



**ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ  
V PRAZE**

**Fakulta elektrotechnická**

**Katedra telekomunikační techniky**

**Řízení přístupu v počítačových sítích  
pomocí nástroje PacketFence**

**Květen 2015**

**Bakalant:** Martin Charvát

**Vedoucí práce:** Ing. Tomáš Vaněk, Ph.D.

## **Poděkování**

Rád bych poděkoval Ing. Tomáši Vaňkovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

## Čestné prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a konzultanta a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

Datum: 22. 5. 2015

.....

podpis bakalanta

České vysoké učení technické v Praze  
Fakulta elektrotechnická

katedra telekomunikační techniky

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Charvát Martin**

Studijní program: Komunikace, multimédia a elektronika  
Obor: Síťové a informační technologie

Název tématu: **Řízení přístupu v počítačových sítích pomocí nástroje PacketFence**

Pokyny pro vypracování:

Seznamte se s metodami řízení přístupu v lokálních sítích. Stručně a přehledně popište základní funkční bloky a jejich možnosti. Porovnejte možnosti dostupných komerčních (např. Cisco NAC, Check Point Integrity NGX, Juniper Unified Access Control) a open source řešení. V praktické části se zaměřte na nástroj PacketFence. Ve vhodném virtualizačním prostředí zprovozněte a nakonfigurujte linuxovou distribuci Debian rozšířenou o nástroj PacketFence pro řízení přístupu v lokálních sítích. Navrhněte a zrealizujte laboratorní úlohu demonstrující možnost detekce síťových útoků v takto zabezpečené síti.

Seznam odborné literatury:

- [1] Sealman M.: 802.1X-2001 - Port Based Network Access Control [on-line]. Last revision February 02, 2010 [cit. 2013-06-15].
- [2] PacketFence [on-line]. Last revision May 17, 2013 [cit. 2013-06-15].

Vedoucí: Ing. Tomáš Vaněk, Ph.D.

Platnost zadání: do konce letního semestru 2015/2016

prof. Ing. Boris Šimák, CSc.  
vedoucí katedry



prof. Ing. ~~Pavel~~ Ripka, CSc.  
děkan

V Praze dne 12. 12. 2014

## Anotace:

Tato bakalářská práce je zaměřena na řízení přístupu v počítačových sítích. V teoretické části jsou uvedeny základní principy a vlastnosti NAC, dále obsahuje souhrn existujících komerčních a open source variant NAC. V praktické části je ověřena funkčnost PacketFence ve virtuálním prostředí. Síťová infrastruktura včetně všech zařízení je implementována pomocí GNS3. Virtuální stroje, pomocí kterých byly testy prováděny, jsou provozovány v prostředí VirtualBox. Open source projekty Snort a Suricata byly použity jako síťový IDS/IPS. PacketFence podporuje jak Snort, tak suricatu a stará se o detekci síťových útoků.

## Klíčová slova:

PacketFence, Snort, Suricata, GNS3, NAC, kontrola přístupu, IDS, síťové útoky

## Summary:

This bachelor thesis is focused on network access control technologies. General characterization of NAC principles followed by brief description of existing commercial and Open source NACs is provided in theroretical part of the thesis. In practical part a functionality of PacketFence in virtual environment is tested. Network infrastructure including all network device was implemented in GNS3 simulator. Virtual machines representing the attacker and victim were also operated in virtual environment using a VirtualBox. Open source projects Snort and Suricate were used as a network IDS/IPS. PackedFence supports both Snort and Suricate and take care of detection and mitigation of networks attacks.

## Index Terms:

PacketFence, Snort, Suricata, GNS3, NAC, access control, IDS, network attacks

# Obsah

1 Úvod.....	3
1.1 Cíl práce.....	3
1.2 Co je to NAC .....	3
1.3 Komponenty NAC .....	3
1.4 Důvod nasazení NAC technologií do firemní sítě .....	4
2 Souhrn dostupných NAC .....	5
2.1 Komerční zástupci .....	5
2.1.1 Microsoft: Network Access Protection.....	5
2.1.2 Cisco NAC .....	8
2.1.3 ForeScout CounterACT .....	10
2.1.4 BRADFORD NETWORKS .....	12
2.2 Výhody komerčního přístupu .....	12
2.3 Nevýhody komerčního přístupu.....	12
2.4 Opensource NAC .....	13
2.4.1 OpenNAC .....	13
2.4.2 FreeNAC .....	14
3 PacketFence .....	15
3.1 Autentizace a Registrace.....	15
3.2 Dohled.....	15
3.3 Administrace .....	16
3.4 Historie.....	17
3.5 Pokročilé funkce .....	18
3.6 Komponenty.....	22
4 Praktická část .....	24
4.1 Rozdíl mezi VLAN a Inline enforcement.....	24
4.2 Topologie sítě: VLAN enforcement topologie.....	25
4.3 Konfigurace PacketFence: VLAN enforcement.....	29
4.4 Topologie virtuální sítě: Inline.....	32
4.5 Konfigurace síťových prvků: Inline.....	33
4.6 Konfigurace PacketFence: Inline .....	35
4.7 Instalace Suricata a Snort.....	39
4.8 Pravidla IDS.....	40
5 Závěr .....	45

6 Seznam zkratk .....	46
7 Seznam obrázků a tabulek .....	48
7.1 Obrázky:.....	48
7.2 Tabulky: .....	48
8 Zdroje.....	49
Podporovaná zařízení.....	51

# 1 Úvod

## 1.1 Cíl práce

Cílem této práce je vytvoření souhrnu dnes již běžně dostupných NAC (Network Access Control) technologií, v praktické části pak ověření správné funkčnosti technologie PacketFence pomocí řady testů. V první kapitole jsou uvedeny nejrozšířenější komerční technologie. Následující část je věnována open source a je zakončena podrobným popisem technologie PacketFence. U zmíněných technologií jsou uvedeny jejich hlavní bezpečnostní funkce a případně také komponenty, se kterými spolupracují, uvedena je též kompatibilita se síťovými zařízeními. V praktické části bude ověřena správná funkčnost, schopnost detekce různým síťovým útoků a kompatibilita s různými síťovými prvky.

## 1.2 Co je to NAC

Pokud začneme hledat informace o službách, které nabízí Network Access Control, často se setkáme také s pojmy Network Access Protection a Network Admission Control. To může být poněkud zmatečné, ale jejich podstata je velmi podobná, jedná se pouze o názvy, které si zvolili jednotlivé společnosti vyvíjející svoji verzi NAC. Konkrétně systém od Microsoftu je pojmenován Network Access Protection a systém Cisco Network Admission Control. Ostatní, převážně open source varianty, používají název Network Access Control. V dalším textu již budeme používat pouze zkratky NAC či NAP, pokud půjde výhradně o řešení Microsoftu.

Technologie NAC lze rozdělit hned dle několika kritérií. Jedním z nich je umístění technologie jako takové, ta může být centralizována na serveru, v takovém případě hovoříme o takzvané Clientless NAC. Na koncových zařízeních není nainstalovaný žádný software, který by pomáhal při procesu vyhodnocení bezpečnostního stavu. Opakem tohoto přístupu je Client-based NAC, u kterého na zařízení takový software nainstalovaný je. Dále se dělí na Pre-Admission a Post-Admission NAC. Rozdíl v těchto přístupech je takový, že u Pre-Admission probíhá kontrola před vstupem zařízení do sítě, zatímco u Post-Admission se tato kontrola provádí až v době, kdy má zařízení přístup k síti.[1]

## 1.3 Komponenty NAC

NAC je složen z více různých komponent, obecně je lze rozdělit takto [1]:

- Technologie pro analýzu bezpečnostního stavu a ověření zařízení.
- Komponenta zodpovědná za nastavení a analýzu požadovaných kritérií, která mají zařízení splňovat.
- Komponenta zodpovědná za šíření bezpečnostního stavu zařízení mezi dalšími částmi NAC/NAP řešení.
- Mechanismus, který přijme bezpečnostní stav zařízení a na základě toho podnikne příslušné kroky.
- Mechanismus, který zařadí podle provedených akcí zařízení do určité skupiny.
- Komponenta zodpovědná za přijetí zařízení zpět mezi vyhovující.
- Ohlašující mechanismus.

## 1.4 Důvod nasazení NAC technologií do firemní sítě

NAC technologie obecně zabraňují nebezpečným nebo nežádoucím zařízením v přístupu do privátní firemní sítě. Největší nebezpečí, v dnešní době, představují pracovní notebooky, které si zaměstnanci nosí domů. Takové zařízení nemůže zákonitě být 100% pod kontrolou, a proto je nutné ho vždy při vstupu znovu prověřit. Z tohoto důvodu se nejčastěji kontroluje přítomnost antivirového programu a aktuálnost operačního systému. Pokud zařízení splní veškeré podmínky nastavené při vstupní kontrole, je vpuštěno do privátní sítě. Dále lze u těchto technologií nastavit více uživatelských skupin. Například sekretářka jistě nemusí mít stejný přístup ke všem funkcím jako administrátor. Pokud ale při kontrole systém vyhodnotí, že zařízení nelze přistup do sítě povolit, zpravidla dojde k jeho přesměrování do části, ze které má přístup k Internetu, nikoli však do firemní sítě. Nejnovější vývoj v oblasti NAC technologií se zaměřuje především na oblast automatického napravení problému, který vedl k odepření přístupu do firemní sítě. Jako příklad můžeme uvést případ odepření přístupu z důvodu chybějící aktualizace operačního systému. Nejjednodušší využívanou variantou je upozornění uživatele na tento problém, případně poskytnutí odkazu ke stažení aktualizace. Pokročilejší systémy se ale snaží tento proces automatizovat a naistalují aktualizaci samy.[1]

## 2 Souhrn dostupných NAC

### 2.1 Komerční zástupci

V této kapitole jsou popsány nejvýznamější zástupci komerčně dostupných NAC. Mezi dva nejvýznamější patří Cisco NAC a Microsoft NAP.

#### 2.1.1 Microsoft: Network Access Protection

NAP je implementován přímo v serverovém operačním systému od verze Windows Server 2008. Na klientských zařízeních musí být nainstalován Windows XP SP3, Windows Vista nebo novější.

NAP je navržený tak, aby byl rozšiřitelný. Je schopen spolupracovat s každým softwarem, který je schopen zajistit SHAs (System Health Agents) a SHVs (System Health Validators). Hlavní oblasti, ve kterých má NAP využití jsou [2]:

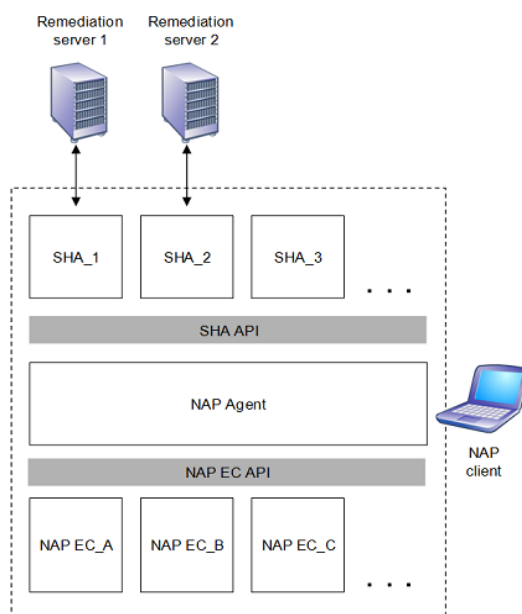
- ověření zdraví přenosného notebooku,
- zajištění zdraví stolních počítačů,
- potvrzení vyhovujícího stavu zdraví počítačů ve vzdálených kancelářích,
- určení zdraví notebooku, který je v síti pouze jako host,
- potvrzení vyhovujícího stavu zdraví nespravovaných domácích počítačů.

#### **Ze strany klienta, je NAP architektura složena následovně**

- Vrstva EC (Enforcement Client) komponentů

Každý NAP EC je definován pro různý typ síťového přístupu. Například je NAP EC pro DHCP (Dynamic Host Configuration Protocol) nebo NAP EC pro vzdálený přístup přes VPN (Virtual private network).

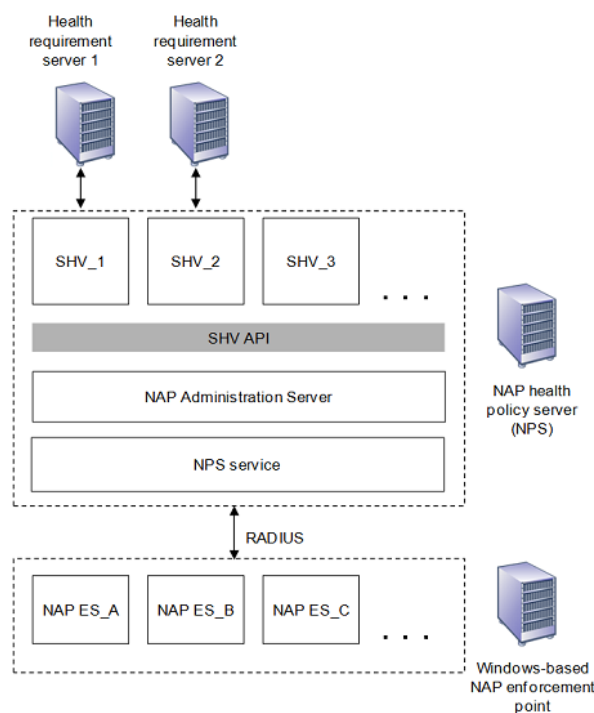
- Vrstva SHA komponentů  
SHA udržuje a hlídá aktuálnost jednoho nebo více prvků systémového zdraví. Například může být SHA kontrolující antivirus nebo updaty operačního systému.
- NAP Agent  
hlídá aktuální stav NAP klienta a zajišťuje komunikaci mezi NAP EC a SHA vrstvami.



Obr. 1: NAP architektura z pohledu klienta [3]

## Ze strany serveru, je NAP architektura složena následovně

- Vrstva ES (Enforcement Server) komponentů  
Každý NAP ES je definován pro různý typ síťového přístupu. Například je NAP ES pro DHCP nebo NAP ES pro vzdálený přístup přes VPN. Typicky jsou ES spárovány tak, aby spolupracovaly se stejně nastaveným EC.
- Network Policy Server (NPS)  
Přijímá RADIUS zprávu s požadavkem o povolení přístupu. Rozbalí SSoH a předá ho dál NAP Administration Serveru. NPS je součástí Windows Server 2008.
- NAP Administration Server  
Zajišťuje komunikaci mezi NPS a System Health Validators (SHVs).
- Vrstva SHV komponentů  
Každý SHV má definován jeden nebo více typů systémového zdraví, které se mohou být spojeny s SHA. Například může být SHV pro kontrolu antivirového programu. SHV může být spojen s jedním nebo více severu obsahujícími požadavky na zdraví systému. SHV nemusí mít vlastní server s požadavky, ale může klienty pouze přinutit, aby zkontrolovali lokální nastavení. Takto lze kontrolovat, zda je aktivní firewall.
- SHV API (Application Programming Interface)  
Zprostředkovává funkce, které dovolují SHV registrovat se u NAP Administration Serveru, přijímat Statements of Health (SoHs) a odesílat Statement of Health Responses (SoHRs).



Obr. 2: NAP architektura z pohledu serveru [4]

## Komunikace mezi NAP klientem a serverem

NAP Agent může komunikovat s NAP Administration Serverem následovně:

1. NAP Agent pošle SSoH do NAP EC.
2. NAP EC pošle SSoH do NAP ES.
3. NAP ES pošle do NPS.
4. NPS pošle SSoH do NAP Administration Serveru.

SHA může komunikovat s příslušným SHV následovně:

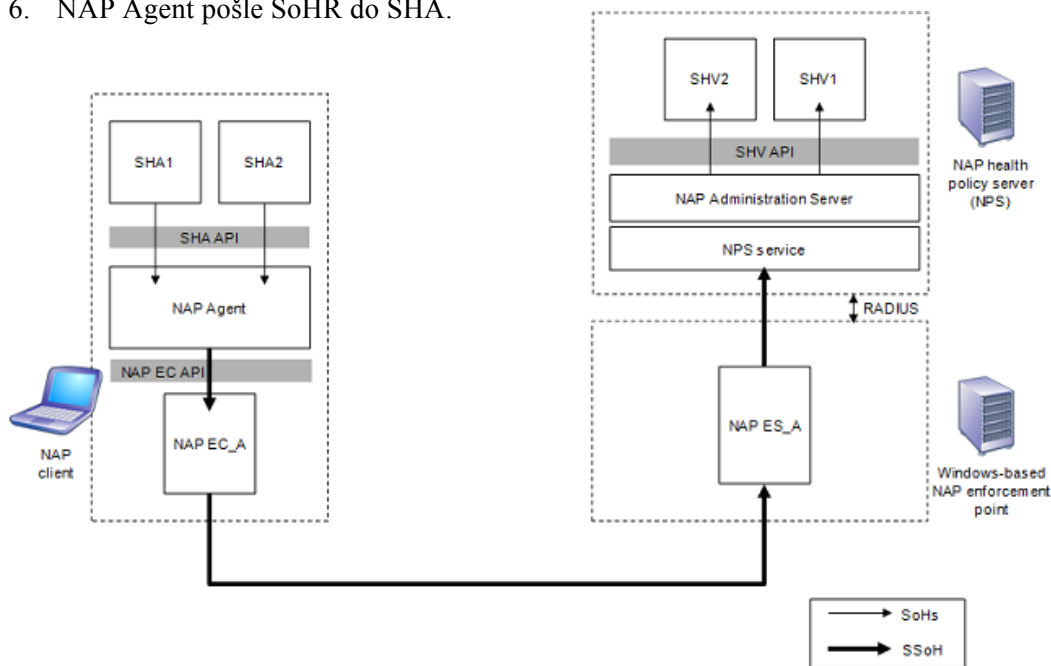
1. SHA pošle SoH do NAP Agentovi.
2. NAP Agent pošle SoH, který obsahuje SSoH do NAP EC.
3. NAP EC pošle SoH do NAP ES.
4. NAP ES pošle SoH do NAP Administration Serveru.
5. NAP Administration Server pošle SoH do SHV.

NAP Administration Server může komunikovat s NAP následovně:

1. NAP Administration Server pošle SoHRs do NPS.
2. NPS service pošle SSoHR do NAP ES.
3. NAP ES pošle SSoHR do NAP EC.
4. NAP EC pošle SSoHR do NAP Agentu.

SHV může komunikovat s příslušným SHA následovně:

1. SHV pošle SoHR do NAP Administration Server.
2. NAP Administration Server pošle SoHR do NPS service.
3. NPS pošle SoHR, který obsahuje SSoHR, do NAP ES.
4. NAP ES pošle SoHR do NAP EC.
5. NAP EC pošle SoHR do NAP Agentu.
6. NAP Agent pošle SoHR do SHA.



Obr. 3: Komunikace mezi NAP Agentem a NAP Administration Serverem [5]

## 2.1.2 Cisco NAC

V této kapitole jsou uvedeny základní vlastnosti a komponenty Cisco NAC [6].

### **NAC obsahuje**

- přístup na základě určených rolí,
- vnucení bezpečnostních pravidel na koncových zařízeních,
- přístup v roli hosta,
- podporu různých zařízení (nejen PC) a shromažďování dat.

### **Přístup na základě určených rolí**

Cisco NAC pomáhá snížit riziko potenciální ztráty informace tím, že umožňuje organizacím ověření uživatelských práv ještě před umožněním přístupu do sítě. To pomáhá zabránit neoprávněnému přístupu do sítě přes lokální, bezdrátovou nebo vzdálenou síť. Cisco NAC lze použít s VPN a 802.1X. V rámci maximalizace bezpečnostních výhod a minimalizace dopadu na uživatele lze implementovat jednotné přihlášení SSO (Single Sign-On).

### **Vnucení bezpečnostních pravidel na koncových zařízeních**

Vzhledem k tomu, že uživatelé často své notebooky přenášejí mimo místní síť organizace, je nezbytné zajistit, aby byla bezpečnostní ochrana těchto zařízení aktuální. Kontrola tohoto stavu se provádí při pokusu o připojení do firemní sítě. Cisco NAC zajišťuje komplexní prosazování těchto zásad a jejich podporu. Cisco NAC spolupracuje s celou řadou bezpečnostních aplikací fungujících na koncových zařízeních, podporuje více než 350 aplikací zahrnujících lídry v antivirových i dalších bezpečnostních oblastech. Také obsahuje možnosti pro automatické uvedení zařízení do kompatibilního stavu tak, aby bylo možné se do firemní sítě připojit, to vede ke snížení vlivu na koncového uživatele.

### **Přístup v roli hosta**

Cisco NAC pomáhá organizacím zlepšit provozní efektivitu a produktivitu zajištěním zabezpečeného přístupu hostům a přidělením interního přístupu dle nastavených práv. Zabezpečený návštěvníkový přístup dovoluje hostům být v kontaktu se svými vlastními organizacemi, a to bez nutnosti splnění bezpečnostních požadavků sítě, ve které se momentálně nacházejí.

### **Podpora různých zařízení (nejen PC) a shromažďování dat**

V klasické síti je hodně různých zařízení, která nejsou přiřazena k žádnému uživatelskému účtu. Jako příklad lze uvést IP telefony, tiskárny nebo skenery. Obvykle bývá velice náročné takováto zařízení lokalizovat, sledovat a zajišťovat jejich bezpečnostní ochranu. Cisco NAC přináší automatizovanou podporu těchto zařízení. Pomocí identifikace a sledování jsou tato zařízení umístěna do přednastavených oblastí sítě, které jsou rozdělené podle určených bezpečnostních požadavků. Tato technologie tedy značně přispívá k provozní efektivitě IT oddělení organizace. Dále je Cisco NAC schopný shromažďovat síťovou aktivitu uživatelů a zařízení, kterou lze následně využít k analýzám, plánování a dalším činnostem.

## Jednotlivé komponenty Cisco NAC

### Cisco NAC Manager

Cisco NAC Manager je webové rozhraní, které je určeno k vytváření bezpečnostních pravidel a pro správu online uživatelů. Také může poskytovat ověřovací proxy pro ověřovací server na páteřní síti. Administrátoři mohou použít Cisco NAC Manager k nastavení uživatelských rolí, kontrolu dodržování nastavených bezpečnostních pravidel a požadavků pro přístup do sítě. Cisco NAC Manager komunikuje a spravuje Cisco NAC Server, který je hlavním rozhodujícím komponentem pro Cisco NAC.

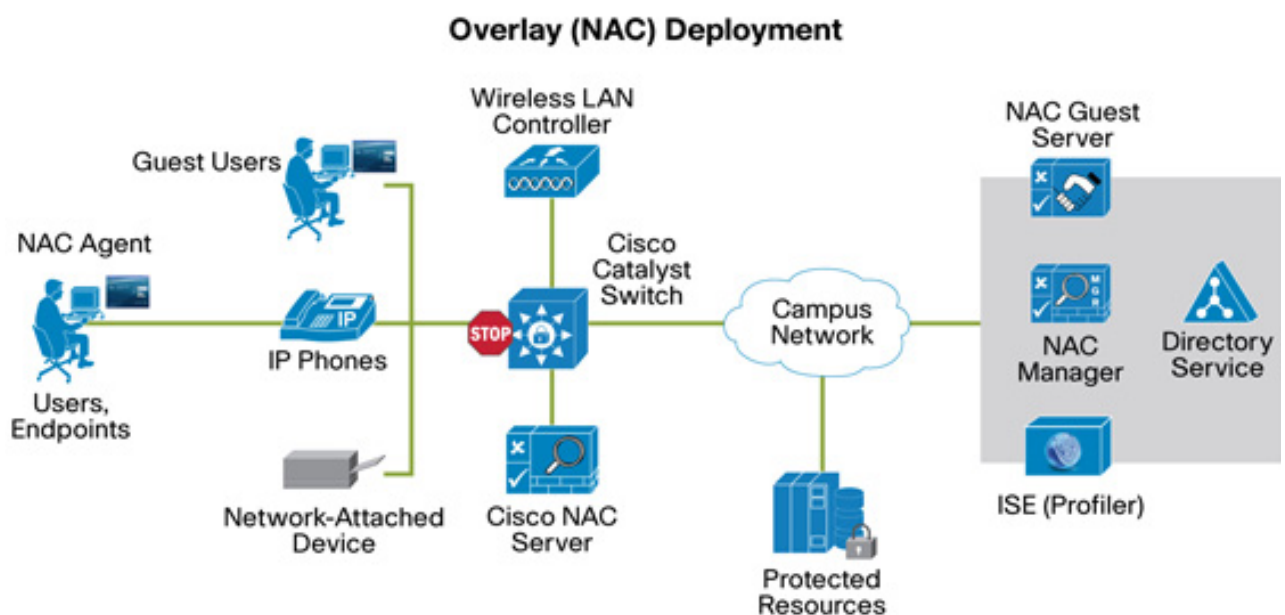
### Cisco NAC Server

Cisco NAC Server zajišťuje kontrolu dodržování bezpečnostních pravidel nastavených administrátorem v případě, že se uživatel pokouší připojit do sítě. Toto zabezpečovací zařízení je nasazeno na síťové vrstvě. Cisco NAC Server může být implementován inline i out of band, na Vrstvě 2 nebo Vrstvě 3, jako virtuální gateway nebo reálná IP gateway. Lze ho nasadit lokálně nebo kdekoli na světě.

### Nepovinná součást Cisco NAC

#### Cisco NAC Agent

Cisco NAC Agent je odlehčený agent určený pouze pro čtení, který běží na koncových zařízeních. Provádí hloubkovou kontrolu bezpečnostního profilu zařízení. Tato kontrola je prováděna analýzou nastavení registrů, služeb a složek. Během této kontroly lze tedy zjistit, zda má koncové zařízení požadovaný hotfix, nainstalovanu a spuštěnu požadovanou verzi antivirového programu nebo jiný bezpečnostní program jako například Cisco Security Agent. Cisco NAC Agent je dostupný jako běžná i jako webová aplikace.



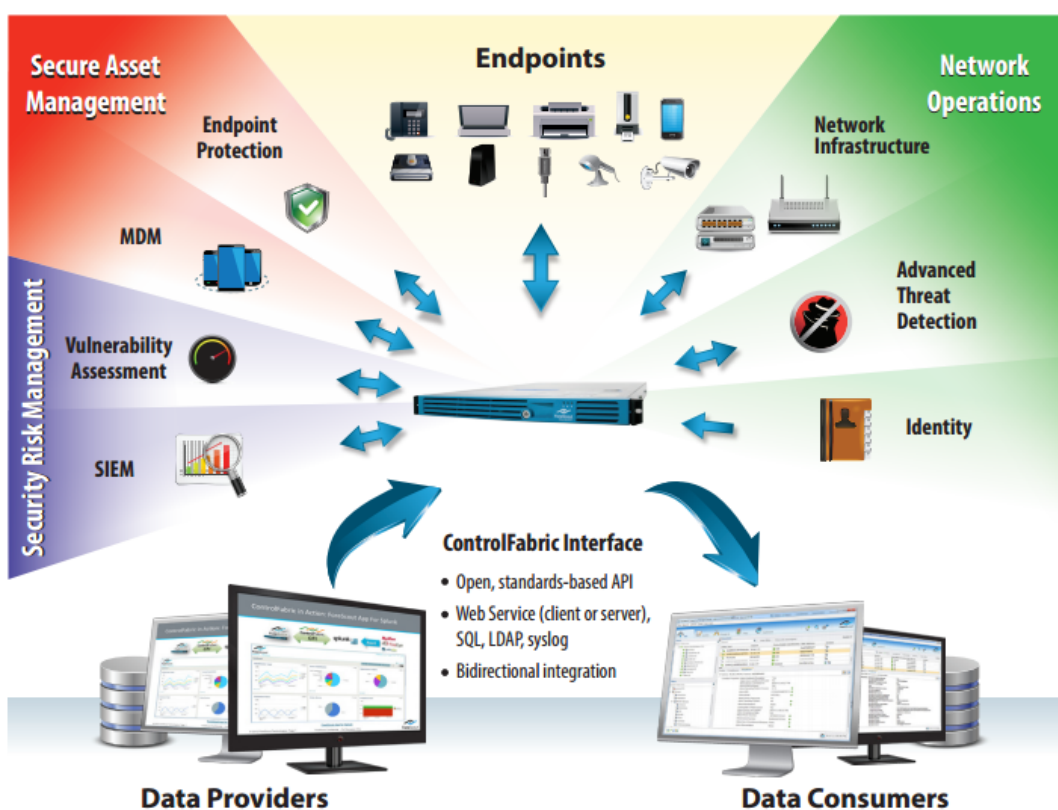
Obr. 4: Schéma sítě s podporou Cisco NAC [7]

### 2.1.3 ForeScout CounterACT

ForeScout CounterACT je síťová bezpečnostní technologie, která umožňuje efektivní kontrolu přístupu, dodržování zásad na koncových zařízeních nebo zajištění bezpečnosti mobilních zařízení v dnešních komplexních firemních sítích. Jedná se o NAC nové generace, díky kterému je možné [8]:

- Získávání informací o zařízeních, systémech, aplikacích a uživateli připojených do sítě v reálném čase.
- Flexibilní a rozmanitou správu bezpečnostních pravidel pro přístup do sítě a dodržování těchto pravidel koncovými zařízeními.
- Šíření a koordinaci informací napříč IT bezpečnostními systémy.
- Automatickou detekci a opravu bezpečnostních hrozeb.

ForeScout CounterACT se integruje do stávající síťové, bezpečnostní a uživatelské infrastruktury pomocí ControlFabric architektury. ForeScout ControlFabric je sada technologií, která umožňuje výměnu informací mezi CounterACT a dalšími IT řešeními. Dále slouží k posílení kontroly a snížení vlivu velké rozmanitosti sítě. Tím přispívá k řešení bezpečnostních a provozních problémů, které díky této rozmanitosti mohou nastat. V současnosti je CounterACT integrován s více než 60 různými síťovými, bezpečnostními, mobilními a IT management produkty. Navíc lze díky otevřenosti ControlFabric rozhraní přidávat nové funkce třetích stran, které jsou založeny na běžně používaných protokolech.



Obr. 5: Součásti ForeScout CounterACT [9]

ForeScout tedy vyniká hlavně těmito vlastnostmi:

- rychlé a snadné nasazení do síťové infrastruktury,
- nezávislost na výrobci síťových prvků použitých ve firemní síti,
- není vyžadována aplikace na koncových zařízeních, což značně usnadňuje BYOD integraci,
- škálovatelnost, díky které není problém spravovat 500 000 koncových zařízení,
- interoperabilita, která zajišťuje komunikaci se stávající bezpečnostní infrastrukturou.

## 2.1.4 BRADFORD NETWORKS

### NETWORK SENTRY

Hlavními vlastnostmi network sentry jsou [10]:

- Přehled o připojených zařízeních
- Pokročilá zpráva bezpečnostních pravidel
- Přístup v roli hosta
- Nastavení profilu zařízení
- Bezpečné nasazení nových zařízení
- Centralizovaný management
- Flexibilita
- Ochrana investice

Síťová Infrastruktura	3Com, Aerohive, Alcatel, Aruba, Brocade, Cisco, Dell, D-Link, Enterasys, Extreme HP, Juniper, Meru, Motorola, Ruckus, SMC, Xirrus, and others
Bezpečnostní Infrastruktura	ArcSight, Fortinet, Lancope, McAfee, NitroSecurity, Nokia, Packeteer, Palo Alto, Sonicwall, Sourcefire, Stonesoft, TippingPoint, TopLayer, and others
Autentizační & Directory Služby	RADIUS: All standard RADIUS servers LDAP: All standard LDAP directories
Operační Systémy	Desktop: Microsoft Windows, Apple OS X, Linux Mobilní: Apple iOS, Android
Zabezpečení koncových zařízení	Avast, AVG, Avira, CalmWin, DrWeb, ESET, F-Secure, GDATA, Kaspersky, Lavasoft, McAfee, Microsoft, Norton, Panda, Softwin, Sophos, Symantec, Trend Micro, Vipre, and others

Tabulka 1: Kompatibilita systému Network Sentry

## 2.2 Výhody komerčního přístupu

Pokud se organizace rozhodne pro komerční NAC, je jednou z hlavních výhod kvalitní podpora od výrobce. Ta se sice může velmi lišit s ohledem na konkrétního poskytovatele NAC řešení, ale obecně lze jistě říci, že u komerčních NAC lze očekávat rychlejší reakční dobu a kvalitnější přístup.

Mohlo by se zdát, že pokud organizace nasadí například Cisco NAC, je svázána s produkty Cisco, ale v posledních letech došlo v tomto směru k velmi výraznému posunu a například Cisco NAC a Microsoft NAP lze již mít nasazený v rámci jedné sítě. U menších poskytovatelů NAC je tato kompatibilita obvykle také zaručena.

## 2.3 Nevýhody komerčního přístupu

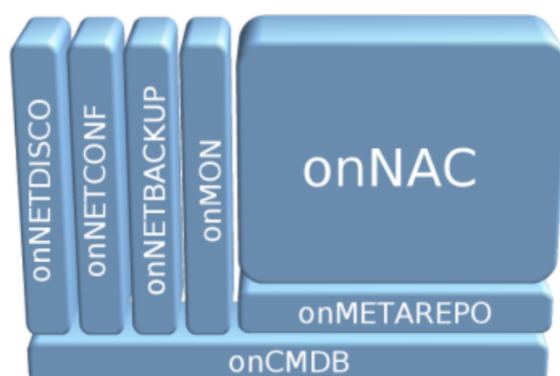
Mezi největší nevýhody komerčních NAC řešení v dnešní době patří především postupné ukončování podpory těchto systémů (zejména menšími společnostmi). Po velkém nárůstu zájmu o tento segment síťové bezpečnosti kolem roku 2005 dochází k postupnému odlivu zájmu. Například společnost Symantec tak 28. 11. 2014 oznámila, že s podporou svého NAC řešení končí 5. 10. 2017. Další známkou toho, že NAC jako pouhá kontrola bezpečnostního stavu koncových zařízení již není tak atraktivní, jako tomu bylo před 6 lety, kdy Microsoft ve Windows Serveru 2008 zavedl NAP, je i skutečnost, že u Windows Serveru 2012 R2 je tato technologie označena za zastaralou. Dnes se tedy spíše zavádí zabezpečení na úrovni jednotlivých zařízení místo celkového systému, který by přístup do sítě hlídal centrálně.

## 2.4 Open source NAC

V této kapitole jsou uvedeny open source varianty s výjimkou PacketFence, kterému je věnována samostatná kapitola.

### 2.4.1 OpenNAC

Jedná se o open source NAC, který zajišťuje bezpečné připojení k LAN/WAN. Pomocí něj lze flexibilně nastavit přístupová pravidla pro jednotlivé aplikace. Podporována jsou zařízení od Extreme Networks, Cisco, Alcatel a 3Com. Tato technologie je založena na ověřených open source komponentech jako jsou FreeRadius, iTop, Icinga a na vlastním softwaru vyvíjeném v rámci openNAC. Jedná se o velice flexibilní a rozšiřitelnou technologii, ke které lze snadno přidávat nové funkce. Mimo hlavní funkci, kterou je Network Access Control OpenNAC, nabízí také funkce přídatné. Mezi rozšířené funkce OpenNAC patří síťová konfigurace a průzkum, nastavení, záloha a monitorování síťových prvků. [11]



Obr. č. 6: Hlavními komponenty OpenNAC [12]

#### **onNAC**

Jedná se o základní Network Access control službu, která umožňuje prosazení autentizační a autorizační politiky u firemních sítí. Pomocí Management Console Administrátoru lze vyhledat a spravovat uživatele. Lze je identifikovat pomocí uživatelského jména, IP, MAC nebo fyzické lokace v případě, že je fyzická správa systému integrována. Pro přehled nad aktivitou sítě jsou k dispozici auditovací a ohlašovací mechanismy.

#### **onNETCONF**

Tento síťový konfigurační nástroj umožňuje konfiguraci síťových zařízení přes webové GUI. Pomocí předpřipravených šablon lze nakonfigurovat velké množství od stovek až po tisíce zařízení nebo lze nastavit, kdy a jak budou jednotlivé konfigurace prováděny. Je k dispozici také API pro rozšíření stávající funkcionality.

#### **onNETBACKUP**

Slouží k automatickému zálohování konfigurace síťových zařízení.

#### **onNETDISCO**

Modul, který zajišťuje průzkum sítě a udržuje inventář.

#### **onMON**

Monitorovací modul, který slouží k monitorování stavu síťových zařízení.

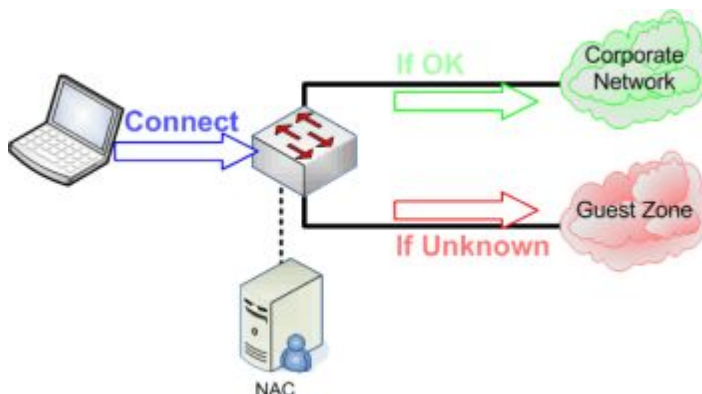
#### **onCMDB**

Síťový modul zálohující všechna data z inventáře do formátu, který je vhodný pro sdílení s dalšími platformami.

## 2.4.2 FreeNAC

FreeNAC umožňuje přehledné řešení pro správu dynamických VLAN a zároveň omezuje připojení do LAN sítě neznámým zařízením. Z bezpečnostního hlediska jde tedy o detekci neznámých zařízení, která se snaží připojit do sítě. Pokud se o připojení pokusí registrované zařízení, je přepnuto do LAN, kterou má přidělenou podle nastavených pravidel. V případě, že je nutné zajistit internetovou konektivitu také zařízením hostů, kteří nebyli prověřeni, lze je přesměrovat do Hostovské VLAN.

Ve chvíli, kdy se zařízení pokusí připojit do sítě, je jeho MAC adresa odeslána na server, kde je uložena. Následně se ověří, zdali je zařízení povolen přístup do sítě. Pokud je MAC adresa zařízení známa, pošle server přepínači informaci o tom, do které VLAN má zařízení připojit. V případě, že zařízení není na seznamu povolených, je buď zablokováno, nebo umístěno do Hostovské VLAN. Toto rozhodnutí záleží pouze na tom jaké jsou nastaveny parametry zabezpečení.



Obr. č. 7: Ukázka rozdělení do VLAN pomocí FreeNAC [13]

FreeNAC je schopný pracovat ve dvou různých módech [14]:

- **VMPS**
- **802.1X**

### **VMPS (VLAN Management Polici Server)**

Jedná se o mód, při kterém jsou jednotlivé porty přepínače přiřazeny do VLAN na základě MAC adresy připojovaného zařízení. V VMPS módu detekuje přepínač PC a vytvoří VMPS žádost o autorizaci od FreeNAC, který zkontroluje databázi. Na základě této kontroly buď povolí, nebo odepře přístup do sítě. Přepínač tedy buď přiřadí zařízení do určené VLAN, nebo odepře přístup.

### **802.1X**

Jedná se o IEEE standard pro Network Access Control založený na kontrole portů. Umožňuje autentizaci zařízení, které je připojené k LAN portu, vytvoření propojení bod-bod nebo odepření přístupu k portu v případě, že autentizace selhala. 802.1X je dostupný na některých přepínačích a může být nastaven tak, aby ověřil hosty s určitým softwarem nebo odepřel přístup k síti na spojení vrstvě. V 802.1X módu ověřuje FreeNAC uživatelské přihlašovací údaje (pomocí autentizačního serveru třetích stran) a použije jeho MAC adresu pro připojení zařízení do odpovídající VLAN, tím se vytvoří dvojice uživatelského jména a zařízení, která je pro každého klienta jedinečná. Takto je zvýšena klientova bezpečnost, protože útočníkovi by již nestačila pouze MAC adresa, ale potřeboval by znát i správné přihlašovací údaje.

## 3 PacketFence

PacketFence je plně podporované, ověřené a zdarma volně šiřitelné NAC řešení. Obsahuje velké množství funkcí – centralizovaná správa síťových zařízení, podpora 802.1X, izolace zařízení na druhé vrstvě modelu OSI, integrace se Snort IDS a Nessus nebo skener zranitelností. Může být použit od malých, až po velmi rozsáhlé sítě.[15]

### 3.1 Autentizace a Registrace

#### **Podpora 802.1X**

Jak bezdrátový, tak i drátový protokol 802.1X, je podporován díky modulu FreeRADIUS (bude popsán dále), který je součástí PacketFence.

#### **Podpora VoIP**

Tato technologie, někdy nazývaná také IP Telephony (IPT), je plně podporována v prostředí s více druhy koncových zařízení.

#### **Bezdrátová integrace**

PacketFence je integrován s bezdrátovou sítí pomocí modulu FreeRADIUS. To umožňuje zabezpečit bezdrátovou síť s pomocí stejné databáze a přístupového portálu pro zachování konzistentních uživatelských zkušeností. Použití různých výrobců přístupových bodů je také podporováno.

#### **Registrace zařízení**

PacketFence podporuje volitelný registrační mechanismus podobný přístupovému portálu. V závislosti na konfiguraci lze umožnit, aby si PacketFence pamatoval uživatele, kteří se již dříve přihlásili. Pokud je tato možnost aktivní, nebude při příštím přihlášení vyžadováno zadání přihlašovacích údajů.

### 3.2 Dohled

#### **Detekce abnormální síťové aktivity**

Abnormální síťové aktivity jako viry, červi, spyware nebo provozování nepovolených služeb lze detekovat pomocí Snort (bude popsán dále), Suricata nebo dalších komerčních sensorů. Mimo běžné detekce obsahuje vrstva PacketFence také vlastní alarmy. Díky tomu lze ke každému typu nežádoucí aktivity přiřadit odpovídající akci.

#### **Statement of Health**

Během autentizace 802.1X může PacketFence provést kompletní kontrolu zařízení, které se snaží připojit do sítě pomocí TNC Statement of Health protokolu. Například tak lze ověřit, zda má zařízení instalovaný a aktualizovaný antivirus nebo všechny potřebné aktualizace operačního systému. To a mnohem více lze zjistit bez nutnosti instalace agenta na koncovém zařízení.

## Proaktivní skenování zranitelností

Nessus nebo OpenVAS skeny zranitelností mohou být spuštěny při registraci, plánovaně v určitou dobu nebo na základě určitých okolností.

## Řešení problému pomocí přístupového portálu

Pokud je zařízení zachyceno z důvodu detekce hrozby, je veškerý provoz ukončen systémem PacketFence. Na základě aktuálního stavu (neregistrovaný, neznámý atd.) je uživatel přesměrován na odpovídající URL odkaz. V případě výskytu některé ze zranitelností jsou uživateli zobrazeny instrukce pro odstranění konkrétního problému. Tento postup značně omezuje nutnost zásahu technické podpory.

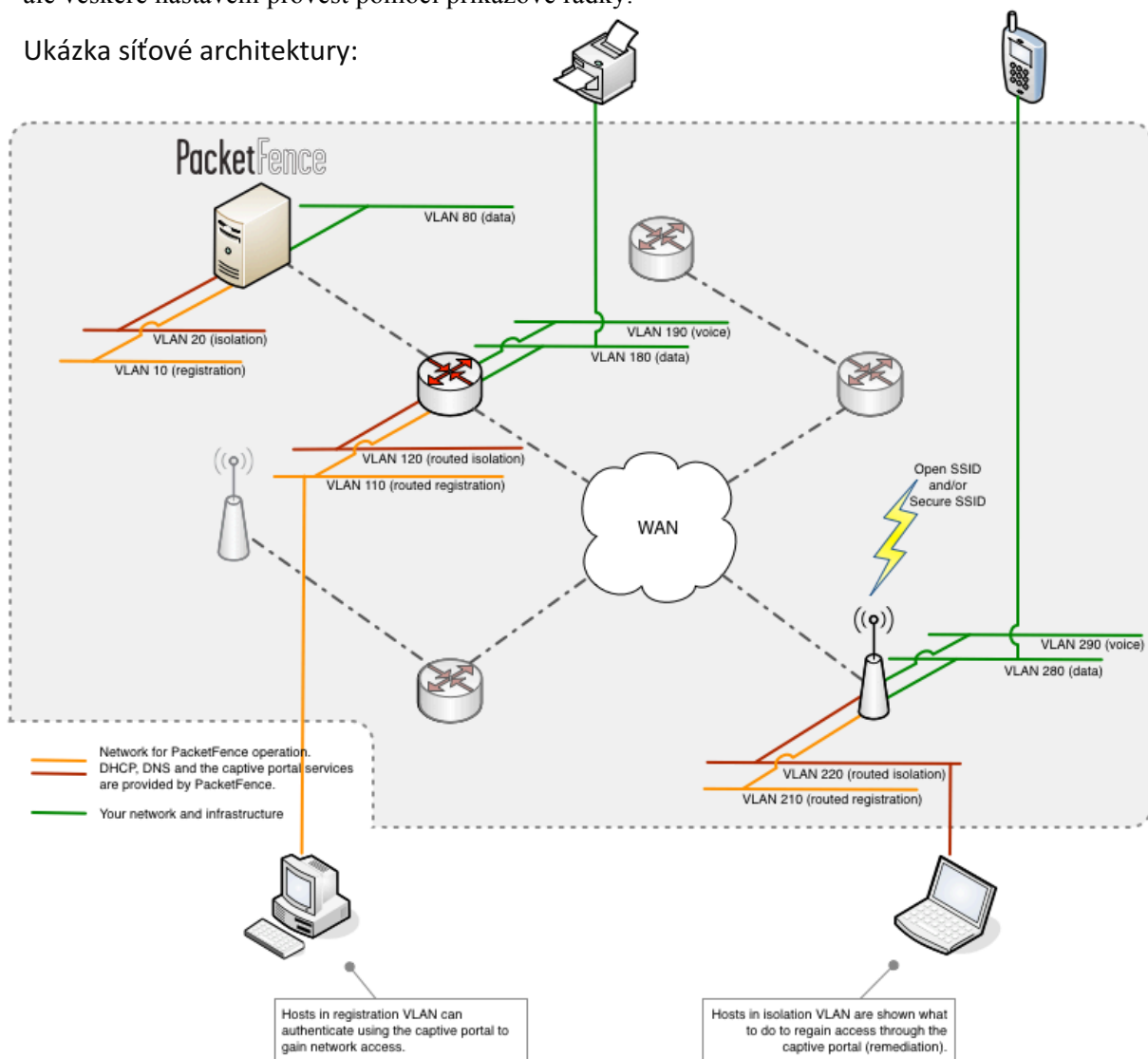
## Izolace problematických zařízení

PacketFence podporuje několik izolačních technik, včetně izolace pomocí přiřazení zařízení do určité VLAN na základě detekovaného problému.

## 3.3 Administrace

PacketFence nabízí webové prostředí, ve kterém lze nastavit různé úrovně zabezpečení. Také lze ale veškeré nastavení provést pomocí příkazové řádky.

Ukázka síťové architektury:



Obr. č. 8: Architektura PacketFence [16]

### 3.4 Historie

Počátky PacketFence lze vysledovat směrem ke dvěma zaměstnancům z Harvardské Univerzity. Ve svém volném čase se Dave LaPorte a Kevin Amarin věnovali vývoji tohoto systému pro kontrolu síťového přístupu. V roce 2008 již ale přešlo vedení vývoje na Inverse, což je společnost, která se zabývá vývojem open source softwaru a již dříve pomáhala tvůrcům s vývojem.

V následujícím seznamu jsou uvedeny nejvýznamnější funkce, které byly do PacketFence přidány:

#### **2008 ( 1.7.0-1.7.5)**

- VLAN izolace
- Podpora bezdrátových sítí
- Podpora autentizace pomocí RADIUS
- PacketFence ZEN edice – tato verze je určena pro rychlé nasazení do sítě (Zero effort NAC)
- Vydání dokumentace pro zjednodušení instalace administrace a vývoje

#### **2009 (1.8.0-1.8.6)**

- Podpora SNMP třetí verze
- Integrace NESSUS technologie
- Komptabilita se Snort

#### **2010 (1.8.7-2.0.0)**

- Zjednodušení konfigurace bezdrátové autentizace
- Možnost nastavení přístupu k specifickým stránkám i v případě že uživatel neprojde kontrolou

#### **2011 (2.0.1-3.1.0)**

- Autodetekce VoIP
- Zlepšení služeb pro hosty (dočasná hesla, předregistrace )
- Kontrola nad konfigurací firewallu lokálního serveru
- Podpora RedHat Enterprise Linus 6 / CentOS 6
- Podpora Statement of Health

#### **2012 (3.2.0-3.6.0)**

- Integrace OpenVAS
- Kontrola přístupu na základě rolí
- Podpora až 100 VLAN
- Podpora Suricata IDS
- Radius Inline

#### **2013 (3.6.1-4.1.0)**

- Nové webové rozhraní
- Odstranění nutnosti restartovat FreeRADIUS server po přidání přepínače

#### **2014 (4.2.0-4.5.1)**

- Agent zajišťující přístup zařízením s operačním systémem Android
- Přidání lokální autentizace pomocí EAP
- Nově může admin vyžádat znovu ověření zařízení
- Možnost hledání přepínačů

#### **2015 (4.6.0-5.0.1)**

- Přispůsobitelné administrativní GUI
- Všechna lokálně uložená hesla jsou šifrována pomocí bcrypt
- Nově přepracovaná dokumentace

Vzhledem ke snaze o stručný popis vývoje PacketFence zde nejsou ani zdaleka uvedeny všechny nové funkce, které byly v daných letech uvedeny. Jejich kompletní seznam lze snadno dohledat na webových stránkách výrobce. Také zde není uvedeno postupné přidávání podpory jednotlivých síťových prvků, tento seznam bude uveden v příloze, jako kompletní seznam kompatibilních zařízení aktuální k datu vytvoření této práce.

### **3.5 Pokročilé funkce**

#### **Flexibilní management VLAN a kontrola přístupu na základě rolí**

Toto řešení je založeno na konceptu izolace pomocí přiřazení do VLAN. Díky dlouholetým zkušenostem je PacketFence VLAN management velice flexibilní. Firemní VLAN topologie může zůstat nezměněna a pouze se přidají dvě nové VLAN. Jedná se o VLAN určenou pro registraci a VLAN pro izolaci. Také může PacketFence využít rozdělení na role poskytované výrobcí síťových prvků.

#### **Návštěvnícký přístup – Bring Your Own Device (BYOD)**

Dnes je již naprosto běžné, že se ve firmě vyskytují lidé, kteří si donesli své vlastní zařízení. Ať už se jedná o konzultanty z různých společností nebo klienty. Tito uživatelé ovšem běžně nepotřebují mít přímý přístup do firemní sítě a postačí jim pouze přístup k internetu. Z tohoto důvodu podporuje PacketFence speciální Hostovskou VLAN, která přesně tyto požadavky splňuje. Přístupový portál a registrační VLAN slouží k seznámení hosta se způsobem připojení. PacketFence nabízí několik možností jakými lze hosty registrovat:

- Manuální registrace hosta
- Heslo dne
- Host se registruje sám (s nebo bez přihlašovacích údajů)
- Sponzorovaný přístup (zaměstnanec se zaručí za hosta)
- Přístup na základě emailové pozvánky
- Přístup na základě potvrzovací SMS
- Přístup na základě autentizace přes Facebook/Google/GitHub

## Metody blokace zařízení

- **DHCP fingerprint**

PacketFence je schopný blokovat zařízení na základě jejich DHCP fingerprint. Téměř všechny dnes používané operační systémy mají svůj vlastní DHCP fingerprint. PacketFence může tuto informaci využít a zablokovat přístup k síti na základě DHCP fingerprint. Lze takto blokovat například herní konzole, bezdrátové přístupové body nebo VoIP telefony.

- **Uživatel-Agent**

PacketFence umožňuje zablokovat přístup na základě webového prohlížeče, který je na zařízení spuštěn. Díky tomu lze blokovat například iPody, iPhony nebo kohokoli, kdo používá starou verzi prohlížeče Internet Explorer.

- **MAC adresa**

Také lze blokovat přístup na základě MAC adresy. To se může hodit, pokud je požadováno například zakázání přístupu všech zařízení od určitého výrobce.

## Doba možnosti připojení k síti

Doba, během které se může zařízení připojit do sítě, lze nastavit několika způsoby. Lze nastavit konkrétní datum (např. "Út Led 20 20:00:00 EST 2014"), časový interval (např. čtyři dny od prvního přihlášení) nebo omezení přístupu hned v okamžiku, kdy přestane být zařízení aktivní. Ve chvíli, kdy tato doba uplyne, jsou zařízení nezaregistrovaná. S trochou úprav mohou být tato nastavení závislá na typu zařízení. Dobu pro jednotlivá zařízení lze nastavit také manuálně.

## Automatická registrace

Vzhledem k tomu, že většina dnešních sítí je již velice rozsáhlá a komplexní, umožňuje PacketFence několik způsobů automatické registrace klienta nebo zařízení.

- Registrace na základě typu zařízení
- Registrace na základě DHCP fingerprint
- Registrace na základě MAC adresy
- Dále lze využít Snort, Nessus, OpenVAS

## Správa zařízení

PacketFence poskytuje správu zařízení pomocí doplňkových řešení. Tato řešení běžně vyžadují agenta nainstalovaného na uživatelském zařízení. PacketFence je schopný ověřit, zda je agent nainstalován během procesu registrace a při každém dalším přihlášení.

Podporována jsou tato řešení:

- MobileIron
- OPSWAT GEARS
- Symantec SEPM

Zároveň PacketFence poskytuje své vlastní konfigurační agenty pro Android, Apple a Windows zařízení.

## **Integrace Firewallu**

Při připojení, ať už bezdrátově nebo drátově, může PacketFence dynamicky aktualizovat IP/uživatel záznam na firewallu k uplatnění uživatelských nebo skupinových oprávnění.

Podporována jsou následující řešení:

- Barracuda
- Fortinet FortiGate
- PaloAlto

## **Kontrola na základě přenosové rychlosti**

PacketFence může automaticky kontrolovat přenosovou rychlost využívanou jednotlivými zařízeními. S podporou upozornění umožňuje omezit nebo úplně zakázat přístup zařízením, která využívají příliš velkou část z dostupné přenosové rychlosti během určitého časového úseku. Také lze ukládat záznamy o množství přenesených dat, a na základě těchto informací například omezit přístup uživatelům, kteří neúměrně zatěžují síťovou infrastrukturu.

## **Pass-Through**

Přístup k vybraným zdrojům jako jsou například aktualizace nebo jiné specifické nástroje lze garantovat i v případě, že je zařízení v izolaci.

## **Plovoucí síťová zařízení**

Mezi plovoucí zařízení patří přepínače a přístupové body. Tato zařízení lze přemísťovat v rámci sítě a připojovat k přístupovým portům. V případě, že je vše správně nakonfigurováno, PacketFence rozpozná takové zařízení a aktivuje příslušné VLAN a MAC adresy. V okamžiku odpojení PacketFence opět nastaví vše do původního stavu.

## **Integrace Microsoft Active Directory**

PacketFence umožňuje použití webových služeb, které jsou vyhrazeny pouze pro Windows PowerShell skripty. Obsahuje skripty pro automatické smazání registrace zařízením, která byla v Active Directory uživatele který byl zablokován nebo smazán.

## **Směrované Sítě**

Architektura PacketFence umožňuje, aby byl server umístěn v data centru, a i přesto efektivně zabezpečoval pobočky rozmístěné po celém světě.

## Flexibilní autentizace

PacketFence umožňuje použití několika autentizačních protokolů. To umožňuje přizpůsobit přihlašování tak, aby si uživatelé nemuseli vytvářet nové přihlašovací jméno a heslo.

Podporovány jsou tyto autentizační zdroje:

- LDAP
  - Microsoft Active Directory
  - Novell eDirectory
  - OpenLDAP
  - Další kompatibilní LDAP servery
- RADIUS
  - Cisco ACS
  - RADIUS (FreeRADIUS, Radiator, atd.)
  - Microsoft NPS
  - Další kompatibilní RADIUS servery
- Lokální uživatelský soubor (Apache htpasswd formát)
- OAuth2
  - Facebook
  - Google
  - GitHub
  - LinkedIn
  - Microsoft Live

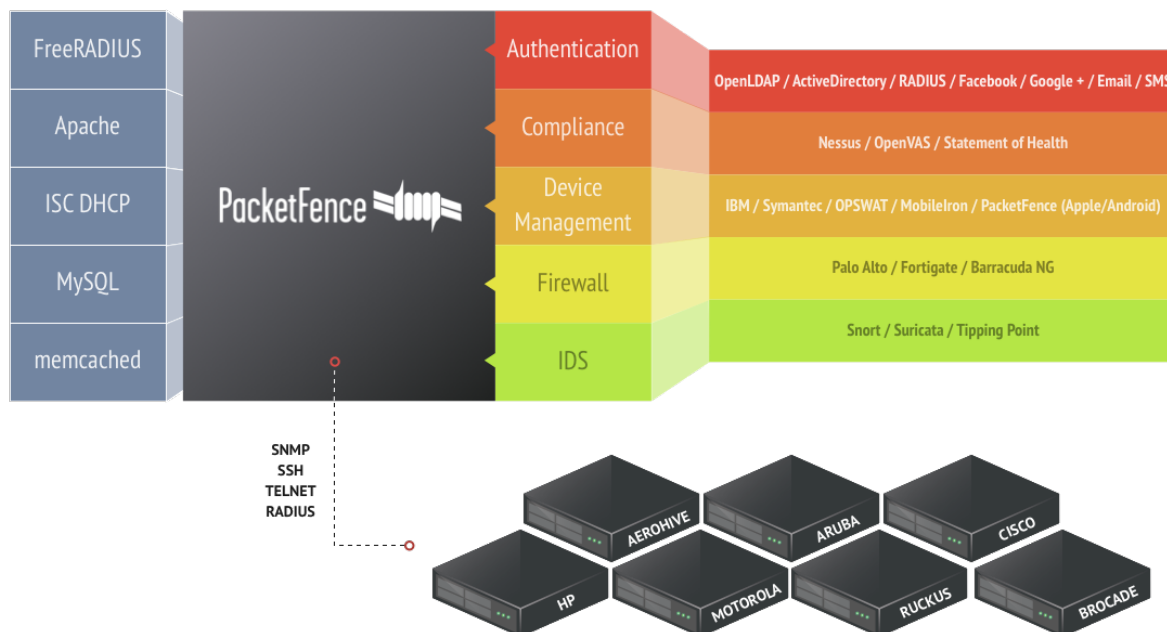
Dále je možné využít interní SQL databázi pro autentizaci lokálně vytvořených uživatelů.

## Postupné zavádění

Vzhledem k tomu, že NAC může být v případě špatné implementace spíš na obtíž, lze PacketFence zavádět do firemní sítě postupně. Je proto možné postupovat rychlostí, která nejlépe vyhovuje konkrétnímu prostředí. Například lze zapojit pouze jeden přepínač, jedno podlaží nebo jednu budovu. Stejně možnosti máme i u funkcí, které slouží k izolaci. Nejdřív lze zapnout pouze upozornění na nežádoucí aktivitu a teprve ve chvíli, kdy se ověří, že je vše nastaveno správně, se zapne VLAN izolace.

## 3.6 Komponenty

V této kapitole jsou popsány vybrané komponenty, které PacketFence využívá ke zprostředkování svých funkcí. Jsou zde převážně open source řešení, přestože PacketFence podporuje také integraci některých komerčních řešení.



Obr. č. 9: Souhrn komponentů PacketFence [17]

### FreeRADIUS

Jedná se o zdarma volně šiřitelnou verzi RADIUS serveru, která je distribuována pomocí GNU GPL licence. Podporuje všechny běžně využívané autentizační protokoly a obsahuje webové rozhraní založené na PHP nazývané dialupadmin. Je využíván velkým množstvím společností z Fortune-500 nebo Tier 2 ISP. Také je velice často využíván na akademické půdě, včetně sítě eduroam. Mezi podporované databáze patří LDAP, MySQL, PostgreSQL, Oracle a mnoho dalších. Dále podporuje všechny běžně užívané EAP autentizační typy, včetně PEAP a EAP-TTLS. Ve verzi 2.0.0 byla přidána podpora IPv6 a VMPS.[18]

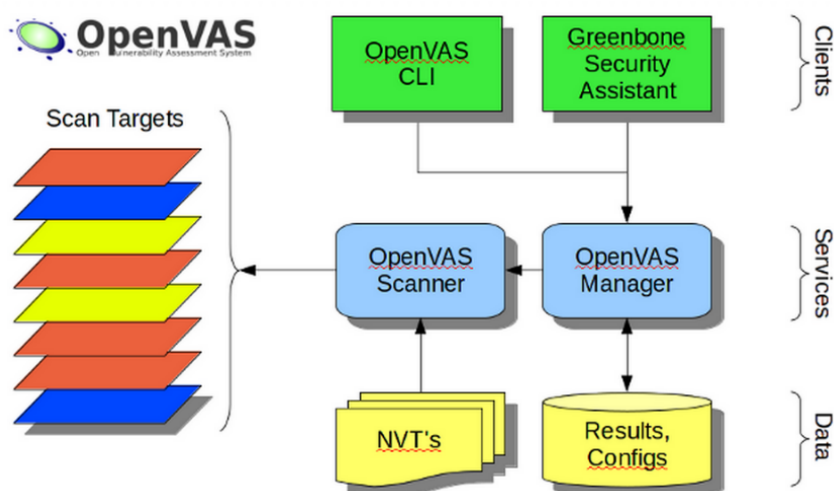
### Nessus

Nessus je komerčním lídrem v oblasti skenování zranitelností. Je schopen identifikovat zranitelnosti, snížit riziko a zajistit odpovídající stav virtuálních, mobilních a cloudových prostředí. Poskytuje analýzu zranitelností, detekci malwaru, správu aktualizací nebo průzkum citlivých dat. Je nabízen ve dvou variantách, a to pro jednotlivce za 1500\$/rok a pro firmy za 5000\$/rok.[19]

- Skenování bez nutnosti instalace agenta na cílovém zařízení
- Rozdělení zranitelností do skupin na základě CVE (Critical, High, Medium, Low, Info)
- Flexibilní formát výsledků (XML, PDF, HTML, CSV)
- Odesílání výsledků emailem
- Sdílení výsledků (vyžaduje firemní verzi)

## OpenVAS (Open Vulnerability Assessment Systém)

Jedná se o spojení několika služeb a nástrojů, které nabízejí velice účinný skener zranitelností. Také lze pomocí OpenVAS tyto zranitelnosti účinně spravovat. Samotný bezpečnostní skener je doprovázen denně aktualizovaným zdrojem zranitelností Network Vulnerability Tests (NVTs), který obsahuje více než 35 000 záznamů (platí pro Duben 2014). Všechny produkty OpenVAS jsou zcela zdarma a jsou licencovány pomocí GNU GPL.[20]



Obr. č. 10: Architektura OpenVAS [21]

- Lze skenovat velké množství zařízení současně
- Naplánování skenování
- Zastavení, pozastavení a obnovení skenování
- Uživatelská správa

## Snort

Jedná se o zdarma volně šiřitelný síťový systém pro prevenci narušení (NIPS) a zároveň také síťový systém pro detekci narušení (NIDS). Umožňuje analýzu síťového provozu v reálném čase v IP sítích. Provádí analýzu protokolu, prohledává a kontroluje, zda odpovídá obsah kontrolovaných dat. Lze ho také využít k detekci útoků jako je tajné skenování portů nebo překročení velikosti bufferu. Přímě na stránkách [snort.org](http://snort.org) jsou k dispozici verze pro operační systémy Windows, Fedora, Centos a FreeBSD.[22]

## Suricata

Stejně jako Snort se jedná o NIPS a NIDS systém. Je podporován operačními systémy Linux, FreeBSD, OpenBSD, Mac OS X a Windows. Pomocí Suricata lze detekovat nebezpečné chování síťových zařízení, zranitelnosti a známé hrozby. Nemá problém s kontrolou více gigabitových provozů. V případě, že jsou požadovány náročné úkony lze využít i výkon grafické karty. Automaticky jsou detekovány protokoly jako například HTTP na kterémkoli portu a uplatní se odpovídající detekční pravidla. To značně napomáhá detekci malwaru a CnC kanálů.[23]

## 4 Praktická část

V rámci praktické části bude předvedena funkčnost NAC ve virtuálním prostředí s využitím GNS3. Budeme konfigurovat inline variantu PacketFence, která je vhodná hlavně pro menší organizace, ve kterých nejsou k dispozici servisovatelné přepínače. VLAN enforcement varianta PacketFence je pokročilejší a původně zvažovaná, ale vzhledem k problémům s jejím nasazením s dostupnými prostředky jsme jí museli opustit. Problém je pravděpodobně způsoben tím, že při instalaci ve virtualboxu dochází při komunikaci mezi přepínačem a serverem k odstranění VLAN tagů. K tomuto závěru jsme došli po řadě testů a sledování komunikace pomocí nástroje Wireshark. Z tohoto důvodu nebylo možné úspěšně zprovoznit VLAN enforcement variantu. Využita tedy bude inline varianta pro demonstraci základních funkčních prvků NAC.

Během našich testů jsme používali PacketFence 5.0.1 ve variantě ZEN. Tato varianta je předkonfigurována pro nasazení ve virtuálním prostředí. Při importu je v základu nastaveno 8 GB RAM. Velikost operační paměti jsme snížili na 4 GB, jelikož host, na kterém jsme virtuální zařízení provozovali, měl pouze 8 GB RAM. Bylo třeba nechat rezervu pro jeho vlastní operační systém a také bylo nutné během testů spouštět další virtuální stroje. V případě, že snížíme hodnotu pod 4 GB RAM, dochází k problémům s provozem některých služeb.

### 4.1 Rozdíl mezi VLAN a Inline enforcement

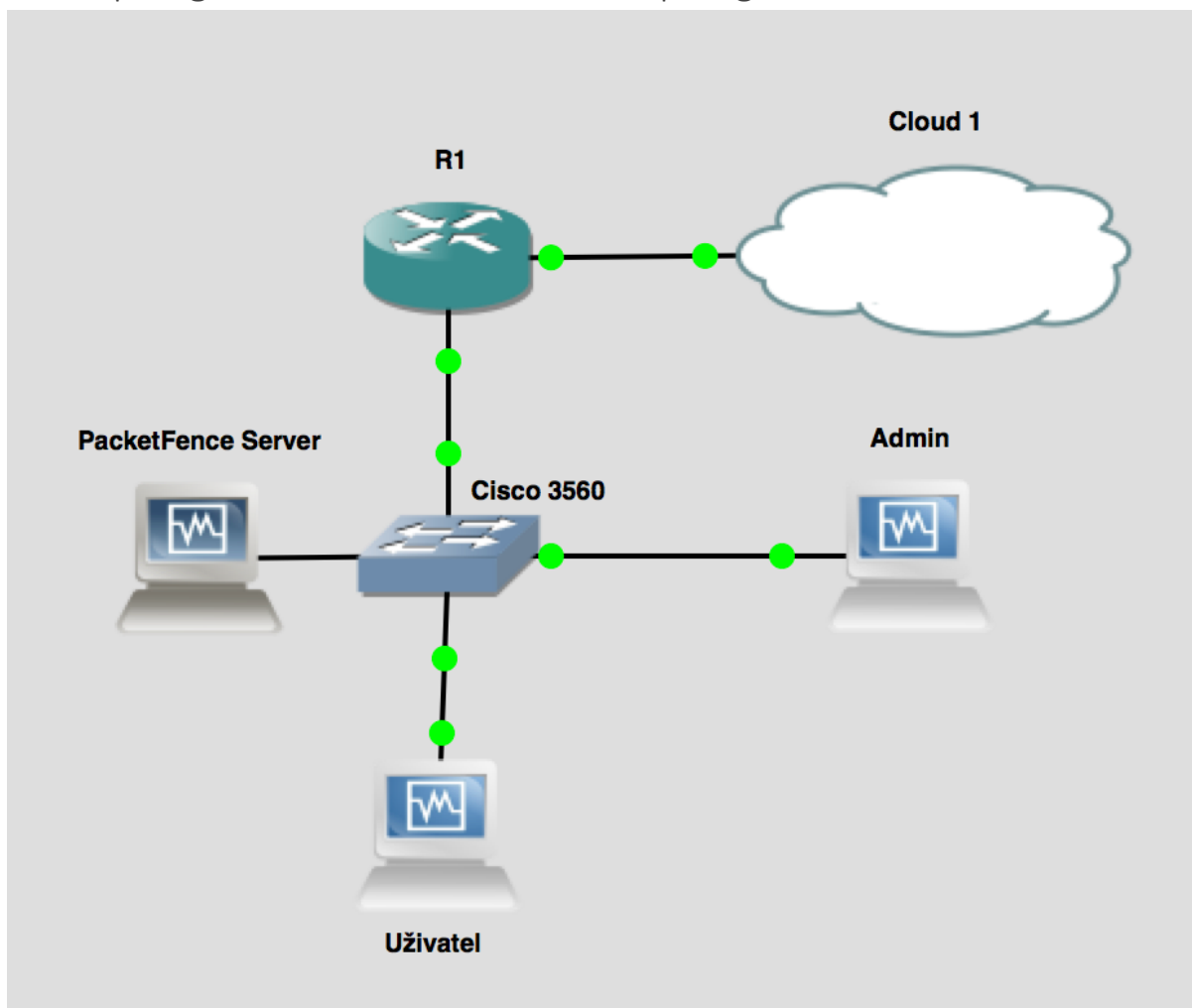
#### **VLAN enforcement**

Tato varianta nasazení je doporučována v případě, že máme k dispozici přepínače, které podporují protokol 802.1X a jedná se tedy o vyšší třídu síťových zařízení. Používá se hlavně ve větších organizacích se složitou síťovou infrastrukturou. Základní konfigurace počítá minimálně se třemi VLAN. Jedna z nich je registrační, do té jsou připojena všechna zařízení, která se poprvé pokouší připojit do sítě. Při pokusu o načtení webových stránek v prohlížeči je uživatel přesměrován na captive portál, pomocí kterého lze zadat přihlašovací údaje. Případně je možné, pokud je to požadováno, nastavit vlastní registraci. V případě schválení přístupu je zařízení přesunuto do základní VLAN, ve které má přístup jak k internetu, tak do firemní sítě. Poslední požadovaná VLAN je izolační. Do té je zařízení přesunuto v případě, že neodpovídá požadavkům pro přístup. Jako volitelná možnost je nastavení hostovské VLAN, ve které má zařízení přístup pouze na internet.

#### **Inline**

V této variantě nasazení prochází veškerá komunikace mezi lokální sítí a internetem skrz PacketFence server. Není nutné nastavovat žádné VLAN, ale je potřeba připojit server pomocí dvou konektorů tak, že jeden je v lokální síti a druhý je připojený k internetu. Nevýhodou této varianty je, že jsou veškerá zařízení na stejné L2 vrstvě. Výhodou je mnohem jednodušší konfigurace a cena přepínačů. Lze využít všechny běžně používané přepínače bez pokročilých funkcí a protokolů.

## 4.2 Topologie sítě: VLAN enforcement topologie



Obr. č. 11: VLAN enforcement topologie

Na obrázku je zobrazena topologie, kterou jsme konfigurovali. Jedná se o Router R1, který je připojen ke cloudu a pomocí trunk portu na přepínači je připojen Cisco 3560. K přepínači je pomocí trunk portu připojen také PacketFence server a jsou na něm nakonfigurovány potřebné VLAN. Dále jsou k přepínači připojeni uživatelé a jeden počítač sloužící k administraci. Topologii lze snadno rozšířit přidáním dalších přepínačů.

## Konfigurace síťových prvků: VLAN enforcement

Tabulka použitých VLAN:

VLAN	ID
Registrace	2
Izolace	3
Základní	10

Tabulka č. 2: Použité VLAN

### Konfigurace přepínače Cisco 3560

Pro naší úvodní konfiguraci je potřeba na přepínači vytvořit mimo nativní VLAN další 3 VLAN. K vytvoření VLAN je potřeba být v modu globální konfigurace, do kterého se dostaneme zadáním příkazu `configure terminal`.

Následně zadáme příkaz:

```
vlan 10
```

Pro vytvoření VLAN s ID 10. U všech ostatních VLAN tento postup zopakujeme.

Dalším krokem, který je na přepínači potřeba nakonfigurovat, jsou dva trunk porty, kterými bude procházet komunikace mezi switchem a PacketFence serverem + switchem a routrem. Příkazy pro vytvoření těchto portů jsou:

```
int fastEthernet 0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 1,2,3,10

int fastEthernet 0/23
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 1,2,3,10
```

Pro správu přepínače pomocí PacketFence ještě přidáme IP adresu

```
vlan 1
ip address 192.168.1.15 255.255.255.0
```

## Konfigurace routeru

Jako první na routeru nakonfigurujeme DHCP tak, aby každé zařízení, které připojíme ke switchy, dostalo odpovídající adresu. Nastavení DHCP je provedeno těmito příkazy:

(x nahrazuje VLAN ID a je použito pro zkrácení zápisu tak, že všechny příkazy obsahující x je nutno zadat pro všechny VLAN)

```
service dhcp
ip dhcp pool vlanx
network 192.168.x.0 255.255.255.0
ip dhcp excluded-address 192.168.x.1
```

Dále je na routeru zapotřebí nakonfigurovat virtuální rozhraní.

```
interface fa0/0
no shut
interface fa0/0.x
encapsulation dot1q x
ip address 192.168.x.1 255.255.255.0
```

Pro přístup naší síťové topologie k internetu je potřeba na routeru nastavit NAT

```
interface fastethernet0/0.1
ip nat inside
interface fastethernet0/0.10
ip nat inside
interface fastethernet0/1
ip nat outside
ip address dhcp
no shutdown
exit
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
access-list 100 permit ip 192.168.10.0 0.0.0.255 any
ip nat inside source list 100 interface fastethernet0/1 overload
```

## Konfigurace 802.1X a MAB

Než začneme konfigurovat 802.1X a MAB, je důležité se ujistit, že máme na přepínači vytvořený účet, pomocí kterého se budeme přihlašovat. Po konfiguraci 802.1X je totiž vyžadováno přihlášení a v případě, že není účet vytvořen, se nelze připojit. Zroveň také nakonfigurujeme vzdálený přístup.

```
line vty 0 15
login local
password cisco
username cisco privilege level 15 password cisco
```

Zadáním následujících příkazů nakonfigurujeme ověřování pomocí 802.1X. Jako záložní varianta je použit MAB.

```
dot1x system-auth-control
int range fa0/3-20
    switchport mode access
    authentication order dot1x mab
    authentication priority dot1x mab
    authentication port-control auto
    authentication periodic
    authentication timer restart 10800
    authentication timer reauthenticate 7200
    mab
    no snmp trap link-status
    dot1x pae authenticator
    dot1x timeout quiet-period 2
    dot1x timeout tx-period 3
exit
aaa new-model
aaa group server radius packetfence
server 192.168.1.3 auth-port 1812 acct-port 1813
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
```

```
radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 timeout 2 key SilneHeslo
radius-server vsa send authentication
aaa server radius dynamic-author
client 192.168.1.3 server-key SilneHeslo
port 3799
snmp-server community public RW
```

### 4.3 Konfigurace PacketFence: VLAN enforcment

Konfigurace PacketFence se pro varianty inline a VLAN enforcment liší pouze v prvních dvou krocích, a proto je zde popíšeme, další čtyři přeskočíme. Všechny kroky jsou podrobně popsány v následující části, ve které je popsán postup pro konfiguraci inline módu, který jsme nakonec z dříve zmíněných důvodů použili.

#### Krok 1: Způsob nasazení

Zvolíme VLAN enforcment.

#### Krok 2: Sítě

Nejprve nesmíme zapomenout přiřadit rozhraní eth0 do management sítě.

```
eth0: Management
eth0 VLAN 2: Registration
eth0 VLAN 3: Isolation
```

Následně vytvoříme 3 VLAN.

```
Virtual LAN ID: 2
IP Address: 192.168.2.10
Netmask: 255.255.255.0

Virtual LAN ID: 3
IP Address: 192.168.3.10
Netmask: 255.255.255.0

Virtual LAN ID: 10
IP Address: 192.168.10.10
Netmask: 255.255.255.0
```

## Síťová zařízení

V administrativní části PacketFence serveru je třeba přidat přepínač. To lze udělat v položce configuration/Network/Switches. Po přidání nového switchu vyplníme hodnoty podle následujícího příkladu. Položky, které nejsou zmíněny, necháme beze změny.

### Definition

IP: 192.168.1.15  
Description: Cisco Catalyst 3560  
Type: Cisco::Catalyst\_3560  
Mode: Production  
Deauthentication: RADIUS  
Dynamic Uplinks: Označeno

### Roles

Role by VLAN ID: checked  
registration VLAN: 2  
isolation VLAN: 3  
default: 10

### Radius

Secret Passphrase: SilneHeslo

### Snmpp

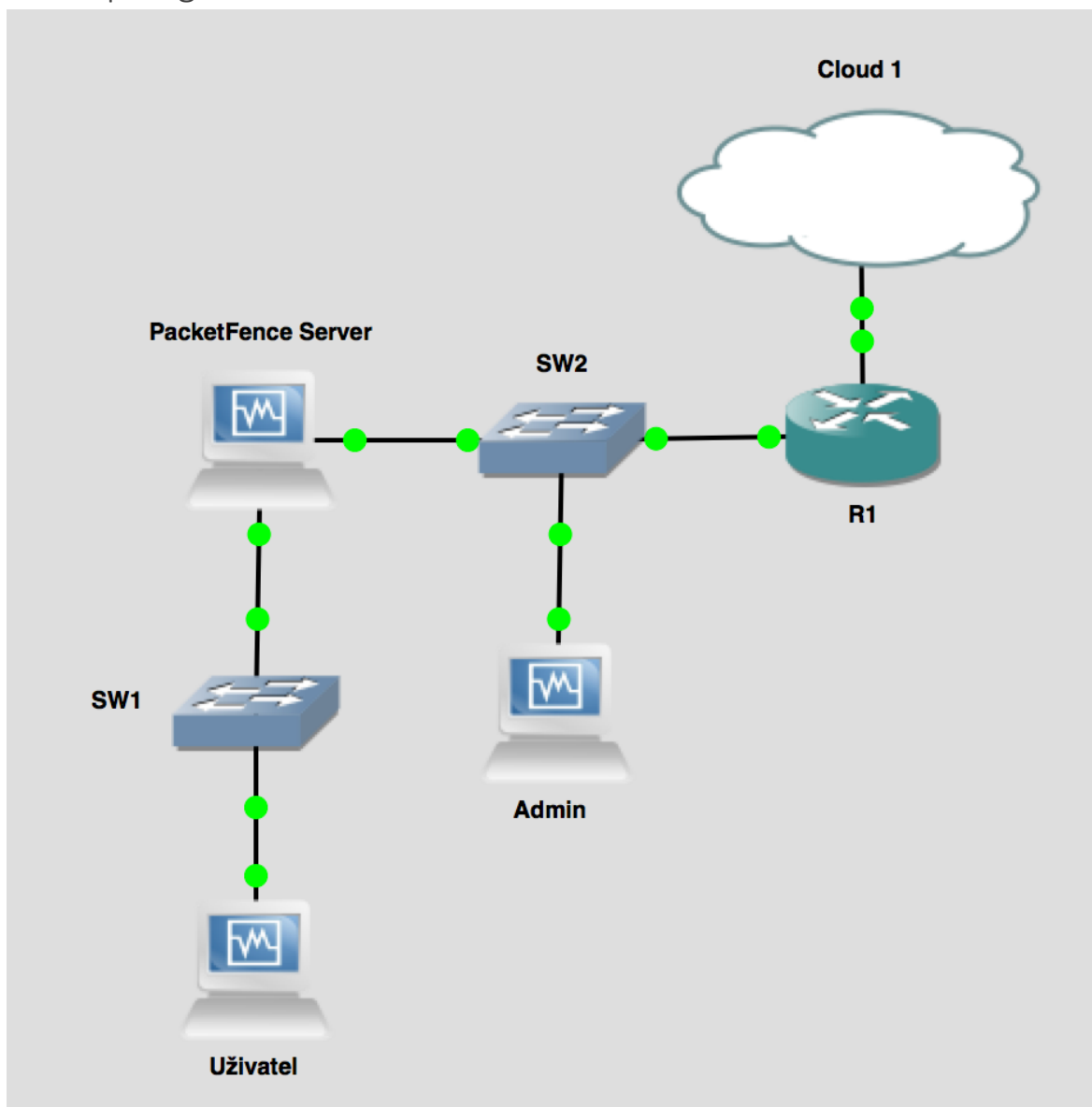
SNMP Version: 2c  
SNMP Read Community: ciscoRead  
SNMP Write Community: ciscoWrite

## Ověření konfigurace

Jak již bylo zmíněno, ověření správné konfigurace jsme nemohli provést s největší pravděpodobností z důvodu problému s VLAN tagy na síťovém rozhraní serveru. Uvedeme zde proto postup, pomocí kterého se ověří správná konfigurace v případě, že tento problém nenastane.

- Připojíme nezaregistrované zařízení.
- Ověříme, zda PacketFence obdrží autentizační žádost od přepínače.
- Ověříme, že port, ke kterému je zařízení připojeno, byl přiřazen do VLAN 2.
- Na zařízení otevřeme prohlížeč.
- Pokusili jsme se připojit k HTTP stránce (nikoli HTTPS, například <http://www.google.com>).
- Ověřili jsme, že bez závislosti na požadované stránce jsme vždy přesměrováni na captive portal, ve kterém je požadováno přihlášení.
- Přihlásíme se pomocí předem vytvořených uživatelských údajů.
- Zkontrolujeme, že port, ke kterému je zařízení připojeno, byl přiřazen do VLAN 10.
- Ověříme, že máme volný přístup k internetu.

#### 4.4 Topologie virtuální sítě: Inline



Obr. č. 12: Inline topologie

Základní topologie inline varianty je zobrazena na obrázku číslo 12. Jedná se o Router R1 připojený k internetu. K routeru je připojen switch, který je v části, která slouží pro management topologie. K tomuto přepínači je připojen počítač, ze kterého je prováděna konfigurace PacketFence a zároveň je připojen také samotný PacketFence server. K PacketFence serveru je připojen další přepínač, který je již součástí lokální sítě. K tomuto přepínači již jsou přímo připojeni uživatelé případně další přepínače.

## 4.5 Konfigurace síťových prvků: Inline

Pro demonstraci konfigurace PacketFence jsme použili operační systém OS X 10.10.3 a program pro virtualizaci síťových zařízení GNS3 verze 1.3.1. PacketFence server a všechny další zařízení používané v prostředí GNS3 jsou virtualizovány ve VirtualBoxu verze 4.3.26.

Jako první je potřeba vytvořit virtuální rozhraní na fyzickém stroji, ke kterému bude připojena virtuální síť v GNS3. K tomu jsme použili TunTap, který vytvoří několik virtuálních rozhraní. Jednomu z těchto rozhraní nastavíme IP adresu a nastavíme NAT tak, aby byla možná komunikace mezi GNS3 a internetem. To vše nastavíme pomocí následujícího skriptu:

```
#!/bin/bash
#konfigurace tap0 (virtuální rozhraní vytvořené pomocí TunTap)
ifconfig tap0 100.100.100.1 netmask 255.255.255.0 up
#aktivace packet forwarding
sudo sysctl -w net.inet.ip.forwarding=1
sudo sysctl -w net.inet.ip.fw.enable=1
#konfigurace a zapnutí NAT
# parametr -d slouží k deaktivaci packet filtru
pfctl -d
# pomocí parametru -F smažeme všechna aktuálně nastavená pravidla
pfctl -F all
# konečně pomocí -f nahrajeme soubor pfrule ve, kterém jsou definována námi
# požadovaná pravidla
# -e znovu aktivuje packet filtr
pfctl -f ./pfrule -e
```

Soubor pfrule obsahuje konfiguraci NAT.

```
nat on en0 from tap0:network to any -> (en0)
pass inet proto icmp all
pass in on tap0 proto udp from any to any port domain keep state
pass quick on en0 proto udp from any to any port domain keep state
```

Tím je dokončena konfigurace přímo na fyzickém zařízení a lze se přesunout ke konfiguraci virtuálních zařízení v GNS3. Nejprve vložíme cloud. Otevřeme jeho konfiguraci a přejdeme na položku NIO TAP. Zde vložíme námi nakonfigurovaný Tap0. Je důležité tuto volbu potvrdit, jinak se neprojeví. Nyní již můžeme přidat router a propojit ho s cloudem. V případě, že GNS3 zahlásí chybu, která hlásí že nemáme oprávnění toto spojení provést, máme dvě možnosti. Můžeme změnit uživatele, který je oprávněn používat rozhraní Tap0 nebo spustit GNS3 jako root pomocí následujícího příkazu:

```
user$ sudo /Applications/GNS3.app/Contents/MacOS/GNS3
```

V momentě kdy máme propojený cloud a router, můžeme přejít ke konfiguraci routeru.

```
conf t
interface FastEthernet0/0
  ip address 100.100.100.254 255.255.255.0
  ip nat outside
  no shutdown
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
  no shutdown
exit
ip route 0.0.0.0 0.0.0.0 100.100.100.1
ip domain-lookup
ip forward-protocol nd
ip name-server 8.8.8.8
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
access-list 100 permit ip 192.168.2.0 0.0.0.255 any
ip nat inside source list 100 interface fastethernet0/0 overload
service dhcp
ip dhcp pool management
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 8.8.8.8
ip dhcp excluded-address 192.168.1.1
```

Rozhraní FastEthernet 0/0 nastavíme adresu ze stejného rozsahu jako u Tap0. Rozhraní FastEthernet 0/1 bude propojeno se serverem PacketFence a zvolíme mu tedy adresu z rozsahu, který máme určený pro management. Důležité jsou příkazy no shutdown, které zaručí, že budou rozhraní aktivní. Také nastavíme vnitřní a vnější rozhraní pro NAT tak, aby to odpovídalo zapojení. Vytvoříme access list, ve kterém definujeme adresové rozsahy, které mají být pomocí NAT překládány. Nakonec Nastavíme DHCP pro naši management síť tak, aby PacketFence a zařízení, ze kterého budeme PacketFence konfigurovat dostali automaticky adresu.

Otestujeme zda lze z routeru pingnout internet. V případě, že je ping úspěšný, můžeme přejít k vytvoření kompletní topologie.

Pro přidání PacketFence serveru a dalších virtuálních počítačů je potřeba je mít již nainstalované ve VirtualBoxu. V případě, že máme GNS3 zapnutý jako root uživatel, je potřeba mít i VirtualBox zapnutý jako root. Virtuální zařízení se do GNS3 přidávají v položce Preferences/VirtualBox VMs. Zde postupně vyhledáme a přidáme veškeré virtuální stroje požadované v naší topologii. Nyní již máme vše připraveno a můžeme vytvořit topologii tak jak je vidět na obrázku 11.

## 4.6 Konfigurace PacketFence: Inline

V této práci je použita verze PacketFence ZEN 5.0.1, která je distribuovaná pomocí OVA souboru, který lze přímo importovat do VirtualBoxu. Vzhledem k tomu, že je tato verze určena pro import do VMware je potřeba vyřešit problém s neexistujícím rozhraním eth0 při prvním zapnutí. Tento problém lze vyřešit nejrychleji tak, že smažeme soubor.

```
/etc/udev/rules.d/70-persistent-net.rules
```

Následně server restartujeme. Po této úpravě se již rozhraní eth0 načte a je mu přiřazena adresa díky DHCP, které jsme nakonfigurovali na routeru. Po úspěšném nabootování PacketFence zobrazí adresu, kterou od DHCP dostal i s portem 1443. Pomocí [https://PacketFence\\_IP:1443/configurator](https://PacketFence_IP:1443/configurator) se lze připojit k úvodní konfiguraci. K tomu využijeme zařízení v topologii označené jako Admin. Do prohlížeče zadáme adresu a objeví se nám konfigurator, který nás provede pěti kroky základního nastavení.

### Krok 1: Způsob nasazení

Je potřeba zvolit zda chceme inline nebo VLAN enforcement. Případně lze zvolit obojí. Tato volba ovlivní průběh dalšího kroku, a proto je potřeba mít předem určeno kterou možnost chceme zvolit.

V našem případě to bude z dříve uvedených důvodů možnost INLINE.

### Krok 2: Konfigurace Sítě

V tomto kroku je nutné staticky nakonfigurovat rozhraní serveru. DHCP není podporováno.

Webový konfigurator zobrazí všechny aktivní rozhraní serveru. Pokud se zobrazí pouze rozhraní eth0, je potřeba v GNS3 konfiguraci virtuálního stroje druhé rozhraní manuálně přidat. Pro rozhraní eth0 je již IP adresa a maska nakonfigurována díky DHCP z routeru, ale u rozhraní eth1 je tento krok potřeba provést manuálně. V případě, že je z nějakého důvodu potřeba změnit nastavení eth0, lze tak provést, ale je třeba si uvědomit, že se tím také změní IP adresa webového rozhraní pro konfiguraci a bude potřeba ho znovu načíst.

Pro Inline enforcement je třeba zvolit tyto druhy rozhraní:

Management  
Inline layer 2

V našem případě bude rozhraní eth0 sloužit pro management a rozhraní eth1 pro inline vrstvu. Rozhraní eth1 je tedy připojeno k přepínači v lokální síti.

Námi použitá konfigurace:

eth0: Management  
IP Address: 192.168.1.5  
Netmask: 255.255.255.0  
Gateway: 192.168.1.1

eth1: Inline Layer 2  
IP Address: 192.168.2.1  
Netmask: 255.255.255.0  
DNS Servers: 192.168.1.10

### Krok 3: Konfigurace databáze

Tento krok nakonfiguruje MySQL server, který je PacketFencem požadován. Bude vytvořena databáze, schéma a uživatel potřebný k provádění požadovaných operací. V případě, že není spuštěna služba MySQLd, je zde tlačítko, kterým ji lze spustit.

Je zapotřebí vytvořit root heslo MySQL databáze. K jeho zadání se dostaneme kliknutím na tlačítko test bez předchozího vyplnění jiných polí. Pokud vyplníme pole pro heslo při stisku tlačítka, test pouze spustí ověření, zda je heslo správné, což se nemůže stat, protože jsme ho ještě nenastavili. Po kliknutí na tlačítko test tedy dvakrát zadáme silné heslo a potvrdíme naši volbu. Následně toto heslo znovu zadáme a tlačítkem test nyní potvrdíme správnost hesla.

V další sekci se vytvoří databáze a nahraje se do ní požadované schéma. Jednoduše necháme předvyplněné hodnoty a jen potvrdíme vytvoření databáze.

V poslední části je nutné vytvořit uživatele, opět pouze necháme předvyplněný název a zvolíme heslo. Tím se vše automaticky nastaví do konfigurace packetfence, kde lze toto nastavení kdykoliv změnit.

V případě zobrazení zprávy a úspěšném vytvoření všech součástí MySQL database, se můžeme přesunout k dalšímu kroku.

### Krok 4: Konfigurace PacketFence

Tento krok se soustředí na volitelné možnosti instalace PacketFence, které budou ve většině případů odpovídat požadavkům zákazníka.

Především je nutné určit doménu a hostname. Na takto definovanou adresu bude přesměrováno každé zařízení, které se pokusí poprvé připojit do sítě. Zobrazí se mu captive portal, ve kterém po něm bude vyžadováno uživatelské jméno a heslo.

Také je v této části možné zvolit zda budeme chtít hesla uživatelů šifrovat či nikoli.

## Krok 5: Administrace

Zde je zapotřebí vytvořit účet admina, který bude mít přístup do webového rozhraní pro administraci PacketFence. Jednoduše vyplníme požadované uživatelské jméno a heslo.

U tohoto kroku jsme narazili na problem, že nedošlo při pokusu o potvrzení požadavku k odeslání. Vyřešit se to dá restartováním PacketFence serveru a opětovným načtením konfiguratoru. Veškeré předchozí nastavení zůstane uloženo a požadavek na vytvoření účtu pro administrativu se odešle.

## Krok 6: Potvrzení funkčnosti služeb

Jako poslední je zapotřebí nastartovat všechny služby potřebné pro provoz PacketFence. Jednoduše klikneme na tlačítko start a počkáme několik minut. V případě, že vše proběhne v pořádku, budeme přesměrováni do webového rozhraní pro administraci.

V případě, že se nepodaří všechny služby nastartovat, došlo buď k chybnému zadání adres v druhém kroku nebo nemá server dostatečné množství paměti RAM.

## Konfigurační soubory

V případě, že je potřeba změnit konfiguraci, lze tak provést pomocí webového rozhraní nebo úpravou těchto souborů:

conf/pf.conf : Konfigurace jednotlivých služeb PacketFence

conf/networks.conf : Konfigurace síťových rozhraní

Za normálních okolností není potřeba cokoli měnit, aby byl PacketFence funkční. Manuálně tyto soubory upravovat není doporučováno. Vše lze změnit ve webovém rozhraní.

Pro správnou funkci inline módu je ještě zapotřebí, aby byl na serveru aktivní ip\_forwarding. Ten lze v aktivovat úpravou souboru:

/etc/sysctl.conf

Změníme hodnotu parametru net.ipv4.ip\_forward z 0 na 1.

# Controls IP packet forwarding

net.ipv4.ip\_forward = 1

## Síťová zařízení

V inline módu je zapotřebí zaručit, že jsou všechna zařízení schopna komunikovat s PacketFence serverem. Je tedy nutné všechny porty přepínačů nastavit následujícím způsobem:

```
interface range [port-range]
  switchport mode access vlan 1
  no shutdown
interface [packetfence_eth1]
  switchport mode access vlan 1
  no shutdown
end
copy running-configuration startup-configuration
```

## Test konfigurace

Nejprve jsme ve webovém rozhraní vytvořili uživatele, se kterým se pokusíme ověřit, zda bude mít přístup do lokální sítě.

Pro otestování procesu, při kterém se nové zařízení přihlašuje do lokální sítě, jsme postupovali následovně:

- Připojili jsme zařízení k přepínači.
- Ověřili jsme, že obdrželo od PacketFence IP adresu ze správného rozsahu.
- Otevřeli jsme webový prohlížeč.
- Pokusili jsme se připojit k HTTP stránce (nikoli HTTPS, například <http://www.google.com>).
- Ověřili jsme, že bez závislosti na požadované stránce jsme vždy přesměrováni na captive portal, ve kterém je požadováno přihlášení.
- Přihlásili jsme se pomocí dříve vytvořených přihlašovacích údajů.
- Ověřili jsme, že se v administrativním webovém rozhraní zařízení zobrazilo jako zaregistrované.
- Ověřili jsme, že zařízení má přístup k internetu.

U tohoto postupu nastal problém, který spočíval v nemožnosti připojení k internetu ani po úspěšné registraci. Problém byl v době vypracování práce hlášen jako chyba více uživatelům a k jeho vyřešení bylo doporučeno restartovat PacketFence server. Tento postup je funkční, ale pro běžné nasazení jistě nevhodný. Znamenalo by to totiž při každé registraci uživatele na určitý čas odpojit od přístupu k internetu všechny ostatní uživatele.

## 4.7 Instalace Suricata a Snort

Před instalací IDS je nutné si vybrat, který z těchto systémů chceme v našem prostředí nasadit, protože ve webové konfiguraci lze zvolit vždy pouze jeden z nich. V následující části je popsána instalace obou těchto detekčních systémů.

### Snort

Pro instalaci Snort stačí zadat tento příkaz:

```
yum install snort
```

Configurační soubor se nachází ve složce `/usr/local/pf/conf` a jmenuje se `snort.conf`. Úprava tohoto souboru je potřebná pouze vzácně. Je důležité, aby se změny neprováděly v souboru `snort.conf`, který je umístěn ve složce `/usr/local/pf/var/conf`, protože všechny tyto změny budou ztraceny po restartu PacketFence serveru.

### Suricata

Suricata není součástí většiny distribucí, a proto ji budeme muset nainstalovat pomocí návodu, který vytvořila OISF [24]. Vzhledem k tomu, že jedinou distribucí, která Suricata podporuje přímo, je Fedora, využijeme její součásti k instalaci na náš systém.

Nejprve pomocí zadání následujícího příkazu nahrajeme Fedore EPEL:

```
sudo rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

Zadáním následujícího příkazu ověříme případně doinstalujeme součásti potřebné pro spuštění Suricaty.

```
sudo yum -y install libpcap libpcap-devel libnet libnet-devel pcre pcre-devel gcc \
gcc-c++ automake autoconf libtool make libyaml libyaml-devel zlib zlib-devel file-devel
```

### Instalace libcap-ng

```
sudo yum -y install python-devel
wget http://people.redhat.com/sgrubb/libcap-ng/libcap-ng-0.6.4.tar.gz
tar -xzf libcap-ng-0.6.4.tar.gz
cd libcap-ng-0.6.4
./configure
make
sudo make install
```

## Suricata

Pomocí následujících příkazů bude nainstalována samotná suricata.

```
wget http://www.openinfosecfoundation.org/download/suricata-2.0.7.tar.gz
tar -xvzf suricata-2.0.7.tar.gz
cd suricata-2.0.7

./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
make
sudo make install
```

Pro instalaci lze využít několika různých verzí automatického nastavení.

```
./configure && make && make install-conf
```

Tato varianta nainstaluje suricatu a automaticky vytvoří všechny potřebné složky a soubor `suricata.yaml`, pomocí kterého probíhá nastavování suricaty.

```
./configure && make && make install-rules
```

Tato varianta nainstaluje suricatu a automaticky stáhne aktuálně dostupnou sadu pravidel, které budou používány.

```
./configure && make && make install-full
```

Tato možnost kombinuje obě předchozí varianty a dojde tedy jak ke stažení pravidel, tak k vytvoření potřebných složek i souboru `suricata.yaml`.

Pro spuštění zadáme

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth1 --init-errors-fatal
```

## 4.8 Pravidla IDS

Aby PacketFence reagoval na upozornění generovaná Snortem je zapotřebí tuto reakci správně nastavit. Jinak budou tato hlášení ignorována. Politika porušování pravidel je konfigurována pomocí souboru umístěného na následující adrese:

```
/usr/local/pf/conf/violations.conf
```

Obecná forma těchto pravidel vypadá následovně:

```
[1234]
desc= Vlastní popis nažádoucí aktivity
priority=8
template=<template>
enable=Y
trigger=Detect::2200032,Nessus::11808
actions=email,log,trap
vlan=isolationVlan
whitelisted_categories=
```

## Popis:

**[1234]** – Jedná se o ID pravidla. Lze zvolit libovolný integer s výjimkou 120000-120099. Tento rozsah je rezervován pro administrativu.

**desc** – Jedná se o jednořádkový popis daného pravidla

**priority** – V rozsahu od 1-10. 1 je nejvyšší priorita a 10 nejnižší. V případě, že host aktivuje více než jedno pravidlo, bude pořadí jejich vykonání odpovídat právě přiřazené prioritě.

**template** – Jméno templatu používaného během doby kdy host aktivuje pravidlo. Musí odpovídat názvu HTML souboru bez přípony, který se nachází ve složce violations templates.

**enable** – Lze nastavit buď N nebo Y. V případě, že je nastaveno N, nebude pravidlo aktivní. Pokud nastavíme Y aktivujeme tím pravidlo.

**trigger** – Tento parametr slouží k odkazu na externí detekční službu. Formát parametru je typ:ID. Mezi typy patří Detect(Snort), Nessus, OpenVAS, OS, UserAgent, VendorMAC a další. V uvedeném příkladě se jedná o Snort ID 2200032 a 11808 je číslo pluginu Nessus. ID pravidla nemusí odpovídat Snort ID.

**actions** – Jedná se o seznam akcí, které jsou provedeny v případě aktivace pravidla.

log – záznam do určené složky

email – odeslání upozornění na předem definovanou emailovou adresu

trap – umístění hosta do izolace po dobu aktuálnosti pravidla, ve chvíli kdy host přestane porušovat pravidlo, je opět připojen do sítě

close – vypnutí určitého pravidla definovaného pomocí ID

role – změna role zařízení

autoreg – zaregistrování zařízení

unreg – odregistrování zařízení

vlan – v případě použití VLAN enforcement definuje do jaké VLAN má být zařízení přesunuto

V rámci violations.conf je také definována sekce se základním nastavením. V této sekci jsou definovány hodnoty jednotlivých parametrů, které budou nastaveny v případě, že u pravidla nejsou zmíněny.

Základní definované parametry jsou:

```
[defaults]
priority=4
max_enable=3
actions=email,log
auto_enable=Y
enable=N
grace=120m
delay_by=0
window=0
vclose=
target_category=
button_text=Enable Network
snort_rules=local.rules,bleeding-attack_response.rules,bleeding-
exploit.rules,bleeding-p2p.rules,bleeding-scan.rules,bleeding-virus.rules
vlan=isolationVlan
whitelisted_categories=
```

**max\_enable** – určí počet možností pro uživatele odkliknout upozornění na porušení pravidla

**auto\_enable** – určí zda uživatel má možnost sám požádat o povolení přístupu nebo musí požádat help desk

**grace** – časový interval mezi deaktivací izolace a opětovným zákazem v případě, že stále dochází k jeho porušování.

**delay\_by** – nastavení času, který uplyne mezi detekcí porušení pravidla a aktivací příslušných akcí

**Window** – nastavení časového rozmezí, po kterém bude uživatel znovu připojen do sítě, toho lze využít například pokud nastavíme omezení na množství přenesení dat, v okamžiku kdy bude limit překročen dojde k izolaci uživatele a opět bude připojen, například první den nového měsíce

**target\_category** – v případě aktivace akce **role**, bude zařízení přesunuto do skupiny definované v tomto parametru

**button\_text** – text, který bude zobrazen uživateli na tlačítku pro obnovení přístupu

**snort\_rules** – adresa k souboru, který obsahuje snort pravidla

## Příklady pravidel:

Na obrázku č.12 je praktická ukázka pravidel ze souboru violations.conf. Jedná se o detekci LSASS zneužití. Při jeho aktivaci je zařízení přesměrováno na uvedenou adresu. Druhý příklad slouží pro detekci Trojanu. V případě aktivace tohoto pravidla je zařízení odpojeno od lokální sítě, je odeslán informační email a záznam je uložen do logu.

```
[2000032]
desc=LSASS Exploit
priority=4
template=lsass
redirect_url=/proxies/tools/stinger.exe
enabled=N
trigger=Detect::2000032,Detect::2000033,Detect::2000046,Detect::2001286,Detect::
2001337,Detect::2001302

[2002030]
desc=IRC Trojan
priority=3
auto_enable=N
template=trojan
enabled=N
trigger=Detect::2002029,Detect::2002030,Detect::2002031,Detect::2002032,Detect::
2002033,Detect::2000345,Detect::2000347,Detect::2000348,Detect::2000349,Detect::
2000350,Detect::2000351,Detect::2000352
actions=trap,email,log
```

Obr č. 13: Snort Pravidla

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS (msg:"GPL SQL create_m
view_repgroup ordered fname buffer overflow attempt"; flow:to_server,established
; content:"dbms_repat.create_mvview_repgroup"; nocase; pcre:"/((\s*(\x27[\^\\\x27
l*'|\x22[\^\\\x22]|\x22)\s*,){4}\s*((\x27[\^\\\x27]{1000})|(\x22[\^\\\x22]{1000}))/Rmsi"
; reference:url,www.appsecinc.com/Policy/PolicyCheck633.html; classtype:attempte
d-user; sid:2102604; rev:3;)
```

Obr č. 14: Suricata SQL pravidlo

```
#by matt jonkman and waldo kitty
#
alert udp $EXTERNAL_NET 123 -> $HOME_NET 123 (msg:"ET DOS Potential Inbound NTP
denial-of-service attempt (repeated mode 7 reply)"; dsize:4; content:"!97 00 00
00!"; threshold:type limit, count 1, seconds 60, track by_src; reference:url,www
.kb.cert.org/vuls/id/568372; reference:cve,2009-3563; reference:url,doc.emerging
threats.net/2010487; classtype:attempted-dos; sid:2010487; rev:2;)
```

Obr č. 15: Suricata DoS pravidlo

Na obrázcích 13 a 14 jsou ukázky pravidel, která byla stažena během instalace Suricaty. V případě obrázku číslo 13 je se jedná o detekci pokusu přehlcení buferu SQL. Toto pravidlo je umístěno v souboru emerging-sql.rules. Obrázek číslo 14 je ukázkou jednoho z mnoha pravidel uložených v souboru emerging.dos.rules a slouží k detekci DOS útoků.

K otestování funkčnosti Suricaty jsme vytvořili vlastní pravidlo na detekci HTTP (Hyper Text Transfer Protocol) provozu.

```
alert http any any -> any any (msg:"Testovací pravidlo  
content:"GET"; nocase; classtype:policy-violation; sid:1; rev:1;)
```

Po aktivaci tohoto pravidla jsme na jednom z virtuálních strojů zapnuli webový prohlížeč a načetli několik webových stránek. Při otevření souboru fast.log se jsme zjistili, že pravidlo funguje a úspěšně zachytilo HTTP provoz. Během těchto testů jsme narazili na problém, při kterém se nám soubor fast.log zaplnil upozorněními o chybném součtu packetu. Tento problém lze vyřešit tak, že při zapínání Suricaty přidáme parametr `-k none`.

V konfiguratoru PacketFence je potřeba aktivovat detekci pomocí Suricaty a také zadat cestu, ve které ji máme nainstalováno. Pro přesměrování upozornění na PacketFence je použit parametr `sid`, který byl u našeho pravidla nastaven na 1. Pomocí výše zmíněného postupu tedy vytvoříme záznam v souboru `violations.conf`. Tím zaručíme, že bude pravidlo detekováno PacketFencem, který provede definované akce.

## 5 Závěr

V této bakalářské práci jsem se seznámil s prostředím kontroly přístupu v počítačových sítích. Tato oblast prošla v posledních letech velkým rozvojem a je jí věnováno hodně pozornosti jak v komerční, tak v open source sféře. Postupem času se jak v komerční tak open source oblasti odělily služby, které byly konkurence schopné, a tak již dnes jistá část variant není nebo nebude v blízké době oficiálně podporována. PacketFence patří do skupiny těch úspěšných, což lze dokázat například i tím, že poslední aktualizace byla vydána 16.4.2015.

Při snaze o nasazení PacketFence na naší testovací topologii jsem narazil na řadu komplikací. S většinou z nich jsem se úspěšně vypořádal hlavně díky popularitě PacketFence a značné podpoře na veřejně dostupných fórech. Pokud jde o dokumentaci, která je dostupná na webových stránkách PacketFence, lze jednoznačně konstatovat, že každá aktualizace se snaží o její vylepšení. Ve verzi 5.0.1 se tak již jedná o kvalitní materiál, který dobře popisuje postup potřebný k nasazení PacketFence.

Během vypracovávání této práce jsem si úspěšně otestoval prostředí GNS3, pomocí kterého jsem vytvořil virtuální topologii. Díky této virtualizaci jsem mohl testovat PacketFence bez nutnosti přístupu k reálné síťové infrastruktuře. Další nespornou výhodou virtualizace byla možnost vytvoření snímků aktuálního stavu virtuálních strojů. Díky propojení PacketFence s řadou dalších open source projektů jako například Suricata nebo OpenVAS jsem si uvědomil další značnou výhodu tohoto přístupu. Také jsem se ovšem setkal s negativními vlastnostmi, kterými je omezená podpora a častější výskyt chyb než v komerčních projektech. Dále jsem se naučil lépe pracovat v příkazové řádce operačních systémů unixového typu a naučil jsem se jak zálohovat a znovu obnovovat konfiguraci síťových prvků.

Tato práce pro mě byla jedním z prvních projektů v oblasti zabezpečení počítačových sítí a potvrdil jsem si, že je tato oblast velice zajímavá. Rád bych se jí i nadále věnoval. Díky práci na souhrnu dostupných možností jsem si uvědomil jak rychle se tato oblast vyvíjí. Z toho důvodu je pravděpodobně open source varianta velmi dobrou možností. V oblasti, kde se situace mění z roku na rok, jistě není vhodné být svázan s jedním konkrétním řešením. Nutno dodat, že Cisco i další výrobci komerčních řešení, se již snaží mít své technologie provázány s ostatními.

## 6 Seznam zkratek

API – Application Programming Interface

BYOD – Bring Your Own Device

DHCP – Dynamic Host Configuration Protocol

DoS – Denial of service

EAP – Extensible Authentication Protocol

EC – Enforcement Client

EPEL – Extra Packages for Enterprise Linux

ES – Enforcement Server

GNS – Graphical Network Simulator

GNU – GNU's Not Unix

GPL – General Public License

GUI – Graphical user interface

HTTP – Hyper Text Transfer Protocol

IDS – intrusion detection systém

IP – Internet protocol

ISE – Identity Services Engine

LDAP – Lightweight Directory Access Protocol

LSASS – Local Security Authority Subsystem Service

MAB – MAC Authentication Bypass

MySQL – My Structured Query Language

NAC – Network Access Control nebo Network Admission Control

NAP – Network Access Protection

NAT – Network address translation

NIDS – Network Intrusion Detection System

NIPS – Network Intrusion Prevention System

NPS – Network Policy Server

NVT – Network Vulnerability Tests

OpenVAS – The Open Vulnerability Assessment Systém

OSI – Open Systems Interconnection

OVA – Open Virtualization Archive

RAM – Random Access Memory

SHA – system health agent

SHV – system health validator

SNMP – Simple Network Management Protocol

SoH – statement of health

SoHRs – Statement of Health Responses

SSoH – system statement of health

SSO – Single Sign-On

TNC – Trusted Network Connect

URL – Uniform Resource Locator

VLAN – Virtual Local Area Network

VMPS – VLAN Management Policy Server

VoIP – Voice over IP

VPN – Virtual private network

ZEN – Zero Effort NAC

## 7 Seznam obrázků a tabulek

### 7.1 Obrázky:

Obr č. 1: NAP architektura z pohledu klienta	str. 5
Obr č. 2: NAP architektura z pohledu serveru	str. 6
Obr č. 3: Komunikace mezi NAP Agentem a NAP Administration Serverem	str. 7
Obr č. 4: Schéma sítě s podporou Cisco NAC	str. 9
Obr č. 5: Součásti ForeScout CounterACT	str. 10
Obr č. 6: Hlavními komponenty OpenNAC	str. 12
Obr č. 7: Ukázka rozdělení do VLAN pomocí FreeNAC	str. 13
Obr č. 8: Architektura PacketFence	str. 15
Obr č. 9: Souhrn komponentů PacketFence	str. 21
Obr č. 10: Architektura OpenVAS	str. 22
Obr č. 11: VLAN enforment topologie	str. 24
Obr č. 12: Inline topologie	str. 30
Obr č. 13: Snort Pravidla	str. 41
Obr č. 14: Suricata SQL pravidlo	str. 41
Obr č. 15: Suricata DOS pravidlo	str. 41

### 7.2 Tabulky:

Tabulka č. 1: kompatibilita systému Network Sentry	str. 10
Tabulka č. 2: Použité VLAN	str. 25

## 8 Zdroje

- [1] HOFFMAN, Daniel V. Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control. Indianapolis: Wiley Publishing, 2008. ISBN 978-0470238387.
- [2] MICROSOFT. Microsoft NAP [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://msdn.microsoft.com/>
- [3] MS NAP. NAP architektura z pohledu klienta [online]. 2014 [cit. 2015-01-26]. Dostupné z: <https://i-msdn.sec.s-msft.com/dynimg/IC534245.png>
- [4] MS NAP. NAP architektura z pohledu server [online]. 2014 [cit. 2015-01-26]. Dostupné z: <https://i-msdn.sec.s-msft.com/dynimg/IC534246.png>
- [5] MS NAP. Komunikace mezi NAP Agentem a NAP Administration Serverem [online]. 2014 [cit. 2015-01-26]. Dostupné z: <https://i-msdn.sec.s-msft.com/dynimg/IC534243.png>
- [6] CISCO. Cisco NAC [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.cisco.com/go/nac>
- [7] Cisco. Schéma sítě s podporou Cisco NAC [online]. 2014 [cit. 2015-01-26]. Dostupné z: [http://www.cisco.com/assets/prod/sec/images/nac\\_overlay\\_small.jpg](http://www.cisco.com/assets/prod/sec/images/nac_overlay_small.jpg)
- [8] ForeScout CounterACT [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.forescout.com/product/counteract/>
- [9] Forescout. Součásti ForeScout CounterACT [online]. 2014 [cit. 2015-01-26]. Dostupné z: <http://www.forescout.com/wp-content/media/ControlFabric-graphic-brochure.png>
- [10] NETWORK SENTRY [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.bradfordnetworks.com/products/network-sentry/>
- [11] OpenNAC [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.opennac.org/>
- [12] OpenNAC. Hlavními komponenty OpenNAC [online]. 2014 [cit. 2015-01-26]. Dostupné z: [http://www.opennac.org/\\_imaging/stk/pop/content/dms/opennac/diagrams/opennac\\_architecture/document/opennac\\_architecture.png](http://www.opennac.org/_imaging/stk/pop/content/dms/opennac/diagrams/opennac_architecture/document/opennac_architecture.png)
- [13] FreeNAC. Ukázka rozdělení do VLAN pomocí FreeNAC [online]. 2014 [cit. 2015-01-26]. Dostupné z: <http://freenac.net/files/u3/howitworks.jpg>
- [14] FreeNAC [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://freenac.net/>

- [15] PacketFence [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.packetfence.org/>
- [16] PacketFence. Architektura PacketFence [online]. 2014 [cit. 2015-01-26]. Dostupné z: <http://www.packetfence.org/fileadmin/images/pf/network.png>
- [17] PacketFence. Souhrn komponentů PacketFence [online]. 2014 [cit. 2015-01-26]. Dostupné z: <http://www.packetfence.org/fileadmin/images/pf/components.png>
- [18] FreeRADIUS [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://freeradius.org/>
- [19] Nessus [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.tenable.com/>
- [20] OpenVAS [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.openvas.org/>  
Suricata [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://suricata-ids.org/>
- [21] OpenVAS. Architektura OpenVAS [online]. 2014 [cit. 2015-01-26]. Dostupné z: <http://www.openvas.org/img/OpenVAS-7-Structure.png>
- [22] Snort [online]. 2014 [cit. 2014-11-30]. Dostupné z: <https://www.snort.org/>
- [23] Suricata [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://suricata-ids.org>
- [24] Instalace Suricaty [online]. 2014 [cit. 2015-05-15]. Dostupné z: [https://redmine.openinfosecfoundation.org/projects/suricata/wiki/CentOS\\_65\\_Installation](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/CentOS_65_Installation)

## Příloha:

### Podporovaná zařízení

Následující seznam obsahuje zařízení, která jsou kompatibilní s PacketFence. Výrobce rozděluje kompatibilitu těchto zařízení také podle protokolů, se kterými jsou tato zařízení schopna pracovat. Jedná se o SNMP, MAC autentizaci a 802.1X. Pokud není zařízení v níže uvedeném seznamu, neznamená to automaticky, že není schopno s PacketFence spolupracovat. Je velká pravděpodobnost, že spolupracovat bude, pouze ještě nebylo otestováno a nahlášeno jako funkční.

### Podpora přepínačů s bezdrátovou technologií:

Přepínač	SNMP	MAC Authentication	802.1X
AeroHIVE AP Series	x	x	x
Aruba Networks (200, 600 Series, 800, 2400, 3000 Series, 6000)	x	x	x
AnyFi Controller	x	x	
Avaya Wireless controllers		x	
BelAir Networks (Ericsson)	x	x	
Brocade Mobility Wireless LAN controllers	x	x	
Cisco Wireless Services Module (WiSM, WiSM2), WLC (2100, 2500, 4400, 5500)	x	x	x
D-Link DWS 3026	x	x	
Enterasys V2110 wireless controller	x	x	
Extreme Networks Summit Wireless controllers	x	x	
Extricom EXSW Wireless Switches (controllers)	x	x	
HP ProCurve MSM710 Mobility controller	x	x	
Huawei AC6605 wireless controller	x	x	
Juniper (Trapeze) Wireless controllers	x	x	
Meru Networks Wireless controllers	x	x	
Motorola RF Switches (controllers)	x	x	
Ruckus Wireless controllers	x	x	x
Xirrus WiFi Arrays	x	x	x

Tabulka 2: Podpora přepínačů s bezdrátovou technologií

Seznam podporovaných přístupových bodů:

AeroHIVE AP Series, Cisco 1130AG, Cisco 1240AG, 1250, D-Link DWL Access Points, HP ProCurve, OpenWRT with hostapd, Xirrus WiFi Arrays

**Podpora Přepínačů bez bezdrátové technologie:**

Přepínač	SNMP	MAC Authentication	802.1X
3COM NJ220, SS4200, SS4500	x		
3COM 4200G,E4800G,E5500G	x	x	x
Accton ES3526XA,ES3528M	x		
Allied Telisis AT8000GS		x	x
Amer SS2R24i	x		
Avaya (see Nortels)	x		
Brocade ICX64XX,ICX66XX,FCXXXXXX,FI-SXXXX		x	x
Brocade FastIron 4802	x		
Cisco 2900XL,2900XL,3500XL Series,ISR 1800 Series	x		
Cisco 2950	x		x
Cisco 3550,3560,3750,4500,6500	x	x	x
Dell PowerConnect 3424	x		
Dell/Force 10		x	x
D-Link DES3526,DES3550	x		
D-Link DGS3100,DGS3200		x	x
Edge-corE 4510		x	
Enterasys D2	x	x	
Enterasys Matrix N3,SecureStack C2,SecureStack C3	x		
Extreme Networks Summit (XOS)	x	x	x
Extreme Networks EAS		x	x
HP E4800G,E5500G,Procurve 2500,2600,5300 a 5400 Series	x	x	x
HP Procurve 3400cl a 4100 Series	x		
HP/H3C S5120		x	x
Huawei S2700,S3700,S5700,S6700,S7700,S9700		x	x
Intel Express 460 a 530	x		
Juniper Networks EX Series		x	x
LG iPecs Series	x	x	x
Linksys SRW224G4	x		
Netgear FGS Series	x		
Nortel BayStack 470,4550 a 5500 Series	x		
Nortel ERS 2500,4500,5500 Series	x		
Nortel ERS 4000 Series		x	
Nortel ES325,BPS2000	x		
SMC TS6128L2,TS6224M,SMC8824M - SMC8848M	x		

Tabulka 3: Podpora přepínačů bez bezdrátové technologie