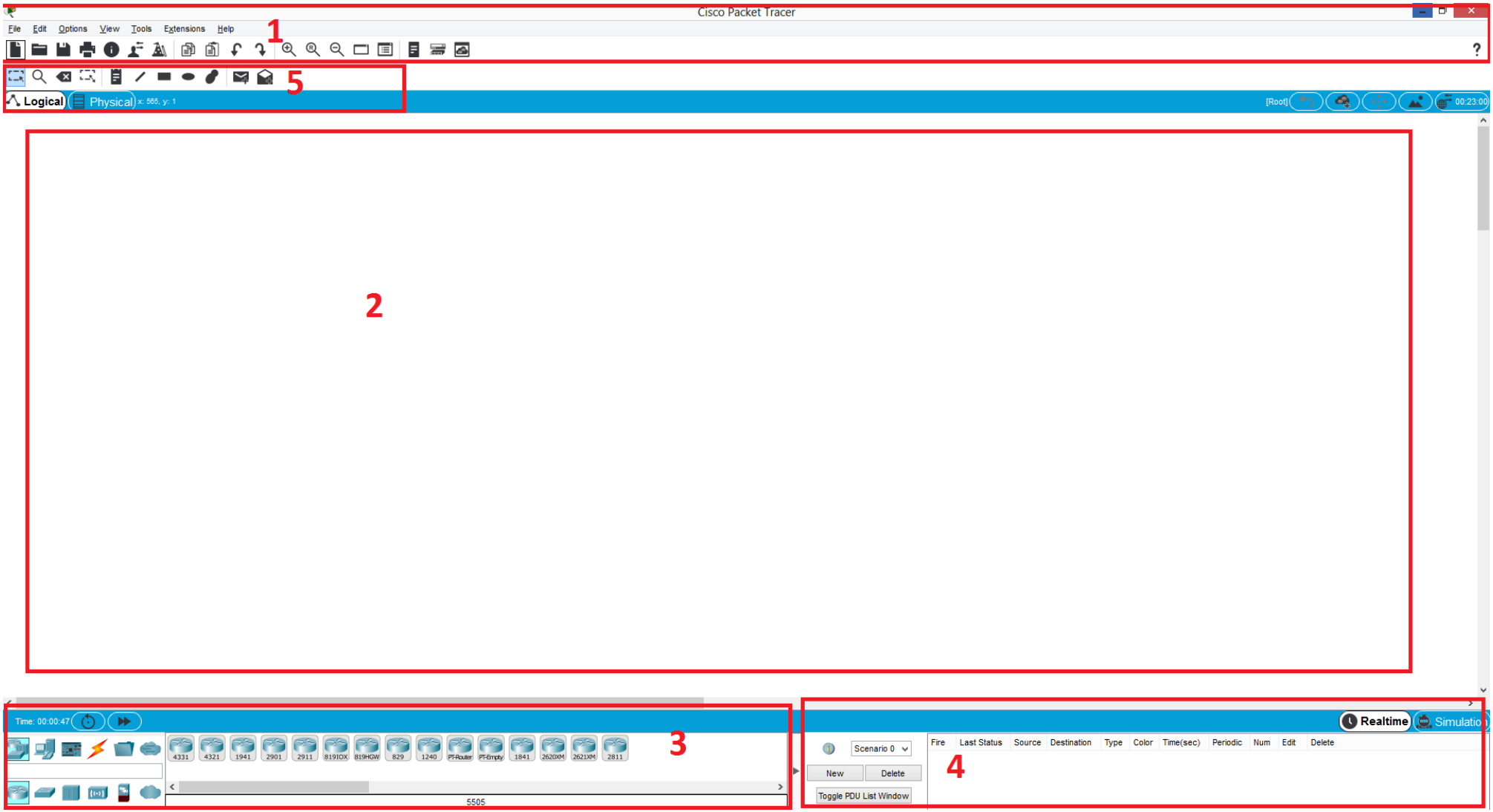
Obrázek 23 - Cisco Packet Tracer přihlašovací okno [16]

4.1.3 **Vzhled a uspořádání prostředí**

Po úspěšném přihlášení je spuštěna aplikace Cisco Packet Tracer. Je možné vidět počáteční nastavení na nadcházejícím obrázku (Obrázek 24). Prostředí se rozděluje na pět hlavních částí. Hlavní menu, pracovní prostor, nástroje, okno paketů, sekundární menu. Jednotlivé části charakterizovány v následující tabulce (Tabulka 1).

1	**Hlavní menu**	První lišta obsahuje soubor, upravit, možnosti, zobrazit, nástroje, rozšíření, a nápověda. Druhá lišta obsahuje nový soubor ,otevřít, uložit, tisk.
2	**Pracovní prostor**	V této oblasti se tvoří sítová topologie z jednotlivých zařízení.
3	**Nástroje**	Lišta nástroje obsahuje typy CISCO zařízení.
4	**Okno paketů**	Okno spravuje pakety, které uživatel vložil do sítě během simulačních scénářů.
5	**Panel běžných nástrojů**	Lišta poskytuje nástroje malování, umístit poznámku , odstranit , zkontrolovat , změnit tvar Významný nástroj je PDU (Protocol data unit)

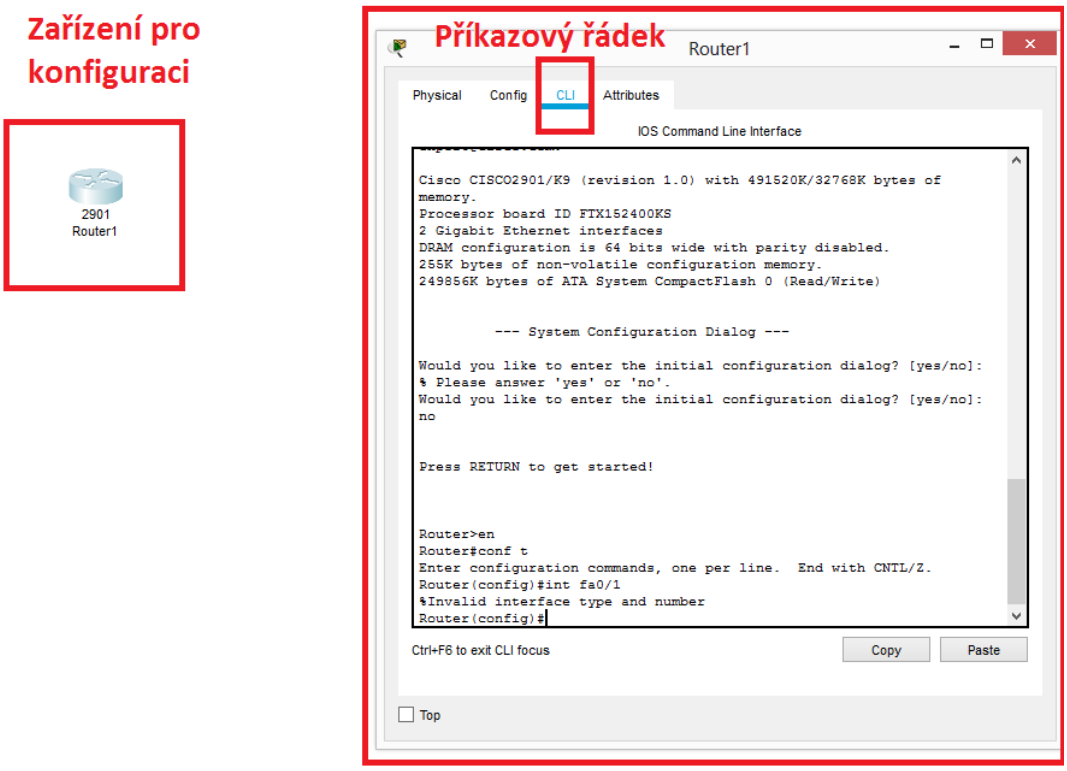
Tabulka 1 - Charakteristika Cisco Packet Tracer [16]



Obrázek 24 Cisco Packet Tracer prostředí [16]

Konfigurace zařízení

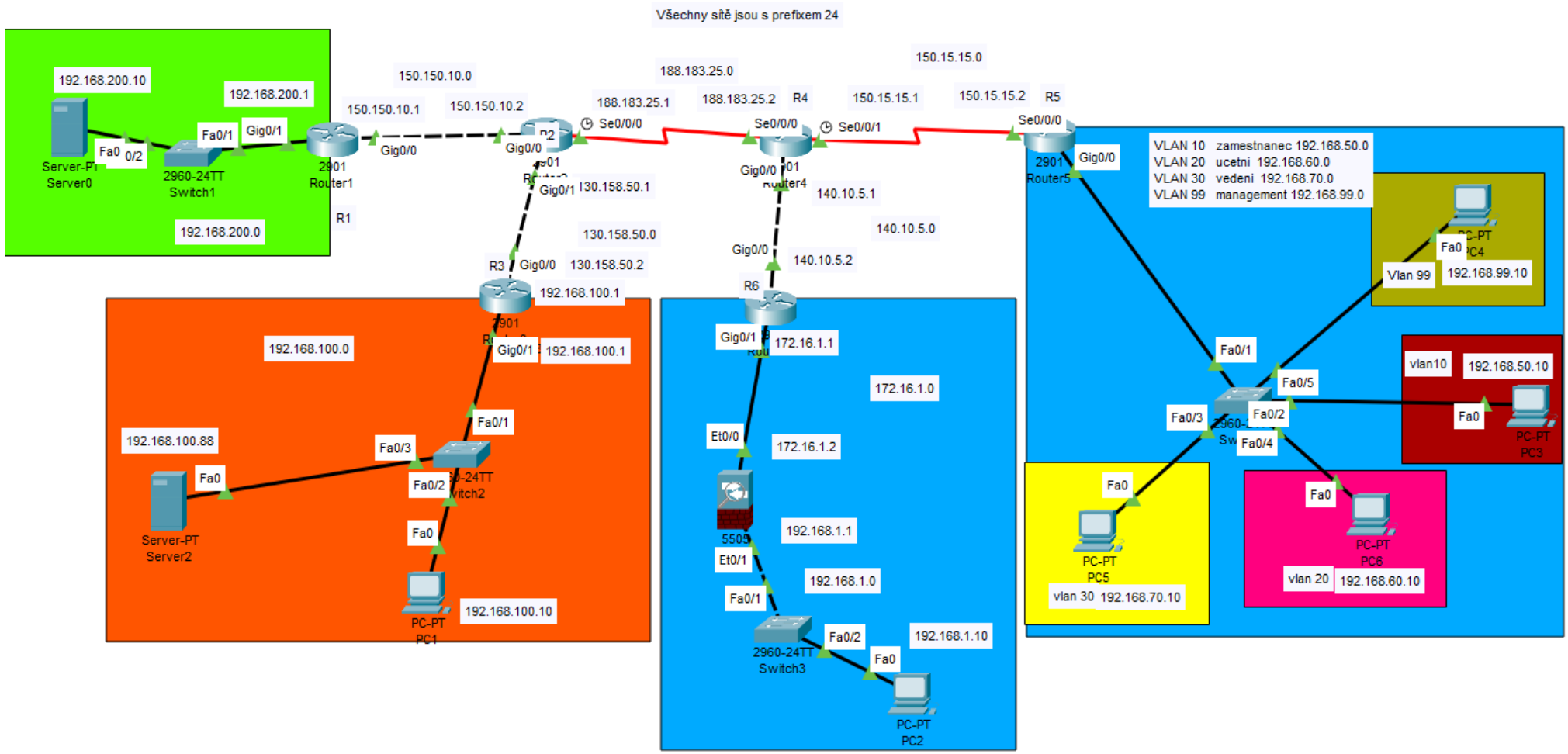
Jednotlivé konfigurace Cisco zařízení lze provádět v CLI (Příkazový řádek) (Obrázek 25). Packet Tracer umožnuje nastavení jednotlivých zařízení v globálním nastavení, ale v reálném prostředí tato možnost není dostupná. Uživatel musí brát na vědomí, že se pohybuje v simulačním prostředí.



Obrázek 25 Grafické prostředí pro příkazový řádek [16]

4.1.4 Konkrétní návrh počítačové sítě

Návrh sítové topologie je založen na předchozích zkušenostech z Cisco Networking Academy. Návrh je zaměřen na síťovou bezpečnost 2 a 3 vrstvy referenčního modelu ISO /OSI. Grafický návrh je možné vidět na následujícím obrázku (Obrázek 26).



Obrázek 26 - Vlastní návrh topologie sítě [16]

Návrh se skládá z pěti oblastí a čtyř podoblastí (VLAN). Každá oblast má svoji charakteristiku. Cílem zelené oblasti je poskytování DNS pro zbytek topologie. Červená oblast představuje případné bezpeční na základě vydané zprávy od Národního úřadu pro kybernetickou a informační bezpečnost. Modré oblasti jsou firemní prostředí. V pravé část je hlavní kampus firmy, který obsluhuje router jménem R5 a rozbočovač (SW4). Switch vytváří VLAN pro oddělené spojení zařízení ve firmě. Druhá oblast modré zóny obsahuje router a ASA firewall. Jeho hlavním úkolem je zabezpečit komunikaci mezi oběma zónami, která je šifrovaná. Na ASA bude proto vytvořena služba VPN, která bude spojena s routerem (R5). Celá topologie obsahuje šest routerů typu Cisco 2901, čtyři rozbočovače typu Cisco 2960, šest počítačů, dva servery a ASA. Návrh je redukovaný na základní funkce pro simulaci.

4.1.5 **IP Adresace**

Součástí návrhu topologie je IP adresace (Tabulka 2). Patří k nejdůležitějším úkolům při tvoření návrhu topologie. Hlavním účelem IP adresace je komunikace mezi jednotlivými zařízeními. Všechny IP adresy jsou typu IPv4. Pro adresování mezi routery je využita veřejná sítová kategorie s prefixem 24. Mezi routerem (Router6) a ASA je využita privátní síťová kategorie třídy B s prefixem 24. Pro adresování koncových síťových zařízení v oblastech (oranžová, zelená, modrá) je použita privátní síťová třída kategorie C s prefixem 24. U VLAN sítě je využita síťová kategorie C s prefixem 24.

Zařízení	Rozhraní	IP adresa	Maska podsítě	Výchozí brána	DNS server
Router1	G0/0	150.150.10.1	255.255.255.0		
	G0/1	192.168.200.1	255.255.255.0		
Router2	S0/0/0	188.183.25.1	255.255.255.0		
	G0/0	150.150.10.2	255.255.255.0		
	G0/1	130.158.50.1	255.255.255.0		
Router3	G0/0	130.158.50.2	255.255.255.0		
	G0/1	192.168.100.1	255.255.255.0		
Router4	S0/0/0	188.183.25.2	255.255.255.0		
	S0/0/1	150.15.15.1	255.255.255.0		
	G0/0	140.10.5.1	255.255.255.0		
Router5	S0/0/0	150.15.15.2	255.255.255.0		
	G0/0		255.255.255.0		
	G0/0.10	192.168.50.1	255.255.255.0		
	G0/0.20	192.168.60.1	255.255.255.0		
	G0/0.30	192.168.70.1	255.255.255.0		
	G0/0.99	192.168.99.1	255.255.255.0		
Router6	G0/0	140.10.5.2	255.255.255.0		
	G0/1	172.16.1.1	255.255.255.0		
ASA	Ethernet 0/0	172.16.1.2	255.255.255.0		192.135.250.5
	Ethernet 0/1	192.168.1.1	255.255.255.0		
Server 1	192.168.200.10		255.255.255.0	192.168.200.1	
Server 2	192.168.100.88		255.255.255.0	192.168.100.1	192.168.200.10
PC 1		192.168.100.10	255.255.255.0	192.168.100.1	192.168.200.10
PC 2		DHCP			192.168.200.10
PC 3		DHCP			192.168.200.10
PC 4		DHCP			192.168.200.10
PC 5		DHCP			192.168.200.10
PC 6		192.168.99.10	255.255.255.0	192.168.99.1	192.168.200.10
Switch 1					
Switch 2					
Switch 3					
Switch 4		VLAN 99 - 192.168.99.5			

Tabulka 2 - IP Adresace [16]

4.1.6 **Základní konfigurace pro komunikaci – adresace**

Následující část představuje základní konfigurace adresace pro fungování topologie mezi routery a switchi. IP adresace vychází z tabulky (Tabulka 3).

R1	Konfigurace routeru R1
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R1	Nástavní jména zařízení
R1(config)#interface gig0/0	Vstup do konfigurace rozhraní gig0/0
R1(config-if)#ip address 150.150.10.1 255.255.255.0	Přidělení IP adresy s maskou
R1(config-if)#no shutdown	Zapnutí rozhraní
R1(config-if)#interface gig0/1	Vstup do konfigurace rozhraní gig0/1
R1(config-if)#ip address 192.168.200.1 255.255.255.0	Přidělení IP adresy s maskou
R1(config-if)#no shutdown	Zapnutí rozhraní
R2	Konfigurace routeru R2
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R2	Nástavní jména zařízení
R2(config)#interface s0/0/0	Vstup do konfigurace rozhraní s0/0/0
R2(config-if)#ip address 188.183.25.1 255.255.255.0	Přidělení IP adresy s maskou
R2(config-if)#no shutdown	Zapnutí rozhraní
R2(config-if)#exit	Vystoupení z rozhraní do privilegovaného modu
R2(config)#interface gig0/0	Vstup do konfigurace rozhraní gig0/0
R2(config-if)#ip address 150.150.10.2 255.255.255.0	Přidělení IP adresy s maskou
R2(config-if)#no shutdown	Zapnutí rozhraní
R2(config-if)#interface gig0/1	Vstup do konfigurace rozhraní gig0/1
R2(config-if)#ip address 130.158.50.1 255.255.255.0	Přidělení IP adresy s maskou
R2(config-if)#no shutdown	Zapnutí rozhraní
R3	Konfigurace routeru R3
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R3	Nástavní jména zařízení
R3(config)#interface gig0/0	Vstup do konfigurace rozhraní gig0/0
R3(config-if)#ip address 130.158.50.2 255.255.255.0	Přidělení IP adresy s maskou

R3(config-if)#no shutdown	Zapnutí rozhraní
R3(config-if)#interface gig0/1	Vstup do konfigurace rozhraní gig0/1
R3(config-if)#ip address 192.168.100.1 255.255.255.0	Přidělení IP adresy s maskou
R3(config-if)#no shutdown	Zapnutí rozhraní
R4	Konfigurace routeru R4
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R4	Nástavní jména zařízení
R4(config)#interface gig0/0	Vstup do konfigurace rozhraní gig0/0
R4(config-if)#ip address 140.10.5.1 255.255.255.0	Přidělení IP adresy s maskou
R4(config-if)#no shutdown	Zapnutí rozhraní
R4(config-if)#interface s0/0/0	Vstup do konfigurace rozhraní s0/0/0
R4(config-if)#ip address 188.183.25.2 255.255.255.0	Přidělení IP adresy s maskou
R4(config-if)#no shutdown	Zapnutí rozhraní
R4(config-if)#interface s0/0/1	Vstup do konfigurace rozhraní s0/0/1
R4(config-if)#ip address 150.15.15.1 255.255.255.0	Přidělení IP adresy s maskou
R4(config-if)#no shutdown	Zapnutí rozhraní
R5	Konfigurace routeru R5
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R5	Nástavní jména zařízení
R5(config)#interface s0/0/0	Vstup do konfigurace rozhraní s0/0/0
R5(config-if)#ip address 150.15.15.2 255.255.255.0	Přidělení IP adresy s maskou
R5(config-if)#no shutdown	Zapnutí rozhraní
R6	Konfigurace routeru R6
Router>en	Vstup do privilegovaného módu
Router#conf t	Vstup do konfiguračního modu
Router(config)#hostname R6	Nástavní jména zařízení
R6(config)#interface gig0/0	Vstup do konfigurace rozhraní gig0/0
R6(config-if)#ip address 140.10.5.2 255.255.255.0	Přidělení IP adresy s maskou
R6(config-if)#no shutdown	Zapnutí rozhraní
R6(config-if)#interface gig0/1	Vstup do konfigurace rozhraní gig0/1
R6(config-if)#ip address 172.16.1.1 255.255.255.0	Přidělení IP adresy s maskou
R6(config-if)#no shutdown	Zapnutí rozhraní

Tabulka 3 - Základní konfigurace pro komunikaci – adresace [16]

4.1.7 **Vytvoření VLAN**

V pravé modré oblasti je topologie rozdělená do čtyř VLAN. Všechna koncová zařízení jsou následně připojena k určitým VLAN. Každá VLAN má svoji charakteristiku, pod kterou si můžeme představit adresaci, číslo VLAN. Defaultně VLAN nemohou mezi sebou komunikovat. Ke komunikaci mezi VLAN slouží router, který využívá termín routování na klacku (router on stick). Router v síti používá jedeno rozhraní (interface) pro všechny VLAN s pomocí tzv. podrozhraní (sub interface). Podrozhraní je více virtuální rozhraní spojené s jedním fyzickým rozhraním nakonfigurovaného jako kmenové sloučení 802.1q. Přidělení adres bude provedeno pomoci protokolu DHCP ,který je nakonfigurován na router (R5) (Tabulka 4).

Tabulky VLAN jejich vlastnosti:

- VLAN 10 zamestnanec 192.168.50.0
- VLAN 20 ucetni 192.168.60.0
- VLAN 30 vedeni 192.168.70.0
- VLAN 99 management 192.168.99.0

SW4	Konfigurace switche SW4
Switch>en	Vstup do privilegovaného módu
Switch#conf t	Vstup do konfiguračního modu
Switch(config)#hostname sw4	Nástavní jména zařízení
sw4(config)#vlan 10	Přidání VLAN 10
sw4(config-vlan)#name zamestnanec	Jméno vlan
sw4(config-vlan)#vlan 20	Přidání VLAN 20
sw4(config-vlan)#name ucetni	Jméno vlan
sw4(config-vlan)#vlan 30	Přidání VLAN 30
sw4(config-vlan)#name vedeni	Jméno vlan
sw4(config-vlan)#vlan 99	Přidání VLAN 99
sw4(config-vlan)#name management	Jméno vlan
sw4(config-vlan)#exit	Vystoupení z rozhraní do privilegovaného modu
sw4(config)#interface fa0/1	Vstup do konfigurace rozhraní fa0/1
sw4(config-if)#switchport mode trunk	Nastavení módu trunk
sw4(config-if)#no shutdown	Zapnutí rozhraní
sw4(config-if)#exit	Vystoupení z rozhraní do privilegovaného modu
sw4(config)#interface fa0/3	Vstup do konfigurace rozhraní fa0/3
sw4(config-if)#switchport mode access	Nastavení módu acces
sw4(config-if)#switchport access vlan 30	Přiřadí rozhraní do VLAN 30
sw4(config-if)#interface fa0/4	Vstup do konfigurace rozhraní fa0/4
sw4(config-if)#switchport mode access	Nastavení módu acces
sw4(config-if)#switchport access vlan 20	Přiřadí rozhraní do VLAN 20

sw4(config-if)#interface fa0/2	Vstup do konfigurace rozhraní fa0/2
sw4(config-if)#switchport mode access	Nastavení módu acces
sw4(config-if)#switchport access vlan 10	Přiřadí rozhraní do VLAN 10
sw4(config-if)#interface fa0/5	Vstup do konfigurace rozhraní fa0/5
sw4(config-if)#switchport mode access	Nastavení módu acces
sw4(config-if)#switchport access vlan 99	Přiřadí rozhraní do VLAN 99
sw4(config)#interface vlan 99	Vstup do konfigurace rozhraní VLAN 99
sw4(config-if)#ip address 192.168.99.5 255.255.255.0	Přidělení IP adresy s maskou
sw4(config-if)#no shutdown	Zapnutí rozhraní
R5>en	Vstup do privilegovaného módu
R5#conf t	Vstup do konfiguračního modu
R5(config)#interface gig0/0.10	Vstup do konfigurace rozhraní gig0/0.10
R5(config-subif)#encapsulation dot1Q 10	Určení číslo VLAN stanovému sub-portu
R5(config-subif)#ip address 192.168.50.1 255.255.255.0	Přidělení IP adresy s maskou
R5(config-subif)#interface gig0/0.20	Vstup do konfigurace rozhraní gig0/0.20
R5(config-subif)#encapsulation dot1Q 20	Určení číslo VLAN stanovému sub-portu
R5(config-subif)#ip address 192.168.60.1 255.255.255.0	Přidělení IP adresy s maskou
R5(config-subif)#interface gig0/0.30	Vstup do konfigurace rozhraní gig0/0.30
R5(config-subif)#encapsulation dot1Q 30	Určení číslo VLAN stanovému sub-portu
R5(config-subif)#ip address 192.168.70.1 255.255.255.0	Přidělení IP adresy s maskou
R5(config-subif)#interface gig0/0.99	Vstup do konfigurace rozhraní gig0/0.99
R5(config-subif)#encapsulation dot1Q 99	Určení číslo VLAN stanovému sub-portu
R5(config-subif)#ip address 192.168.99.1 255.255.255.0	Přidělení IP adresy s maskou
R5(config-subif)#int gig0/0	Vstup do konfigurace rozhraní gig0/0
R5(config-if)#no shutdown	Zapnutí rozhraní
R5(config-if)#exit	Vystoupení z rozhraní do privilegovaného modu
R5(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.9	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.50.19 192.168.50.255	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.70.1 192.168.70.9	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.70.19 192.168.70.255	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.60.1 192.168.60.9	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.60.19 192.168.60.255	Adresy, které nebudou přirazeny

R5(config)#ip dhcp excluded-address 192.168.99.1 192.168.99.9	Adresy, které nebudou přirazeny
R5(config)#ip dhcp excluded-address 192.168.99.19 192.168.99.255	Adresy, které nebudou přirazeny
R5(config)#ip dhcp pool zamestnanec	Vstup do konfigurace DHCP zamestnanec
R5(dhcp-config)#network 192.168.50.0 255.255.255.0	Rozsah sítě
R5(dhcp-config)#default-router 192.168.50.1	Výchozí brána
R5(dhcp-config)#dns-server 192.168.200.10	DNS server
R5(dhcp-config)#domain-name r5zamestnanec.cz	Doména
R5(dhcp-config)#ip dhcp pool ucetni	Vstup do konfigurace DHCP ucetni
R5(dhcp-config)#network 192.168.60.0 255.255.255.0	Rozsah sítě
R5(dhcp-config)#default-router 192.168.60.1	Výchozí brána
R5(dhcp-config)#dns-server 192.168.200.10	DNS server
R5(dhcp-config)#domain-name r5ucetni.cz	Doména
R5(dhcp-config)#ip dhcp pool vedeni	Vstup do konfigurace DHCP ucetni
R5(dhcp-config)#network 192.168.70.0 255.255.255.0	Rozsah sítě
R5(dhcp-config)#default-router 192.168.70.1	Výchozí brána
R5(dhcp-config)#dns-server 192.168.200.10	DNS server
R5(dhcp-config)#domain-name r5vedeni.cz	Doména
R5(dhcp-config)#ip dhcp pool management	Vstup do konfigurace DHCP management
R5(dhcp-config)#network 192.168.99.0 255.255.255.0	Rozsah sítě
R5(dhcp-config)#default-router 192.168.99.1	Výchozí brána
R5(dhcp-config)#dns-server 192.168.200.10	DNS server
R5(dhcp-config)#domain-name r5management.cz	Doména
R5(dhcp-config)#	

Tabulka 4 - Vytvoření VLAN [16]

4.1.8 **OSPF směrovací protokol**

Celá topologie komunikuje prostřednictvím routovacího protokolu OSPF. Jeho hlavním úkolem je propojovat jednotlivé sítě v navrhnuté topologii. Všechny směrovače (routery) fungují na stejném routovacím protokolu. Konfigurace protokolu OSPF se zahajuje příkazem Router(config)# router ospf <ID procesu>. Číslo charakterizuje jenom lokální informaci. V této kapitole bude konfigurováno OPSF s číslem 10 (R5(config)#router ospf 10). U protokolu OSPF je nutné nakonfigurovat všechny připojené podsítě, inverzní masky a oblast (Tabulka5). Inversní maska je speciální zápis síťové masky. Jedná se o opak ke klasické masce, počítají se zde nuly místo jedniček. Protokolem OSPF je možné šířit i statické routování, které má větší Administrative distance (Administrativní vzdálenost).

R1#en	Vstup do privilegovaného módu
R1#conf t	Vstup do konfiguračního modu
R1(config)#router ospf 10	Vstup do konfigurace OSPF
R1(config-router)#network 150.150.10.0 0.0.0.255 area 0	Přidání sítě a area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0	Přidání sítě a area 0
R2>en	Vstup do privilegovaného módu
R2#conf t	Vstup do konfiguračního modu
R2(config)#ip route 192.168.100.0 255.255.255.0 130.158.50.2	Přidání statického směrování
R2(config)#router ospf 10	Vstup do konfigurace OSPF
R2(config-router)#redistribute static subnets tag 33	Redistribuované statické routování
R2(config-router)#network 130.158.50.0 0.0.0.255 area 0	Přidání sítě a area 0
R2(config-router)#network 150.150.10.0 0.0.0.255 area 0	Přidání sítě a area 0
R2(config-router)#network 188.183.25.0 0.0.0.255 area 0	Přidání sítě a area 0
R3>en	Vstup do privilegovaného módu
R3#conf t	Vstup do konfiguračního modu
R3(config)#ip route 0.0.0.0 0.0.0.0 130.158.50.1	Přidání statického směrování
R4>en	Vstup do privilegovaného módu
R4#conf t	Vstup do konfiguračního modu
R4(config)#router ospf 10	Vstup do konfigurace OSPF
R4(config-router)#network 140.10.5.0 0.0.0.255 area 0	Přidání sítě a area 0
R4(config-router)#network 150.15.15.0 0.0.0.255 area 0	Přidání sítě a area 0
R4(config-router)#network 188.183.25.0 0.0.0.255 area 0	Přidání sítě a area 0
R5>en	Vstup do privilegovaného módu
R5#conf t	Vstup do konfiguračního modu
R5(config)#router ospf 10	Vstup do konfigurace OSPF
R5(config-router)#network 150.15.15.0 0.0.0.255 area 0	Přidání sítě a area 0
R5(config-router)#network 192.168.50.0 0.0.0.255 area 0	Přidání sítě a area 0
R5(config-router)#network 192.168.70.0 0.0.0.255 area 0	Přidání sítě a area 0
R5(config-router)#network 192.168.60.0 0.0.0.255 area 0	Přidání sítě a area 0
R6>en	Vstup do privilegovaného módu
R6#conf t	Vstup do konfiguračního modu
R6(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2	Redistribuované statické routování
R6(config)#router ospf 10	Vstup do konfigurace OSPF
R6(config-router)#redistribute static subnets tag 22	Přidání sítě a area 0
R6(config-router)#network 140.10.5.0 0.0.0.255 area 0	Přidání sítě a area 0
R6(config-router)#network 172.16.1.0 0.0.0.255 area 0	Přidání sítě a area 0

Tabulka 5 - OSPF směrovací protokol [16]

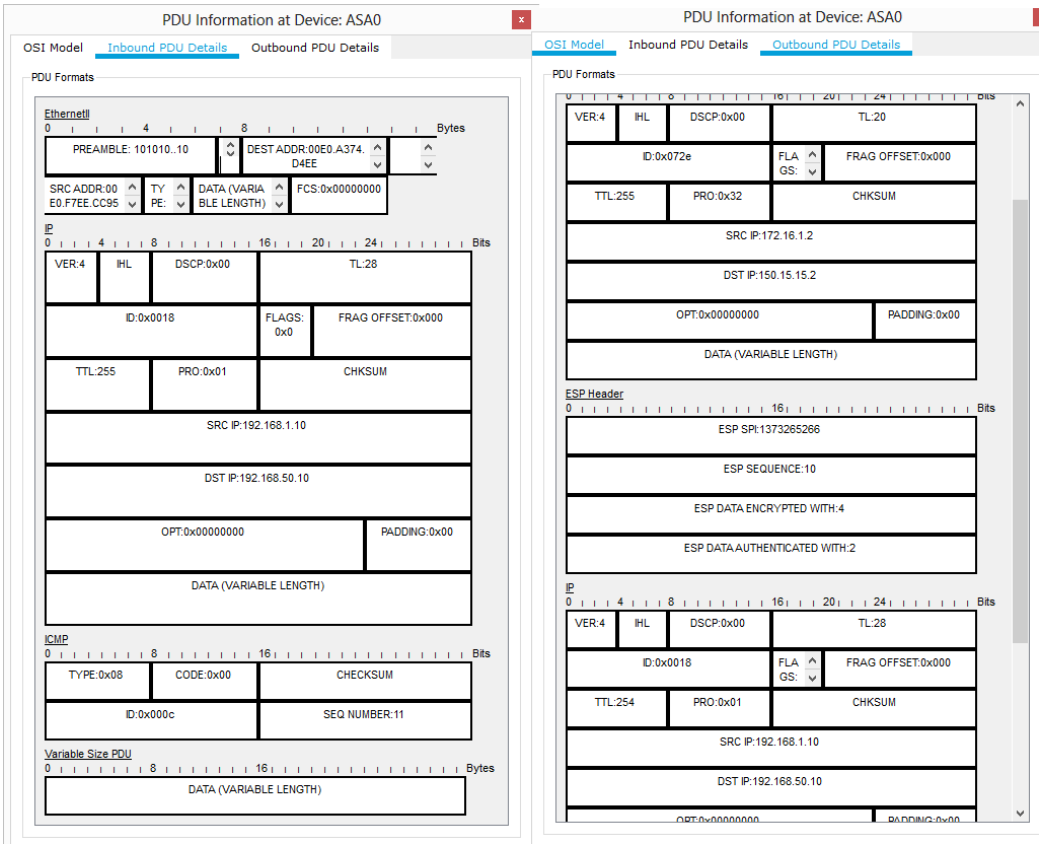
4.1.9 **VPN přenos**

Pro bezpečnou komunikaci mezi modrými zónami bude využit protokol IPsec (IP security). IPsec je sada protokolů k dosažení bezpečných služeb prostřednictvím sítí s přepínáním IP paketů. Pomocí protokolu IPsec lze vytvořit VPN pro vzdálený přístup k síti. VPN je soukromá v tom, že přenos je šifrován, aby data zůstala důvěrná, zatímco jsou přenášena přes veřejnou síť. VPN je vytvořena mezi zařízením ASA a routerem (R5) (Tabulka 6). V nejjednodušším smyslu VPN (Virtuální privátní síť) spojuje dva koncové body, jako jsou dvě vzdálené kanceláře. Cílem této komunikace bude šifrovaný obsah mezi VLAN 10 (zamestnanec) a sítí 192.168.1.0 v modré zóně (Obrázek 27).

R5>en	Vstup do privilegovaného módu
R5#conf t	Vstup do konfiguračního modu
R5(config)#crypto isakmp policy 10	ISAKMP politika
R5(config-isakmp)#authentication pre-share	Metoda autentizace je předem sdílený klíč
R5(config-isakmp)#encryption aes	Šifrování AES
R5(config-isakmp)#hash sha	Algoritmus SHA
R5(config-isakmp)#group 2	Skupina 2
R5(config-isakmp)#lifetime 86400	Životnost
R5(config-isakmp)#exit	Vstup do konfiguračního modu
R5(config)#crypto isakmp key cisco address 172.16.1.2	Určení hesla a adresy
R5(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac	Nastavení šifrování a autentizace IPSec tunelu
R5(config)#crypto map VPN-MAP 10 ipsec-isakmp	Vytvoření šifrovací mapy
R5(config-crypto-map)#set peer 172.16.1.2	Vzdálená IP adresa
R5(config-crypto-map)#set transform-set VPN-SET	Propojení transformační sady
R5(config-crypto-map)#match address VPN-ACL	Konfigurace krypto mapy
R5(config-crypto-map)#exit	Vstup do konfiguračního modu
R5(config)#ip access-list extended VPN-ACL	Vytvoření ACL VPN-ACL
R5(config-ext-nacl)#permit ip 192.168.50.0 0.0.0.255 192.168.1.0 0.0.0.255	Povolení IP adresy
R5(config-ext-nacl)#exit	Vstup do konfiguračního modu
R5(config)#int s0/0/0	Vstup do konfigurace rozhraní s0/0/0
R5(config-if)#crypto map VPN-MAP	Přiřazení šifrovaní mapy
ciscoasa>en	Vstup do privilegovaného módu
Password:	
ciscoasa#conf t	Vstup do konfiguračního modu
ciscoasa(config)#int vlan 1	Vstup do konfigurace rozhraní vlan 1
ciscoasa(config-if)#nameif inside	Určení vnitřního rozhraní
ciscoasa(config-if)#security-level 0	Algoritmus zabezpečení

ciscoasa(config-if)#exit	Vstup do konfiguračního modu
ciscoasa(config)#int vlan 2	Vstup do konfigurace rozhraní vlan 1
ciscoasa(config-if)#nameif outside	Určení všějšího rozhraní
ciscoasa(config-if)#security-level 0	Algoritmus zabezpečení
ciscoasa(config-if)#ip address 172.16.1.2 255.255.255.252	Přidělení IP adresy s maskou
ciscoasa(config-if)#exit	Vstup do konfiguračního modu
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 172.16.1.1	Konfigurace statické trasy rozhraní outside
ciscoasa(config)#crypto ikev1 policy 10	ikev1 politika
ciscoasa(config-ikev1-policy)#authentication pre-share	Metoda autentizace je předem sdílený klíč
ciscoasa(config-ikev1-policy)#encryption aes	Šifrování AES
ciscoasa(config-ikev1-policy)#hash sha	Algoritmus SHA
ciscoasa(config-ikev1-policy)#group 2	Skupina 2
ciscoasa(config-ikev1-policy)#lifetime 86400	Životnost
ciscoasa(config-ikev1-policy)#exit	Vstup do konfiguračního modu
ciscoasa(config)#crypto ikev1 enable outside	Konfigurace IKEV1 politiky na rozhraní outside
ciscoasa(config)#tunnel-group 150.15.15.2 type ipsec-l2l	Vytvoření databáze připojení
ciscoasa(config)#tunnel-group 150.15.15.2 ipsec-attributes	Vytvoření databáze připojení
ciscoasa(config-tunnel-ipsec)#ikev1 pre-shared-key cisco	Definování profilu připojení
ciscoasa(config-tunnel-ipsec)#exit	Vstup do konfiguračního modu
ciscoasa(config)#crypto ipsec ikev1 transform-set VPN-SET esp-aes esp-sha-hmac	Definujte transformaci a nastavení
ciscoasa(config)#crypto map VPN-MAP 10 set peer 150.15.15.2	Nakonfigurujte kryptografii
ciscoasa(config)#crypto map VPN-MAP 10 set ikev1 transform-set VPN-SET	Nakonfigurujte kryptografii
ciscoasa(config)#object network LOCAL-NET	Určuje adresy IP hostitele, podsítě nebo rozsahu
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0	Určení specifické sítě
ciscoasa(config-network-object)#exit	Vstup do konfiguračního modu
ciscoasa(config)#object network REMOTE-NET	Určuje adresy IP hostitele, podsítě nebo rozsahu
ciscoasa(config-network-object)#subnet 192.168.50.0 255.255.255.0	Určení specifické sítě
ciscoasa(config-network-object)#exit	Vstup do konfiguračního modu
ciscoasa(config)#access-list VPN-ACL extended permit ip object LOCAL-NET object REMOTE-NET	Určení ACL politiky
ciscoasa(config)#crypto map VPN-MAP 10 match address VPN-ACL	Určení šifrovací mapy
ciscoasa(config)#crypto map VPN-MAP interface outside	Určení šifrovací mapy a rozhraní
ciscoasa(config)#dhcpd address 192.168.1.10-192.168.1.30 inside	Vytvoření DHCP v rozsahu
ciscoasa(config)#dhcpd dns 192.168.200.10 interface inside	Nastavení DNS pro DHCP
ciscoasa(config)#dhcpd option 3 ip 192.168.1.1	Nastavení
ciscoasa(config)#dhcpd enable inside	Povolení DHPC šíření do vnitřní sítě

Tabulka 6 - Konfigurace VPN přenosu [16]



Obrázek 27 - Ověření VPN a šifrování paketů [16]

4.1.10 **NAT**

NAT (Network Address Translation) je navržen pro zachování IP adres. Umožňuje připojení privátních sítí IP k Internetu. NAT má mnoho využití, ale jeho primárním využitím je šetření veřejných IPv4 adres. NAT má výhodu v přidávání stupně ochrany soukromí a zabezpečení do sítě, protože skrývá interní adresy IPv4 z privátních sítí. NAT využívá třech typů překladu, které jsou statický překlad adres, dynamický překlad adres a port address translation (PAT). IP adresy, které jsou v modré oblasti se překládají na veřejné adresy pomocí procesu NAT (Network Address Translation). Hlavní roli určuje router na základě konfigurace . V konfiguraci (Tabulka 7) jsou výlučně překládány sítě 192.168.60.0 a 192.168.70.0. Síť 192.168.99.0 (VLAN 99) slouží jenom ke správě zařízení routeru (R5) a switche (SW4) v modré oblasti. Síť 192.168.50.0 (VLAN 10) má šifrovanou komunikaci, Viz. úloha 4.1.9. Sítě 192.168.50.0 a 192.168.60.0 jsou překládaný na veřejnou IP (Obrázek 28) adresu 150.15.15.2 v rozhraní Serial0/0/0 na routeru R5 (Obrázek 29). NAT je nakonfigurováno pomocí dynamické metody.

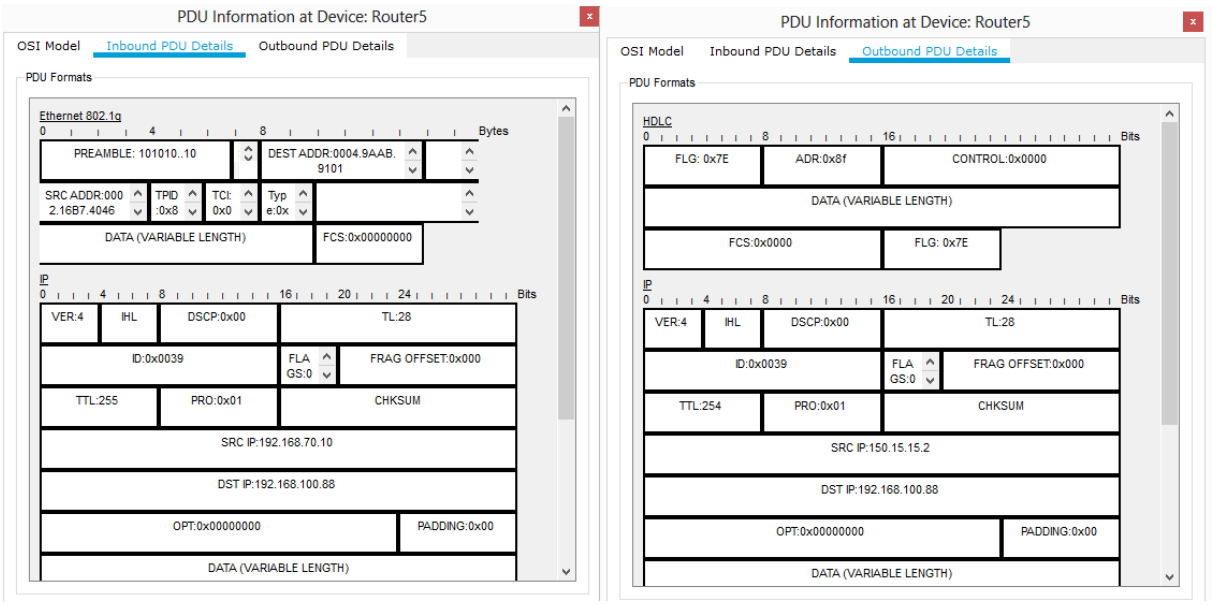
R5>en	Vstup do privilegovaného módu
R5#conf t	Vstup do konfiguračního modu
R5(config)#ip access-list extended VLAN30	Vytvoření ACL pravidla
R5(config-ext-nacl)#permit ip 192.168.70.0 0.0.0.255 any	Přidání pravidla
R5(config-ext-nacl)#exit	Vstup do konfiguračního modu
R5(config)#ip nat inside source list VLAN30 interface Serial0/0/0 overload	Definuje PAT
R5(config)#ip access-list extended VLAN20	Vytvoření ACL pravidla
R5(config-ext-nacl)#permit ip 192.168.60.0 0.0.0.255 any	Přidání pravidla
R5(config-ext-nacl)#exit	Vstup do konfiguračního modu
R5(config)#ip nat inside source list VLAN20 interface Serial0/0/0 overload	Definuje PAT
R5(config-if)#int Serial0/0/0	Vstup do konfigurace rozhraní s0/0/0
R5(config-if)#ip nat outside	Identifikace NATu vnější sítě
R5(config-if)#int gig0/0.20	Vstup do konfigurace rozhraní gig0/0.20
R5(config-subif)#ip nat inside	Identifikace NATu vnitřní sítě
R5(config-subif)#int gig0/0.30	Vstup do konfigurace rozhraní gig0/0.30
R5(config-subif)#ip nat inside	Identifikace NATu vnitřní sítě

Tabulka 7 - Konfigurace NAT na R5 [16]

```
R5#show ip nat
R5#show ip nat tr
R5#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 150.15.15.2:22    192.168.60.10:22   192.168.100.10:22  192.168.100.10:22
icmp 150.15.15.2:33    192.168.70.10:33   192.168.100.10:33  192.168.100.10:33
icmp 150.15.15.2:34    192.168.70.10:34   150.150.10.1:34    150.150.10.1:34
udp 150.15.15.2:1024   192.168.70.10:1025 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1025   192.168.60.10:1025 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1026   192.168.60.10:1026 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1027   192.168.60.10:1027 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1028   192.168.60.10:1028 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1029   192.168.60.10:1029 192.168.200.10:53  192.168.200.10:53
udp 150.15.15.2:1030   192.168.60.10:1030 192.168.200.10:53  192.168.200.10:53
tcp 150.15.15.2:1024   192.168.70.10:1025 192.168.100.88:80  192.168.100.88:80
tcp 150.15.15.2:1025   192.168.60.10:1025 192.168.200.10:80  192.168.200.10:80
tcp 150.15.15.2:1026   192.168.60.10:1026 192.168.100.88:80  192.168.100.88:80
tcp 150.15.15.2:1027   192.168.60.10:1027 192.168.100.88:80  192.168.100.88:80
tcp 150.15.15.2:1028   192.168.60.10:1028 192.168.100.88:80  192.168.100.88:80
tcp 150.15.15.2:1029   192.168.60.10:1029 192.168.100.88:80  192.168.100.88:80

R5#
```

Obrázek 28 - Překlad NAT [16]



Obrázek 29 - Překlad NAT v paketu [16]

4.1.11 **Zabezpečení 2. vrstvy**

Cílem této úlohy je zabezpečení 2. vrstvy referenčního modelu ISO/OSI. Na síť může dojít k několika útokům. V této úloze se bude předpokládat možnost MAC útoku, DHCP útoku a VLAN útoku. Za účelem zamezení útoků na protokol spaning tree, je nutné tento protokol ochránit, aby nemohlo dojít ke smyčkám v LAN síti. Nejefektivnějším způsobem zabezpečení mnoha útoků je používat služby switchport port-security. Optimální obecné řešení proti útokům je vypnutí nevyužitých portů na daném zařízení. Pro ochranu DHCP protokolu slouží příkaz sw4(config-if)#ip dhcp snooping trust na rozhraní, kde je protokol přijímán (Tabulka 8).

sw4(config)#spanning-tree mode rapid-pvst	Zapnutí rapid spaning tree
sw4(config)#spanning-tree portfast bpduguard default	Ochrana portů proti jinému switchi
sw4(config)#interface range fa0/1-24	Vstup do konfigurace rozhraní fa 0/1 až fa0/24
sw4(config-if-range)#switchport mode access	Přepnutí portu do přístupového modu
sw4(config-if-range)#switchport port-security	Zapnutí port security
sw4(config-if-range)#switchport port-security maximum 1	Zvolení počet adres
sw4(config-if-range)#switchport port-security mac-address sticky	Ukládá dynamicky mac adresy
sw4(config-if-range)#switchport port-security violation shutdown	Při porušení vypne port
sw4(config-if-range)#interface range gig0/1-2	Vstup do konfigurace rozhraní gig0/1 až gig0/2
sw4(config-if-range)#shutdown	Vypnutí rozhraní
sw4(config-if-range)#interface range fa0/6-24	Vstup do konfigurace rozhraní fa 0/6 až fa0/24
sw4(config-if-range)#shutdown	Vypnutí rozhraní
sw4(config-if-range)#int fa0/1	Vstup do konfigurace rozhraní fa0/1
sw4(config-if)#ip dhcp snooping trust	Nastavení důvěryhodnosti portu pro DHCP
sw3(config)#interface range fa0/1-24	Vstup do konfigurace rozhraní fa 0/1 až fa0/24
sw3(config-if-range)#switchport mode access	Přepnutí portu do přístupového modu
sw3(config-if-range)#switchport port-security	Zapnutí port security
sw3(config-if-range)#switchport port-security maximum 1	Zvolení počet adres
sw3(config-if-range)#switchport port-security mac-address sticky	Ukládá dynamicky mac adresy
sw3(config-if-range)#switchport port-security violation shutdown	Při porušení vypne port
sw3(config-if-range)#interface range gig0/1-2	Vstup do konfigurace rozhraní gig0/1 až gig0/2
sw3(config-if-range)#shutdown	Vypnutí rozhraní
sw3(config-if-range)#interface range fa0/3-24	Vstup do konfigurace rozhraní fa 0/3 až fa0/24
sw3(config-if-range)#shutdown	Vypnutí rozhraní
sw3(config-if-range)#int fa0/1	Vstup do konfigurace rozhraní fa0/1
sw3(config-if)#ip dhcp snooping trust	Nastavení důvěryhodnosti portu pro DHCP

Tabulka 8 - Konfigurace zabezpečení 2. vrstvy [16]

4.1.12 **Zabezpečení 3. vrstvy**

Seznamy ACL lze použít ke zmírnění mnoha síťových hrozeb, jako jsou podvody s adresami IP a útoky typu DoS. Účinnou strategií pro zmírnění útoků je výslovně povolit pouze určité typy komunikace prostřednictvím brány firewall. V úloze bude zabráněn přístup počítačů v síti VLAN 20 a 30 na webový portál www.thepiratebay.org, který se nachází na serveru 2 (192.168.100.88). Bude simulováno, že Národní úřad pro kybernetickou a informační bezpečnost podal prohlášení, že tento server je potenciální hrozbou pro Českou republiku. Na základě doporučení bude tato IP adresa filtrována pomocí seznamu oprávnění ACL (access control list) na routeru (R5) (Tabulka 9).

R5(config)#access-list 102 deny tcp 192.168.70.0 0.0.0.255 host 192.168.100.88 eq www	Blokování webové stránky ip adresy 192.168.100.88
R5(config)#access-list 102 permit ip 192.168.70.0 0.0.0.255 any	Povolení všech IP adress daného rozsahu
R5(config)#access-list 103 deny tcp 192.168.60.0 0.0.0.255 host 192.168.100.88 eq www	Blokování webové stránky ip adresy 192.168.100.88
R5(config)#access-list 103 permit ip 192.168.60.0 0.0.0.255 any	Povolení všech IP adress daného rozsahu
R5(config)#interface GigabitEthernet0/0.20	Vstup do konfigurace rozhraní gig0/0.20
R5(config-subif)#ip access-group 103 in	Aktivace pravidla 103
R5(config-subif)#interface GigabitEthernet0/0.30	Vstup do konfigurace rozhraní gig0/0.30
R5(config-subif)#ip access-group 102 in	Aktivace pravidla 102
ciscoasa(config)#access-list 103 deny tcp 192.168.1.0 255.255.255.0 host 192.168.100.88 eq www	Blokování webové stránky ip adresy 192.168.100.88
ciscoasa(config)#access-list 103 permit ip 192.168.1.0 255.255.255.0 any	Povolení všech IP adress daného rozsahu
ciscoasa(config)#access-group 103 in interface inside	Aktivace pravidla 103 na daném rozhraní do vnitř

Tabulka 9 - Konfigurace zabezpečení 3. vrstvy [16]

4.1.13 **Nastavení hesel**

Poslední úloha byla zaměřena na zabezpečení přístupu pomocí hesel, AAA, SSH. V této úloze bude realizace lokální AAA. Je využita služba login on-failure log, která má za úkol sledovat počet pokusů o přihlášení. Pro případný útok brute force je použit příkaz R5(config)#login block-for 10 attempts 3 within 60. Router R5 a R6 mají stejnou konfiguraci (Tabulka 11). Tabulka (Tabulka 10) jednotlivých hesel pro dané routery a switche.

	AAA		Enable
	uživatel	heslo	heslo
R5	adminr5	adminr5	cisco
R6	adminr6	adminr6	cisco
ASA	adminasa	adminasa	cisco
SW4	adminsw4	adminsw4	cisco
SW3	admins3	adminsw3	cisco

Tabulka 10 - Tabulka hesel [16]

R5>en	Vstup do privilegovaného módu
R5#conf t	Vstup do konfiguračního modu
R5(config)#enable secret level 15 cisco	Heslo do konfiguračního modu. Šifrované
R5(config)#username adminr5 secret adminr5	Vytvoření uživatele a hesla
R5(config)#aaa new-model	Zapnutí služby AAA
R5(config)#aaa authentication login default local	Nastavení autentizace
R5(config)#line console 0	Vstup do konfigurace rozhraní console
R5(config-line)#login authentication default	Přidělený definovaný seznam "default"
R5(config-line)#exit	Vstup do konfiguračního modu
R5(config)#ip domain-name r5.cz	Jméno domény
R5(config)#crypto key generate rsa 1024	Vytvoření certifikátu
R5(config)#aaa authentication login SSH local	Nastavení autentizace
R5(config)#line vty 0 15	Vstup do konfigurace rozhraní Virtual teletype
R5(config-line)#login authentication SSH	Přidělený definovaný seznam "SSH"
R5(config-line)#transport input SSH	Vstup pouze pro SSH
R5(config-line)#exit	Vstup do konfiguračního modu
R5(config)#login on-failure log	Vytvoření záznamu po neúspěšném přihlášení
R5(config)#login on-success log	Vytvoření záznamu po úspěšném přihlášení
R5(config)#login block-for 10 attempts 3 within 60	Ochrana proti Brute Force útokům
sw4>en	Vstup do privilegovaného módu
sw4#conf t	Vstup do konfiguračního modu
sw4(config)#enable secret cisco	Heslo do konfiguračního modu. Šifrované
sw4(config)#username adminsw4 secret adminsw4	Vytvoření uživatele a hesla
sw4(config)#line console 0	Vstup do konfigurace rozhraní console
sw4(config-line)#login local	Lokální uživatel
sw4(config-line)#line vty 0 15	Vstup do konfigurace rozhraní Virtual teletype
sw4(config-line)#login local	Lokální uživatel
sw4(config-line)#transport input ssh	Vstup pouze pro SSH
ciscoasa(config)#enable password cisco level 15	Heslo do konfiguračního modu. Šifrované
ciscoasa(config)#username adminasa password adminasa	Vytvoření uživatele a hesla
ciscoasa(config)#aaa authentication ssh console local	Používání místní databáze pro SSH a konzoli
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside	Povolená sít z vnější pro SSH
ciscoasa(config)#ssh 172.16.1.0 255.255.255.0 outside	Povolená sít z vnitřní sítě pro SSH

Tabulka 11 - Konfigurace nastavení hesel [16]

4.2 Cisco laboratoř - reálné řešení

Reálné testování navrhnuté konfigurace počítačové sítě z 4.1 bude probíhat v laboratoři síťových a internetových technologií (LSIT) (Obrázek 30). Učebna D326 se nachází na Provozně ekonomické fakultě v Praze. V laboratoři jsou realizovány kurzy CISCO a disponuje CISCO hardware pro realizaci. Pro konfiguraci navrhnuté počítačové sítě byl využit následující hardware (Tabulka 12).

Zařízení	Počet	Operační systém - verze
Cisco 2811	6	ISO 12.4(13b)
Cisco Catalyst 2960	5	ISO 15.0(2)SE
Cisco ASA 5505	1	ISO 9.4.2
Dell Inspiron SE 7720	1	Windows Server 2019
Dell Inspiron SE 7720	1	Windows 8
Acer Aspire One D255	1	Windows 7 Starter

Tabulka 12 - Přehled zařízení pro konfiguraci [16]

Obrázek 30 - Učebna D326 [32]

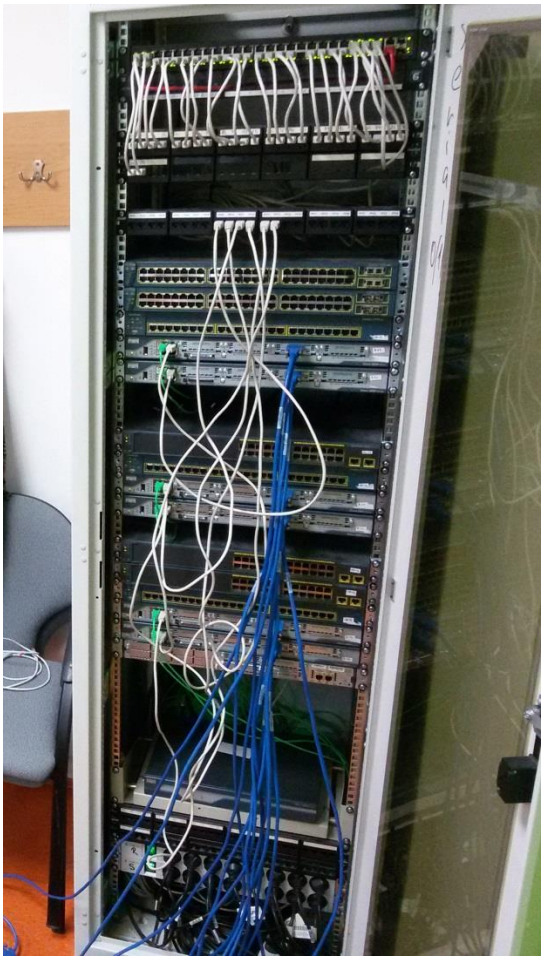
4.2.1 **Postup při využití laboratoře**

V kapitole 4.1 byla provedena simulace v software Cisco Packet Tracer, kde byla navrhnuta počítačová topologie. V praxi však není žádoucí spoléhat se na tento software, protože nemůže vynahradit skutečné chování zařízení (hardware). Je nezbytně nutné tyto konfigurace prověřit za skutečných podmínek. Postup tvorby v následujících bodech:

- Propojení zařízení pomocí kabeláže
- Nastavení jednotlivých zařízení
- Ověření fungování topologie
- Skenování sítě

4.2.2 **Propojení zařízení pomocí kabeláže**

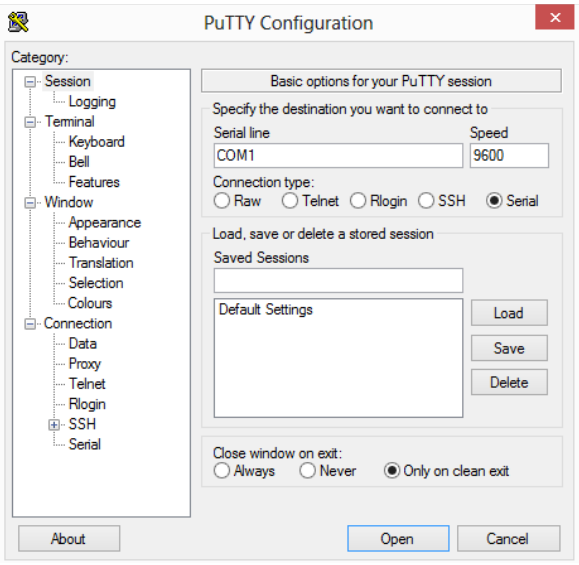
Zapojení kabeláže bylo realizováno pomocí síťových kabelů typu CAT5E UTP a Cisco Smart Serial Cable. Síťové kabely typu CAT5E UTP byly využity k propojení veškerých portů, které zahrnují Fast Ethernet a Gigabitový Ethernet. Kabely Cisco Smart Serial Cable byly využity jenom pro propojení se serial interface, které byly mezi routery R2,R4,R5.



Obrázek 31 - Cisco rack [16]

4.2.2.1 **PuTTY**

PuTTY je bezplatný open-source pro emulaci terminálu vyvinutý původně pro platformu Windows. Podporuje několik síťových protokolů včetně SCP , SSH a Telnet. Může také posloužit k připojení pomocí sériového portu [28]. Všechna komunikace během konfigurace s routery, switchy a ASA byla realizována pomocí klientu PuTTY. Pomocí tohoto klientu bylo možné úspěšně nakonfigurovat všechny zařízení od společnosti CISCO. Pro úspěšné propojení byl zapotřební kabel Cisco CAB-CONSOLE-RJ45 (Obrázek 33) a počítač s předinstalovaným klientem PuTTY (Obrázek 32). Software byl stažen bezplatně z webových stránek www.putty.org. Byl využíván na Dell Inspiron SE 7720 s operačním systémem Windows 8.



Obrázek 32 - PuTTY [16]

Obrázek 33 - Cisco CAB-CONSOLE-RJ45 [29]

4.2.3 **Konfigurace jednotlivých zařízení**

Konfigurace jednotlivých zařízení byla čerpána z kapitoly 4.1.6 až 4.1.13 pro ověření bezpečnosti sítové infrastruktury. Pro jednotlivá zařízení byl využit textový dokument cisco_konfigurace.txt pro rychlejší nastavení, který se nachází v příloze na CD. Funkcí tohoto textového souboru je rychlejší nastavení CISCO, které vychází z návrhu Cisco Packet Traceru. Konfigurace byla úspěšně nastavena a zajistila fungování navrhnuté počítačové topologie z předchozích kapitol.

Byly využity dva počítače Dell Inspiron SE 7720 (Obrázek 34) s odlišnými operačními systémy. Jeden slouží k nastavení CISCO zařízení a simulaci koncového zařízení pro ověření komunikace (blokace, ping). Druhý počítač Dell Inspiron SE 7720 slouží pro vytvoření DNS serveru. Úkolem bylo vytvoření stránky www.thepiratebay.org a následná blokace pomocí ACL na routeru (R5). Poslední počítač Acer Aspire One D255 s operačním systémem Windows 7 Starter slouží jako koncový klient v modré oblasti, kde se nachází CISCO ASA. Počítač Acer Aspire One D255 nese označení PC2 (Obrázek 26).

Obrázek 34 - Dell inspiron 7720 [16]

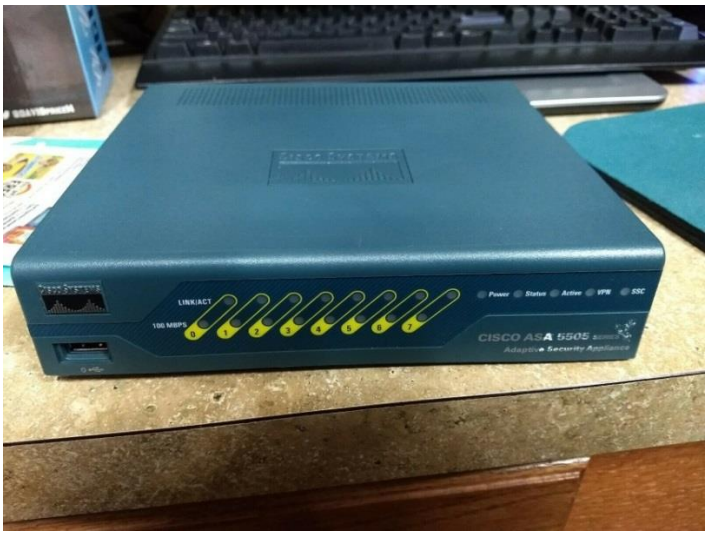
4.2.4 **Ověření fungování topologie**

Pro ověření správného fungování počítačové sítě je použit ping. Používá se běžně pro ověření komunikace mezi jednotlivými zařízeními nebo v tomto případě je to jediný nástroj pro ověření. Zdrojové zařízení odešle žádost o ping, pokud komunikace dosáhne cíle, pak cíl pošle odpověď ping. Zdrojové zařízení přijímá odpověď z cíle, ověřuje komunikaci a vypočítává množství zpoždění. Pro ověření přidělení DHCP bude připojen počítač do sítě a následně odešle DHCPREQUEST. Pro ověření bezpečnosti připojení VPN je využit bezplatný software WireShark, který slouží k zachycení paketů v počítačové síti. Poslední ověření je blokace webové stránky. Bylo zjištěno, že ne vždy chce router komunikovat s počítačem, i přestože byl dobře nastaven. Často bylo nutné pro fungování počítač restartovat.

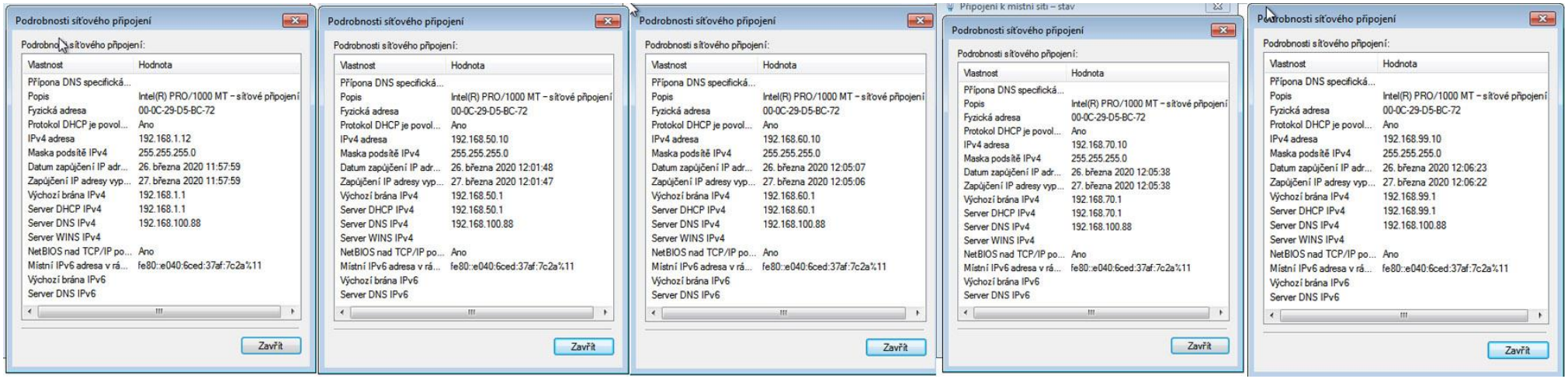
4.2.4.1 **Přidělení DHCP**

Počítač Dell Inspiron SE 7720 (Windows 8) byl následně připojen postupně do VLAN 10,20,30,99 v modré oblasti a pomocí něho je ověřováno, zda poskytne IP adresu od DHCP serveru (Obrázek 36), který je nakonfigurován na routeru (R5). Bylo taky ověřená funkční komunikace mezi počítačem a routerem (Obrázek 37). K propojení mezi počítačem a switchem (SW4) slouží sítový kabel CAT5E UTP. Počítač Acer Aspire One D255 je připojen síťovým kabelem do switche (SW3) a ověřuje požadavek na DHCP server od zařízení CISCO ASA (Obrázek 35).

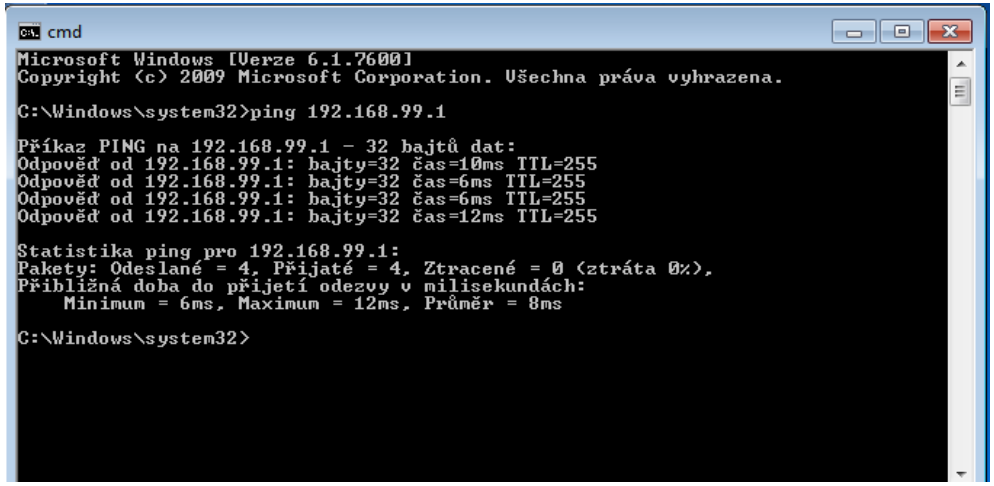
Přidělování IP adresy od ASA zařízení trvalo déle než u ostatních VLAN. Nakonec všechny IP adresy z daných VLAN byly úspěšně přiděleny.



Obrázek 35 - Cisco ASA 5505 [16]



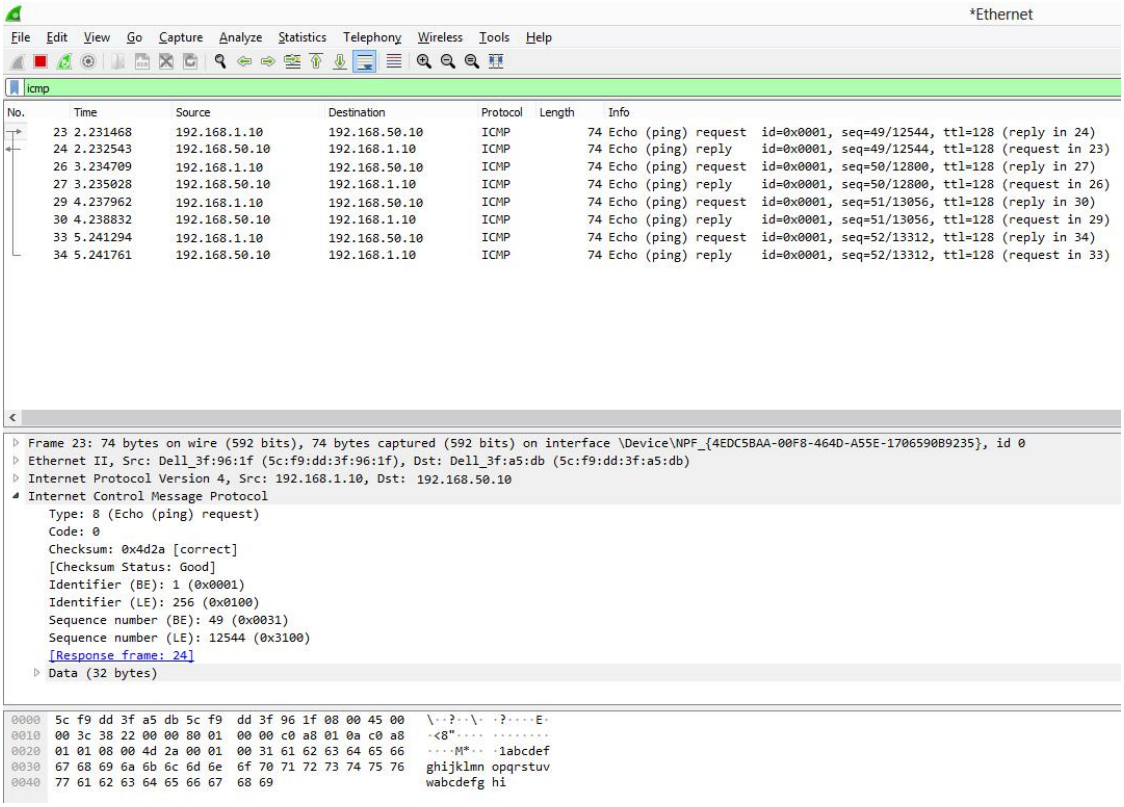
Obrázek 36 - Ověření DHCP [16]



Obrázek 37 - Ověření připojení [16]

4.2.4.2 **Ověření VPN zabezpečení spojení**

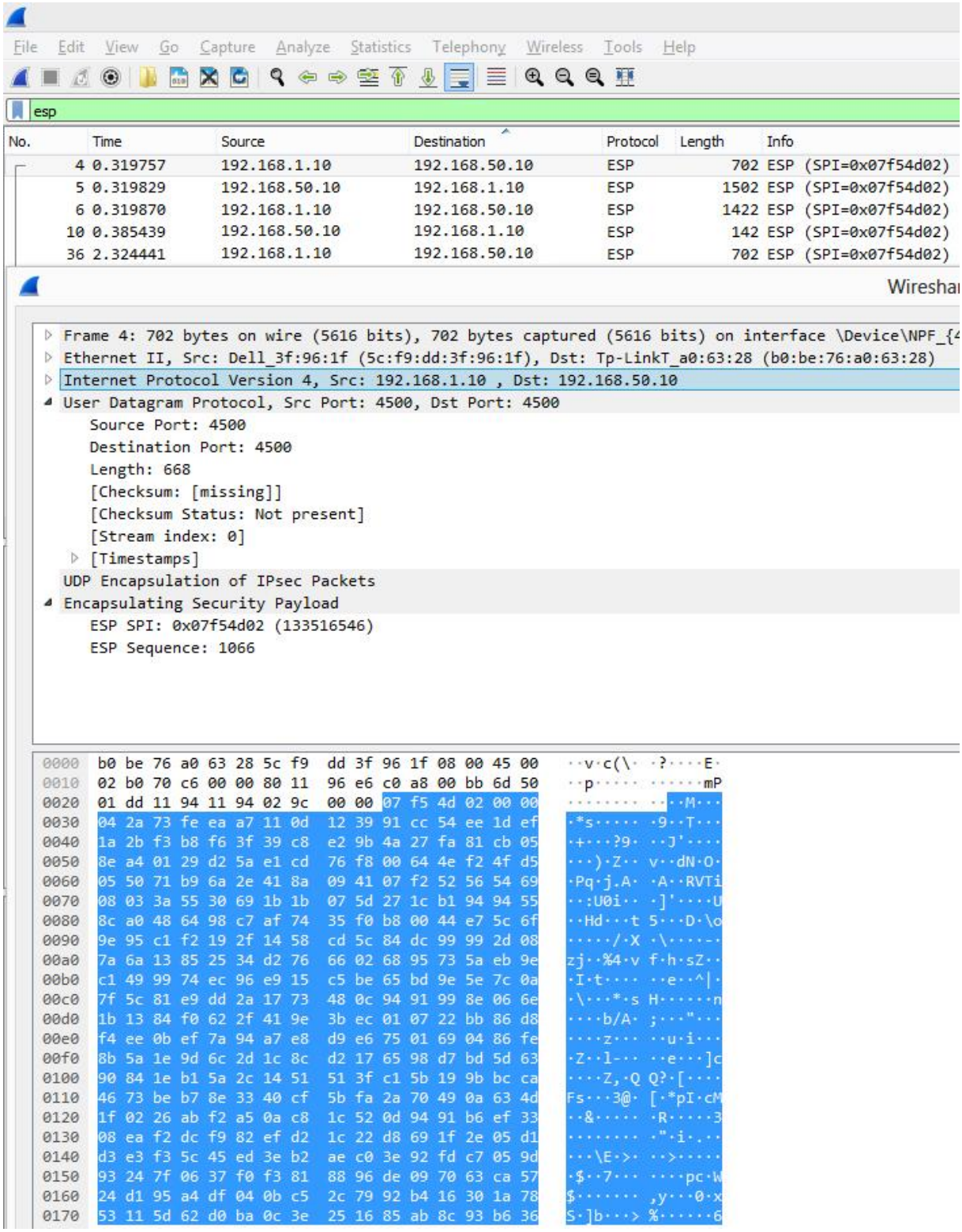
Pro ověření byl využit program WireShark. Tento program dokáže odchytávat procházející pakety a ověřit, zda VPN funguje. Pro ověření byl využít počítač Dell Inspiron SE 7720 (Windows Server 2019), který bude připojen mezi routery R4 a R6. Mezi těmito routery se nachází Cisco Catalyst 2960. Toto propojení neodpovídá obrázku č. 22. Cisco Packet Tracer obsahuje trasování paketů. Pro ověření v reálném prostření je využit tento způsob. Zda není komunikace VPN zapnutá, a tak útočník zachytit pakety a nich zjistit informace. Příkladem toho mohou být hesla k přihlášení. Byla ověřená komunikace pomocí protokolu ICMP z IP adresy 192.168.1.10 na adresu 192.168.50.10 (Obrázek 38).



Obrázek 38 - Wireshark - ping [16]

Po zapnutí funkce VPN už nelze vyčíst informace. Pakety jsou šifrované pomocí protokolu ESP(Encapsulating Security Payload) a pro útočníka je obtížně to rozšifrovat. Protokol ESP poskytuje paketům důvěrnost a také volitelně poskytuje původní autentizaci, kontrolu integrity dat a ochranu proti zpětným dotazům. Protokol ESP využívá k šifrování symetrický klíč, který obě komunikující strany používají k šifrování a dekódování vyměňovaných dat. Z odchycených paketů již zjistit, jakého typu je probíhající komunikace. Služba VPN byla nastavena úspěšně a šifrovaná komunikace funguje.

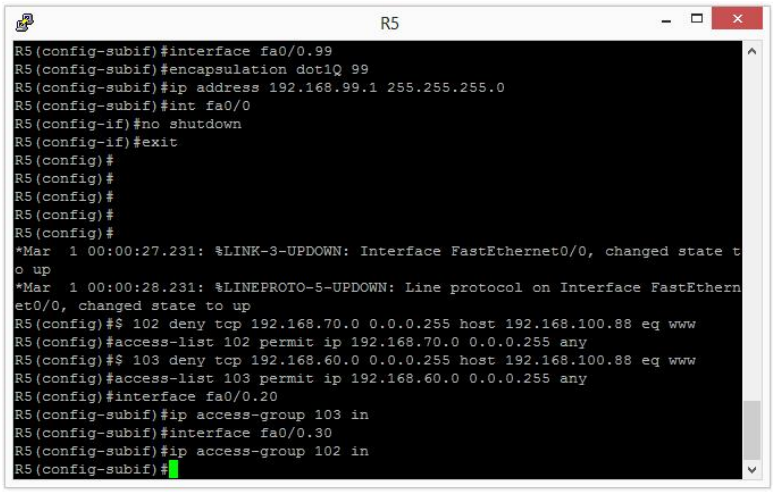
Byla ověřená šifrovaná komunikace pomocí protokolu ESP z IP adresy 192.168.1.10 na adresu 192.168.50.10 (Obrázek 39).



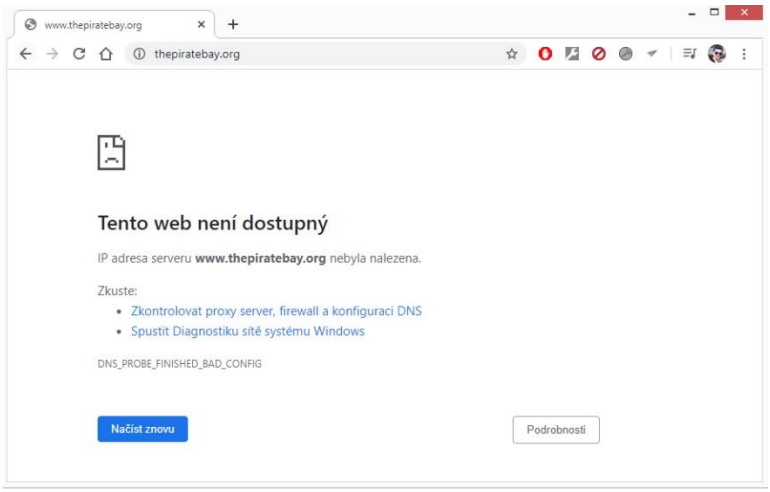
Obrázek 39 - Wireshark - ESP [16]

4.2.4.3 **Blokace webové stránky pomocí firewallu**

Na počítači Dell Inspiron SE 7720 (Windows Server 2019) funguje služba DNS, která poskytuje všem koncovým zařízením DNS adresu. Počítač byl připojen k routeru (R3) pomocí kabelu CAT5E UTP. Jeho IP adresa je 192.168.100.88. Počítač poskytuje také server pro webovou stránku www.thepiratebay.org. Na routeru (R5) byla provedena blokace zmíněné webové stránky pomocí seznamu pravidel (ACL) pro filtrovaní paketů. Seznam pravidel (ACL) je následně vypsán na obrázku (Obrázek 40). Je využit extended ACL (rozšířené ACL) příkaz, který používá čísla 100-199.Příkaz access-list 102 slouží pro VLAN 30 a access-list 103 pro VLAN 20, následně byla aplikována pravidla na přístupné pod-rozhraní (sub interface) příkazem *ip acces-group*. Bylo ověřeno, že nebude možné na tuto stránku přistoupit ze sítí VLAN 20 a 30 v modré oblasti přes webový prohlížeč (Obrázek 41).



Obrázek 40 - Putty nastavení ACL [16]



Obrázek 41 - Blokace webové stránky [16]

4.2.5 **Skenování sítě**

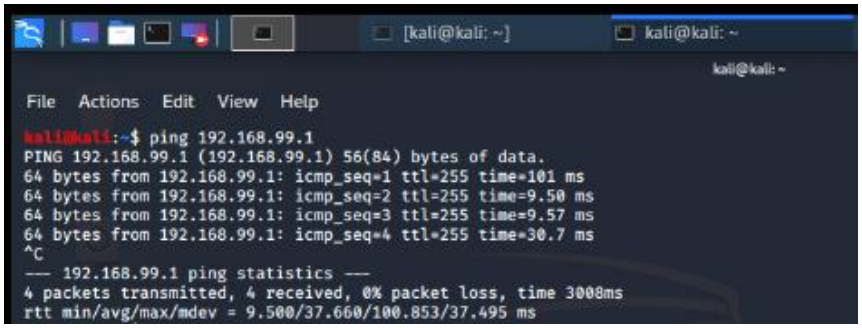
Pro odhalení slabin byl využit nástroj (příkaz) NMap (Network Mapper). Umožnuje objevovat jednotlivé prvky v počítačové síti ve které je připojen. Detekuje otevřené porty v síti a zobrazuje jednotlivé názvy a verze běžících služeb. NMap je využíván pro ověření zabezpečení sítě. Ovládání nástroje NMap spočívá pouze v použití příkazového řádku pomocí příkazů „nmap“ a parametru, který definuje oblast prohledávání. V našem případě se jedná o IP adresu daného routeru (R5) 192.168.99.1. Možné příkazy jsou prezentovány v následující tabulce (Tabulka 13).

Naskenujte jednu IP	nmap x.x.x.x
Naskenujte hostitele	nmap *„www.seznam.cz“*
Skenujte řadu IP adres	nmap x.x.x.x-y.y
Prohledání podsítě	nmap x.x.x.0/yy
Naskenujte cíle z textového souboru	nmap -iL *„seznam.txt“*

Tabulka 13 - Sada příkazu NMap [16]

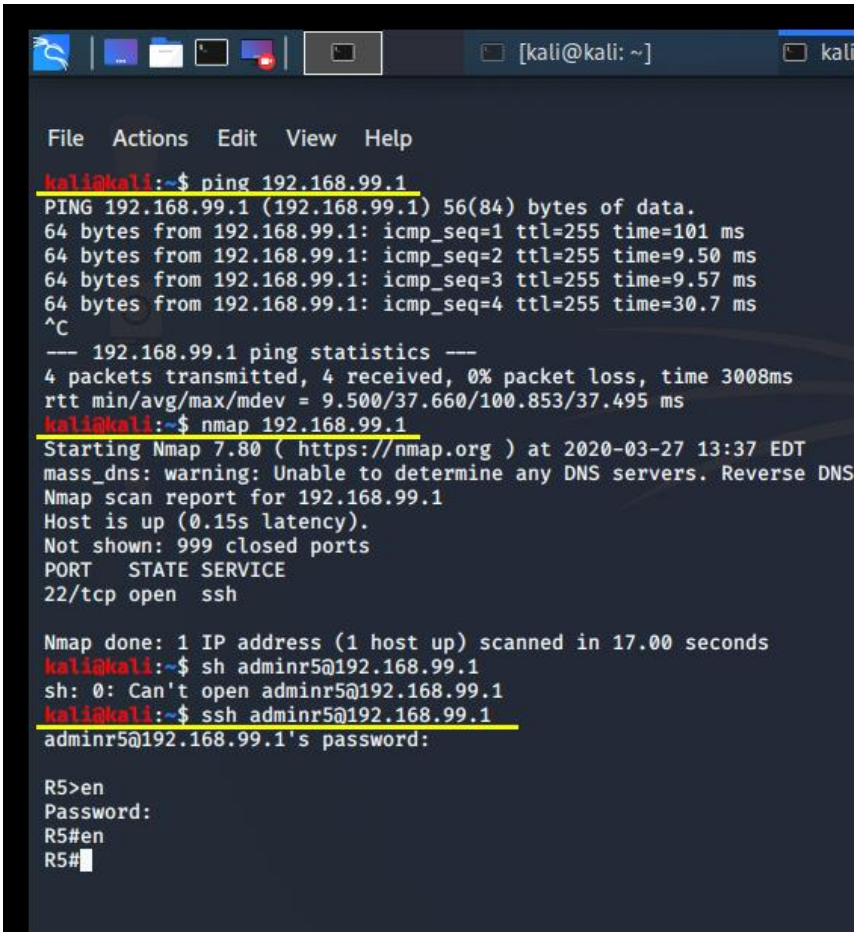
Nástroj NMap je možné využít pomocí operačního systému Kali Linux. Kali Linux je linuxová distribuce odvozená od Debianu, navržená pro digitální forenzní analýzu a penetrační testy. Kali Linux patří do rodiny tzv. open-source operačních systému a je možné ho využívat zdarma. Byl stažen pod verzí kali-linux-2020-1-vmware-amd64-7z ze stránky https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download. Pro jeho fungování bylo zapotřebí nainstalovat VMware Workstation 15 Pro (verze 15.5.2 Pro) na počítači Dell Inspiron SE 7720 (Windows 8), který podporuje virtualizaci. VMware Workstation je virtualizační program (software), který umožňuje spustit na jednom počítači více virtuálních strojů.VMware Workstation podléhá licenci EULA (End User License Agreement). Pro účely diplomové práce byla využitá bezplatná 30 denní trial verze.

Počítač Dell Inspiron SE 7720 (Windows 8) byl zapojen jako počítač PC4 (192.168.99.10) z navrhnuté topologie do switche Cisco Catalyst 2960 pomocí kabelu CAT5E UTP. Cisco Catalyst 2960 představuje switch (SW4) z navrhnuté topologie. Nejprve bylo ověřeno pomocí pingu, zda router (R5) a Kali linux spolu komunikují, což je vidět na obrázku (Obrázek 42).



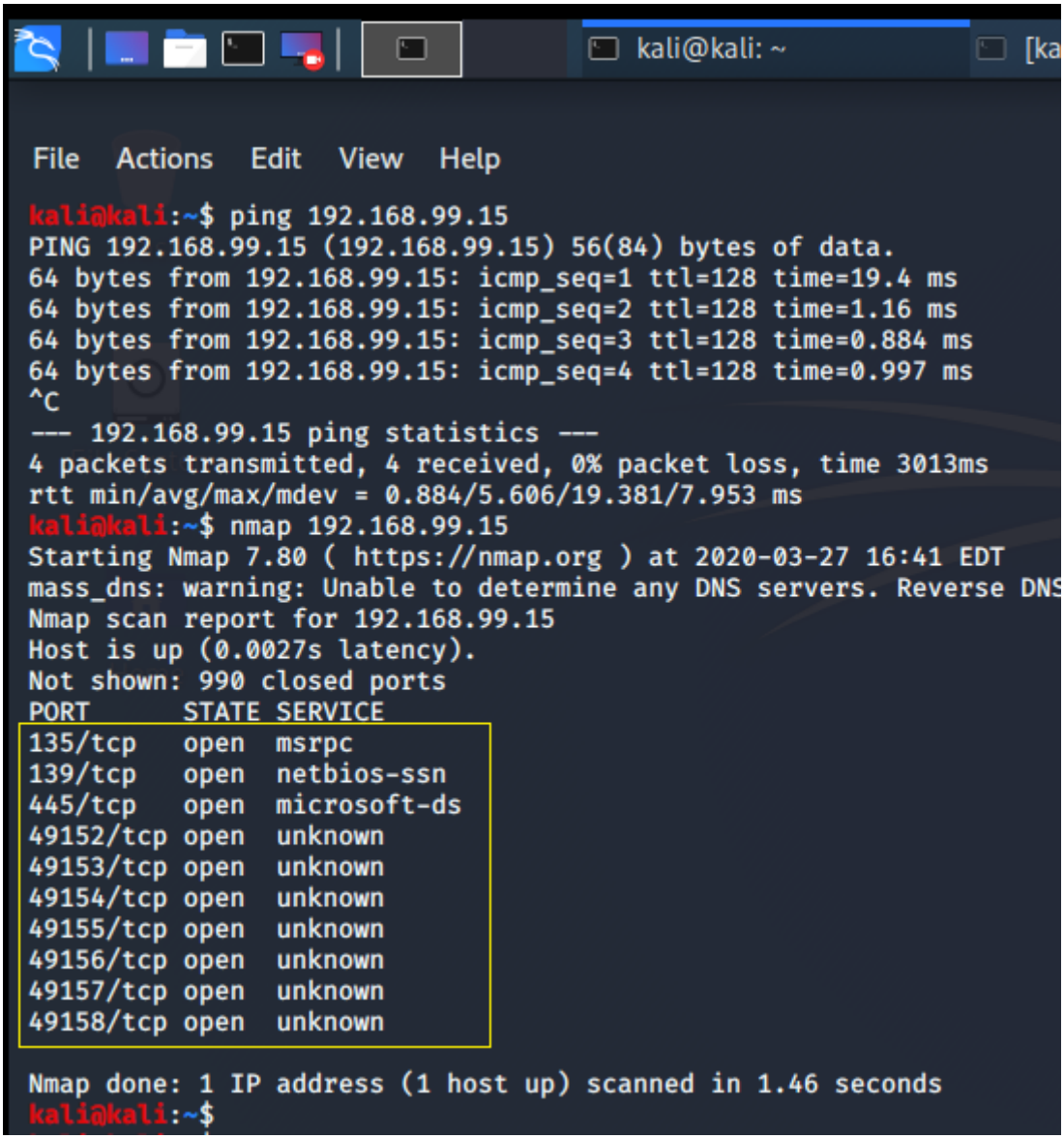
Obrázek 42 - Kali Linux ověření spojení [16]

Následně byl využit nástroj NMap, který byl zadán do příkazové řádky jako „nmap 192.168.99.1“. Bylo zjištěno, že SSH port je otevřený a je možné se k němu připojit. Byl ověřen protokol SSH z Kali Lunuxu pro připojení šifrované komunikace pomocí příkazu „ssh adminr5@192.168.99.1“. První slovo prezentuje protokol SSH, následuje heslo „adminr5“, které je nastaveno na routeru (R5) pro protokol SSH a poslední je IP adresa, na kterou je protokol adresován. Připojení pomocí protokolu SSH bylo úspěšně navázáno, což je demonstrováno na obrázku (Obrázek 43).



Obrázek 43 - Kali Linux - skenování sítě [16]

Pro demonstraci ověření více portů a nástroje NMap byl zapojen počítač Dell Inspiron SE 7720 (Windows Server 2019) do sítě VLAN 99 pod ID adresou 192.168.99.15, na kterém je nainstalovaný server. Bylo nutné na switchu (SW4) otevřít jeden port pro tento počítač, aby byla umožněna komunikace. Výsledek je možné vidět na obrázku (Obrázek 44). Je ověřeno, že všechny porty ve žlutém rámečku jsou otevřené. Mohou být využity k možnému útoku.



Obrázek 44 - Kali linux - skenování portů serveru [16]

4.3 Ekonomické zhodnocení projektu

U zhodnocení je nutné brát v potaz, že počítačová síť byla konfigurována v počítačové učebně D326. Celkové náklady se mohou lišit od skutečné sítě, která může fungovat v praxi. V následujícím zhodnocení budou blíže charakterizovány dvě kategorie možné realizace.

Cisco počítačová topologie

Tabulka (Tabulka 14) vyjadřuje cenu hardwarových komponentů, které byly využity pro návrh dané počítačové sítě. V tabulce nejsou započítané osobní počítače.

Zařízení	Množství	Cena
Cisco 2811	6	540 960 Kč
Cisco Catalyst 2960	5	196 420 Kč
Cisco ASA 5505	1	15 327 Kč
Cena celkem		**752 707 Kč**

Tabulka 14 - Ekonomické zhodnocení Cisco [1, 2]

MikroTik počítačová topologie

Alternativní varianta (Tabulka 15) sestává pomocí stejnakých sítových zařízení, které mohou sloužit pro navrhnutou topologii. Cílem této varianty je prezentovat úspornějšíc typ topologie.

Zařízení	Množství	Cena
MikroTik Routerboard RB3011UiAS-RM	6	21 144 Kč
MikroTik Switch CRS354-48G-4S+2Q+RM	5	62 190 Kč
Mikrotik RB1100AHx2 2GB RAM	1	4 500 Kč
Cena celkem		**87 834 Kč**

Tabulka 15 - Ekonomické zhodnocení MikroTik [3]

[1] Veškeré ceny, které byly ve finančním zhodnocení vyčísleny, jsou včetně DPH.
[2] ABCTECH: výpočetní technika a elektronika. [online]. [cit. 2020-04-04]. Dostupné z: www.abctech.cza
[3] IT Price: checks Cisco Price, latest Cisco Global Price List [online]. [cit. 2020-04-04]. Dostupné z: https://itprice.com/

5 Výsledky a diskuse

Výsledkem mé práce je vytvoření vhodné sestavy funkční konfigurace počítačové sítě, která je zaměřená na bezpečnost. Bezpečnost je realizována na 2. a 3. vrstvě referenčního modelu ISO/OSI. Je vhodná pro základní obranné mechanizmy a útoky. Výsledkem byla funkční síťová topologie, která fungovala ve specializované laboratoři. K lepším výsledkům by mohlo přispět testování ve vybrané firmě, která používá Cisco zařízení.

5.1 Výsledky skenování sítě

Pro získání ucelené představy o bezpečnosti dané topologie byl k odhalení slabin využit nástroj (příkaz) NMap (Network Mapper),který odhalil, že port SSH na routeru (R5) je otevřený. Kdyby nebyl daný router ošetřen heslem, bylo by možné provést snadný útok, který by mohlo vést k narušení fungování daného routeru. Tím pádem by nemusel fungovat zbytek dané oblasti. Skenování sítě je možné v současné době provést z jakéhokoliv počítače. Stačí k tomu mít operační systém Kali Linux, který je bezplatný. Základní útoky na počítačové topologie může zvládnout každý člověk. Na internetu existuje mnoho návodů a videí jak, tento software používat a využívat pro útoky na počítačové sítě. Počítačový administrátor nikdy nemůže mít jistotu nad tím, že jeho síť je zabezpečená. Stále platí, že nejslabší článek konfigurací a budování topologie je člověk. Platí to i pro zařízení a šifrovací algoritmy, které se mohou tvářit jako velice bezpečné. Po pár letech se vždy objeví bezpečnostní chyba, která může být využívaná pro daný útok. Dnešní svět je propojen pomocí internetu, informačních systému, data center, cloudových platforem a internetových služeb. Informační kriminalistika je nejrychleji se rozvíjející forma kriminality na území České republiky i celosvětově. Proto vznikl zákon o kybernetické bezpečnosti, který jasně ukládá provozovatelům, jak mají předcházet útokům na jejich firemní data. Údaje a data o lidech jsou velice cenné a mají být zabezpečeny.

5.2 Možné reálné nasazení

Popisovaný návrh zajišťuje konektivitu pro připojení jednoho nebo více vzdálených pracovišť pomocí VPN. Využití spoje je možné v podnikovém prostředí. Nasazení je vhodné i pro větší podnik nebo subjekt, který má více poboček. Bezpečnost

je realizována na síťové vrstvě pomocí kryptografických nástrojů, které poskytuje sada protokolů IPsec.

5.3 **Diskuse**

Můj návrh na počítačovou bezpečnost je ve stejné podobnosti s návrhy autorů Lukáše Králíka (2019) a Martina Mikésky (2016). Návrh počítačové sítě se liší od zmíněných autorů tím, že řeší prvotní návrh, který je otestován v simulačním prostředí ,následně je ověřen na reálných zařízeních a pomocí skenování sítě.

Výzkumná otázka se vztahuje k tomu, zda by měla Česká republika uvažovat nad investicí.pro budoucí generace o informační bezpečnosti v oblasti školství. Další výzkumná otázka se týká oblasti bezpečnosti počítačových sítí ve státních zařízeních jako jsou například nemocnice, ministerstva a úřady.

Zařízení od společnosti Cisco jsou kvalitní zařízení pro bezpečnost počítačové sítě. Mají veliké portfolio a celosvětovou podporu. Investují svoji energii a finance do výzkumu což, je další faktor pro zvolení těchto produktů. Jejich slabinou je vysoká cena, která může být velice diskutabilní pro začínající podniky. Z pohledu bezpečnosti počítačové sítě se vyplácí investovat do školení personálu a nákupu zařízení, aby nedocházelo k možným únikům dat z firmy.

Závěrem lze konstatovat, že bezpečnost počítačových sítí se týká většiny společnosti, aniž by o tom měly nejmenší tušení.

6 Závěr

Hlavním cílem diplomové práce bylo ověřit bezpečnost síťové infrastruktury na platformě Cisco. Jednalo se o přepínače (switch) a směrovače (router) na 2 a 3 vrstvy ISO/OSI modelu.

Byla provedena konfigurace počítačové sítě středně velkého rozsahu, která simulovala potenciální reálné prostředí. Při tvorbě této práce v simulačním prostředí Packet Tracer byly využity teoretické poznatky a praktické zkušenosti z kurzů CCNA Cisco Academy, které se převedly do praktické části. K vybudování a ověření funkčnosti daného návrhu sloužila laboratoř síťových a internetových technologií (LSIT) v učebně D326, která se nachází na Provozně ekonomické fakultě v Praze. Úroveň práce a náročnost provedení odpovídá certifikaci Cisco CCNA a Cisco CCNA Security.

Aby navrhnutá počítačová síť fungovala správně, bylo nutné od začátku vybudovat přehledný postup, který umožní jednoduchou správu sítě a případně budoucí rozšíření o další technologie v rámci návrhu. Vlastní návrh může být nadále do budoucna rozšířen o možnost zabezpečení počítačové sítě obzvlášť proti fyzickým útokům a živelným pohromám.

Vzhledem k tomu, že Packet Tracer je výukový program, který slouží k simulaci, má rozdílné chování na rozdíl od reálných aktivních prvků, které se využívají v praxi. Proto bylo nutné ověřit v reálném prostředí vlastní návrh a odhalit slabiny. Bylo zjištěno, že reálné prostředí se chová jinak než v simulačním prostředí. Počítačová síť byla úspěšně vybudována podle vlastního návrhu v Packet Traceru a byla ověřena její funkčnost.

Následné skenování sítě odhalilo slabinu v otevřeném portu SSH na, kterou musí být daný správce sítě připraven. Neznalost v této oblasti bezpečnosti může mít často negativní dopad na ochranu dané sítě. Největší slabinou nefunkčnosti konfigurace a bezpečnosti je lidský faktor, který byl reálně ověřen na vlastních zkušenostech při budování konfigurace v učebně.

Tvorba počítačové sítě na platformě Cisco je finančně náročná. Pokud se jakákoliv firma rozhodne pro zařízení od společnosti Cisco, je nutné počítat s částkami ve výši stovek tisíc případně i milionů korun. Výstavba této počítačové topologie odpovídá ekonomické náročnosti 752 707 Kč. Ekonomická náročnost alternativní řešení od společnosti MikroTik je 87 834 Kč.

Výsledkem diplomové práce je tedy komplexní materiál, který je volně dostupný pro veřejnost, např. pro správce malých a středních firem pro zlepšení bezpečnosti počítačové sítě. Celkový přínos této práce je v uložený v příloze, kterou je možné libovolně nakonfigurovat znovu na zařízeních Cisco. Díky tomu je možné znovu sestavit a zprovoznit celou síť a následně ji znovu testovat.

7 Seznam použitých zdrojů

[1] LAMMLE, Todd. CCNA: výukový průvodce. Brno: Computer Press, 2015. ISBN 978-802-5146-026.

[2] CARROLL, Michael Wenstrom. Zabezpečení sítí Cisco: autorizovaný výukový průvodce. Brno: Computer Press, 2003. Samostudium. ISBN 80-7226-952-6.

[3] PUŽMANOVÁ, Rita. TCP/IP v kostce. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009. ISBN 978-80-7232-388-3.

[4] Kolektiv: Online kurikulum CCNA Routing and Switching: Scaling Networks verze 5.0 (aktuální verze je pro registrovené uživatele dostupná na portále netacad.com)

[5] Kolektiv: Online kurikulum CCNA Security: Implementing Network Security 2.0 (aktuální verze je pro registrovené uživatele dostupná na portále netacad.com)

[6] PETRO, Jozef. Výkladový slovník internetu. Praha: CP Books, 2005. ISBN 80-722-6222-X.

[7] Kyberkriminalita: Policie ČR [online]. [cit. 2020-02-12]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[8] VALENTOVÁ, Hana. Novela zákona o kybernetické bezpečnosti: a její dopady na zdravotnictví [online]. 11/2018 [cit. 2020-02-12]. Dostupné z: https://www.systemonline.cz/it-security/novela-zakona-o-kyberneticke-bezpecnosti.htm

[9] MALIŠ, Mgr. Petr a Jakub KEJVAL. Právní aspekty přijetí zákona o kybernetické bezpečnosti. Systemonline: s přehledem ve světe podnikové informatiky. 2015(3), 3.

[10] DVOŘÁKOVÁ, Reneta a Jaroslava IGNÁCIKOVÁ. Co lze čekat od zákona o kybernetické bezpečnosti. ITSystems: Pro veřejný sektor a zdravotnictví. 2014, 2014(Special), 2.

[11] KASS, Josh. : Omezte bezpečnostní hrozby a zabraňte jejich šíření díky segmentaci sítě. In: Rockwell Automation: Rockwell Automation je jedna z vedoucích světových společností produkující průmyslovou elektroniku a elektrotechniku [online]. 2018 [cit. 2020-02-19]. Dostupné z: https://www.rockwellautomation.com/cs_CZ/news/blog/detail.page?pagetitle=Omezte-bezpe%C4%8Dnostn%C3%AD-hrozby-a-zabra%C5%88te-jejich-

%C5%A1%C3%AD%C5%99en%C3%AD-d%C3%ADky-segmentaci-s%C3%ADt%C4%9B

[12] intercityuser. Next-generation firewall (NGFW) vs. traditional firewall. Security Boulevard [online]. 2019 [cit. 2020-02-19]. Dostupné z: https://securityboulevard.com/2019/06/next-generation-firewall-ngfw-vs-traditional-firewall/

[13] Národní úřad pro kybernetickou a informační bezpečnost [online]. In: . [cit. 2020-02-29]. Dostupné z: https://www.nukib.cz/images/Nukib-MU-s.png

[14] The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack. [online]. In: . [cit. 2020-02-29]. Dostupné z: https://www.researchgate.net/publication/327483011/figure/fig2/AS:668030367436802@1536282259885/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack.jpg

[15] Třídy IP adres [online]. In: . [cit. 2020-02-29]. Dostupné z: https://cs.wikipedia.org/wiki/T%C5%99%C3%ADdy_IP_adres

[16] Fotoarchiv autora

[17] Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: . 29.08.2014, ročník 2014, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[18] Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: . 28.05.2018, ročník 2018, číslo 82. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

[19] Lokální sítě (LAN) [online]. [cit. 2020-03-03]. Dostupné z: https://is.muni.cz/do/ics/el/sitmu/law/html/lokalni-site-lan.html

[20] Hacker [online]. [cit. 2020-03-09]. Dostupné z: https://www.merriam-webster.com/dictionary/hacker

[21] 2019 CONSUMER SURVEY: TRUST AND ACCOUNTABILITY IN THE ERA OF DATA MISUSE [online]. In: . 10.08.19 [cit. 2020-03-09]. Dostupné z: https://www.pingidentity.com/content/dam/ping-6-2-assets/Assets/Misc/en/3464-consumersurvey-execsummary.pdf

[22] Isaac Kohen. Five cyber risks that will define 2020 [online]. January 6, 2020 [cit. 2020-03-09]. Dostupné z: https://www.helpnetsecurity.com/2020/01/06/cyber-risks-2020/

[23] IBM Security a Ponemon institute. Cost of a Data Breach Report 2019 [online]. 2019, , 75 [cit. 2020-03-11]. Dostupné z: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

[24] Cisco Application Centric Infrastructure [online]. [cit. 2020-03-11]. Dostupné z: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html

[25] Materiál poskytnutý od firmy VUMS DataCom, spol. s r.o.

[26] Hacker [online]. In: . [cit. 2020-04-03]. Dostupné z: https://i.iinfo.cz/images/336/hacker-karty-zlodej-1-prev.jpg

[27] Network-Computer-Systems-Administrator [online]. In: . [cit. 2020-04-03]. Dostupné z: https://highpaymajors.com/wp-content/uploads/2019/03/Network-Computer-Systems-Administrator-840x505.jpg

[28] PuTTY [online]. [cit. 2020-03-30]. Dostupné z: https://www.putty.org/

[29] Cisco CAB-CONSOLE-RJ45 [online]. In: . [cit. 2020-04-03]. Dostupné z: https://www.macpalace.com/images/images.php?pid=CAB-CONSOLE-RJ45=

[30] A-typical-Access-Control-List-ACL [online]. In: . [cit. 2020-04-03]. Dostupné z: https://www.researchgate.net/profile/Vic_Grout/publication/228827122/figure/fig1/AS:339487512121376@1457951538291/A-typical-Access-Control-List-ACL.p

[31] Windows_acl [online]. In: . [cit. 2020-04-03]. Dostupné z: https://www.qnap.com/images/products/Application/notes/windows_acl_01.png

[32] Budova_pef_2019_062_msl-1 [online]. In: . [cit. 2020-04-05]. Dostupné z: https://katedry.czu.cz/storage/0aea8959-budova_pef_2019_062_msl-1-.jpg

Přílohy

Příloha A - přiložené CD

CD obsahuje vyhotovenou práci ve formátu PDF, projekt Cisco Packet Tracer, výpis všech zařízení z topologie a soubor pro konfiguraci na reálném zařízení. Seznam souboru na CD :

cisco_konfigurace.txt
Diplomová_práce_Packet_Tracer_v03_final.pkt
ASA_startup-config.txt
Router1_startup-config.txt
Router2_startup-config.txt
Router3_startup-config.txt
Router4_startup-config.txt
Router5_startup-config.txt
Router6_startup-config.txt
Switch1_startup-config.txt
Switch2_startup-config.txt
Switch3_startup-config.txt
Switch4_startup-config.txt
xvetj005_DP_v18_final.pdf