UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

# DIPLOMOVÁ PRÁCE

2017 Bc. Jiří Broulík

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

# Jednotné přihlášení v síťových firewallech

Bc. Jiří Broulík

Diplomová práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Jiří Broulík** |
| Osobní číslo: | **I15196** |
| Studijní program: | **N2646 Informační technologie** |
| Studijní obor: | **Informační technologie** |
| Název tématu: | **Jednotné přihlášení v síťových firewallech** |
| Zadávající katedra: | **Katedra softwarových technologií** |

Zásady pro vypracování:

Cílem diplomové práce je otestovat funkčnost jednotného přihlašování uživatelů do sítě a spolehlivost Single Sign-On systému firewallu pro kontrolu přístupu jednotlivých uživatelů, do různých sítí, na základě firemních bezpečnostních politik. Následovat bude analýza výsledků provedených testů a návrh na zlepšení funkcionality systému. Pro testování budou použity následující komponenty: síťový firewall Fortigate, Windows servery, Windows a Linux hosty, Mikrotik Access Pointu a virtuální Cisco router. Výsledkem práce bude plnohodnotná analýza síťového Single Sign-On řešení při různých variantách konfigurace a pro různé druhy implementací.

Rozsah grafických prací:

Rozsah pracovní zprávy: **50 stran**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

***GARMAN, Jason. Kerberos: the definitive guide. Beijing: O'Reilly, c2003. ISBN 0-596-00403-6.**
***HOWES, Tim., Mark SMITH a Gordon S. GOOD. Understanding and deploying LDAP directory services. 2nd ed. Boston: Addison-Wesley, c2003. ISBN 0-672-32316-8.**

Vedoucí diplomové práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání diplomové práce: **31. října 2016**

Termín odevzdání diplomové práce: **17. května 2017**

Ing. Zdeněk Němec, Ph.D.
děkan

L.S.

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2016

**Prohlášení autora**

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 09. 04. 2017 Bc. Jiří Broulík

## PODĚKOVÁNÍ

Rád bych poděkoval vedoucí práce Ing. Soně Neradové, Ph.D. za ochotu a pomoc při zpracování této diplomové práce. Dále bych rád poděkoval Ing. Petru Šubovi za věnovaný čas, uvedení do problematiky a za půjčení fyzického firewallu Fortigate a potřebného softwaru pro zpracování praktické části práce. Dále děkuji své rodině za podporu a porozumění.

## ANOTACE

Tato diplomová práce pojednává o technologii jednotného přihlášení v síťových firewallech. Teoretická část práce vymezuje základní pojmy z hlediska infrastrukturních služeb týkajících se autentizace. Dále popisuje hojně užívané protokoly pro ověřování identit a konkrétní technologie jednotného přihlášení v síťovém firewallu Fortigate.

V praktické části byly vytvořeny různé topologie pro otestování rozdílných variant implementací jednotného síťového přihlášení s cílem zjištění potenciálních nedostatků testované technologie. V případě takového objevení byl o problému podán report a návrh na případné zlepšení.

## KLÍČOVÁ SLOVA

Firewall, Fortigate, autentizace, Single Sign-On, SSO, FSSO, RSSO, SSL VPN, NPS, LDAP, AD, DC, RADIUS, Kerberos, NTLM

## TITLE

Single Sign-On authentication in network firewalls

## ANNOTATION

This Master Thesis discusses Single Sign-On authentication technology in network firewalls. The theoretical part defines the basic concepts of infrastructure services dealing with authentication as well as frequently used protocols for identity verification. It also describes specific Single Sign-On technologies available in Fortigate network firewall.

In the practical part, a set of different network topologies were created to test variety of distinct Single Sign-On implementations. The goal was to find out potential imperfections of these technologies. If such a defect was encountered a report was written about it with a suggestion for improvement.

## KEYWORDS

Firewall, Fortigate, authentication, Single Sign-On, SSO, FSSO, RSSO, SSL VPN, NPS, LDAP, AD, DC, RADIUS, Kerberos, NTLM

# OBSAH

# Seznam ilustrací a tabulek

# Seznam zkratek a značek

| | |
|---|---|
| AAA | Authentication, Authorization, Accounting |
| AD | Active Directory |
| AES | Advanced Encryption Standard |
| AP | Access Point |
| BYOD | Bring Your Own Device |
| CA | Collector Agent |
| DC | Domain Controller |
| DIT | Directory Information Tree |
| DN | Distinguished Name |
| DHCP | Dynamic Host Configuration Protocol |
| DoS | Denial of Service |
| FortiOS | Fortinet Operating System |
| FSSO | Fortinet Single Sign-On |
| HIPPA | Health Insurance Portability and Accountability Act |
| CHAP | Challenge Handshake Authentication Protocol |
| IP | Internet Protocol |
| KDC | Key Distribution Center |
| LDAP | Lightweight Directory Access Protocol |
| NAS | Network Access Server |
| NAT | Network Address Translation |
| NPS | Network Policy Server |
| NTCR | NT Challenge/Response protokol |
| NTLM | NT LAN Manager |

| | |
|---|---|
| RDN | Relative Distinguished Name |
| RPC | Remote Procedure Call |
| RSSO | RADIUS Single Sign-On |
| SSO | Single Sign-On |
| SSL | Secure Socket Layer |
| TCP | Transmission Control Protocol |
| TS | Terminal Server |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |

# Úvod

Bezpečnost je stále aktuální téma týkající se prakticky každé organizace. Bez dobře navržené bezpečnostní politiky s přihlédnutím k četnosti kybernetických útoků na zdroje firem zvenku i zevnitř nemá organizace sebemenší šanci na úspěch.

Jedna z nezbytných komponent bezpečnosti je autentizace. Ta zajišťuje, že daná identita je skutečně tím, za co se vydává. S autentizací je však spojeno velké množství problémů, od zabezpečení komunikace v průběhu ověřování přes správu účtů a hesel až po zabezpečení zařízení, jenž autentizaci zajišťují. Na druhou stranu se díky ní dají vykonávat důležité funkce jako je například účetnictví či rozlišování mezi identitami. Bez takových služeb by se dnes již většina organizací neobešla. Příkladem jsou zdravotní organizace, které musí striktně dodržovat utajení choulostivých dat svých pacientů a bez správné autentizace identit by taková správa dat byla nemožná.

Jedním z předních problémů autentizace zůstává četnost systémů, do kterých se identita musí přihlašovat. V případě, že bude slovo identita chápáno jako běžný člověk či uživatel, pak je s množstvím přihlašovacích aktivit spojeno i neefektivní využití pracovního času a množství hesel, jež si takový jedinec musí pamatovat.

Tehdy přichází jako řešení těchto problémů systém jednotného přihlašování, který identitě umožňuje se autentizovat jednou na centrálním systému a při nutnosti ověření identity na jiných systémech se přes komunikační kanál provádí automatická autentizace již ověřené identity. Tento způsob například umožňuje uživateli se přihlásit pouze na začátku dne do jednoho systému a jeho identita bude automaticky rozpoznána i dalšími systémy, které spolupracují s centrálním systémem pro ověřování. Takový uživatel bude automaticky přihlašován do spolupracujících systémů bez nutnosti jeho dalšího inputu a bude nucen si pamatovat pouze jedno heslo. Takové řešení uživatelům šetří čas a zabraňuje prolomení bezpečnosti účtu tím, že pro komplexnost hesel bude uživatel donucen si svá hesla poznamenat v čistém textu na papír či do elektronického dokumentu.

Jako cíl této práce bylo seznámit čtenáře se základními pojmy, protokoly a metodami systému jednotného přihlášení na úrovni síťové infrastruktury, a to společně s vykonáním kvalifikovaného testování různých druhů implementací a nastavení v sítích, jež tento druh autentizace vyžadují. Výstupem testování je sada odhalených nedokonalostí, které mohou v rutinním provozu nastat a příslušným způsobem popsané potenciální řešení zmíněných problémů.

Práce je zaměřena zejména na testování systému jednotného přihlášení síťového firewallu Fortigate s využíváním služeb serveru Windows. Jako další komponenty byly použity například virtualizační platforma Hyper-V, virtuální router Cisco CSR 1000v, bezdrátový router Mikrotik, systémy s operačním systémem Linux apod.

Cílem práce naopak není pokrýt všechny možné varianty technologie jednotného přihlášení. Zároveň není cílem pokrýt veškeré funkce firewallu či Windows serveru. Předpokládá se již určitá znalost těchto prvků, na kterou práce navazuje, a proto v teoretické části jen relativně stručně seznamuje s nezbytnou terminologií, protokoly a principy užitými v praktické části práce v průběhu testování.

# 1 Základní pojmy

Hlavním účelem této části práce je seznámit čtenáře se základními pojmy týkající se síťové autentizace. Vysvětleny jsou zejména koncepty, o které se později opírá praktická část práce.

## 1.1 Autentizace

Autentizace je proces ověřování, zda jedinec nebo nějaké zařízení jsou skutečně to, za co se vydávají. V případě uživatelské autentizace se nejčastěji jedná o ověření lidské bytosti vůči informačnímu systému, například operačnímu systému, drátové nebo bezdrátové síti či různým druhům aplikací. Ověření zařízení je nutné zejména při automatických akcích v síti. Příkladem mohou být aktualizace systémů, zálohování nebo vzdálený monitoring.

Autentizace může probíhat v různých formách, například za použití jména a hesla, certifikátu, nebo biologických údajů.

## 1.2 Firewall

Na síťový firewall se dá pohlížet jako na zařízení, které odděluje nezabezpečenou síť od zabezpečené. Obecněji se dá říci, že odděluje různé sítě a segmenty a nahlíží do komunikace, která přes něho prochází. Na základě svých bezpečnostních politik může určitou komunikaci zastavit, zahodit nebo nechat projít. V obecném případě má kontrolu nad neautentizovanými pakety, avšak některé firewally umožňují pakety ověřovat a na základě identity uživatele odesílajícího pakety rozhodnout, co s takovou komunikací udělat.

Firewallem může být myšleno síťové zařízení stejně tak jako software v počítači. Nicméně tato práce pod pojmem firewall vyjadřuje fyzické síťové zařízení, pokud není explicitně zmíněno, že se jedná například o software v rámci operačního systému.

## 1.3 SSL VPN

SSL VPN je virtuální privátní síť vytvořená mezi jednotlivými koncovými uživateli a zařízeními většinou sloužící jako výchozí brána na okraji sítě. Pro tuto práci se předpokládá, že takovým zařízením je síťový firewall. SSL VPN zajišťuje zabezpečené připojení k firemním zdrojům přes nezabezpečenou internetovou síť, kde hlavní výhodou je SSL protokol. SSL šifrování je dostupné v každém prohlížeči a zároveň užívá pro svou komunikaci port 443,

jenž je povolen skrze firewally prakticky ve všech sítích, kde se uživatel může nacházet. Je tedy možné se připojit k jakékoliv síti, například v hotelu, obchodním centru, kavárně, doma, navázat spojení s interní firemní sítí pomocí SSL VPN a mít tak zabezpečenou komunikaci do interní sítě i přes Internet.

## 1.4 NPS (Network Policy Server)

NPS je implementace RADIUS serveru společností Microsoft, je k dispozici jako role na Windows serverech a umožňuje následující funkce:

- Autentizaci.
- Autorizaci.
- Účetnictví.

Hlavní využití NPS je (dle Microsoft Developer Network, 2008) v oblasti bezdrátových sítí, v ověřování přístupu k síťovým zařízením, VPN, apod.

Příkladem užití může být situace, kdy bezdrátové přístupové body (AP) v síti jsou nastaveny na zabezpečení Enterprise AES a ověřování příchozích žádostí o ověření od uživatelů přeposláním autentizačních paketů na NPS server. Po rozhodnutí je dotyčný do sítě připuštěn nebo mu je přístup odmítnut.

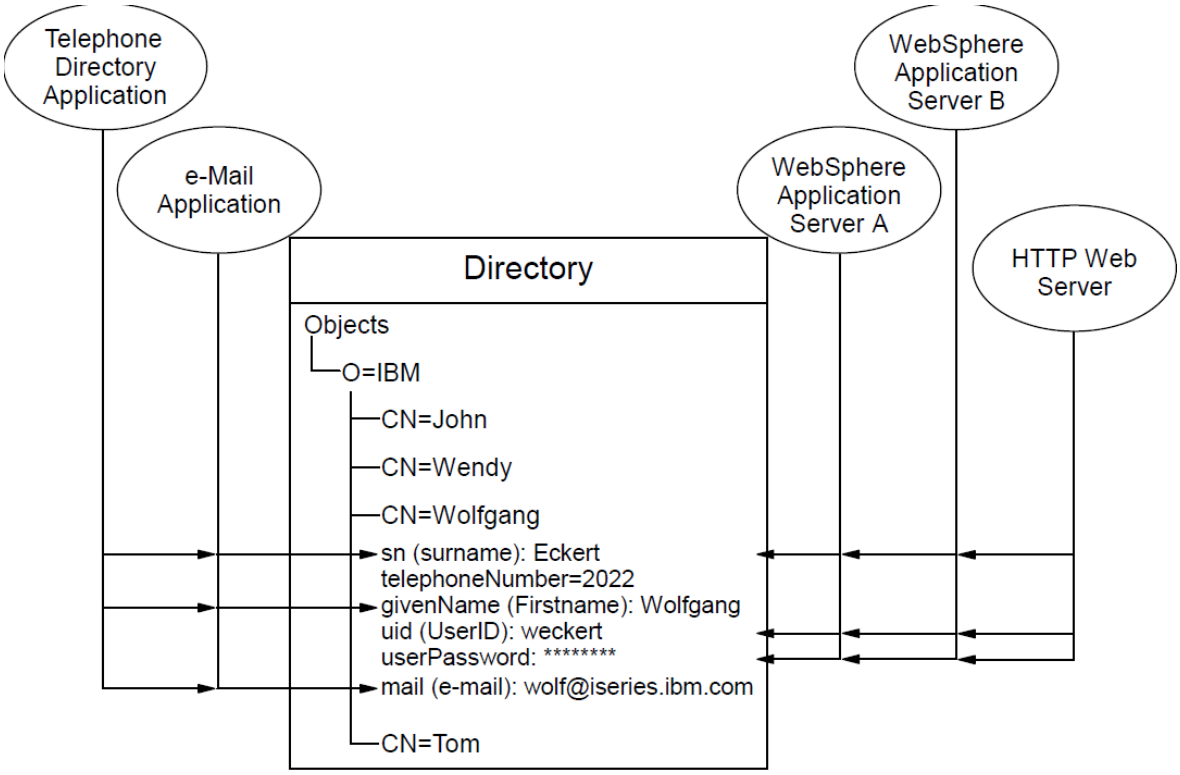
## 1.5 LDAP protokol

Zkratka LDAP vznikla z celého názvu Lightweight Directory Access Protocol. Dle (Tuttle, Ehlenberger, Gorthi a další, 2004, s. 7) se jedná o implementaci jednodušší podmnožiny standardů z původního X.500 standardu. Funguje na síťovém modelu TCP/IP a definuje standardizovaný způsob přístupu. Dále určuje metodu pro aktualizování informací v adresáři a dle (Tuttle, Ehlenberger, Gorthi a další, 2004, s. 7) je nejpoužívanějším protokolem pro přístup k adresářům. Princip fungování a typy zpráv používané adresářovými klienty a servery jsou blíže popsané v podkapitole níže.

Obecně - u protokolu LDAP není klient závislý na konkrétní implementaci serveru a server si může adresář implementovat jakkoliv chce. Je to možné proto, že LDAP určuje komunikační protokol, ale neurčuje, jak má být adresář, ke kterému díky LDAPu klient přistupuje,

implementován. Dle (Tuttle, Ehlenberger, Gorthi a další, 2004, s. 7) je aktuální verze LDAP protokolu verze 3.

Hlavní výhodou LDAP protokolu je, že určitá data o objektech mohou být uložena na jednom centrálním místě (případně replikovaná na vícero míst), zatímco různé aplikace pro různé účely mohou z adresáře získávat konkrétní atributy o daných objektech. Ukázka je na obrázku níže.




**Obrázek 1: Přístup k LDAP atributům objektu**

*Zdroj: (Tuttle, Ehlenberger, Gorthi a další, 2004, s. 11)*

### 1.5.1 Princip fungování LDAP

Vzájemné působení a interakce mezi LDAP klientem a LDAP serverem se dají dle (Carter, 2003, s. 16) obecně popsat následovně:

1. Klient vytvoří session s LDAP serverem tím, že specifikuje jeho název nebo IP adresu včetně TCP/IP portu, na kterém server naslouchá. Tento krok je známý jako svázání (binding) se serverem.
2. Klient uvede uživatelské jméno a heslo, aby se patřičně autentizoval na serveru. Případně může klient vytvořit autonomní session, kde obdrží pouze výchozí práva.

Nebo může klient vytvořit se serverem zabezpečenou session, v níž bude docházet k šifrování dat.

3. Klient nyní může vykonávat operace nad objekty adresáře. LDAP umožňuje jak číst, tak zapisovat, což dovoluje se na záznamy v adresáři nejen ptát, ale též upravovat. Umožňuje také vyhledávat v záznamech dle libovolných uživatelských kritérií. Klient může například specifikovat, jakou část adresáře chce prohledat a jaké informace vrátit.
4. Když klient přestane posílat dotazy na server, dojde k rozvázání session mezi nimi. Tato operace se nazývá unbinding.

### 1.5.2 Operace LDAP

LDAP definuje operace pro přístup a úpravu záznamů v adresářové struktuře. Příkladem jsou dle (Carter, 2003, s. 198) následující operace:

- Svázání/rozvázání (binding/unbinding).
- Vyhledávání záznamů vyhovující určitým kritériím.
- Přidání záznamu.
- Odebrání záznamu.
- Úprava záznamu.
- Úprava DN nebo RDN záznamu (to znamená přesun záznamu v hierarchii).
- Porovnání záznamu.

V následující podkapitole bude zmínka o adresářových službách. Uveden bude nejen rozdíl mezi adresářovou službou a LDAP protokolem, ale také jak se vzájemně doplňují.

## 1.6 Adresářová služba

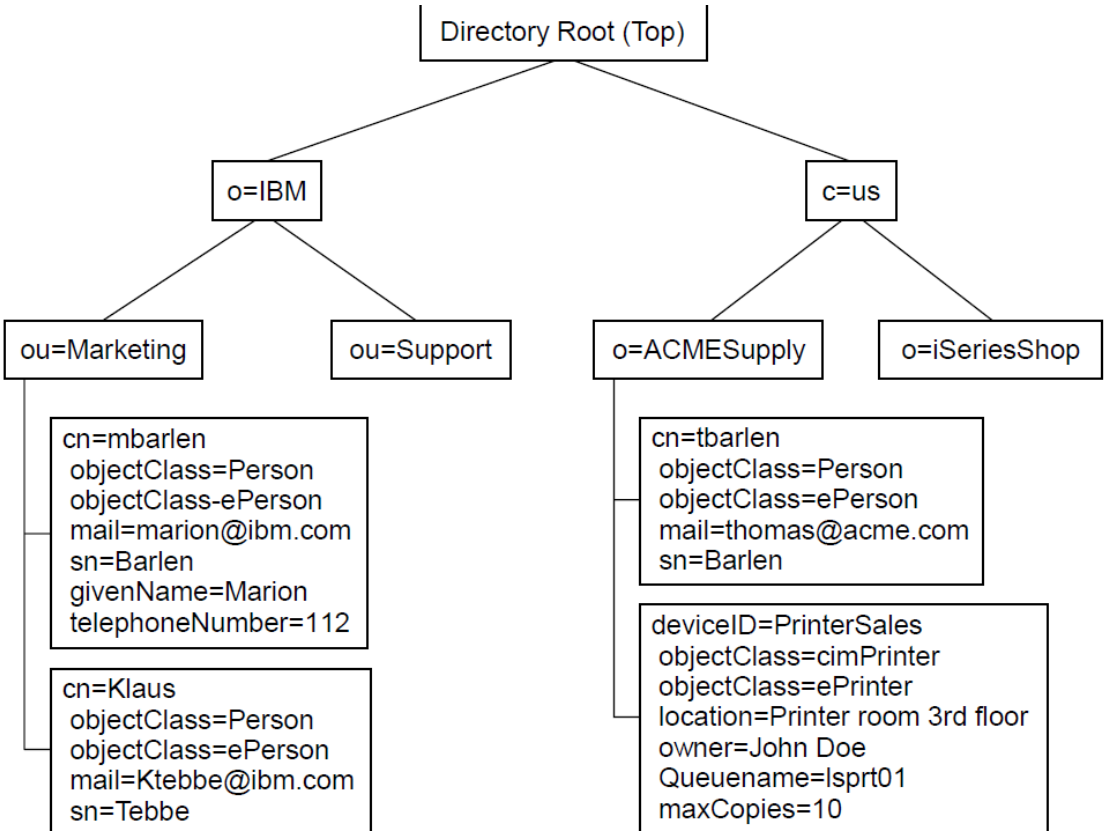
Zatímco LDAP určuje, jak jsou záznamy v adresáři identifikovány a organizovány, adresář je specializovaná databáze uchovávající typové, uspořádané informace o určitých objektech organizovaných do stromové struktury. Příkladem adresáře může být Active Directory od společnosti Microsoft.

Adresář ve své podstatě tvoří strom, který se nazývá DIT (Directory Information Tree) a záznamy jsou v něm uspořádány na základě DN (Distinguished Name), které představuje unikátní jméno jednoznačně identifikující záznam. DN se dále skládá ze sekvence RDNs (Relative Distinguished Names) oddělenými od sebe čárkami. RDN pak může vypadat například následovně:

CN=Jiri Broulik,OU=IT,DC=jiricorp,DC=COM

Každé RDN v DN odpovídá větvi v DIT jdoucí od kořene DIT dolů až k danému záznamu v adresáři.

Každý administrátor je schopen si vytvořit své DIT podle svých potřeb. Má-li například firma různé oddělení, je možné pod kořenem začít budovat strukturu podle daných oddělení. Ten samý princip se dá použít také například na pobočky v různých městech, zemích, apod.




**Obrázek 2: Directory Information Tree**

*Zdroj: (Tuttle, Ehlenberger, Gorthi a další, 2004, s. 17)*

Adresářová služba dále definuje schéma, ve kterém udává, jaké třídy se mohou vyskytovat v určitých místech, jaké atributy musí mít nebo jaké jsou volitelné a syntaxi pro dané atributy. Příkladem je třída Osoba. Schéma této třídy pak definuje, že musí mít atribut příjmení typu řetězec. Dále že může mít atribut email, taktéž typu řetězec, apod.

# 2 Autentizační protokoly

V této části je věnována pozornost protokolům, jež jsou běžně užívány pro autentizaci identit nejen v doméně, ale i mimo ni. Zaměřena je na protokol Kerberos, NTLM a RADIUS, které jsou v praktické části práce dále používány spolu se síťovým firewallem, servery Windows a dalšími prvky.

## 2.1 Kerberos

Kerberos je dle (Garman, 2003, s. 7) veřejně přístupný od roku 1989 a aktuální implementovaná verze protokolu Kerberos v dnešních systémech je verze 5. Organizace využívající Kerberos jsou schopny vytvořit systém jednotného přihlašování nezávisle na platformě (operačním systému), který dává koncovým uživatelům možnost využívat jediné přihlašovací údaje pro přístup k různým zdrojům v síti. Kerberos snižuje počet hesel, které si uživatel musí pamatovat na jedno jediné pro celou korporátní síť. Zároveň poskytuje mechanizmus šifrování a integrity zpráv a zajišťuje, že citlivá autentizační data jsou poslána po síti v zašifrované podobě. Kerberos používá tickety, časově omezené kryptografické zprávy, které prokazují identitu uživatele bez nutnosti ukládání si uživatelských údajů do mezipaměti klientského počítače.

Cílem Kerberosu je provádět ověřování na jednom serveru (nebo vícero serverech se stejnými daty kvůli redundanci). Jedná se o centralizované KDC (Key Distribution Centers), kde každé KDC disponuje databází uživatelů a hesel jak pro uživatele, tak pro služby využívající protokol Kerberos. Takové centralizované řešení usnadňuje práci administrátorům a zjednodušuje nastavení bezpečnosti, kdy je nutné důkladně zabezpečit pouze jedno nebo pár zařízení. Dále namísto posílání hesel přes síť v čitelné podobě, používá Kerberos zašifrované tickety, které mají za cíl ověřit identitu nejen koncových uživatelů, ale také serverů. Tickety jsou generovány centralizovanými KDC servery jménem uživatelů snažících se přihlásit do sítě.

### 2.1.1 Základní pojmy Kerberosu

V této části budou představeny základní pojmy protokolu Kerberos, na které správce sítě jistě narazí nejen v určitých publikacích, ale též při každodenní práci. Při popisu následujících pojmů bylo čerpáno z (Garman, 2003, s. 17).

**Realm** – odpovídá administrativní doméně. Hlavním cílem Realmu je vymezit oblast, ve které má práva autentizovat uživatele, hosty nebo služby. Název Realmu je citlivý na malá a velká písmena, ale většinou se udávají veškerá písmena velká.

Existují-li 2 objekty v jiných Realmech, může dojít k autentizaci objektů tehdy, je-li mezi Realmy vytvořen vztah důvěry (Trust).

**Principal** – je název, který se používá pro identifikaci záznamu v databázi serveru a je spojen s každým uživatelem, hostem nebo službou v Realmu. Příkladem pro uživatele mohou být například:

- jiribr@JIRICORP.LOCAL
- admin/admin@JIRICORP.LOCAL

**Ticket** – vydává autentizační server (KDC) a je šifrovaný klíčem (heslem) služby, pro kterou je určen. Vzhledem k faktu, že daný klíč je sdílen jen mezi autentizačním serverem a samotnou službou, nemá klient žádající o daný ticket možnost se jeho obsah dozvědět nebo jej změnit. Jedny z hlavních komponentů Ticketu jsou:

- Principal uživatele žádající o Ticket.
- Principal služby pro kterou je Ticket určen.
- IP adresa klientského zařízení, které může daný Ticket používat.
- Datum a čas od kdy je Ticket platný.
- Doba životnosti Ticketu.
- Klíč session.

**Šifrování** – Kerberos šifruje a dešifruje zprávy. Konkrétně se jedná o tickety a uživatele. Nepočítaje například projekt pkinit, Kerberos dle (Petrová, Čapek, Ballard, 2016, s. 12) využívá pro šifrování pouze symetrické klíče, tj. stejný klíč je použit pro zašifrování i pro dešifrování.

**Key distribution center** (KDC) – je server sloužící k ověřování a distribuci ticketů pro přístup ke službám, přičemž uživatelé i služby s KDC sdílí svůj tajný klíč. Člení se na 3 různé komponenty:

- Databáze – obsahuje záznamy o uživatelích a službách.
- Autentizační server – na přijatou žádost o autentizaci uživatele vystaví tzv. Ticket Granting Ticket (TGT). Pomocí tohoto ticketu může úspěšně ověřený uživatel získat tickety jiných služeb bez nutnosti opětovného zadávání hesla.
- Ticket Granting Server (TGS) – vykonává distribuci ticketů služeb s platným TGT.

**Session key** – uživatel a požadovaná služba využívají v průběhu mezi nimi otevřené session tzv. session key, který je známý oběma stranám a také KDC, jenž jej vygeneroval. Tento klíč se používá pro šifrování komunikace mezi nimi.

**Authenticator** – generuje klient kvůli posílení autentičnosti a obsahuje následující komponenty:

- Principal uživatele.
- Časové razítko (je-li odlišnost časů větší než 2 minuty, ověření uživatele bude neúspěšné).
- Zašifrování pomocí Session key.

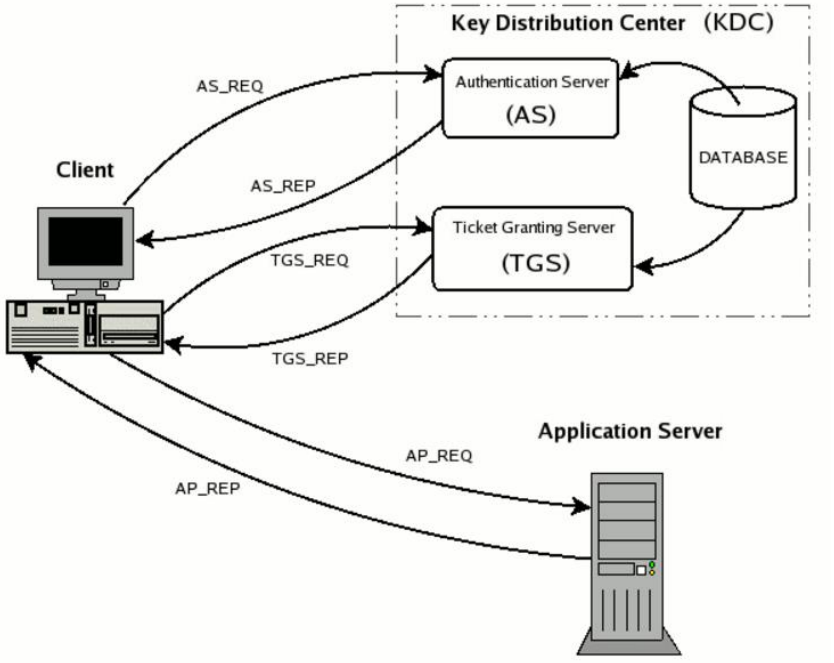
### 2.1.2 Princip fungování Kerberos autentizace

Základním poznatkem fungování Kerberosu je fakt, že aplikační server nikdy napřímo nekomunikuje s KDC. Vydaný ticket služby aplikačního serveru se k ní dostane pouze pomocí klienta (například uživatele), jenž si přístup k dané službě vyžaduje. Kerberos tedy používá sadu zpráv, jež realizují komunikaci mezi klientem, KDC a aplikačním serverem za účelem autentizace klienta na aplikačním serveru. Mezi základní typy zpráv dle (Ricciardi, 2006) patří:

- **AS_REQ** – jedná se o nezašifrovanou úvodní zprávu uživatele, vyjadřující žádost o autentizaci. Směřována je na KDC, konkrétně na autentizační server (AS). Tato zpráva obsahuje mimo jiné Principal klienta a Principal služby. Po obdržení zprávy provede AS kontrolu, zda oba z poskytnutých Principálů existují v databázi. Pokud ne, vrátí chybu.
- **AS_REP** – zpráva s odpovědí od autentizačního serveru (AS) na předchozí žádost o ověření. Tato zpráva obsahuje TGT (disponující mimo jiné též Principal uživatele a služby), jež je zašifrované pomocí tajného klíče TGS, a Session key, který je zašifrován pomocí tajného klíče uživatele.
- **TGS_REQ** – žádost o ticket služby od klienta na TGS. Tato zpráva obsahuje TGT obdržené v předchozí zprávě a klientem vygenerovaný Authenticator, jenž je zašifrovaný pomocí Session key.
- **TGS_REP** – zpráva od TGS s odpovědí na předchozí zprávu. Obsahuje vyžádaný ticket služby, jenž je zašifrovaný pomocí tajného klíče dané služby, a také Session key služby

vygenerovaný na TGS, který je zašifrovaný pomocí dříve vytvořeného Session key na autentizačním serveru.

- **AP_REQ** – tuto zprávu posílá klient na aplikační server s žádostí o přístup ke službě. Obsahuje ticket služby získaný od TGS v předchozí zprávě a klientem vygenerovaný Authenticator, jenž je zašifrovaný pomocí Session key služby vygenerovaný na TGS.
- **AP_REP** – je odpověď aplikačního serveru klientovi jako důkaz, že se jedná o správný server. Klient si tento typ zprávy od serveru vyžádá jen tehdy, pokud je vyžadována vzájemná autentizace, jinak tato zpráva vyžadována není.




**Obrázek 3: Protokol Kerberos**

*Zdroj: (Ricciardi, 2006)*

## 2.2 NTLM

Ačkoliv Kerberos byl zvolen jako preferovaný autentizační protokol společností Microsoft v Active Directory, NTLM je použitelný jak v případě používání AD, tak i v případě jeho nepoužívání. Konkrétní scénáře, kdy je možné použít NTLM jsou dle (Ramaswamy, 2013) následující:

- Klient se ověřuje na server používání IP adresy.
- Klient se ověřuje na server, který patří do jiného AD lesa, který má dříve používaný NTLM trust namísto novějšího tranzitivního trustu mezi lesy.

- Klient se autentizuje na server, který nepatří do domény.
- Neexistuje žádná AD doména.
- Pokud pakety prochází skrze firewall, který blokuje komunikaci na port Kerberosu. Typicky TCP port 88.

### 2.2.1 Princip fungování NTLM autentizace

V této podkapitole je blíže věnována pozornost fungování NTLM. Níže jsou popsány jednotlivé kroky a proces autentizace. Čerpáno bylo z (Glass, 2006).

1. Uživatel poskytne na svém PC název domény, jméno uživatele a heslo. Dojde k vypočítání hashe hesla a samotné heslo je poté odstraněno.
2. Klient zašle uživatelské jméno v prostém textu na server.
3. Server vygeneruje náhodné číslo o velikosti 16 bajtů a zašle jej klientovi. Tato zpráva se nazývá challenge.
4. Klient zašifruje obdrženou challenge zprávu pomocí hashe uživatelského hesla a výsledek vrátí serveru. Tato zpráva se nazývá response.
5. Server poté zašle následující informace na doménový kontrolér:
    - Jméno uživatele.
    - Zprávu challenge, kterou dříve poslal klientovi.
    - Zprávu response, kterou v předchozím kroku obdržel od klienta.
6. Doménový kontrolér použije jméno uživatele, aby získal hash jeho hesla ze Security Account Manager databáze. Následně tento hash hesla použije na zašifrování zprávy challenge.
7. Doménový kontrolér poté porovná zašifrovaný challenge, který si v předešlém kroku sám vypočítal z response od klienta z kroku 4. Zjistí-li, že jsou totožné, pak autentizace byla úspěšná.

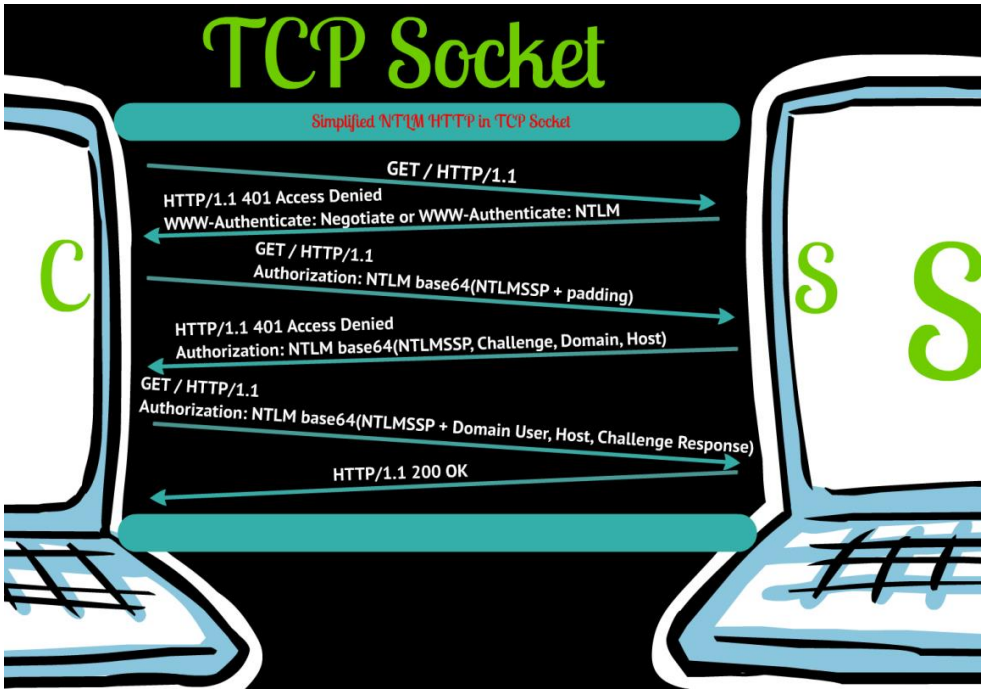
### 2.2.2 NTLM autentizace technicky

V předchozí podkapitole bylo popsáno fungování NTLM autentizace principiálně. V této části budou blíže zmíněny interakce probíhající na klientovi a serveru v průběhu NTLM autentizace.

NTLM pro svou komunikaci používá NT Challenge/Response protokol (NTCR). Ten se od Kerberosu liší tím, že server zasílá zprávu challenge HTTP klientovi a ten poté zašle response zpět na server. Tímto způsobem není heslo klienta nikdy posíláno přes síť.

Autentizace pomocí NTCR protokolu probíhá dle (Glass, 2006) následovně:

1. Klient zašle anonymní žádost na webový server. Server odpoví chybovou zprávou 401.2 a zprávou, že je nutné se autentizovat.
2. Pokud klient nepodporuje Kerberos, pak NTLM inicializuje NTCR autentizaci. Klient zavře stávající TCP spojení a otevře nové spojení a zašle žádost, která obsahuje mimo jiné NTLM záznam, jenž obsahuje uživatelské jméno, název počítače a domény. Tyto údaje jsou poté použity pro vygenerování zprávy challenge. Pokud uživatelský účet není lokální účet na webovém serveru, pak jsou data předána na doménový kontrolér, který vygeneruje challenge.
3. Zpráva challenge je zaslána klientovi, kde webový server vrací chybu 401.1.
4. Klient použije své heslo a zprávu challenge na vytvoření hashe. Poté vygenerovaný hash zašle v Response zprávě zpět na server.
5. Server přijme zprávu, poté vygeneruje sám, případně nechá vygenerovat doménový kontrolér, hash a porovná je. Pokud se rovnají, pak je autentizace úspěšná.




**Obrázek 4: NTLM autentizace**

*Zdroj: (Ofer, 2014)*

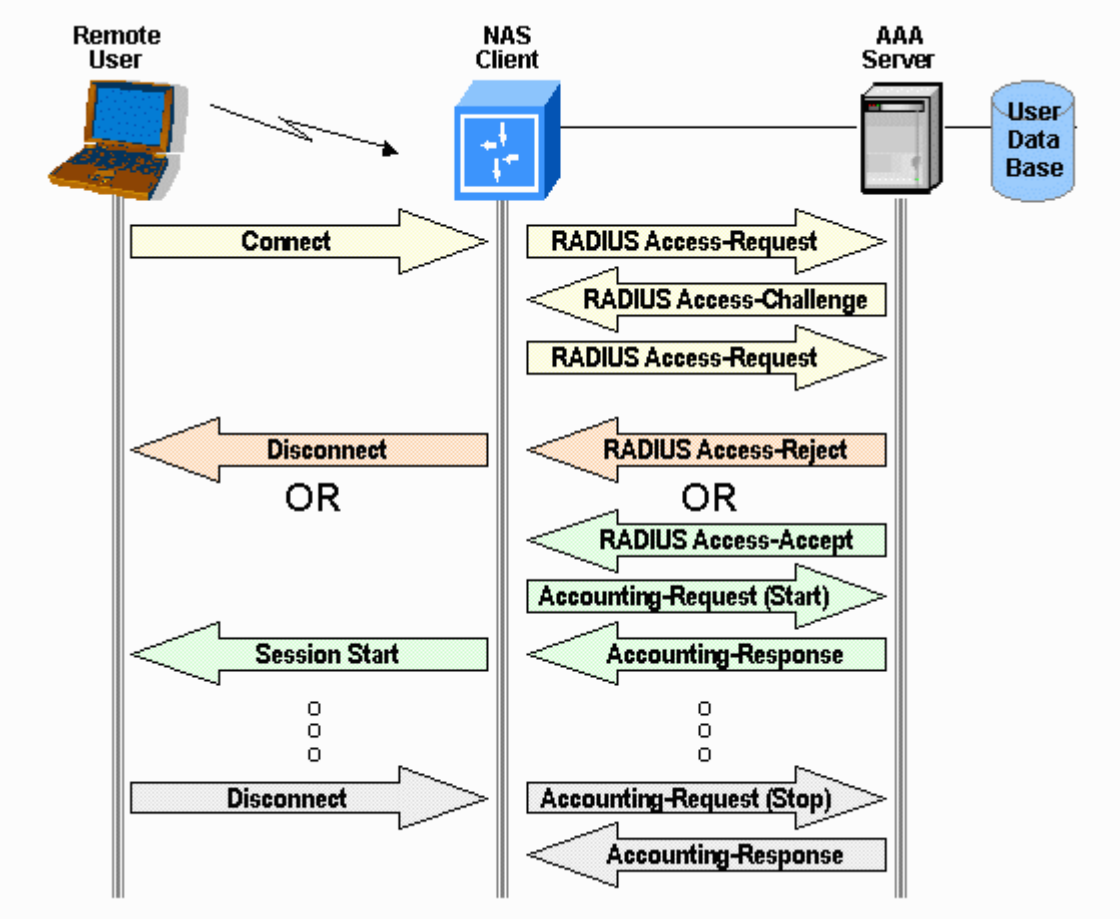
## 2.3 RADIUS

RADIUS protokol byl vytvořen za účelem centralizace autentizace, autorizace a účetnictví. Odtud také název AAA (Authentication, Authorization, Accounting), jenž je s protokolem RADIUS úzce spjatý. Jeho cílem je ulehčit síťovým přístupovým serverům (NAS) v tom smyslu, že u sebe nemusejí uchovávat informace o uživatelských účtech. Žádosti o získání přístupu ke zdrojům v síti jsou protokolem RADIUS posílány na autentizační server (AAA server) uchovávající si centrální databázi uživatelů, který rozhoduje o jejich přístupu. Tímto způsobem je možné zajistit jednoduchou škálovatelnost a obsloužit tak velké množství NAS zařízení.

Na obrázku níže je zobrazena funkčnost protokolu v bezdrátové síti. Jedná se o komunikaci mezi třemi základními zařízeními – přenosné zařízení uživatele, přístupový bod (AP) – v tomto případě NAS klient a AAA server, jenž disponuje databází uživatelů. Komunikace mezi těmito zařízeními probíhá dle (Hassell, 2003, s. 64) díky protokolu RADIUS následovně:

1. Po připojení uživatele k AP zašle NAS zařízení RADIUS Access-Request zprávu na AAA server. V dané zprávě předává informace o uživateli, například uživatelské jméno, heslo, port či identifikace NASu.
2. Po obdržení zprávy AAA server provede kontrolu, zda se dané zařízení NAS může vůbec AAA serveru dotazovat. Pokud ano, vyhledá uživatele v databázi, porovná hesla, případně další atributy a provede rozhodnutí, zda je daný uživatel úspěšně autentizován či nikoliv.
3. Poté záleží na použité autentizační metodě. AAA server může vrátit RADIUS Access-Challenge zprávu obsahující náhodné číslo. NAS jej předá uživateli (například užitím CHAP). Uživatel poté musí odpovědět správnou hodnotou (například zašifrováním Challenge zprávy svým heslem). NAS tuto zprávu předá zpět na AAA server uvnitř nové RADIUS Access-Request zprávy.
4. Pokud AAA server rozhodne, že uživatel může ke zdroji, pak vrátí RADIUS Access-Accept zprávu. Pokud rozhodne v neprospěch uživatele, zašle RADIUS Access-Reject zprávu a NAS zařízení uživatele odpojí.
5. Pokud AAA server zašle Access-Accept zprávu a RADIUS účetnictví je nakonfigurováno, pak NAS zašle RADIUS Accounting-Request zprávu na AAA server (jedná se o účetní zprávu typu Start). AAA server poté vloží účetní zprávu do svého logu a potvrdí přijetí zasláním Accounting-Response zprávy. Po obdržení této zprávy NAS aktivuje uživateli session.

6. V případě, že chce NAS poté ukončit session uživateli, pošle zároveň na AAA server Accounting-Request(Stop) zprávu, jež se propíše do logu a zašle zpět potvrzení zprávou Accounting-Response.




**Obrázek 5: RADIUS autentizace**

*Zdroj: (Phifer, 2003)*

# 3 Jednotné přihlášení

Současnost klade na zabezpečení sítě velký důraz a jednou z jejích hlavních složek je autentizace. Ta se dá chápat jako vstupní bod nebo též brána ke zdrojům, které se nachází na určitém místě v nějaký čas. Tyto zdroje mohou mít hardwarový či softwarový charakter. Mohou mít též datový a finanční charakter, pokud se k nim dostane neoprávněná osoba. Například únik citlivých informací ze společnosti může mít za následek velké finanční ztráty a v těch nejhorších situacích i úplný konec firmy. Zejména z tohoto důvodu je požadováno, aby byla korporátní síť co nejlépe zabezpečena proti vniknutí neoprávněné osoby. Aplikovat se dá hned v několika vrstvách:

- První vrstvou je fyzicky zabezpečit přístup do místností s infrastrukturními prvky tak, aby skutečně pouze povolené osoby měli možnost se k zařízením dostat.
- Druhou vrstvou je systém zabezpečení samotného přihlašování uživatelů do sítě.
- Třetí vrstvou je způsob kontroly komunikace přihlášeného uživatele mezi jednotlivými sítěmi.
- Čtvrtou vrstvou je autentizace ke službám či aplikacím.

## 3.1 Výhody jednotného přihlášení

Z výše uvedeného systému zabezpečení je zřejmé, že takový uživatel bude nucen být autentizován relativně často. Nicméně časté zadávání přihlašovacích údajů do systému vede k potenciálnímu problému s jejich únikem buď při odposlechu sítě, nebo prozrazení při zadávání, kdy se dotyčnému jiná osoba kouká přes rameno.

Řešením takového problému je omezit zadávání těchto údajů na minimum. Takové řešení si vyžaduje centrální autentizační systém, který bude uchovávat přihlašovací data uživatelů a musí umožňovat ostatním systémům v síti, aby dané události mohly číst. Ostatní systémy tak získají potřebná data o jednotlivcích, kteří se už přihlásili, a nebude po nich již žádné další zadávání údajů vyžadovat. Takové řešení umožňuje zachovat maximální integritu uživatelských údajů a rapidně zefektivňuje práci jednotlivců, kteří se nemusí neustále ověřovat u různých systémů svým uživatelským jménem a heslem.

## 3.2 Jak jednotné přihlášení v síti funguje

Síťové jednotné přihlášení v praxi znamená, že se jedinec přihlásí na svém pracovním počítači do domény nejčastěji zadáním svého identifikačního řetězce a hesla, provede se ověření správných údajů na doménovém řadiči, kde je vytvořena patřičná událost indikující buď úspěch, nebo neúspěch přihlášení. Uživatel dostane zpět zprávu, zda došlo k úspěšnému přihlášení či nikoliv. Pokud celý proces proběhl neúspěšně, uživatel může zkusit další pokus. Pokud vše proběhlo úspěšně, je uživatel připuštěn do sítě a může začít komunikovat s okolím a případně se světem.

Nyní se však nabízí otázka, jak daného uživatele nejen chránit proti malwaru, spamu, virům, trojským koňům apod., ale také jak konkrétního jedince nebo skupinu jedinců omezit v přístupu k určitým zdrojům sítě. Například každá větší firma má servery spravující choulostivá data a správci chtějí mít kontrolu nad tím, jak se k nim bude přistupovat, kdo k serverům bude mít povolení přístupu, jakým protokolem, s jakým operačním systémem apod. To vše je možné definovat až na úroveň jednotlivců nebo skupin a provádí se na síťových firewallech nebo obecně na zařízeních podporující identifikaci uživatele a aplikování patřičných bezpečnostních politik na základě jeho identity. Aby toto zařízení bylo schopné uživatele rozpoznat, a zároveň jej neobtěžovalo s další výzvou o autentizaci, informuje se o jeho přihlášení na doménovém řadiči automaticky.

Nyní když uživatel začne posílat pakety přes dané zařízení dál do sítě, bude jeho komunikace identifikována. Poté na ní bude aplikována patřičná bezpečnostní politika a dojde k rozhodnutí, zda komunikaci povolit nebo zahodit.

## 3.3 Nevýhody jednotného přihlášení

Systém jednotného přihlášení však nedisponuje pouze pozitivními vlastnostmi a ty negativní mohou mít v případě úspěšného zneužití tragický dopad.

SSO využívá centrální databázi pro správu a ověřování identit. To znamená, že prolomí-li útočník zabezpečení tohoto serveru, pak je schopen získat přístup do všech služeb na síti využívající systém jednotného přihlášení. To samé platí při prozrazení hesla libovolného uživatele. V takovém případě získá útočník opět přístup ke všem zdrojům, ke kterým má daný uživatel povolení. Bez SSO by uživatel měl ideálně disponovat sadou uživatelských údajů a ke každé službě použít jinou. Každá služba by tedy měla vlastní databázi s uživatelskými

údaji, které se liší od údajů uživatele v databázi jiné služby, a autentizace by probíhala přímo mezi uživatelem a danou službou (nikoliv přes centrální autentizační server). Pokud by nyní útočník získal data uživatele, získal by přístup pouze k jedné jediné službě.

Další potenciální nevýhodou SSO je závislost přenosu dat při autentizaci přes síť. V případě, že jsou linky, případně síťové karty autentizačního serveru přetíženy, pak ověřování identit bude pomalé či zcela nefunkční. Podobný problém může též nastat při nadměrném přetížení výpočetní kapacity serveru.

Problémy může způsobit také využívání pouze jednoho autentizačního serveru. Důvodem je neredundantnost. To znamená, že v případě výpadku daného serveru nebude schopen žádný server provádět centrální autentizaci. Děje se tak proto, že prakticky existuje pouze jeden takový, který se náhle stal nefunkčním. Ověřit svoji identitu tak nebude moci absolutně nikdo a nic prakticky až do doby jeho znovuzprovoznění.

Na všechny výše uvedené potenciální problémy samozřejmě existují metody a technologie, které jsou schopné je řešit a v některých případech vyřešit úplně. Je však zapotřebí je mít hned v úvodu na mysli, aby se s nimi již při implementaci počítalo a nedošlo k selhání sítě.

V následující sekci 3.4 je uvedena hrstka legislativních důvodů, které systém jednotného přihlášení pomáhá řešit nejen v České republice, ale také ve světě.

## 3.4 Legislativa a SSO

Prakticky v každé vyspělé zemi existuje zákon o ochraně osobních údajů. V České republice se jedná o zákon č. 101/2000 Sb., který například v § 5 odst. 1 písm. f) říká, že lze zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny. Dále, zaměří-li se čtenář například do sekce zdravotnictví, dle (Úřad pro ochranu osobních údajů, 2013) osoby oprávněné nahlížet do zdravotnické dokumentace, jsou taxativně vyjmenovány v § 67b odst. 10 zákona č. 20/1966 Sb. Jedná se zejména o osoby vykonávající zdravotnickou činnost a o osoby pracující ve státní správě řešící zdravotnictví.

Obecně lze tedy tvrdit, že každý subjekt zpracovávající osobní údaje občanů České republiky, musí získaná data patřičným způsobem chránit. Ve zdravotnictví to pak platí dvojnásob. Jsou-li data uchovávána elektronicky, pak je nutností umožnit přístup k získaným informacím pouze oprávněným osobám. V takovém případě může být jednotné síťové přihlášení ve spolupráci s bezpečnostními politikami nastavenými například na síťovém firewallu prakticky jedním

ze základních bezpečnostních prvků, jenž odstíní přístup k citlivým informacím nechtěným osobám. Děje se tak proto, že firewall identifikuje jedince na základě jejich identity a při průchodu jejich paketů skrze síťový firewall dojde ke kontrole a komunikaci neoprávněných osob ke zdrojům s citlivými daty zahodí.

Při pohledu do jiných zemí světa je například ve Spojených státech amerických platná regulace HIPPA (Health Insurance Portability and Accountability Act) jehož sekce s názvem Privacy Rule (pravidlo soukromí) striktně reguluje a chrání osobní data občanů ve zdravotnictví. Dle (Oracle Corporation, 2010) jsou zdravotnické organizace prakticky nuceni využít technologie SSO a tím se tak zabezpečit proti úniku citlivých dat z organizace.

V další části textu bude pojednáváno o konkrétní implementaci jednotného přihlašování na zařízeních celosvětového výrobce nejen síťových firewallů společnosti Fortinet. Nicméně velice podobný způsob implementace byl realizován též například společnostmi Cisco i Checkpoint.

## 3.5 Fortinet Single Sign-On (FSSO)

Fortigate firewall od společnosti Fortinet umožňuje ověřovat uživatele ve spolupráci s adresářovou službou Windows Active Directory (AD). Následně aplikuje bezpečnostní politiky na komunikaci přihlášeného uživatele, a zároveň nepotřebuje, aby se daný jedinec znovu ověřoval na Fortigate.

### 3.5.1 FSSO bezpečnostní politiky

Bezpečnostní politiky určují fungování firewallu a z pohledu FSSO se dají pochopit a klasifikovat na dva druhy:

1. Obecné politiky – nedefinují na jakou FSSO skupinu uživatelů se vztahují. Platí obecně pro všechny uživatele bez ohledu na kontrolu identity.
2. FSSO politiky – říká se jim též politiky založené na identifikaci uživatele. Definují na jakou FSSO skupinu uživatelů budou mít vliv a je aplikována jen a pouze na komunikaci pocházející od uživatelů patřící do dané FSSO skupiny.

Jelikož jedním z cílů je mít přehled nad tím, co uživatel na síti dělá a umožnit mu průchod na základě jeho práv, je vhodné a žádoucí používat pouze politiky typu FSSO. U politik obecných totiž nedochází k rozhodování na základě práv jednotlivců nebo skupin, ale dochází pouze

k rozhodování, zda bude paketu průchod povolen nebo zamítnut. V takovém případě by docházelo k obejití FSSO mechanizmu a celý proces identifikace by ztrácel na významu.

### 3.5.2 FSSO skupiny

Jednotlivci, skupiny nebo celé organizační jednotky z AD jsou zvoleny správcem pomocí LDAP protokolu (z globálního katalogu) a následně vloženy do speciální FSSO skupiny na firewallu. Společně s explicitně definovanými FSSO skupinami se při vytváření Single Sign-On systému automaticky vytvoří též implicitní skupina s názvem SSO_Guest_users. Tuto skupinu je možné využít v případě, že některá zařízení v síti nejsou vložena do domény. Může se jednat o síť vyhrazenou pro návštěvníky, BYOD (Bring your own device) zařízení zaměstnanců, například tablety, notebooky, smartphony apod.. Z pohledu firewallu jsou taková zařízení neautentizována a veškerá komunikace pocházející od nich by byla defaultně zahozena. Proto je možné vytvořit bezpečnostní politiku s velmi limitujícím přístupem do sítě umožňujícím neautentizovaným zařízením komunikovat s okolím alespoň nějakým způsobem. Například pouze pomocí HTTP/HTTPS protokolu a to pouze na bezpečné webové stránky. Důležitým postřehem je, že politika využívající SSO_Guest_Users se stává aktivní teprve v tom případě, že všechny ostatní politiky jsou také typu FSSO. Výjimkou je výchozí Deny politika, která má za úkol zahodit veškeré pakety neshodující se s žádnou explicitně definovanou politikou. Pokud má tedy firewall definovány FSSO politiky včetně té pro neautentizovaná zařízení a disponuje též politikou obecnou (nikoliv FSSO), pak bude vždy při průchodu paketů od neověřených zařízení zachycena shoda s obecnou politikou nikoliv s FSSO politikou pro neověřené hosty.

### 3.5.3 Agenti

FSSO používá různé agenty, které mají společný cíl, a to monitorovat logony (přihlášení) uživatelů a předat je Fortigate. V momentě, kdy se uživatel přihlásí na svém pracovním zařízení do domény, agenti dle (FortiOS Handbook, 2016, s. 626)

- detekují logon události a zaznamenávají si
    - název zařízení,
    - název domény,
    - jméno uživatele,
- dále z názvu zařízení zjistí jeho IP adresu,
- zjistí, do jakých doménových skupin uživatel patří,

- pošle informace a přihlášení uživatele na Fortigate včetně IP adresy a názvů skupin, do kterých patří,
- z těchto údajů vytvoří jeden nebo více logovaných záznamů na Fortigate.

Fortinet vytvořil agenta také pro sítě disponující technologií od společnosti Novell, nicméně zaměření této práce je zejména na prostředí Windows a bude se týkat tří různých agentů, které pro něj existují:

1. Domain Controller (DC) agent
2. Citrix/Terminal Server (TS) agent
3. Collector agent (CA)

Pro hlubší porozumění těchto nezbytných komponent FSSO jim bude v následující části textu věnována větší pozornost.

### 3.5.4 Domain Controller (DC) agent

Musí být nainstalován na každém doménovém řadiči, pokud je použit režim DC Agent. Není však potřeba, pokud je FSSO užíváno v Polling režimu.

### 3.5.5 Citrix/Terminal Server (TS) agent

Je instalován na terminálový server a monitoruje uživatele, kteří se na něj přihlašují a vytváří si tam své relace. TS agent má za úkol na terminálovém serveru alokovat pro každého přihlášeného uživatele jiné rozmezí portů, které identifikuje odesílání a příjem paketů pro konkrétního jedince.

### 3.5.6 Collector agent (CA)

Instaluje se na libovolný server ve Windows AD doméně. Jeho cílem je monitorovat a uchovávat logon informace a zasílat je na Fortigate. Je schopen získávat informace trojím různým způsobem.

- Od DC agenta.
- Od TS agenta.
- Dotazováním se přímo na doménový řadič (Polling režim). V tomto způsobu implementace není potřeba instalovat na doménové kontroléry DC agenta.

**Další fakta o CA:**

- Collector agent slouží mimo jiné k odbavování NTLM žádostí od klientských prohlížečů tehdy, když je Fortigate nastaven na přeposílání NTLM komunikace na CA.
- Dle (FortiOS Handbook, 2016, s. 627) CA je též zodpovědné za DNS vyhledávání, kontrolu skupin a zařízení. Posílá také lokální doménovou bezpečnostní skupinu a globální bezpečnostní skupinu na Fortigate.
- CA využívá pro komunikaci s Fortigatem TCP port 8000 a pro komunikaci s DC agenty naslouchá na UDP portu 8002.
- Každý Fortigate může mít nastaven maximálně 5 Collector agentů, kdy v jeden čas probíhá komunikace maximálně s jedním CA. Pokud se aktivní CA stane nedostupné, zkusí Fortigate kontaktovat další CA v pořadí.

### A) Režim Collector agenta (Standard/Advanced)

Administrátor má možnost využívat CA v režimu Standard (klasický) nebo Advanced (pokročilý). Vztahuje se ke způsobu přístupu k Active Directory a práci s uživateli. Oba režimy fungují stejně až na 3 odlišnosti:

1. Standardní režim používá klasickou Windows syntaxi typu doména\uživatel, zatímco Advanced režim používá LDAP syntaxi typu: CN=uživatel, OU=název, DC=doména.
2. Na CA se běžně nastavují tzv. skupinové filtry. To jsou filtry, které specifikují, jaké uživatele, skupiny či organizační jednotky má CA sledovat a posílat na Fortigate. V případě, že je CA nastaven v Advanced módu, dochází k definování skupinových filtrů od Fortigate. Pokud je nastaven na chod ve Standard režimu, musí si je administrátor nadefinovat sám v uživatelském rozhraní Collector agenta.
3. Dle (FortiOS Handbook, 2016, s. 630) Advanced režim podporuje vnořené skupiny a jejich dědičnost. Například při monitorování určité rodičovské skupiny jsou automaticky monitorovány i její potomci, tj. skupiny, které od rodičovské skupiny dědí až dolů po hierarchii. To Collector agent ve Standard režimu nepodporuje a je tedy nutné definovat jednotlivé skupiny uživatelů explicitně.

### B) Porty na CA serveru

Při instalaci Collector agenta se v softwarovém firewallu operačního systému serveru neotevřou automaticky porty pro komunikaci s DC agentem a Fortigate. To je zapotřebí udělat manuálně.

Pokud to administrátor neudělá, nebude mezi nimi zasílání zpráv fungovat. Ve výchozím nastavení probíhá komunikace na

- TCP portu 8000 vůči Fortigate a
- UDP portu 8002 vůči DC agentům.

**C) Periodická kontrola přihlášených**

Při vykonávání kontroly přihlášených uživatelů na určitém zařízení posílá Collector agent pakety na cílové TCP porty 139 a 445. Proto je třeba nejdříve otevřít zmíněné porty nejen ve Windows firewallu hostů, ale také na všech síťových firewallech, které se nacházejí v cestě mezi CA a kontrolovanými klientskými zařízeními. Cílem této verifikace je ověřit, zda je daný uživatel na zařízení stále přihlášen. Ve výchozím nastavení dochází ke kontrole každých 5 minut.

**D) Smazání neaktivních záznamů**

Aby se počet záznamů v Collector agentovi neustále jen nerozšiřoval, Fortinet do něho implementoval mechanizmus odmazávání dle (FortiOS Handbook, 2016, s. 644) již neaktivních (neverifikovaných) záznamů ze své databáze. Záznam se stává neverifikovaným tehdy, když zařízení není dostupné nebo se uživatel zapomněl odhlásit. Ve výchozím nastavení se jedná o interval kontroly po osmi hodinách.

**E) Periodická kontrola IP adres hostů**

Vzhledem k dynamickému přidělování IP adres pomocí DHCP většině hostů v síti je dobré kontrolovat, zda zařízení, na kterém je uživatel aktuálně přihlášený, má stále stejnou IP adresu, jako měl při prvotní autentizaci. Pokud by se jeho IP adresa změnila a CA by změnu neuměl zaznamenat, mohlo by být s takovým uživatelem zacházeno podle jiných bezpečnostních pravidel, než jsou mu vlastní na Fortigate. Takové chování by pro něj jistě přineslo nepříjemnosti a nepochybně potenciálně využitelnou zranitelnost sítě.

Z takového důvodu CA umožňuje periodicky kontrolovat, zda se IP adresa přihlášeného uživatele nezměnila, pokud ano, provede aktualizaci zjištěné informace nejen u sebe, ale i na Fortigate. Dle (FortiOS Handbook, 2016, s. 644) ve výchozím nastavení provádí kontrolu každých 60 sekund.

Pokud však administrátor spravuje síť, která nepoužívá dynamické přidělování IP adres (DHCP) a všechna zařízení mají adresy statické, je tato kontrola zbytečná. Správce má pak tu možnost verifikace adres zrušit.

Dle (FortiOS Handbook, 2016, s. 644) Kontrola změny IP adres není aplikovatelná na uživatele, kteří se verifikovali pomocí NTLM. Zde je třeba po změně IP adresy provést autentizaci znova.

**F) Skupinové filtry a seznam ignorovaných uživatelů**

Jedním z úkolů Collector agenta je vyfiltrovat logon informace, které posílá na Fortigate. Pokud správce sítě zajímají jen určité LDAP skupiny uživatelů, bylo by zcela zbytečné posílat na Fortigate informace o všech realizovaných přihlášeních (děje se ve výchozím nastavení) jen proto, aby je následně Fortigate vůbec nevyužil. Takové mrhání prostředků by firewall jen zbytečně zatěžovalo nejen po stránce zpracovávání, ale též po stránce větší alokace místa v paměti. Nehledě na zbytečné mrhání prostředků na ostatních zařízeních v síti, například při routování paketů, včetně zbytečného vytěžování linek mezi nimi.

Definováním skupinových filtrů (group filters) a seznamu ignorovaných uživatelů (ignore user list) je možné omezit množství zasílaných logon informací na Fortigate a tím tak šetřit nejen jeho zdroje, ale i zdroje dalších zařízení v síti.

### 3.5.7 Režimy FSSO

Jednotné síťové přihlášení od Fortinetu disponuje hned několika režimy. Záleží na topologii, technologii a v neposlední řadě také na propustnosti a výkonu serverů, kterými daná síť disponuje. Po jejich analýze se administrátor může rozhodnout, jaký režim bude nejvhodnější zvolit. Na výběr má mezi těmito režimy:

- DC agent
- Polling
- TS agent
- NTLM

V následujících sekcích je jednotlivým režimům věnována bližší pozornost.

**A) Režim DC Agent**

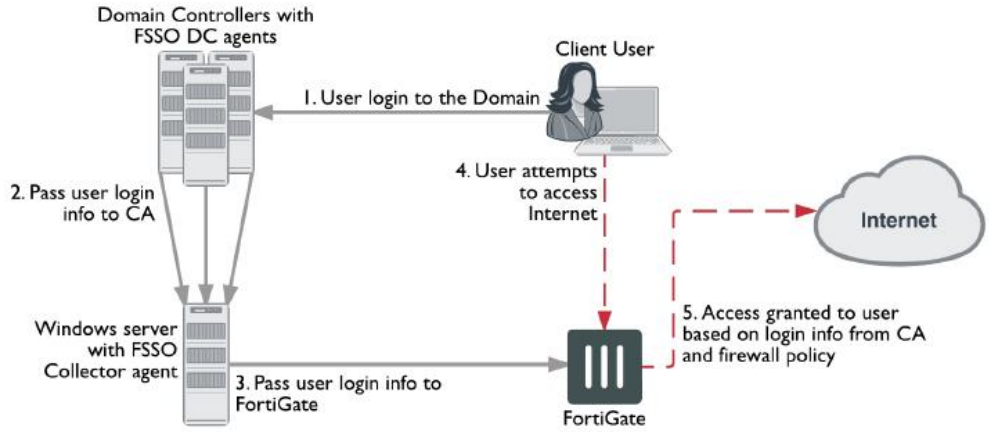
DC agent je běžně instalován na všechny doménové řadiče a jeho činnost spočívá v monitorování lokálních logon událostí a následné jejich předání Collector agentovi, jenž si dané informace uloží a poté pošle na Fortigate.

Vzhledem k tomu, že se do domény mohou uživatelé autentizovat pomocí jakéhokoliv řadiče, je nutné sledovat logon události na každém doménovém kontroléru v síti. Pokud by se tak

nedělo, docházelo by k nezachycení určité části přihlašovacích informací a někteří jedinci by byli Fortigatem vnímáni jako neautentizovaní.

Na obrázku níže je názorně ukázáno fungování FSSO v režimu DC Agent. Sestává se celkem z pěti kroků:

1. Uživatel se přihlásí do domény na svém pracovním zařízení. Ověření jeho údajů probíhá na jednom z doménových kontrolérů, kde je nainstalován DC agent.
2. DC agent monitoruje logon události a posílá je na Collector agenta.
3. Collector agent si je zaznamená a pošle na Fortigate.
4. Fortigate si informace o logon událostech uloží a při pokusu přihlášeného uživatele posílat pakety skrze firewall je úspěšně identifikován.
5. Přístup do Internetu mu je v tomto případě povolen.




**Obrázek 6: FSSO v režimu DC Agent**

*Zdroj: (FortiOS Handbook, 2016, s. 629)*

### Výhody a nevýhody DC Agent režimu

Výraznou nevýhodou na produkčních systémech je, že po instalaci DC agenta je vyžadován restart doménového řadiče. To je v některých případech velký problém a někdy je to dokonce i nereálné. Ve většině případů je nutné připravit plán údržby doménového kontroléru a počkat na ideální čas na restart. Takové čekání může v určitých případech trvat relativně dlouhou dobu.

Další nevýhodou DC agenta je, že sdílí prostředky spolu s doménovým řadičem. Některé doménové kontroléry mohou být natolik vytížené, že by již nebylo dobré, aby vykonávaly další úkoly. V jiných situacích se může jednat o princip, kdy hlavním cílem je okamžité zpracování žádosti o přihlášení a opět snaha doménový kontrolér nezatěžovat věcmi, které s okamžitým

přihlášením přímo nesouvisí. Nehledě na fakt, že dle (FortiOS Handbook, 2016, s. 629) DC agent vyžaduje minimálně 64kbps bandwidth/propustnost linky, což přidává na jejím vytížení.

Tyto problémy se dají řešit implementací FSSO v dotazovacím režimu. Než to však administrátor udělá, bylo by dobré se zmínit o jedné velmi podstatné výhodě. Značným plusem režimu DC Agent je spolehlivější monitoring logon událostí v porovnání s dotazovacím režimem (Polling). DC agent nepřetržitě hlídá, aby mu neunikl jediný údaj o přihlášení. Může tak dělat proto, že se nachází fyzicky přímo na serveru (DC), který autentizaci vykonává. Naopak dotazovací režim (Polling) je schopen doménové řadiče požádat o logon informace jen v určitých intervalech. Pokud je na systém nahrnuto velké množství žádostí o přihlášení, nemusí aktualizační zpráva od DC obsahovat všechny logon informace, a tak může dojít k jejich nezaznamenání.

**Tabulka 1: Zhodnocení DC Agent režimu**

| Výhody | Nevýhody |
|---|---|
| Spolehlivý monitoring událostí o přihlášení | Nutný restart doménového kontroléru |
| | Sdílení prostředků s doménovým kontrolérem |

*Zdroj: vlastní*

### B) Dotazovací režim (Polling)

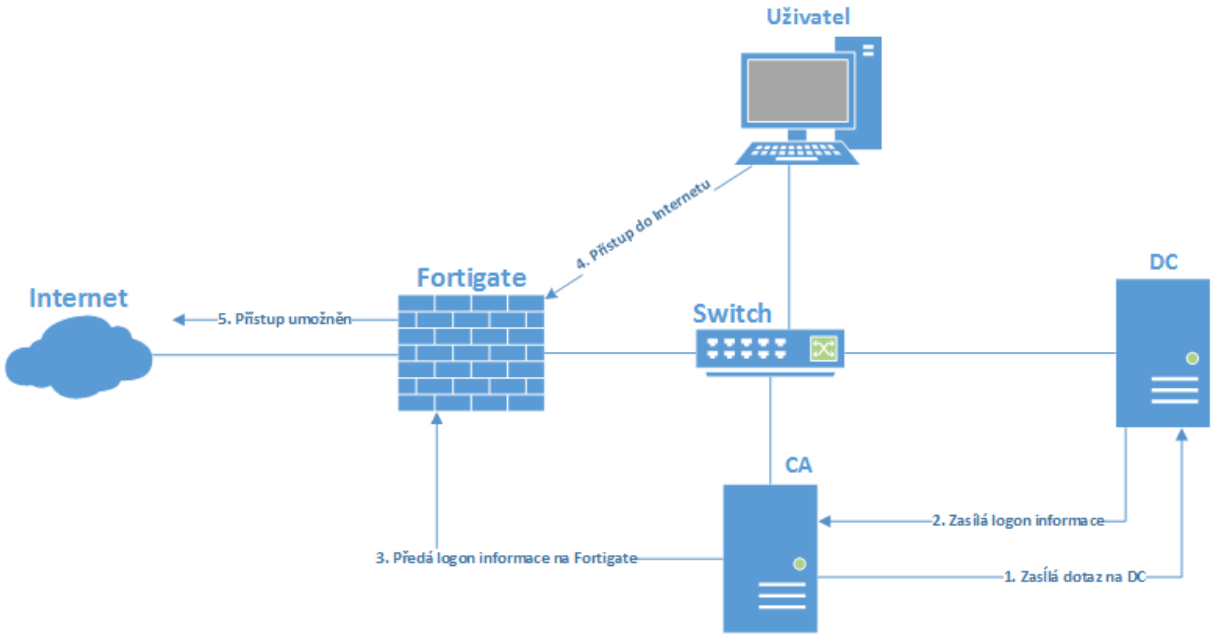
Pro konfiguraci tohoto režimu není nutné instalovat DC agenta na doménový kontrolér. Dotazování probíhá ze dvou zdrojů:

1. Collector agent
2. Fortigate

O logon informace se tedy může na doménový kontrolér dotazovat Collector agent anebo přímo Fortigate. Na obrázku níže je názorně ukázáno fungování FSSO v dotazovacím režimu. Sestává se celkem z pěti kroků:

1. Collector agent, jenž je nainstalovaný na obyčejném serveru v doméně, zašle žádost na doménový kontrolér za použití NetAPI, Event log nebo Event log s WMI (vysvětleny níže).
2. DC pošle zpět logon informace na CA, jenž si je uloží a pošle aktualizační zprávu na Fortigate.
3. Fortigate provede zápis přihlášených do své databáze.
4. Klient iniciuje připojení do Internetu přes Fortigate.

5. Firewall klientovi v tomto případě přístup do Internetu umožní.




**Obrázek 7: FSSO v Polling režimu**

*Zdroj: vlastní*

Každých pár sekund Collector agent posílá na doménové kontroléry, na cílový port 445, žádost o logon informace a po jejich obdržení si je zaznamená a přepošle na Fortigate. Aby mu žádné logon informace neunikly, je důležité na CA nastavit dotazování se na všechny doménové řadiče v síti, neboť uživatelé se mohou autentizovat do domény pomocí jakéhokoliv doménového kontroléru.

### NetAPI, Event log nebo Event log s WMI

Při dotazování se na doménový kontrolér je možné použít jednu z následujících metod:

1. **NetAPI dotazování** – dle (Fortinet Knowledge Base, 2014) každých 9 sekund provede sken doménových řadičů. Využívá k tomu API společnosti Microsoft z knihovny netapi32.dll, konkrétně funkci NetSessionEnum. Snaží se objevit uživatele, kteří vytvořili session s doménovým kontrolérem. V případě, že je DC pod velkým nátlakem přihlašovacích relací, může dojít k vynechání či nepovšimnutí si některých údajů z počtu přihlášených jedinců. Jeho fungování je rychlejší než Event log dotazování.
2. **Event log dotazování** – dle (FortiOS Handbook, 2016, s. 629) musí být tento typ dotazování nastaven, pokud v síti existují uživatelé s operačním systémem Mac OS,

kteří se snaží se přihlásit do Windows AD domény. Vyžaduje si rychlé linky, ale jeho velkou výhodou je, že na rozdíl od NetAPI, nevynechá logon informace.

3. **Event log s WMI dotazováním** – dle (Microsoft Developer Network, 2016) je Windows API rozhraní umožňující získání událostí z Windows serveru a tedy i z doménového řadiče. V tomto případě Collector agent zastává roli WMI událostního konzumenta, jenž si určí, které události chce z DC obdržet. WMI událostní poskytovatel (role DC) mu informace o specifikovaných událostech zašle. Výhodou je redukované vytížení linek.

### Výhody a nevýhody Polling režimu

Jak bylo poznamenáno v úvodu, je možné přimět Fortigate dotazovat se na DC přímo. Tato varianta je jednoduchá na konfiguraci a údržbu. Je však vhodná pouze pro malé sítě typu SOHO (Small office / Home office) a dle (Fortinet Customer Service & Support, 2015) není doporučena pro rozsáhlejší implementaci.

Výraznou potenciální nevýhodou je nezaznamenání některých logon informací v případě, že je po systému vyžadováno velké množství přihlášených uživatelů v daném čase.

Naopak výhodou je snazší implementace a údržba, neboť není nutné instalovat DC agenta přímo na doménový kontrolér, a tím pádem není ani nutné žádné klíčové zařízení kvůli FSSO restartovat.

Další výhodou je disponování s vlastními zdroji. CA může být nainstalován na jakýkoliv server v síti. Nemusí se dělit o zdroje s doménovým řadičem.

**Tabulka 2: Zhodnocení Polling režimu**

| Výhody | Nevýhody |
|---|---|
| Jednoduché nastavení a údržba | Možnost nezaznamenání událostí o přihlášení |
| Nevyžadován restart doménového kontroléru | |
| Není nutnost sdílet prostředky s doménovým kontrolérem | |

*Zdroj: vlastní*

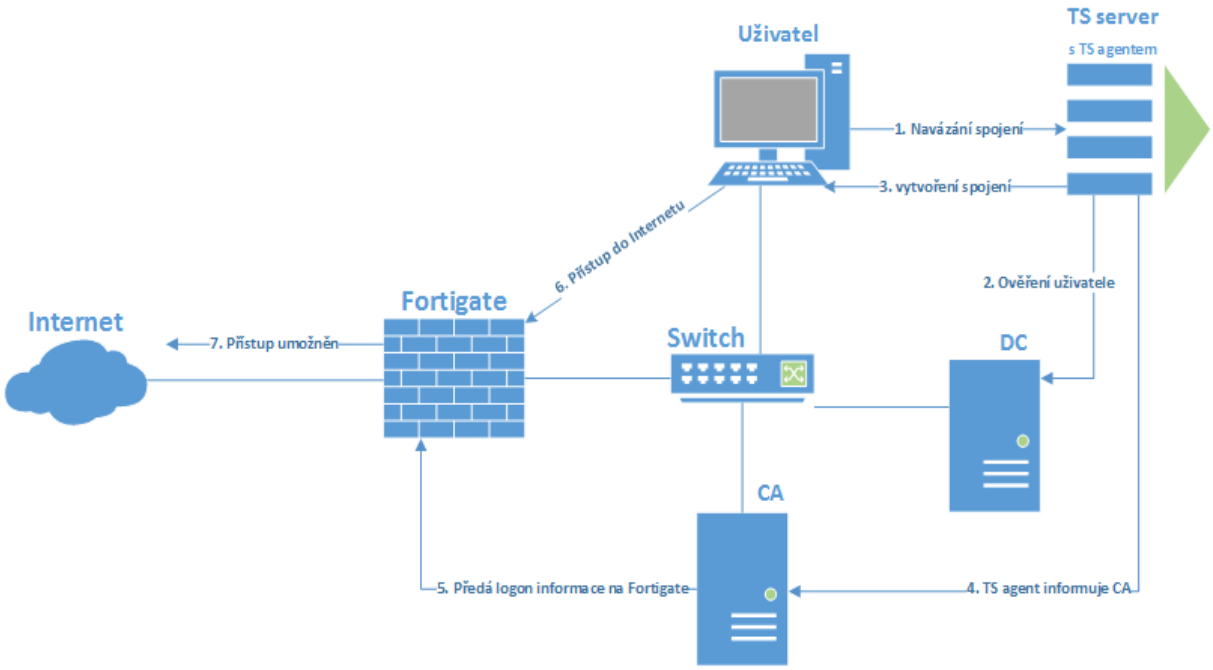
### C) Režim TS Agent

Všichni uživatelé přihlašující se na terminálový server sdílí jednu a tu samou IP adresu serveru. V takovém případě není možné odlišit jejich komunikaci použitím IP adresy. Z tohoto důvodu se na každý terminálový server v síti instaluje TS agent, který monitoruje aktivní relace uživatelů na TS serveru, přidělí jim rozmezí portů, které mohou používat a pošle tyto informace na Collector agenta, jenž má za úkol informovat Fortigate. Tímto způsobem se jedinec nemusí znovu autentizovat na firewallu vyžadujícího si směrování na základě jeho identity. Při inicializaci své komunikace jednoduše používá zdrojové porty v rozmezí těch alokovaných a při průchodu skrze Fortigate je identifikován na základě zdrojových portů. Výchozí nastavení TS agenta je přidělovat porty v rozmezí 1024 – 49151. Každému uživateli přidělí 200 sekvenčně po sobě jdoucích portů. A pokud se stane, že daný počet portů nestačí, TS agent umožňuje alokovat ještě jedenkrát dalších 200 portů. Výchozí nastavení je konfigurovatelné a každý správce sítě si atributy TS agenta může přizpůsobit dle požadavků vlastní sítě.

Potenciálním problémem bývá, že ne všechny aplikace se rozhodnou používat alokované zdrojové porty a snaží se komunikovat jinými. Tehdy musí být myšleno i na zadní vrátka. Je třeba vytvořit na Fortigate bezpečnostní politiku, která pakety z náhodných portů bude umožňovat. Buď definováním politiky pro neautentizované uživatele za použití SSO_Guest_Users skupiny anebo vytvořením vlastní služby identifikující rozmezí TS agentem nealokovaných portů pro jednotlivé protokoly.

TS Agent režimu se někdy také říká Citrix FSSO, protože se dá použít též na Citrix TS serverech. Z tohoto důvodu jsou autentizovaní jedinci na Fortigate vedeni jako FSSO_Citrix uživatelé.

Na obrázku níže je zobrazeno uspořádání sítě v režimu TS Agent s jednotlivými kroky, které jsou pod ním řádně vysvětleny.




**Obrázek 8: FSSO v režimu TS Agent**

*Zdroj: vlastní*

1. Uživatel inicializuje terminálové spojení například pomocí RDP protokolu.
2. TS server požádá Active Directory o autentizaci uživatele.
3. Po úspěšném ověření se vytvoří spojení mezi klientem a TS serverem. Zároveň TS agent alokuje porty pro navázanou relaci.
4. Uživatel se snaží komunikovat s jinou sítí nebo internetem.
5. Fortigate uživatele rozpozná na základě jeho zdrojových portů v komunikaci a umožní mu přístup.

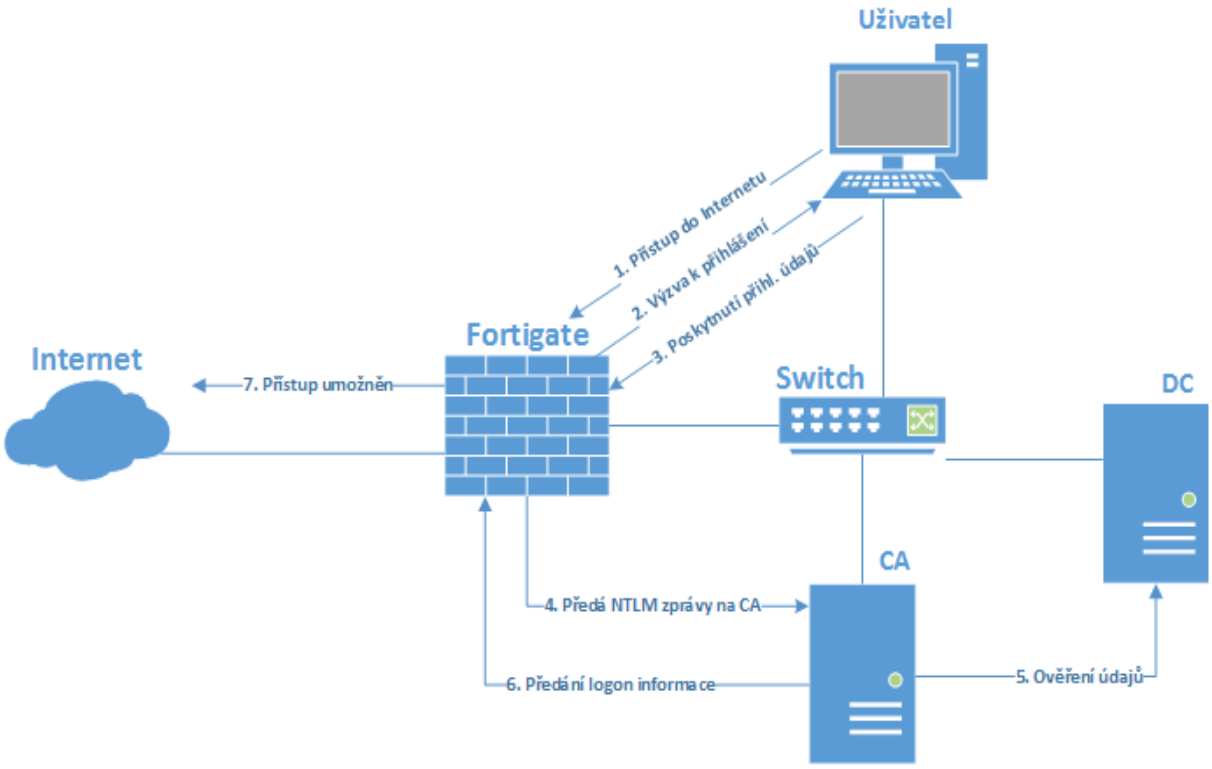
### D) Režim NTLM

Pomocí NTLM ověření je možné zajistit, aby i zařízení, která nejsou vložená do domény (tj. používají jen lokální účty), byla schopna ověřit uživatele (doménovým účtem) přes webové rozhraní. Takový jedinec pak ze svého zařízení může komunikovat stejně jako z počítače fyzicky přidaného v doméně a nemusí se již ověřovat znovu. Na takovém zařízení je nutné v prohlížeči nastavit proxy přes Fortigate, aby se uživatel byl schopen přihlásit a informoval Single Sign-On systém o své prezenci na daném zařízení.

Collector agent ve spolupráci s doménovými řadiči, poskytuje možnost vykonávat NTLM ověřování pro Fortigate. Pokud uživatel provede akci, která si vyžaduje autentizaci, Fortigate inicializuje spojení s klientským prohlížečem a veškeré další NTLM pakety posílá na Collector agenta ke zpracování. To vše za předpokladu, že klientský prohlížeč podporuje NTLM protokol.

NTLM protokol chrání uživatelská hesla tím, že je neposílá po síti. Komunikace se koná tak, že server nejdříve zašle klientovi náhodné číslo, které klient musí zašifrovat pomocí heše hesla uživatele a pošle jej na server. Server vykoná stejný proces zašifrování na původně poslané náhodně vygenerované číslo a výsledek porovná s obdrženým zašifrovaným číslem. Pokud při výsledném porovnání dojde ke shodě, je zřejmé, že obě strany používají stejné heslo. Po úspěšném ověření údajů na doménovém řadiči bude uživateli umožněno dokončit vyžádané spojení skrze Fortigate.

Na obrázku níže jsou zobrazeny postupné kroky NTLM ověřování, které jsou pod ním řádně vysvětleny.




**Obrázek 9: FSSO v režimu NTLM**

*Zdroj: vlastní*

1. Neověřený uživatel se snaží navázat spojení do Internetu pomocí webového prohlížeče.
2. Fortigate komunikaci z neověřeného zdroje odchytí a vyžádá si přihlašovací údaje (doménového účtu).
3. Uživatel poskytne své přihlašovací údaje a zašle je na Fortigate.
4. Fortigate přijaté údaje přepošle na Collector agenta.
5. CA ověří přihlašovací údaje na doménovém řadiči.
6. CA pošle informaci na Fortigate, že došlo k úspěšnému přihlášení.
7. Fortigate umožní uživateli navázat spojení do Internetu a jiných sítí dle patřičné bezpečnostní politiky.

Je-li požadováno, aby administrátor měl stoprocentní kontrolu nad typem komunikace, který může pocházet ze zařízení v síti, na kterém se mohou uživatelé přihlásit do domény i na lokální účet, pak mu SSO technologie umožňuje nastavit proxy v prohlížečích daného zařízení na IP adresu Fortigate. Přihlásí-li se poté uživatel na daném zařízení použitím doménového účtu, nebude se již muset autentizovat v prohlížeči. Pokud se naopak uživatel přihlásí na daném zařízení použitím lokálního účtu, bude muset dojít k ověření přes prohlížeč a tedy NTLM. V případě, že se neautentizuje vůbec, budou jeho pakety na Fortigate vnímány jako neověřená komunikace a bude s nimi naloženo podle odpovídajících bezpečnostních pravidel.

### E) Společné vlastnosti FSSO režimů

Hesla uživatelů nejsou nikdy posílána mezi FSSO komponentami. Posílána jsou pouze jeho

- jméno,
- skupina nebo skupiny, do kterých patří a
- IP adresa.

Patří-li uživatel do několika monitorovaných LDAP skupin, pak se Fortigate snaží najít shodu v bezpečnostních politikách podle každé skupiny zvlášť. Je-li například členem skupiny HK_IT a PCE_IT, tak si nejprve vezme skupinu HK_IT a snaží se pro ni najít patřičnou shodu v politikách firewallu. Pokud shodu nenajde, vezme si PCE_IT a provede to samé znovu. Tento způsob procesování dává správci svobodu v definování různých typů pravidel pro různé skupiny, kterých je uživatel součástí.

Pokud se mezi hosty, servery a Fortigate nachází další síťový firewall je nutné, aby na něm byly propustné následující porty:

- 139
- 389
- 445
- 636
- 8000
- 8002

Touto podkapitolou končí pojednání o Fortinet Single Sign-On (FSSO) a následovat bude technologie, využívající protokol RADIUS, umožňující též jednotné přihlášení v síťovém firewallu Fortigate.

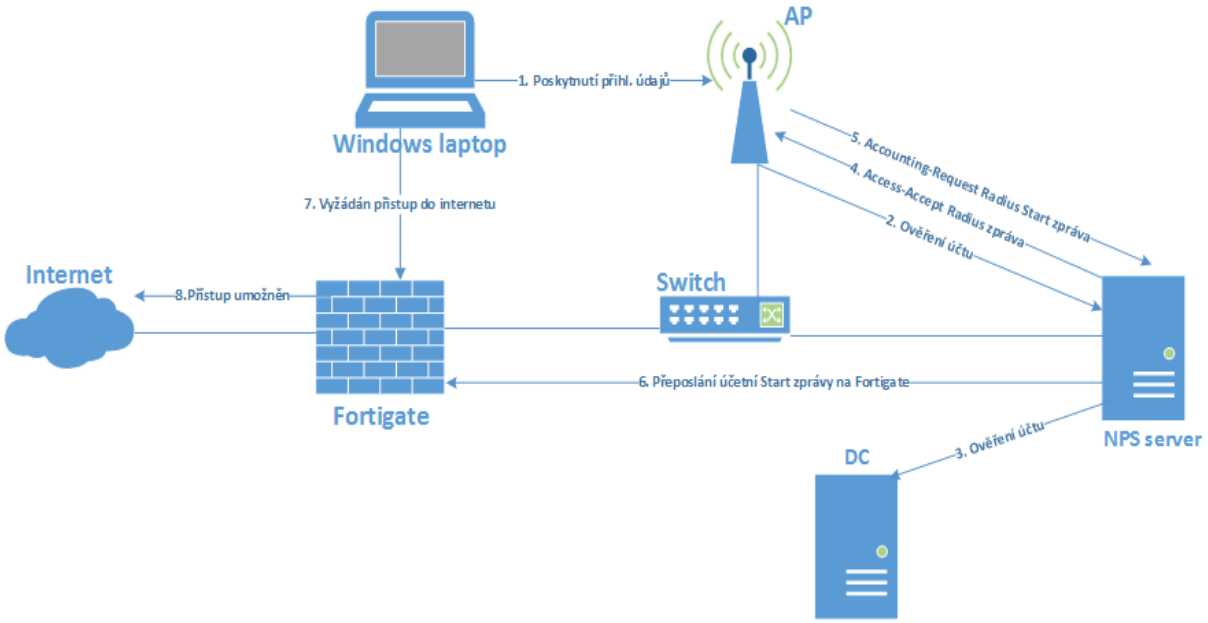
## 3.6 RADIUS Single Sign-On (RSSO)

Jak již samotný název napovídá, jedná se o technologii, která pro své fungování využívá standardizovaný protokol RADIUS. Díky němu se přihlašující se uživatelé do sítě mohou ověřovat pomocí RADIUS serveru, který díky RSSO umožňuje jednotné přihlášení pro autentizované jedince i z pohledu síťového firewallu.

RSSO využívá účetní RADIUS Start a Stop zprávy generované RADIUS klientem v době úspěšného přihlášení a odhlášení uživatele. Jsou zasílané na RADIUS server, který je přepošle na Fortigate. Ten si z přijaté zprávy vezme potřebné informace a vytvoří si pro autentizovaného uživatele u sebe záznam. Když poté dojde k zasílání paketů skrze firewall, není již nutné, aby se jedinec ověřoval znovu a Fortigate na danou komunikaci aplikuje patřičnou bezpečnostní politiku dle skupiny uživatele.

RSSO je možné v praxi využít například pro autentizaci uživatelů přistupující do sítě přes bezdrátové spojení nebo při kabelovém ověřování entit pomocí 802.1x. Další využití má v případě, že daná síť nedisponuje Active Directory, tj. doménovými řadiči. Při takovém scénáři je možné vytvořit databázi uživatelských účtů na RADIUS serveru a při přihlášení se uživatel ověří přímo proti RADIUS serveru. Není tedy vždy nutné mít pro RSSO k dispozici doménové kontroléry, je však nutné, aby uživatelé provedli své ověření pomocí RADIUS klienta.

Na obrázku níže je zobrazen tok zpráv pro RSSO ověřování za použití autentizace do bezdrátové sítě. Jednotlivé kroky jsou pod ním řádně vysvětleny.




**Obrázek 10: RSSO**

*Zdroj: vlastní*

1. Uživatel poskytne své údaje pro přihlášení do WIFI sítě za použití svého doménového účtu.
2. AP pošle dotaz na RADIUS server.
3. RADIUS server ověří přihlašovací údaje uživatele na doménovém řadiči.
4. Pokud byla poskytnuta správná přihlašovací data, pošle RADIUS server Access-Accept zprávu na AP.
5. AP vygeneruje Accounting-Request zprávu typu Start a zašle ji na RADIUS server.
6. Ten danou zprávu přepošle na Fortigate, který přijatou zprávu rozpozná a spáruje ji se svojí lokální RSSO skupinou podle nastaveného řetězce atributu Class.
7. Uživatel jde přes Fortigate do Internetu.
8. Fortigate mu přístup umožní bez nutnosti další autentizace.

Tímto byl popsán princip fungování RSSO a v následující kapitole bude věnována pozornost SSO pro autentizaci uživatelů připojující se do sítě primárně z externích sítí.

## 3.7 LDAP autentizace pro SSL VPN

Většina velkých organizací řeší otázku zabezpečeného přístupu uživatelů do korporátní sítě z nezabezpečeného Internetu. Ruku v ruce s tím jde otázka správy uživatelských účtů. Důvodem je fakt, že vzdálení uživatelé připojující se k SSL VPN se musí nejprve autentizovat, než budou moci využívat vnitřních zdrojů dané sítě. Přičemž organizacím, disponujícím velkým množstvím uživatelů, nezbývá nic jiného, než pro ověřování přihlašovacích údajů jednotlivců implementovat škálovatelný systém autentizace. Některé způsoby jsou z pohledu škálovatelnosti lepší, jiné horší. V každém případě má administrátor na výběr několik možností:

- Uchovávat přímo na firewallu přihlašovací údaje uživatelů.
- Přeposílat požadavky o autentizaci na RADIUS, TACACS+ nebo LDAP server.
- Využít PKI certifikátu.

První zmíněná varianta představuje hodně práce se správou a nezdá se být zcela ideální. Navíc ve většině případů by docházelo k uchovávání redundantních uživatelských účtů, což je z pohledu větší organizace neefektivní. Využívá-li však korporátní síť již adresářovou službu, je možné bez dalšího lidského úsilí navíc využít LDAP serveru, na kterém dost možná již existují uživatelské údaje pro celou doménu. Velkou výhodou tedy je, že existuje jedna centrální správa uživatelů pro celou doménu (nejen pro uživatele nacházející se uvnitř sítě, ale též uživatele připojující se do sítě z nezabezpečeného Internetu) a uživatel tak může pro své ověření použít vždy svůj jediný účet. Je to tedy výhodné pro obě strany. Jak pro koncové uživatele, tak pro správce sítě. Uživateli stačí pamatovat si pouze jedny přihlašovací údaje a správce nemusí vést různé účty pro stejné uživatele.

### 3.7.1 Fungování SSL VPN s LDAP

V momentě, kdy se uživatel připojuje do korporátní sítě se dějí následující věci:

- Firewall vyzve jedince k zadání přihlašovacích údajů.
- Uživatel zadá své údaje, které jsou zaslány zpět na firewall.
- Firewall přepošle obdržené informace, čímž provede dotaz na LDAP server.
- Dojde k rozhodnutí o úspěšné nebo neúspěšné autentizaci a výsledek je zaslán zpět na firewall.
- Dle obdrženého výsledku firewall uživatele buď připustí do sítě nebo přístup odmítne a zašle danou informaci vzdálenému uživateli.

Firewall tedy v tomto případě funguje jako proxy pro autentizaci mezi vzdáleným uživatelem a LDAP serverem.

### 3.7.2 Proč firewall jako proxy

Pro uživatele nacházející se v síti, která má přístup k adresářové službě, není proxy zapotřebí, protože autentizační pakety se k ní dostanou a může tak dojít k ověření. Pokud však uživatel přistupuje z Internetu, síťový firewall nastavuje zeď mezi nezabezpečenou sítí a „bezpečnou“ sítí organizace. Pakety k adresářové službě z Internetu jsou tedy blokovány. Nehledě na fakt, že při užívání IPv4 adresace, bez NAT mapování, se k privátní IP adrese serveru s adresářovou službou ani není možno dostat.

Využitím firewallu jako autentizační proxy a LDAP serveru nacházející se v interní síti je možno autentizovat vzdáleného uživatele přicházejícího z Internetu doménovým účtem, i když sám o sobě nemá před samotným ověřením přímý přístup k adresářové službě.

# 4 Případová studie

V následující části jsou v práci uvedeny postupy, metody, nastavení a topologie, které byly realizovány pro otestování různých situací při užívání technologie jednotného přihlašování z různých úhlů pohledu. Cílem bylo najít nedokonalosti síťového SSO řešení na firewallech Fortigate, jež by se mohly v určitých situacích objevit v reálném provozu. Následně zjištěné nedokonalosti byly popsány a u každého potenciálního problému bylo navrženo řešení, které by z pohledu síťového testera mohlo problém odstranit.

Testování proběhlo celkem ve třech iteracích pro každý hlavní režim SSO zvlášť. Nejprve byla pozornost zaměřena na FSSO a jeho jednotlivé podrežimy, poté proběhlo testování RSSO a nakonec byla nastavena a vyzkoušena technologie pro SSO autentizaci SSL VPN uživatelů přistupující do korporátní sítě z Internetu.

## 4.1 Fortinet Single Sign-On (FSSO)

V první iteraci testování byly prozkoumány jednotlivé varianty nastavení FSSO. Testy byly provedeny postupně na jednotlivé jeho podrežimy, včetně zakomponování testů například pro Linux hosty. Do testů byly mimo jiné zakomponovány také různé scénáře s cílem zjistit, jak FSSO funguje, když se operační systémy Windows nebo Linux nenachází v doméně. Postupně byly prozkoumány varianty, které se zaměřují na DC Agenta, Polling režim, Linux hosty, TS Agenta, NTLM a na závěr krátká zmínka o obecných problémech, které jsou společné pro všechny režimy FSSO.

### 4.1.1 DC Agent

První testovaný režim FSSO se týkal DC Agenta. V tomto režimu byly provedeny 2 testy a objeveny 2 potenciální problémy, které byly níže zdokumentovány.

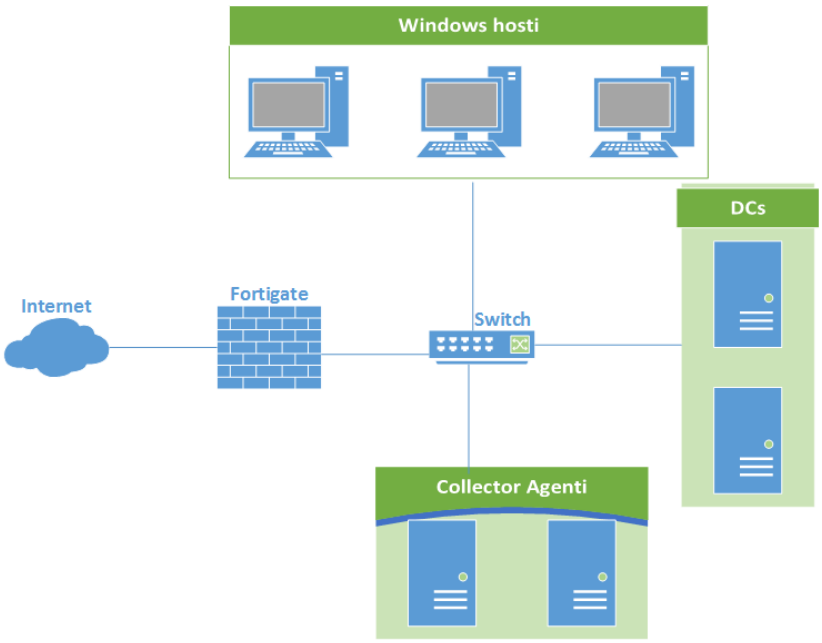
**Test 1:**

V prvním testu byla vytvořena jednoduchá topologie skládající se ze tří Windows hostů a jednoho Windows Serveru 2012 R2, který byl povýšen na doménový kontrolér. Na doménovém kontroléru byl nainstalován také DC agent a Collector agent v Advanced módu. Po nastavení Fortigate 60D byl u Collector agenta vytvořen group filter a při různém

přihlašování a odhlašování různých uživatelů do domény na různých Windows hostech se neprojevil žádný problém a celý systém fungoval spolehlivě.

**Test 2:**

Ve druhém testu se topologie skládala ze tří Windows hostů, dvou doménových kontrolérů s DC agentem a dvou Windows serverů s nastaveným Collector agentem.




**Obrázek 11: Testování - DC Agent**

*Zdroj: vlastní*

Při každém přihlášení uživatele do domény DC agent poslal UDP paket na cílový port 8002 na adresu obou Collector agentů, kde se uživatelské přístupy do sítě zaznamenávaly. Funkčnost systému byla stoprocentní a téměř okamžitá až do doby, kdy byl jeden server s Collector agentem úmyslně odpojen ze sítě.

V Advanced módu si totiž Fortigate zaregistruje skupinový filtr (group filter) pouze u jednoho Collector agenta a ostatní CA daný záznam nemají. Z čehož plyne, že Fortigate v daný čas dostává přihlašovací informace uživatelů jen od jednoho CA. Když tedy přestane využívané CA pracovat, musí dojít k failover scénáři a Fortigate musí začít dostávat přihlašovací informace od jiného CA. Při testování byl však zjištěn problém v čase nutnému k přechodu na další CA. Naměřen byl čas 4 minuty 53 sekund od doby nedostupnosti původně využívaného CA. V mezidobí druhý CA funguje normálně a přihlašovací záznamy standardně uchovává.

Na straně Fortigate však nedochází k přesunu na funkční CA po celou dobu naměřeného času. To je poměrně velký problém, zvlášť při pohledu na dnešní požadavky na dostupnost sítě, kdy přihlášený uživatel velmi pravděpodobně nemá přístup tam, kam by potřeboval.

Možná ještě horší scénář je, že na Fortigate zůstane informace o tom, že na určitém počítači je stále zalogován uživatel, který se však již odhlásil a na daný počítač se přihlásil někdo jiný. Po dobu necelých pěti minut bude s tímto novým uživatelem nakládáno podle politik původně přihlášeno uživatele, což by mohla být potenciální hrozba zneužití sítě nejen pro uživatele, kteří by chtěli firmě vědomě uškodit, ale také pro únik soukromých informací běžných uživatelů. Kdyby potenciální hacker věděl o této hrozbě v zabezpečení, mohl by použít například denial-of-service (DoS) útok proti aktivnímu CA, čímž by jej udělal natolik vytíženým, že by server nebyl dostupný. Dále by se přihlásil na počítač, kde byl před chvílí přihlášen uživatel s administrátorskými právy. Tím by získal přístup prakticky ke všem zdrojům v síti a mohl by v příštích pěti minutách realizovat své další cílené kroky.

Další potenciální problém je získávání informací pouze od jednoho CA v jeden čas. V případě, že by vypadla linka mezi CA a doménovým kontrolérem, který provedl autentizaci uživatele, pak se CA o této informaci vůbec nedozví. V takovém případě nemůže zaslat záznamy ani na Fortigate, a tak může být s legitimním uživatelem nakládáno podle jiných bezpečnostních politik, než mu mají být přiděleny.

**Problém 1:** Doba trvání failoveru při iniciálním připojení nového CA.

**Návrh řešení:** Pro zrychlení doby přechodu z nedostupného CA na další CA v pořadí by se nabízela možnost periodické kontroly dostupnosti aktivně využívaného CA a alespoň jednoho dalšího. Četnost kontroly by dle požadavků na konvergenci dnešních sítí měla být maximálně v rámci několika sekund. V případě, že by aktivní CA nebyl dostupný a jiný CA ano, provedla by se transakce z aktivního nedostupného CA na standby dostupný CA, který by se tímto stal aktivním. Takové řešení by pro Fortigate znamenalo jen velmi malou zátěž navíc, ale pro síťový Single Sign-On systém by to bylo relativně velké zlepšení.

**Problém 2:** Chybějící redundance.

**Návrh řešení:** Umožnit Fortigate získávat přihlašovací informace uživatelů alespoň ze dvou zdrojů najednou. Při obdržení aktualizačních zpráv od vícero CA by se vždy provedlo porovnání obdržených záznamů, redundantní by se vyřadily a následně by proběhlo porovnání s již známými záznamy v databázi Fortigate. Podle časově nejaktuálnějších záznamů by pak

došlo k aktualizaci databáze ve Fortigate. Tímto způsobem by se eliminovalo riziko vypadnutí linky mezi DC a CA, ale také pomalá konvergence při přechodu z jednoho CA na druhý, jak bylo řečeno v problému číslo 1. Stinnou stránkou tohoto řešení zůstává fakt, že takové porovnávání záznamů z různých zdrojů si vyžaduje výpočetní výkon firewallu a při jejich velkém počtu může být taková režie neakceptovatelná.

### 4.1.2 Polling režim

Druhý testovaný režim FSSO byl Polling. V tomto režimu byly provedeny 4 testy a objeveno celkem 5 potenciálních problémů, které byly níže zdokumentovány.

**Test 1:**

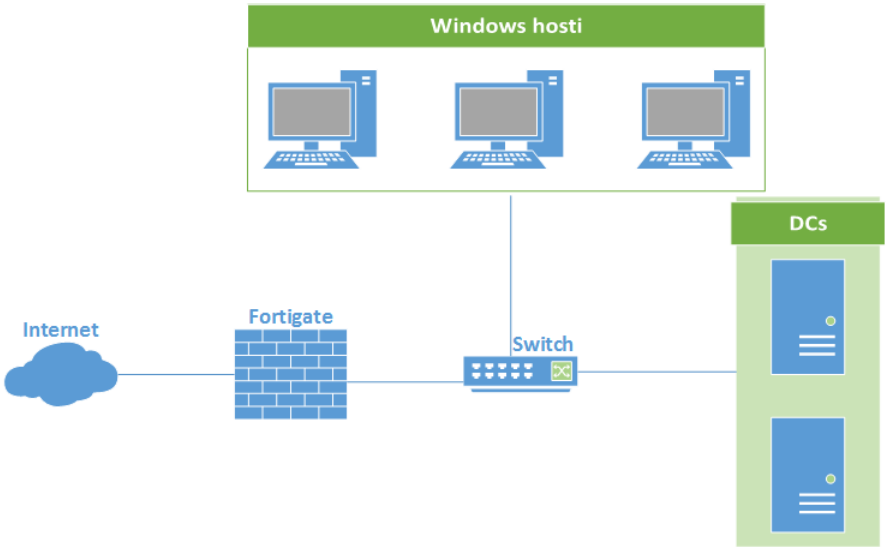
V prvním testu byla zvolena stejná topologie jako v testu číslo 2 předcházející sekce. Jedná se o 3 hosty Windows, 2 doménové kontroléry bez nainstalovaného DC agenta a 2 servery s nainstalovaným Collector agentem, který byl nastaven na dotazování se (polling) na oba doménové kontroléry, aby od nich získal potřebné přihlašovací údaje. Bylo zjištěno, že ve výchozím nastavení CA posílá dotaz na doménové kontroléry každé 3 sekundy a následně je předá firewallu. Fortigate byl nastaven na obdržení informací od CA.

Při testování se projevila maximálně tří sekundová prodleva mezi přihlášeným uživatelem a zaznamenáním informací o daném uživateli v logu událostí na Fortigate. Důvodem je právě periodické tří sekundové dotazování CA na doménové kontroléry.

Patrné problémy se opět vyskytly při náhlé nedostupnosti aktivně využívaného CA. V dotazovacím (Polling) režimu je opět nemožné, aby Fortigate využíval několik CA najednou. Omezení na jedno aktivní CA opět trvá a problémy s tím spojené taktéž. Konkrétně se jedná o stejné dva problémy popsané již v předcházející sekci týkající se téměř pěti minutové prodlevy při přechodu mezi náhle nedostupným aktivním CA a novým, aktivně využívaným, a tedy dostupným CA (viz. Problém 1 v předchozí sekci). Podobně přetrvává také problém s chybějící redundancí (viz. Problém 2 v předchozí sekci).

**Test 2:**

Při druhém testu byla zvolena topologie 3 Windows hostů, 2 doménových kontrolérů bez DC agenta i bez Collector agenta a Fortigate 60D s operačním systémem FortiOS v5.4.1,build5447(GA), který byl nastaven na dotazování se přímo kontrolérů.




**Obrázek 12: Testování - Polling režim**

*Zdroj: vlastní*

Na žádné zařízení nebyl instalován CA a dotazování probíhalo přímo mezi firewallem a doménovými kontroléry. Fortigate se po nastavení dotazoval každých 20 sekund obou DC (komunikace byla zachycena Wiresharkem), oba zaslaly v Response zprávě protokolu Eventlog správně přihlášené uživatele, ale Fortigate s touto verzí operačního systému FortiOS nebyl schopen obdržené informace zaznamenat do svého logu událostí. Po kompletním resetu konfigurace a opětovném nastavení, i po restartu celého firewallu, nebyl schopen zaznamenat žádnou přihlašovací událost.

Z tohoto důvodu byl zprovozněn virtuální firewall běžící nad virtualizační platformou Hyper-V, který se stejnou konfigurací fungoval již správně (viz. Test 3).

**Problém 1:** Příchozí Eventlog zprávy od DC firewall nezapíše do svého logu událostí.

**Návrh řešení:** V jiných verzích FortiOS je naslouchání a čtení obdržených Eventlog zpráv úspěšně vyřešené, proto by bylo nejjednodušší upgradovat na jinou verzi.

**Test 3:**

Vzhledem k bugu, který se objevil v operačním systému FortiOS na fyzickém zařízení v Testu 2, byl proveden další test s topologií stejnou jako v předcházejícím testu, tj. 3 Windows hosty, 2 doménové kontroléry a jeden virtuální Fortigate v5.4.1,build1064(GA) běžící nad Hyper-V. Firewall se každých 10 sekund dotazoval obou doménových kontrolérů, které mu disciplinovaně posílaly logon informace pomocí Eventlog protokolu. Přihlašování uživatelů

fungovalo bezproblémově bez ohledu na to, na jakém DC byli autentizováni. Jediný problém, který při testování správného fungování jednotného ověřování nastal, byl tehdy, když linka mezi DC a Fortigate přestala dočasně fungovat. Po obnovení spojení totiž firewall již nebyl zpětně schopen získat od daného DC uživatelská data těch uživatelů, jenž realizovali své přihlášení do domény v době, kdy byla linka mezi DC a firewallem nefunkční. S takovým uživatelem bude firewall zacházet jako s hostem nebo jako s uživatelem, který se v průběhu nefunkční linky ze stejného počítače odhlásil. V takovém případě v záznamech firewallu zůstal odhlášený uživatel zalogován a záznam s nově přihlášeným uživatelem na stejném zařízení, nebyl firewallu doručen.

Nastane-li podobný scénář v produkční síti, nezbývá nic jiného, než zprovoznit nefunkční linku (případně odstavit ze sítě doménový kontrolér) a následně požádat dotyčného o nové ověření. Poté budou jeho informace opět úspěšně zaslány na Fortigate, kde se zaznamená do logu událostí a dojde k aplikování správných bezpečnostních politik při průchodu paketů daného uživatele skrze firewall.

**Problém 1:** Neschopnost zpětně získat data přihlášených uživatelů, při výpadku linky mezi DC a firewallem.

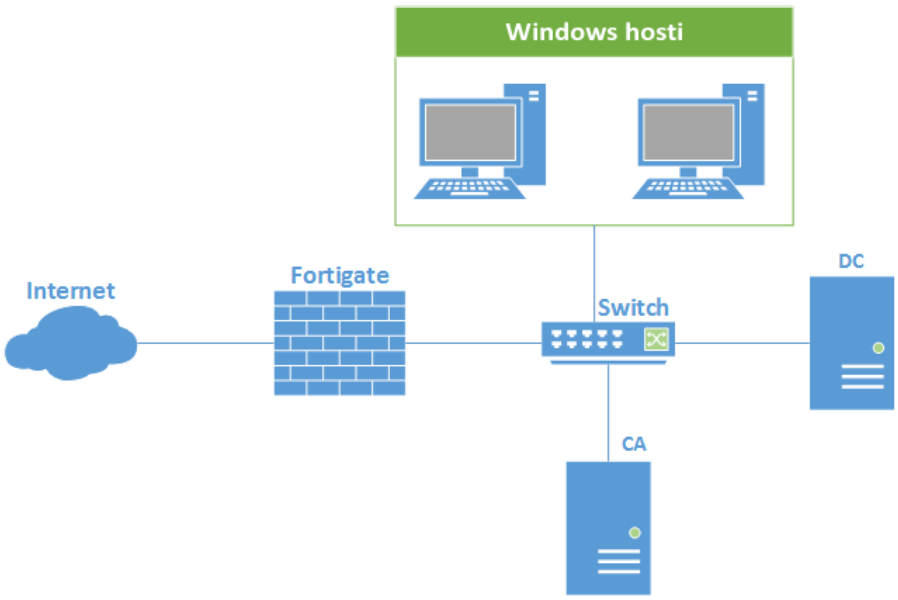
**Návrh řešení:** Jedním z potenciálních řešení by mohl být systém, kdy si Fortigate bude vést status o dostupnosti doménových kontrolérů. Například pomocí úspěšně nebo neúspěšně navázaného TCP spojení při dotazování (polling). Pokud by nebyl úspěšný, zaznamenal by si datum a čas. Jakmile by spojení s doménovým kontrolérem opět fungovalo, zaslal by dotaz s žádostí o větší počet přihlašovacích údajů, a to ideálně od data a času, kdy byla zaznamenána nedostupnost DC. Následně by firewall provedl porovnání svých záznamů a těch obdržených a poté by provedl aktualizaci svého logu událostí. Pokud by se například jednalo jen o výpadek v řádech desítek sekund, nemuseli by se uživatelé znovu přihlašovat a jejich záznamy by byly takto zpětně propsány na Fortigate.

**Problém 2:** Při nedostupnosti doménového řadiče zůstává na Fortigate záznam odhlášeného uživatele i poté, co se na stejné zařízení autentizoval uživatel jiný (platí pouze za předpokladu, že oba provedli ověření pomocí stejného DC).

**Návrh řešení:** Fortigate by si vedl status o dostupnosti doménových kontrolérů. Pokud by se stal nedostupným, poslal by urgentní zprávu správci sítě o nutnosti rychlého zprovoznění linky nebo odstavení DC ze sítě.

**Test 4:**

Hlavním úkolem v testu čtyři bylo ověřit fungování časovačů FSSO Collector agenta a zjištění jejich dopadů na síť. V testu byly použity dva Windows hosty, jeden doménový řadič, jeden Collector agent v dotazovacím režimu a Fortigate, který dostával logon informace od CA. Na hostech byly ve Windows firewallu otevřeny TCP porty 139 a 445, aby byla umožněna komunikace od CA. Workstation verify interval je nastavitelný parametr, jenž umožňuje Collector agentovi, aby se ve výchozím nastavení dotazoval každých 5 minut hostů, zda jsou stále přihlášeni. Při testování se na oba Windows hosty přihlásili dva uživatelé a bylo ověřeno, že dané informace CA zaznamenal. Dále bylo zkontrolováno, že vždy po uplynutí časového intervalu došlo k zápisu bezpečnostních logů na hostech, které byly vytvořeny dotazy Collector agenta. Poté došlo k odhlášení obou uživatelů, ale CA změnu nezaznamenal. Uživatelé měli na CA stále záznam o svém aktivním přihlášení. Tím pádem nebylo možné o změně informovat ani Fortigate. Odhlášení uživatelé tedy na firewallu zůstali také stále přihlášeni, i když již na daném zařízení nepracují.




**Obrázek 13: Testování - Polling režim s časovači**

*Zdroj: vlastní*

Další test časovačů se týkal Dead entry timeout intervalu, který ve výchozím nastavení po osmi hodinách vymaže záznam o přihlášeném uživateli z Collector agenta. Ten opět neinformuje Fortigate o vymazání jedinců ze své databáze. Pokud je tedy uživatel stále přihlášen, může přes firewall dále komunikovat dle svých bezpečnostních politik. Důležitou poznámkou je,

že Fortinet v (FortiOS Handbook, 2016, s. 644) uvádí, že po výchozím intervalu osmi hodin dojde k vymazání pouze již neaktivních uživatelských relací. Při testování bylo však objeveno, že po uplynutí daného intervalu dojde na CA k vymazání jakéhokoliv přihlášení, který má stáří větší než je zmíněný interval. Vzhledem k tomu, že CA o vymazání daných záznamů Fortigate neinformuje, chová se Fortigate ke stále přihlášenému uživateli stejně, to znamená dle politik na základě jeho identity. Jedná se nicméně o trochu matoucí chování, protože běžný správce by očekával, že logon záznamy na CA budou stejné, jako záznamy na Fortigate (protože od něj logon informace získává), nehledě na fakt, že pokud přihlášení uživatele na Fortigate nikdy nevyprší (vyprší jen tehdy, když se na určité zařízení s danou IP adresou přihlásí někdo jiný), jedná se bezpečnostní hrozbu pro vstup do sítě, která je časově téměř neomezená.

Další test časovačů byl zaměřen na tzv. IP address change verify interval, jenž má za úkol periodicky posílat dotazy na zařízení, pro které má CA logon záznamy. Cílem je odhalit změnu IP adresy hosta, aktualizovat své záznamy a informovat Fortigate. Ve výchozím nastavení dochází ke kontrole každých 60 sekund. Při testování došlo ke změně IP adresy přihlášených uživatelů celkem 6x na dvou různých počítačích a po uplynutí intervalu kontroly byly vždy aktualizovány nejen záznamy na CA, ale také na Fortigate. Takové výsledky znamenají pro uživatele, kterému se někdy po přihlášení změní IP adresa (např. po třech hodinách) jen velmi krátkou nedostupnost sítí nacházející se za firewallem. Doba je přímo odvozená z délky kontrolních intervalů. Pokud se správce rozhodne o kontrolu v intervalu 10 sekund, bude mít uživatel jistotu, že při změně IP adresy nebude čekat déle než tento nastavený čas.

**Problém 1:** Workstation verify interval na CA neodhalil odhlášení uživatelů ani po uplynutí několika kontrolních intervalů.

**Návrh řešení:** Pomocí RPC (vzdálené volání procedur) se CA zeptá, kdo je na daném zařízení aktuálně přihlášen. Pokud CA nenajde shodu ve svých záznamech, odstraní jej u sebe a pošle žádost na Fortigate, aby si stejný záznam odstranil také.

**Problém 2:** Po uplynutí Dead entry timeout intervalu se po vymazání přihlašovacích záznamů z CA neprovede předání aktualizací na Fortigate.

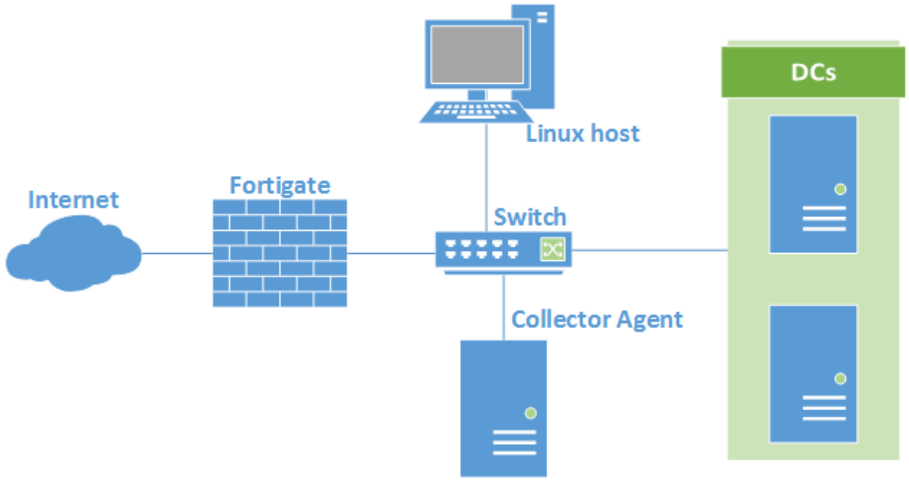
**Návrh řešení:** Umožnit CA zaslat na Fortigate informace o vyřazených přihlášeních, aby si je mohl Fortigate odmazat.

### 4.1.3 Linux – DCAgent a Polling mode

V této sekci testování byla věnována pozornost Linux hostům v prostředí Windows společně se síťovými Single Sign-On systémy od společnosti Fortinet. Zde byly provedeny 3 testy a objeveny 3 potenciální problémy, které byly níže zdokumentovány.

**Test 1:**

V prvním testu byla zvolena topologie jednoho CA serveru, dvou doménových kontrolérů a jednoho Linux hosta s desktopovým operačním systémem Ubuntu verze 16.04 (Xenial), který byl vložen do domény tak, aby se zde mohl přihlásit jakýkoliv uživatel mající účet v Active Directory. Collector agent se dotazoval na doménové kontroléry o logon informace.




**Obrázek 14: Testování - Linux a Collector agent**

*Zdroj: vlastní*

Kromě již popsaných problémů v předchozích sekcích se zde vyskytl následující problém:

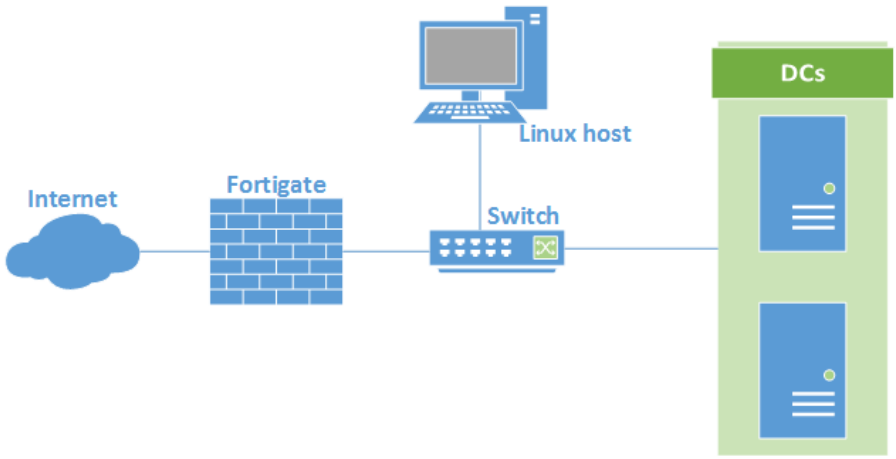
Při stejné konfiguraci fyzického boxu Fortigate 60D s operačním systémem FortiOS v5.4.1,build5447(GA) a virtuálního Fortigate s FortiOS v5.4.1,build1064(GA) se ukázalo, že oba firewally umí logony od CA získat, avšak Fortigate 60D nebyl schopen počítat statistiky posílaných bajtů z IP adresy Linux hosta směřující například do Internetu. V SSO databázi na Fortigate 60D přibývala u přihlášeného uživatele z Ubuntu komunikace pouze v bajtech, ačkoliv na něm probíhalo stahování souboru v řádu desítek MB. U virtuálního firewallu statistiky probíhaly v pořádku.

**Problém 1:** Nefunkční statistiky přenášených packetů od Linux hosta se projevila pouze na Fortigate 60D ve FortiOS v5.4.1,build5447(GA).

**Návrh řešení:** Upgradovat FortiOS na funkční verzi, kde byl již problém vyřešen.

**Test 2:**

Při provádění dalšího testu byla zvolena topologie dvou doménových kontrolérů, jednoho Linux hosta a Fortigate, který byl nastaven na dotazování se doménových kontrolérů přímo na logon informace.




**Obrázek 15: Testování - Linux a přímé dotazy na DC**

*Zdroj: vlastní*

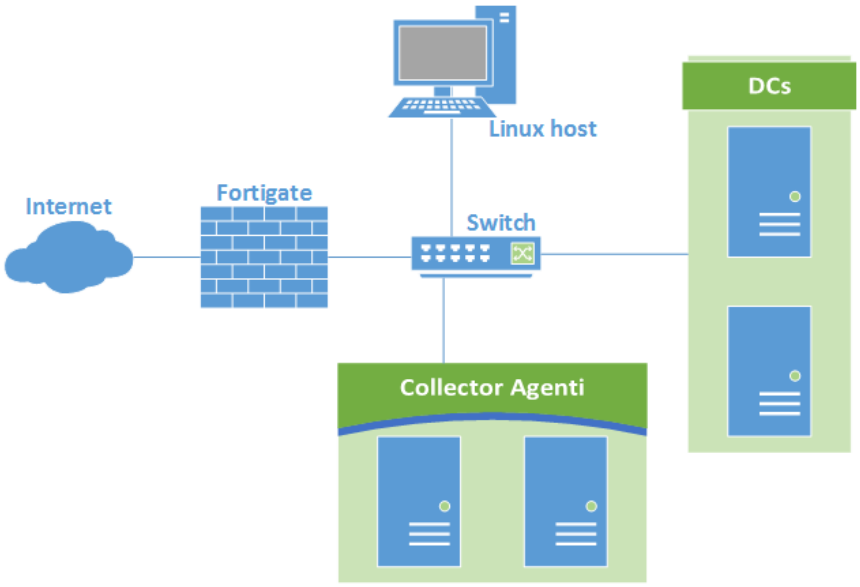
Rozdíl mezi předchozím testem a tímto je fakt, že nebylo zapotřebí nastavovat Collector agenta na žádném z dostupných serverů. Na Fortigate 60D v5.4.1,build5447(GA) se zde opět projevil problém probíraný v testu 2 předchozí sekce, kde bylo dotazování přímo na DC nefunkční. Virtuální firewall fungoval korektně.

**Problém 1:** Pouze Fortigate 60D nebyl schopen zasílat dotazy přímo na DC.

**Návrh řešení:** Upgradovat FortiOS na funkční verzi, kde byl již bug vyřešen.

**Test 3:**

Posledním provedeným testem v této sekci mělo za cíl vyzkoušet, zda DC agent funguje správně i s operačním systémem Linux v doméně. Nastaveny byly dva doménové kontroléry, kde každý z nich disponoval DC agentem. Dále dva Collector agenti a jeden Linux host, na kterém se přihlašovali různí uživatelé do domény.




**Obrázek 16: Testování - Linux a DC Agent**

*Zdroj: vlastní*

Zde DC agent nefungoval prakticky vůbec. Po zapnutí Wiresharku na CA serverech bylo zjištěno, že DC agent údaje přihlášených uživatelů z Linuxu vůbec nepředá Collector agentům (ač ve stejný čas bez problémů předává logony přihlášených jedinců na Windows hostech). CA tedy nemají vůbec možnost záznamy uchovávat a informovat tak o tom Fortigate.

**Problém 1:** DC agent neposílá Collector agentům informace o logon událostech, které vzniknou díky uživatelům operačního systému Linux.

**Návrh řešení:** Na doménovém kontroléru byla zjištěna jiná posloupnost logon událostí při přihlášení uživatele z operačního systému Windows a Linux. To by mohl být potenciální důvod proč DC agent nerozezná a nepošle logon událost Linux hosta na CA. Zdrojový kód DC agenta však pro testování poskytnut nebyl.

### 4.1.4 TS Agent

TS Agent režim poskytuje FSSO autentizaci na terminálových serverech. Týká se spojení přes vzdálenou plochu (tzv. Remote desktop connections), kdy se na jeden terminálový server připojují uživatelé pod svým účtem, kde každý z nich má svoji unikátní relaci. Jelikož uživatelé sdílí společně jednu IP adresu mezi sebou, je nutné jejich relace od sebe odlišit. O to se stará TS agent, který si zarezervuje pool portů pro sebe a při každém připojení uživatele alokuje dle

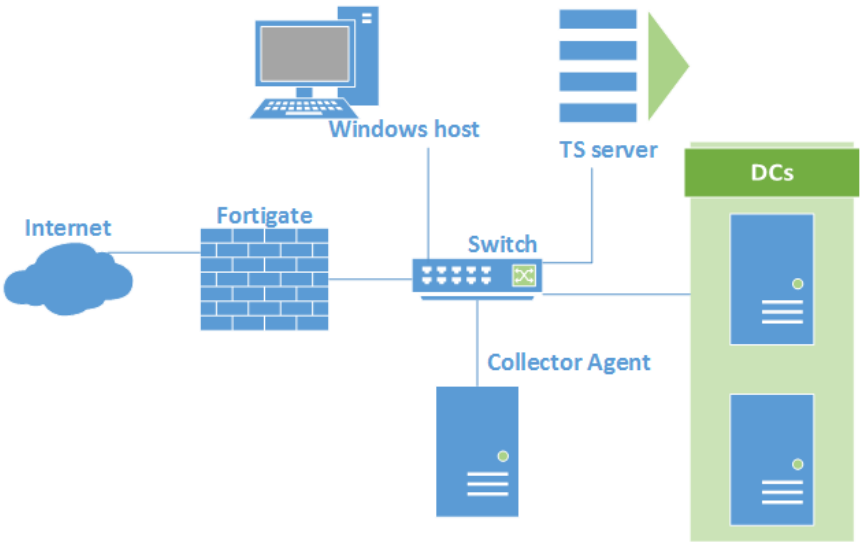
nastavení například 200 portů. Každá relace přihlášeného uživatele pak bude začínat komunikací ze zdrojových portů, který mu byly přiděleny. Tímto způsobem Fortigate rozezná, že se jedná o uživatele XY, protože komunikuje ze svých přidělených portů.

TS agent posílá aktualizace na Collector agenty každých 10 sekund a obsahuje odhlášené a přihlášené uživatele za poslední periodu. V případě, že se uživatelé pouze odpojí, nikoliv odhlásí, pošle TS agent aktualizaci o jeho odpojení. Což umožňuje dealokovat poskytnuté rozmezí portů a vymazání patřičného zápisu na Fortigate. Po jeho opětovném přihlášení mu je přidělené stejné nebo jiné rozmezí portů a provede se opět zápis na Fortigate. Tímto způsobem se řeší otázka limitovaného počtu portů k alokaci a občasná uživatelská neschopnost se řádně odhlásit z relace vzdálené plochy.

V následující části této podkapitoly bude čtenář seznámen s testem provedeným v režimu TS Agent, který odhalil 2 potenciální problémy, které byly níže zdokumentovány.

**Test 1:**

Pro uspokojení požadavků na tento test byl vytvořen jeden terminálový server na platformě Windows s nainstalovaným a řádně nastaveným TS agentem, dva doménové kontroléry, jeden Collector agent a jeden Windows host, který měl za úkol iniciovat desítky různých spojení k terminálovému serveru.




**Obrázek 17: Testování - TS Agent**

*Zdroj: vlastní*

Při testování bylo zaznamenáno bezchybné fungování systému až na pár věcí, které musí správce sítě znát, aby je mohl jednoduše vyřešit. Problém číslo jedna se týká určitých aplikací, které nehledí na regulace TS agenta a využívají jiné porty než ty, které byly pro danou relaci alokovány. Konkrétně se tento problém vyskytl u aplikací Microsoft Edge, FortiClient a služby Windows Update. Týká se jistě i dalších aplikací, které však nebyly za chodu systému otestovány. Tyto aplikace používají jiné zdrojové porty při inicializaci komunikace s okolím, a tím pádem si Fortigate danou komunikace nemůže zařadit pod konkrétní relaci jdoucí z IP adresy terminálového serveru.

Dalším potenciálním problémem je limitující počet portů, které může TS agent přidělit. Defaultně si alokuje porty od 1024 do 49151 a každé relaci je ochoten vybrat a přidělit jedenkrát 200 portů. Je-li potřeba přidělit portů více, je ochoten alokovat ten samý počet portů ještě jednou. Pokud by bylo využito výchozí nastavení, mohlo by se na terminálový server vzdáleně připojit maximálně 240 uživatelů, což pro korporátní sítě větších velikostí, které disponují výkonnými servery, může znamenat potenciální problém.

**Problém 1:** Určité aplikace využívají jiné zdrojové porty, než jim byly přiděleny.

**Návrh řešení 1:** Nejsnazší způsob, jak si s takovými aplikacemi poradit je využít předpřipravené skupiny SSO_Guest_Users s politikou umožňující, ale zároveň omezující komunikaci do Internetu. Takové nastavení problémovým aplikacím umožní, aby si provedly, co potřebují. Zároveň neohrožuje bezpečnost firemní sítě.

**Návrh řešení 2:** Druhé řešení problému číslo 1 - na Fortigate si vytvořit vlastní službu definující, pro jaké cílové porty se mohou objevit zdrojové porty mimo alokované rozmezí portů TS agentem. Následně vytvořit politiku shodující se s IP adresou terminálového serveru, skupiny SSO_Guest_Users a vytvořené vlastní služby. Pokud tedy síť disponuje jedním TS agentem alokujícím porty v rozmezí 19999 a 49000 a problémové aplikace využívají pro komunikaci cílové porty 80 a 443, pak takové nastavení je možno při konfiguraci vlastní služby definovat následujícím příkazem:

*set tcp-portrange 80:1024-19999 80:49000-65535 443:1024-19999 443:49000-65535*

**Problém 2:** TS agent je limitován počtem portů, které může alokovat.

**Návrh řešení:** Pokud je zapotřebí, aby se na terminálový server připojilo více než 240 uživatelů, pak má administrátor možnost změnit počet alokovaných portů jednotlivým přihlášeným relacím a případně i celkové rozmezí portů, které může všem ostatním přidělit.

### 4.1.5 NTLM autentizace

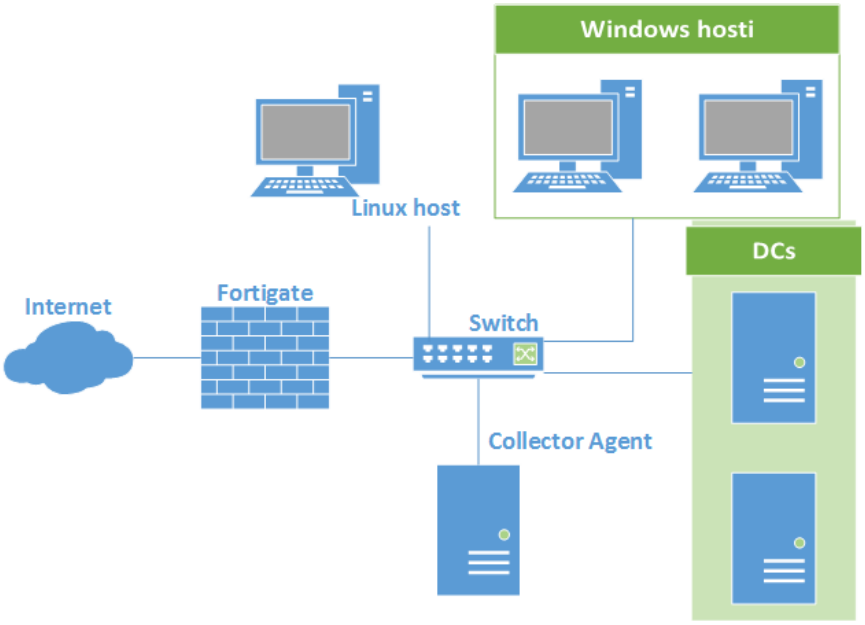
Pro zařízení, která nejsou vložená do domény, například mobilní telefony, tablety, osobní notebooky apod., je možné nastavit omezený přístup ke zdrojům díky defaultní SSO_Guest_Users skupině. Pokud jsou však na firewallu vytvořené pouze bezpečnostní politiky pro přihlášené uživatele, je možné taková zařízení připojit do sítě za použití NTLM autentizace.

Pomocí NTLM ověření je tedy možné zajistit, aby i zařízení, která nejsou vložená do domény (tj. používají jen lokální účty), byla schopna ověřit uživatele přes webové rozhraní. Takový uživatel pak ze svého zařízení může komunikovat stejně jako z počítače fyzicky přidaného v doméně a nemusí se již ověřovat znovu. Na takovém zařízení je nutné v prohlížeči nastavit proxy přes Fortigate, aby se uživatel byl schopen přihlásit a Single Sign-On systém tak informoval o své prezenci na daném zařízení. Děje se tak přes doménový kontrolér po vložení správných údajů uživatele.

V tomto FSSO režimu byly provedeny celkem 2 testy a objeven byl 1 potenciální problém, který je níže zdokumentován.

**Test 1:**

Topologie použitá v tomto testu obsahovala jednoho Linux hosta, dva Windows hosty, dva doménové controlery, jednoho Collector agenta a Fortigate 60D.




**Obrázek 18: Testování – NTLM**

*Zdroj: vlastní*

Po nastavení explicitního webového proxy na Fortigate a následně v prohlížečích Mozilla Firefox na jednotlivých klientech bylo provedeno přihlášení přes webové rozhraní za použití doménového účtu. Po ověření bylo pro Windows hosty možné komunikovat s webovými stránkami na Internetu a dostat se pingem všude, kam to bezpečnostní politiky aplikované pro uživatele povolovaly. Jediný problém byl na straně Linux hosta, který nemohl v síti nijak komunikovat. Po ověření se jeho záznam objevil na Fortigate, ale žádná síťová komunikace od Linux hosta přes Fortigate nefungovala.

**Problém 1:** Linux host nebyl schopen žádné síťové komunikace jdoucí přes Fortigate.

**Návrh řešení:** Vzhledem k faktu, že ověřený uživatel z Linuxu se objeví na Fortigate by bylo pravděpodobně nejlepší debugovat, z jakého důvodu Fortigate neautentizuje pakety jdoucí skrze něho od ověřeného Linux hosta.

**Test 2:**

Při druhém testu byla zvolena stejná topologie jako v testu číslo 1, cílem však bylo zjistit, co se stane tehdy, když se Windows a Linux hosté přihlásí do domény a jejich prohlížeče jsou nastaveny na IP adresu Fortigate jako proxy. Bylo zjištěno, že přihlášením do domény proběhl

SSO cyklus a Fortigate obdržel záznamy přihlášených. Při pokusu o ověření prohlížeče došlo k automatickému ověření uživatele, který byl bez další nutnosti autentizace směrován na cílový server. Pokud tedy správce sítě nastaví na prohlížečích zařízení proxy, má uživatel možnost se autentizovat hned při přihlášení do domény anebo pomocí prohlížeče. V obou případech mu stačí jediné vyplnění jeho údajů.

Při vykonávání tohoto testu nebyl zaznamenán žádný problém týkající se přístupu do sítě na žádném z použitých operačních systémů.

### 4.1.6 Obecné FSSO problémy

V této části bude poukázáno na obecné problémy týkající se FSSO a vztahuje se ke všem režimům a variantám jeho implementací.

**Problém 1:**

Prakticky při jakémkoliv FSSO nastavení a topologii bude potenciální problém s lokálně přihlášenými uživateli na počítačích v doméně. Testovaným příkladem je situace, kdy se na určitém zařízení přihlásí uživatel A do domény, následně se odhlásí a poté se přihlásí uživatel B pod lokálním účtem. Fortigate nemá způsob, jak by se dozvěděl, že se na daném počítači někdo odhlásil. Navíc už vůbec nemá způsob, jak by se dozvěděl, že se na daném počítači v doméně někdo přihlásil na lokální účet zařízení. V takové situaci záznam o přihlášení uživatele A na PC zůstane v databázi firewallu. Informaci o jeho odhlášení není schopen firewall dostat. A při přihlášení uživatele B na lokální účet počítače si bude Fortigate stále myslet, že na daném zařízení pracuje uživatel A a bude na jeho pakety aplikovat bezpečnostní politiky platící pro uživatele A, i přesto, že uživatel B nemá v Active Directory ani svůj účet.

Dále se nabízí otázka, kdy vyprší záznam ve Fortigate, když se přihlásil uživatel. Dle (FortiOS Handbook, 2016, s. 644) vyprší po osmi hodinách nečinnosti nebo s přihlášením jiného uživatele na dané zařízení (konkrétně na zařízení se stejnou IP adresou).

**Návrh řešení:** Nastavit politiku přihlašování pro veškeré zařízení v doméně tak, aby se žádný uživatel nemohl přihlásit pod lokálním účtem PC. Tím se eliminuje výše uvedený problém a komunikace v síti se stane transparentnější.

**Problém 2:** Při užívání Collector agenta bylo velice nepohodlné nemít možnost zvětšit okno programu CA. Obzvláště pak při větším počtu přihlášených uživatelů a jejich kontrole

v podokně s názvem „Show logon users“, musí správce rolovat zleva doprava a nahoru dolů. Tato jednoduchá vlastnost programu by podstatně dodala na pohodlnosti a přehlednosti jeho užívání.

**Návrh řešení:** Naimplementovat nejen možnost celoobrazovkového režimu programu, ale také možnost okna roztáhnout a zmenšit dle vlastních požadavků osoby, která s Collector agentem pracuje.

**Problém 3:**

Uvažována je situace, že na zařízeních není nainstalován TS agent. Správce sítě se přihlásí do domény na svém pracovním počítači. Poté se chce pod jiným účtem pomocí vzdálené plochy přihlásit do jiného zařízení. V takovém případě proběhla autentizace na obou počítačích a Fortigate si bude myslet, že oba počítače jsou užívány posledně použitým účtem. Problémem to začíná být například v situaci, kdy se správce potřebuje dostat do sítě, kam on sám může, ale použitý účet pro vzdálenou plochu nikoliv. Dojde k odpojení a nebude prakticky možné se do cílového bodu dostat.

**Návrh řešení:** Vždy si zkontrolovat, zda použitý účet pro vzdálenou plochu má patřičné oprávnění se do cíle dostat.

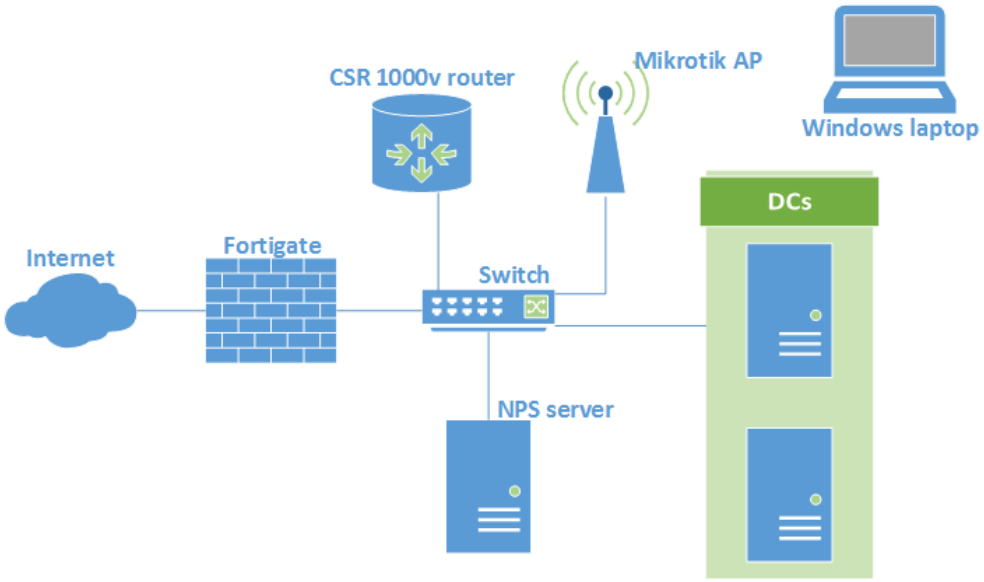
## 4.2 RADIUS Single Sign-On (RSSO)

RSSO umožňuje síťové jednotné přihlášení tím, že využívá účetních zpráv protokolu RADIUS, které mohou být generovány RADIUS klientem a přeposlány na Fortigate. V této části testování byla věnována pozornost zejména ověření bezdrátových zařízení do sítě a předání logon informací na Fortigate z toho důvodu, aby bylo možné na komunikaci přihlášeného uživatele automaticky aplikovat bezpečnostní politiky firewallu, aniž by se uživatel musel autentizovat znovu k firewallu.

V následujícím části této podkapitoly je popsán uskutečněný test technologie RSSO, při kterém byl objeven potenciální problém, který je níže zdokumentován.

**Test 1:**

Nastavená topologie se skládala z jednoho Windows Network Policy Serveru (NPS), dvou doménových kontrolérů, jednoho přístupového bodu Mikrotik (AP), Cisco CSR 1000v virtuálního routeru a Windows hosta.




**Obrázek 19: Testování – RSSO**

*Zdroj: vlastní*

Zabezpečení Mikrotik AP bylo nastaveno na WPA2 Enterprise a autentizaci uživatelů na NPS serveru. Ten byl nastaven na ověření účtů v doméně. Po úspěšném přihlášení uživatele k bezdrátové síti byly Mikrotikem vygenerovány RADIUS účetní zprávy a zaslány na NPS server, který je přeposlal na Fortigate. Problém však nastal na Fortigate, který účetní zprávu typu Start dostal, nebyl však schopen ji zpracovat a zaznamenat do RSSO databáze (logu událostí). Stejný scénář pokračoval i při nastavení AAA autentizace na Cisco CSR 1000v, který ověřil uživatele přes NPS server a po úspěšném přihlášení do uživatelského (exec) módu vygeneroval RADIUS účetní zprávu, která byla opět NPS serverem přeposlána na Fortigate, který nebyl schopen jej přečíst. Uživatel se tedy úspěšně autentizoval do bezdrátové sítě i do Cisco routeru, ale na Fortigate ověřen nebyl. SSO v provedeném RSSO testu tedy nefungovalo. Důsledkem je, že takový uživatel zůstává v očích firewallu neautentizován a nebude s ním nakládáno podle jeho bezpečnostních politik.

Pro jistotu, zda se nejedná pouze o bug ve verzi FortiOS, byl stejný test vykonán ještě jednou, za použití virtuálního Fortigate disponující jinou verzí FortiOS, který měl však v obou případech stejně neúspěšný výsledek při čtení účetní RADIUS zprávy.

Na obrázku 20 je zobrazena RADIUS účetní zpráva, jenž byla zachycena na Fortigate po úspěšné autentizaci uživatele.

```
2.851355 port1 -- 192.168.1.13.56371 -> 192.168.1.93.1813: udp 298
0x0000   0015 5d00 7909 0015 5d00 7905 0800 4500      ..].y...].y...E.
0x0010   0146 79aa 0000 8011 3c42 c0a8 010d c0a8      .Fy.....<B......
0x0020   015d dc33 0715 0132 da6c 0424 012a ecc2      .].3...2.l.$.*..
0x0030   2044 1e27 fe4a 384b dd7d 1490 dc8c 0606      .D.'.J8K.}......
0x0040   0000 0002 5707 776c 616e 313d 0600 0000      ....W.wlan1=....
0x0050   1301 126a 6972 6963 6f72 705c 6a61 6e6e      ...jiricorp\jann
0x0060   6f76 7919 0e75 6e72 6573 7472 6963 7465      ovy..unrestricte
0x0070   6419 2eb8 f009 6d00 0001 3700 0102 00c0      d.....m...7.....
0x0080   a801 0d00 0000 0070 ee58 b1af 24f1 8701      .......p.X..$...
0x0090   d20d 8769 0b57 9200 0000 0000 0000 452c      ...i.W........E,
0x00a0   0a38 3230 3030 3031 3432 3d45 342d 3844      .820000142=E4-8D
0x00b0   2d38 432d 4344 2d44 302d 4243 2d32 302d      -8C-CD-D0-BC-20-
0x00c0   3638 2d39 442d 4641 2d35 352d 3539 2d38      68-9D-FA-55-59-8
0x00d0   322d 3030 2d30 302d 3030 2d30 302d 3030      2-00-00-00-00-00
0x00e0   2d30 302d 3035 1f13 3230 2d36 382d 3944      -00-05..20-68-9D
0x00f0   2d46 412d 3535 2d35 391e 2345 342d 3844      -FA-55-59.#E4-8D
0x0100   2d38 432d 4344 2d44 302d 4243 3a4d 696b      -8C-CD-D0-BC:Mik
0x0110   726f 5469 6b2d 4344 4430 4243 2d06 0000      roTik-CDD0BC-....
0x0120   0001 2806 0000 0001 200a 4d69 6b72 6f54      ..(.......MikroT
0x0130   696b 2906 0000 0000 0406 c0a8 0102 2116      ik)...........!.
0x0140   fe80 0000 0000 0000 70ee 58b1 af24 f187      ........p.X..$..
0x0150   0000 0048                                    ...H
```

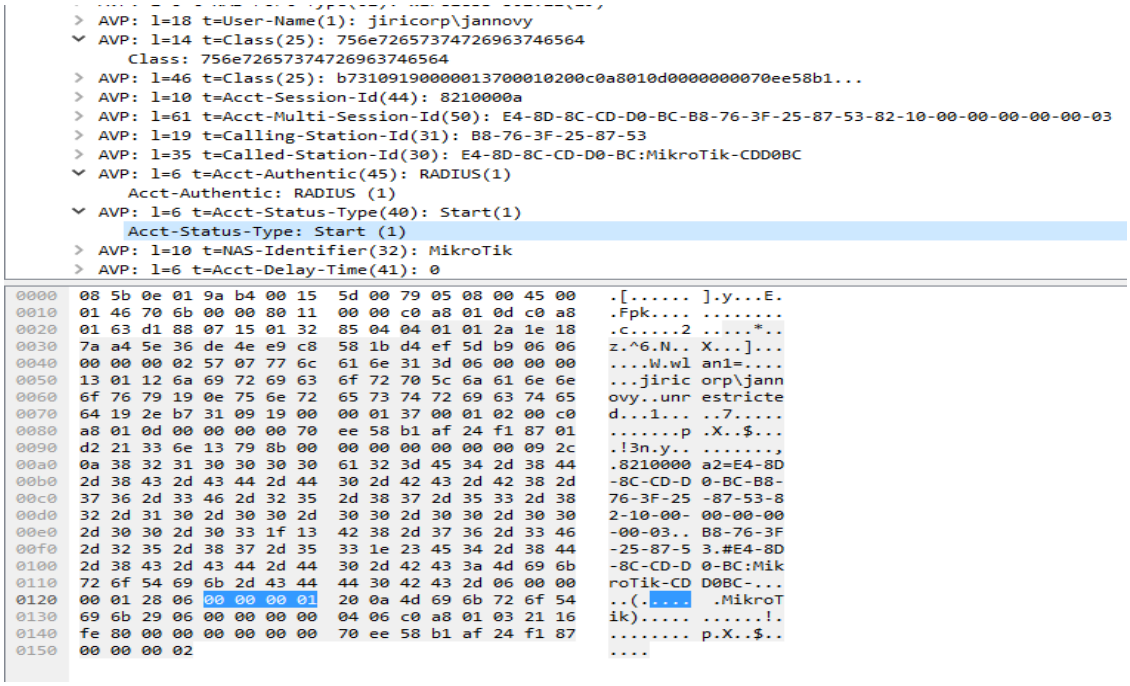
**Obrázek 20: RADIUS účetní zpráva na Fortigate**

*Zdroj: vlastní*

Na obrázku 21 je dále zobrazena RADIUS účetní Start zpráva, která byla zachycena programem Wireshark na NPS serveru po úspěšné autentizaci uživatele do bezdrátové sítě. Jedná se o stejnou zprávu, která byla v předchozím obrázku zachycena také na Fortigate.

Ze zachycených informací je zřejmé, že NPS server nezaslal rámcovou IP adresu (Framed IP address), a proto Fortigate nebyl schopen uživatele správně asociovat a přidat tak do svého RSSO logu událostí ověřeného uživatele.

Na doporučení vedoucího práce byl tento test opakován celkem 3x. NPS server byl nastaven dle manuálu (FortiGate - RSSO with Windows Server 2012 R2 and NPS, 2016, s. 15), avšak rámcovou IP adresu nebylo možné na Fortigate obdržet ani v jednom případě.




**Obrázek 21: RADIUS účetní zpráva na NPS**

*Zdroj: vlastní*

**Problém 1:** NPS server nepředá nutné účetní RADIUS informace na Fortigate a tím pádem je řešení nefunkční.

**Návrh řešení:** Ověřit společností Fortinet správné nastavení NPS serveru ve výše zmíněném manuálu.

## 4.3 LDAP autentizace pro SSL VPN

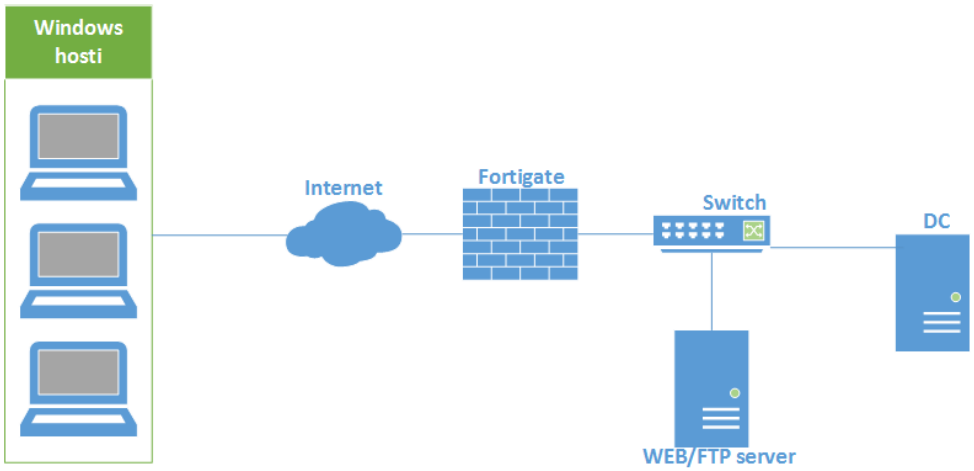
Cílem SSL VPN je zajistit zabezpečený přístup určitým uživatelům nacházejícím se v Internetu do korporátní sítě. Tito uživatelé potřebují mít přístup ke korporátním datům, hardware a software i ze sítí, které nejsou pod správou dané korporace. Pokud se tedy uživatel snaží využít SSL VPN, pak je veškerá jeho komunikace směrována přes Fortigate. Zde je možné aplikovat takové bezpečnostní politiky, které jsou svázány s konkrétním uživatelem a mít tak kontrolu nad zdroji, ke kterým bude mít přístup.

Dále je nutné, aby každý uživatel v doméně měl pouze jeden účet a autentizace a identifikace uživatele probíhala vždy za použití daného účtu. Problém se objevuje, když uživatel není uvnitř

korporátní sítě, protože není schopen kontaktovat doménový kontrolér. Z Internetu je většinou dostupný Fortigate, který naslouchá na VPN spojení. Po předání přihlašovacích údajů je pošle na LDAP server, který uživatele odmítne nebo přijme. Zprávu s rozhodnutím pošle na Fortigate, který opět buď zamítne anebo spojení povolí. Pomocí autentizace přes LDAP server je tedy možné používat doménové účty i pro šifrované VPN spojení. V následujícím testu byla spolehlivost takového systému zkoušena. V tomto scénáři nebyl objeven žádný potenciální problém.

**Test 1:**

Testovaná síť se skládala ze tří Windows hostů, jednoho Fortigate, doménového kontroléru a Web/FTP serveru.




**Obrázek 22: Testování - SSL VPN a LDAP**

*Zdroj: vlastní*

Po patřičném nastavení bylo provedeno celkem 20 autentizací na různé doménové účty a následná webová komunikace do korporátního serveru a do Internetu. Při testování nebyly zjištěny žádné patrné problémy. Ověřování i komunikace probíhala bez komplikací.

## 4.4 Vyhodnocení testů

Testování proběhlo systematicky v předem určených iteracích, dle použité technologie SSO. Pro každý test v každé iteraci testování byla vybudována potřebná síť, proběhlo nastavení technologií a vykonání patřičných kroků pro zjištění funkčnosti a problémových částí systému jednotného přihlašování.

Testovací případy poukázaly na různé problémy týkající se různých technologií SSO. Některé potíže slouží spíše k uvědomění si určitých omezení a vykonání patřičných kroků k optimalizovanému nastavení. Příkladem je TS agent a jeho:

- Omezené množství portů pro alokaci.
- Problémové aplikace využívající jiné než přidělené zdrojové porty.

Některé testy odhalily pouze malé potíže a některé naopak poukázaly na problémy závažné. Mezi ty nejpodstatnější patří:

- Doba trvání failoveru při úvodním přechodu mezi Collector agenty – naměřeny byly 4 minuty 53 sekund
- Chybějící redundance naslouchání vícero CA najednou
- Občasné bugy v různých verzích FortiOS
- Lokální účet a jeho možnost využít bezpečnostní politiky odhlášeného doménového účtu
- Problémy při výpadku linky mezi DC a Fortigate při přímém dotazování se na doménový kontrolér
- Problémy s Linux hosty
- Nefunkční čtení účetních RADIUS zpráv u RSSO.

Na všechny problémy byl vypracován návrh řešení. Nicméně v této části budou stručně uvedeny jen ty řešení týkající se uvedených závažnějších problémů a to ve stejném pořadí:

- Sledovat stav dostupnosti Collector agentů
- Naslouchání vícero CA a porovnání obdržených aktualizačních zpráv od Collector agentů. Následné provedení srovnání získaných unikátních údajů s těmi již existujícími na firewallu
- Upgrade na funkční verzi FortiOS
- Zajistit přihlašování jen na doménové účty
- Doimplementovat funkční systém pro Linux

- Ověřit správné a kompatibilní nastavení NPS serveru a Fortigate

Všechny problémy byly blíže popsány a vysvětleny v předcházejících podkapitolách včetně detailního popisu navrhovaného řešení. U některých problémů bylo popsáno vícero navrhovaných řešení.

# 5 Závěr

Oblast zabezpečení síťového provozu je v dnešní době aktuálním tématem. Hlavním důvodem jsou neustále se objevující pokusy o krádež hodnotných dat, financí či poškození firmy. Nejedná se však pouze o útoky z Internetu, ale vyskytují se též pokusy o napadení z řad vlastních zaměstnanců. Dále na důležitosti problematiky přidává i tlak legislativní, jenž organizacím přikazuje zajistit ochranu osobních údajů jednotlivců. Vyhovět takovým komplexním požadavkům si vyžaduje propracovaný systém zabezpečení, v jejímž čele stojí autentizace a dobře postavené bezpečnostní politiky. Právě ty se staly předmětem zkoumání v této diplomové práci, v níž bylo hlavním cílem porozumět, zdokumentovat a otestovat síťový systém jednotného přihlašování, kde primární zaměření je na Single Sign-On řešení od společnosti Fortinet.

Práce byla rozdělena na dvě hlavní části, teoretickou a praktickou. Teoretická část se zabývala základními pojmy, autentizačními protokoly a různými druhy implementací síťového Single Sign-On řešení v síťových firewallech se zaměřením na Fortigate. V praktické části bylo vykonáno celkem 14 hlavních testů (s několika dílčími testy), které měly za úkol odzkoušet spolehlivost, funkčnost a škálovatelnost celého systému a odhalit jeho případné nedostatky.

Vyskytlo se celkem 15 problémů, z nichž některé jsou relativně závažné, jiné by bylo ideální vyřešit v dohledné době a některé problémy se dají považovat spíše za informativní. Ty posledně jmenované je nutné si pouze uvědomit a přizpůsobit jim konfiguraci dle vlastních požadavků na užívání sítě.

Nejzávažnější odhalené problémy se týkají neschopnosti Fortigate naslouchat více než jen jednomu Collector agentovi (CA) v daném čase. S tím jde ruku v ruce nezbytný rychlý přechod na užívání jiného Collector agenta v případě, že ten původní aktivní selhal. V opakovaných testech se však ukázalo, že doba trvání přechodu je necelých pět minut, což je na dnešní poměry velmi dlouhá doba. Dále byly objeveny nefunkční vlastnosti SSO ve FortiOS v5.4.1.build5447(GA). Také relativně velkým potenciálním problémem se zdá být možnost zneužití bezpečnostních politik při přihlášení uživatele do zařízení v doméně za použití lokálního účtu. Nepříjemná je občasná nefunkčnost Linuxových systémů a problémy související s výpadkem linky mezi doménovým kontrolérem a Fortigate. V neposlední řadě též poskytnuté nekompatibilní nastavení NPS serveru s Fortigate pro úspěšné čtení účetních RADIUS zpráv pro potřeby jednotného přihlášení.

Pro každou odhalenou nedokonalost bylo vypracováno navrhované řešení a detailně popsáno ve čtvrté kapitole s názvem Případová studie. V této kapitole byly blíže popsány také všechny zjištěné problémy, avšak vzhledem k jejich složitosti a nutnému porozumění situacím, které mohou nastat, je čtenáři doporučeno nahlédnout do zmíněné čtvrté kapitoly.

Pro vyhodnocení této diplomové práce, a celého Single Sign-On systému od společnosti Fortinet, je nutné zmínit, že většina testů byla prováděna na krajních hranicích užívání systému. Proto se dá považovat většina zjištěných problémů a navrhovaných řešení za nadstandardní služby, které by síťové SSO mohly pomoci jen doladit. Při běžném chodu systému jednotného přihlašování je SSO spolehlivé a plnohodnotně funkční. Jedná se o propracované řešení, které umožňuje uživateli se v doméně autentizovat pouze jednou. Zároveň s tímto ověřením dojde automaticky k autentizaci také ve firewallu Fortigate. Jakmile začnou kolovat pakety od uživatele skrze firewall, nebude potřeba se u něho již znovu autentizovat, ale Fortigate již sám určí, jaké skupinové bezpečnostní politiky má na danou identitu aplikovat.

Po vykonání všech testů výše zmíněné technologie, byly scénáře a výsledky testů předány společnosti Fortinet, která je nyní oprávněna implementovat případné opravy či vylepšení svého síťového SSO řešení do firewallů Fortigate a potenciálně vylepšit již velmi propracovaný systém jednotného přihlašování uživatelů.

# 6 Použitá literatura


BOUŠKA, Petr. *Samuraj-cz.com: Kerberos protokol a Single sign-on* [online]. 2010 [cit. 2016-12-30]. Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/

BOUŠKA, Petr. *Živě.cz: Kerberos, část 2 – popis metody SSO a protokolu Kerberos Více na: http://www.zive.cz/clanky/kerberos-cast-2--popis-metody-sso-a-protokolu-kerberos/sc-3-a-174389/default.aspx* [online]. 2014 [cit. 2016-12-30]. Dostupné z: http://www.zive.cz/clanky/kerberos-cast-2--popis-metody-sso-a-protokolu-kerberos/sc-3-a-174389/default.aspx

CARTER, Gerald. *LDAP system administration*. Beijing: O'Reilly, 2003. ISBN 15-659-2491-6.

DONAHUE, Joe. *National Institute of Standards and Technology: Single Sign-on and Identity Management* [online]. 2002 [cit. 2017-01-01]. Dostupné z: http://csrc.nist.gov/archive/pki-twg/y2003/presentations/twg-03-08.pdf

FortiGate - RSSO with Windows Server 2012 R2 and NPS [online]. Fortinet Technologies, 2016 [cit. 2017-03-11]. Dostupné z: http://docs.fortinet.com/uploaded/files/2716/fortios-rsso-with-win-server-2012-and-nps.pdf

Fortinet Customer Service & Support. *FSSO - polling mode limit* [online]. 2015 [cit. 2016-12-29]. Dostupné z: https://forum.fortinet.com/tm.aspx?m=122200

Fortinet. *FortiManager VM (Microsoft Hyper-V) Install Guide* [online]. 2014 [cit. 2017-01-01]. Dostupné z: http://docs.fortinet.com/uploaded/files/1129/fortimanager-vm-hyper-v-install.pdf

Fortinet Knowledge Base. *Technical Note: FSSO NetAPI polling bandwidth usage calculator* [online]. 2014 [cit. 2016-12-29]. Dostupné z: http://kb.fortinet.com/kb/documentLink.do?externalID=FD34906

Fortinet. *The FortiGate Cookbook 5.4* [online]. 2016 [cit. 2017-01-01]. Dostupné z: http://docs.fortinet.com/uploaded/files/2915/fortigate-cookbook-54.pdf

FortiOS™ Handbook: *VERSION 5.4.1* [online]. Fortinet, 2016 [cit. 2017-02-26]. Dostupné z: http://docs.fortinet.com/uploaded/files/2827/fortios-handbook-54.pdf

GARMAN, Jason. *Kerberos: the definitive guide*. Beijing: O'Reilly, c2003. ISBN 05-960-0403-6.

GLASS, Eric. *The NTLM Authentication Protocol and Security Support Provider* [online]. 2006 [cit. 2016-12-30]. Dostupné z: http://davenport.sourceforge.net/ntlm.html

HASSELL, Jonathan. *RADIUS*. Sebastopol: O'Reilly, 2003. ISBN 05-960-0322-6.

HOTSPOTSYSTEM. *How to Setup Your Own Hotspot with MIKROTIK routers* [online]. 2011 [cit. 2016-12-30]. Dostupné z: http://www.hotspotsystem.com/installation-guide-mikrotik-manual

HOWES, Tim., Mark SMITH a Gordon S. GOOD. *Understanding and deploying LDAP directory services*. 2nd ed. Boston: Addison-Wesley, c2003. ISBN 06-723-2316-8.

Microsoft Developer Network. *Network Policy Server* [online]. 2008 [cit. 2016-12-29]. Dostupné z: https://msdn.microsoft.com/en-us/library/bb892034(v=vs.85).aspx

Microsoft Developer Network. *Receiving a WMI Event* [online]. 2016 [cit. 2016-12-29]. Dostupné z: https://msdn.microsoft.com/en-us/library/aa393013(v=vs.85).aspx

OFER, Oren. *OWASP Israel: NTLM Based Authentication in Web Applications* [online]. 2014 [cit. 2017-01-01]. Dostupné z: https://www.owasp.org/images/3/37/OWASP-IL-2014-01_nhastie-presentation.pdf

Oracle Corporation. *Enterprise Single Sign-On and HIPAA* [online]. 2010 [cit. 2016-12-30]. Dostupné z: http://www.oracle.com/us/solutions/wp-esso-hipaa-207204.pdf

PETROVÁ, Aneta, Tomáš ČAPEK a Ella Deon BALLARD. *Red Hat: Red Hat Enterprise Linux 6 Managing Single Sign-On and Smart Cards* [online]. 2016 [cit. 2017-01-01]. Dostupné z: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Managing_Smart_Cards/Red_Hat_Enterprise_Linux-6-Managing_Smart_Cards-en-US.pdf

PHIFER, Lisa. *Using RADIUS For WLAN Authentication* [online]. 2003 [cit. 2016-12-29]. Dostupné z: http://www.wi-fiplanet.com/tutorials/article.php/3114511/

PŘIBYL, Tomáš. *ICTsecurity: Single-Sign-On a jeho použití v praxi* [online]. 2009 [cit. 2016-12-30]. Dostupné z: http://www.ictsecurity.cz/component/content/article?id=2713

RAMASWAMY, Chiranth. *Microsoft Developer blog: Overview and working of NTLM* [online]. 2013 [cit. 2017-01-01]. Dostupné z: https://blogs.msdn.microsoft.com/chiranth/2013/09/20/ntlm-want-to-know-how-it-works/

RICCIARDI, Fulvio. *The Kerberos protocol and its implementations* [online]. 2006 [cit. 2016-12-29]. Dostupné z: http://www.zeroshell.org/kerberos/

ROBINSON, Kayla. *Fortinet Cookbook: FSSO in Polling mode* [online]. 2014 [cit. 2017-01-01]. Dostupné z: http://cookbook.fortinet.com/fsso-polling-mode/

TUNG, Brian. *Kerberos: a network authentication system*. Reading: Addison-Wesley, c1999. Addison-Wesley networking basic series. ISBN 02-013-7924-4.

STALLINGS, William. *Network security essentials: applications and standards*. 3rd ed. Upper Saddle River, NJ: Pearson Education, c2007. Addison-Wesley networking basic series. ISBN 01-323-8033-1.

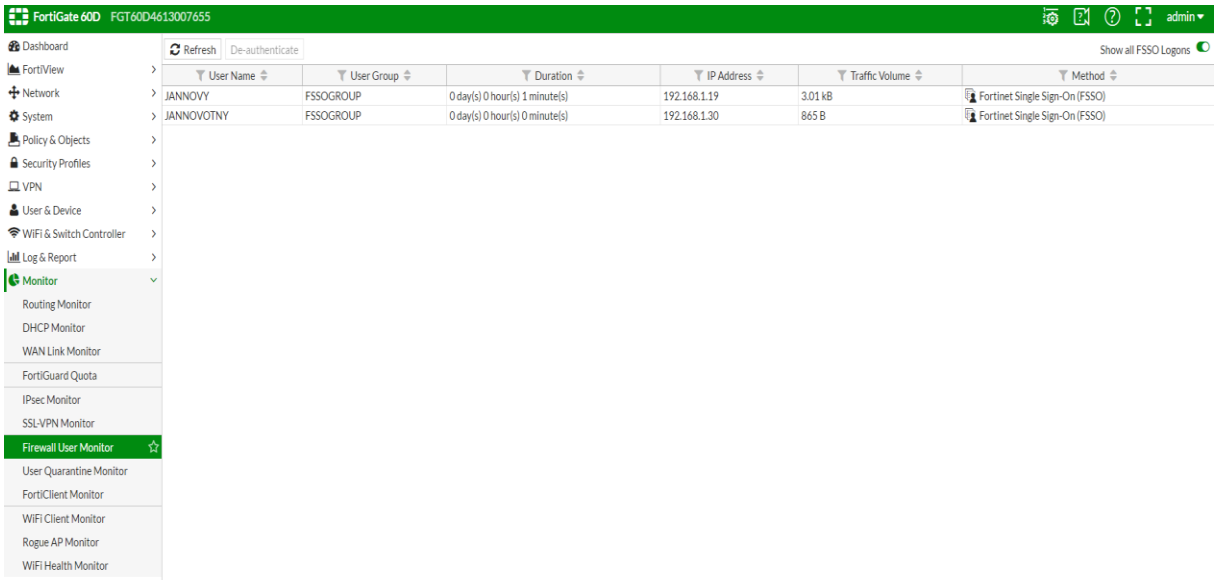
TUTTLE, Steven, Ami EHLENBERGER, Ramakrishna GORTHI, a další. *Understanding LDAP design and implementation*. 2nd ed. White Plains, NY: IBM, International Technical Support Organization, c2004. IBM redbooks. ISBN 073849786X.

Úřad pro ochranu osobních údajů. *Zdravotnictví – vedení zdravotnické dokumentace a zpracování osobních údajů* [online]. 2013 [cit. 2016-12-30]. Dostupné z: https://www.uoou.cz/zdravotnictvi-vedeni-zdravotnicke-dokumentace-a-zpracovani-osobnich-udaju/d-1

Zákon o péči o zdraví lidu [online]. In: . Poslanecká sněmovna Parlamentu České republiky, 1965 [cit. 2017-03-12]. Dostupné z: http://www.psp.cz/eknih/1964ns/tisky/t0052_01.htm

# Seznam příloh

# Příloha A – ukázka přihlášených SSO uživatelů ve webovém rozhraní firewallu Fortigate



# Příloha B – log událostí Windows serveru při přihlášení uživatele do domény