UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

OCHRANA PŘÍSTUPU DO SÍTĚ

Jovkhar Issayev

Bakalářská práce

2020

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jovkhar Issayev**
Osobní číslo:	**I17110**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Ochrana přístupu do sítě**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Student v teoretické části práce popíše obecnou problematiku zabezpečování sítí pomocí technologií ochrany přístupu do sítě z pohledu síťového administrátora a přípravu sítě na implementaci takového systému. Dále se bude student zaobírat protokolem 802.1x, který k systémům přístupu ochrany do sítě neodmyslitelně patří. V praktické části vytvoří LAB, kde bude tento systém za pomocí Windows Server NPS(Network Policy Server)/NAP(Network Access protection) implementován.

Rozsah pracovní zprávy: **30**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná**

Seznam doporučené literatury:

ROUNTREE, Derrick. Security for Microsoft Windows system administrators: introduction to key information security concepts. Boston: Syngress, c2011. ISBN 1597495948.

BLOKDYK, Gerardus. Network Policy Server Standard Requirements. 5STARCooks, 2018. ISBN 9780655199656.

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

Datum zadání bakalářské práce: **15. listopadu 2019**
Termín odevzdání bakalářské práce: **7. května 2020**

Univerzita Pardubice
Česká republika
L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Ing. Lukáš Čegan, Ph.D.
pověřený vedením katedry

V Pardubicích dne 17. prosince 2019

Prohlašuji

Tuto práci jsem 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., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, 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.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 12. 8. 2020 ……

Jovkhar Issayev

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Soně Neradové, Ph. D za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování bakalářské práce. Rád bych poděkoval také své rodině a všem přátelům, kteří mě při vytváření této práce podpořili, a bez jejichž pomoci by nebylo možné práci dokončit.

Anotace

Bakalářská práce se zaměřuje na bezpečnostní problémy počítačových sítí a konfiguraci síťové infrastruktury pomocí NPS/NAP a protokolu 802.1x. Úvod práce je zaměřen na analýzu problematiky zabezpečení počítačových sítí pomocí technologií ochrany přístupu do počítačových sítí. V praktické části je vytvořen testovací scénář, kde ochrana přístupu do počítačové sítě je realizována za použití protokolu 802.1x a služby NPS.

Klíčová slova

AAA, EAP, IEEE 802.1x, NAP, NPS, RADIUS, MAB

Title

Security analysis based on NPS/NAP and the IEEE 802.1x protocol

Annotation

The bachelor's thesis focuses on security issues of computer networks and configuration of network infrastructure using NPS/NAP and the 802.1x protocol. The introduction is focused on the analysis of network security issues using computer network access protection technologies. The practical part is focused on creating a lab, where the protection of access to the computer network will be implemented using the 802.1x protocol and the NPS service.

Keywords

AAA, EAP, IEEE 802.1x, NAP, NPS, RADIUS, MAB

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AAA	Authentication, Authorization and Accounting
ACL	Access-control list
ACS	Access Control Software
AD CS	Active Directory Certificate Services
AD	Active Directory
AP	Access Point
API	Application Programming Interface
AS	Authentication server
AVP	Attribute Value Pair
BYOD	Bring your own device
CA	Certificate authority
CHAP	Challenge Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAPOR	EAP over RADIUS
EC	Enforcement Client
ES	Enforcement Server
HRA	Health Registration Authority
HTTP	Hypertext Transfer Protocol
IAS	Internet Authentication Service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
KDC	Key Distribution Centre
LEAP	Lightweight EAP Protocol
MAB	MAC Authentication Bypass
MAC	Media Access Control
MD5	Message-Digest algorithm
MITM	Man in the middle

NAC	Network Access Control
NAD	Network Access Device
NAS	Network Access Server
NPAS	Network Policy and Access Services
NPS	Network Policy Server
OTP	One-Time Passwords
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PK	Private Key
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
RFC	Request for Comments
SHA	System Health Agent
SHV	System Health Validator
SoH	Statement of Health
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TGS	Ticket Granting Server
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VMPS	VLAN Management Policy Server
VoIP	Voice over Internet Protocol
VPN	Virtual private network
WSUS	Windows Server Update Services

Úvod

Ještě nedávno síťová bezpečnost nehrála tak důležitou roli, jakou hraje dnes. Většina firem neměla osobní počítače, nepoužívala internet. Situace se postupně začala měnit a informační technologie se začaly rozvíjet neuvěřitelnou rychlostí. Na trhu se objevily osobní počítače, vznikla první počítačová síť ARPANET, která je prarodičem internetu. Ve dnešní době prakticky každá firma, ať malá nebo velká, má alespoň nějakou síťovou infrastrukturu, přístup k internetu, čímž se riziko nebezpečí zvyšuje, počítače, tiskárny a další zařízení, která obsahují důležitá data a neoprávněné osoby by neměly mít k nim přístup.

Pohled na síťovou bezpečnost také nezůstal na svém místě a postupem času se začal měnit. Vše, co může být zneužito a představuje nějakou hodnotu z pohledu kyberbezpečnosti by mělo být zabezpečeno. Příkladem jsou aplikace, data přenášená po sítích, hardware, přístup k počítačovým sítím. Síťová bezpečnost je velmi rozsáhle téma, proto tato bakalářská práce bude zaměřena na jednu z její oblastí – ochranu přístupu do počítačových sítí.

Cílem bakalářské práce bylo realizovat nasazení architektury NAP se zaměřením na drátové připojení prostřednictvím protokolu 802.1x.

Teoretická část bakalářské práce popisuje problematiku ochrany přístupu do počítačových sítí a technologie zajišťující její řešení.

V praktické části je navrhnuta a realizována testovací topologie počítačové sítě, která zabrání přístup do sítě neoprávněným osobám. Pro implementaci byl použit protokol 802.1x a NPS/NAP.

1 Pohled na síťovou bezpečnost

Každá problematika má svoji historii vývoje, zabezpečení a řízení přístupu do počítačových sítí není výjimkou. Historie dává možnost pochopit kořen problematiky, vznikla řešení a možnost předpovídat směr její vývoje v budoucnu. Právě první kapitola je věnována historii a vzniklým řešením v oblasti ochrany přístupu do počítačových sítí.

Dnešní představení o ochraně síťového přístupu představuje logický řetězec dlouhodobých změn pohledu na otázku síťové bezpečnosti. Dřív základem síťové bezpečnosti byla ochrana tzv. perimetru – zóna na styku vnitřní a veřejné sítě. Velkou popularitu v tu dobu měl firewall, ale obrovské rozšíření internetu přineslo nové bezpečnostní problémy a hrozby vniknutí do počítačové sítě, které mohou pocházet od útočníků jak pomocí fyzického, tak i vzdáleného přístupu přes internet. Další důležitou fází byl přechod k individuálnímu zabezpečení síťových rozhraní a mantrou se stal personální firewall. Spoléhat se na ochranu jediným firewallem již nestačilo, škodlivý software útočí zevnitř, a svou popularitu získal bezpečnostní software (antivirový program, antispyware). Později, s nástupem bezdrátových sítí, které obnažují další problém – zabezpečení fyzického přístupu do vnitřní sítě, ať již té bezdrátové, nebo tradiční kabelové. Novou otázkou síťové bezpečnosti se stalo zajištění ochrany přístupu do sítě, jelikož dřív přístup k počítačům, síťovým prvkům měly jenom zodpovědné a řádně vyškolené osoby. Pro zabezpečení sítě je nutné zajistit kontrolu přístupu uživatelů k různým síťovým prvkům. Takovými prvky mohou být síťová zařízení, servery, počítače, aplikace a jiné prvky sítě. Pro zabránění přístupu k počítačové sítě byly zavedeny bezpečnostní opatření, která jsou popsána v řadě norem ISO/IEC 27000. Důležitou částí daných opatření je řízení přístupu uživatelů k počítačové síti a její aktivům (Afanasjev, 2012).

Pokud je síť malá, pak zabezpečení a řízení přístupu není obtížné a je v zodpovědnosti jednoho správce sítě. Má-li však organizace rozsáhlou podnikovou síť, pak zajištění řízení přístupu do sítě se dostává na jinou úroveň. V tomto případě přichází řešení v podobě AAA architektury, která umožňuje autentizaci, autorizaci a účtování uživatelů, tj. řídí přístup a zaznamenává provedené akce za použití protokolů rodiny AAA: TACACS+, RADIUS a Diameter. Například v ARPANETU problém řízení přístupu k počítačové síti řešil síťový protokol TACACS. TACACS umožňoval pouze autentizaci a autorizaci. Časem protokol TACACS nebyl schopen poskytnout nutnou spolehlivost a vznikly nové protokoly: TACACS+ a RADIUS. Jejich standardizace proběhla v roce 1997. Dané protokoly kromě autentizace a autorizace umožňovaly také účtování přístupu. Tak vzniklá nová třída protokolů – AAA, které slouží k centralizovanému řízení a účtování přístupu uživatelů do počítačové sítě. Jedním z posledních členů dané třídy protokolů je Diameter z roku 2003. Protokoly typu AAA dnes jsou velmi rozšířené a použité v různých autentizačních mechanismech: 802.1x, MAB, VPN nebo webová autentizace (Burda, 2009).

Samotné protokoly AAA architektury poskytují bezpečnostní služby, ale negarantují bezpečnost připojených zařízení (notebooků, tiskáren). Kritická situace je u větších firem, jejichž pracovníci se běžně připojují vzdáleně k síti z různých počítačů, o jejichž momentálním stavu jsou jen mlhavá představení, i když se dnes klientské stanice vybavují důležitými softwarovými prostředky (antivir, antispyware, firewall, ochrana spouštění aplikací pod vysokými oprávněními atd.). Docela často se stává, že připojené k počítačové síti zařízení obsahuje škodlivé programy, nesplňuje nastavená bezpečnostní pravidla (zapnutý firewall, nainstalovaný antivirový program) a tím ohrožuje bezpečnosti celé sítě. Pro zajištění kontroly splnění připojenými zařízeními nastavených bezpečnostních pravidel slouží NAC. Různé společnosti nabízí různá řešení: NAP od společnosti Microsoft, PacketFence nebo Cisco NAC (Afanasjev, 2012; Kenin, 2019).

2 AAA architektura

Před tím, než přejdeme k samotným technologiím zabezpečení a řízení přístupu k počítačovým sítím, je důležité se zmínit o AAA architektuře, která poskytuje rozšířené zabezpečení síťové infrastruktury a je důležitou součástí způsobů ochrany přístupu do počítačových sítí.

Hlavním cílem AAA architektury je zajistit centralizované řízení přístupu k prostředkům sítě a provedení účtování akcí uživatelů. Pro tyto účely AAA poskytuje tři nezávislé bezpečnostní služby: autentizaci, autorizaci a účtování (Burda, 2009).

AAA používá model klient-server. Přístupové zařízení, na kterém běží klient AAA, se obvykle nazývá NAS. NAS je zodpovědný za ověření identity uživatele a správu přístupu uživatelů. Server AAA poskytuje služby ověřování, autorizace a účtování, odpovídá za centralizovanou správu informací o uživateli (Afanasjev, 2012; Kenin, 2019).

2.1 Bezpečnostní služby AAA architektury

2.1.1 Autentizace

Autentizace – proces ověření totožnosti subjektu, který umožňuje se přesvědčit v tom, že subjekt poskytující svůj identifikátor je tím, čí identifikátor používá. Subjekt při autentizaci poskytuje unikátní informaci – autentizační faktor. K autentizačním faktorům patří faktory, které se využívají v různých kombinacích:

- znalost – něco, co uživatel zná (PIN-kód, heslo);
- vlastnictví – něco, co uživatel vlastní (OTP-token, smart karta);
- biometrie – něco, co jednoznačně identifikuje uživatele (otisk prstů, hlas) (Afanasjev, 2012).

Autentizace může probíhat jak za použití jednoho faktoru – jednofaktorová autentizace, tak i za použití několika faktorů – vícefaktorová autentizace (např. smart-karta a heslo) (Afanasjev, 2012).

Autentizace také může být jednostrannou a oboustrannou. Jednostranná autentizace – autentizace stran, u nichž jedna ze stran ověří, že strana, která s ní spolupracuje, je ta, pro kterou tvrdí, že je (Afanasjev, 2012).

Oboustranná (vzájemná) autentizace – autentizace stran, ve které každá ze stran ověří, že strana, která s ní spolupracuje, je přesně tou, pro kterou tvrdí, že je (Afanasjev, 2012).

Způsoby autentizace

Za účelem ověření uživatele při přístupu do počítačové sítě může být využita jedna z následujících metod:

- **Autentizace bez uživatelského jména a hesla**

Nebezpečná metoda. Uživatel nemusí znát heslo, stačí použít správnou metodu přístupu do sítě. Používá se pro přístup ve veřejných sítích, kde je minimální požadavek na bezpečnostní politiku, nebo kde je bezpečnost zajištěna jiným prvkem (Afanasjev, 2012).

- **Autentizace pomocí zapamatování hesla**

Tento způsob autentizace je založen na faktoru znalosti. Uživatel musí správně zadat uživatelské jméno a heslo pro úspěšnou autentizaci.

Existují různé způsoby autentizace pomocí hesla:

  - autentizace na základě otevřeného klíče, uživatelské jméno a heslo se předává po síti v nezašifrované podobě**;**
  - autentizace na základě zahashovaného klíče, po síti se předává uživatelské jméno a zahashované heslo místo hesla v otevřené podobě**;**
  - autentizace na základě PIN, většinou se používá při autentizaci na lokálních zařízeních (např. bankomaty) (Afanasjev, 2012).

Nevýhodou daného způsobu autentizace je možnost heslo ukrást, nakouknout nebo uhodnout, a hlavně si zapamatovat všechna hesla s dostatečnou úrovní složitostí (Afanasjev, 2012).

- **Autentizace pomocí jednorázového hesla**

Jednorázové heslo (OTP) – dynamická autentizační informace pro autentizaci na jedno použití. Ke generování jednorázových hesel slouží softwarová nebo hardwarová zařízení. Jednorázové heslo je bezpečné proti analýze síťového provozu. Nehledě na to, že útočník může heslo odcizit analýzou síťového provozu, heslo je validní jen jednou a omezenou dobu, což velmi snižuje šance použití útočníkem odposlechnuté informace (Afanasjev, 2012).

Obvykle pro generování jednorázového hesla se používají tokeny OTP. OTP-token – mobilní personální zařízení, které vlastní určitý uživatel a slouží k autentizaci uživatele v systému. OTP-tokeny většinou mají malou velikost a vyrábí se ve formě malé kalkulačky. Pro generování autentizačních dat tokeny používají hašovací funkce nebo kryptografické algoritmy:

- symetrickou kryptografii – k autentizaci se používá jeden unikátní klíč;
- asymetrickou kryptografii – zařízení obsahuje privátní klíč a autentizační systém (server) používá veřejný klíč (Afanasjev, 2012).

Většinou v OTP-tokenech se používá symetrická kryptografie. Zařízení každého uživatele obsahuje unikátní klíč pro šifrování dat. Stejný klíč je uložen na autentizačním systému (serveru), který zajišťuje autentizaci uživatele. Autentizační systém šifruje stejná data, jako uživatel a porovnává výsledky šifrování. Pokud výsledky přijaté od uživatele jsou stejné, uživatel bude úspěšně autentizován v systému (Afanasjev, 2012).

Autentizace pomocí jednorázového hesla se většinou používá při realizaci dvoufaktorové autentizace a je určena k ověření pouze vzdálených, nikoli lokálních uživatelů (Afanasjev, 2012).

- **Autentizace pomocí certifikátu**

Autentizace na základě certifikátu probíhá ve formě klient-server, kde certifikátem je sada atributů, které slouží k identifikaci majitele daného certifikátu. Certifikát podepisuje certifikační autorita (CA). CA vystupuje v roli zprostředkovatele, který zaručuje pravost certifikátu. Certifikát kryptograficky souvisí s privátním klíčem, který vlastní majitel certifikátu a umožňuje jednoznačně potvrdit faktor vlastnictví certifikátu. Na straně uživatele certifikát spolu s privátním klíčem mohou být uložené přímo na pracovní stanici nebo na jiném fyzickém nosiči. Privátní klíč může být navíc chráněn heslem nebo PIN-kódem. Při přihlášení uživatele do sítě probíhá kontrola certifikátu. Nejvíc se používají certifikáty standardu X.509 v3. Při předání certifikátu musí být zajištěna bezpečnost, aby nedošlo k zneužití daného certifikátu neoprávněnou osobou. Privátní klíč také by měl být uložen v bezpečném místě, jinak může dojít k jeho kompromitování (Afanasjev, 2012).

2.1.2 Autorizace

Autorizace – proces ověření oprávnění subjektu. Oprávnění určuje prostředky, ke kterým subjekt může přistupovat. Autorizace může sloužit k omezení přístupu do počítačové sítě, například povolení přístupu jen v určitých hodinách. Proces autentizace a autorizace může probíhat jak současně (RADIUS), tak odděleně (TACACS+) (Afanasjev, 2012).

2.1.3 Účtování

Účtování – proces řízení (monitorování) činnosti subjektu, který slouží k zaznamenávání akcí prováděných subjektem. Cílem účtování je detekovat nežádoucí akce subjektu nebo

zajistit efektivitu využívání aktiv v systému. Záznamy při účtování pak mohou být analyzovány pro správu sítě (Afanasjev, 2012).

2.2 Protokoly AAA architektury

Pro realizaci procesu autentizace, autorizace a účtování se v AAA architektuře používají dva hlavní řešení: RADIUS a TACACS+, proto dále jsou popsány tyto dva protokoly a autentizační mechanismy, se kterými je možné zmíněné protokoly kombinovat. Protokol Diameter většinou používají mobilní operátoři a v této práci není popsán.

2.2.1 TLS

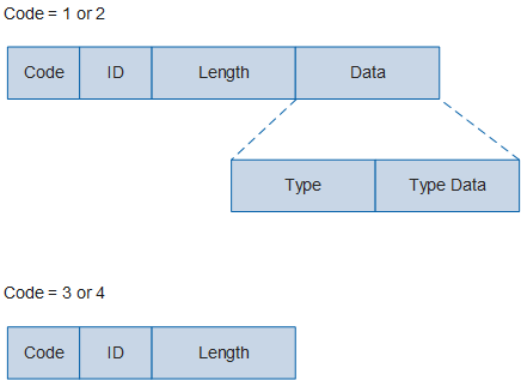
TLS – protokol, zajišťující integritu a důvěrnost přenášených dat, je založen na protokolu SSL, který byl vyvinut společností Netscape. TLS zajišťuje vzájemnou autentizaci a používá se v různých autentizačních mechanismech (PEAP, EAP-TLS). Autentizace v TLS je založena na certifikátech veřejných klíčů. Protokol TLS se rozděluje na dvě úrovně: TLS Record Protocol a TLS Handshake Protocol.

TLS Record Protocol zajišťuje spolehlivý a bezpečný přenos dat pomocí symetrického šifrování. TLS Record Protocol se často používá k zapouzdření protokolu vyšších úrovní jako TLS Handshake Protocol, kontroluje integritu předávaných zpráv pomocí autentizačního kódu (message authentication code, MAC) (Burda, 2009; Afanasjev, 2012).

TLS Handshake Protocol zajišťuje vzájemnou autentizaci. Autentizace vyžaduje nasazení PKI infrastruktury. Účastníci se musí domluvit na algoritmu šifrování, provést výměnu klíčů založenou na šifrování s veřejným klíčem. TLS jako transportní protokol používá TCP, pro použití UDP byla vyvinuta speciální verze DTLS. Poslední verze protokolu je TLS 1.3 (Burda, 2009; Afanasjev, 2012).

2.2.2 EAP

Protokol EAP zajišťuje autentizaci pomocí různých metod a podporuje různé způsoby autentizace (smart-karty, jednorázová hesla). Původně byl vytvořen pro použití s protokolem PPP jako náhrada CHAP, ale dnes se také používá v jiných standardech (např. 802.1x). Formát zpráv protokolu EAP je popsán v RFC 3748 a obnoven v RFC 5274. Protokol EAP neurčuje protokol linkové vrstvy, i když byl vytvořen pro použití s protokolem PPP. Daný protokol tvoří celou skupinu autentizačních metod založených na daném formátu zpráv (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004; Afanasjev, 2012).



Obrázek 1: Formát rámce EAP

Zdroj: (Huawei, 2020)

Formát EAP je uveden na obrázku č. 1. Pole Code má velikost 1 bajt a může nabývat dalších hodnot:

- Request (1);
- Response (2);
- Success (3);
- Failure (4) (Aboba et al., 2004).

Pole Identifier je velikosti 1 bajt a slouží k porovnávání žádosti a odpovědi. Pole Length obsahuje velikost celého paketu, velikost pole je 2 bajty. Pole data má proměnlivou velikost a závisí na poli Code. Jestli hodnota pole Code je 1 nebo 2, pole Data obsahuje pole Type a Type Data. Pole Type je velikosti 1 bajt a slouží k identifikaci typu paketu (žádost nebo odpověď). Možné hodnoty pole Type:

- Identity – požaduje nebo vrací informaci o uživatelském jméně uživatele;
- NAK – negativní potvrzení, používá se při odpovědi. Klient může požádat o jinou metodu EAP zasláním zprávy EAP-Response Auth NAK, která také specifikuje metodu autentizace EAP, kterou chce klient použít;
- EAP-TLS – označuje, že metoda ověřování je EAP-TLS (Aboba et al., 2004).

Pole Type Data má proměnlivou délku, hodnota závisí na poli Type. Pokud hodnota pole Code je 3 nebo 4, pole Data je prázdné (Aboba et al., 2004).

Obsah EAP zpráv závisí na konkrétní autentizační metodě. Množství EAP metod lze rozdělit následovaně:

- znalost hesla (např. EAP-MD5, EAP-OTP);
- vlastnictví předmětu (EAP-GTC, EAP-SIM, EAP-AKA);
- použití soukromého klíče (EAP-TLS);

- hybridní – každá strana používá svůj dokazovací faktor (např. EAP-IKEv2, EAP-TTLS) (Burda, 2009).

Metody EAP

Jak již bylo zmíněno výš, existuje velké množství EAP metod, mezi nimiž existují jednoduché metody založené na kontrolním součtu a metody tunelů, které zahrnují vytvoření bezpečného tunelu, ve kterém mohou být použity různé způsoby ověřování. Některé z nich jsou uvedeny níže.

EAP-MD5 – jednostranná autentizace žadatele, původně navržena pro metalické sítě. Proces autentizace je podobný protokolu CHAP. Žadatel pomocí algoritmu MD5 hašuje heslo, které posílá na autentizační server v otevřené formě. Daná metoda je nebezpečná, nedoporučuje se ji používat (Afanasjev, 2012).

LEAP metoda byla vyvinuta společností Cisco Systems v roce 2000. LEAP je snadno nastavitelný, což vychází z názvu Lightweight. Autentizace probíhá s využitím uživatelského jména a hesla prostřednictvím serveru RADIUS. Většinou se používá v bezdrátových sítích. LEAP umožňuje generovat dynamické WEP klíče při každé autentizaci uživatele do sítě. V roce 2004 Joshua Wright napsal exploit ASLEAP, který umožnil metodu snadno prolomit. Metoda LEAP je dnes zastaralá a nebezpečná. Společnost Cisco Systems nahradila LEAP metodou EAP-FAST, která by měla odstranit bezpečnostní problémy LEAP (Afanasjev, 2012).

EAP-FAST byla vydána společností Cisco Systems. EAP-FAST chrání přihlašovací údaje pomocí sdíleného tajného klíče generovaného ověřovacím serverem. Tento sdílený tajný klíč se nazývá PAC a používá se pro vzájemnou autentizaci. K problémům dané metody patří distribuce souboru PAC. EAP-FAST umožňuje manuální a automatickou distribuci daného souboru. Manuální distribuce může být zajištěna pomocí USB flash disku nebo jiného nosiče. Automatická distribuce může být nebezpečná, proto se doporučuje nainstalovat na autentizační server serverový certifikát (Afanasjev, 2012).

EAP-TLS zajišťuje vzájemnou autentizaci pomocí certifikátů. Metoda EAP-TLS je založena na protokolu *SSLv3*. Certifikát musí vlastnit jak klient, tak autentizační server. Server otevírá TLS seanci se žadatelem a posílá mu svůj certifikát. Žadatel po kontrole přijatého od serveru certifikátu posílá na server svůj certifikát, server také provádí jeho kontrolu. Autentizace proběhne úspěšně, pokud kontrola certifikátů z obou stran bude úspěšná. EAP-TLS zajišťuje vysokou úroveň bezpečnosti, ale je docela náročný na použití kvůli PKI (Afanasjev, 2012).

EAP-TTLS byla vyvinuta společností Funk Software a Certicom, je rozšířením EAP-TLS. V dané metodě autentizace klienta není nutná, což zjednodušuje konfiguraci, protože není potřeba generovat a předávat každému klientovi unikátní certifikát. Po autentizaci serveru na straně klienta se vytváří zabezpečený tunel, který slouží k autentizaci klienta. Tunel

umožňuje použití autentizačních protokolů přes kanály, nezabezpečené proti útoku MITM nebo odposlechu (Afanasjev, 2012).

EAP-MS-CHAPv2/ PEAPv0 je populárním způsobem autentizace při použití PEAP v prostředí Microsoft Windows. Metoda EAP-MS-CHAPv2 je založena na protokolu MS-CHAPv2, který provádí ověřování na základě hesla (Afanasjev, 2012).

Protokol **PEAP** slouží k bezpečnému přenosu autentizačních dat. PEAP byl vyvinut společností Cisco Systems, Microsoft a RSA Security. Bezpečnost autentizačních údajů je zajištěna protokolem TLS, který vytváří šifrovaný tunel. Protokol PEAP neurčuje metodu ověřování, zajišťuje pouze zabezpečený přenos autentizačních dat. Autentizace se většinou zajišťuje použitím certifikátů (EAP-TLS) nebo uživatelského jména a hesla (MSCHAPv2). Navázání PEAP spojení se skládá ze dvou etap (Afanasjev, 2012).

První etapa:

- klient dostává žádost o navázání spojení za použití protokolu EAP;
- klient posílá svoje uživatelské jméno;
- server nabízí použití PEAP pro autentizaci;
- klient potvrzuje typ protokolu a zasílá identifikátor spojení TLS (Client Hello);
- server předává klientovi svůj certifikát a identifikátor spojení TLS (Server Hello);
- klient provádí kontrolu certifikátu serveru, generuje klíč seance TLS, šifruje daný klíč pomocí veřejného klíče serveru a zasílá šifrovaný klíč serveru;
- server dešifruje přijatý klíč pomocí svého privátního klíče a potvrzuje konec dané fáze (Afanasjev, 2012).

Druhá etapa:

- server posílá klientovi žádost o uživatelské jméno klienta (identifikátoru);
- klient odesílá serveru svůj identifikátor;
- server nabízí použití jedné z autentizačních metod;
- klient odesílá data potřebná pro provedení autentizace (hash hesla, certifikát, digitální podpis apod.) nebo nabízí použití jiné autentizační metody;
- server provádí kontrolu přijatých dat a v případě úspěchu klient bude úspěšně autentizován (Afanasjev, 2012).

Poslední verze PEAP je podobná EAP-TTLS tím, že není nutné mít nainstalovaný certifikát na straně klienta (Afanasjev, 2012).

2.2.3 EAPOL

EAPOL je formát zapouzdření paketů definovaný protokolem 802.1x. EAPOL se používá hlavně k přenosu paketů EAP přes LAN mezi klientem a přístupovým zařízením v prostředí 802.1x. Obrázek č. 2 ukazuje formát rámce EAPOL (Afanasjev, 2012).

Obrázek 2: Formát rámce EAPOL

Zdroj: (Huawei, 2020)

Pole PAE Ethernet Type určuje typ protokolu, hodnota je pevná a rovná se 0x888E pro EAPOL. Pole Protocol Version označuje verzi protokolu. Pole Type určuje typ paketu EAPOL. Možné hodnoty pole Type:

- EAP-Packet (0000 0000) – autentizační paket, který obsahuje autentizační informace;
- EAPOL-Start (0000 001) – autentizační startovací paket odeslány klientem;
- EAPOL-LogOff (0000 0010) – paket, obsahující požadavek na odhlášení odeslány klientem;
- EAPOL-Key (0000 0011) – paket pro výměnu informací o kryptografických klíčích (Afanasjev, 2012).

Pole Length obsahuje velikost dat v poli Packet Body. Pole Packet Body – obsah paketu. Pokud typ paketu EAPOL je EAP-Packet, pole Packet Body obsahuje EAP paket (Afanasjev, 2012).

2.2.4 Kerberos

Kerberos je autentizační a autorizační protokol, který má zaručit bezpečné využívání síťových zdrojů. Je popsán v RFC 1510. Hlavní myšlenka spočívá v tom, že se předpokládá, že celá síť je nedůvěryhodná. Kerberos pak definuje jeden velmi zabezpečený počítač, který zajišťuje autentizační a autorizační služby a je důvěryhodný pro celou síť. Tento počítač obsahuje informace o heslech a přístupových právech pro každého uživatele sítě. Jestliže chce uživatel využívat síťové služby nebo prostředků, nejprve se musí autentizovat u tohoto důvěryhodného počítače. Ten mu vydá lístek, který ho opravňuje využívat jemu dostupné služby nebo zdroje (Afanasjev, 2012).

Autentizace uživatelů pomocí protokolu Kerberos je založena na důvěryhodné třetí straně. Touto důvěryhodnou třetí stranou je centrální autentizační server (KDC). KDC spra-

vuje databázi uživatelů a přiděluje jim lístky. Autentizace pomocí Kerberos systému je navržena tak, aby nemuselo po síti poletovat heslo, místo něj se používá přidělený lístek, který se může používat i na nezabezpečené síti. KDC se dělí na dva subsystémy:

- AS – je zodpovědný za autentizaci a autorizaci uživatelů a služeb;
- TGS – je zodpovědný za přidělování oprávnění-lístků k použití zdrojů (služeb) (Afanasjev, 2012).

2.2.5 TACACS+

TACACS+ je zlepšená verze svého předchůdce TACACS, který byl vyvinut společností Cisco Systems. Jako transportní protokol používá TCP. TACACS+ je založen na architektuře klient-server, kde klientem obvykle je NAS a serverem většinou je démon (spuštěný proces na unixovém systému). Všechny verze protokolu TACACS používají port 49. Protokol TACACS+, na rozdíl od RADIUS, rozděluje proces autentizace, autorizace a účtování, což umožňuje používat různé autentizační mechanismy (PAP, CHAP, MSCHAP nebo Kerberos). TACACS+ nepodporuje metody EAP. Autentizace v TACACS+ není nutná. Obvykle proces autorizace probíhá po autentizaci, ale není to podmínkou. Při autorizaci je možné uvést, že klient neprocházel proces autentizace. Ověřovatel pak sám rozhoduje o povolení přístupu žadatele k aktivům. TACACS+ umožňuje provádět účtování jakékoliv činnosti uživatelů. TACACS+ a RADIUS používají sdílený tajný klíč k zabezpečení komunikace mezi klientem a serverem, na rozdíl od TACACS+, RADIUS šifruje pouze heslo klienta, ostatní komunikaci nezabezpečuje. Sdílený tajný klíč se nikdy nepřenáší po síti. Obvykle tajný klíč se nastavuje jak na straně serveru, tak i na straně klienta (Afanasjev, 2012).

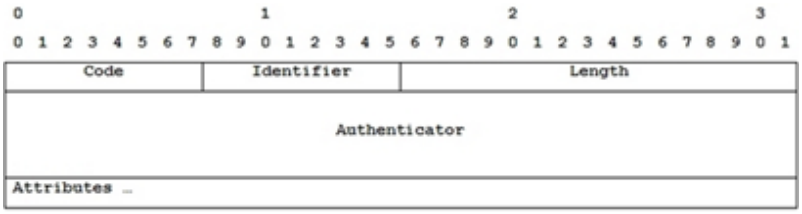
2.2.6 RADIUS

Protokol RADIUS byl vyvinut společností Livingston Enterprises, je popsán v RFC 2058 a RFC 2059 (poslední verze RFC 2865 a RFC 2866). Používá se při řízení přístupu k přístupovým bodům, přepínačům a jiným zařízením. RADIUS jako transportní protokol používá UDP. Pro autentizaci slouží port 1812/1645, 1813/1646 pro účtování. Princip činnosti je založen na architektuře klient-server, kde klientem obvykle je NAS a serverem většinou je démon. Servery RADIUS přijímají požadavky uživatelů na připojení a provádějí ověřování uživatelů. Pro jiné servery RADIUS server může hrát roli proxy serveru. Účty uživatelů se ukládají do databáze, textových souborů nebo vnějších serverů. Server RADIUS může podporovat různé metody autentizace (PAP, CHAP, MS-CHAP a EAP metody). Proces autentizace a autorizace u RADIUSu je sloučen, proces účtování probíhá samostatně (Rigney, Willnes, Rubens, & Simpson, 2000; Afanasjev, 2012).

Proces autentizace pomocí RADIUS serveru

1) zařízení uživatele (notebook, IP-telefon apod.) inicializuje spojení s NAS (autentizátor; např. přepínač, přístupový bod, směrovač) přes PPP nebo jiný protokol;
2) NAS posílá žádost o autentizační údaje;
3) uživatel poskytuje požadované autentizační údaje;
4) NAS po přijetí dané informace od klienta provádí proces autentizace klienta na RADIUS serveru: vytváří žádost Access-Request obsahující v atributech potřebnou autentizační informaci. V případě, že NAS nedostane odpověď, zpráva bude opakována;
5) pokud NAS je autentizován, RADIUS server provádí kontrolu uživatele a odpovídá NAS zprávou Accept, Reject nebo Challenge.V případě zprávy Access-Challenge NAS požádá uživatelské zařízení o doplňující informaci a zase pošle zprávu Access-Request, na kterou RADIUS server odpoví zprávou Accept nebo Reject;
6) NAS zpracovává odpověď RADIUS serveru a přeposílá výsledek uživatelskému zařízení (Afanasjev, 2012).

Formát rámce RADIUS je uveden na obrázku č. 3. Pole Code identifikuje typ RADIUS paketu. Pokud paket obsahuje neplatnou hodnotu, paket bude zahozen (Rigney et al., 2000).



Obrázek 3: Formát rámce RADIUS

Zdroj: (Rigney et al., 2000)

Hodnoty pole Code

- Access-Request (1) – žádost o autentizaci ze strany autentizátoru. Paket obsahuje informace k určení, zda má uživatel povolen přístup k NAS a jaké služby jsou pro uživatele dostupné;
- Access-Accept (2) – potvrzení úspěšné autentizace RADIUS serverem;
- Access-Reject (3) – neúspěšná autentizace, přístup uživatele byl odepřen. RADIUS server může doplnit odpověď textovou zprávou;
- Access-Challenge (11) – žádost RADIUS serveru o doplňující informaci od klienta. Například druhé heslo, PIN, číslo karty apod (Rigney et al., 2000).

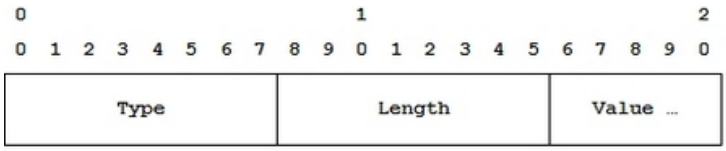
- Accounting-Request (4) – zpráva, kterou posílá autentizátor RADIUS serveru. Zpráva obsahuje akce, které byly provedeny uživatelem. Pakety Accounting-Request obsahují atribut Acct-Status-Type s dalšími hodnotami: start pro spuštění procesu účtování, stop pro ukončení procesu a interim-update pro aktualizace informace;
- Accounting-Response (5) – potvrzení o přijetí zprávy Accounting-Request, která byla odeslána autentizátorem.

Pole Identifier obsahuje hodnotu sloužící k identifikaci duplicitních paketů. Důležité pole, protože RADIUS využívá bezstavový UDP protokol. Velikost je 1 oktet. Pole Length obsahuje velikost paketu a zabírá 2 oktety. Pokud je velikost přijatého paketu menší než hodnota Length, paket se zahodí. Pole Authenticator se skládá ze 16 oktetů, je použito k zabezpečení komunikace mezi autentizátorem a serverem RADIUS. Obsahem pole je náhodné číslo. Pokud paket pochází ze serveru RADIUS, jeho hodnotou je MD5 hash vypočítaný z přijaté zprávy Access-Request / Accounting-Request a sdíleného hesla, které je známé jak autentizátorovi, tak serveru RADIUS (Rigney et al., 2000).

V protokolu RADIUS jsou všechna data přenášena v prvcích nazývaných atributy (Attribute Value Pairs, AVPs). Atributy RADIUS se používají pří přenosu:

- autentizačních dat uživatelů,
- autorizačních dat uživatelů,
- dat, nezbytných pro účtování činnosti uživatelů (Rigney et al., 2000).

Formát atributů RADIUS je uveden na obrázku č. 4. Hodnoty pole Type jsou čísla, jejich význam je jednoznačně určen v standardech RADIUS. Pole Length určuje velikost atributu. Položka Value – vlastní obsah atributu. Možných atributů protokolu RADIUS existuje více než 100, v prostředí 802.1x se však smí vyskytovat jen několik desítek z nich. Atribut může být určen v specifikaci protokolu RADIUS (standard attribute) nebo výrobcem (vendor-specific attribute) (Rigney et al., 2000; Afanasjev, 2012).



Obrázek 4: Formát atributů RADIUS

Zdroj: (Rigney et al., 2000)

3 Způsoby zabezpečení přístupu do sítě

Tato kapitola je nejdůležitější částí této práce, protože v ní jsou popsány technologie ochrany přístupu do počítačových sítí. Ve dnešní době existuje široká škála technologií pro zabezpečení a řízení přístupu do počítačových sítí, z toho důvodu tato kapitola je zaměřena na následující řešení:

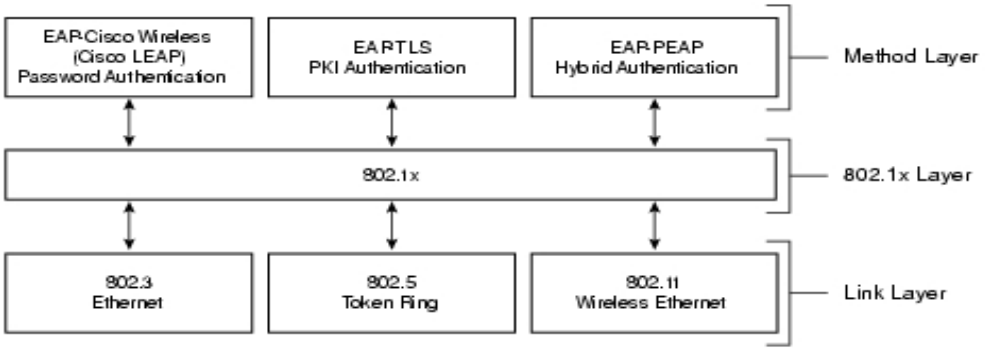
- IEEE 802.1x,
- MAB,
- NAC.

3.1 802.1x

Standard IEEE 802.1x je součástí architektury AAA, který určuje mechanismus autentifikace a autorizace na úrovni portu (port based security). 802.1x provádí kontrolu přístupu a neumožňuje se připojit k síti přes porty síťových prvků neautentizovaným zařízením. Portem v daném kontextu může být port přepínače Ethernet nebo virtuální port AP. Tento standard se stal docela populárním u výrobců síťových zařízení a programového vybavení. Největší rozšíření 802.1x dostal v bezdrátových sítích (Kubát, 2014; Afanasjev, 2012).

Vrstvy architektury 802.1 x jsou uvedeny na obrázku č. 5 a vykonávají následující funkce:

- linková vrstva – slouží k uzpůsobení konkrétní LAN technologii (definice specifických rámců);
- vrstva 802.1x – slouží k zajištění pravidel pro komunikaci mezi komponentami systému (suplikant, autentizátor a autentizační server);
- vrstva ověřovací metody – řeší konkrétní metodu ověření uživatele (Kubát, 2014).



Obrázek 5: Vrstvy architektury 802.1x

Zdroj: (Kubát, 2014)

Díky standardu 802.1x je možné poskytovat uživatelům přístupová práva k síti a jejím službám v závislosti na skupině nebo pozici, kterou tento uživatel zastává. Připojením k bezdrátové síti nebo k síťové zásuvce kdekoli v síti bude uživatel automaticky umístěn do této VLAN, což je předem určeno zásadami skupiny, ke které je uživatelský účet nebo jeho pracovní stanice připojena. Odpovídající seznam ACL (statický nebo dynamický) může být vázán na tuto VLAN pro řízení přístupu k podnikovým službám. Kromě přístupových seznamů mohou být politiky QoS spojené s VLAN pro řízení šířky pásma (Kubát, 2014; Afanasjev, 2012).

3.1.1 Průběh 802.1x

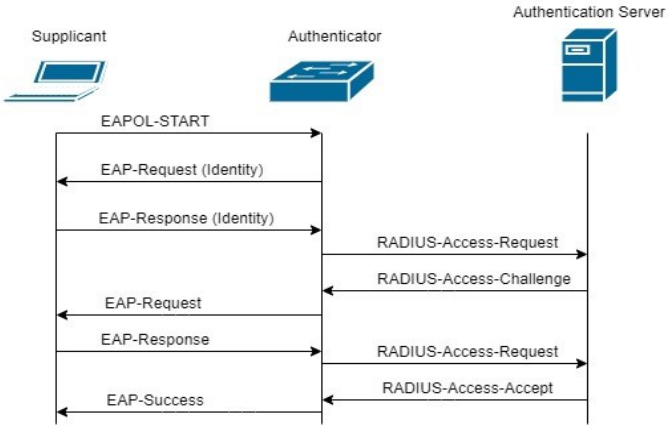
Proces řízení přístupu se skládá z tří komponent:

- suplikant (supplicant) – žádá o připojení. Posílá informaci potřebnou pro provedení autentizace. Autentizační údaje mohou být zaslány jako odpověď na žádost autentizátoru nebo suplikant může sám iniciovat autentizační proces. Roli suplikanta může hrát síťová karta počítače, na kterém je nainstalován potřebný software pro podporu 802.1x;
- autentizátor (authenticator) – fyzický nebo virtuální port síťového zařízení podporující 802.1x. Autentizátor je zodpovědný za spuštění autentizačního procesu před tím, než povolit přístup k službám, které jsou přes daný port dostupné. Hraje roli proxy mezi uživatelským zařízením a autentizačním serverem;
- autentizační server (authentication server) – poskytuje autentizační informaci autentizátoru. Na základě přijaté informace od autentizátoru rozhoduje o povolení nebo odepření přístupu k síti. Roli autentizačního serveru většinou hraje RADIUS server (Kubát, 2014; Afanasjev, 2012).

802.1x pro autentizaci používá EAP protokol a umožňuje neautentizovaným uživatelům posílat jenom EAP zprávy. EAP slouží k zajištění spolupráce:

- suplikanta a autentizátoru,
- autentizátoru a autentizačního serveru (Afanasjev, 2012).

Na úseku *suplikant & autentizátor* se používá protokol EAP zabaleny do ethernetového rámce – EAPOL. Hlavním rozdílem při komunikaci pomocí protokolů EAP a EAPOL je v tom, že EAPOL umožnuje suplikantovi posílat zprávy EAPOL-Start a EAPOL-Logoff (Afanasjev, 2012).



Obrázek 6: Průběh 802.1x

Zdroj: (Afanasjev, 2012)

Na úseku *autentizátor & autentizační server* data protokolu EAP se zapouzdřují do paketů určených pro autentizační server. Standard 802.1x nestanoví přesný protokol, který by měl používat server autentizace, proto se obvykle používá RADIUS. V tomto případě data protokolu EAP se budou přenášet pomocí protokolu RADIUS. Takový způsob inkapsulace se nazývá EAPOR. Data klienta a jiná důležitá informace se přenáší jako atributy v poli AVP. Pro podporu přenosu EAP zpráv byly do protokolu RADIUS přidány následující atributy:

- EAP-Message – slouží k zapouzdření dat od klienta k RADIUS serveru;
- Message-Authenticator – slouží k zajištění integrity dat a prevenci proti spoofingu na úseku *autentizátor & autentizační server* (Kubát, 2014; Afanasjev, 2012).

K dalším atributům protokolu RADIUS, které je možné použít v prostředí 802.1x patří:

- Tunnel Attributes – atributy, sloužící k dynamickému přiřazení VLAN. K dané skupině patří atributy Tunnel-Type, Tunnel-Medium-Type a Tunnel-Private-Group-ID. Atribut Tunnel-Typ musí být nastaven na hodnotu VLAN nebo 13, Tunnel-Medium-Type na 802 nebo 6 a Tunnel-Private-Group-ID označuje identifikátor VLAN;
- NAS-Port – atribut, který slouží k identifikaci fyzického portu NAS. Místo daného atributu může být použit atribut NAS-Port-Type;
- Service-Type – atribut označuje typ služby, kterou požádal suplikant (Congdon, Bernard, Smith, Roese, & Zorn, 2003).

Ostatní atributy jsou popsány v specifikaci RFC 3580. Pro autentizaci suplikanta může být použit jeden z následujících způsobů: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP a jiné EAP metody, které již byly popsány výš (Congdon et al., 2003).

Proces ověřování klienta

Proces ověřování klienta je znázorněn na obrázku č. 6 a je následující:

1) počítač se připojí k síťovému portu (switch port nebo virtuální port přístupového bodu). Síťový port je v zablokovaném stavu a prochází přes něj jenom autentizační rámce. Klient pošle informaci o tom, že se chce přihlásit do sítě (EAPOL-Start). Po přijetí zprávy od suplikanta autentizátor posílá požadavek na ověření totožnosti (EAP-Request/Identity). Autentizátor pravidelně odesílá EAP-Request, a to ještě před tím, než dostane zprávu EAPOL-Start**;**
2) suplikant žádost vyhodnotí a odpoví zprávou, obsahující informaci o totožnosti klienta (EAP-Response/Identity)**;**
3) autentizátor zprávu přebalí z rámce EAPOL do datagramu protokolu RADIUS a odešle ji pro ověření na RADIUS server**;**
4) autentizační server rozhodne jaký typ autentifikace EAP použít. Vytvoří zprávu Access-Challenge a pošle zpět na autentizátor. Zpráva Access-Challenge kromě výzvy (řetězec znaků), obsahuje způsob autentizace, který bude použit při komunikaci. Suplikant může odmítnout metodu autentizace a požádat o jinou, kterou sám podporuje zasláním zprávy EAP-Response Auth NAK**;**
5) autentizátor zase přebalí zprávu z formátu RADIUS do EAPOL a pošle ji suplikantovi**;**
6) suplikant provede potřebné operace (např. výpočet za použití svého hesla a přijaté zprávy Access-Challenge). Výsledky odešle autentizátoru zprávou EAP-Response, který opět přebalí paket a odešle na RADIUS-server**;**
7) v případě, že výsledky vypočtu klienta a serveru budou stejné, klient dostane od autentizátoru EAP-Success zprávu o úspěšné autentizaci. Autentizátor port odblokuje (změny stav na authorized) a provede potřebná nastavení portu (např. VLAN). Tím autentizační proces je ukončen a klient by měl mít přístup k síti (Kubát, 2014; Afanasjev, 2012).

Ukončení komunikace probíhá zasláním EAP-Logoff zprávy ze strany klienta. V případě ukončení komunikace buď korektním způsobem, nebo kvůli jiným problémům se spojením, port přejde do blokovaného stavu a uživatel se bude muset zase přihlásit (Kubát, 2014; Afanasjev, 2012).

3.1.2 Implementace 802.1x

Pro realizaci 802.1x je potřeba mít síťové zařízení podporující protokol 802.1x, RADIUS server, databázi uživatelů a klienta 802.1x na uživatelském zařízení. Klient 802.1x

je už předem nainstalován ve většině operačních systému jako je Linux, Solaris, Apple OS X, Windows XP/Vista/7/CE/Mobile (Afanasjev, 2012).

Možné způsoby realizace serveru RADIUS:

- Network Policy Server (Microsoft),
- FreeRadius,
- Cisco ACS (Afanasjev, 2012).

Podrobný proces nastavení 802.1x je uveden v praktické části.

3.2 MAB

802.1x je skvělý způsob, jak chránit síť autentizací všeho, co se připojí k síti. Jednou z nevýhod technologie 802.1x je však to, že je musí podporovat koncová zařízení. Pokud není možné použít 802.1x, ale přesto je nutné nějakým způsobem zabezpečit porty síťových zařízení, je možné použít MAB. Při zapnutí MAB budou zahozené všechny rámce, kromě prvního, který se používá k zjištění MAC adresy zařízení (viz. Obrázek 7). K zjištění MAC adresy lze použít téměř libovolný rámec s výjimkou na CDP, LLDP, STP a DTP. Jakmile přepínač zjistí adresu MAC, kontaktuje ověřovací server (RADIUS) a kontroluje, zda povoluje adresu MAC. MAB také podporuje dynamické hodnoty ze serveru RADIUS. Dynamický ACL a přiřazení VLAN je možné použít stejně jako u 802.1x. MAB nemůže kontrolovat nic jiného kromě MAC adresy. MAB má své bezpečnostní problémy, protože je možné snadno spoofovat (měnit) MAC adresy. Předchůdcem MAB je server Cisco VMPS (Cisco, 2011).

Způsoby konfigurace MAB

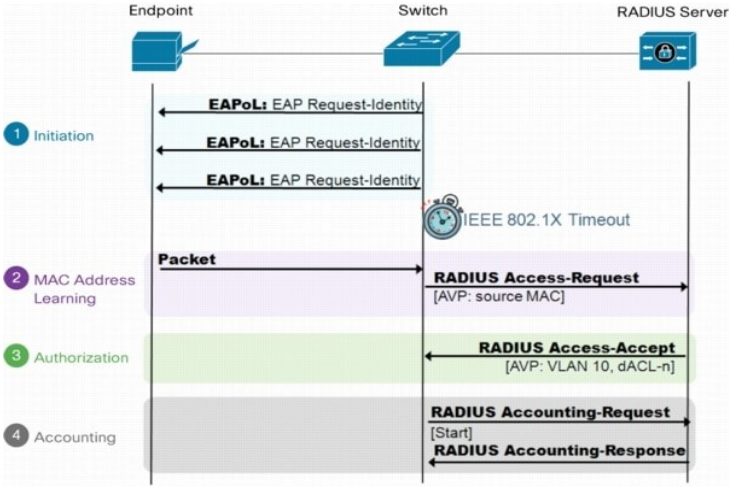
- Standalone MAB se používá pouze pro autentizaci (Cisco, 2011).
- Fallback MAB se používá jako záložní verze pro 802.1x. Přepínač se nejprve pokusí 802.1x a pokud selže, použije pro autentizaci MAB. Ve výchozím nastavení podporuje MAB pouze jedno zařízení na portu. Pokud MAB vidí více než jednu zdrojovou adresu MAC, dojde k narušení zabezpečení. To může být problém, když se například používá IP telefon s PC za ním. Toto chování je možné změnit nastavením režimu MAB (Cisco, 2011).

Režimy MAB

- Single-host mode – ověření pouze jediné zdrojové MAC adresy. Když přepínač detekuje po ověření jinou zdrojovou adresu MAC, dojde k narušení zabezpečení. Toto je výchozí nastavení (Cisco, 2011).

- Multi-domain authentication host mode – ověření dvou zdrojových MAC adres, jednu v hlasové VLAN a druhou v datové VLAN. Toto je scénář, kdy je IP telefon a počítač na jednom přepínači. Jakékoli další zdrojové adresy MAC způsobují narušení zabezpečení (Cisco, 2011).
- Multi-authentication host mode – ověření více zdrojových MAC adres. Je možné použít, když je přepínač připojen k jinému přepínači. Každá zdrojová adresa MAC je ověřena samostatně (Cisco, 2011).
- Multi-host mode – více zdrojových MAC adres. Ověřena je pouze první zdrojová adresa MAC, všechny ostatní zdrojové adresy MAC jsou automaticky povoleny (Cisco, 2011).

Zatímco 802.1x je standard, MAB standardem není. Každý výrobce může mít svoji implementaci, ale jen za předpokladu, že komunikace pomocí RADIUS odpovídá standardu.



Obrázek 7: Průběh MAB autentizace

Zdroj: (Cisco, 2011)

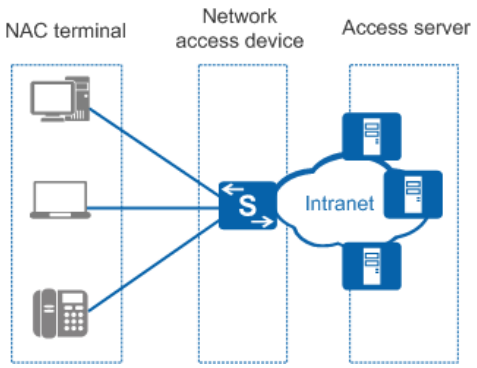
3.3 NAC

S rozvojem podnikové sítě hrozby stále více přinášejí rizika, jako jsou viry, trojské koně, spyware a škodlivé síťové útoky. Přestože podniková síť může mít velmi zabezpečenou konfiguraci, připojení uživatele s nedostatečnou ochranou může infikovat soubory v síti virem nebo náhodně otevřít důležité firemní informace, protože jeho počítač může být infikován trojským koněm. Škodlivý software se pak může šířit ve vnitřní síti. Jedním z řešení tohoto problému je NAC (Hoffman, 2008).

Technologie NAC slouží k řízení přístupu koncových zařízení (notebooků, IP-telefonů, tiskáren apod.) k síti. NAC na základě předem nastavených politik (přítomnost antiviru, verze OS, nastavení firewallu) buď zařízení přístup povolí, nebo zakáže. NAC nedělá

nic, aby zabránil neautorizovanému přístupu do sítě. Pokud má útočník počítač, který splňuje bezpečnostní požadavky, NAC neudělá nic, aby se pokusil útočníka zastavit. NAC je nezávislá na způsobu připojení zařízení k síti (Ethernet, VPN) (Hoffman, 2008).

Jak je uvedeno na obrázku č. 8, NAC obsahuje tři komponenty: klienty NAC, zařízení pro přístup k síti (NAD) a přístupový server. Klienti NAC komunikují se NAD pro autentizaci uživatele. NAD povoluje, odmítá, izoluje nebo omezuje uživateli přístup k síti na základě nastavených politik. Přístupový server zahrnuje server řízení přístupu, server pro správu, antivirový server a server aktualizací. Přístupový server zajišťuje kontrolu dodržování bezpečnostních pravidel, provádí aktualizaci uživatelského zařízení, monitoruje akce uživatelů (Hoffman, 2008).



Obrázek 8: Diagram použití NAC

Zdroj: (Huawei, 2020)

NAC má různá řešení. Nejčastěji se používají další variace: Cisco NAC, Symantec NAC, Microsoft NAP, Juniper Networks Unified Access Control, PacketFence, OpenNAC (Hoffman, 2008).

Zobecněný proces NAC

- klient se připojí k síti. Přístupový server dostane oznámení o novém zařízení;
- přístupový server zahájí proces kontroly klienta;
- klient odešle požadovanou informaci serveru NAC;
- NAC server přeposílá doručenou informaci interním serverům a od každého dostává rozhodnutí o stavu zařízení;
- výsledky se odesílají danému zařízení. Přístupové zařízení modifikuje přístupová práva klientského zařízení podle autorizačních informací dodaných NAC serverem;
- klientské zařízení získává přístup k síti – plný, omezený nebo pouze k serveru aktualizací (Hoffman, 2008; Kenin, 2019).

NAC řešení se mohou lišit, v zásadě spadají do dvou kategorií: clientless a client-based. Client-based na rozdíl od clientless požaduje na klientském zařízení mít nainstalovaný software – NAC client (Hoffman, 2008).

3.3.1 NAP na serveru NPS

Technologie NAP představuje NAC řešení od společnosti Microsoft. NAP patří mezi client-based NAC. Technologie NAP poprvé byla realizována ve Windows XP Service Pack 3, Windows Vista a Windows Server 2008. Pomocí architektury NAP lze vytvořit zásady stavu, které definují například požadavky na software, požadavky na aktualizace zabezpečení a požadovaná nastavení konfigurace počítačů, které se připojují k síti. Pokud počítač nesplňuje nastavené zásady sítě, bude mu plný přístup odmítnut, dokud nebudou zjištěné problémy vyřešeny. Podle nastavení jsou počítače, které neprošly kontrolou, buď zcela zablokovány, nebo umístěny do karantény (například jsou jim přiděleny adresy IP z jiného rozsahu). Alternativně je možné nastavit logování takových událostí bez přijetí jakýchkoli opatření. Karanténní podsíť může obsahovat nápravné servery (remediation server) poskytující prostředky k odstranění identifikovaných problémů, například aktualizační server WSUS. Po upgradu zařízení je znovu zkontrolováno, pokud je vše v pořádku, zařízení získá přístup k síti. V nastavení je možné určit webovou stránku, která popisuje, proč se uživatel nemůže připojit a co pro to musí udělat. Kontrola stavu zařízení se provádí pravidelně po celou dobu připojení k síti (Hoffman, 2008; Kenin, 2019).

Technologie NAP je založena na architektuře klient-server. Informaci o klientském zařízení poskytuje NAP klient, který je realizován ve Windows Vista, Windows 7, Windows 8 and Windows 8.1. Windows XP Service Pack 3 obsahuje omezenou verzi NAP klient. NAP klient odesílá zprávu obsahující stav zařízení NPS serveru, kde NPS/NAP rozhoduje o přidělení nebo odepření přístupu na základě nastavených zásad stavu a poskytnuté informace o stavu koncového zařízení NAP klientem (Hoffman, 2008; Rountree, 2011).

NAP nechrání síť a nenahrazuje antivirus a firewall. NAP pro řízení a zabezpečení přístupu používá body vynucení. Body vynucení mohou být přepínače podporující IEEE 802.1x, servery VPN, servery DHCP, HRAs se systémem Windows Server 2008 nebo novějším (Hoffman, 2008; Rountree, 2011).

Body vynucení používají různé metody vynucení:

- DHCP – tento typ vynucení používá systém Windows Server, na kterém je spuštěna služba DHCP. Počítače, které splňují požadavky, získají přístup k síti, zatímco počítače, které nejsou kompatibilní, mohou být přesměrovány na nápravné servery nebo jim může být odepřen přístup k síti. Tuto metodu lze obejít pomocí statické IP adresy.

Kontrola klientského zařízení se provádí pokaždé po vypršení doby zapůjčení IP adresy (Hoffman, 2008; Rountree, 2011).

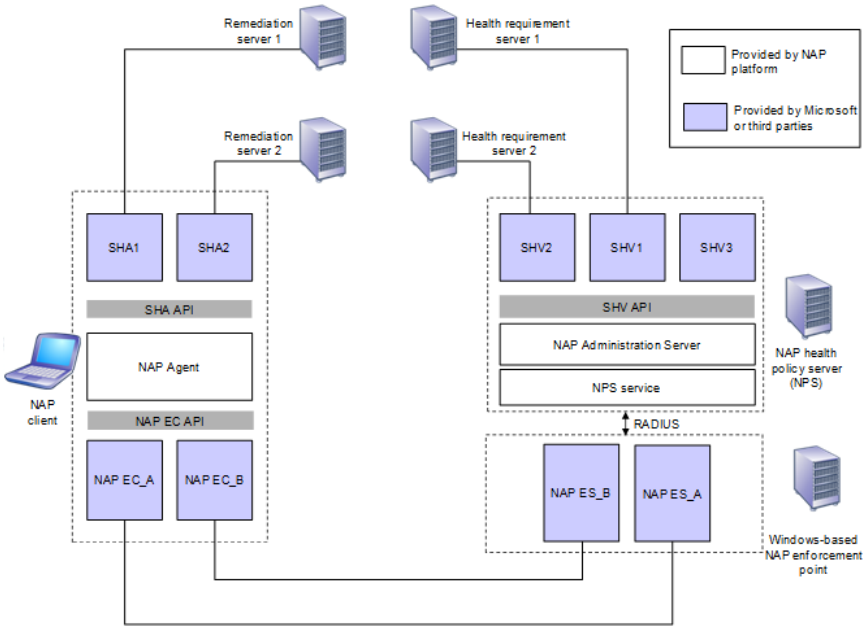
- IPsec – vynucení typu NAP IPsec poskytuje nejsilnější a nejflexibilnější metodu ze všech. Vyžaduje PKI, k ověření se používají pouze certifikáty. Vyžaduje další roli v síti – HRA, která poskytuje zabezpečení IPsec (Hoffman, 2008; Kenin, 2019).
- IEEE 802.1x – tento typ vynucení NAP využívá k ověřování počítačů pomocí přepínačů a přístupových bodů kompatibilních s 802.1x. Server, na kterém je spuštěna služba NPS, zkontroluje každý počítač před jeho ověřením a pokud stav není kompatibilní se zásadami sítě, bude počítač přesměrován do sítě pro nápravu. Může být použit v kombinaci s DHCP nebo IPsec (Hoffman, 2008; Rountree, 2011).
- TS-Gateway (Terminal Services Gateway) – tento způsob vynucení umožňuje omezit přístup klientů TS-Gateway k síti. TS-Gateway poskytuje bezpečný přístup k vnitřním zdrojům sítě autentizovaným uživatelům přes internet. TS-Gateway pro připojení uživatelů k vnitřní síti používá protokol RDP (Hoffman, 2008; Kenin, 2019).
- VPN – tento typ vynucení ověří každého vzdáleného klienta, který se pokusí autentizovat v síti pomocí VPN. Technologie VPN slouží pro vzdálené připojení do firemní sítě. Metoda vynucení VPN podporuje EAP metody pro zabezpečení autentizace (Hoffman, 2008; Rountree, 2011).

Jedním z úkolů správce sítě při nasazení NAP spočívá ve výběru vlastní metody vynucení.

NAP architektura

Celková architektura NAP se skládá z následujících komponent:

- tři komponenty klienta NAP (vrstva SHA, agent NAP a vrstva EC NAP);
- čtyři komponenty na straně serveru NAP (vrstva SHV, NAP Administration Server, služba NPS a vrstva NAP ES na vynucovacích bodech);
- servery zásad stavu, což jsou počítače, které mohou poskytnout aktuální požadavky na konfiguraci klientských počítačů;
- nápravné servery, což jsou počítače, které obsahují prostředky aktualizace stavu, ke kterým mají klienti NAP přístup k nápravě jejich nekompatibilního stavu (Microsoft, 2018).



Obrázek 9: Komponenty NAP architektury

Zdroj: (Microsoft, 2018)

Jak je uvedeno na obrázku č. 9 architektura NAP klienta se skládá z následujících komponent:

- Vrstva Enforcement Client (EC) komponentů

EC poskytuje přístup k síti na základě stavu systému. Vrstva EC obsahuje různé komponenty pro různé způsoby připojení k síti. Například NAP EC pro DHCP, NAP EC pro vzdálené připojení přes VPN (Microsoft, 2018).

- Vrstva System Health Agent (SHA) komponentů

SHA komponenta odpovídá za ověření splnění nastavených bezpečnostních podmínek klienta NAP. Na klientském NAP může současně pracovat několik takových agentů. Například může existovat SHA pro antivirový program a SHA pro aktualizace operačního systému. K informování o stavu konkrétní SHA komponenta vytvoří stavovou zprávu SoH a předá ji agentovi NAP. Například SHA pro antivirový program může vytvořit SoH obsahující stav antivirového softwaru spuštěného v počítači, jeho verzi a poslední obdrženou aktualizaci. SoH obsahuje informace, které může server zásad NAP použít k ověření, zda je klientský počítač v požadovaném stavu. Kdykoli SHA aktualizuje svůj stav, vytvoří novou zprávu SoH a předá ji agentovi NAP. K označení celkového stavu klienta NAP používá agent NAP zprávu SSoH. Každá SHA komponenta je přiřazena k System Health Validator (SHV) na straně serveru. Odpovídající SHV může vrátit odpověď SoHR klientovi NAP, který je předán odpovídající SHA

komponente a informuje ji o tom, co dělat, pokud není SHA v požadovaném stavu (Microsoft, 2018).

- NAP Agent

Obsahuje aktuální informace stavu klienta NAP a usnadňuje komunikaci mezi vrstvami EC a SHA NAP (Microsoft, 2018).

- System Health Agent API

SHA API umožňuje vytvářet a instalovat další SHA komponenty (Microsoft, 2018).

Architektura NAP na straně serveru je také uvedena na obrázku č. 9 a je následující**:**

- Vrstva NAP Enforcement Server

Každý NAP ES je definován pro různé typy přístupu k síti nebo komunikaci. NAP ES je obvykle přiřazen ke konkrétnímu typu NAP EC. Například DHCP NAP EC na klientovi NAP je přiřazen DHCP NAP ES na serveru DHCP (Microsoft, 2018).

- NPS

Dostává zprávu RADIUS Access-Request, extrahuje SSoH a předá ji komponentě NAP Administration Server (Microsoft, 2018).

- NAP Administration Server

Usnadňuje komunikaci mezi vrstvami NPS a SHVs (Microsoft, 2018).

- Vrstva SHV komponent

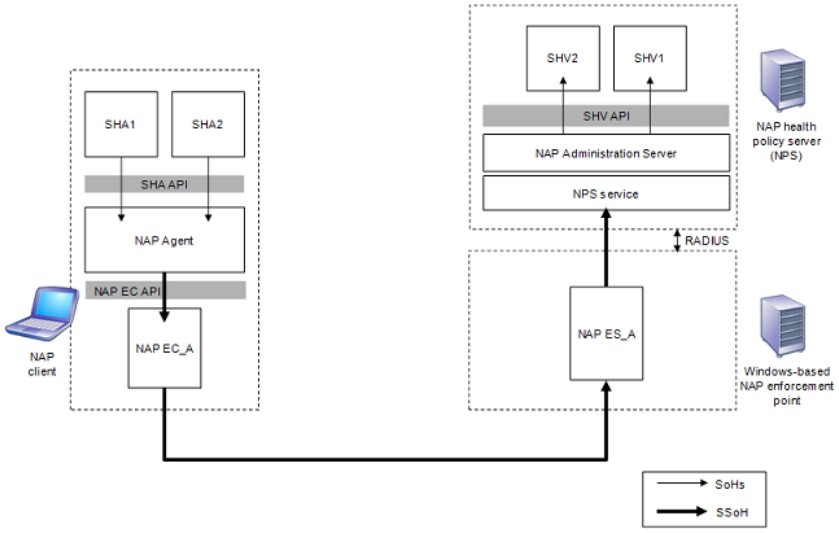
Každý SHV je definován pro jeden nebo více typů informací o stavu systému a může být přiřazen k SHA. SHV přijímá SoH od NAP Administration Server a porovnává informace o stavu systému s požadovaným stavem. Pokud například SoH pochází od komponenty SHA pro antivirový program, může příslušný antivirový SHV zkontrolovat u serveru zásad stavu požadovanou verzi antiviru, aby ověřil SoH klienta NAP. SHV vrátí SoHR serveru NAP Administration Server. SoHR může obsahovat informace o tom, jak může odpovídající SHA na klientovi NAP splnit aktuální požadavky zásad stavu systému (Microsoft, 2018).

- SHV API

Poskytuje sadu funkcí, které umožňují SHV se zaregistrovat u NAP Administration Server, přijímat zprávy SoH ze komponenty NAP Administration Server a odesílat zprávy SoHR komponentě NAP Administration Server (Microsoft, 2018).

Komunikace v NAP architektuře

Na obrázku č. 10 je uveden proces komunikace v NAP architektuře mezi klientskými komponentami NAP a komponentami na straně serveru.



Obrázek 10: NAP – komunikace mezi komponentami

Zdroj: (Microsoft, 2018).

Komponenta NAP Agent může komunikovat s komponentou NAP Administration Server prostřednictvím následujícího procesu:

- agent NAP předá zprávu SSoH NAP EC;
- NAP EC předá zprávu SSoH NAP ES;
- NAP ES předá zprávu SSoH službě Network Policy Server;
- služba NPS předá zprávu SSoH NAP Administration serveru. (Microsoft, 2018).

SHA může komunikovat se svým odpovídajícím SHV pomocí následujícího procesu:

- SHA předá zprávu SoH agentovi NAP;
- agent NAP předává zprávu SoH, jako součást zprávy SSoH, do NAP EC;
- NAP EC předává zprávu SoH do NAP ES;
- NAP ES předá zprávu SoH serveru NAP Administration Server;
- NAP Administration Server předává zprávu SoH do SHV. (Microsoft, 2018).

NAP Administration server může komunikovat s agentem NAP pomocí následujícího procesu:

- NAP Administration server předává SoHRs službě NPS;
- služba NPS předá SSoHR NAP ES;
- NAP ES předá SSoHR EC NAP;
- NAP EC předá SSoHR agentovi NAP (Microsoft, 2018).

SHV může komunikovat s odpovídající SHA pomocí následujícího procesu:

- SHV předává svůj SoHR serveru NAP Administration Server;
- server pro správu NAP předává SoHR službě NPS;
- služba NPS předává zprávu SoHR, jako součást SSoHR do NAP ES;
- NAP ES předává SoHR NAP EC;
- NAP EC předá SoHR agentovi NAP;
- agent NAP předává zprávu SoHR SHA (Microsoft, 2018).

NPS

NPS je implementován jako role serveru v systému Windows Server 2012 a novějších verzích. Při instalaci role NPS je třeba rozhodnout, zda použít NPS jako server RADIUS, proxy RADIUS nebo server zásad NAP. Po instalaci je možné použít NPS Management Console nebo Windows PowerShell ke konfiguraci NPS (Hoffman, 2008; Blokdyk, 2018).

Ve Windows Server 2012 R2 NPS je možné používat v kombinaci následujících funkcí:

- RADIUS server – provádí autentizaci, autorizaci a účtování uživatelů. NPS je implementací RADIUS serveru společnosti Microsoft, zlepšená varianta IAS, která se používala do Windows Server 2008. Pokud je server NPS členem domény Active Directory Domain Services (AD DS), NPS používá službu AD DS jako databázi uživatelských účtů a poskytuje jednotné přihlášení (single sign-on), což umožní použít jedno přihlášení do více aplikací zároveň. Při použití NPS jako RADIUS server je možné přidávat přístupové body, přepínače a jiná zařízení jako klienty RADIUS serveru (Hoffman, 2008; Blokdyk, 2018).
- RADIUS Proxy – provádí přesměrování požadavků na připojení jiným RADIUS serverům (Hoffman, 2008; Blokdyk, 2018).
- Server zásad NAP – slouží k vyhodnocení zpráv SoH odeslaných NAP klientem počítačů, které se pokoušejí připojit k síti. NPS funguje také jako server RADIUS, když je nakonfigurován jako NAP, provádí ověřování a autorizaci požadavků na připojení.

Pomocí NAP je možné nastavit zásady NAP, včetně SHV, nápravné servery, které umožní klientským počítačům aktualizovat jejich konfiguraci tak, aby byla v souladu se síťovými zásadami organizace (Hoffman, 2008; Blokdyk, 2019).

Nastavení připojení pomocí NPS/NAP a protokolu 802.1x

Při nasazení architektury NAP pro protokol 802.1x je nutné provést následující konfiguraci:

- Nakonfigurovat zásady vyžádání nového připojení, zásady sítě a zásady stavu NAP architektury na serveru NPS (Microsoft, 2018).

- Nakonfigurovat protokol 802.1x na ověřovacím přepínači (Microsoft, 2018).

- U klientských počítačů s podporou klienta NAP povolit klienta vynucení architektury NAP pro protokol EAP, spustit službu NAP a Wired AutoConfig (Microsoft, 2018).

- Nakonfigurovat validátor stavu zabezpečení systému Windows (WSHV) nebo nainstalovat a nakonfigurovat jiné agenty stavu systému (SHA) a validátory stavu systému (SHV) (Microsoft, 2008).

- V případě použití PEAP-TLS nebo EAP-TLS s čipovými kartami nebo certifikáty, nasadit infrastrukturu veřejných klíčů (PKI) se službou AD CS (Microsoft, 2018).

- V případě použití PEAP-MSCHAPv2, vydat pomocí služby AD CS certifikáty serveru nebo pořídit certifikáty serveru od jiné důvěryhodné kořenové certifikační autority (Microsoft, 2018).

3.3.2 NAC řešení jiných výrobců

PacketFence

PacketFence je plně podporovaný, bezplatný a open source network access control system. PacketFence patří mezi clientless NAC a obsahuje velký počet různých modulů. Nejčastěji se používají další: databázový server (MySQL nebo MariaDB), web server Apache, DHCP server (ISC DHCP), RADIUS server (FreeRADIUS), DNS server (Bind) (Packetfence, 2014).

PacketFence podporuje rozsáhlý počet funkcionalit:

- drátová a bezdrátová autentizace pomocí protokolu 802.1x za přítomnosti Free-RADIUS;
- internetová telefonie (VoIP);
- detekce podivných aktivit (počítačové viry, červy, trojské koně apod.) pomocí skeneru Snort, Suricata;
- kontrola připojených zařízení pomocí protokolu TNC Statement of Health (nastavení firewallu, verze OS apod.);
- izolace problematických zařízení;
- captive portal (webová autentizace) (Packetfence, 2014)

PacketFence nabízí tři způsoby správy sítě:

- out of band (VLAN Enforcement) - je jedním z nejpoužívanějších způsobů správy, vyžaduje spravovatelné síťové prvky;
- in band (Inline Enforcement) - PacketFence funguje jako síťová brána, umožňuje spravovat starší zařízení. Veškerý provoz probíhá přes PacketFence, nevhodné řešení pro velké sítě;
- hybrid support (Inline Enforcement with RADIUS support) -je podobné in-band, ale na rozdíl od in-band podporuje RADIUS, což umožňuje použít 802.1x a MAC autentizaci (Packetfence, 2014).

Cisco NAC

Technologie Cisco NAC slouží k zesílení bezpečností síťové infrastruktury a patří mezi client-based NAC. Pomocí Cisco NAC je možné řídit přístup koncových zařízení. V případě, že zařízení nesplňuje podmínky bezpečnostní politiky, bude mu odepřen přístup a dané zařízení bude umístěno do karantény nebo bude poskytnut omezený přístup k informačním zdrojům. Cisco NAC používá infrastrukturu síti pro kontrolu dodržování bezpečnostní politiky jednotlivými zařízení a podporuje standard 802.1x, což například umožňuje provádět kontrolu uživatelů při připojení k bezdrátovým bodům (Afanasjev, 2012).

Cisco NAC umožňuje zabezpečit vzdálený přístup k síti. Předtím, než vzdálený uživatel dostane přístup k síti za použití protokolu IPsec nebo jiného, bude provedena kontrola daného zařízení podle nastavených bezpečnostních pravidel (Afanasjev, 2012).

Důležité komponenty Cisco NAC

- Cisco trust agent – programové vybavení, umístěné na koncových zařízeních. Trust agent sbírá informaci o stavu zabezpečení zařízení a předává ji NAD (Afanasjev, 2012).

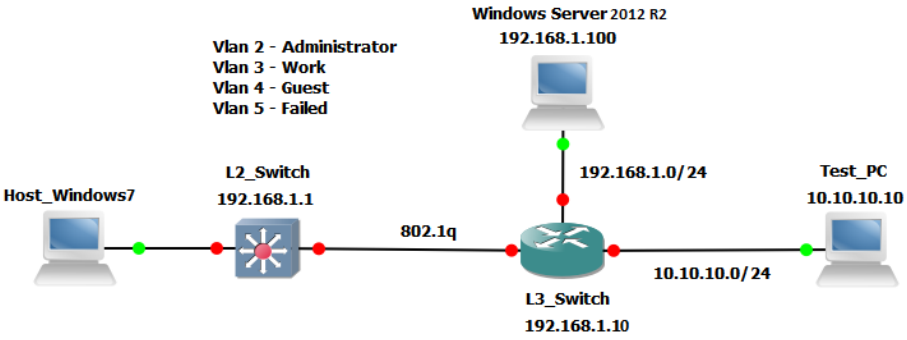
- NAD – slouží ke kontrole přístupů koncových zařízení. V roli NAD může být směrovač, přepínač a jiná zařízení. NAD předává informaci od koncových zařízení na server politiky, který rozhoduje o povolení či odepření přístupu zařízení k síti (Afanasjev, 2012).
- Policy server – hodnotí úroveň bezpečnosti koncových zařízení na základě informace od NAD a rozhoduje o přidělení či odepření přístupu (Afanasjev, 2012).
- Management system – CiscoWorks VPN/Security Management Solution (VMS) řídí elementy Cisco NAC, CiscoWorks Security Information Management Solution (SIMS) nabízí nástroje pro monitorování (Afanasjev, 2012).

4 Praktická část

V dané části je vytvořena testovací topologie pro konfiguraci a testování NAP a metody vynucení prostřednictvím port-based 802.1x přes drátové připojení za použití Windows Server 2012 R2 (Evaluation). Roli RADIUS serveru a serveru politik NAP hraje služba NPS. Windows Server je spuštěn ve VMware Workstation 15 Player. Simulace počítačové sítě je realizována ve virtuálním prostředí GNS3 verze 1.5 za použití emulátoru Dynamips.

4.1 Síťová topologie

Síťová topologie je uvedena na obrázku č. 11. Síť se skládá ze dvou síťových zařízení: L2 a L3 přepínače. L3_Switch zajišťuje směrování VLAN, každé síti VLAN odpovídá určitý rozsah IP adres. K zařízení L3_Switch je připojen Test_PC (Virtual PC Simulator) a Windows Server 2012 R2. Na Windows Serveru jsou nastaveny všechny potřebné služby: AD DS, DHCP, AD CS, DNS, NAP a IIS. Také byla vytvořena kořenová doména *mva.com* s 1 doménovým řadičem (v praxi Microsoft doporučuje vždy mít alespoň 1 záložní řadič). Z důvodu omezenosti hardwarových prostředků nastavení všech služeb bylo provedeno na jedné stanici, což v praxi může být nevhodným řešením. Lepším způsobem je rozdělit kritické služby (například NPS a AD).



Obrázek 11: Topologie sítě

Zdroj: Vlastní

Zařízení L2_Switch slouží k připojení koncových zařízení a vystupuje v roli autentizátoru. V dané implementaci k L2_Switch je připojen počítač se systémem Windows 7 – Host_Windows7. Host_Windows7 hraje roli suplikanta. Test_PC slouží jako testovací zařízení, které by měl Host_Windows7 při splnění zásad sítě úspěšné pinknout. Autentizace koncových zařízení je zajištěna pomocí PEAP (MSCHAPv2). Na základě výsledků autentizace uživatele port L2_Switch bude přiřazen do určité VLANy.

VLANy, které je potřeba nastavit:

- VLAN 2 (Administrator) – rozsah IP adres je 192.168.1.0/24. Všechna síťová zařízení a Windows Server se nachází v dané VLAN. Administrátorovi sítě po úspěšné autentizaci je přidělena tato síť VLAN.
- VLAN 3 (Work) – rozsah IP adres je 192.168.2.0/24. VLAN 3 je určena pro pracovníky firmy;
- VLAN 4 (Guest) – rozsah IP adres je 192.168.3.0/24. VLAN 4 je určena pro návštěvníky firmy;
- VLAN 5 (Failed) – rozsah IP adres je 192.168.4.0/24. VLAN 5 je určena pro zařízení, která mají jakékoliv potíže s autentizaci. Uživatelé této sítě VLAN mohou pingovat jenom svoji implicitní bránu (192.168.4.1) a dostávat IP adresu od služby DHCP.
- VLAN 6 (Test) - rozsah IP adres je 10.10.10.0/24. VLAN 6 je určena pro testování Test_PC patří do této VLANy.

4.2 Konfigurace Windows Server 2012 R2

Na začátku je potřeba provést instalaci všech potřebných rolí a nainstalované role nakonfigurovat.

4.2.1 Instalace rolí

Ve Windows Server role – je to sada programů, které umožňují počítači vykonávat určitou funkci pro uživatele nebo jiné počítače v síti. Role, které je potřebovat nainstalovat:

- AD DS – slouží k ukládání uživatelských údajů;
- DNS – slouží k překladu názvů domén na adresy IP a naopak;
- AD CS – umožňuje instalovat a konfigurovat kořenové (root) nebo podřízené (subordinate) certifikační autority, které se používají k vydávání certifikátů uživatelům, počítačům a službám. Důležitým komponentem CS je Web Enrollment, který se používá pro vyžádání certifikátů a získání informací o zneplatnění certifikátu prostřednictvím webového prohlížeče;
- IIS – webový server, který umožňuje snadno požádat o certifikát přes webový prohlížeč;
- NPAS – RADIUS server a server zásad NAP (Microsoft, 2008).

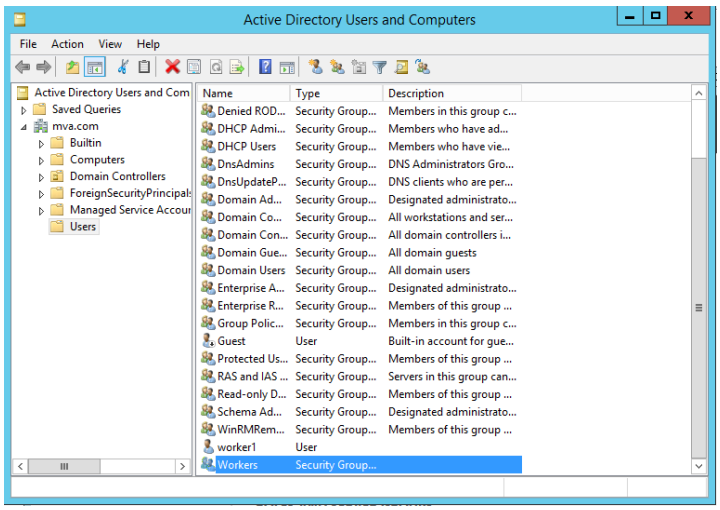
Pro přidání nových rolí ve Windows Server 2012 R2 je třeba spustit *Add Roles and Features* kliknutím na tlačítko *Add Roles* v *Start > Administrative Tools > Server Man-*

ager. V dialogovém okně je třeba vybrat potřebnou roli a provést její instalaci. Všechny nainstalované role se objeví v Server Manageru (Tools) (Microsoft, 2008). Proces instalace rolí ve Windows Server je docela jednoduchý a postup je přibližně stejný, proto podrobná instalace se nebude rozebírat.

4.2.2 Konfigurace rolí

Active Directory

Pro zajištění přiřazení portu, přes který je uživatel připojen do správné VLANy je třeba vytvořit skupiny a členy těchto skupin. Skupiny souvisí s VLANami (viz. Tabulka č. 2). Vytvoření skupin a uživatelů se provádí kliknutím na *Start* > *Administrative Tools* > *Active Directory Users and Computers*. V otevřeném dialogovém okně je třeba rozkliknout *Active Directory Users and Computers* > *Domain name* > *Users* a kliknutím pravým tlačítkem myši na prázdné místo vybrat *New* > *Group* (nebo *User* pro vytvoření uživatele) (Microsoft, 2008).



Obrázek 12: Vytvoření skupin a uživatelů v AD

Zdroj: Vlastní

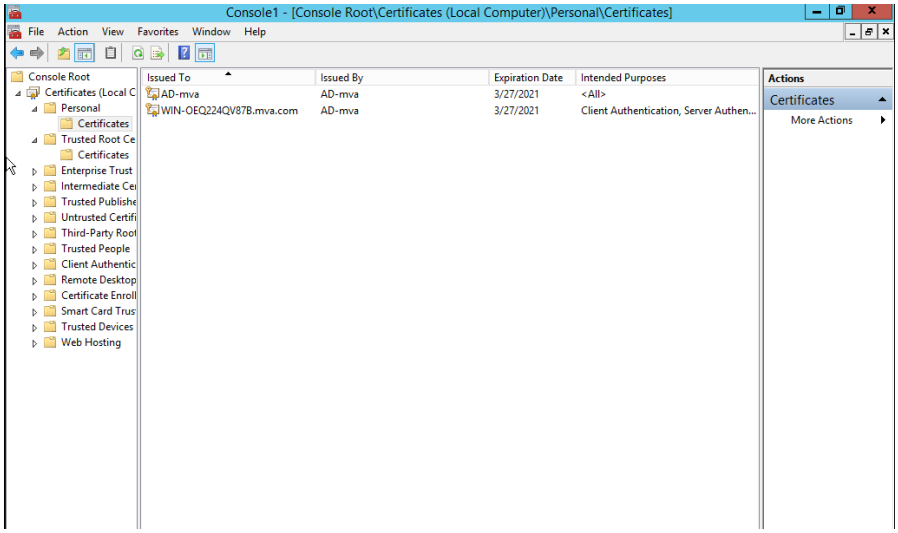
Pro daný případ byly vytvořeny následující globální skupiny: GuestUsers, Workers, a Admins (viz. Obrázek 12). Po vytvoření skupin je třeba vytvořit a přidat uživatele pro dané skupiny. Přidání uživatelů do skupin se provádí kliknutím na vybraného uživatele pravým tlačítkem myši a výběrem *Properties* > *Member of* > *Add*. V otevřeném dialogovém okně je třeba do textového pole zadat správný název skupiny, do které vybraný uživatel bude přidán. Skupiny a jejich členy jsou vytvořeny a tím pádem AD je nastaven (Microsoft, 2008).

Vytvoření žádosti o certifikát

Server RADIUS musí uživatelům předložit certifikát, aby uživatele si mohli ověřit, zda komunikují se správným RADIUS serverem Je důležité, aby klient přijímal pouze platné

certifikáty, což pomůže zabránit spoofing útokům, kdy útočník může spustit falešný server RADIUS. PEAP vyžaduje pouze certifikát RADIUS serveru. V případě použití metody EAP-TLS navíc se vyžaduje klientský certifikát pro každého uživatele, který se chce připojit k síti. Vytvoření certifikátu zajišťuje certifikační autorita.

Pro vygenerování certifikátu ve Windows Server je třeba spustit službu *mmc* a v otevřeném okně kliknout na *File* > *Add/Remove Snap-in* a vybrat položku *Certificates* z *Available snap-ins* a kliknout *Add*. Dále vybrat *Computer account* a *Local Computer*. Na pravé straně by se měl zobrazit úspěšně přidaný modul snap-in a v levém menu služby *mmc se* objeví modul *Certificates*, kde by se měly po otevření složky *Personal* > *Certificates* zobrazit certifikáty počítače (viz. Obrázek 13). Pokud certifikát se nevygeneroval, tak je třeba kliknutím na *All Tasks* > *Request New Certificate* vytvořit nový certifikát. Vygenerovaný PK se zobrazí po otevření složky *Certificate Enrollment Requests* (Microsoft, 2008; Molenaar, 2013).



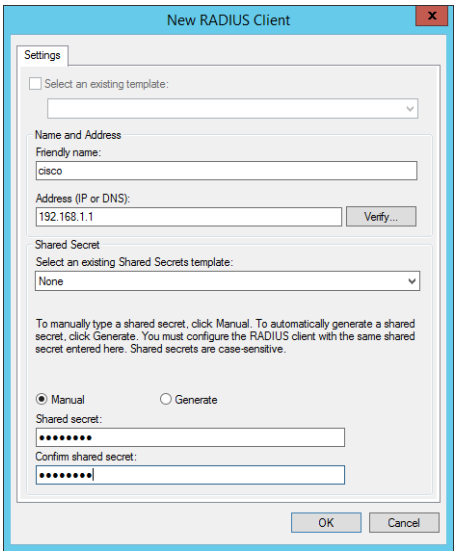
Obrázek 13: Certifikáty RADIUS serveru

Zdroj: Vlastní

Server má nyní certifikát, který může být poskytnut klientům, když požádají o identifikaci serveru RADIUS. Certifikát je nutné importovat na zařízení uživatele. Jedním ze způsobů je otevřít v *mmc* složku *Certificates (Local Computer)* > *Trusted Root Certification Authorities* > *Certificates***.** Na pravé straně se objeví kořenový CA. Kliknutím pravým tlačítkem myši certifikát exportovat ve formáte X.509 bez privátního klíče. Exportovaný certifikát je třeba přesunout na uživatelské zařízení pomocí USB flash disku. Po přesunutí certifikátu na uživatelské zařízení je třeba provést jeho instalaci. Při instalaci certifikátu jako úložiště musí být vybrána složka *Trusted Root Certification Authorities*. Nastavení je dokončeno a uživatelský počítač by teď měl důvěřovat certifikátu RADIUS serveru (Microsoft, 2008; Molenaar, 2013).

NPS

NPS hraje roli RADIUS serveru a serveru zásad NAP. Nejdřív je nutné zaregistrovat NPS v AD. Pro otevření NPS je třeba vybrat *Start* > *Administrative Tools* > *Network Policy Server* a kliknutím na *NPS* > *Register server in Active Directory* bude provedena registrace NPS v AD (Microsoft, 2008; Molenaar, 2013).



Obrázek 14: Nastavení klienta RADIUS serveru

Zdroj: Vlastní

Aby server věděl, se kterými zařízeními naváže komunikaci, je nutné přidat autentizátor do klientů RADIUS serveru. RADIUS klienta přidáme kliknutím na *NPS* > *RADIUS Clients and Servers* > *RADIUS Clients* > *New*. V otevřeném dialogovém okně se požaduje vyplnit potřebné údaje (viz. Obrázek 14). *Friendly name* je označení RADIUS klienta, kterým ho rozpoznáte od ostatních klientů. Vybral jsem jméno *Cisco*, IP-adresa klienta v mém případě je 192.168.1.1. Aby se zařízení mohlo přihlásit k serveru, je nutné zadat sdílený klíč. Sdílený klíč se vytváří na serveru buď ručně, nebo se generuje automaticky. Preferoval jsem první možnost. Po přidání RADIUS klienta se musí vytvořit zásady vyžádání nového připojení, zásady stavu klienta a zásady sítě, které umožňují určit uživatele, kteří mají povoleno nebo zakázáno připojení k síti. Zásady vyžádání nového připojení se vytváří kliknutím na *Connection request policies* > *New*. Pro tento případ byla vytvořena zásada *NAP 802.1x (Wired)* a podmínka *NAS IPv4 Address*, což je 192.168.1.1. Zásady stavu klienta se vytváří kliknutím na *Health Policies* > *New*, kde je nutné zadat název, vybrat *SHVs*, které budou použity a jejich kritérium. Pro nastavení *WSHV* (SHV ve Windows) je třeba kliknout na *Network Access Protection* > *System Health Validators* > *Windows Security Health Validator* > *Settings* a vytvořit potřebné nastavení. V daném scénáři WSHV bude vyžadovat pouze zapnutý firewall (Microsoft, 2008; Molenaar, 2013). Nastavené zásady stavu klientského zařízení jsou uvedeny v tabulce č. 1.

Název politiky	Kritérium SHV	SHV		
		Název	Nastavení	
			Název	Kritérium
NAP 802.1x Compliant	Client passes all SHV checks	WSHV	Default Configuration	Zapnutý firewall
NAP 802.1x Non-Compliant	Client fails on or more SHV checks	WSHV	Default Configuration	Zapnutý firewall

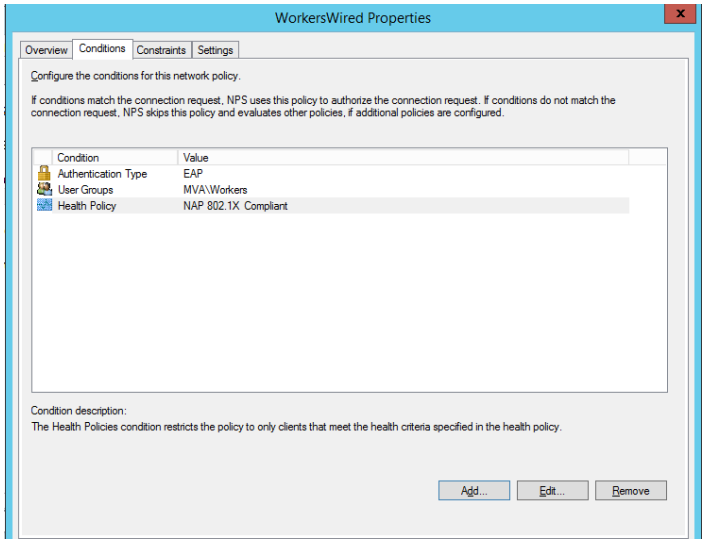
Tabulka 1: Hodnoty pro nastavení zásad stavu klientského zařízení

Zdroj: Vlastní

Politiky sítě se vytváří kliknutím na *Policies* > *Network Policies* > *New*. Politiky, které je potřeba vytvořit:

- Guests Wired;
- Workers Wired;
- Admins Wired;
- Failed Wired.

Dále je nutné specifikovat potřebné podmínky, které jsou nutné, aby klient odpovídal dané politice. (viz. Obrázek 15).



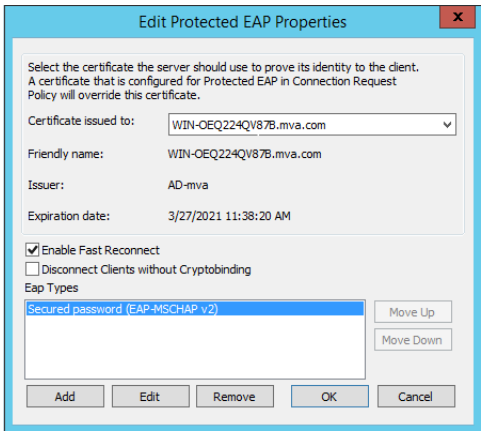
Obrázek 15: Nastavení politiky v NPS

Zdroj: Vlastní

Byly vybrány následující podmínky:

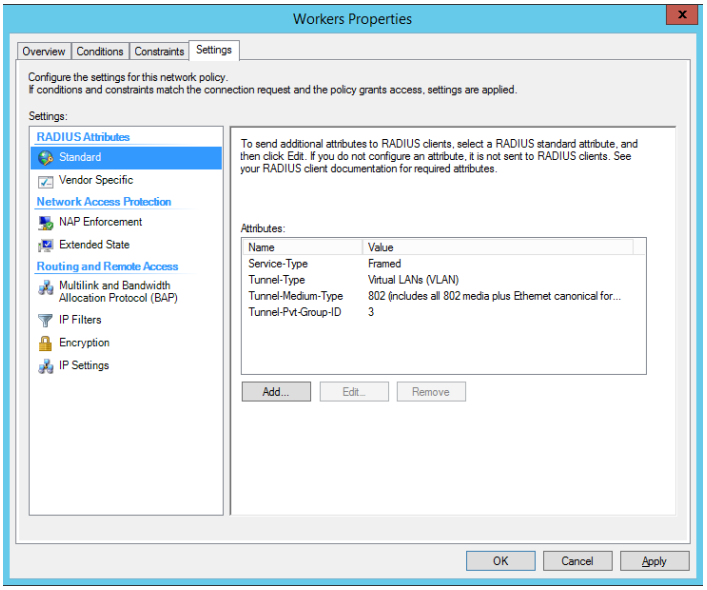
- Authentication Type: EAP;
- User Groups: MVA\Workers;
- Health Policy.

Při splnění nastavených podmínek připojení může být povoleno nebo zakázáno. V daném případě při splnění nastavených podmínek uživatelskému zařízení bude přístup povolen. Způsob autentizace, který byl vybrán je PEAP (EAP-MSCHAPv2) a také byl vybrán certifikát, který slouží k ověřování RADIUS serveru ze strany klienta (viz Obrázek 16).



Obrázek 16: Nastavení vlastností PEAP

Zdroj: Vlastní



Obrázek 17: Nastavení atributů RADIUS serveru

Zdroj: Vlastní

Dále je třeba nastavit atributy RADIUS serveru, které budou odeslány autentizátoru RADIUS serverem po úspěšné autentizace uživatelského zařízení. Atributy RADIUS serveru, které je potřeba nastavit (viz. Obrázek 17):

- Service-Type: Framed;
- Tunnel-Type: VLAN;
- Tunnel-Medium-Type: 802;

- Tunnel-PVT-Group-ID: <VLAN Number>.

Také v položce *NAP Enforcement* je třeba nastavit typ přístupu k síti a *Auto remediation*, což umožní provést automatickou nápravu zařízení klienta (Microsoft, 2008). Stejným způsobem musí být vytvořeny ostatní 3 politiky (Guests Wired, Administrator Wired a Failed Wired). Hodnoty pro nastavení potřebných politik jsou uvedeny v tabulce č. 2.

Název politiky	Typ autentizace	Skupiny uživatelů	Zásady stavu	Atributy RADIUS Serveru				NAP Enforcement	
				Service-Type	Tunnel-Type	Tunnel-Medium-Type	Tunnel-PVT-Group-ID	Access Type	Auto remediation
Guests Wired	EAP	GuestUsers	NAP 802.1x Compliant	Framed	VLAN	802	4	full	-
Workers Wired	EAP	Workers	NAP 802.1x Compliant	Framed	VLAN	802	3	full	-
Admins Wired	EAP	Admins	NAP 802.1x Compliant	Framed	VLAN	802	2	full	-
Failed Wired	EAP		NAP 802.1x NonCompliant	Framed	VLAN	802	5	limited	+

Tabulka 2: Hodnoty pro nastavení politik v NPS

Zdroj: Vlastní

DHCP

Po úspěšné autentizace uživatel musí automaticky dostat IP adresu pomocí služby DHCP. Pro každý VLAN je nutné nastavit rozsah IP adres, které budou přiřazeny uživatelům. Pro otevření DHCP je třeba přejít do *Start > Administrative Tools > DHCP*. Pro přidání nového rozsahu IP adres vybrat *DHCP > Domain name > IPv4 > New Scope.* V otevřeném dialogovém okně je třeba vyplnit potřebné údaje jako je maska sítě a implicitní brána (Molenaar, 2013). Všechny rozsahy IP adres, které byly nastaveny, jsou uvedeny v tabulce č. 3.

Název rozsahu	Počáteční adresa IP	Koncová adresa IP	Maska sítě	Implicitní brána	Doba zapůjčení (dny)
Admins_VLAN2	192.168.1.11	192.168.1.99	255.255.255.0	192.168.1.10	8
Workers_VLAN3	192.168.2.11	192.168.2.99	255.255.255.0	192.168.2.1	8
Guests_VLAN4	192.168.3.11	192.168.3.99	255.255.255.0	192.168.3.1	8
FaileddUsers_VLAN5	192.168.4.11	192.168.4.99	255.255.255.0	192.168.4.1	8

Tabulka 3: Hodnoty pro nastavení rozsahů IP adres

Zdroj: Vlastní

4.3 Konfigurace 802.1x

Na zařízení L2_Switch je nutné nastavit 802.1x. L2_Switch bude udržovat port v neautorizovaném stavu, dokud nebude autentizace úspěšná. Nastavení zařízení se provádí následujícím způsobem:

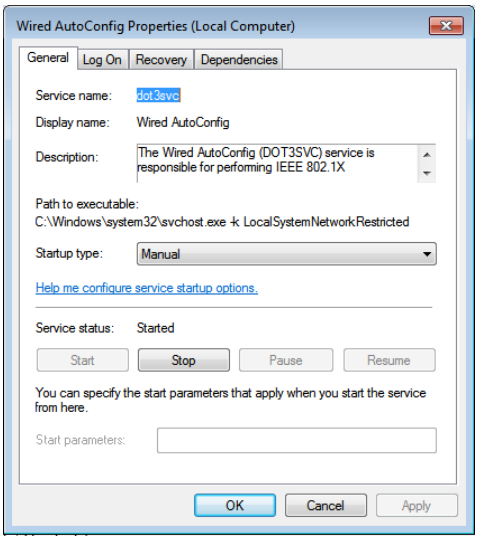
- L2_Switch(config)#aaa new-model – aktivace AAA;
- L2_Switch(config)#aaa authentication dot1x default group radius – nastavení použití protokolu RADIUS při autentizaci pomocí 802.1x na všech rozhraních;
- L2_Switch(config)#aaa authorization network default group radius – nastavení použití RADIUS při autorizaci;
- L2_Switch(config)#ip radius source-interface vlan 2 – nastavení rozhraní, ze kterého se bude posílat informace na RADIUS server;
- L2_Switch(config)#radius-server host 192.168.1.100 auth-port 1812 acct-port 1813 – nastavení IP adresy, portu autentizace a účtování RADIUS serveru;
- L2_Switch(config)#radius-server key *KEY* – nastavení server key, který bude použit při autentizaci RADIUS klienta;
- L2_Switch(config)#dot1x system-auth-control – aktivace 802.1x na přepínači;
- L2_Switch(config)#int fa 0/1 – přechod do rozhraní, kde bude nastaven 802.1x;
- L2_Switch(config-if) #dot1x port-control auto – nastavení stavu rozhraní na auto, stav rozhraní bude určen podle výsledku autentizace;
- L2_Switch(config) #dot1x reauthentication – aktivace opakované autentizace;
- L2_Switch#show dot1x – zobrazení informace;
- L2_Switch#test aaa group radius client password legacy – testování autentizace klienta (Sheshko, 2013).

  Ostatní nastavení L2_Switch a L3_Switch jsou uvedeny v příloze č. 2.

4.4 Konfigurace uživatelského zařízení

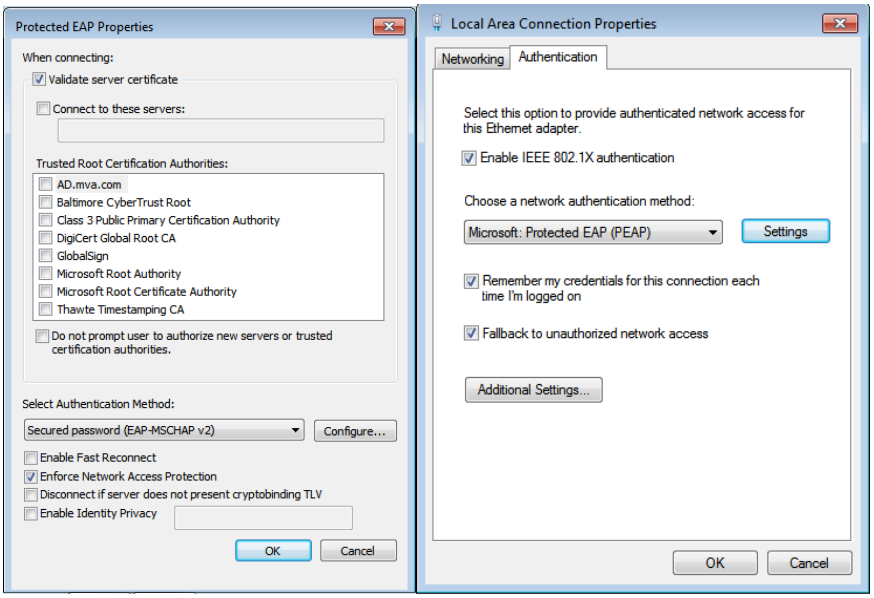
Pro zapnutí autentizace pomocí 802.1x v OS Windows 7 je potřeba otevřít *Services* a spustit službu *Wired AutoConfig*, v sekci *Startup type* vybrat možnost *Automatic,* jestli služba není spuštěna. (viz. Obrázek 18). Stejným způsobem spustit službu *Network Access Protection Agent*. Také je potřeba ve službě *mmc* přidat snap-in *NAP Client Configuration (Local Computer)* a vybrat metodu vynucení *EAP Quarantine Enforcement Client.* Dále je třeba nastavit parametry rozhraní, přes které bude probíhat autentizace: v *Network Connections* najít potřebné rozhraní a vybrat *Properties > Authentication > Enable IEEE 802.1x* (viz. Obrázek 19 b). Způsob autentizace je PEAP (EAP-MSCHAPv2). Při nastavení PEAP je třeba označit *Validate server certificate*, což umožní provést kontrolu certifikátu

RADIUS serveru a vybrat *Enforce Network Access Protection*. V seznamu *Trusted Roots Certification Authorities* by měl byt certifikát RADIUS serveru, který již byl importován (viz. Obrázek 19 a). V *Configure* je třeba zrušit autentizaci pomocí *Windows username/password* (Microsoft, 2008; Molenaar, 2013).



Obrázek 18: Nastavení vlastností služby Wired AutoConfig

Zdroj: Vlastní



(a) Vlastnosti PEAP (b) Vlastnosti rozhraní Ethernet

Obrázek 19: Konfigurace rozhraní Ethernet

Zdroj: Vlastní

4.5 Vyhodnocení testování připojení

Při testování se nejdřív prováděla analýza provozu sítě pomocí Wireshark. Pro přihlášení byl použit uživatel *worker1@mva.com*, který je členem skupiny *workers*. Na obrázcích číslo 22 a 23 je vidět komunikaci mezi suplikantem, autentizátorem a RADIUS serverem. Suplikant dostal od autentizátoru zprávu EAP Request a zprávou EAP Response odeslal své autentizační údaje. Při analýze zprávy EAP Response je vidět, že pro přihlášení bylo použito uživatelské jméno *worker1@mva.com*. Autentizační údaje uživatele byly úspěšně ověřeny RADIUS serverem a byla odeslána zpráva RADIUS Access-Accept, která obsahuje nastavené atributy (viz. Obrázek 22). Na obrázku číslo 21 je také vidět, že autentizace probíhala pomocí PEAP, proces autentizace je znázorněn na obrázku číslo 23. Úspěšnou autentizaci také potvrzuje log ze služby Event Viewer (viz. Obrázek 20 a 21). Uživatel dostal od DHCP serveru IP adresu, masku sítě a implicitní bránu (viz. Obrázek č. 25). Dále na obrázku číslo 24 je vidět, že rozhraní, ke kterému je připojen uživatel byla přiřazena správná síť VLAN. Pomocí příkazu ping bylo otestováno připojení k Test_PC, na obrázku č. 26 je zobrazen úspěšný ping. Také na obrázku číslo 25 je vidět, že nastavení Host_Windows7 je v souladu s požadavky sítě, i když firewall byl vypnutý a proběhlo automatické napravení. Dalším testovacím případem byl pokus o přihlášení za použití nesprávných přihlašovacích údajů. Přístup k síti byl odepřen, výsledky komunikace mezi suplikantem, autentizátorem a RADIUS serverem jsou znázorněny na obrázcích č. 27 a 28, záznamy prohlížeče událostí Windows Server na obrázcích č. 29 a 30.

V posledním testovacím případě bylo vypnuto automatické napravení u zásady sítě FailedWired a provedeno přihlášení pomocí uživatele worker1@mva.com při vypnutém firewallu na klientském zařízení. Po přihlášení rozhraní klienta bylo připojeno do 5 sítě VLAN (viz. Obrázek 33) a klientské zařízení dostalo IP adresu od služby DHCP ze rozsahu FailedUsers_VLAN5 (viz. Obrázek 31). Zároveň NAP klient upozornil na vypnutý firewall a pro plný přístup k síti doporučil zapnout firewall manuálně (viz. Obrázek 32). Na obrázku č. 34 je zobrazen záznam z prohlížeče událostí Windows Server, který také potvrzuje, že přístup klienta k síti byl omezen a kvůli nastavenému ACL pro VLAN 5 klientské zařízení nebylo schopné pinknout Test_PC.

Závěr

Cílem bakalářské práce bylo popsat jak problematiku zabezpečení a řízení přístupu do počítačových sítí z pohledu síťového administrátora, tak i vznikla technologie pro její řešení.

Úvod teoretické části popisuje historický pohled na problematiku síťové bezpečnosti a ochrany přístupu k počítačovým sítím jako její neoddělitelnou součást. Dále byla popsána AAA architektura, bezpečnostní služby a protokoly rodiny AAA. V poslední kapitole byly popsány technologie, které postupem času vznikly jako možná řešení pro zabezpečení a ochranu přístupu do počítačových sítí: 802.1x, MAB a NAP.

V praktické části byla vytvořena testovací topologie počítačové sítě ve virtuálním prostředí GNS3. Zabezpečení a řízení přístupu v této testovací topologii bylo zajištěno pomocí technologie NPS/NAP a způsobem vynucení 802.1x pro drátové připojení. Nejdřív byla vytvořena topologie sítě, která obsahovala L2 a L3 přepínače. K L3 přepínači byl připojen počítač se systémem Windows Server 2012 R2 a další počítač pro testování. L2 přepínač vystupoval v roli autentizátoru. K L2 přepínači byl připojen klient, který hrál roli suplikanta. Dále na Windows Serveru byly nainstalovány a nakonfigurovány potřebné role. Síť byla rozdělena na 5 VLAN. Pro 4 VLANy v AD byly vytvořeny skupiny a jejich členové, nastaveny rozsahy IP adres. V NPS/NAP byly vytvořeny zásady vyžádání nového připojení, zásady sítě a zásady stavu klientského zařízení, podle kterých se určoval stav počítačů, které se připojují k síti. Testování se provádělo pomocí Wireshark: byl odchycen provoz sítě při autentizaci uživatele. Výsledky odchycené komunikace mezi suplikantem, autentizátorem a RADIUS serverem potvrdily, že při zadání správných autentizačních údajů a požadovaném stavu zařízení klienta, port přepínače bude přiřazen do správné VLAN sítě a klient dostane IP adresu od služby DHCP. Ověření úspěšné autentizace bylo také provedeno odesláním ICMP zpráv na Test_PC a kontrolou logů NPS serveru.

Technologie NAP byla nedoporučena k použití ve Windows Server 2012 R2 a odstraněna v Windows Server 2016. NAP klient byl odstraněn ve Windows 10. Technologie NAP nebyla Microsoftem oficiálně něčím nahrazena. Důvody odstranění NAP jsou různé. Například pro identifikaci klientských zařízení, která nesplňují nastavené zásady sítě lze použít System Center Configuration Manager a WSUS pro nápravu. Dalším problémem NAP je v tom, že NAP není "BYOD přátelský", protože v době jeho vzniku ještě nebyla trendem BYOD politika, která znamená, že si zaměstnanci nosí jakákoli svá zařízení do firemního prostředí, připojí je k síti a vykonávají svoji práci, i když NAP klient existuje pro různé operační systémy (Linux, macOS).

Ochrana přístupu do počítačových sítí je důležitou částí bezpečnostní politiky každé firmy. Podcenění daného problému může vést k bezpečnostním problémům a mít vážné následky, proto musí být zajištěno efektivní řízení přístupu do počítačové sítě za použití vhodných technologií.

Použitá literatura

ABOBA, B., L. BLUNK, J. VOLLBRECHT, J. CARLSON a H. LEVKOWETZ. *Remote Authentication Dial In User Service (RADIUS)* [online]. 2004 [cit. 2020-05-01]. Dostupné z: https://tools.ietf.org/html/rfc3748

AFANASJEV, A. a L. VEDENJEV. *Аутентификация Теория и практика обеспечения безопасного доступа к информационным ресурсам* [online]. 2-е издание. Москва: Горячая линия–Телеком, 2012 [cit. 2020-04-29]. ISBN 978-5-9912-0257-2.

BLOKDYK, Gerardus. *Network Policy Server Standard Requirements*. 5STARCooks, 2018. ISBN 9780655199656.

BURDA, Karel. AAA systémy a protokoly. *Elektrorevue* [online]. Brno: International Society for Science and Engineering, 2009, 29. 9. 2009, 1-7 [cit. 2020-05-04]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/clanky/informacni-technologie/35/aaa-systemy-a-protokoly-1/

CISCO. MAC Authentication Bypass Deployment Guide. *Cisco* [online]. 2011 [cit. 2020-05-04]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

Configuration Guide – User Access and Authentication. *Huawei* [online]. 2020 [cit. 2020-05-04]. Dostupné z: https://download.huawei.com/mdl/imgDownload?uuid=e587db03e1d2407ea3d77a61adaabbbc.png

CONGDON, Paul, Bernard ABOBA, Andrew SMITH, John ROESE a Glen ZORN. *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* [online]. 2003 [cit. 2020-06-19]. Dostupné z: https://tools.ietf.org/html/rfc3580

HOFFMAN, Daniel V. *Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control* [online]. Indianapolis: Wiley Publishing, 2008 [cit. 2020-07-06]. ISBN 978-0-470-23838-7. Dostupné z: http://index-of.co.uk/Hacking-Coleccion/Implementing%20NAP%20&%20NAC%20Security%20Technologies%20-%20The%20Complete%20Guide%20to%20Network%20Access%20Control.pdf

HUAWEI. Understanding 802.1X Authentication. *Huawei* [online]. 2020 [cit. 2020-05-04]. Dostupné z: https://download-hk.huawei.com/mdl/imgDownload?uuid=70d427207151454895515652e55268f9.png

HUAWEI. Understanding 802.1X Authentication. *Huawei* [online]. 2020 [cit. 2020-05-04]. Dostupné z: https://download.huawei.com/mdl/imgDownload?uuid=1fd43f221e974c9fabe208c955f31591.png

HUAWEI. What is NAC. *Huawei* [online]. 2020 [cit. 2020-05-04]. Dostupné z: https://download.huawei.com/mdl/imgDownload?uuid=21dd2eb349fd4fd2ada9ee92469fed21.png

KENIN, Alexander a Denis KOLISNICHENKO. *Самоучитель системного администратора*. 5-е издание. Санкт-Петербург: БХВ-Петербург, 2019 [cit. 2020-04-27]. ISBN 978-5-9775-4028-5.

KUBÁT, Michal. *Standard 802.1x* [online]. 2014 [cit. 2020-05-11]. Dostupné z: https://www.pbwcz.cz/Odborne%20clanky/standard_8021x.html

MICROSOFT. *NAP Client and Server-side Component Communication. Microsoft* [online]. 2018 [cit. 2020-06-19]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/nap/nap-client-and-server-side-component-communication

MICROSOFT. *NAP Client Architecture. Microsoft* [online]. 2018 [cit. 2020-06-19]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/nap/nap-client-architecture

MICROSOFT. *NAP Server-side Architecture. Microsoft* [online]. 2018 [cit. 2020-06-19]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/nap/nap-server-side-architecture

MICROSOFT. *Step By Step Guide: Demonstrate 802.1X NAP Enforcement in a Test Lab. Microsoft* [online]. 2008 [cit. 2020-06-29]. Dostupné z: https://pdfslide.net/documents/nap-8021x-step-by-step.html

MOLENAAR, Rene. PEAP and EAP-TLS on Server 2008 and Cisco WLC. *NetworkLessons* [online]. 2013 [cit. 2020-06-29]. Dostupné z: https://networklessons.com/wireless/peap-and-eap-tls-on-server-2008-and-cisco-wlc/#RADIUS-Computer-Certificate

Packetfence [online]. 2014 [cit. 2020-05-06]. Dostupné z: https://packetfence.org/about.html

RIGNEY, C., S. WILLENS, A. RUBENS a W. SIMPSON. *Remote Authentication Dial In User Service (RADIUS)* [online]. 2000 [cit. 2020-05-01]. Dostupné z: https://tools.ietf.org/html/rfc2865

ROUNTREE, Derrick. *Security for Microsoft Windows system administrators: introduction to key information security concepts*. Boston: Syngress, 2011. ISBN 1597495948.

SHESHKO, Anton. *Настройка 802.1x на оборудовании cisco* [online]. 2013 [cit. 2020-06-20]. Dostupné z: http://www.go-to-easyit.com/2013/11/8021x-cisco-1.html

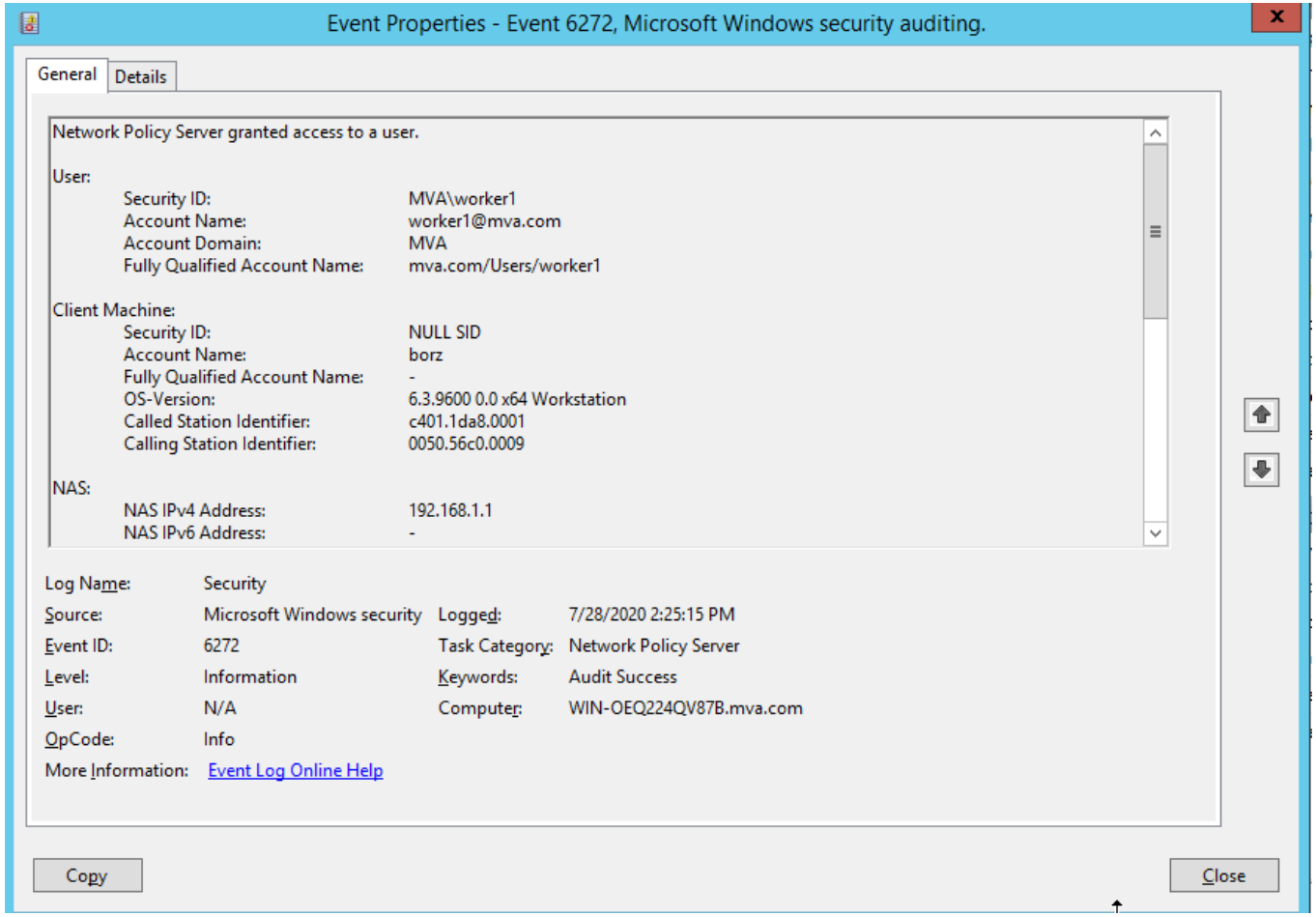
Seznam příloh

Příloha I: Seznam potřebných komponentů pro provedení testovacího scénáře

- Windows Server 2012 R2,
- Dynamips emulátor spolu s jeho grafickou nadstavbou GNS3 1.5 a obraz IOS Cisco c3640 s modulem NM-16ESW,
- Windows 7 Enterprise,
- VMware Workstation 15 Player,
- Jeden počítač s následujícími minimálními požadavky: procesor 2.4 GHz (x64), paměť RAM 8 GB, 70-80 GB volného místa na disku.

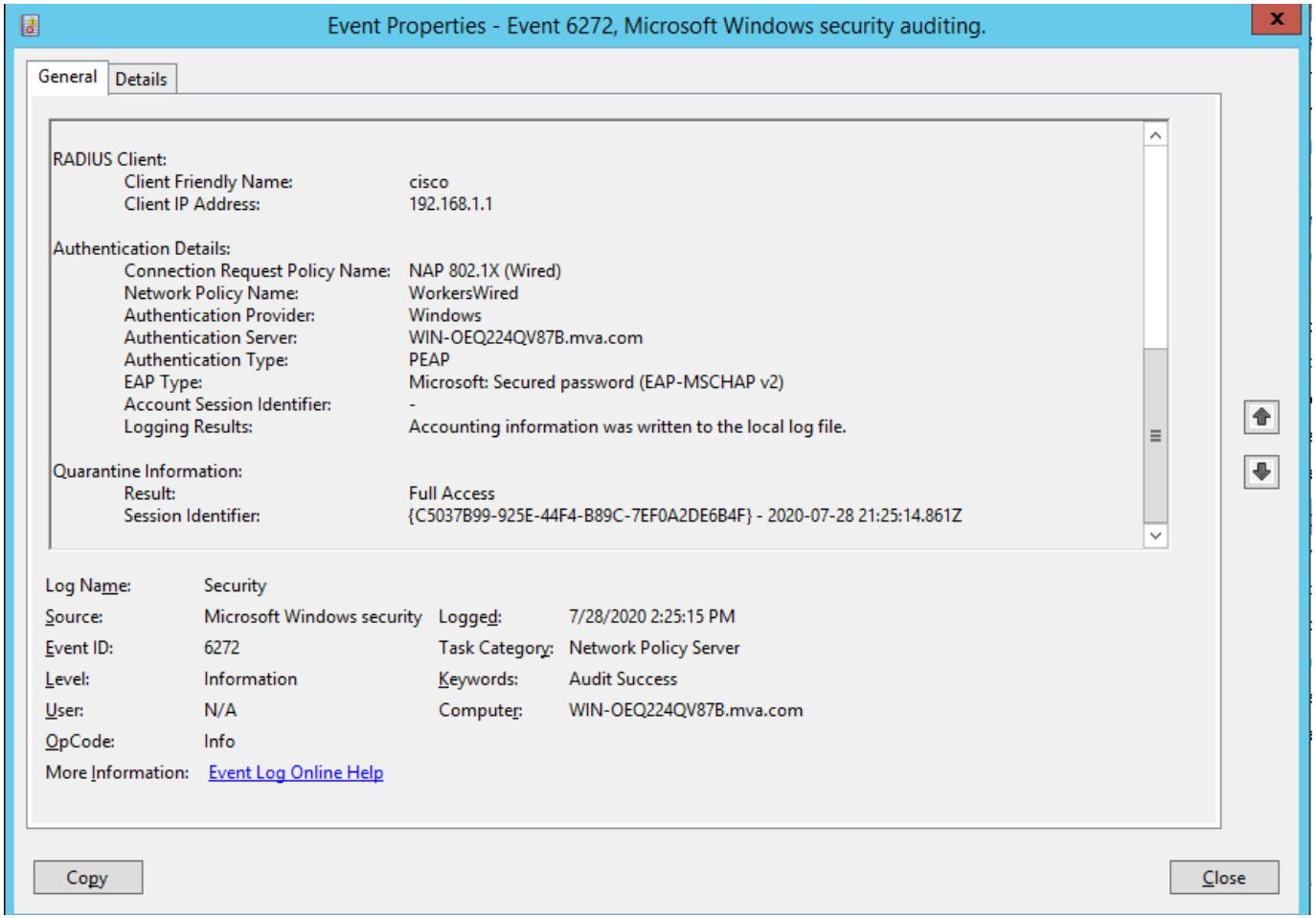
```
L3_Switch#vlan database
L3_Switch(vlan)#vlan 2 name Administrator
L3_Switch(vlan)#vlan 3 name WORK
L3_Switch(vlan)#vlan 4 name GUEST
L3_Switch(vlan)#vlan 5 name FAILED
L3_Switch(vlan)#vlan 6 name Test
L3_Switch(vlan)#exit
L3_Switch#conf t
L3_Switch(config)#ip routing
L3_Switch(config)#int vlan 2
L3_Switch(config-if)#ip address 192.168.1.10 255.255.255.0
L3_Switch(config-if)#ip helper-address 192.168.1.100
L3_Switch(config)#int vlan 3
L3_Switch(config-if)#ip address 192.168.2.1 255.255.255.0
L3_Switch(config-if)#ip helper-address 192.168.1.100
L3_Switch(config-if)#int vlan 4
L3_Switch(config-if)#ip address 192.168.3.1 255.255.255.0
L3_Switch(config-if)#ip helper-address 192.168.1.100
L3_Switch(config-if)#int vlan 5
L3_Switch(config-if)#ip address 192.168.4.1 255.255.255.0
L3_Switch(config-if)#ip helper-address 192.168.1.100
L3_Switch(config-if#int vlan 6
L3_Switch(config-if)#ip address 10.10.10.1 255.255.255.0
L3_Switch(config-if)#exit
L3_Switch(config)#int fa 0/1 (směr L2_Switch)
L3_Switch(config-if#switchport trunk encapsulation dot1q
L3_Switch(config-if)#switchport mode trunk
L3_Switch(config-if)#switchport trunk allowed vlan 1,2,3,4,5,1002-1005
L3_Switch(config-if)#exit
L3_Switch(config)#int fa 0/0
L3_Switch(config-if)#switchport mode access
L3_Switch(config-if)#switchport access vlan 2
L3_Switch(config-if)#spanning-tree portfast
L3_Switch(config)#int fa 0/2
L3_Switch(config-if#switchport mode access
L3_Switch(config-if)#switchport access vlan 6
L3_Switch(config-if)#spanning-tree portfast
L3_Switch(config-if)#exit
L3_Switch(config)#ip access-list extended FAILED
L3_Switch(config-ext-nacl)#permit icmp 192.168.4.0 0.0.0.255 host
192.168.4.1
L3_Switch(config-ext-nacl)#permit udp any any eq 67
L3_Switch(config-ext-nacl)#deny ip any any
L3_Switch(config-ext-nacl)#exit
L3_Switch(config)#int vlan 5
L3_Switch(config-if)#ip access-group FAILED in
L3_Switch(config-if)#exit
L3_Switch(config)#exit
L3_Switch#wr

L2_Switch(config)#vlan 2
L2_Switch(config-vlan)#name Administrator
L2_Switch(config-vlan)#vlan 3
L2_Switch(config-vlan)#name WORK
L2_Switch(config-vlan)#vlan 4
L2_Switch(config-vlan)#name GUEST
```

```
L2_Switch(config-vlan)#vlan 5
L2_Switch(config-vlan)#name FAILED
L2_Switch(config-vlan)#exit
L2_Switch(config)#int vlan 2
L2_Switch(config-if)#ip address 192.168.1.1 255.255.255.0
L2_Switch(config-if)#exit
L2_Switch(config)#int fa 0/1 (směr L3_Switch)
L2_Switch(config-if)#switchport trunk encapsulation dot1q
L2_Switch(config-if)#switchport mode trunk
L2_Switch(config-if)#switchport trunk allowed vlan 1-5,1002-1005
L2_Switch(config-if)#exit
```



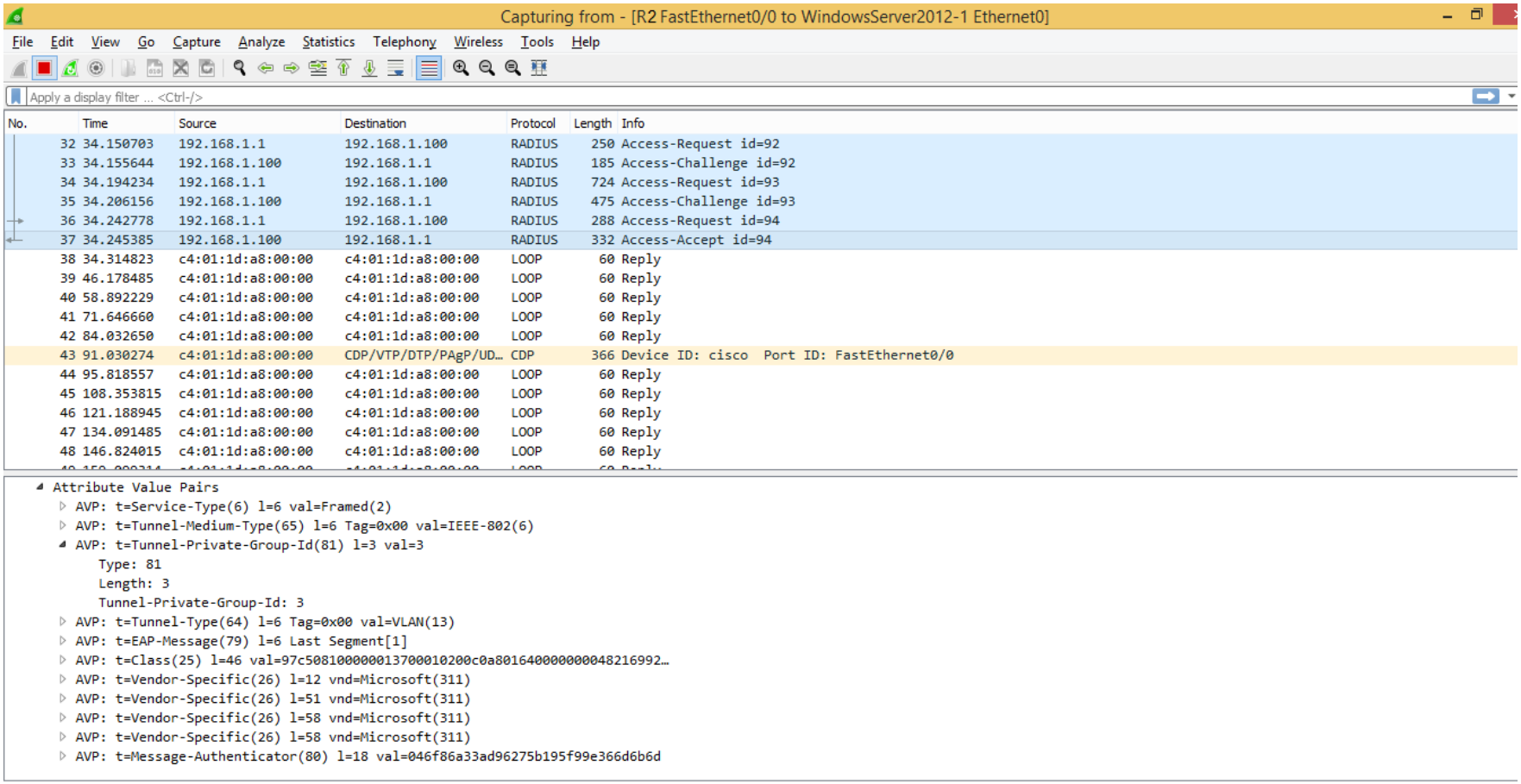
Obrázek 20: Event Viewer – plný přístup k síti 1

Zdroj: Vlastní



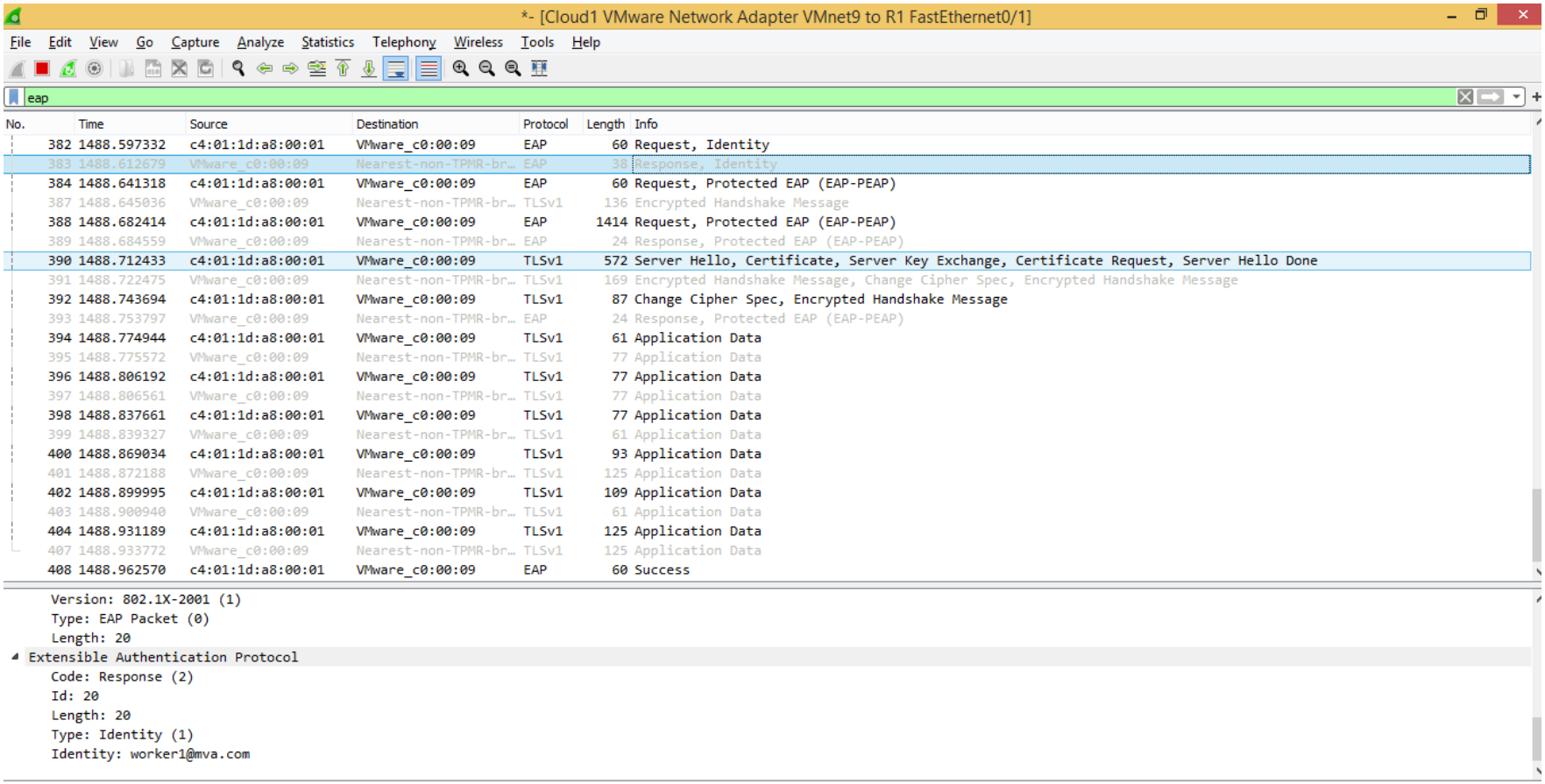
Obrázek 21: Event Viewer – plný přístup k síti 2

Zdroj: Vlastní



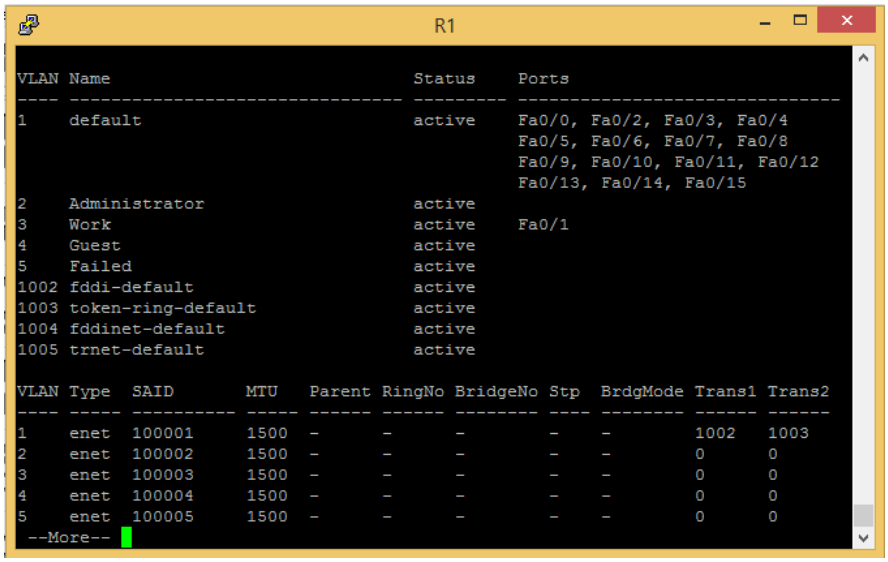
Obrázek 22: Wireshark – ověření klienta RADIUS serverem – plný přístup k síti

Zdroj: Vlastní



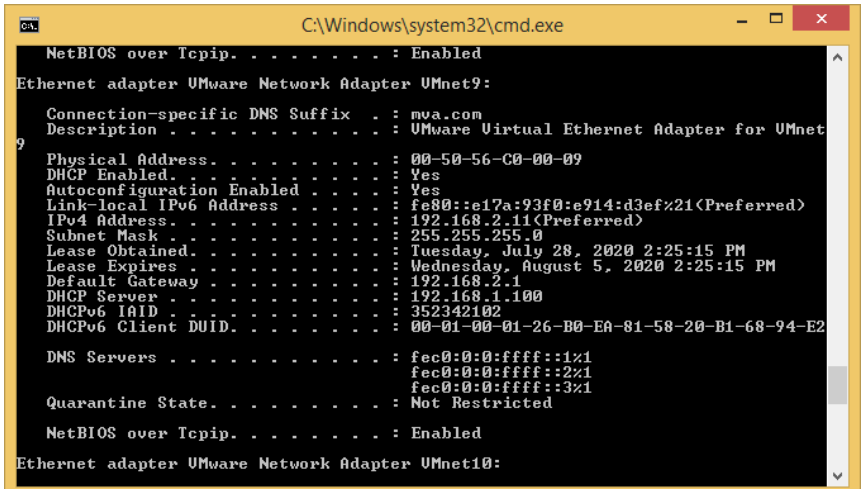
Obrázek 23: Wireshark – autentizace klienta pomocí PEAP – plný přístup k síti

Zdroj: Vlastní



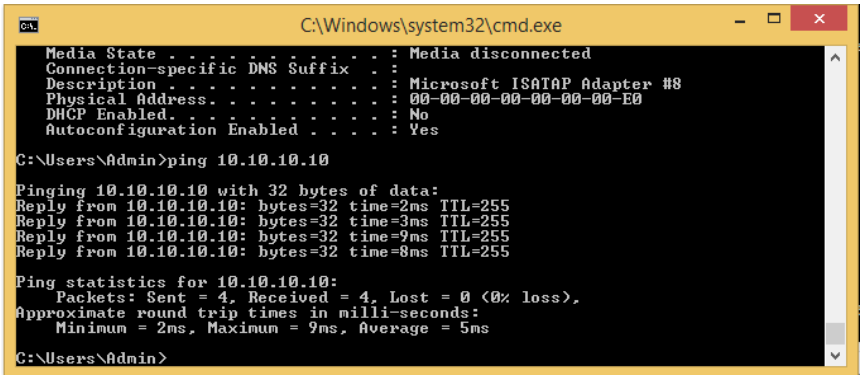
Obrázek 24: L2_Switch – ověření VLAN rozhraní – plný přístup k síti

Zdroj: Vlastní



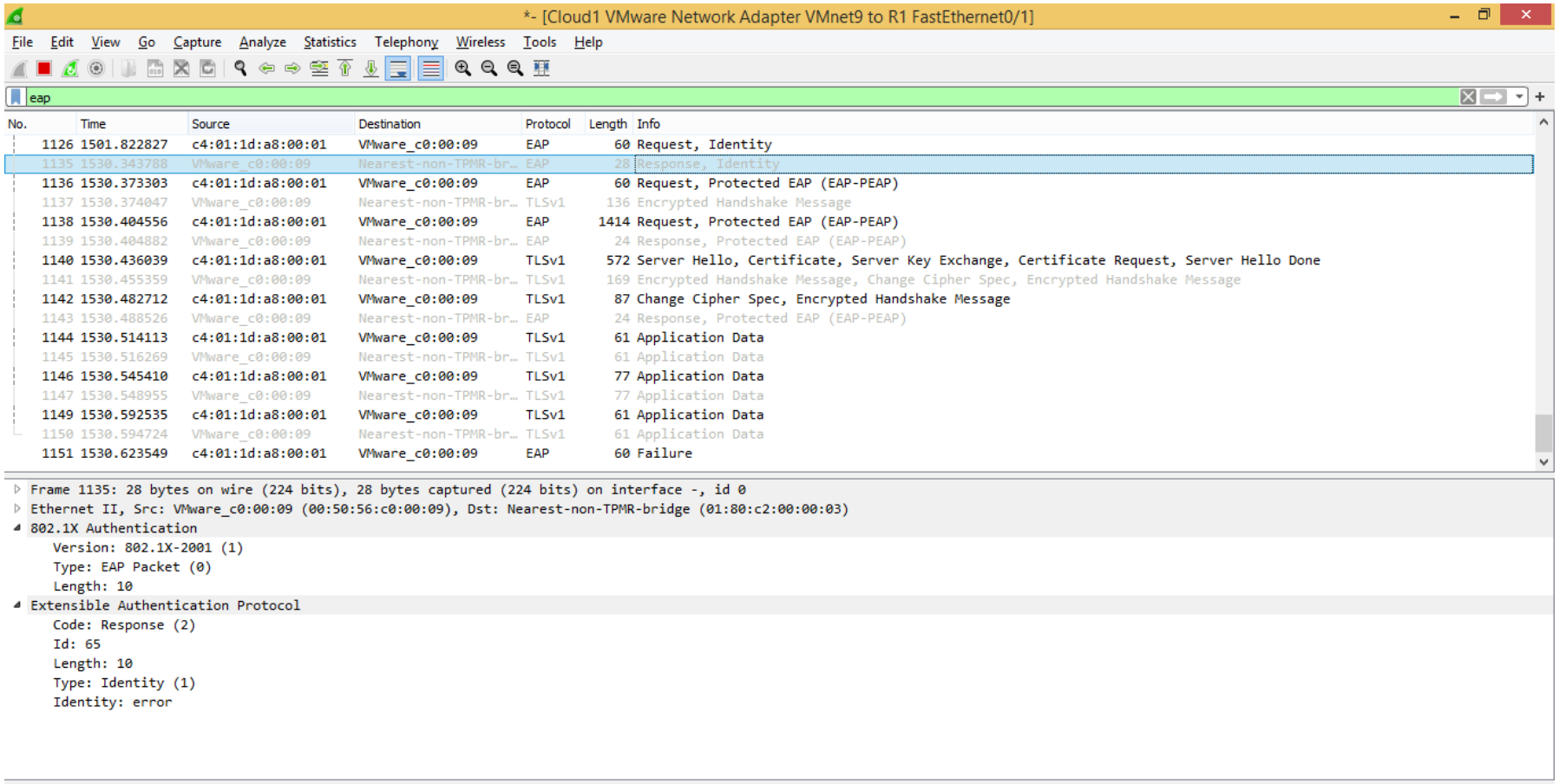
Obrázek 25: Host_Windows7 – ověření IP adresy a NAP statusu – plný přístup k síti

Zdroj: Vlastní



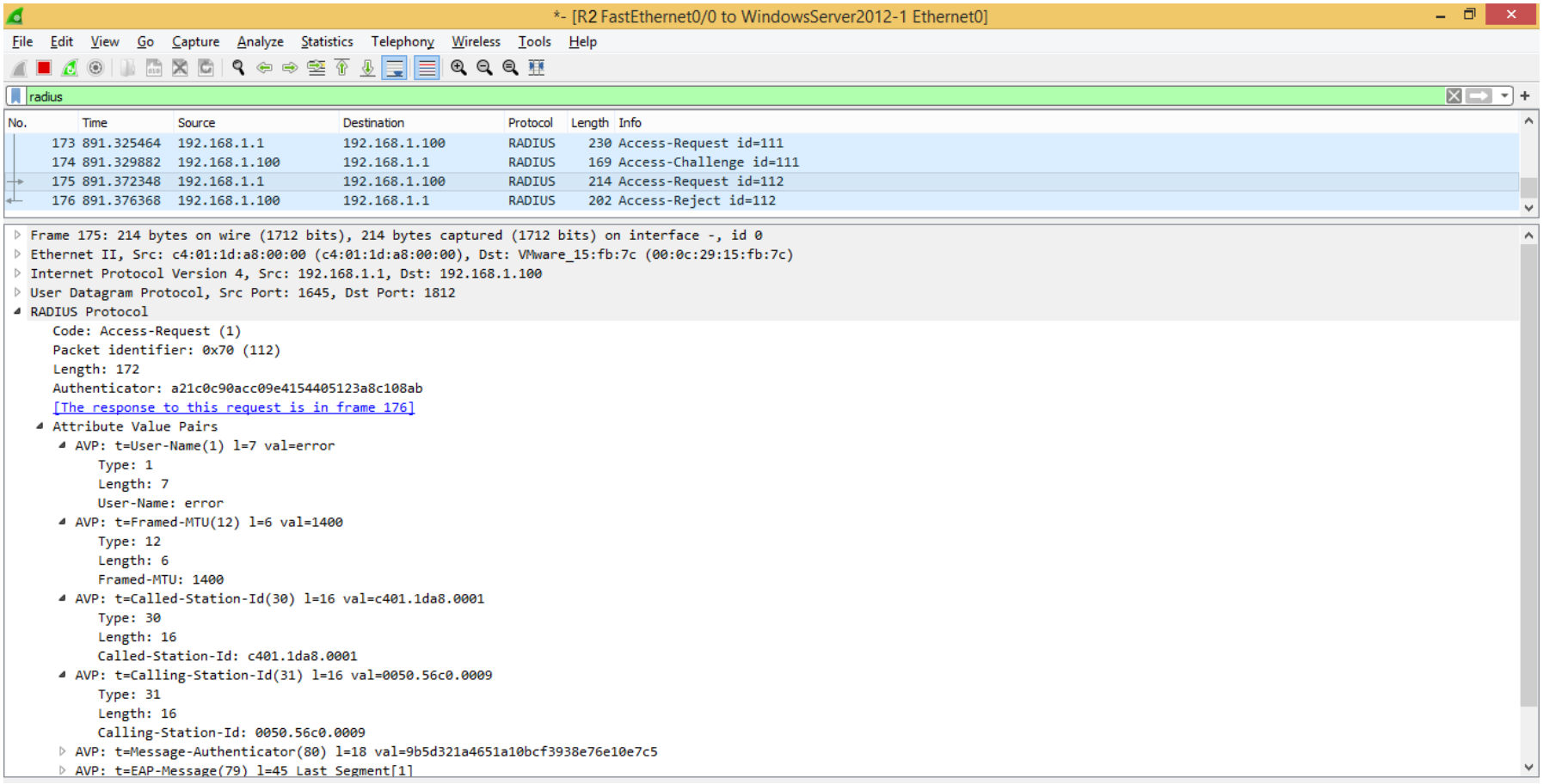
Obrázek 26: Host_Windows7 – test spojení s Test_PC

Zdroj: Vlastní



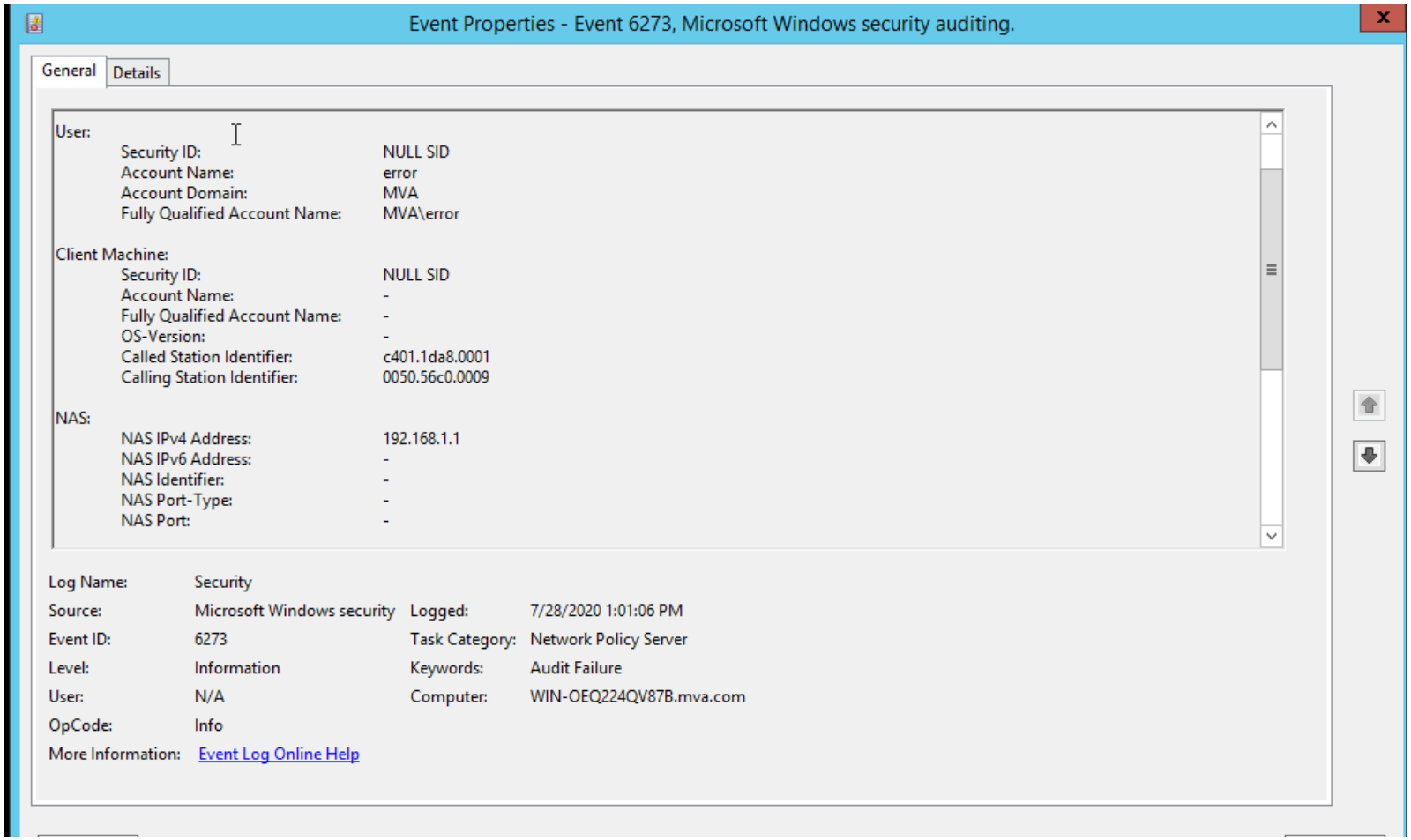
Obrázek 27: Wireshark – neúspěšná autentizace klienta pomocí PEAP

Zdroj: Vlastní



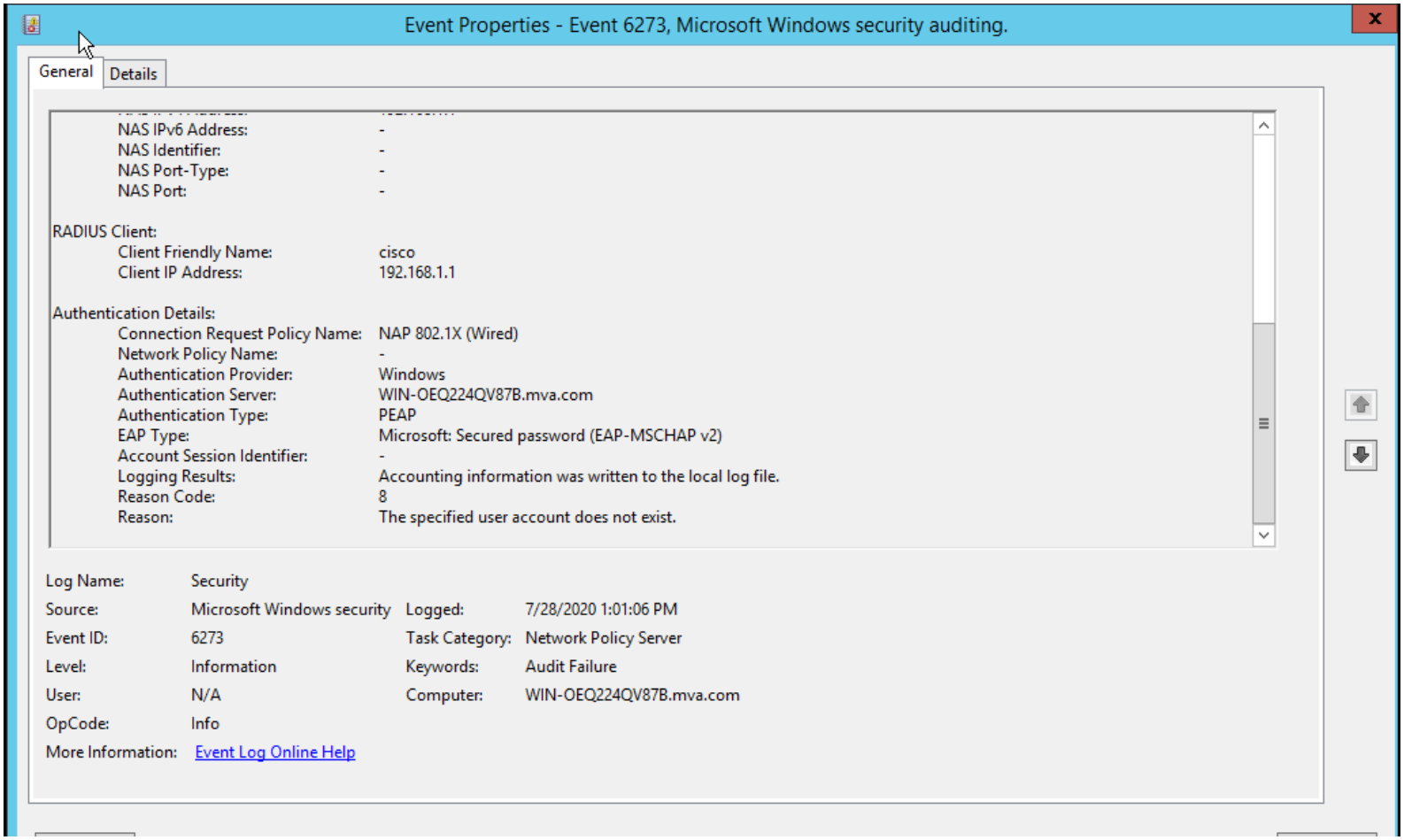
Obrázek 28: Wireshark – neúspěšné ověření klienta RADIUS serverem

Zdroj: Vlastní



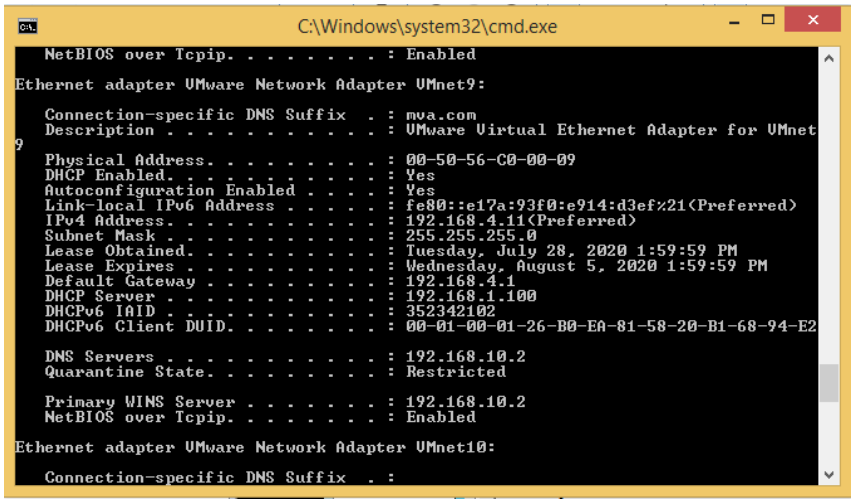
Obrázek 29: Event Viewer – neúspěšná autentizace 1

Zdroj: Vlastní



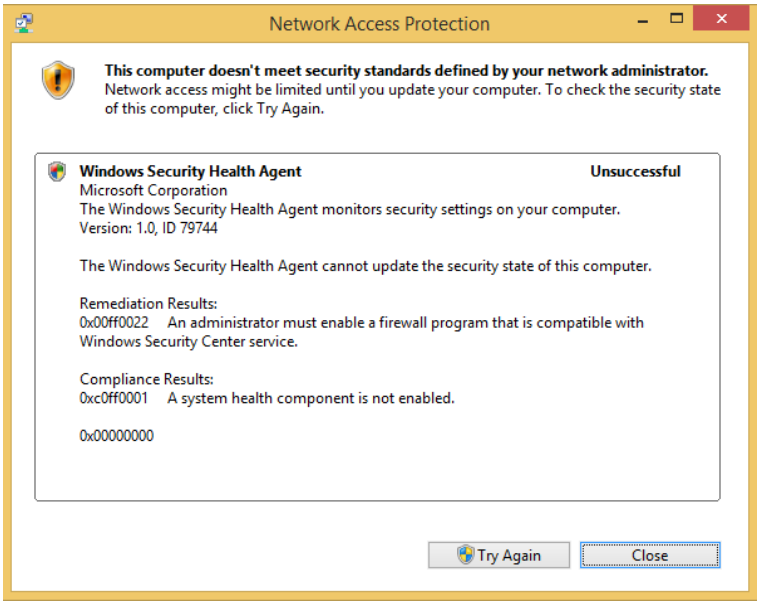
Obrázek 30: Event Viewer – neúspěšná autentizace 2

Zdroj: Vlastní



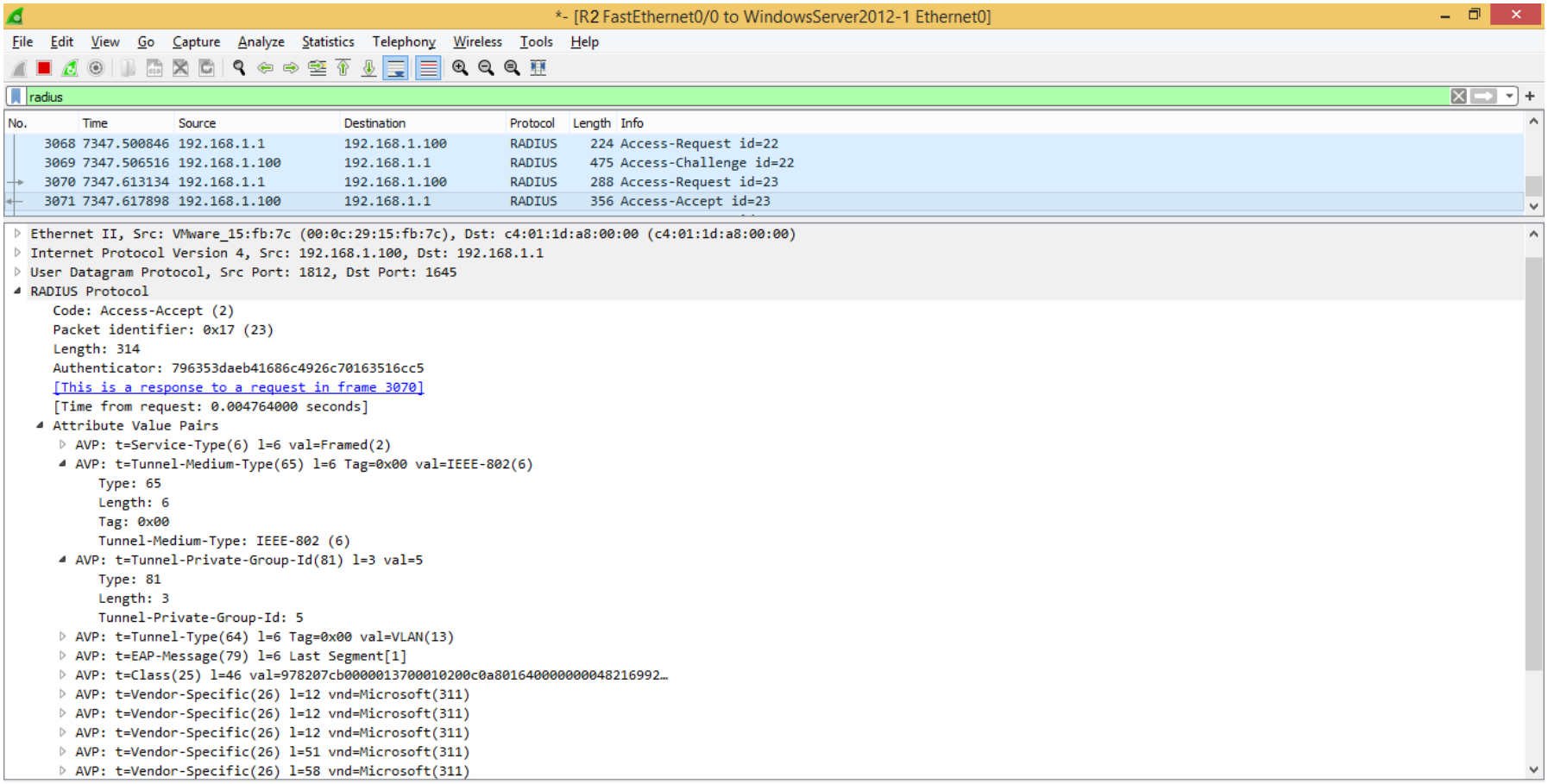
Obrázek 31: Host_Windows7 – ověření IP adresy a NAP – omezený přístup k síti

Zdroj: Vlastní



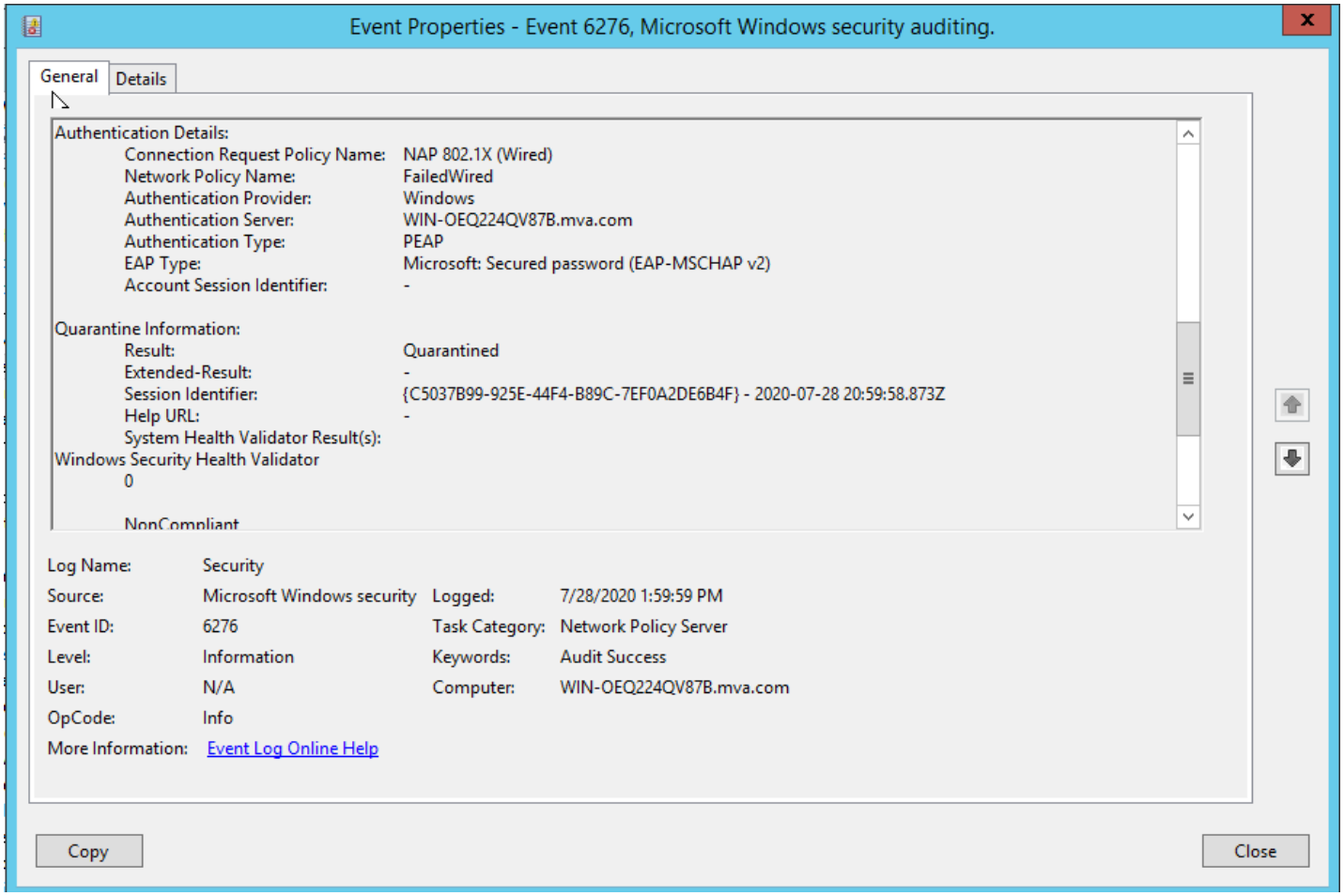
Obrázek 32: Host_Windows7 – upozornění NAP – omezený přístup k síti

Zdroj: Vlastní



Obrázek 33: Wireshark – ověření klienta RADIUS serverem – omezený přístup k síti

Zdroj: Vlastní



Obrázek 34: Event Viewer – omezený přístup k síti

Zdroj: Vlastní