UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Problematika Host Intrusion Prevention System

Bc. Jan Januš

Diplomová práce
2015

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2014/2015**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Januš**
Osobní číslo:	**I13412**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Problematika Host Intrusion Prevention System**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je popsat principy a možnosti nasazení HIPS v prostředí podnikové sítě. Autor v teoretické části představí principy (IPS/IDS) Intrusion Prevention Systems/ Intrusion Detection Systems, systém dělení IPS na Network-based Intrusion Prevention (NIPS), Wireless Intrusion Prevention Systems (WIPS, Network Behavior Analysis (NBA) a Host-based Intrusion Prevention (HIPS). Teoretická část bude použita na rozšíření wiki.upce.cz. V praktické části autor provede komparativní analýzu dostupných HIPS systémů a navrhne jejich implementaci v prostředí podnikové sítě a provede zátěžové testy nasazení HIPS v operačních systémech. Testy budou zaměřeny na ovlivnění výkonu operačího systému s/bez impelementace HIPS.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

RASH, Michael. Intrusion prevention and active response. Vyd. 1. Massachusetts: Syngress Media, 2005, 402 s. ISBN 19-322-6647-X.
DAVIS, Michael. Hacking exposed malware: malware. Vyd. 1. New York: McGraw-Hill, c2010, xxi, 377 s. ISBN 978-0-07-159118-8.
EDITED BY DAVID HUTCHISON, Takeo Kanade. Detection of Intrusions and Malware, and Vulnerability Assessment 6th International Conference, DIMVA 2009, Como, Italy, July 9-10, 2009. Proceedings: malware. Online-Ausg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, xxi, 377 s. ISBN 978-364-2029-189.

Vedoucí diplomové práce: **Mgr. Josef Horálek, Ph.D.**
Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2014**
Termín odevzdání diplomové práce: **15. května 2015**

prof. Ing. Simeon Karamazov, Dr.
děkan

L.S.

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

V Pardubicích dne 15. listopadu 2014

Prohlášení autora

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 3. 2. 2015 Jan Januš

Poděkování

Tímto bych rád poděkoval svému vedoucímu práce panu Mgr. Josefu Horálkovi, Ph.D. za jeho odbornou pomoc a cenné rady, které mi pomohly při zpracování diplomové práce. Dále pak své rodině a zejména přítelkyni za podporu během studia.

Anotace

Cílem práce je popsat principy a možnosti nasazení Host-based Intrusion Detection Prevention System (HIDPS) v prostředí podnikové sítě. V teoretické části jsou představeny principy Intrusion Prevention Systems (IPS) a Intrusion Detection Systems (IDS), systém dělení IPS a IDS na Network-based (NIDPS), Wireless (WIDPS), Network Behavior Analysis (NBA) a Host-based (HIDPS). Teoretická část bude použita na rozšíření wiki.upce.cz. V rámci praktické části byla provedena komparativní analýza dostupných HIDPS systémů a návrh jejich implementace v prostředí podnikové sítě. Dále byly provedeny zátěžové testy nasazení HIDPS v operačních systémech Windows a Linux. Testy byly zaměřeny na ovlivnění výkonu operačního systému s/bez implementace HIDPS.

Klíčová slova

počítačová síť, systémy prevence průniků, systémy detekce průniků, zabezpečení sítě, komparativní analýza, HIPS, IDS, IPS

Title

Problematics of the Host Intrusion Prevention System

Annotation

The main aim of this diploma thesis is to describe principles and possibilities of deployment the Host-based Intrusion Detection Prevention System (HIDPS) in the company network infrastructure. In the theoretical part, basic principles of the Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS), are introduced. These systems are divided into four technologies, which are described more specifically. It is the Network-based (NIDPS), the Wireless (WIDPS), the Network Behavior Analysis (NBA) and the Host-based (HIDPS). The theoretical part will be used to extend the wiki.upce.cz webpage. In the practical part, a comparative analysis of an available HIDPS and a proposal of their implementation in the company network infrastructure, was performed. In the practical part were also performed load tests of deployment the HIDPS in Windows and Linux operating systems. The tests were focused on how implementation of the HIDPS affect performance of the test subject in operating systems.

Keywords

computer network, intrusion prevetion systems, intrusion detection systems, network security, comparative analysis, HIPS, IDS, IPS

Obsah

Seznam zkratek

IDPS	Intrusion Detection Prevention System
IPS	Intrusion Prevention System
IDS	Intrusion Detection Systém
NIDPS	Network-based Intrusion Detection System
WIDPS	Wireless-based Intrusion Detection System
NBA	Network Behavior Analysis
HIDPS	Host-based Intrusion Detection Prevention System
FW	Firewall
DoS	Denial of Service
DDoS	Distributed Denial of Service
OS	Operating System
IP	Internet Protocol
VoIP	Voice over Internet Protocol
ID	Identification Document
PC	Personal Computer
SW	Software
HW	Hardware
VLAN	Virtual Local Area Network
NTP	Network Time Protocol
TLS	Transport Layer Security
GUI	Graphical User Interface
CLI	Command Line Interface
SSH	Secure Shell
CD	Compact Disc
DVD	Digital Video Disc
TCP/IP	Transmission Control Protocol/Internet Protocol
NIC	Network Interface Card
SSL	Secure Socket Layer
DMZ	Demilitarized Zone
TAP	Test Access Port
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
LAN	Local Area Network
WLAN	Wireless Local Area Network
AP	Access Point
STA	Station
MAC	Media Access Control
SSID	Service Set Identifier
IEEE	Institute of Electrical and Electronics Engineers
WEP	Wired Equivalent Privacy

FS	File System
USB	Universal Serial Bus
VPN	Virtual Private Network
HTTP	Hypertext Transfer Protocol
RAID	Redundant Array of Inexpensive/Independent Disks
SSD	Solid State Drive
CPU	Central Processing Unit
RAM	Random Access Memory
MB	Mega Byte
GB	Giga Byte
GHz	Giga Hertz
MHz	Mega Hertz
GPU	Graphic Processing Unit
SDRAM	Synchronous Dynamic Random Access Memory
DDR	Double Data Rate
PCI-E	Peripheral Component Interconnect Express

Seznam obrázků

Seznam tabulek

Úvod

Bezpečnost počítačové sítě je, se stále se vyvíjejícími hrozbami, které se vyskytují na internetu, stále aktuální téma. Je třeba si ale uvědomit, že nebezpečí se pro konkrétní počítačové zařízení nenachází pouze v rámci počítačové sítě, tedy po připojení k internetu. Dnes již není chráněný perimetr počítačové sítě, jako například centrální firewall, dostačující na ochranu počítačových zařízení a jejich důležitých dat. Proto je třeba chránit i tato samotná zařízení před útoky ze všech stran a nejen z internetu. Určité paměťové médium, na kterém je škodlivý kód, daný firewall nezastaví. Z tohoto důvodu by měl být na každém počítačovém zařízení, které je vůči těmto typům útoků náchylné, přítomný nějaký software, který je schopný útok detekovat a provést nezbytná preventivní opatření k zabránění potenciálně způsobeným škodám. Tento software nasazovaný přímo na konkrétní počítačové zařízení, se nazývá Host Intrusion Detection Prevention System (HIDPS). Z názvu lze usoudit, že Host Intrusion Detection System hrozby pouze detekuje a zasílá o nich upozornění danému správci, zatímco Host Intrusion Prevention System provádí i opatření, aby přicházející hrozby zastavil. Většina současných produktů nabízí obě tyto funkčnosti.

Diplomová práce je rozdělena na část teoretickou a praktickou. V teoretické části jsou popsány principy fungování HIDPS. Dále je popsáno dělení daných systémů podle technologií nasazení. V dalších kapitolách jsou podrobně popsány jednotlivé technologie Intrusion Detection Prevention systémů (IDPS), jako jsou síťové, bezdrátové a systémy založené na analýze chování sítě. Poslední kapitola teoretické části je věnována popisu nasazení a správě IDPS.

Právě nasazení těchto systémů přináší určitá omezení výkonu zařízení, na kterém jsou nasazeny. Cílem praktické části diplomové práce je, na základě autorem stanovených kritérií, vybrat dostupná softwarová řešení HIDPS a porovnat, jak ovlivňují výkon hostitele, na kterém jsou nasazena. Porovnání je provedeno také v rámci operačních systémů Windows a Linux. Dále je cílem navržení implementace systému HIDPS v lokální síťové infrastruktuře podniku.

V praktické části je tedy proveden výběr dostupných řešení na základě stanovených kritérií, přičemž dnešní HIDPS jsou ve velké míře součástí antivirových řešení, případně firewallu. Kritéria výběru byla spíše směřována, i z hlediska cíle porovnání řešení v rámci více operačních systémů, k samotným řešením. Tedy těm, které nejsou součástí určitého softwaru. Po výběru konkrétních produktů následuje přehled konfigurace testovacího hostitele (počítačového zařízení), na který jsou daná řešení následně nasazena. Dále je provedena komparativní analýza nasazení a funkcí vybraných řešení a průběh zátěžových testů na ovlivnění výkonu testovacího hostitele. Poslední kapitolou je již zmíněný návrh implementace HIDPS v rámci podnikové sítě.

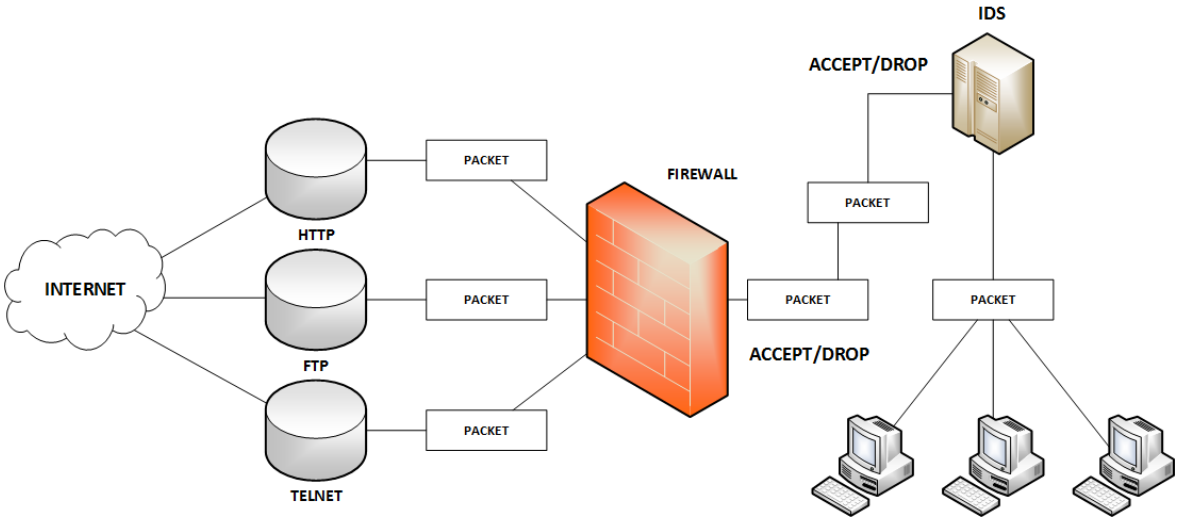
Problematice ovlivnění výkonu hostitele v rámci odlišných operačních systémů po nasazení HIDPS není v současnosti věnována dostatečná pozornost. Z tohoto důvodu by diplomová práce měla přinést nové poznatky do segmentu analýzy současných řešení HIDPS.

1 Principy Intrusion Detection Prevention systémů

Systémy Intrusion Detection a Prevention (IDP) se primárně zaměřují na identifikování možných bezpečnostních incidentů, uchovávání informací o nich, snahu je zastavit a oznamovat jejich výskyt a stavy správcům bezpečnosti sítě (ALEXANDER, 2009).

1.1 Rozdíl mezi IPS a IDS

Intrusion Detection System (IDS) je proces monitorování událostí, objevujících se na síti nebo v počítačovém systému a jejich následná analýza na znaky možných bezpečnostních incidentů[1]. Je to pasivní technologie, která upozorňuje správce bezpečnosti sítě o zmíněných incidentech. Její funkce nicméně neposkytují žádné preventivní mechanismy, na základě kterých by bylo možné se s nastalými hrozbami vypořádat. Zjednodušeně se dá říci, že IDS mají pouze informativní charakter.



Obrázek 1 – IDS příklad

Zdroj: Přepracováno od: (DAVE, a další, 2013)

Intrusion Prevention System (IPS) je proces, který v sobě zahrnuje IDS a k tomu přidává možnost nejen detekovat určité potenciálně nebezpečné incidenty, ale také je zastavit. Jedná se o reaktivní technologii, která může na základě povahy dané hrozby například změnit konfiguraci firewallu (FW), nebo celkově změnit obsah škodlivého kódu, který dělá nadcházející útok nebezpečným, a tím ho zcela zastavit.

(ALEXANDER, 2009)

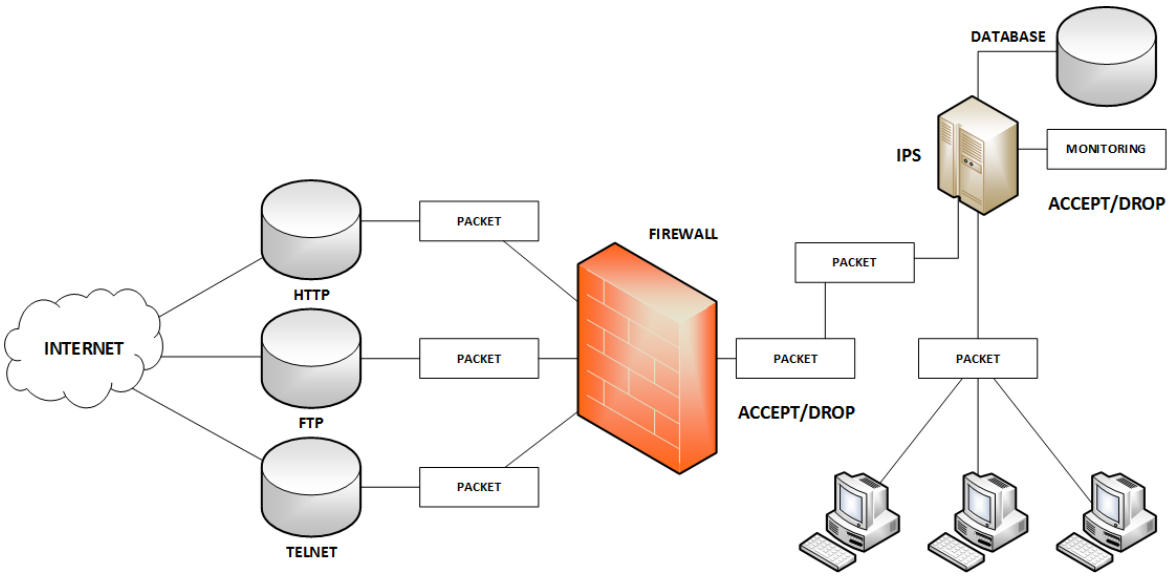
Reakce IPS na daný incident se dají rozdělit do následujících kategorií:

[1] Zmiňované bezpečnostní incidenty jsou z velké míry škodlivé kódy (viry, červi). Útočníci za pomocí nich získají přístup do systémů s takovým oprávněním, které jim dovoluje napadený systém zneužít.

- **IPS zastaví samotný útok –** realizováno například ukončením síťového spojení, blokováním přístupu k cíli z účtu, Internet Protocol (IP) adresy nebo jiných atributů útočníka.

- **IPS změní bezpečnostní prostředí –** IPS může změnit konfiguraci síťových zařízení (například FW, přepínače nebo směrovače) tak, aby byl zablokován přístup od útočníka k cílovému hostiteli. IPS může také detekovat určité bezpečnostní slabiny u hostitele a aplikovat na ně nejrůznější záplaty.

- **IPS změní obsah útoku –** Jak již bylo zmíněno výše, některé IPS umožňují změnit škodlivou část útoku a tím změnit jeho povahu na bezpečný. Nejčastěji je to například odstranění škodlivého souboru z přílohy z mailu a následné doručení již bezpečného mailu příjemci.



Obrázek 2 – IPS příklad

Zdroj: Přepracováno od: (DAVE, a další, 2013)

Celkově lze říci, že IDPS technologie neumožňují úplnou a přesnou detekci incidentů. Problémy s detekcí se dají rozdělit na:

- **False positive –** IDPS nesprávně identifikuje bezpečné incidenty na síti jako nebezpečné

- **False negative –** IDPS selžou při identifikaci nebezpečných incidentů

False positive a false negative problémy není možné kompletně vyloučit. Pokud se například změní konfigurace IDPS na snížení false negative, zvyšuje se výskyt false positive. Právě takovéto změny konfigurace IDPS, za účelem zlepšení přesnosti detekce nebezpečných incidentů, se nazývají ladění (tuning).

Útočník může používat techniku uhýbání (evasion). Jedná se o modifikaci časování nebo formátu útoku z hlediska venkovního projevu, přičemž efekt útoku zůstává nezměněn. Pro příklad lze uvést překódování znaků textu útočníkem specifickým způsobem, o kterém ví, že mu cíl (hostitel) porozumí, ale monitorující IDPS nikoliv. Proti této technice útoku je většina IDPS technologií vybavena odpovídajícími funkcionalitami.

(HUDEC, 200-?)

1.2 Způsoby užití a hlavní funkce IDPS

Obecně se dá říci, že IDPS jsou primárně určené k identifikaci možných bezpečnostních incidentů a následné reakci na ně. Může to být například detekce kompromitace systému útočníkem, který využil určitou slabinu daného systému. IDPS potom oznámí tento incident správci bezpečnosti sítě a zahájí nezbytnou proceduru reakce na incident. K tomu je možné si nechat vygenerovat informační záznam, který obsahuje informace o nastalém incidentu. Dále jsou IDPS používány pro monitorování přenosu souborů a identifikování podezřelých přenosů a pro detekci různých průzkumných aktivit útočníka, jako je například skenování portů (HUDEC, 200-?).

Kromě výše uvedených způsobů, lze využít IDPS také na:

- **Identifikace problémů s bezpečnostní politikou systémů –** IDPS poskytuje možnost řídit kvalitu implementace bezpečnostní politiky. Například si nastaví vlastní množinu pravidel FW, a na základě těchto pravidel detekuje síťový provoz, který by měl být blokován.

- **Dokumentace existujících hrozeb v rámci společnosti –** Zaznamenávání intenzity útoků a jejich povahy je důležitým faktorem z hlediska bezpečnostních opatření v rámci společnosti. Té tyto informace poskytují možnost navrhnout a implementovat lepší bezpečnostní opatření do budoucna.

- **Odrazení potenciálních útočníků od porušování bezpečnostní politiky –** Při pokusu o narušení bezpečnostní politiky je útočník informován o tom, že jeho akce jsou monitorovány IDPS. Útočník pak může přestat s narušováním bezpečnostní politiky, protože riskuje odhalení.

Hlavní funkce technologií IDPS jsou:

- **Zaznamenávání informací vztažených k pozorovaným událostem –** Tyto informace jsou obvykle zaznamenávány lokálně, případně posílány na centrální logovací servery.

- **Upozorňování správců bezpečnosti o důležitých pozorovaných událostech –** V podstatě se jedná o výstražné hlášení v různých formách (email, stránka, systémový log, zpráva v IDPS administraci). Tato hlášení obsahují často pouze

základní informace o nastalé události. Pro detailnější popis je nutný přístup do administrace IDPS.

- **Vytváření reportů –** Jedná se o statistické souhrny informací o monitorovaných událostech nebo se také může jednat o detailní report vztažený pouze k jedné události.

(SCARFONE, a další, 2007)

1.3 Detekční mechanismy IDPS

Jednotlivé technologie IDPS používají mnoho mechanismů pro detekování bezpečnostních incidentů. Tyto mechanismy se dají rozdělit na Signature-based, Anomaly-based a Stateful protocol analysis.

1.3.1 Mechanismus založený na příznacích

Jako příznak je v tomto případě myšlen určitý vzorek, který odpovídá známé bezpečnostní hrozbě. Tento mechanismus tak porovnává daný vzorek s pozorovanými událostmi, s cílem identifikovat možné incidenty. Jako příklad lze uvést například email s předmětem a přílohou, které odpovídají škodlivému kódu nebo pokus o spuštění nějaké definované služby s určitým oprávněním (HUDEC, 200-?).

Jak již z textu výše vyplývá, mechanismus založený na příznacích (Signature-based) je efektivní v detekování známých hrozeb, ale velice neefektivní v detekování hrozeb neznámých (SCARFONE, a další, 2007).

Jedná se v podstatě o takový filtr, který detekuje přesně to, co mu je definováno. Když bude například filtr nastaven na detekování bezpečnostní hrozby ve formě přílohy emailu přímo na její název. Útočník může změnit název přílohy a pokusit se o útok znovu. V tuto chvíli bude úspěšný, protože filtr nebude tento název odchytávat[2].

1.3.2 Mechanismus založený na anomáliích

Detekční mechanismus založený na anomáliích (Anomaly-based) je proces vyhodnocení aktivit na základě toho, zda je u nich identifikováno jiné než předem definované/očekávané chování. IDPS používající tento detekční mechanismus obsahuje profily, které reprezentují normální chování samotných uživatelů, síťových připojení nebo aplikací. Profily jsou vytvářeny na základě monitorování charakteristik daných aktivit po určitý časový interval (SCARFONE, a další, 2007). Jako příklad lze uvést sledování počtu přístupů k webovému serveru apache v určitou hodinu. Na základě sledování po určitý čas se vytvoří profil typického počtu přístupů k webovému serveru. IDPS potom na základě detekčního mechanismu založeného na anomáliích porovnává tento profil s aktuálním stavem, a pokud se razantně liší, upozorňuje o nastalé anomálii správce bezpečnosti. Profily mohou být vytvářeny pro různé situace a služby. Například pro počet emailů odeslaných konkrétním

[2] Toto je pouze ilustrační příklad. Samozřejmě se jedná v praxi o složitější mechanismus. Příznaky jsou uložené v určitém seznamu a pomocí porovnávání řetězců se provádí porovnání na dané aktivity.

uživatelem, počet chybných pokusů o připojení ke konkrétnímu uzlu v síti nebo také pro monitorování využití procesorů serveru.

Na rozdíl od Signature-based detekčních metod jsou Anomaly-based mechanismy velice vhodné pro detekování předem neznámých hrozeb.

Jednotlivé profily jsou vytvářeny dny až týdny v časovém intervalu nazývaném training period (trénovací perioda). Mohou být statické nebo dynamické. Statické jsou neměnné a musí se vždy celé přegenerovat, pokud nastane očekávaná změna na síti nebo v systému. Dynamické se dynamicky mění na základě pozorovaných událostí a nemusí se tedy celé generovat znovu, nicméně jsou náchylné k technice evasion. Může se například stát, že útočník pozvolna mění frekvenci útoku. Dynamický profil na tuto pozvolnou změnu reaguje tak, že nerozpozná útok od očekávané změny a tento incident tak nedetekuje. Bezpečnostní incidenty mohou být také sledovány už v rámci generování profilu (SCARFONE, a další, 2007).

Tento mechanismus je náchylný na problémy, kdy jsou neúmyslně zahrnuty nebezpečné aktivity jako součást profilu nebo naopak bezpečné z profilu vylučovány. Potom nastává situace kdy je vytvářeno velké množství false positive upozornění (HUDEC, 200-?).

1.3.3 Analýza stavových protokolů

Analýza stavových protokolů je podobně jako Anomaly-based mechanismus proces porovnání profilů s všeobecně akceptovatelnými aktivitami oproti aktuálně sledovaným aktivitám, ovšem na úrovni stavů protokolů v jednotlivých aktivitách. Anomaly-based využívá hostitelské či síťové profily pro porovnání, ale Analýza stavových protokolů (Stateful protocol analysis) využívá dodavatelem vyvinuté profily a určuje, jak mají být použité protokoly, na základě svých stavů, užity. Jedná se o protokoly síťové, transportní a aplikační vrstvy. IDPS s tímto detekčním mechanismem sleduje právě stavy těchto protokolů. Příkladem může být otevření FTP spojení, kdy při inicializaci je toto spojení v neautentifikovaném stavu. Uživatelé, kteří nejsou autentifikováni mohou pouštět jen omezené množství příkazů. IDPS potom může získat stavový kód, značící provedení autentifikace. Když se uživatel autentifikuje, spojení je ve stavu autentifikace a může spouštět více příkazů. Provádění těchto příkazů v neautentifikovaném stavu by bylo IDPS považováno za podezřelou aktivitu, nicméně v rámci autentifikovaného stavu jde o normální jev (SCARFONE, a další, 2007).

Tento mechanismus umožňuje také identifikovat neočekávané posloupnosti příkazů. Například opakované zadání jednoho samého příkazu nebo zadání příkazu bez toho, aby byl zadán příkaz, na kterém je ten předchozí závislý. Mechanismus kontroluje také správné zadávání příkazů jako je maximální a minimální délka argumentů. Hlavní nevýhodou mechanismu stateful protocol analysis je jeho náročnost na výpočetní prostředky, kvůli analýze stavů všech souběžných vytvořených spojení (HUDEC, 200-?).

Dalším problém může být, že tento mechanismus nedetekuje útoky, které neporušují charakteristiku chování protokolu samotného. Jako příklad lze uvést provádění mnoha akcí,

které se v rámci chování protokolu tváří bezpečně, nicméně jich je tolik, že mohou způsobit Denial of Service (DoS). Další problém může být ten, že model protokolu použitý v IDPS může kolidovat se způsobem, jak je implementován v různých verzích konkrétních aplikací a operačních systémech (OS), nebo také jak spolu různé implementace protokolu v rámci klienta a serveru komunikují (SCARFONE, a další, 2007).

2 Technologie systémů IDP obecně

IDPS se dají rozdělit na několik technologií z hlediska způsobu užití. Jedná se o Network-based technologie, které monitorují provoz na síti. Analyzují činnosti síťového a aplikačního protokolu a identifikují podezřelé aktivity. Další technologie se nazývají Wireless a jak už z názvu vyplývá, monitorují provoz bezdrátové sítě. Jejich funkcionalita sestává z analýzy bezdrátových síťových protokolů. Network Behaviour Analysis je technologie IDPS, která zkoumá určité neobvyklé chování síťového provozu. Identifikuje například Distributed Denial of Service (DDoS) útoky, různé typy malwaru a skenování portů. Poslední zástupce technologií IDPS je Host-based, která monitoruje události týkající se přímo konkrétního hostitele na síti (ALEXANDER, 2009).

Tyto technologie sestávají z určitých komponent, které mají určitou architekturu.

2.1 Komponenty technologií IDPS

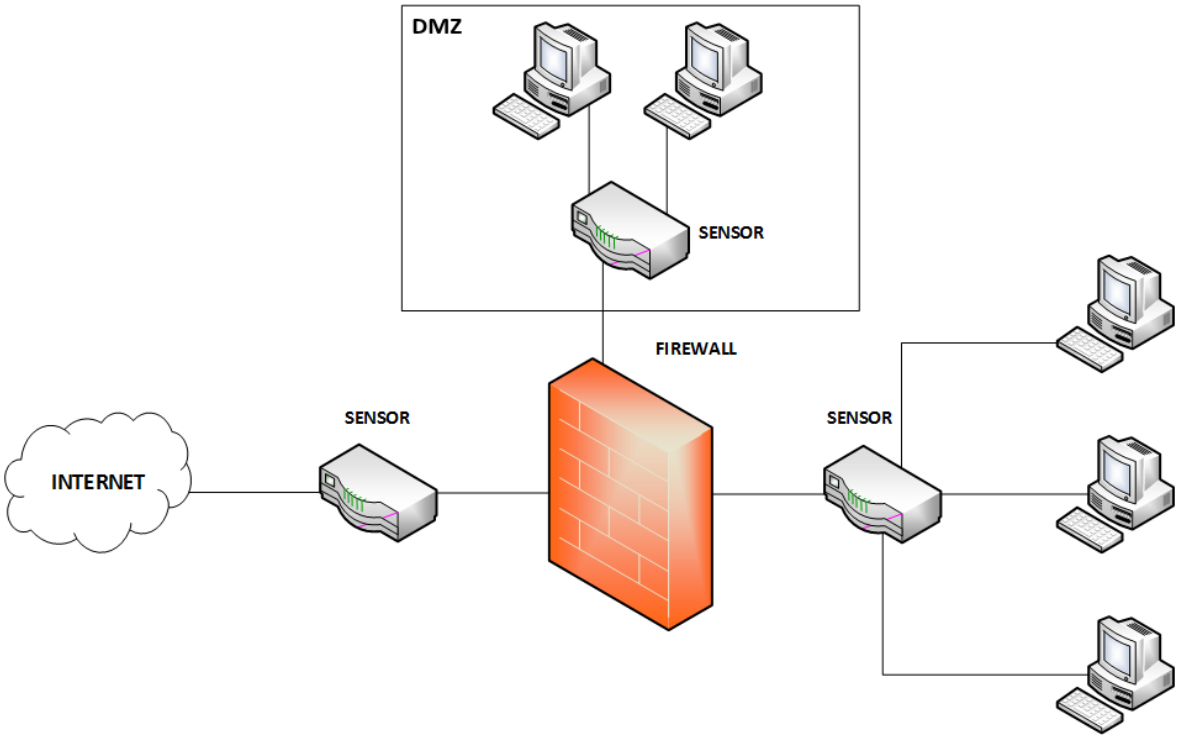
Existují 4 druhy typických komponentů technologií IDPS.

2.1.1 Senzory, Agenti

Jedná se o komponenty monitorující a analyzující události na síti. Senzory (Senzors) se nazývá komponentům pro monitorování sítí použitých v technologiích Network-based, Wireless a Network Behavior Analysis (NBA). Termín agent, je užit v poslední zbývající technologii IDPS, a to Host-based (SCARFONE, a další, 2007).

Existují 3 způsoby připojení senzorů k síti. Inline připojení je takové, kde je IPS senzor umístěn za FW, směrovač nebo přepínač, takže přes ně proudí síťový provoz. Další možnost připojení je tzv. Network test access point (tap). Jedná se o hardware (HW) zařízení, které poskytuje způsob k získání dat proudících skrze síť. Poslední způsob je Switch span port. Je to port na přepínači, kde může být monitorována kopie celého síťového provozu, který proudí skrze daný přepínač (PIPER, 2011).

Obecně je vhodné senzory umisťovat na vstupní body do sítě, jako jsou výchozí brány, body spojení mezi jednotlivými sítěmi a Virtual Private Network (VPN) zařízení. Obecné umístění senzorů je zobrazeno na obrázku (Obrázek 3) a lze vidět, že jejich klasické umístění je až za FW.



Obrázek 3 – Možné umístění senzorů v síti

Zdroj: Přepracováno od: (Neznámý, 2014)

2.1.2 Management Server

V podnikové sféře funguje Management Server jako centralizovaný přijímač informací ze Senzorů a Agentů, se kterými následně pracuje. Samozřejmě je možné nasadit Senzory a Agenty bez příslušného Management Serveru. Správce je potom obsluhuje přímo bez určitého centralizovaného serveru.

Management Server je také schopný identifikovat události, které jednotlivé Senzory a Agenti nejsou schopni identifikovat. Dokáže například párovat informace o události z více Senzorů a Agentů, na základě spuštění dané události z jedné IP adresy. Tato funkce se nazývá korelace (correlation). Management serverů může být v rámci systému IDP několik nebo také žádný. Závisí na konkrétní implementaci.

2.1.3 Databázový server

Databázový (database) server je v podstatě pouze úložiště informací o nastalých událostech, které jsou nahrané a reportované od senzorů, agentů případně management serverů.

2.1.4 Konzole

Tento komponent je program, který zajišťuje klasické uživatelské rozhraní pro správu IDPS. Klasicky je instalován na standardní pracovní stanici (PC – Personal Computer) nebo notebook. Konzole (Console) mohou mít v jednom případě pouze funkce pro rutinní administraci IDPS, jako je nastavení ostatních komponent systému, jeho aktualizace atd. Ve druhém případě mohou být také vybaveny funkcemi pro monitorování a analýzu. Některé IDPS konzole kombinují tyto funkce obě (SCARFONE, a další, 2007).

2.2 Síťová architektura komponentů

Jednotlivé komponenty technologií IDPS mohou být spojeny mezi sebou v rámci standardní podnikové sítě. To sebou nese bezpečnostní rizika, protože IDPS je často první na řadě co se týče důležitosti vyřazení při probíhajícím útoku. Mnohem lepší, z hlediska bezpečnosti, je komponenty spojit v rámci oddělené sítě, navržené pro obsluhu bezpečnostního softwaru (SW), jakým je právě IDPS. Taková síťová architektura se v rámci těchto systémů nazývá Management Network.

Ta umožňuje skrýt existenci a identitu IDPS před potenciálními útočníky a izoluje ho od standardních produkčních sítí. Nevýhodou použití Management network architektury mohou být zvýšené náklady na síťové vybavení a jiný HW.

Pokud by bylo IDPS nasazeno bez použití architektury Management network, dala by se bezpečnost systému zvýšit vytvořením virtuální management sítě použitím Virtual Local Area Network (VLAN) v rámci standardní sítě. Tento způsob ale nedosahuje takové bezpečnosti jako separování celé sítě IDPS. Může nastat například problém s konfigurací VLAN a na základě toho, odhalení citlivých dat IDPS.

(SCARFONE, a další, 2007)

2.3 Bezpečnostní možnosti

Systémy IDPS poskytují rozsáhlé bezpečnostní možnosti, které jsou členěny na: Logování, sbírání informací a možnosti detekce a prevence.

2.3.1 Logování

Systémy IDP, jak již bylo zmíněno výše, provádějí rozsáhlé logování dat o událostech. Tato data mohou být pak použita k různým účelům, nejčastěji však k potvrzování správnosti posílaných upozornění správci, zkoumání nastalých bezpečnostních incidentů a porovnávat události mezi IDPS a jiným zdrojem logování.

Obecně logovaná data v rámci technologií IDPS obsahují čas a datum události[3], typ události, míru důležitosti (závisí např. na prioritě a možném dopadu na systém) a zda už na tuto událost byla vykonána nějaká preventivní akce. Dále se pak obsah může lišit v závislosti na použité technologii. Pro příklad lze uvést technologii Host-based, která v logu obsahuje ještě například ID uživatele.

Logy mohou být správci IDPS ukládány lokálně a jejich kopie například posílány na centralizovaný log server. Obecně by měly být ukládány jak lokálně, tak na určitém centralizovaném serveru, z důvodu nejen lepší přístupnosti dat, ale i z důvodu bezpečnosti. Při útoku na IDPS by mohly být lokální logy zničeny nebo nějakým způsobem zkompromitovány.

[3] Ke vložení korektní časové značky k určitému logu, je nutné, aby měl IDPS správně synchronizované své hodiny pomocí Network Time Protocol (NTP).

2.3.2 Sbírání informací

Některé IDPS technologie jsou schopné sbírat informace o jednotlivých hostitelích či celých sítích ze sledovaných aktivit. Na základě nich mohou rozpoznat daný OS hostitele a aplikace, které využívá. V rámci sítě to potom může být její obecná charakteristika.

2.3.3 Detekce

Co se týče detekčních schopností IDPS, tak jsou poměrně široké a rozsáhlé. Většina z nich používá kombinaci detekčních technik, které všeobecně zabezpečují přesnější detekování potenciální hrozby a větší flexibilitu při ladění a přizpůsobení. Právě ladění a přizpůsobování je důležité z hlediska zvýšení přesnosti samotné detekce. Ladící a přizpůsobovací možnosti jsou:

- **Prahy** – Jedná se o hodnoty, které nastavují limity mezi normálním a abnormálním chováním. Obvykle jsou užity pro nastavení maximální možné úrovně. Prahy se nejvíce užívají v detekčních mechanismech založených na anomáliích a analýze stavových protokolů.

- **Nastavení upozornění** – Většina technologií IDPS dovoluje správci systému přizpůsobit každý typ výstražného upozornění. Přizpůsobení může být takového rázu, že se dané upozornění zcela vypne, nastaví se mu určitá priorita a důležitost nebo se mu specifikují informace, které by měly být zaznamenávány.

- **Blacklisty a whitelisty** – Jsou to v podstatě seznamy povolených a nepovolených entit. V blacklistech jsou ukládány entity, které byly v minulosti označeny jako součást škodlivých aktivit. Jedná se o celé hostitele, čísla portů, jména uživatelů, jména souborů atd. Některé IDPS vytvářejí dynamické blacklisty, do kterých se dynamicky ukládají nedávno detekované hrozby. Whitelist je seznam entit, které jsou známé jako neškodné. Blacklisty a whitelisty se užívají nejvíce u detekčních mechanismů založených na bázi příznaků a analýzy stavového protokolu.

- **Zobrazení kódu a jeho úpravy** – Některé technologie IDPS umožňují správcům zobrazit a upravit kód detekčního mechanismu. Obecně jsou úpravy omezené pouze na příznaky, nicméně některé technologie umožňují zobrazení dalšího kódu, a to například programů použitých pro vykonání analýzy stavového protokolu. Možnost zobrazit kód může pomoci vyvodit závěry, proč bylo určité výstražné upozornění vygenerováno. Možnost kód dokonce upravit může ještě více zvýšit přizpůsobitelnost detekčních schopností. To sebou nese určitá úskalí, protože editace kódu určitě vyžaduje určité znalosti programování a také systémů IDP. Pokud by vznikla v kódu chyba, mohlo by to mít za následek nesprávnou funkčnost IDPS.

(HUDEC, 200-?)

2.3.4 Prevence

Většina IDPS má více možností prevence proti bezpečnostním incidentům, které se liší v závislosti na použité technologii. Správci mohou specifikovat konfiguraci prevence pro

každý typ reportovaných oznámení. To v sobě zahrnuje celkové vypnutí nebo zapnutí prevence, stejně jako to, jaký typ má být použit.

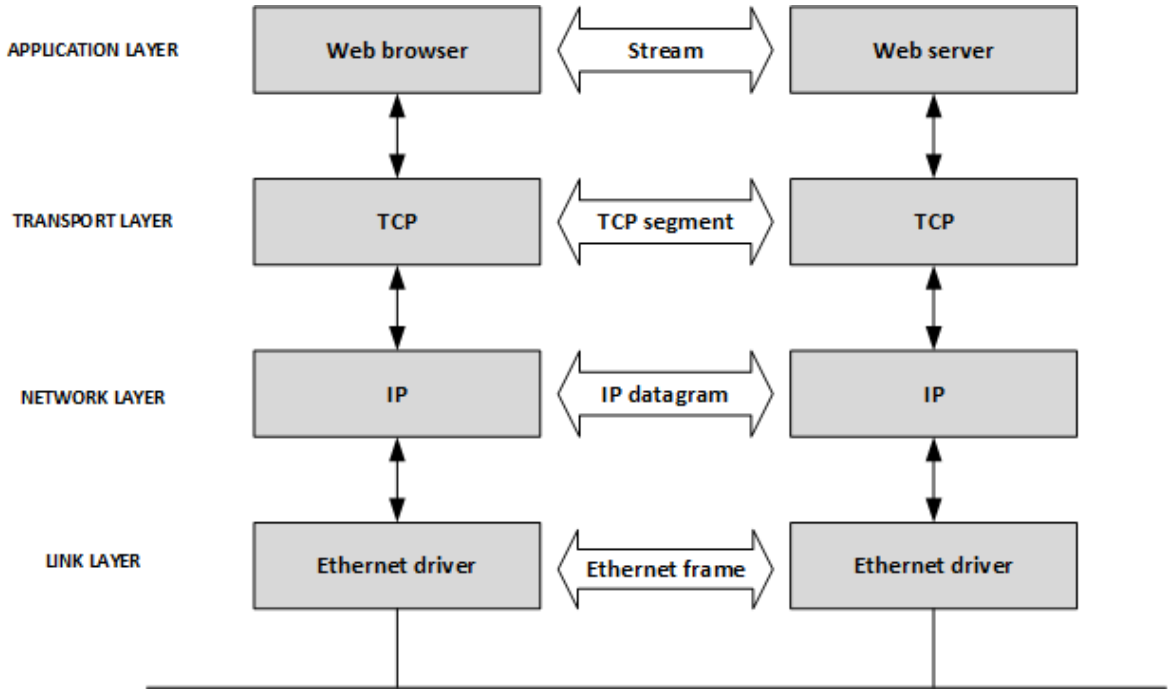
Některé senzory mají speciální simulační mód, který potlačuje všechny preventivní akce a místo toho pouze indikuje, kdy by byly určité preventivní akce vykonány. To umožňuje správcům monitorovat a správně vyladit konfiguraci prevence před ostrým nasazením, což snižuje možnost preventivně zablokovat neškodné aktivity.

(SCARFONE, a další, 2007)

3 Network-based Intrusion Detection Prevention System

Network-based IDPS (NIDPS) monitorují síťový provoz na určité části TCP/IP (Transmission Control Protocol/Internet Protocol) sítě nebo zařízení a analyzují síťové, transportní a aplikační protokoly na podezřelé bezpečnostní aktivity (SCARFONE, a další, 2007).

Primárním zdrojem pro NIDPS je tedy síťový provoz. V TCP/IP sítích data prochází skrze čtyři vrstvy od zdroje až po cíl. Jedná se o linkovou vrstvu (někdy označována jako HW vrstva), síťovou vrstvu (někdy označována jako IP vrstva), transportní vrstvu a aplikační vrstvu (STANCIU, 2013). Na obrázku (Obrázek 4) jsou znázorněny čtyři vrstvy architektury TCP/IP.



Obrázek 4 – Model architektury TCP/IP

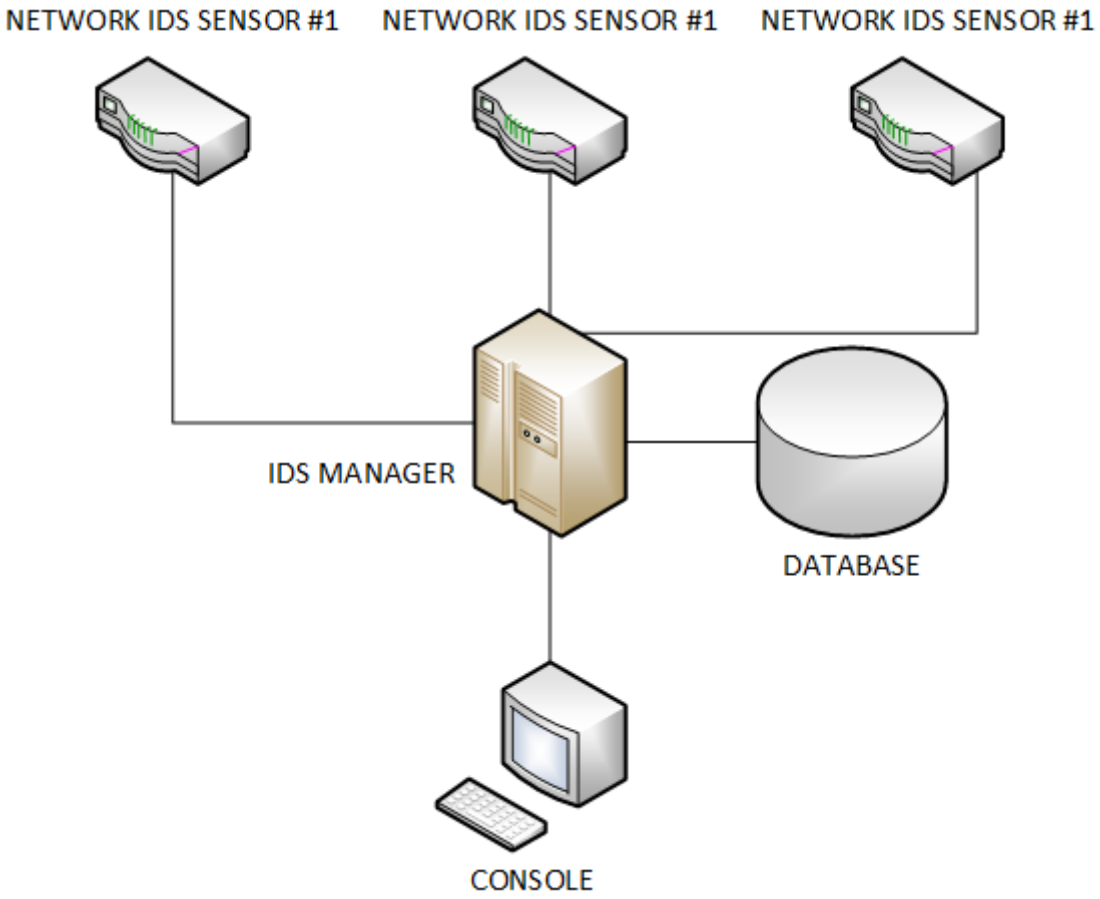
Zdroj: Přepracováno od: (STANCIU, 2013)

Dle Whitmana, NIDPS v podstatě fungují na bázi podobné jako tcpdump[4]. Když NIDPS (konkrétně jeho určitý komponent – Senzor) identifikuje aktivitu, která je vyhodnocena jako nebezpečná, zareaguje tím, že zašle upozornění správci. NIDPS při analyzování příchozích paketů hledá na základě různých vzorů podezřelých aktivit. Například velké množství na sobě závislých paketů určitého typu může vyústit v DoS útok. Výměna sérií paketů, které spolu také určitým způsobem souvisí, může indikovat problém skenování portů. Celkově

[4] Program tcpdump se většinou používá v unixových systémech pro analýzu chování, výkonu a aplikací sítí, které generují nebo přijímají síťové pakety. Také může být využit pro analýzu síťové infrastruktury nebo pro zachytávání a zobrazování komunikace jiného uživatele nebo počítače. V podstatě vytiskne popis obsahu paketů na síťovém rozhraní, která odpovídá určité hodnotě (Neznámý, 2014).

mohou být NIDPS efektivnější než například Host-based IDPS, ale vyžadují komplexnější konfiguraci a správu.

NIDPS je instalováno na konkrétní místo v síti (například vnitřní strana odpovídajícího směrovače), odkud je možné monitorovat provoz mířící do a z určité části síťového segmentu. NIDPS může monitorovat všechen provoz na síti dohromady nebo monitoring rozdělit mezi konkrétní skupiny hostitelských PC na určité části sítě (WHITMAN, a další, 2013).



Obrázek 5 – Základní NIDPS model

Zdroj: Přepracováno od: (WHITMAN, a další, 2013)

3.1 Komponenty NIDPS

NIDPS se skládá ze senzorů, jednoho nebo více management serverů, vícera konzolí a jednoho či více databázových serverů. Všechny tyto komponenty jsou stejné, co se týče funkčnosti, i v ostatních IDPS technologiích vyjma senzorů. NIDPS senzory monitorují a analyzují síťový provoz na jednom (hromadném) nebo více síťových segmentech. Network Interface Card (NIC), které provádějí monitoring, pracují v promiskuitním režimu, což znamená, že propouštějí všechny příchozí pakety, nezávisle na jejich cílové destinaci.

Některá velká nasazení systémů IDP mohou mít až stovky senzorů (SCARFONE, a další, 2007). Existují dvě provedení těchto komponent:

- **Senzory jako zařízení:** Toto provedení sestává ze specializovaného HW a SW, optimalizovaných přímo pro daný senzor. HW obsahuje NIC, ovladače pro zachytávání paketů a procesory, či jiné specializované HW komponenty, které pomáhají při následné analýze. Tento typ senzorů často obsahuje svůj zabezpečený OS, ke kterému se nepředpokládá přímý přístup ze strany správců (SCARFONE, a další, 2007). Příkladem senzoru tohoto typu je Cisco IDS 4250 Senzor.

- **Senzory jako SW:** Na trhu se vyskytují senzory prodávané jako pouhý SW bez HW zařízení. Správci pak tento SW nainstalují na zařízení, které splňuje určité požadavky daného SW. Tyto senzory mohou obsahovat také svůj přizpůsobený OS nebo může být klasicky nainstalován na standardní OS jako ostatní aplikace. Příkladem může být senzor Snort (HUDEC, 200-?).

3.2 Síťová architektura komponent

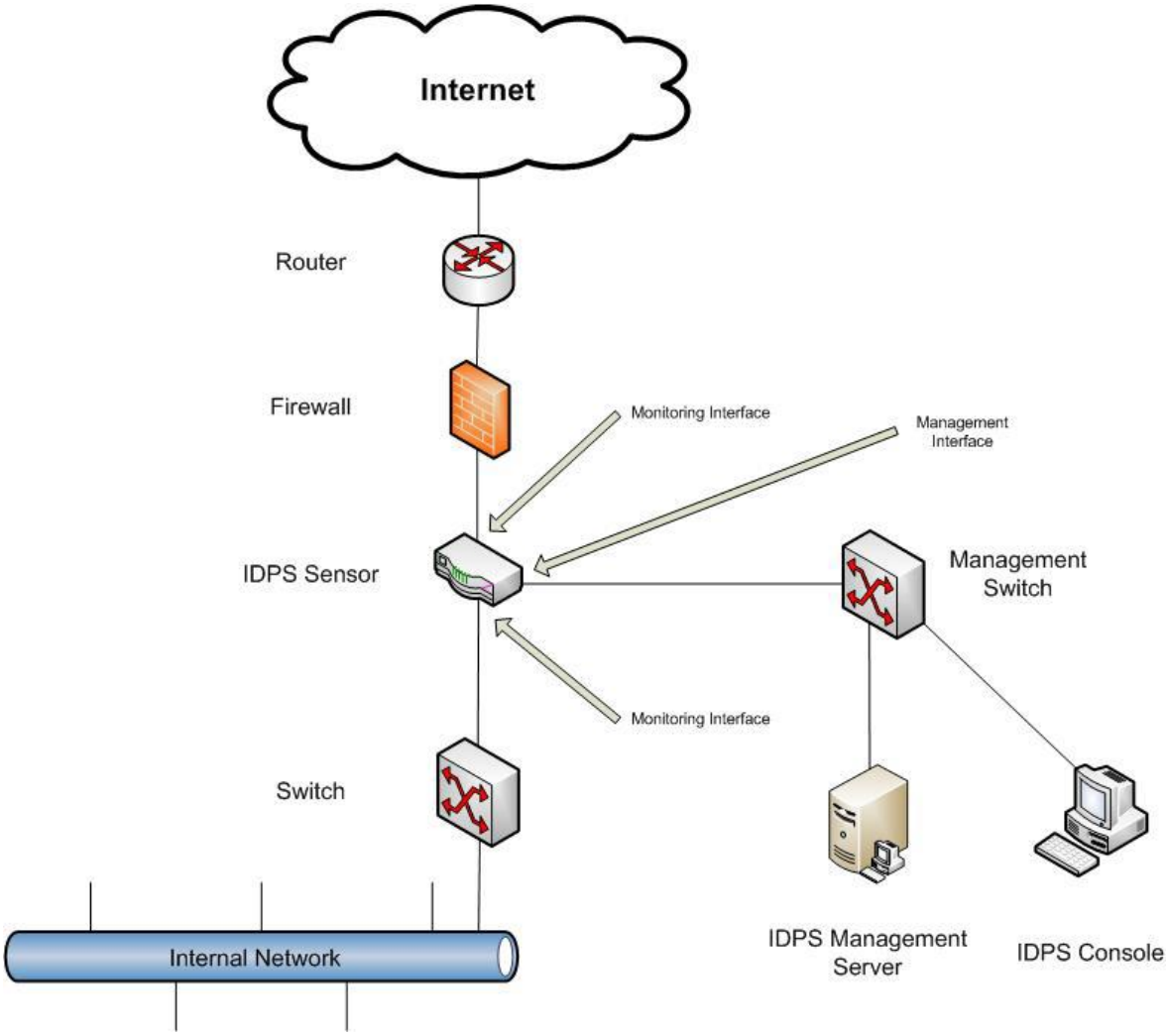
Jednotlivé organizace by měly zvážit použití oddělených management sítí pro jejich NIDPS. Pokud to z nějakého důvodu není možné, mělo by být využito technologie VLAN. Přinejmenším je nutné alespoň zajistit, aby všechny přístupy do systému byly šifrované, tzn. využití technologií Secure Shell (SSH) nebo Secure Socket Layer (SSL). V návaznosti na síťovou architekturu komponent by mělo být rozhodnuto o umístění IDS/IPS senzorů. Ty mohou být nasazeny v podstatě ve dvou módech a to Inline, či Passive.

3.2.1 Inline senzory

Inline senzor je nasazen tak, že skrze něho musí procházet jím monitorovaný síťový provoz. Hlavním důvodem nasazení Inline senzorů je využití možnosti IPS na jejich nastavení tak, aby zastavily potenciální útok blokováním síťového provozu. Inline senzory jsou obvykle umisťovány tam, kde jsou FW a jiné bezpečnostní zařízení nebo na pomezí mezi různými interními sítěmi, které by měly být odděleny. Obecně platí, že jsou umístěny na „bezpečnější“ stranu dané sítě a mají tak o něco méně provozu ke zpracování. Mohou být ale umístěny i na druhou stranu sítě k zajištění ochrany (např. FW a ke zmírnění zátěže na těchto zařízeních). Nicméně na „méně bezpečné“ straně sítě jsou Inline senzory umisťovány spíše pro výzkumné účely, protože je většinou generováno obrovské množství upozornění (alerts).

(ALEXANDER, 2009)

Inline senzory mají dvě síťová rozhraní. Jedno na monitoring síťového provozu, přes které tento provoz proudí. Druhé na samotné připojení do management sítě (HUDEC, 200-?).



Obrázek 6 – Příklad umístění Inline NIDPS senzoru

Zdroj: (ALEXANDER, 2009)

3.2.2 Pasivní senzory

Tento typ senzorů je nasazován za účelem monitorování kopie aktuálního síťového provozu. Fyzicky tak žádný provoz senzorem neprochází. Nejčastěji monitorují klíčová síťová místa, jako jsou hranice mezi sítěmi nebo různé síťové segmenty, například aktivity na Demilitarized Zone (DMZ) podsíti[5].

(ALEXANDER, 2009)

Existují různé metody, jak mohou pasivní senzory monitorovat síťový provoz:

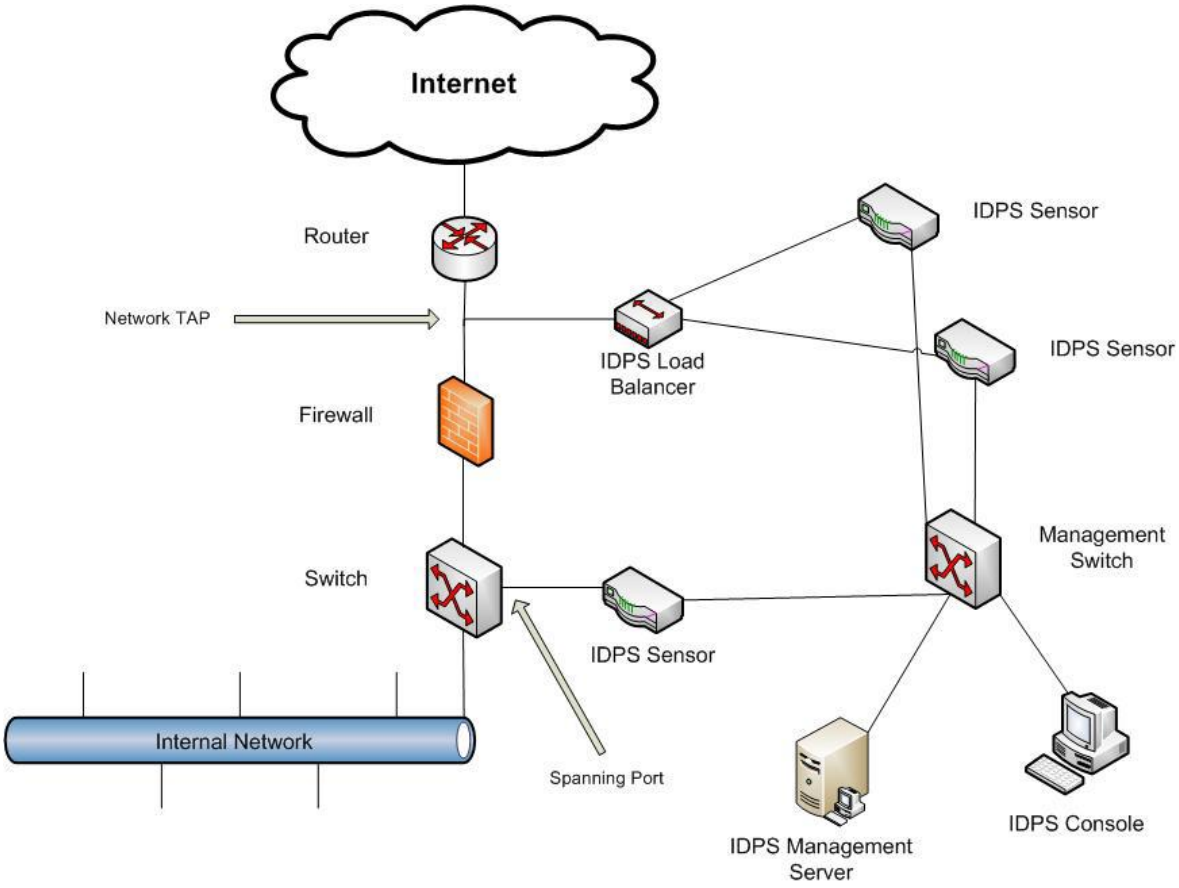
- **Network TAP –** Zařízení poskytující přímé připojení mezi senzorem a samotným fyzickým médiem, jako je například optické vlákno. Běžně tato zařízení sestávají ze 4 portů. Do dvou se portů se připojuje přímo dané zařízení a další dva se využívají

[5] DMZ podsíť je v podstatě „nárazníková“ zóna, která odděluje interní síť od často nebezpečného prostředí internetu (SHINDER, 2005).

pro monitorování provozu. Network TAP dodává senzoru kopii celého síťového provozu, který se přenáší skrze médium. V podstatě funguje velice podobně jako následující spanning port s rozdílem, že přepínače obsahují spanning porty od výroby, nicméně network TAP je nutné opatřit a nainstalovat (HUDEC, 200-?). Dle Alexandra se jedná o celkem drahou záležitost (ALEXANDER, 2009).

- **Spanning ports –** Jedná se o porty přepínače, schopné monitorovat veškerý síťový provoz, procházející daným přepínačem. Obvykle se tedy připojí senzor na spanning port a monitoruje tak příchozí a odchozí síťový provoz na daném uzlu sítě, který se kopíruje na daný port. Výhoda této metody je, že je relativně snadná na implementaci a také levná. Nevýhoda může spočívat v nesprávné konfiguraci přepínače, což vyústí v to, že spanning port může vynechávat určitou část síťového provozu. K vynechání, může dojít také při vysoké zátěži přepínače, kdy je dána větší priorita procházejícím paketům než jejich kopírování na daný spanning port. Proto některé pakety nemusí být zkopírovány a tím být vyloučeny monitoringu. Dále může být problémem dočasně zablokovaný spanning port přepínače nebo jednoduše jejich nedostatek (ALEXANDER, 2009).

- **IDS Load Balancer –** IDS Load Balancer je zařízení, které agreguje a směruje síťový provoz do monitorujících systémů, jako jsou právě IDPS senzory. Na Load Balancer přijde provoz z jednoho nebo více spanning portů, či network TAP a ten pak tedy agreguje síťový provoz z různých sítí (například znovu skládá relaci, která byla rozdělena mezi dvě sítě). Dále pak posílá, na základě určitých pravidel nastavených správcem, kopii síťového provozu jednomu nebo více přijímacím zařízením (senzorům). Zmíněná pravidla určují, jaký typ provozu se pošle na jaký určitý senzor.



Obrázek 7 – Příklad umístění Passive NIDPS senzoru

Zdroj: (ALEXANDER, 2009)

3.3 Bezpečnostní možnosti NIDPS

NIDPS poskytují širokou škálu různých bezpečnostních možností. Následující kapitola je rozdělena analogicky k podkapitole 2.3, kde byly zmíněny bezpečnostní možnosti platící obecně pro všechny technologie. V této kapitole se jedná o konkretizované možnosti přímo pro systémy Network-based IDP.

3.3.1 Logování

NIDPS provádějí rozsáhlé logování dat příslušících k daným detekovaným událostem. Pole dat obvykle obsahují následující záznamy: časová razítka, identifikaci spojení, typ události, ohodnocení (počítané na základě priority, dopadu na daný systém atd.), zdrojovou a cílovou IP adresu paketu, informace o Transmission Control Protocol (TCP) a User Datagram Protocol (UDP) portech a použitých síťových a transportních protokolech, počet přenesených bytů skrze dané spojení a také zda již byla vykonána určitá preventivní akce z hlediska potenciálně nebezpečné události.

3.3.2 Sbírání informací

NIDPS poskytují možnosti sbírání informací na hostitelích, z hlediska síťové aktivity zahrnující i dané hostitele.

Je možná identifikace daných hostitelů, kde IDPS senzor dokáže vytvořit seznam všech hostitelských zařízení na základě jejich IP, případně Media Access Control (MAC) adres. Na základě tohoto seznamu je pak možné identifikovat nového hostitele na podnikové síti.

Další možnost je identifikace operačního systému. IDPS senzor může například zjistit, jaké porty jsou užity na jednotlivých hostitelích a tím pádem zjistit danou rodinu operačních systémů. Další technika vychází z analýzy hlaviček paketů (tato technika se nazývá passive fingerprinting) a na základě jejich charakteristik tak senzor dokáže poznat daný OS. Dále je možné zjistit OS na základě identifikace verzí aplikací používaných na daných hostitelích. Informace o OS jsou vhodné zejména v případě potřeby identifikovat potenciálně nechráněného hostitele respektive PC/server (uzel v dané síti). Podobně jako s identifikací OS pracuje senzor pro identifikaci verzí aplikací.

NIDPS umožňuje také identifikování síťové charakteristiky. To vše právě díky sběru informací o síťovém provozu vztažených ke konfiguraci síťových zařízení a hostitelů. Jako příklad lze uvést počet skoků mezi zdrojovým a cílovým zařízením. Informace o síti jsou užitečné především kvůli detekování změn v konfiguraci.

3.3.3 Detekce

Network-based IDPS používají kombinaci signature-based detekce, anomaly-based detekce a také techniky stateful protocol analysis. Všechny tyto detekční techniky pracují spolu v kooperaci, kde například stateful protocol analysis rozčlení určitou aktivitu na požadavky a odpovědi, ty jsou (za pomocí techniky založené na anomáliích) zkontrolovány na anomálie a následně porovnány se signaturami známých nebezpečných aktivit. Některé produkty také poskytují stejnou funkcionalitu jako NBA software.

(SCARFONE, a další, 2007)

3.3.4 Prevence

V podstatě existují tři druhy prevenčních schopností INDPS. Rozlišují se podle typu senzorů. Jsou to:

- **Pouze pasivní senzory –** Pasivní senzory mohou ukončit existující TCP spojení resp. relaci posláním TCP reset paketů na oba komunikující konce. Tomuto způsobu se někdy říká session snipping. Takto se senzor snaží, aby to pro jeden konec spojení vypadalo, že druhý konec chce ukončit spojení. Cílem je, aby jeden komunikující konec ukončil spojení předtím, než bude útok úspěšný. Problémem je, že často není tento způsob dostatečně rychlý, jelikož TCP reset pakety musí být poslány přes celou síť, k čemuž se musí ještě připočíst čas analýzy síťového provozu a detekce nebezpečné události. Vzhledem k tomu, že je tato technika použitelná pouze pro TCP spojení, nemůže zabránit útokům zahrnujících typy paketů jako například UDP nebo Internet Control Message Protocol (ICMP). Nejen kvůli tomu, již dnes není široce využívána a je spíše nahrazena novějšími technikami.

- **Pouze Inline senzory –** Inline senzory poskytují FW možnosti. Na základě nich mohou zahazovat či odmítat podezřelé aktivity v síťovém provozu. Inline senzory mohou také při nesprávném užití protokolu jako při DoS útoku omezit procento síťového přenosového pásma, které protokol používá. Tím se zabrání aktivitám, které mají negativní dopad na použití přenosového pásma pro jiné zdroje. Další možností, kterou Inline senzory disponují, je nahrazení škodlivého kódu v paketu za neškodný.

- **Použití obou typů senzorů dohromady –** Mnoho IDPS senzorů může dát pokyn k rekonfiguraci různým síťovým zařízením tak, aby blokovaly určité typy aktivit nebo je směrovaly jinam. Tento způsob je vhodný zvláště když je nutné udržet vnějšího útočníka mimo síť a vložit interní uzel sítě, v případě, že byl zkompromitován, do karantény (například je vložen do VLAN přímo určené jako karanténní). Některé senzory mohou také při detekování hrozby spustit administrátorem specifikované skripty.

(HUDEC, 200-?)

3.4 Omezení NIDPS technologie

Navzdory tomu, že NIDPS nabízejí rozsáhlé detekční možnosti, mají také určitá omezení. Mezi nejdůležitější z nich patří analýza zašifrovaného síťového provozu, řešení vysokého zatížení síťového provozu a slabá ochrana proti útokům směřujícím přímo na daný IDPS.

NIDPS nemohou detekovat útoky v rámci šifrovaného síťového provozu, což zahrnuje VPN spojení, HTTP (Hypertext Transfer Protocol) přes SSL a SSH sezení. Alexander doporučuje umístění NIDPS tak, aby dokázaly analyzovat síťový provoz buď před samotným šifrováním, nebo po rozšifrování.

Je důležité, aby byla vyřešena síťová propustnost a analýza zatížení sítě před nasazením NIDPS. Pokud tak nebude učiněno, NIDS může zahazovat pakety pod vysokým zatížením a tím tak nedetekovat bezpečnostní hrozby. Potenciální útočník tak problému souvisejícím s vysokým zatížením síťového provozu může snadno využít.

(ALEXANDER, 2009)

4 Wireless Intrusion Detection Prevention System

Wireless IDPS (WIDPS) monitorují bezdrátový síťový provoz a analyzují jeho bezdrátové síťové protokoly za účelem identifikovat podezřelou aktivitu, která může zahrnovat i protokoly samotné.

Bezdrátové sítě dovolují zařízením spolu komunikovat, aniž by byly fyzicky připojeny do sítě. Zařízení musí být pouze v určité vzdálenosti v rámci infrastruktury bezdrátové sítě. Skupina bezdrátově spojených síťových uzlů v určité omezené vzdálenosti, která si je schopná vyměňovat data, se nazývá Wireless Local Area Network (WLAN). Ty jsou běžně umísťovány do kancelářských budov a jsou implementovány jako rozšíření existujících lokálních sítí (Local Area Network – LAN) k podpoře mobility zaměstnanců.

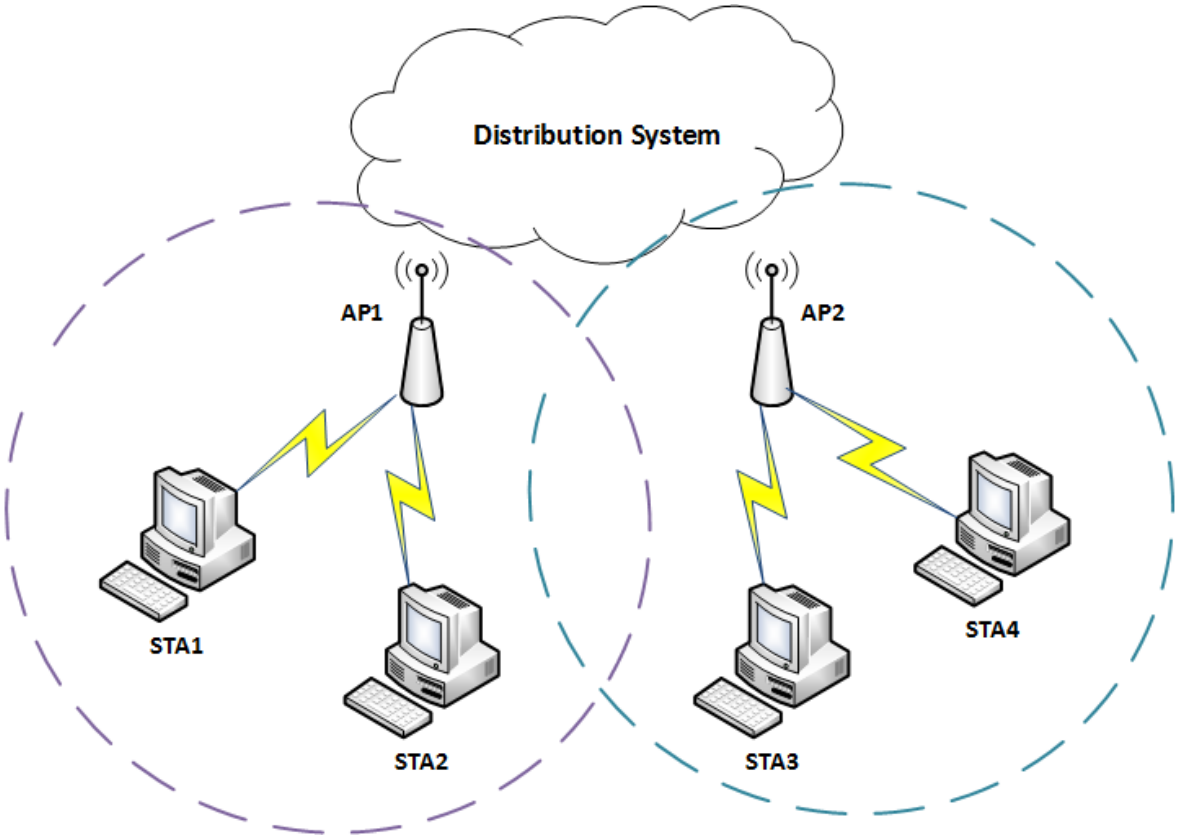
(SCARFONE, a další, 2007)

WLAN se nejčastěji skládá ze dvou komponent:

- **Station (STA) –** Jedná se o bezdrátové koncové zařízení. Typickým příkladem je notebook, chytrý telefon atd.
- **Access Point (AP) –** AP logicky spojuje STA s daným distribučním systémem, kterým je pevná (drátová) infrastruktura společnosti. Distribuční systém je prostředek, díky kterému může STA komunikovat s pevnou LAN a externí sítí jako je internet.

WLAN pracuje převážně ve dvou režimech. Ad hoc režim, který nevyužívá AP. Zahrnuje dvě a více STA komunikujících přímo mezi sebou. Druhý režim se nazývá Infrastrukturní režim**,** ve kterém AP logicky připojuje STA k distribučnímu systému, což je klasicky drátová síť. Téměř všechny organizace používají WLAN v Infrastrukturním režimu.

(HUDEC, 200-?)



Obrázek 8 – Příklad WLAN architektury

Zdroj: Přepracováno od: (SCARFONE, a další, 2007)

Každý AP a STA na WLAN může být identifikován svou MAC adresou, kterou má přidělenou bezdrátová síťová karta. MAC adresa jednoznačně identifikuje každé bezdrátové zařízení. Nicméně je relativně jednoduché ji podstrčit za jinou (SCARFONE, a další, 2007).

Každý AP ve WLAN má přiřazené jméno, které se nazývá Service Set Identifier (SSID). SSID umožňuje STA odlišit jednu WLAN od druhé. AP vysílá SSID ve formátu obyčejného textu, tudíž se může každé přijímací bezdrátové zařízení lehce SSID dané WLAN dozvědět. Samozřejmě pokud se nachází v dosahu zařízení (HUDEC, 200-?).

4.1 Komponenty Wireless IDPS

Komponenty WIDPS jsou shodné jako u NIDPS. Jedná se tedy o konzole, databázové servery, management servery a senzory. Jediné komponenty, které se liší svoji funkcionalitou od NIDPS, jsou právě senzory. Bezdrátové senzory mají stejnou roli jako NIDPS senzory, nicméně jejich funkce je odlišná díky monitoringu právě bezdrátové komunikace (SCARFONE, a další, 2007).

Hlavní rozdíl oproti NIDPS spočívá v tom, že bezdrátové IDPS pracují na principu vzorkování síťového provozu. Existují dvě frekvenční pásma pro monitorování. Je to pásmo 2,4 GHz a 5 GHz. Každé pásmo je rozděleno na kanály. Senzor může v daném čase monitorovat pouze jeden kanál v určitém pásmu a ne celou síťovou komunikaci. V případě,

že senzor monitoruje jeden kanál po delší dobu, vzniká šance, že neodhalí nebezpečnou aktivitu na jiném kanálu. Tento problém se potlačuje metodou zvanou channel scanning (skenování kanálů). Tím dojde k častému přepínání kanálů a tedy k tomu, že senzor monitoruje každý kanál několikrát za sekundu.

(SCARFONE, a další, 2007)

4.1.1 Typy bezdrátových senzorů

Bezdrátové senzory jsou dostupné v několika typech:

- **Dedikované –** Dedikovaný senzor je zařízení, vykonávající funkci WIDPS, ale nepropouští síťovou komunikaci od zdroje k cíli. Tyto senzory jsou často pasivní a jen odchytávají síťový provoz, který mají v daném kanále na dosah. Některé specializované senzory provádějí analýzu síťového provozu samy, nicméně některé ji jen přeposílají na odpovídající management server, kde dojde k následné analýze. Samotný senzor je klasicky připojený ke drátové síti (například ethernetovým kabelem mezi senzorem a přepínačem). Dedikovaný senzor může být fixní, tj. nasazený na určitém místě v závislosti na firemní infrastruktuře. Nebo mobilní pro použití v pohybu. Správce sítě může mobilní senzor použít při procházení budovou společnosti a k vyhledání škodlivého AP. Fixní senzory jsou zpravidla HW zařízení, kdežto mobilní senzory mohou být i speciální SW, nainstalované např. na správcově notebooku s bezdrátovou síťovou kartou.

- **Ve spojení s AP –** Někteří výrobci přidávají určitou funkcionalitu IDP systémů přímo do AP. Obvykle toto spojení ale nedosahuje takové míry zabezpečení jako např. dedikované senzory, jelikož AP musí dělit svůj výpočtový čas mezi poskytování přístupu k síti a monitorování více kanálů, případně pásem, zda neobsahují škodlivé aktivity. V případě, že IDPS musí monitorovat více pásem nebo kanálů, senzor musí provádět skenování kanálů a tím může dojít k přerušení funkčnosti AP senzoru a ten se pak stane nedostupný na jeho primárním pásmu a kanálu. Tento typ senzorů je tedy vhodný spíše pro potřeby monitorování jednoho pásma a kanálu.

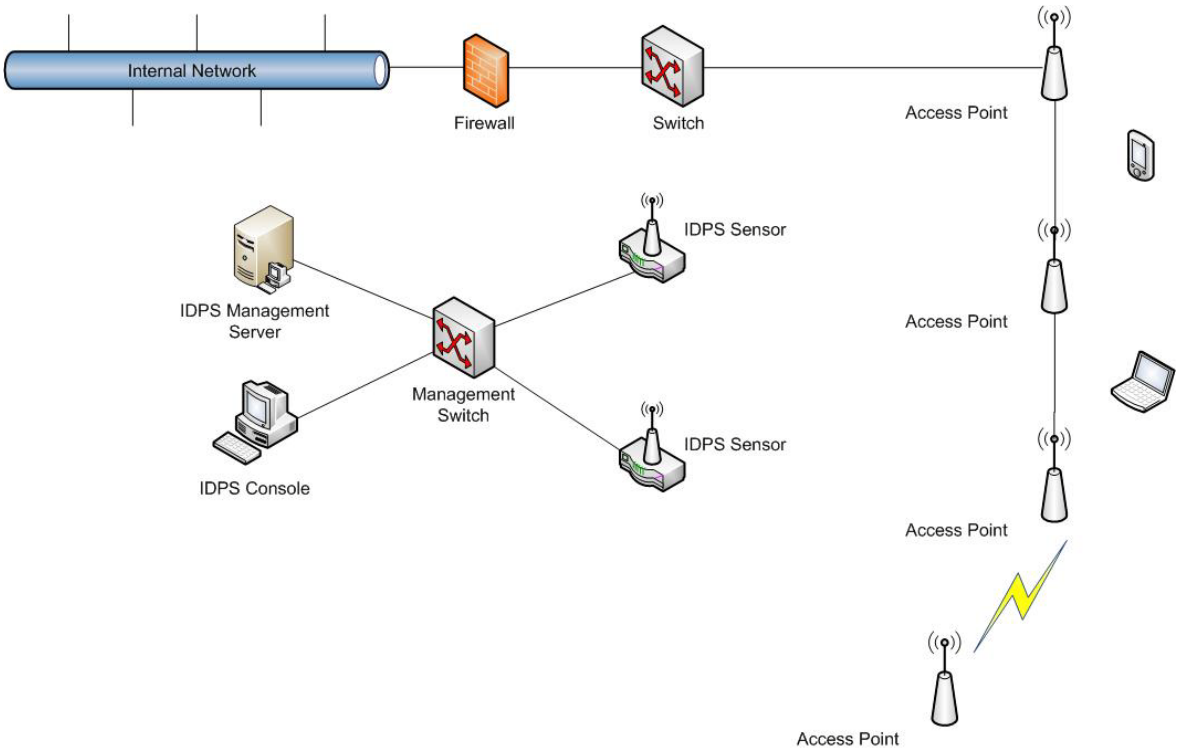
- **Ve spojení s bezdrátovým přepínačem –** Některé bezdrátové přepínače poskytují také určité funkce bezdrátových IDPS, nicméně v porovnání s předešlými dvěma typy nedosahují takových detekčních schopností.

(HUDEC, 200-?)

Dedikované WIDPS senzory nabízejí často největší míru detekce v porovnání s ostatními typy. Je to hlavně z důvodu, že se nemusí starat o bezdrátový provoz. Bohužel jsou ale cenově dražší, složitější na instalaci a náročnější na celkový provoz (SCARFONE, a další, 2007).

4.2 Síťová architektura komponent

WIDPS komponenty jsou spolu spojeny skrze klasickou drátovou síť. Jako u NIDPS je doporučeno separovat management síť pro bezproblémovou komunikaci mezi WIDPS komponenty. Jak již bylo zmíněno, některé WIDPS senzory, většinou mobilní, jsou použity samostatně a nepotřebují drátové síťové spojení (ALEXANDER, 2009).



Obrázek 9 – WIDPS síťová architektura

Zdroj: (ALEXANDER, 2009)

Volba umístění senzorů při nasazení WIDPS je naprosto odlišná od ostatních technologií IDPS. Pro organizace může být žádoucí, nasazovat senzory kvůli monitorování oblastí, kde není žádná WLAN aktivita. To může napomoci k detekování škodlivých AP případně ad hoc sítí WLAN. Typicky se WIDPS senzory umisťují na základě:

- **Fyzické bezpečnosti –** Senzory jsou často umísťovány do otevřených prostranství jako chodby, stropy, místnosti. Někdy jsou senzory umísťovány také do venkovních prostor. Obecně tedy platí, že WIDPS senzory jsou více náchylné k fyzickým poškozením.
- **Dosah senzoru –** Samotný dosah senzoru závisí na okolních budovách, zdech, dveřích atd., přičemž někteří WIDPS výrobci nabízejí SW, který napomáhá při umístění senzorů na základě jejich dosahu.
- **Cena –** V ideálním případě se organizace snaží umístit senzory tak, aby pokryly celou firemní infrastrukturu a mohly tak provádět monitorování bezdrátové sítě. U

větších organizací samozřejmě narůstá požadavek na množství senzorů, s čímž souvisí vyšší náklady. Je tedy nutné nalézt správný poměr ceny a výkonu na základě potřeb dané organizace.

(ALEXANDER, 2009)

- **Připojení k drátové síti –** Senzory je nutno připojit k drátové síti. Pokud nastane situace, kdy je nutné nasadit senzor do prostoru, kde není vyvedeno drátové připojení, je nutné ho v daném prostoru vyvést.

(SCARFONE, a další, 2007)

4.3 Bezpečnostní možnosti WIDPS

WIDPS poskytuje několik typů bezpečnostních možností. Klasicky se dají rozdělit do čtyř kategorií. Jsou jimi: Možnosti logování, sběr informací, detekční možnosti a prevenční možnosti. Z důvodu, že jsou WIDPS relativně nové v porovnáním se zbylými technologiemi, možnosti zabezpečení se vcelku liší napříč nabízenými produkty. Časem by však měly být více konzistentní (SCARFONE, a další, 2007).

4.3.1 Logování

Podobně jako NIDPS, WIDPS provádějí rozsáhlé logování dat příslušících k daným detekovaným událostem. Pole dat obvykle obsahují záznamy jako časová razítka, typ události nebo reportu, ohodnocení (počítané na základě priority, dopadu na daný systém atd.), zdrojovou MAC adresu, číslo kanálu, identifikační číslo senzoru, který zpozoroval danou událost a vykonanou preventivní akci, pokud bylo potřeba nějakou vykonávat.

4.3.2 Sbírání informací

Většina WIDPS může sbírat informace o bezdrátových zařízeních.

Přednostně umožňují identifikovat WLAN zařízení, tím, že si senzory vytvoří seznam pozorovaných WLAN zařízení, který pak spravují a udržují aktuální. Seznam je založen na SSID a MAC adrese bezdrátové NIC daného zařízení. Některé senzory užívají techniku otisku v pozorovaném síťovém provozu ke kontrole výrobce bezdrátové NIC, protože MAC adresu lze poměrně jednoduše podvrhnout. Seznam může také identifikovat nové bezdrátové zařízení nebo odebrat stávající.

Dále je možná identifikace i celých WLAN. Senzory udržují informace o jednotlivých bezdrátových sítích na základě jejich SSID. Správce sítě potom může označovat různé bezdrátové sítě v seznamu jako autorizované, neškodné sousední sítě (například jiná organizace ve stejné budově) a škodlivé WLAN.

(HUDEC, 200-?)

4.3.3 Detekce

WIDPS umožňují detekovat útoky, chybné konfigurace a porušení politiky na úrovni WLAN protokolu, a to hlavně prověřením IEEE (Institute of Electrical and Electronics Engineers)

802.11a, b, g, i a ac standardu. WIDPS neprověřují komunikaci na vyšších úrovních (IP adresy, aplikační data v paketech). Některé produkty provádějí pouze jednoduchou signature-based detekci, některé používají kombinaci signature-based detekce, anomaly-based detekce a techniky stateful protocol analysis.

WIDPS umožňují detekovat následující typy událostí:

- **Neautorizované WLAN a WLAN zařízení –** Skrze možnosti sbírání informací WIDPS mohou senzory detekovat škodlivé AP, neautorizované STA a WLAN.

- **Nedostatečně zabezpečená WLAN zařízení –** Většina WIDPS senzorů dokáže identifikovat nedostatečně zabezpečené AP a STA. To zahrnuje detekci špatné konfigurace a použití slabých WLAN protokolů a jejich implementací. To je docíleno porovnáním odlišností od specifikovaných bezpečnostních politik organizací, jako je typ šifrování, autentifikace, datové přenosy, SSID jména a kanály. Jako příklad lze uvést senzor, který detekuje odlišnost v šifrování použité u konkrétní STA. Organizací je dáno, že by mělo být použito šifrování Wired Equivalent Privacy (WEP) místo použitého WEP2.

- **DoS útoky –** DoS útoky sestávají z logického útoku, který v sobě zahrnuje zasílání velkého množství zpráv o velké intenzitě na určité AP a fyzického útoku, který se skládá z vyslání elektromagnetické energie na WLAN frekvencích tak, aby byly tyto frekvence pro konkrétní WLAN nedostupné. DoS útoky jsou často detekovány skrze techniku stateful protocol analysis a anomaly-based detekcí, které zjistí, zda monitorovaná aktivita je konzistentní s očekávanou. Mnoho DoS útoků je detekováno počítáním událostí v rámci časových period, a pokud jich je více, než je zadaná maximální hodnota, je vysláno upozornění na detekování útoku.

- **Imitace a man-in-the-middle útoky –** Některé WIDPS senzory umožňují zjistit, pokud se zařízení snaží imitovat identitu jiného, a to na základě identifikace odlišností v charakteristice monitorované aktivity (např. určité hodnoty v rámcích).

- **Neobvyklé použití –** Senzory na základě anomaly-based detekce zjistí neobvyklé vzory užití. Jako příklad lze uvést, když v určitý čas užívá konkrétní AP o mnoho více STA, než je obvyklé. Jedno ze zařízení může být kompromitováno.

(SCARFONE, a další, 2007)

Důležitou vlastností WIDPS senzorů je tzv. triangulace. Na základě ní, jsou schopny identifikovat fyzické umístění detekované hrozby. Triangulace funguje na základě odhadu přibližné vzdálenosti hrozby od více senzorů, díky síle signálu hrozby přijatého každým senzorem. Následuje výpočet fyzického místa, na kterém by hrozba měla být umístěna. Organizace potom může poslat pracovníky na konkrétní místo, případně alespoň definovat přibližné místo, kde se hrozba nachází.

(HUDEC, 200-?)

4.3.4 Prevence

Senzory WIDPS nabízejí bezdrátové a drátové možnosti prevence průniků.

Co se týče bezdrátových možností, senzory dokáží ukončit spojení mezi škodlivou, případně špatně nakonfigurovanou STA a autorizovaným AP a naopak. K ukončení spojení obvykle dochází zasláním zprávy na oba koncové body, s příkazem na ukončení stávajícího sezení. Senzor potom odmítne požadavek na založení nového spojení mezi těmito dvěma zařízeními.

Drátová prevence funguje tak, že senzor zašle zprávu na přepínač v drátové síti, která obsahuje požadavek na blokování určité síťové aktivity mezi konkrétními STA a AP na základě jejich MAC adres nebo portu přepínače. Tento způsob prevence je efektivní pouze pro blokování škodlivé STA nebo AP při komunikaci v drátové síti. Nezastaví tedy STA, či AP v pokračování šíření škodlivé aktivity skrze bezdrátové protokoly.

(SCARFONE, a další, 2007)

4.4 Omezení WIDPS technologie

Navzdory tomu, že WIDPS nabízejí rozsáhlé detekční možnosti, mají také určitá omezení. Mezi nejdůležitější z nich patří neschopnost detekovat určité útoky na základě bezdrátového protokolu, citlivost na techniku uhýbání a neschopnost efektivně čelit útokům namířeným přímo proti IDPS.

WIDPS nedokáže detekovat pasivní útoky proti bezdrátovým sítím. Útočník tak může monitorovat bezdrátový provoz, a pokud jsou použity slabé bezpečnostní metody jako například WEP, je schopen dohledat šifrovací klíč. Následně pak může nedetekován rozšifrovat celou bezdrátovou komunikaci.

(ALEXANDER, 2009)

5 Systém Network Behavior Analysis

Network Behavior Analysis (NBA) systém zkoumá síťový provoz nebo jeho statistiky k identifikování neobvyklých proudů síťového provozu, jako např. DDoS útoky, některé formy malwaru (červy, trojské koně) a porušení bezpečnostní politiky.

(SCARFONE, a další, 2007)

5.1 Komponenty systému NBA

Scarfone uvádí, že NBA řešení nabízí obvyklé komponenty jako senzory, konzole a některé produkty také nabízejí management servery, kterým se někdy říká analyzéry. NBA senzory jsou často dostupné pouze ve formě samotného zařízení (SCARFONE, a další, 2007).

Některé NBA IDS/IPS senzory jsou stejné jako NIDPS senzory. Hlavně ve věci odchytávání paketů kvůli monitorování síťové aktivity na jednom nebo více síťových segmentů. Zbylé NBA senzory nemonitorují sítě přímo, ale spoléhají se na informace o síťovém proudu poskytované síťovými zařízeními (ALEXANDER, 2009).

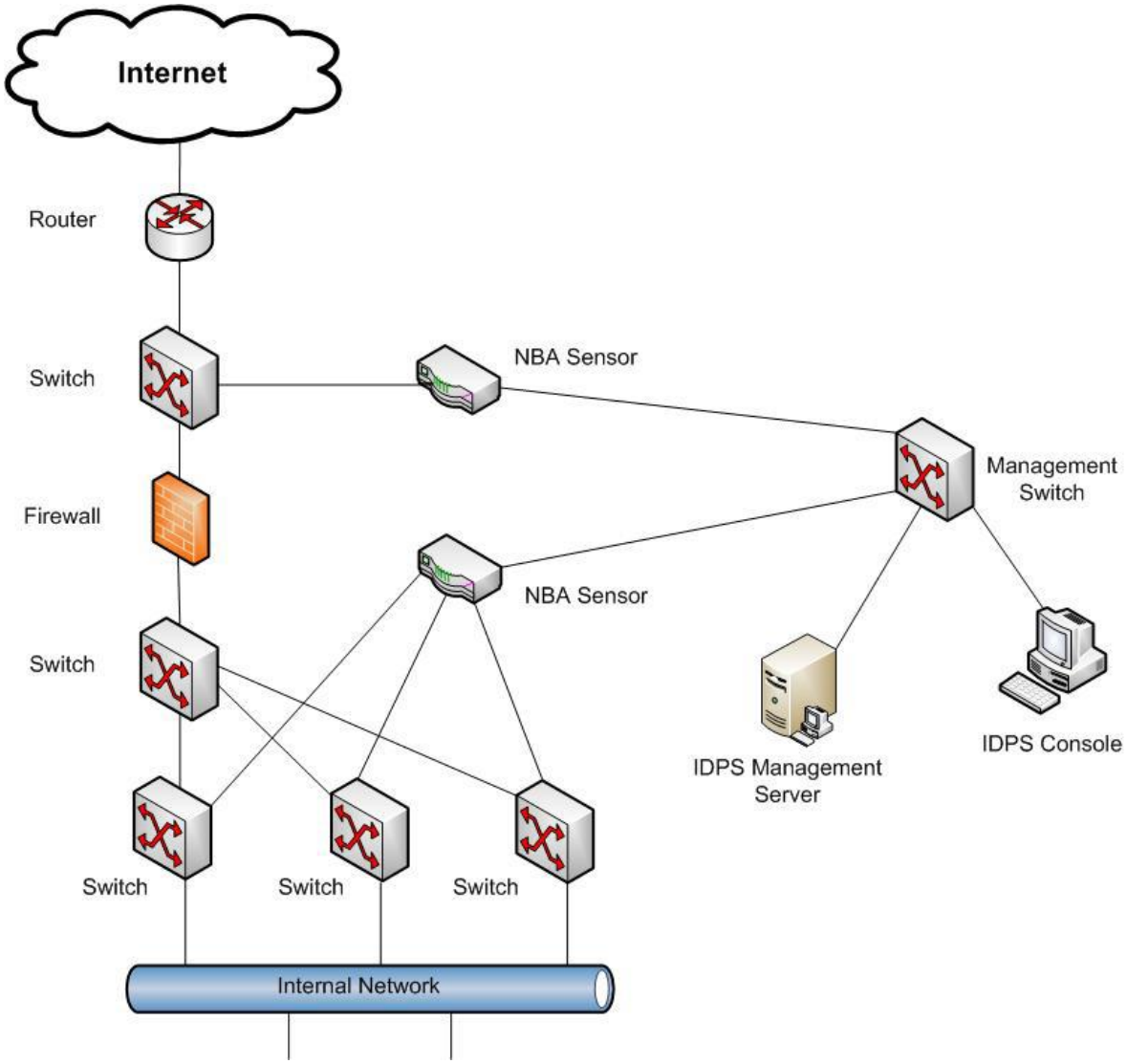
Síťový proud odpovídá komunikačnímu sezení mezi danými uzly sítě. Pro formáty dat, proudícími skrze proud existuje mnoho standardů jako například NetFlow od společnosti Cisco či sFlow. Typické položky obsaženy v datových proudech jsou zdrojová a cílová IP adresa, zdrojové a cílové TCP nebo UDP porty, počet paketů a počet bajtů přenesených v komunikačním sezení. Jako poslední položku datové proudy obsahují časová razítka začátku a konce komunikačního sezení.

(SCARFONE, a další, 2007)

5.2 Síťová architektura komponent

Tak jako u NIDPS, je vhodné separovat management síť i pro komunikaci komponent u NBA technologie. Pokud jsou použity senzory, které zaznamenávají data síťových proudů z jiných zařízení, celé řešení NBA může být logicky separováno mimo produkční síť.

(ALEXANDER, 2009)



Obrázek 10 – NBA síťová architektura

Zdroj: (ALEXANDER, 2009)

Co se týče návrhu odpovídající síťové architektury komponent, správci musejí nejprve rozhodnout o umístění senzorů. Většina NBA senzorů může být nasazena pouze v pasivním módu, používající stejné metody připojení jako NIDPS senzory. Pasivní senzory, které provádějí přímý monitoring sítě, by měly být umístěny tak, aby mohly monitorovat klíčová síťová umístění, jako jsou hranice mezi jednotlivými sítěmi, případně podsítě DMZ. Inline senzory by měly být umístěny v blízkosti FW, často mezi FW a směrovač, na hranici s internetem, aby se omezily příchozí útoky, které by mohly přetížit FW (ALEXANDER, 2009).

5.3 Bezpečnostní možnosti systému NBA

NBA poskytuje několik typů bezpečnostních možností. Obvykle se dělí do čtyř kategorií, kterými jsou: Možnosti logování, sběr informací, detekční možnosti a prevenční možnosti.

5.3.1 Logování

Podobně jako ostatní technologie, NBA provádějí rozsáhlé logování dat příslušících k daným detekovaným událostem. Tato data mohou být použita k potvrzení platnosti upozornění, k prověření bezpečnostních incidentů atd. Pole dat obvykle obsahují záznamy jako časová razítka, typ události nebo upozornění, ohodnocení (počítané na základě priority, dopadu na daný systém atd.), síťové, transportní a aplikační protokoly, zdrojovou a cílovou IP adresu a porty TCP nebo UDP, další pole z paketové hlavičky jako např. TTL, počet bajtů a paketů poslaných od zdroje či cíle za dobu spojení a vykonanou preventivní akci, pokud bylo potřeba nějakou vykonávat.

Některé NBA senzory, které přímo monitorují síťový provoz, jsou schopny logovat omezené informace z datové části hlavičky paketů, jako jsou například identifikační údaje autentifikovaného uživatele. To umožňuje monitorovat aktivity konkrétních uživatelských účtů.

5.3.2 Sbírání informací

IDPS technologie NBA nabízí rozsáhlé možnosti sběru informací. Je to z toho důvodu, že NBA produkty musí znát charakteristiky hostitelů celé organizace, aby mohly efektivně provádět detekci. NBA senzory dokáží automaticky vytvořit a spravovat seznam hostitelů komunikujících na monitorované síti organizace. Konkrétněji monitorují použité porty, provádějí pasivní snímání otisků (passive fingerprinting), a používají další techniky k získání detailních informací o hostitelích. Jsou to například informace o IP adresách, použitém OS a o službách, které jsou používány. NBA senzory neustále monitorují síťovou aktivitu právě kvůli změnám těchto informací.

5.3.3 Detekce

Technologie NBA umožňují detekovat různé typy nebezpečných událostí. Většina produktů používá hlavně anomaly-based detekci v kombinaci s technikou stateful protocol analysis k analyzování síťových proudů. Velká část NBA produktů neposkytuje žádnou signature-based detekci, nicméně správci sítě mohou manuálně nastavit filtry, které mohou sloužit v podstatě jako příznaky a na základě nich detekovat nebo zastavit určité hrozby.

NBA umožňují detekovat následující typy událostí:

- **DoS útoky** – Některé NBA senzory znají charakteristiky běžných DoS prostředků a metod. To jim dopomáhá rychleji rozpoznat tento typ útoku.
- **Skenování** – Skenování může být detekováno neobvyklými datovými proudy na aplikační, transportní a síťové vrstvě.
- **Červy** – Červi mohou být detekováni více způsoby. Nějací červi provádějí skenování, což je vysvětleno v předchozím bodě. Někteří využívají velké množství šířky pásma. Někteří způsobují komunikaci mezi hostiteli, která se obvykle neděje. To samé platí pro porty. Může se stát, že hostitelé začnou používat porty, které normálně nevyužívají.

- **Neočekávané aplikační služby** – Tento typ útoku je detekován za pomocí metod stateful protocol analysis, které dokáží rozhodnout, zda aktivita v rámci daného spojení náleží pod očekávaný aplikační protokol.

- **Porušení bezpečnostní politiky** – Většina NBA senzorů umožňuje správcům nadefinovat detailní bezpečnostní politiku, jako například jaké typy aktivit jsou dovoleny pouze během určité doby atd. Velké množství senzorů také detekuje možné porušení bezpečnostní politiky automaticky. Jedná se kupříkladu o detekování nových služeb běžících na hostitelích, které nejsou autorizované.

NBA senzory také mohou sestavit sérii prozkoumaných událostí za účelem zjistit původ hrozby. Když například červ infikuje síť. NBA senzory mohou analyzovat červův síťový proud a zjistit hostitele na síti, který jako první odeslal červa na dalšího.

5.3.4 Prevence

Prevenční možnosti NBA senzorů závisí na typu senzorů. Pasivní senzory umožňují ukončit aktuální TCP sezení zasláním resetovacích paketů na oba koncové body. Inline senzory zase poskytují možnost inline FW, který slouží k zahození, či odmítnutí podezřelé síťové aktivity. Kombinace pasivních a inline senzorů může sloužit ke změně konfigurace bezpečnostních síťových zařízení (FW, směrovače atd.), aby blokovaly určité typy aktivit nebo je přesměrovaly jinam, například do karanténní VLAN. Mohou také při detekování nebezpečné aktivity spustit správcem definovaný skript či program.

NBA senzory také dovolují správcům specifikovat konfigurace prevenčních možností pro každý typ upozornění. To obvykle zahrnuje úplné povolení nebo zakázání prevence nebo specifikaci, jaký typ prevenčních možností má být použit. Většina implementací NBA používá prevenční možnosti v omezené míře kvůli false positive detekci. Zablokování jediné false positive události může způsobit velké narušení v síťové komunikaci. Prevenční možnosti často používají NBA senzory k zablokování konkrétní známé hrozby, jako například nového červa.

(SCARFONE, a další, 2007)

5.4 Omezení NBA systému

NBA IDPS nabízejí silné detekční možnosti v rámci určitých typů hrozeb, nicméně mají také určitá omezení. Důležité omezení je zpoždění v detekci útoků. Zpoždění je hlavně v metodách založených na detekci anomálií, jako je zvětšená šířka pásma nebo neobvyklé množství pokusů o připojení. Nicméně NBA systém často trpí zpožděním způsobeným jeho zdroji dat, hlavně pokud spoléhají na data z jiných síťových zařízení (ALEXANDER, 2009).

6 Host-based Intrusion Detection Prevention System

HIDPS monitorují charakteristiky jednoho konkrétního hostitele v síti a události, které se v rámci něj objevují, na podezřelé aktivity. Typy charakteristik, které HIDPS mohou monitorovat, jsou např. drátový a bezdrátový síťový provoz, systémové logy, běžící procesy, datové přístupy a jejich modifikace, změny v konfiguraci systému, případně aplikace.

(HUDEC, 200-?)

6.1 Komponenty HIDPS

Většina řešení HIDPS má detekční SW, tzv. agenty. Ten může být instalován na konkrétní hostitele, kteří jsou bodem zájmu v rámci monitoringu. Každý agent provádí monitoring aktivit na jednotlivých hostitelích, a pokud jsou povoleny IPS možnosti, provádí také prevenční akce. Agenti posílají data na management servery, které mohou volitelně používat ještě databázové servery pro ukládání dat. Management servery jsou použity většinou v rámci podnikové sítě. Samozřejmě je možné, aby agenti byli nasazeni samostatně a následně pak spravováni a monitorováni přímo správcem daného hostitele, tedy aniž by posílali data na management server. Správce pak může spravovat a monitorovat agenty skrze konzole.

Některé HIDPS produkty používají ale samostatná zařízení, na kterých běží SW agent. Ten tedy není instalován přímo na hostitele. Zařízení, na kterém se agent nachází, je umístěno tak, aby monitorovalo síťový provoz, směřující do, či z určitého hostitele. Pro jejich inline připojení jsou často tato zařízení považována za klasická NIDPS řešení. Nicméně tato zařízení obvykle monitorují aktivity sítě pouze pro jeden konkrétní typ aplikace, jako například databázový server nebo web server. Z toho vyplývá, že jsou více specializována než standardní NIDPS řešení a SW, který běží na daném zařízení, má z velké části stejnou funkcionalitu jako klasický Host-based agent. Agenti se dělí podle toho, jaký typ zařízení mají ochraňovat na:

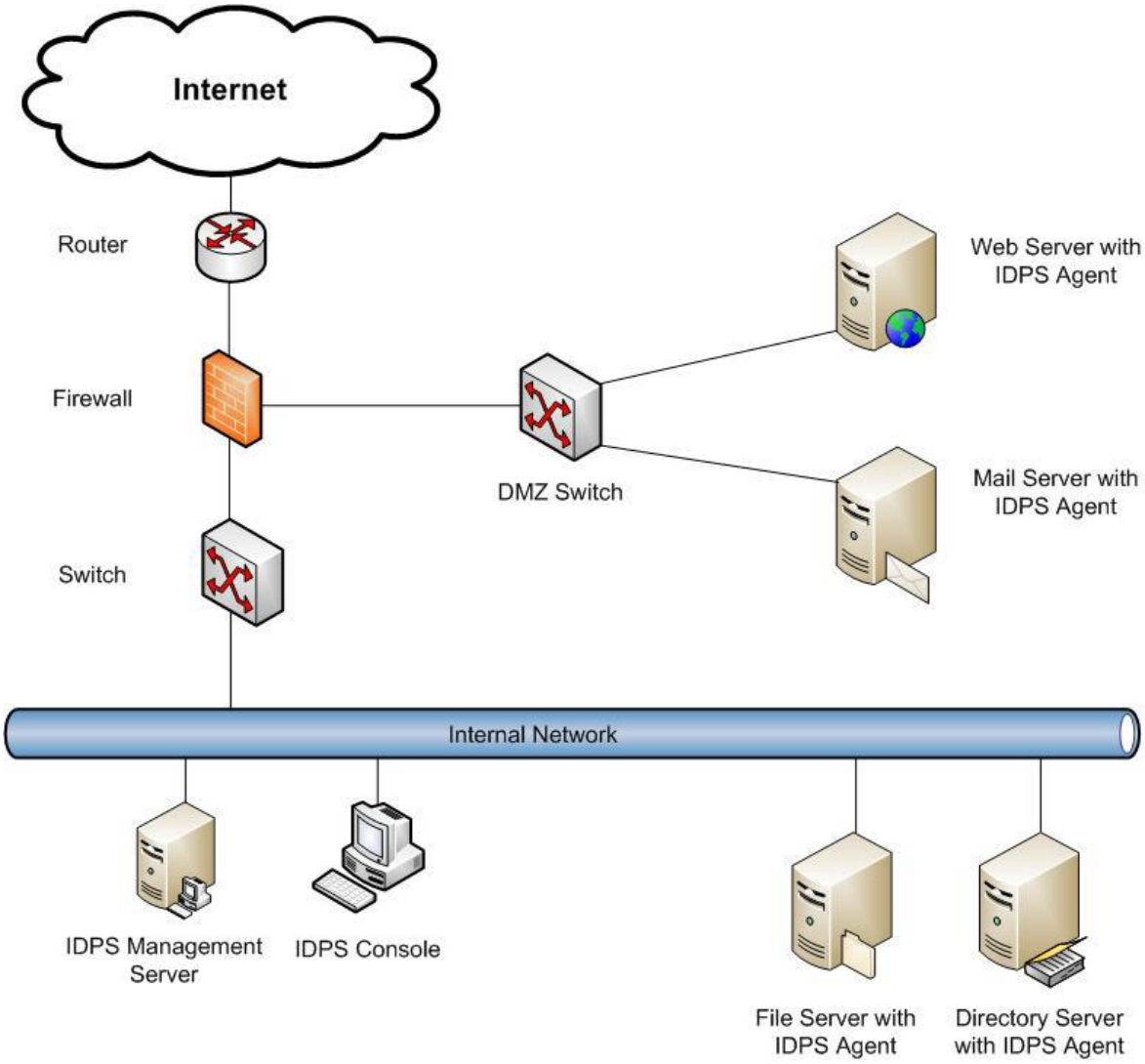
- **Server agenti –** Kromě monitorování OS serveru, mohou agenti této kategorie monitorovat určité běžné aplikace ze strany serveru.
- **Klient agenti –** Monitorování OS a běžných aplikací. Například webových prohlížečů, mailových klientů atd. Zkrátka aplikací ze strany klienta, což je stolní PC, či notebook.
- **Agenti aplikačních služeb –** Provádějí monitoring pouze konkrétní aplikace nebo služby. Například určitý program webového serveru. Tento typ agentů se nazývá Application-based IDPS.

(SCARFONE, a další, 2007)

6.2 Síťová architektura komponent

Síťová architektura pro nasazení systémů HIDP je obvykle velmi prostá. Vzhledem k tomu, že agenti jsou nasazeni většinou na existující hostitele v síti společnosti, komunikují spolu komponenty prostřednictvím této produkční sítě, místo separované management sítě. Drtivá většina produktů HIDPS šifruje svou komunikaci a tím brání útočníkovi například v přístupu k citlivým informacím (ALEXANDER, 2009). Agenti, jako samotná zařízení, jsou nasazováni inline přímo před hostitele, kterého mají ochraňovat (HUDEC, 200-?).

Otázka nasazení agentů jako samostatných zařízení nebo přímo na konkrétního hostitele je velice důležitá. Z hlediska detekce a prevence je totiž vhodnější nainstalovat agenty přímo na hostitele, protože tak mají přímý přístup k jejich charakteristikám a často dovolují provádět mnohem přesnější a obsáhlejší detekční a prevenční aktivity. Na druhou stranu často podporují velice málo základních OS. V tomto případě je možné použít agenta jakožto samostatné zařízení. Další problém je čistě výkonového rázu. Agent totiž může negativně ovlivňovat výkon hostitele, na kterém je nainstalován. Z toho vyplývá další důvod použití agenta jako samostatného zařízení, čímž lze snížit potenciální degradaci výkonu hostitele (SCARFONE, a další, 2007).



Obrázek 11 – HIDPS síťová architektura

Zdroj: (ALEXANDER, 2009)

HIDPS agenti jsou běžně nasazováni na kritické hostitele, jako jsou například veřejně přístupné servery, případně servery obsahující citlivé informace. Z důvodu toho, že jsou agenti dostupní pro různé serverové i desktopové OS, je mohou organizace potenciálně nasadit v rámci celé své infrastruktury (např. interní servery, klasické pracovní stanice). Použití HIDPS dovoluje organizacím monitorovat bezpečnostní události, které by jiné technologie detekovat nemohly. Jako příklad lze uvést NIDPS technologii a její neschopnost analyzovat aktivity v šifrované síťové komunikaci (ALEXANDER, 2009).

Umístění HIDPS agentů závisí na určitých kritériích. Například na ceně nasazení, správy a monitorování daného agenta. Dále na OS a aplikacích, které agenti podporují, na důležitosti dat a služeb na jednotlivých hostitelích, které ukazují, zda se vyplatí na konkrétního hostitele agenta nasadit či nikoliv. V poslední řadě je to schopnost celé infrastruktury podporovat agenty (dostatečná šířka pásma pro přenos upozornění vyslaných z agentů na centralizované

servery a naopak pro zasílání aktualizací z centralizovaných serverů na konkrétní agenty) (SCARFONE, a další, 2007).

Pro poskytnutí schopnosti prevence průniků, většina IDPS agentů mění interní architekturu hostitelů, na kterých jsou nasazeni. To je realizováno speciální vrstvou kódu, která je nasazena mezi již existující vrstvy kódu. Tato vrstva se nazývá shim a zachytává data na místě, kde by za normálních okolností byla předána z jedné části kódu do druhé. Shim potom data analyzuje a rozhoduje o jejich povolení nebo odmítnutí. HIDPS agenti mohou použít shim pro různé zdroje, jako jsou: Síťový provoz, aktivity systému dat, systémová volání, registry OS Windows a běžné aplikace.

Určitá část HIDPS agentů nemění architekturu hostitelů a monitoruje aktivitu bez vrstvy shim nebo analyzuje pouze projevy aktivit, jako jsou položky v logu a modifikace souborů. Tento způsob je pro hostitele méně rušivý, nicméně snižuje možnost IDPS zasahovat do normálních operací daného hostitele a činí ho tak méně efektivní v detekování hrozeb. Často také toto řešení agentů nedokáže provádět žádné prevenční akce k zabránění nebezpečných aktivit na síti.

(HUDEC, 200-?)

6.3 Bezpečnostní možnosti HIDPS

HIDPS poskytují množství bezpečnostních možností. Ty se dělí do čtyř kategorií. Těmi jsou: Možnosti logování, detekční možnosti, prevenční možnosti a ostatní bezpečnostní možnosti.

6.3.1 Logování

HIDPS provádějí logování dat příslušících k daným detekovaným událostem. Tato data mohou být použita k potvrzení platnosti upozornění, k prověření bezpečnostních incidentů a k prověření vztahu událostí mezi HIDPS a jiným zdrojem logování. Data obvykle obsahují následující záznamy: Časová razítka, typ události nebo upozornění, ohodnocení (počítané na základě priority, dopadu na daný systém atd.), detail o události (IP adresu a informace o portech, aplikační informace, jména souborů a cesty k nim a případně uživatelský identifikátor) a vykonanou preventivní akci, pokud bylo potřeba nějakou vykonávat (SCARFONE, a další, 2007).

6.3.2 Detekce

Typy událostí detekovaných HIDPS se liší v závislosti na detekčních metodách, které používají. Některé produkty HIDPS nabízejí více detekčních metod, zatímco jiné se soustředí pouze na jednu. Některé produkty například pouze analyzují síťový provoz a jiné pouze kontrolují integritu důležitých dat.

Nejdůležitější detekční techniky HIDPS technologie jsou:

- **Analýza kódu –** Analýza kódu sestává ze tří metod. Jsou to: Analýza chování kódu, detekce přetečení bufferu a monitorování systémových volání. HIDPS agenti analyzují pokusy na provedení určitého kódu a mohou na základě těchto metod

identifikovat podezřelou aktivitu. Všechny metody dokáží zastavit malware a různé typy útoků, které by povolily neautorizovaný přístup, provedení kódu či změnu práv.

- **Analýza síťového provozu –** Technika podobná detekci používané v technologii NIDPS. Oproti analýze síťové, transportní a aplikační vrstvy jsou agenti HIDPS schopni zahrnout do běžných aplikací zvláštní zpracování. Například u mailových klientů jsou při analýze síťového provozu odeslané přílohy rozbaleny a kontrolovány, zda neobsahují škodlivý kód.

- **Monitorování Systému souborů –** Monitorování FS (File System) může být provedeno metodami jako kontrola integrity souboru, kontrola atributů souboru a pokusy o přístup k souboru. Kontrola integrity souboru funguje na bázi periodického generování kontrolních součtů pro důležité soubory. Ty jsou potom porovnávány s určitou známou hodnotou a jsou zjištěny případné rozdíly. Kontrola atributů souboru je v podstatě periodická kontrola atributů. Například informace o vlastníkovi souboru, práva na změnu souboru atd. Tyto dvě metody pouze zjistí fakt, že došlo ke změně souboru, až když daná změna nastane. Co se týče metody pokusů o přístup k souboru, agent má shim na FS a může monitorovat všechny pokusy o přístup ke kritickým souborům. Může také dané podezřelé pokusy zastavit. Agent má seznam bezpečnostních politik, které se týkají přístupu k souborům, ty pak následně porovná s charakteristikami aktuálních pokusů o přístupy k souboru a rozhodne se, zda je zamítne nebo nikoliv. Tato metoda tedy zabraňuje instalaci některých forem škodlivého kódu, a tím v podstatě splňuje i prevenční možnosti.

- **Analýza logů –** Někteří agenti mohou monitorovat a analyzovat OS a aplikační logy k identifikování podezřelé aktivity. Tyto logy mohou obsahovat informace o systémových událostech, jako je vypnutí systému a spuštění určité služby. Dále mohou být v logu obsaženy informace o bezpečnostních událostech, jako jsou úspěšné a neúspěšné pokusy o autentizaci a změny bezpečnostní politiky. V logu se často objevují také aplikační události, jako spuštění a zastavení konkrétní aplikace, chyby aplikace nebo změny v její konfiguraci.

- **Monitorování síťové konfigurace –** Agenti mohou také monitorovat aktuální síťovou konfiguraci daného hostitele a odhalit v ní změny např. nastavení síťových rozhraní do promiskuitního módu.

(ALEXANDER, 2009)

- **Filtrování síťového provozu –** Agenti často obsahují HIDPS FW, který dokáže omezit příchozí a odchozí provoz pro každou aplikaci v systému a tak zabránit neautorizovanému přístupu a porušení bezpečnostní politiky (např. použití nevhodných externích služeb).

Vzhledem k tomu, že HIDPS mají často rozsáhlé znalosti o vlastnostech a konfiguraci hostitelů, může HIDPS agent určit, zda se útok, který nebude zastaven, podaří nebo ne.

Agenti mohou tuto znalost použít pro výběr prevenčních akcí a přiřadit tak odpovídající priority k daným upozorněním.

(HUDEC, 200-?)

6.3.3 Prevence

Prevenční možnosti jsou rozděleny dle detekčních technik, protože se liší právě na základě detekčních technik, použitých u každého produktu. Mezi prevenční možnosti patří:

- **Analýza kódu –** Techniky analýzy kódu mohou zabránit vykonání kódu včetně malwaru a neautorizovaných aplikací. Některé HIDPS mohou také zastavit síťové aplikace před spuštěním shellu, který může být zneužit k vykonání určitých typů útoků. Pokud je nakonfigurována správně, je technika analýzy kódu velice efektivní v zastavení neznámých útoků.

- **Analýza síťového provozu –** Umožňuje zastavit příchozí síťový provoz před zpracováním daným hostitelem a odchozí provoz před odesláním z hostitele. To může být použito k zastavení útoků na síťové, transportní a aplikační vrstvě, stejně tak jako zastavení používání nepovolených aplikací a protokolů. Analýza síťového provozu umožňuje také identifikovat stahované či přenášené škodlivé soubory a zabránit jim v uložení na konkrétního hostitele. Tato technika je efektivní pro zastavení známých i dříve neznámých hrozeb.

- **Monitoring FS –** Monitoring FS může chránit soubory před přístupy, modifikací, záměnou a smazáním, což může zabránit instalaci malwaru, trojských koní a útoků spočívajících v neoprávněném přístupu k souborům. Tato technika může poskytovat další vrstvu řízení přístupu jakožto doplněk k existujícímu řízení přístupu na konkrétním hostiteli.

- **Filtrování síťového provozu –** Technika pracující jako Host-based FW, který umožňuje zastavit neautorizovaný přístup a porušování stanovené bezpečnostní politiky. Efektivní je pouze na zastavení nebezpečné aktivity, která je identifikovaná dle IP adresy a TCP portu, UDP portu nebo typem a kódem ICMP.

Zbylé detekční techniky, jako analýza logů, monitorování síťové konfigurace, kontrola integrity souboru a atributů obecně, nepodporují prevenční akce, protože identifikují události až poté, co nastaly.

(SCARFONE, a další, 2007)

6.3.4 Ostatní

Mnoho HIDPS agentů nabízí také ne IDPS bezpečnostní možnosti, jako je antivirový SW, filtrování spamu a obsahu mailů, či webu. Tyto možnosti jsou často dodávány odděleně od daného řešení IDPS. Mohou to být například:

- **Omezení odnímatelných zařízení –** Některé produkty vynucují omezení na použití odnímatelných zařízení, jako jsou Universal Serial Bus (USB) flash disky a Digital Video Disc (DVD). To zabraňuje, aby byl malware, případně určité nechtěné soubory, staženy do hostitele, ale i naopak z hostitele na dané médium.

- **Monitorování audiovizuálních zařízení –** Několik málo HIDPS produktů dokáže také detekovat, když je využíván hostitelův mikrofon, web kamera nebo IP telefony. To může indikovat zneužití těchto zařízení útočníkem.

- **Zlepšení bezpečnosti hostitele –** Určité HIDPS produkty mohou automaticky zlepšit bezpečnost hostitele na odchozí bázi. Když je například nějaká aplikace špatně nastavená a vypne určité bezpečnostní funkce, HIDPS toto chování detekuje a znovu ji povolí.

- **Monitorování stavu procesů –** Monitorování stavu procesů nebo služeb běžících na hostiteli je další bezpečnostní možnost, kterou disponují některé produkty HIDPS. Pokud bude detekován proces, který se zastavil, bude systémem HIDP restartován. Do této kategorie lze zahrnout také monitorování antivirového SW.

- **Oprava síťového provozu –** Agenti, nasazení většinou jako samostatná zařízení, dokáží opravit síťový provoz, který monitorují. Takový agent může například pracovat jako proxy a změnit každý požadavek nebo odpověď, co jím projde. Tento způsob může být efektivní v zastavení určitých neobvyklých aktivit, zvláště v hlavičkách paketů a aplikačního protokolu.

(HUDEC, 200-?)

- **Monitorování registrů –** Většina informací o Windows OS se nachází v registrech. Registry obsahují informace o konfiguraci OS, nainstalovaných aplikacích atd. Monitorování registrů chrání právě tato důležitá data v rámci OS Windows. Některé produkty umožňují vytvářet záznamy snapshot o stávajících registrech. Tyto záznamy potom později porovnávají s aktuálními kvůli potenciálním změnám. Některé produkty zase monitorují registry v reálném čase prověřováním programu, který se pokouší o neautorizované změny v registrech.

(Neznámý, 2013)

6.4 Omezení HIDPS technologie

HIDPS disponují několika omezeními, které je nutno brát v potaz při plánovaném jejich budoucího nasazení.

Jedním z nich je prodleva v generován upozornění na nastalé hrozby u určitých detekčních technik. Některé techniky mohou být používány pouze periodicky, takže může docházet ke značným prodlevám v identifikaci hrozeb. Nicméně většina agentů generuje pro většinu detekčních technik upozornění v reálném čase. S generováním upozornění bývají ještě

problémy z hlediska jejich zasílání na centralizované management servery. Ty jsou zasílány v dávkách obvykle každých patnáct až šedesát minut, aby se tak zamezilo přetížení IDPS komponentů a sítě. Menší HIDPS implementace mohou zasílat upozornění častěji, nicméně u větších podnikových implementací je od výrobce doporučeno méně časté zasílání. To způsobuje opět nemalé prodlevy v provádění prevenčních akcí a narůstá tak dopad nastalých incidentů, které se dokáží rychle šířit (například napadení malwarem).

Dalším problémem, který už byl zmíněn v podkapitole 6.2, je dopad na výkon hostitele. Agenti, instalovaní přímo na daného hostitele, mohou mít značný vliv na operační paměť, procesor a diskové úložiště. Použití shim technologie také může zpomalit operace FS nebo přímo na síti. Nasazení agenta také může být v konfliktu s dalšími bezpečnostními prvky, které jsou na něm nainstalovány. Může se jednat například o FW nebo VPN klienty.

Scarfone doporučeno před ostrým nasazením agentů nejdříve otestovat danou implementaci a pokusit se zamezit výše popsaným omezením.

(SCARFONE, a další, 2007)

7 Implementace a správa IDPS

Na trhu jsou k dispozici různé druhy systémů IDP. Může se jednat o open source řešení nebo klasické placené licence. V obou případech je nutné, jak uvádí Scarfone, po výběru vhodného produktu v rámci implementace, navrhnout jeho správnou architekturu, zajistit testování a zabezpečení komponent. Je také nutné rozhodnout o vhodnosti určité technologie pro konkrétní nasazení (SCARFONE, a další, 2007). V tabulce (**Chyba! Nenalezen zdroj dkazů.**) je uvedeno porovnání jednotlivých technologií.

Tabulka 1 – Porovnání typů IDPS technologií

Typ IDPS technologie	Typ detekované škodlivé události	Rozsah v rámci senzoru nebo agenta	Silné stránky
NIDPS	Aktivita síťové, transportní a aplikační TCP/IP vrstvy	Skupiny hostitelů a více podsítí	Schopnost analyzovat nejširší rozsah aplikačních protokolů
WIDPS	Aktivita bezdrátového protokolu, neautorizované použití WLAN	Skupiny bezdrátových klientů a více WLAN	Jediná technologie, která umožňuje monitorovat aktivitu bezdrátového protokolu
NBA	Aktivita síťové, transportní a aplikační TCP/IP vrstvy, která způsobuje neobvyklé síťové proudy	Skupiny hostitelů a více podsítí	Více efektivní než ostatní technologie v identifikaci průzkumného skenování, DoS útoků a infekce malwarem
HIDPS	Aktivita konkrétní aplikace a OS hostitele. Aktivita síťové, transportní a aplikační TCP/IP vrstvy	Konkrétní hostitel	Jediná technologie, která umožňuje analyzovat aktivitu přenesenou v rámci šifrované komunikace

Zdroj: (ALEXANDER, 2009)

7.1 Návrh architektury

Při návrhu architektury je nutné brát v potaz umístění senzorů a agentů, kteří budou monitorovat a analyzovat události v rámci sítě. Je nutné řešit také umístění ostatních IDPS komponentů (management servery, databázové servery a konzole).

Dále je nutné rozhodnout, jak moc má být nasazovaný IDPS spolehlivý a jaký přístup má být zvolen k dosažení oné spolehlivosti. Zda má být například použito více senzorů na monitorování jedné a té samé aktivity pro případ, že jeden ze senzorů selže. Nebo má být zajištěna spolehlivost nasazením více management případně záložních serverů pro případ, že primární server selže (SCARFONE, a další, 2007). Zajištění vyšší spolehlivosti souvisí s vyššími požadavky na celkovou administraci systému a také vyššími finančními náklady. Systém se zkrátka stává robustnější.

Nepostradatelné je také určité rozhraní pro správu systému. Do této kategorie lze zahrnout systémy, které poskytují data ve formě bezpečnostních informací, SW na obsluhu událostí, centralizované log servery, mailové servery atd. Dále systémy, které iniciují reakce na bezpečnostní průniky (FW, přepínače, směrovače). V poslední řadě to jsou systémy sloužící pro obsluhu IDPS komponent (SW pro síťovou obsluhu, SW pro správu aktualizací atd.).

Důležité je také rozhodnutí, zda použít management síť nebo nikoliv. Pokud ano, tak jak bude navržena. Pokud ne, jak bude řešeno zabezpečení síťové komunikace IDPS na standardní síti.

Dále je také nutné určit, jaké všechny technologické a konfigurační změny budou muset být provedeny, za účelem přizpůsobení danému nasazení IDPS. Jedná se například o změnu pravidel FW, aby spolu jednotlivé IDPS komponenty komunikovaly.

(SCARFONE, a další, 2007)

7.2 Nasazení a testování komponentů

Nasazení by mělo být provedeno nejdříve v testovacím prostředí (testovací síť), než se bude nasazovat do prostředí produkčního (produkční síť). Je tomu tak z evidentního důvodu odladění implementace systému, aby nedošlo v produkčním prostředí k nechtěným chybám, které plynou právě z podcenění testování. Nasazení jednotlivých komponentů do produkční sítě by mělo být prováděno tak, že se nejdříve zapnou pouze některé IDPS senzory a agenti s vypnutými funkcemi prevence bezpečnostních průniků. Nové nasazení má totiž obvykle tendenci generovat velké množství false positive detekcí, dokud není plně optimalizováno. To může snadno přetížit management servery, konzole a učinit tak celkovou optimalizaci pro správce systému nelehkou úlohou. Vzhledem ke většinou podobné, či stejné povaze false positive detekcí, nezáleží na tom, kolik bude nasazeno senzorů a agentů na začátku. Tím pádem je lepší postupovat postupně ve fázích nasazení. Tento přístup také pomůže odhalit potenciální problémy s možným rozšířením celého systému.

Z hlediska nasazení IDPS komponentů se dělí na Software-based komponenty a Appliance-based komponenty.

Appliance-based (přístrojově založené) komponenty jsou obecně jednodušší na nasazení. Správce musí provádět pravidelnou aktualizaci SW nebo příznaků (signatur) a zajišťovat tak, aby byl IDPS SW aktuální. Jinak správci stačí v podstatě zapojit síťové kabely, spustit zařízení a provést základní konfiguraci, jako je přidání jména senzoru či zadání licenčního čísla.

Software-based (programově založené) komponenty je těžší nasadit než výše zmiňované. Organizace musí především pořídit příslušný HW, jako například širokopásmovoé síťové karty, a celkově zajistit, aby byl příslušný HW dostatečně robustní na nasazení IDPS. Dále musí správce zajistit instalaci OS kompatibilního s daným softwarem IDPS a příslušného hostitele, na kterém OS bude fungovat řádně zabezpečit. Správce musí také provést základní konfiguraci IDPS SW tak jako u Appliance-based komponentů.

Po samotném nasazení, ať již Appliance nebo Software-based komponentů, je důležité věnovat čas a úsilí konfiguraci detekčních a prevenčních možností daného systému IDP. Bez toho je jasné, že nebude nasazený systém schopný detekovat a zabraňovat bezpečnostním průnikům efektivně.

7.3 Zabezpečení IDPS komponent

Zabezpečení IDPS komponent je velmi důležité, protože je celý systém, jak již bylo zmíněno výše, často vyhledávaný útočníky. Pokud by byl útočník schopen prolomit IDPS, nebylo by možné detekovat následné útoky namířené například proti nechráněným hostitelům v síti. Nehledě na to, že IDPS často obsahují důležité a citlivé informace, jako je například konfigurace jednotlivých hostitelů, či určité bezpečnostní slabiny. Jak je psáno výše, správci zajišťují bezpečnostní aktualizace jednotlivých IDPS komponent, nicméně existují ještě další bezpečnostní doporučení z hlediska zabezpečení komponent.

Správci systému by měli správně vytvářet uživatele (oddělit jednotlivé uživatele od správce) a přidělovat pouze nezbytná práva každému z nich.

Dále by měli nakonfigurovat směrovače, firewally a jiná zařízení, která dokážou filtrovat pakety, aby omezila přístup ke všem IDPS komponentům pouze hostitelům, kteří tento přímý přístup potřebují.

Správci by měli zajistit, že veškerá IDPS komunikace je řádně zabezpečena. Tím je myšleno buď fyzicky, skrze management síť, nebo ji logicky oddělit za pomoci management VLAN. Další možností je šifrování dané komunikace. Mnoho produktů podporuje šifrování použitím Transport Layer Security (TLS). Pro ty, které tento druh šifrování nepodporují, Scarfone doporučuje organizacím zvážit použití VPN nebo jiných tunelovacích metod k ochraně síťového provozu. Některé organizace také požadují použití silné autentizace pro vzdálený přístup k IDPS komponentům, jako je dvoufaktorová autentizace[6]. Tento způsob sám o sobě přidává další vrstvu zabezpečení.

(SCARFONE, a další, 2007)

7.4 Údržba a správa systému IDP

Produkty IDPS se z velké části obsluhují pomocí konzole, která může mít podobu grafického uživatelského rozhraní (GUI – Graphical User Interface). Konzole obvykle dovoluje správcům konfigurovat a aktualizovat senzory, agenty a management servery. Mimo to samozřejmě umožňuje monitorovat jejich stavy (ztráty paketů, výpadky agentů…). V konzoli je pro správce také možnost spravovat uživatelské účty, přidělovat práva jednotlivým uživatelům, na základě čeho jsou potom v konzoli přístupné jiné funkce. Některé systémy dovolují rozlišit, jaké konkrétní senzory a agenty mohou daní uživatelé monitorovat a analyzovat z nich data. To umožňuje dělit velký IDPS na dílčí celky z hlediska

[6] Kombinace faktorů „něco vím“ (heslo) a „něco mám“ (SMS klíč). Typickým příkladem dvoufaktorové autentizace jsou například služby internetového bankovnictví (ŠNAJDR, 2013).

operační působnosti. Dále je možné, na základě konzole, určitým způsobem upravovat výstupy z jednotlivých komponent, monitorovat, analyzovat data z IDPS a generovat různé reporty.

Konzole není mnohdy jediný prostředek pro správu. Některé produkty IDPS také obsahují Command Line Interface (CLI), což je příkazová řádka. Na rozdíl od GUI konzolí, které jsou typické pro vzdálenou obsluhu senzorů, agentů a management serverů, CLI je primárně určeno pro obsluhu lokální. Nicméně CLI daného IDPS komponentu může být dosaženo skrze šifrované připojení přes SSH. Samozřejmě jsou GUI konzole jednodušší na používání, jelikož obsahují grafické prvky pro lepší orientaci.

7.4.1 Práce s konzolí

IDPS konzole nabízejí často mnoho funkcí k usnadnění každodenní práce uživatelů systému. Jedná se například o více vrstev detailních informací o každém bezpečnostním upozornění. Ve výsledku tak může uživatel sledovat základní informace o jednotlivých upozorněních, ale i zobrazit detailní informace o upozorněních, u kterých tyto informace vyžaduje. Co se týče jednotlivých upozornění, o nich jsou generovány všechny důležité informace. Obecně totiž platí, že čím víc dat IDPS uchovává, tím jednodušší je zjistit původ nastalého problému (SCARFONE, a další, 2007).

Mezi pokročilejší funkce lze zařadit například rozesílání určitých reportů v určitý čas pouze určitým uživatelům. Některé konzole umožňují uživatelům generovat reporty a upravovat je, jak je potřeba.

7.4.2 Udržování aktualizovaného systému

Existují dva druhy aktualizací IDPS. SW aktualizace a pak aktualizace příznaků (signatur). Rozdíl mezi nimi je zřejmý. Aktualizace SW odstraňují chyby v předešlých verzích IDPS a přidávají nové funkcionality. Aktualizace příznaků přidávají nové detekční možnosti nebo upravují již stávající, například za účelem snížit počet false positive detekcí.

SW aktualizace zahrnují aktualizace jednotlivých nebo také všech IDPS komponentů. Tyto aktualizace jsou často prováděné pouhým vyměněním média Compact Disc (CD) v mechanice a nabootováním z nového, protože IDP systémy v mnoha případech spouštějí SW přímo z CD a není tedy potřeba ho instalovat. Nicméně některé komponenty, jako jsou agenti, potřebují, aby je správce nainstaloval či aplikoval aktualizace buď manuálně nebo skrze IDPS management software. Někteří výrobci samozřejmě poskytují aktualizace skrze stažení z jejich webové stránky. Často je také obsažena funkce pro stažení a aktualizaci přímo v rozhraní, které správce používá pro správu IDPS.

Scarfone doporučuje kontrolu integrity aktualizací před jejich aplikováním, jelikož mohou být aktualizace nějakým nevhodným způsobem pozměněny nebo poškozeny. Tato kontrola je odvozena od způsobu, jakým jsou aktualizace aplikovány (SCARFONE, a další, 2007).

Buď to může být stažením souboru z webové stránky, nebo FTP serveru. Správce by v tomto případě měl porovnat kontrolní součty poskytované dodavatelem aktualizací nad právě staženými aktualizačními daty.

Pokud jsou aktualizace staženy automaticky přes uživatelské rozhraní IDPS, měl by se opět provést kontrolní součet stažených dat s poskytovaným. To v tomto případě často obstará právě uživatelské rozhraní, které by mělo obsahovat funkce na kontrolu integrity.

V poslední řadě mohou být aktualizace aplikovány skrze vyjmutelná média, jako jsou CD a DVD. V takové situaci by měl správce zjistit věrohodnost daného média a dat na něm. S tím by měl být nápomocen právě dodavatel, například skrze telefonickou podporu, který by měl poskytnout nezbytné rady k zajištění integrity dat. Správcovi poté náleží zkontrolovat médium, zda neobsahuje potenciální malware.

Obecně platí, že IDPS jsou navrženy tak, aby instalování aktualizací nemělo žádný vliv na existující nastavení systému. Výjimkou jsou změny provedené v kódu, které se při aplikaci aktualizace vrátí do původního stavu, respektive do aktualizovaného stavu. Správce tak potom musí změny v kódu, kterými měl upravené určité schopnosti IDPS k obrazu svému, znovu nastavit. Dále je vhodné před instalováním aktualizací provést zálohování nastavení.

(SCARFONE, a další, 2007)

8 Analýza dostupných řešení HIDPS a zátěžové testy zaměřené na ovlivnění výkonu hostitele

V rámci komparativní analýzy dostupných řešení systémů Host-based Intrusion Detection Prevention bylo vybráno jedno open source a jedno komerční řešení v trial verzi. Tato řešení byla následně nasazena na hostitele s danou konfigurací a podrobena zátěžovým testům. Ty byly zejména zaměřeny na to, jaký mají vliv na výkon hostitele, na kterém byla nasazena.

8.1 Dostupná řešení HIDPS a kritéria pro výběr vhodných produktů

Na trhu se v současné době objevuje mnoho produktů HIDPS, ale jen málo z nich vyhovuje požadavkům této diplomové práce.

Jako hlavní kritéria pro výběr odpovídajících produktů byla zvolena:

- nabídka multiplatformních agentů (podpora minimálně v rámci OS Windows a Linux),
- samostatné řešení a ne například řešení obsažené v rámci určitého SW, jako jsou aplikační FW a nebo antivirové programy (ESET Smart Security[7]) a s tím i související robustnost daného řešení,
- výhradně HIDPS řešení,
- nabídka podobných detekčních případně prevenčních funkcionalit.

Z výběru tedy byla odstraněna Windows řešení typu MJ Registry Watcher[8] a např. Win Patrol[9], která nabízejí pouze agenty pro OS Windows případně Tripwire[10], které nabízí agenty naopak pouze pro OS Linux.

Kvůli nutnosti samostatného řešení byly, i za cenu nedokonalých prevenčních schopností, vyloučeny produkty HIDPS obsažené přímo např. v antivirovém programu. Příkladem takto řešeného HIDPS je ESET Smart Security. Bohužel tato řešení jsou svoji robustností náročnější na správu, mají vyšší nároky na výkon hostitele a v neposlední řadě bývají i cenově dražší.

V současnosti existují velice kvalitní a dobře financované IDPS produkty, jako je Snort[11] nebo Suricata[12]. Tyto produkty mají i velkou uživatelskou základnu, což se pozitivně promítne v potenciálním řešení určitého problému s konkrétním produktem. Bohužel jsou

[7] http://www.eset.com/cz/domacnosti/produkty/smart-security/
[8] http://www.jacobsm.com/mjsoft.htm#rgwtchr
[9] http://www.winpatrol.com/
[10] http://www.tripwire.com/
[11] https://www.snort.org/
[12] http://suricata-ids.org/

tato řešení ale založená na síťové technologii, tudíž nesplňují třetí kritérium a jsou tak pro tuto práci opět nevhodná.

Na základě daných kritérií byla vybrána open source a komerční HIDPS řešení popsaná v kapitolách 8.1.1 a 8.1.2.

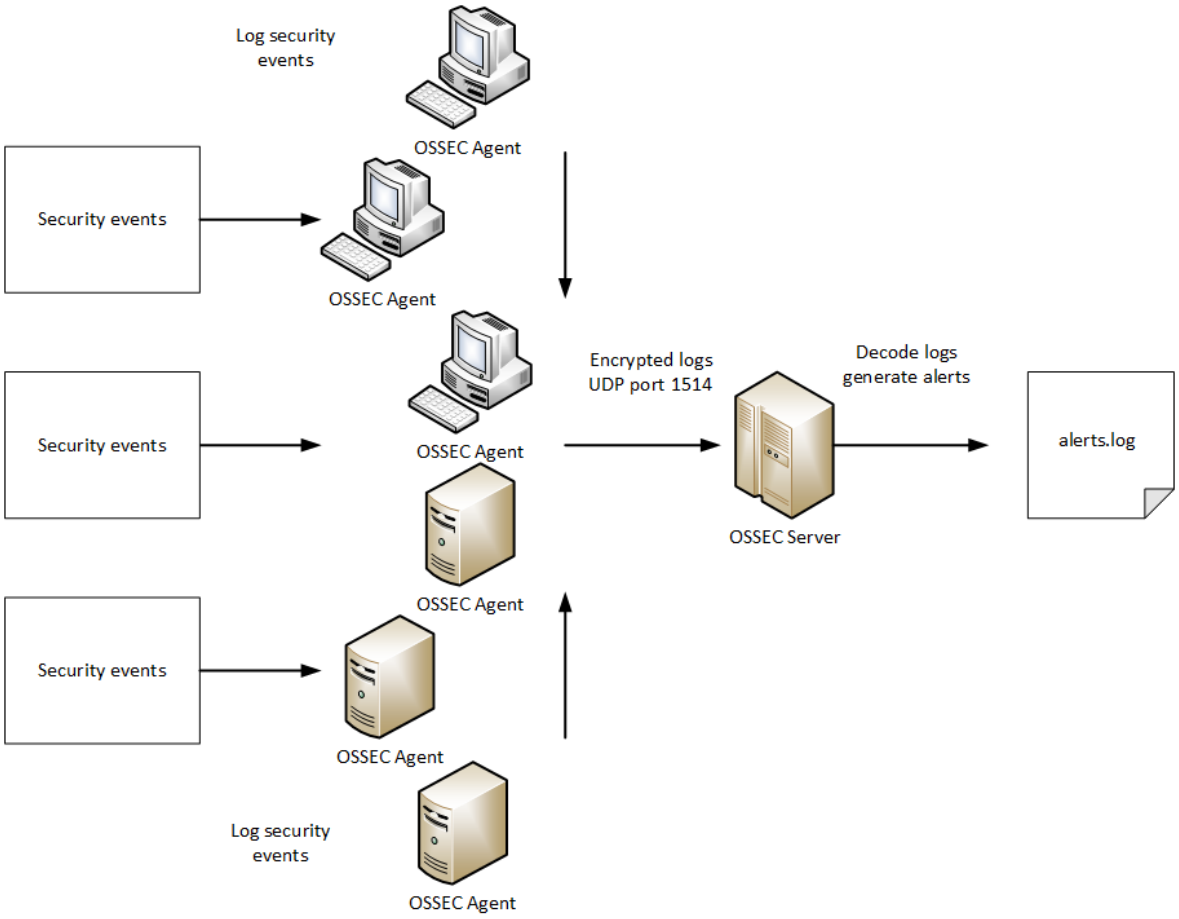
8.1.1 Vybrané open source řešení HIDPS

Jako open source řešení HIDPS bylo vybráno OSSEC[13], hlavně z důvodu, že nabízí agenty pod operační systémy Windows i Linux. Tato vlastnost byla velice důležitá pro diplomovou práci, protože bylo nutné provést zátěžové testy právě v rámci různých OS. Ostatní nalezené open source IDPS tuto vlastnost nenabízely nebo to nebyly IDPS, založené přímo na technologii Host-based.

Mezi zákazníky, využívající OSSEC patří organizace jako: NetFlix, Sansung, Apple, NASA (HARGRAVE, 2013).

OSSEC funguje jako agent-server systém. Agenti obsluhují monitoring logů, souborů a registrů. Logy jsou následně zašifrovány a poslány v této formě na OSSEC management server přes UDP port 1514. Na straně management serveru jsou logy na základě určitého dekodéru dešifrovány a porovnány s pravidly, která generují bezpečnostní upozornění. Pravidel a dekodérů je v OSSEC celá řada a slouží ke sledování důležitých systémových událostí, jako jsou změny souborů, pokusy o připojení atd. Uživatelé si mohou vytvářet svá vlastní pravidla, která budou odpovídat jejich potřebám (HARGRAVE, 2013).

[13] http://www.ossec.net/



Obrázek 12 – Princip fungování OSSEC

Zdroj: Přepracováno od: (HARGRAVE, 2013)

Jak lze vidět na obrázku (Obrázek 12), upozornění z dešifrovaných logů, se ve výchozím stavu ukládají do souboru *alerts.log* v umístění */var/ossec/alerts/* na odpovídajícím management serveru.

Hlavní klíčové dovednosti systému OSSEC jsou:

- **Kontrola integrity souboru** – Cílem této kontroly je detekovat změny v systému a zaslat upozornění, když takové změny nastanou. Může se jednat o útok nebo jen špatné použití a modifikace souboru, registru nebo adresáře zaměstnancem.
- **Monitorování logů –** OSSEC shromažďuje logy z různých zařízení, aplikací nebo celého OS a analyzuje je. Pokud zjistí nějakou neobvyklou událost v rámci těchto nashromážděných logů, dává o ní vědět správci.
- **Detekce rootkitů –** Rootkity často využívají útočníci k maskování svých aktivit. OSSEC dokáže tento maskující SW detekovat a upozornit o něm správce chráněného systému.

- **Aktivní odpovědi –** OSSEC nabízí zasílání automatických odpovědí při náhlých útocích. Na základě nich, je možné potom útoky blokovat včas.

Hlavní přednosti systému OSSEC jsou velmi silná analýza logů a podpora monitorování na základě agentů nebo bez nich.

Hlavní negativa OSSEC spočívají v počtu agentů na management server. Může jich být maximálně 256, což pro větší podniky nemusí být dostačující. Dále OSSEC dovoluje poslat jen omezený počet upozornění v rámci jedné hodiny.

(ARORA, 2012)

8.1.2 Vybrané komerční řešení HIDPS

Jako komerční HIDPS řešení bylo vybráno Deep Security[14] od společnosti Trend Micro, které splňuje veškerá kritéria definovaná dříve a bylo tak vhodnou volbou pro tuto diplomovou práci.

Deep Security nabízí ochranu pro fyzické, virtuální a cloudové servery a desktopy. Nabízí agenty pro širokou škálu linuxových distribucí a nechybí také podpora OS Windows. Jedná se o komerční řešení, kde je možné produkt vyzkoušet v podobě trial verze, která je však omezená klasicky třiceti dny.

Toto řešení tedy obsahuje agenty, kteří jsou nainstalováni na konkrétní hostitele, ať už virtuální nebo fyzické, a potom management server s konzolí (webovým uživatelským rozhraním), které se dohromady nazývá Deep Security Manager. Konzole nabízí vzdálenou správu zasílaných upozornění od agentů, aktualizací daných agentů atd.

Hlavní klíčové přednosti systému Deep Security jsou:

- **Kontrola integrity souborů** – Systém detekuje a upozorňuje na nebezpečné a neobvyklé změny souborů a systémových registrů.
- **Kontrola logů** – Systém kontroluje logy na podezřelé aktivity, které následně ohlašuje.
- **Filtrovací FW** – Deep Security nabízí také FW, který slouží k filtrování paketů a zabraňuje tím např. potenciálním DoS útokům.
- Prevence a detekce průniků – Umožňuje na základě určitých příznaků a pravidel detekovat a zabraňovat nastalým hrozbám.
- **Ochrana proti malwaru**

(HALETKY L., 2011)

[14] http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/

Deep Security Manager komunikuje s agenty přes TCP port 4118, na kterém agenti na konkrétních hostitelích poslouchají. Komunikace opačným směrem, tj. od agentů k managerovi probíhá přes TCP port 4120. Další důležitý port je TCP port 4119, přes který se internetový prohlížeč připojuje ke konzoli. Tento port je také využíván Deep Security Relay agenty k získání SW balíků a aktualizací z konzole.

Deep Security agenti nasazení na konkrétní hostitele poskytují právě výše uvedené možnosti obrany proti potenciálním útokům. Dané možnosti jsou podobné s OSSEC řešením. Může to být zapříčiněno tím, že je OSSEC sponzorováno firmou Trend Micro a to tedy firmou, která stojí za produktem Deep Security.

8.2 Konfigurace testovaného hostitele

Jako testovací hostitel byl použit notebook ASUS N75S, na kterém byly nainstalovány dva OS a to Windows 7 Home Premium a Linux.

Základní HW konfigurace testovaného hostitele:

- **CPU** (Central Processing Unit) – Intel Core i7-2670QM CPU, 2,20 GHz
- **RAM** (Ranom Access Memory) – 8 GB SDRAM DDR3, 1333 MHz
- **GPU** (Graphic Processing Unit) – NVIDIA GeForce GT 555M 2GB DDR3 VRAM/Intel HD Graphics 3000
- **SSD** (Solid State Drive) – Kingston V200 128 GB
- **Síťová zařízení** – Atheros AR8151 PCI-E Gigabit Ethernet, Intel Centrino Wireless-N 1030 802.11 b/g/n

Windows 7 byl použit z důvodu jeho velkého rozšíření na desktopových PC a celosvětovou oblíbeností mezi uživateli. V současnosti, i po příchodu Windows 10, je tento systém stále nejpoužívanější na osobních počítačích či noteboocích. Dá se ale předpokládat, že bude v budoucnu předehnán právě novější verzí Windows 10. Pro testování systémů HIDPS v rámci zadané diplomové práce byl však Windows ve verzi 7 velice vhodný. Většina produktů HIDPS nabízí agenty kompatibilní s touto verzí a při pohledu z druhé strany, tedy potenciálních bezpečnostních hrozeb, hrozících určitému hostiteli, je OS Windows 7 také vhodnou volbou, právě díky jeho rozšíření. Teoreticky platí přímá úměra, že čím více je OS rozšířen mezi uživateli, tím více je na něho produkováno škodlivých kódů.

OS Linux byl vybrán opět v aktuálně nejrozšířenější distribuci, co se týče desktopových počítačů. Jednalo se o distribuci Ubuntu ve stabilní verzi s dlouhou podporou a to 15.04. Tato distribuce je často označována jako Kubuntu, jelikož se liší od klasického Ubuntu použitým GUI. Ubuntu v aktuální verzi používá grafické prostředí Unity. Kubuntu ovšem používá prostředí KDE. Co se týče dostupných balíků a oficiálních repozitářů, rozdíly téměř nejsou, nebo jsou minimální.

Oba OS byly nainstalovány tedy na SSD Kingston V200 o kapacitě 128 GB. Jednalo se také o aktuální verze OS včetně všech dostupných oficiálních aktualizací. U obou byla také provedena čistá instalace, tedy bez jakýchkoliv aplikací a služeb, běžících na pozadí a potenciálně ovlivňujících měřený výkon hostitele. K dispozici byly pouze výchozí aplikace běžně dodávané s daným OS, SW pro monitoring výkonu hostitelů a agenti daných HIDPS produktů. Ve Windows 7 byl také přítomný antivirový program Microsoft Security Essentials, který je v dalších verzích daného OS nainstalovaný ze základu.

Pro monitorování systémových prostředků, hlavně využití CPU a paměti RAM, byl využit open source SW Nagios. Ten poskytuje multiplatformní sledování vytížení jednotlivých klientů v rámci centralizovaného serveru, který disponuje webovým rozhraním pro správu.

Jako distribuci pro Nagios server byl zvolen CentOS verze 6.6 z důvodu výrobcem doporučené kompatibility. Na testovacího hostitele byli potom dle OS nainstalováni odpovídající agenti, kteří zprostředkovávají data pro server.

8.3 Analýza nasazení a funkcí vybraných řešení HIDPS

V následujících dvou kapitolách je popsáno realizované nasazení vybraných řešení HIDPS a provedena analýza jejich hlavních funkcí.

8.3.1 OSSEC ve verzi 2.8.2

K nasazení OSSEC HIDPS agentů bylo zapotřebí nejdříve nasadit na OS Linux OSSEC management server, kterému agenti potřebují zasílat přes protokol UDP zašifrované logy. Management server potom logy následně zpracovává a reportuje správci, jak je popsáno v kapitole 8.1.1.

Instalace byla v rámci testování provedena na Linux distribuci ElementaryOS Freya, která je založena na distribuci Ubuntu 14.04. Co se týče kompatibility, nebyl tedy problém. V konfiguraci serveru byly povoleny veškeré funkce HIDPS, kromě zasílání upozornění na konkrétní email. Následně byli na server nasazeni dva agenti, jeden pro OS Windows a druhý pro OS Linux a vygenerovány příslušné zašifrované klíče pro každého agenta.

Na testovacího hostitele byli potom nasazeni odpovídající agenti dle operačního systému na základě serverem vygenerovaného klíče. Agentům bylo nakonfigurováno, na jaké IP adrese se vyskytuje daný management server.

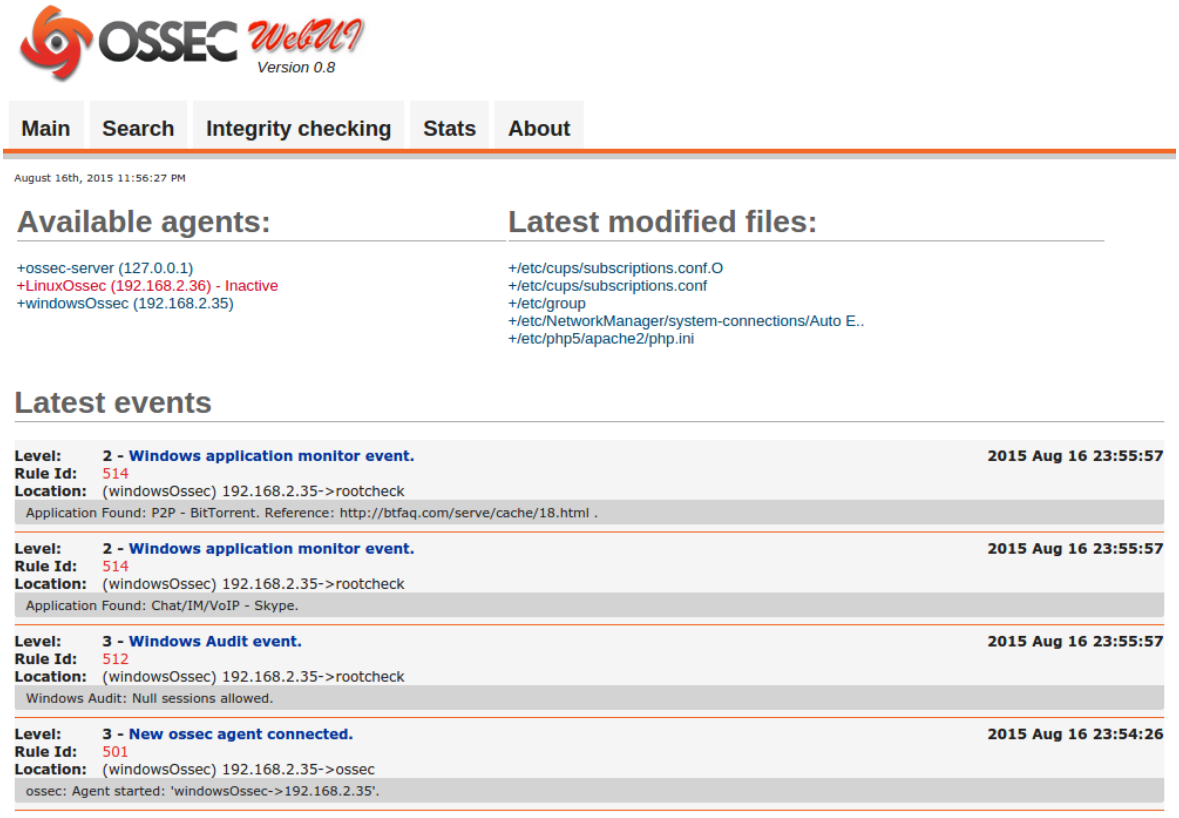
V adresáři */ossec/alerts/* je soubor *alerts.log,* ve kterém jsou upozornění v rámci integrity souborů, rootkit detekce atd. Příklad zaslaných upozornění od agentů je:

```
** Alert 1439760891.318131: - pam,syslog,
2015 Aug 16 23:34:51 (LinuxOssec) 192.168.2.36->/var/log/auth.log
Rule: 5502 (level 3) -> 'Login session closed.'
Aug 16 23:34:50 kubuntu sudo: pam_unix(sudo:session): session closed for
user root
```

```
** Alert 1439762066.318371: mail  - ossec,
2015 Aug 16 23:54:26 (windowsOssec) 192.168.2.35->ossec
Rule: 501 (level 3) -> 'New ossec agent connected.'
ossec: Agent started: 'windowsOssec->192.168.2.35'.
```

První upozornění se týká uzavření sezení uživatele root a pochází od LinuxOssec agenta. Druhé značí start agenta na OS Windows.

OSSEC nabízí také webové rozhraní pro správu daných upozornění. Na obrázku (Obrázek 13) lze spatřit ukázku nasazeného webového uživatelského rozhraní. Jsou vidět aktivní a neaktivní agenti a jejich IP adresy. Naposledy modifikované soubory[15] a podrobnosti od jakého agenta upozornění pochází, stavový kód změny, úroveň hrozby atd. Dále jsou na hlavní stránce přítomny poslední události s identifikačním číslem pravidla[16], na základě kterého bylo upozornění vygenerováno. K dispozici je také možnost sledovat integritu dat v reálném čase a pozorovat statistiky konkrétních hostitelů.



Obrázek 13 – Ukázka nasazeného webového rozhraní OSSEC

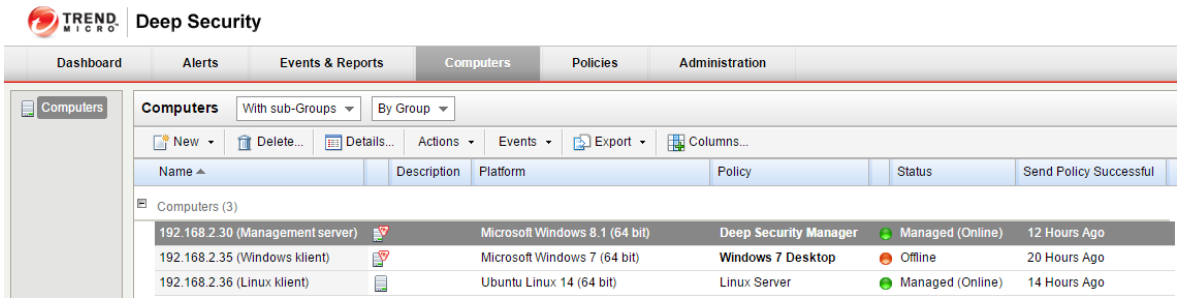
Zdroj: Autor

[15] Soubory, které se mají systémem OSSEC monitorovat na nastalé změny se dají upravit v konfiguračních souborech management serveru a agentů.
[16] Pravidla jsou opět konfigurovatelná skrze konfigurační soubory systému OSSEC.

8.3.2 Deep Security ve verzi 9.5

HIDPS řešení Deep Security poskytuje opět multiplatformní agenty a na rozdíl od OSSEC nabízí centralizovaný management server s vestavěným webovým uživatelským rozhraním zvaným Deep Security Manager a to jen pro OS Windows. Na tento OS byl tedy v rámci testování nainstalován. Pro instalaci plné verze je nutné disponovat buď databází Oracle 10g nebo 11g pro podniková řešení, případně Microsoft SQL Server 2008 nebo 2012. Manager pro trial verzi, která byla použita pro cíle této práce, nabízí ještě možnost použít vestavěnou databázi Apache Derby, která byla zvolena. Na hostitele, kde byl nasazen Deep Security Manager byl ještě nainstalován relay-enabled Deep Security Agent, který slouží ke stahování a distribuci aktualizací na jednotlivé agenty.

Agenti byli nainstalováni na testovaného hostitele a následně aktivovány v management severu daného produktu. Po aktivování agenta se přes relay-enabled agenta začaly aplikovat a stahovat aktualizace modulů jako je FW, HIDPS atd. Na obrázku (Obrázek 14) jsou vidět nasazení hostitelé[17] pro dva testované OS.



Obrázek 14 – Ukázka nasazených testovacích hostitelů v SW Deep Security Manager

Zdroj: Autor

V detailu konkrétního hostitele se dají nalézt informace o všech funkcích řešení Deep Security, jako je ochrana proti malwaru, nastavení a pravidla vestavěného FW, kontrola logů, systém prevence a detekce průniků atd. Z tohoto centrálního rozhraní lze právě spustit pro konkrétního hostitele např. skenování na potenciální malware. Dále je přítomno nastavení, kde lze snížit například interval mezi zasíláním určitých událostí z hostitele a jiné. Samozřejmě se u každého nasazeného hostitele objevuje log nastalých událostí a upozornění. Z nich lze přesně dohledat například, jaký problém na konkrétním hostiteli byl v určitou dobu a jeho detail, kde jsou popsány možné příčiny a jeho stavový kód pro lepší dohledání informací o problému.

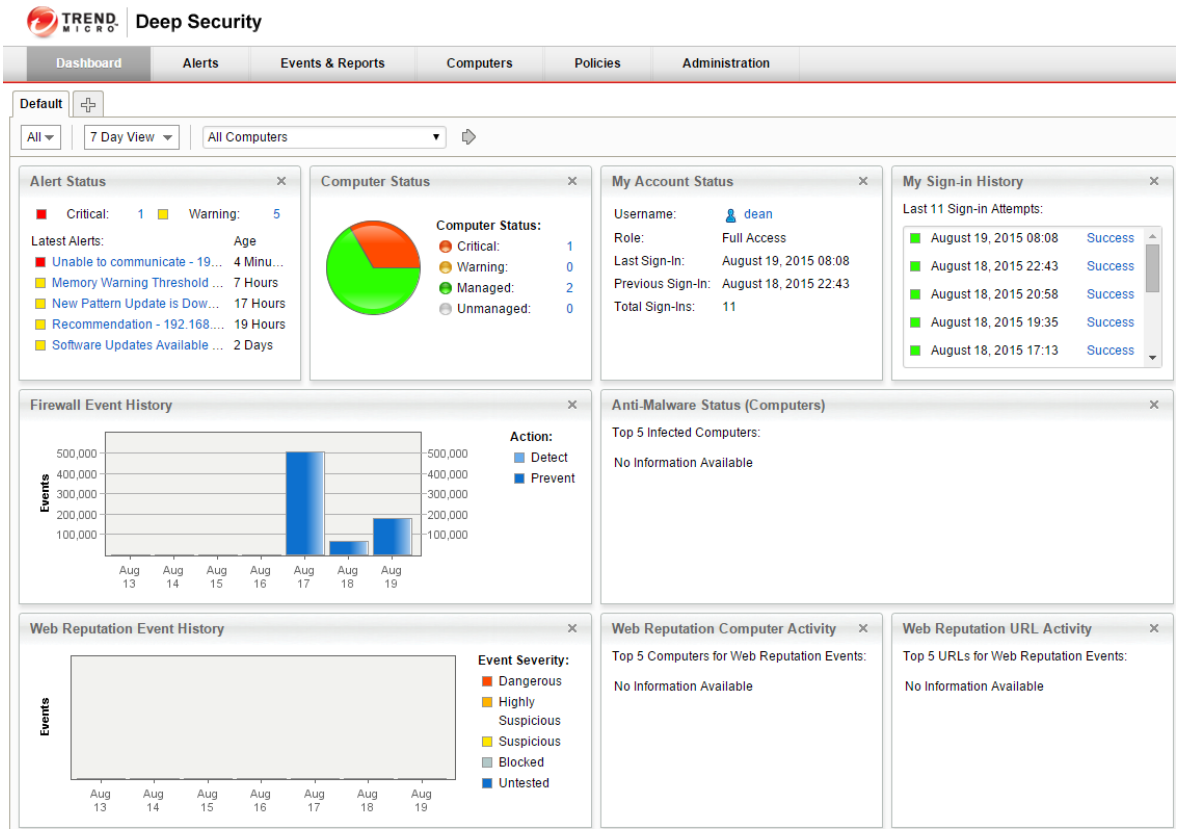
Při aktivování agentů na management serveru se také vybíralo, dle jaké bezpečnostní politiky se má daný agent řídit a provést základní nastavení. K dispozici byly politiky jak pro Linux server, pro Windows server nebo i Windows desktop. Tyto bezpečnostní politiky je samozřejmě možné upravovat dle potřeby. Lze tak změnit pravidla (příznaky), na základě

[17] Jelikož se jedná fyzicky o jednu pracovní stanici, je jeden z hostitelů offline.

kterých modul HIDPS detekuje a provádí příslušná opatření, aby zamezil potenciálním průnikům do systému hostitele.

Co se týče samotných funkcí webového rozhraní Deep Security Manager, lze zmínit například generování bezpečnostních hlášení přímo do pdf formátu. Samozřejmostí také je správa uživatelů a jejich oprávnění pro vstup do rozhraní či naplánování určitých akcí na konkrétní čas v průběhu dne.

Obrázek (Obrázek 15) znázorňuje hlavní stránku uživatele, kterou lze přizpůsobit dle vlastního uvážení nebo přidat více stránek a každou tak například mít zaměřenou na sledování událostí z jiných modulů.



Obrázek 15 – Ukázka hlavní stránky webového rozhraní Deep Security Manager

Zdroj: Autor

Co se týče srovnání s nekomerčním produktem OSSEC, na první pohled je vidět, že Deep Security mělo po nasazení přívětivější rozhraní pro správu systému. U produktu OSSEC bylo nutné vše spravovat ručně v daných konfiguračních souborech agentů nebo management serveru, jelikož webové rozhraní nedisponovalo zdaleka takovými možnostmi jako u komerčního produktu. Testování funkčností jednotlivých řešení z hlediska reakce na určité hrozby bylo mimo rozsah této práce. Testování bylo zaměřeno na ovlivnění výkonu hostitele, na kterém jsou nasazeni odpovídající agenti v rámci daných OS. Výsledky testování jsou podrobně rozepsány v následující kapitole 8.4.

8.4 Zátěžové testy jednotlivých řešení HIDPS z hlediska ovlivnění výkonu hostitele na OS Windows/Linux

Před samotným testováním ovlivnění výkonu hostitele nasazením HIDPS řešení, bylo nutné provést počáteční testy, jakých hodnot dosahují vytížení CPU a RAM v rámci OS Windows a Linux, pokud je hostitel v klidovém stavu[18] bez nasazeného produktu HIDPS.

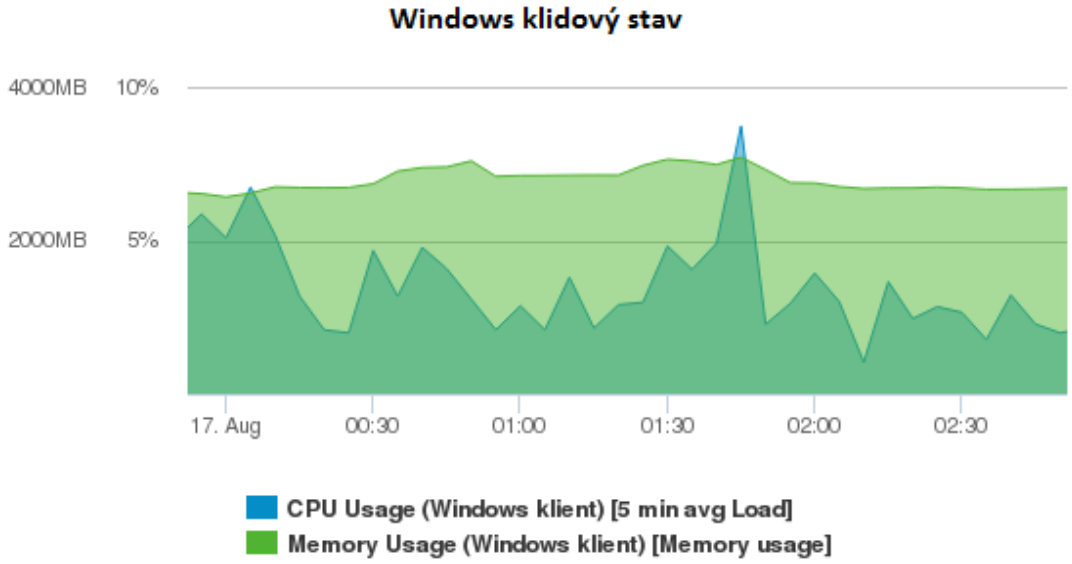
Dále bylo testováno, jak je ovlivněn výkon hostitele v daných OS při nasazení nejdříve open source řešení HIDPS a následně komerčního produktu.

8.4.1 Klidový stav bez použití HIDPS

Test zatížení hostitelů probíhal v klidovém režimu po dobu cca 2 hodin s puštěnými aplikacemi, jako je průzkumník souborů, jeho alternativa v Kubuntu je Dolphin, Libre Office Writer, Microsoft Office Word, internetový prohlížeč Google Chrome se třemi záložkami. V Linuxu byl přítomen ještě zapnutý terminál a ve Windows již avizovaný antivirový program.

Na obrázku (Obrázek 16) lze vidět graf využití systémových prostředků v OS Windows v klidovém stavu. Je vidět, že využití CPU, kolísá kolem 2,5 %.

Využití paměti RAM se drží na hodnotě cca 2 500 MB.



Obrázek 16 – Graf využití CPU a RAM v klidovém stavu v OS Windows

Zdroj: Autor

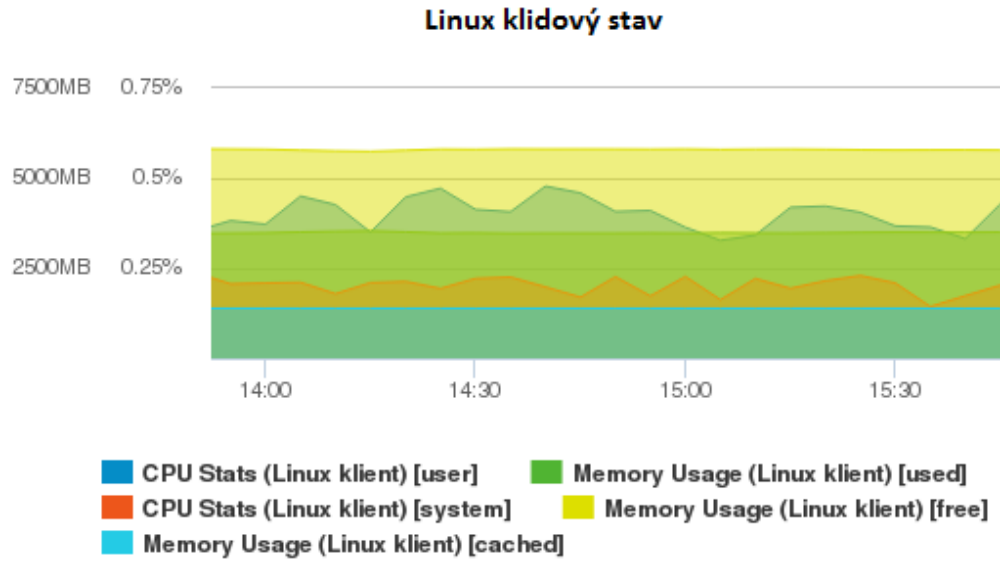
[18] Klidovým stavem se rozumí, že hostitel má puštěné základní programy a služby, běžící po načtení daného OS. Pro větší věrohodnost naměřených výsledků jsou však na hostiteli puštěny i kancelářské programy, prohlížeč souborů, internetový prohlížeč atd. a to ve stejné míře v rámci obou OS. Tímto způsobem byla snaha navodit podobný stav, jaký by hostitel měl při běžné kancelářské práci.

Na obrázku (Obrázek 17) je možné vidět využití prostředků v rámci OS Linux také v klidovém stavu hostitele.

Pro porovnání je nutné zmínit, že oba porovnávané OS přistupují ke správě systémových prostředků, a tím i k jejich využívání, odlišně. To vysvětluje více oblastí grafu využití v OS Linux. Linux, jelikož pracuje ve dvou režimech a to uživatelském a kernel režimu, přistupuje i tak k využívání CPU. Uživatelské využití CPU, značí využití procesorového času procesy mimo jádro (kernel). Systémové využití CPU označuje, kolik procesorového času se spotřebovává v rámci jádra. Jako příklad přechodu mezi režimy lze uvést systémová volání.

Dá se tedy říci, že celkové využití CPU, je součtem uživatelského využití a systémového využití CPU[19]. Z toho vyplývá, že vytížení CPU v OS Linux bylo v klidovém stavu kolem 0,6 %. Z toho uživatelské využití činilo zhruba 0,4 % a systémové přibližně 0,2 %.

Co se týče operační paměti RAM, je také dělena. V grafu níže byla pro přehlednost použita volná paměť, používaná paměť a nacachovaná paměť. Fyzicky bylo na hostiteli 8 GB operační paměti. Celková využitá RAM je v podstatě odečtená nacachovaná paměť od paměti používané. To dalo v tomto případě cca 2 GB využití RAM. Volné paměti tedy zbývalo zhruba 6 GB.



Obrázek 17 – Graf využití CPU a RAM v klidovém stavu v OS Linux

Zdroj: Autor

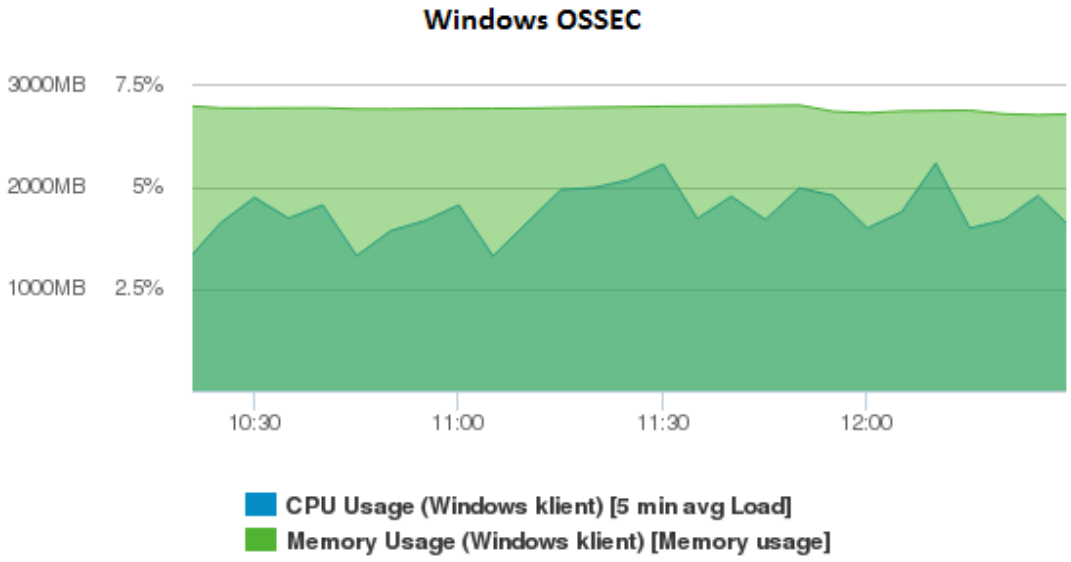
[19] Kromě využití CPU z hlediska uživatele a systému, je v monitoringu také přítomna položka I/O wait, která značí procentuální čas CPU, kdy musel čekat, protože všechny běžící úlohy čekaly na dokončení IO operace. Dá se říci, že je tato hodnota závislá na rychlosti pevného disku. Vzhledem k tomu, že na testovaném hostiteli jsou oba OS nainstalovány na SSD, tato hodnota je velice nízká a tím pádem byla z monitoringu odebrána.

V OS Windows bylo tedy využití prostředků v klidovém stavu dle nezávislého open source monitorovacího SW Nagios vyšší. To lze přisuzovat běžícím službám na pozadí systému a např. antivirovému programu. OS Linux byl v tomto ohledu dle grafů méně náročný.

8.4.2 Open Source řešení OSSEC

Po nasazení agenta OSSEC na hostitele s OS Windows se zatížení CPU zvýšilo zhruba o 1 % oproti klidovému stavu, tedy na cca 4 %.

Využití paměti RAM se také zvětšilo a to z 2,5 GB na přibližně 2,7 GB, tedy o 200 MB.

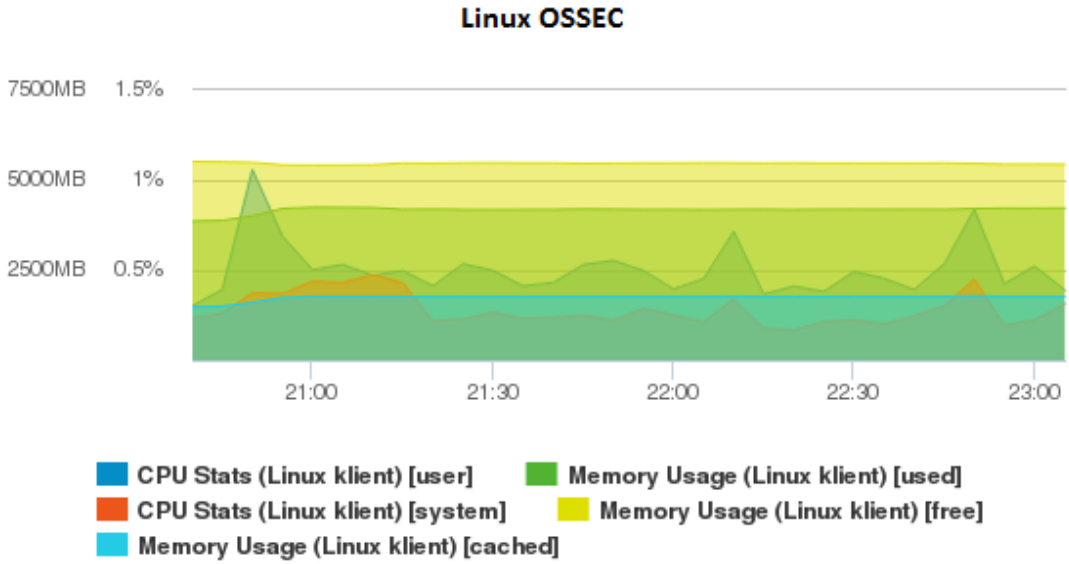


Obrázek 18 – Graf využití CPU a RAM po nasazení OSSEC agenta v OS Windows

Zdroj: Autor

Využití CPU v Linuxu po nasazení agenta OSSEC se od klidového stavu nepatrně lišilo. Uživatelské vytížení kolísalo okolo 0,5 % a systémové se dostávalo na hranici 0,25 %. Celkově se tedy vytížení CPU od klidového stavu změnilo o cca 0,1 % na 0,7 %. Zezačátku bylo možné vidět určité kolísání a zvýšení aktivity CPU. To bylo ale zapříčiněno samotným procesem instalování agenta na daný systém.

U operační paměti je vidět dle obrázku (Obrázek 19) mírný vzrůst v oblasti používané paměti a logicky pokles paměti volné cca o 200 MB, což je v pořádku vzhledem k množství démonů, které OSSEC Agent pouští (kvůli detekci rootkitu, kontrole integrity souborů atd.). Celková použitá pamět tedy po použití nekomerčního řešení OSSEC v OS Linux činila 2,2 GB.



Obrázek 19 – Graf využití CPU a RAM po nasazení OSSEC agenta v OS Linux

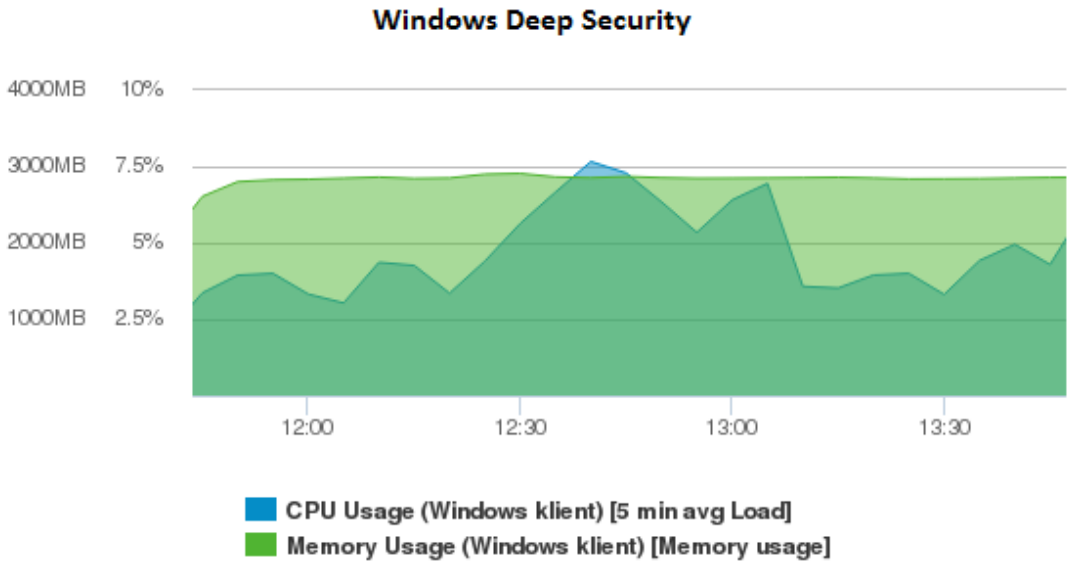
Zdroj: Autor

8.4.3 Komerční řešení Deep Security

Co se týče CPU a RAM zatížení hostitele na OS Windows, výsledky jsou znázorněny na obrázku (Obrázek 20).

Hodnota vytížení CPU kolísala kolem 4 % tzn. oproti testování agenta open source řešení bylo tedy nasazení komerčního agenta z hlediska vytížení CPU na OS Windows téměř totožné. Na daném obrázku je vidět mezi časem 12:30 a 13:00 hod. zvýšené vytížení CPU až na 7,5 %. To bylo způsobené aplikováním aktualizací a pravidel na FW, IPS, integritu souborů a také aktualizací daného agenta. To bylo provedeno po aktivaci agenta na daném hostiteli z centrálního SW Deep Security Manager, kde lze jednotlivé agenty spravovat. Další vytížení přišlo po 13. hodině a je způsobeno, dle logů z managera, prováděním skenování agenta na potenciální malware. Po 13:10 hod. se vytížení vrátilo na výchozí hodnotu. Hodnota vytížení CPU se oproti klidovému stavu zvýšila dosti podobně, jako při nasazení OSSEC agenta a to přibližně o 1 % na 4%.

U testování vytížení paměti RAM je dle obrázku vidět oproti nekomerčnímu řešení drobné navýšení. Toto chování lze přisoudit robustnějšímu GUI daného Windows agenta. Tím pádem lze předpokládat, že Deep Security agent vytíží operační paměť více než OSSEC. Konkrétně se jednalo o kolísání kolem hodnoty 2 800 MB tj. o 100 MB více než agent řešení OSSEC a o 300 MB více než při testování hostitele v klidovém stavu.



Obrázek 20 – Graf využití CPU a RAM po nasazení Deep Security agenta v OS Windows

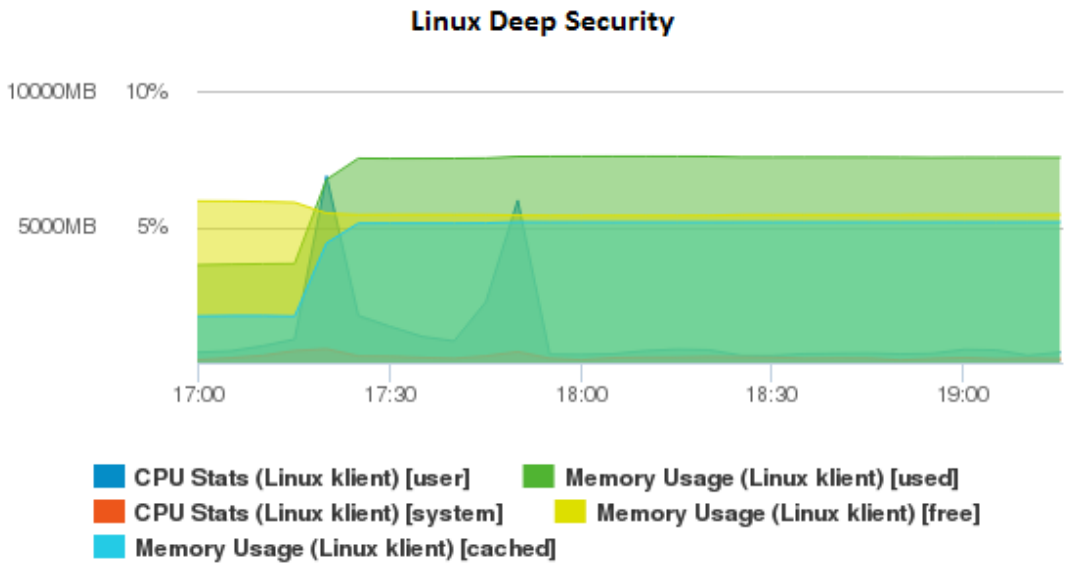
Zdroj: Autor

Instalace Deep Security agenta na OS Linux a jeho následná aktivace na management serveru v SW Deep Security Manager proběhla v 17:15, kdy se také začalo zvyšovat celkové zatížení systémových prostředků hostitele. Toto navýšení je vidět na obrázku (Obrázek 21).

Uživatelské vytížení CPU se dostalo při aktivaci agenta a následné aplikaci pravidel FW, aktualizaci SW modulů atd. až na hodnotu 7,5 %, tedy podobně jako při stejném procesu v OS Windows. Potom vytížení CPU strmě kleslo, nicméně v 17:44 byla správcem nařízena testovací kontrola integrity souborů testovacího hostitele nasazeným agentem. Z toho vyplývá druhé razantní zvýšení vytížení CPU, které je patrné na obrázku. Kontrola integrity souborů skončila zhruba v 17:50 hodin a od té doby se uživatelské vytížení CPU drželo na hodnotě okolo 0,5 %, což je téměř shodné s řešením OSSEC. Co se týče systémového vytížení CPU, tam hodnota v daných špičkách kolísala kolem hodnoty 0,5 % a po aplikování aktualizací a splnění naplánovaných úloh se ustálila na hodnotě 0,2 %. Celkově se tedy dá říci, že bylo vytížení CPU při pouhém běhu agentů, kteří ale nevykonávali určitou vynucenou kontrolu, u obou testovaných řešení shodné a to 0,7 %. V rámci porovnání operačních systémů z hlediska vytížení CPU byl tedy rozdíl okolo 3% ve prospěch Linuxu.

Ve výsledku tomu nebylo jinak, z hlediska testovaných HIDPS řešení, ani u vytížení paměti RAM. Na grafu (Obrázek 21) je sice vidět razantní nárůst spotřeby operační paměti při aktivaci agenta, ale s ním byla společně navyšována i paměť nacachovaná. Dohromady bylo využité paměti přibližně 7,6 GB a z toho nacachované 5,2 GB. Z toho v podstatě vyplývá, že bylo využito 2,4 GB paměti RAM. Oproti využití RAM agentem produktu OSSEC v OS Linux, které činilo 2,2 GB zde byl přeci jen nárůst o cca 200 MB. Rozdíl mezi nasazením agenta Deep Security v OS Windows a OS Linux z hlediska paměti RAM činil zhruba 400 MB, z čehož vyšel tedy lépe OS Linux. Je ale nutné brát v potaz, že v OS Windows disponuje

agent opět GUI, přičemž v Linuxu se obsluhuje pomocí terminálu. Dále je nutné podotknout, že OS Windows vykazoval zvýšenou spotřebu paměti RAM již při monitorování prostředků v klidovém stavu.



Obrázek 21 – Graf využití CPU a RAM po nasazení Deep Security agenta v OS Linux

Zdroj: Autor

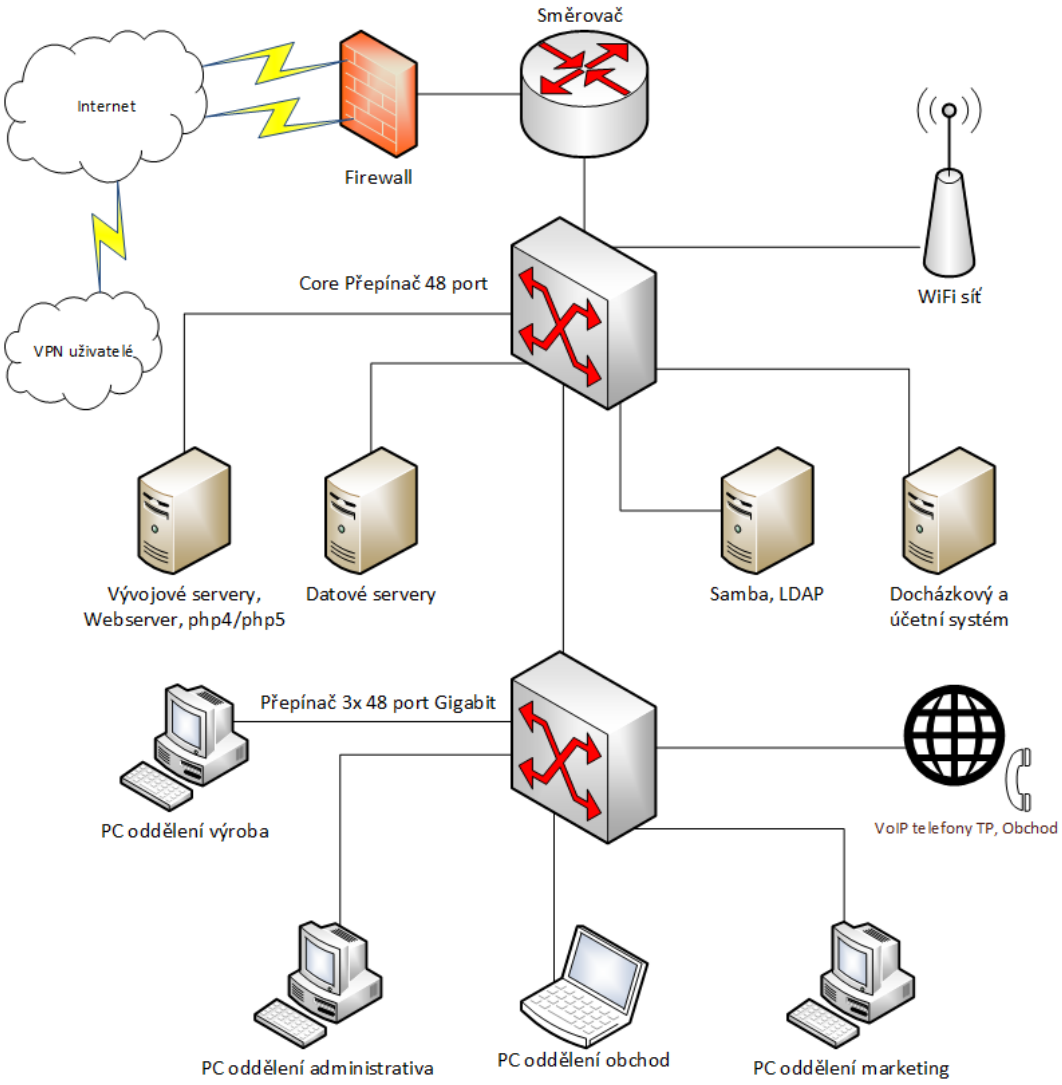
Za zmínku také stojí využití SW Deep Security Manager, který byl pro účely diplomové práce nainstalován na testovací pracovní stanici odlišné konfigurace než má testovací hostitel, na který byli nainstalováni příslušní agenti. Tento SW ubíral dle správce úloh v OS Windows více jak 1 GB paměti RAM a stabilně 0,2 % procesorového času.

8.5 Lokální podniková síť a návrh implementace HIDPS

8.5.1 Infrastruktura podnikové sítě

Na obrázku (Obrázek 22) je znázorněna reálná lokální infrastruktura podnikové sítě. K síti jsou připojeny dvě internetové konektivity. Vstupní branou do sítě je server, na kterém se vyskytuje OS Linux, a který zastává funkci FW, OpenVPN serveru a směrovače. Přes tento server proudí veškerá data. FW je řešen pomocí iptables a filtruje kompletně celý síťový provoz směrem ven i dovnitř.

LAN je dále dělena na tři VLAN. Jedná se o internetovou VLAN, Voice over Internet Protocol (VoIP) VLAN a samotnou LAN. Hlavní směrovač je připojen do core přepínače, ke kterému jsou dále připojeny další tři přepínače. K nim jsou dle jednotlivých VLAN do odpovídajících portů připojeny přes patch panel klasické ethernetové zásuvky RJ45, které jsou umístěny po podniku, a prostřednictvím kterých se připojují pracovní stanice k lokální síti.



Obrázek 22 – Lokální infrastruktura podnikové sítě

Zdroj: Autor

K lokální síti je připojeno zhruba 40 pracovních stanic v rámci různých oddělení. Tyto pracovní stanice mají nainstalován nejčastěji OS Windows 7, nicméně je v plánu do budoucna přechod na Windows 10. Malou výjimkou je obchodní oddělení, kde se střídá cca 30 notebooků také především s OS Windows.

Lokální servery jsou kromě účetního a docházkového systému provozovány na OS Linux. Nejčastěji se jedná o distribuce Ubuntu Server ve stabilní verzi 14.04. Na serverech pro vývojové a testovací účely, kde se vyskytuje php a určitá forma webserveru, je distribuce CentOS verze 7 z důvodu kompatibility s řešením pronajatém v datovém centru. Servery jsou také provozovány na diskových polích RAID (Redundant Array of Inexpensive/Independent Disks), aby byla zajištěna konzistence dat v případě HW problému s pevným diskem.

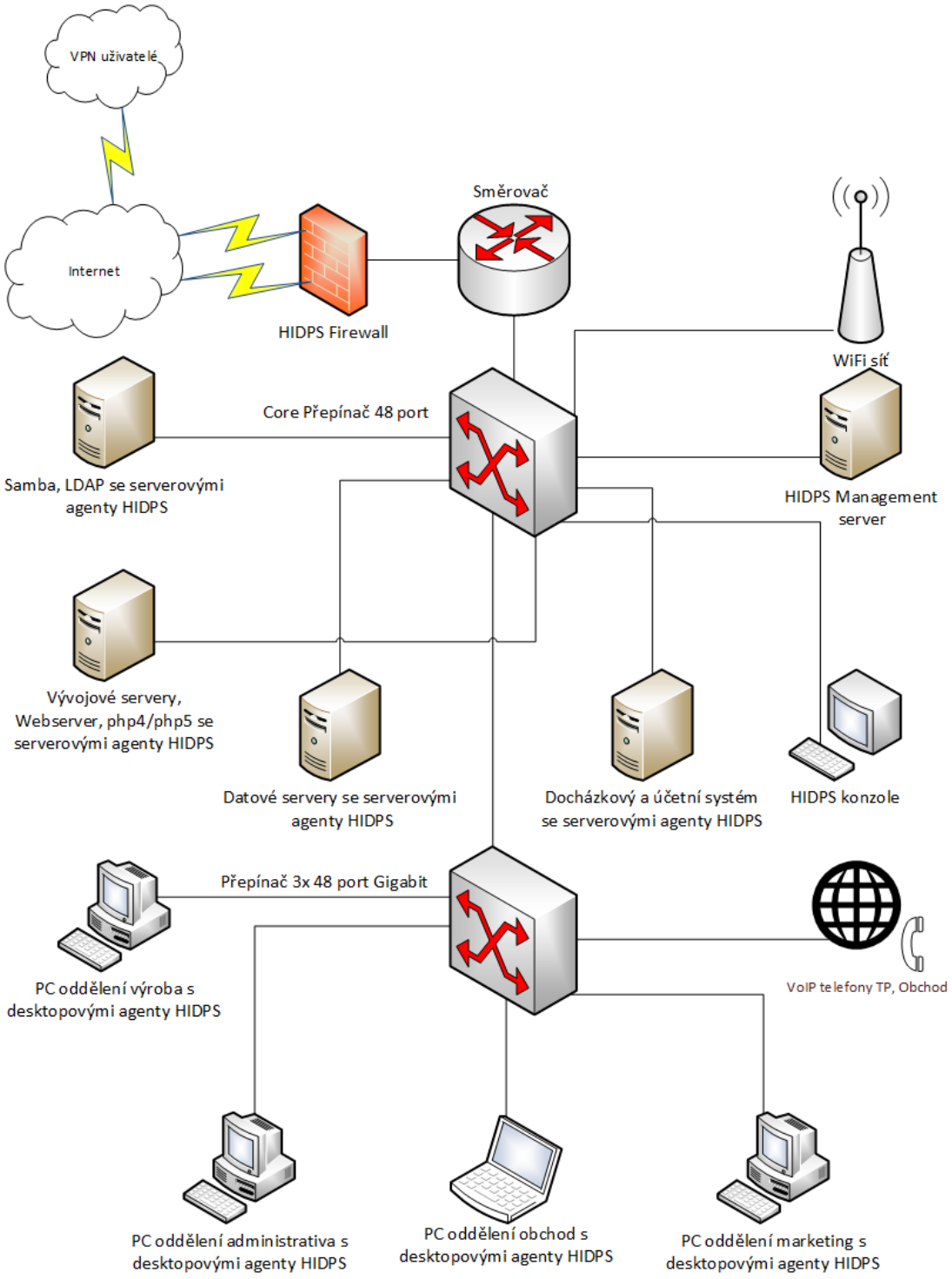
8.5.2 Návrh implementace HIDPS v rámci infrastruktury podnikové sítě

Na obrázku (Obrázek 23) lze vidět realizace návrhu implementace HIDPS v lokální podnikové síti.

Architektura podnikové sítě se v podstatě návrhem nezměnila, protože jak píše Scarfone, jednotliví HIDPS agenti jsou většinou nasazováni přímo na konkrétní hostitele, které mají monitorovat a chránit. Komponenty tak spolu obvykle komunikují skrze danou lokální síť, místo aby byla vytvořena oddělená management síť (SCARFONE, a další, 2007). V tomto návrhu byl tedy zvolen přístup bez oddělené management sítě a s agenty nasazenými přímo na konkrétní hostitele.

Do infrastruktury byly implementovány HIDPS komponenty, jako agenti, jedna konzole pro správu systému a jeden management server, který by měl po implementaci obsluhovat daná upozornění odesílaná z jednotlivých agentů. V rámci návrhu nebylo počítáno se záložním management serverem.

Agenti byli navrženi dvojího typu. Na lokální podnikové servery by měly být nasazeny serverové typy agentů a na pracovní stanice typy desktopové. Tyto dva typy se budou po implementaci lišit hlavně druhem OS (Linux, Windows). Toto kritérium je nutné brát v potaz při budoucím výběru konkrétního produktu HIDPS. Agenty se v rámci implementace plánuje nasadit na všechny pracovní stanice, kromě obchodního oddělení, a všechny servery. Obchodní oddělení, jak již bylo zmíněno v předešlé kapitole, využívá jako pracovní stanice zejména své osobní notebooky z důvodu potřebné mobility. Podniková data jsou dle nařízení z těchto pracovních stanic ukládána na lokální datové servery, kde bude HIDPS agent nasazen. Jinak se jedná o osobní data, která nebude v zájmu podniku monitorovat. Mohl by ale nastat problém, kdyby byl neopatrným zacházením na obchodní notebook nainstalován malware, který by se mohl rozšířit po lokální síti. Malware by se ovšem neměl dostat na jiné pracovní stanice, či servery, jelikož na nich je HIDPS navrženo. Tento útok by tak měl být po implementaci tohoto návrhu včas identifikován a zneškodněn. Při nasazení agentů bude nutné brát v potaz i další faktory než jen platformu, na které budou moci jednotliví agenti pracovat. Bude také nutné brát v potaz výkon hostitele a jeho potenciální snížení z důvodu nasazení agenta, jak je ostatně vysvětleno v podkapitole 6.2.



Obrázek 23 – Návrh implementace HIDPS v rámci podnikové sítě

Zdroj: Autor

HIDPS FW bude řešen jako speciální HIDPS FW dostupný přímo jako SW od výrobce daného produktu HIDPS nebo bude nasazen jako serverový agent přímo na serveru, který zastává funkci směrovače.

HIDPS konzole bude nasazena na určitou pracovní stanici nebo server. Podmínkou však je OS Windows případně Windows server. Konzole ve většině produktů není kompatibilní s OS Linux.

Na druhou stranu je HIDPS management server plánován zcela jistě na OS Linux. Management server bude ukládat a zpracovávat logy a upozornění odesílané z konkrétních agentů.

Nasazení návrhu by mělo být v souladu s kapitolou 7, tedy nejdříve výběr odpovídajícího produktu HIDPS na základě požadavků podniku a také jeho finančních možností. Dále otestování komunikace jednotlivých komponent a jejich zabezpečení nejdříve v určité testovací síti. Prověření schopnosti údržby a správy HIDPS. Teprve až bude vše vyladěno v testovacím prostředí, lze nasadit konkrétní návrh implementace do ostré podnikové sítě.

Závěr

Jedním z cílů diplomové práce bylo popsat principy systémů Intrusion Prevention Detection (IDPS) a následně provést komparativní analýzu vybraných řešení Host Intrusion Detection Prevention (HIDPS), zejména z hlediska ovlivnění výkonu hostitele po nasazení daných systémů v operačních systémech Windows a Linux. Dalším cílem bylo navrhnout nasazení HIDPS v rámci podnikové sítě.

Na základě stanovených kritérií, která byla nutná k nasazení vybraných řešení ve dvou uvedených operačních systémech a k dosažení relevantních výsledků v zátěžových testech, byla vybrána dvě HIDPS řešení. Jedno nekomerční a druhé komerční, aplikované a otestované v trial verzi. S výběrem byl problém hlavně z hlediska kompatibility daných řešení s testovanými operačními systémy. Ne všechny HIDPS nabízí agenty na konkrétní distribuci Linuxu, případně konkrétní verzi operačního systému Windows, která byla nainstalována na testovacího hostitele.

U vybraných řešení byla provedena komparativní analýza na základě složitosti nasazení a poskytovaných funkcí detekce, případně prevence nebezpečných hrozeb. Nasazení bylo u obou řešení velice podobné, nicméně komerční řešení nabízí, z hlediska funkčnosti, rozmanitější nástroje a hlavně uživatelsky přívětivější rozhraní pro správu celého systému.

Pro provedení testů systémového vytížení hostitele po nasazení jednotlivých produktů HIDPS byl, zejména za účelem věrohodnosti a konzistence výsledků, nasazen nezávislý monitorovací software. Z výsledků testů vyplývá, že v rámci testů mezi komerčním a nekomerčním řešením vychází lépe, z hlediska vytížení prostředků hostitele, nekomerční řešení. To ovšem za cenu menšího množství funkcí a méně přehledné správy celého systému. Při porovnání vytížení v rámci operačních systémů je nutné podotknout, že OS Windows využívá bez nasazení určitého řešení více systémových prostředků než OS Linux. Pokud se tento fakt vezme v potaz, lze říci, že rozdíl ovlivnění výkonu hostitele nasazenými řešeními HIDPS je minimální.

Návrh implementace HIDPS byl proveden na modelu reálné lokální podnikové sítě, která funguje v současnosti v praxi.

Do budoucna by bylo možné diplomovou práci rozšířit například o testování jednotlivých řešení HIDPS v rámci určitých útoků na hostitele, namísto testů zaměřených na výkon hostitele v daných operačních systémech. Bylo by ale nutné zaměřit se pouze na jeden operační systém, případně jeden produkt, jelikož nalézt v současnosti samostatné řešení stejné technologie, kompatibilní s různými typy operačních systémů, je nelehký úkol. Případně by bylo možné se zaměřit na jiné technologie nebo realizovat daný návrh nasazení HIDPS řešení v praxi. Co se ale týče cílů stanovených v této diplomové práci, lze je považovat za splněné.

Literatura

ALEXANDER, Jason. 2009. Intrusion Detection and Prevention Systems (IDS/IPS) Good Practice Guide. *systems.hscic.gov.uk.* [Online] 31. Září 2009. [Citace: 22. Březen 2015.] http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/intrusion.pdf.

ARORA, Himanshu. 2012. OSSEC - The open source Intrusion prevention system. *www.ibm.com.* [Online] 21. Říjen 2012. [Citace: 7. Srpen 2015.] https://www.ibm.com/developerworks/community/blogs/6e6f6d1b-95c3-46df-8a26-b7efd8ee4b57/entry/ossec_the_open_source_intrusion_prevention_system49?lang=en.

DAVE, Shalvi, TRIVEDI, Bhushan a MAHADEVIA, Jimit. 2013. Detection Capability of IDPS. *arxiv.org.* [Online] Březen 2013. [Citace: 18. Duben 2015.] http://arxiv.org/ftp/arxiv/papers/1304/1304.5022.pdf.

HALETKY L., Edward. 2011. A Look at Trend Micro Deep Security 7.5. *la.trendmicro.com.* [Online] Březen 2011. [Citace: 16. Srpen 2015.] http://la.trendmicro.com/media/report/deep-security-virtualization-practice-en.pdf.

HARGRAVE, Vic. 2013. Securing Hadoop with OSSEC. *vichargrave.com.* [Online] 28. Září 2013. [Citace: 7. Srpen 2015.] http://vichargrave.com/securing-hadoop-with-ossec/#OSSEC_in_a_Nutshell.

HUDEC, Ladislav. 200-?. Systémy detekcie a prevencie prienikov (IDPS). *www2.fiit.stuba.sk.* [Online] 200-? [Citace: 22. 3 2015.] http://www2.fiit.stuba.sk/~lhudec/SIN/Systemy_IDPS.ppt.

Neznámý. 2014. Guide to network defense and countermeasures. *http://cmsu2.ucmo.edu/.* [Online] 2014. [Citace: 18. Duben 2015.] http://cmsu2.ucmo.edu/public/classes/kesh/CIS5650II/ch01.ppt.

—. 2013. Host Intrusion Prevention Systems. *nsa.gov.* [Online] Říjen 2013. [Citace: 28. Červenec 2015.] https://www.nsa.gov/ia/_files/factsheets/i43v_slick_sheets/slicksheet_hostintrusionpreventionsystems.pdf.

—. 2014. tcpdump. *tcpdump.org.* [Online] 11. Červenec 2014. [Citace: 19. Duben 2015.] http://www.tcpdump.org/tcpdump_man.html.

PIPER, James. 2011. *Intrusion Prevention Systems for Dummies.* Indianapolis : Wiley Publishing, 2011. 978-1-118-00474-6.

SCARFONE, Karen a MELL, Peter. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). *csrc.nist.gov.* [Online] Únor 2007. [Citace: 9. Březen 2015.] http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. 800-94.

SHINDER, Deb. 2005. Strengthen network defenses by using a DMZ. *techrepublic.com.* [Online] 29. Červen 2005. [Citace: 22. Duben 2015.] http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/.

STANCIU, Nicoleta. 2013. Technologies, Methodologies and Challenges in Network Intrusion Detection and Prevention Systems. *revistaie.ase.ro.* [Online] 17. Leden 2013. [Citace: 19. Duben 2015.] http://revistaie.ase.ro/content/65/12%20-%20stanciu.pdf. 14531305.

ŠNAJDR, Petr. 2013. Dvoufaktorová autentifikace mýty a realita. *www.systemonline.cz.* [Online] Červen 2013. [Citace: 15. Duben 2015.] http://www.systemonline.cz/it-security/dvoufaktorova-autentizace-myty-a-realita.htm.

WHITMAN, Martin, a další. 2013. Guide to Network Security. *books.google.cz.* [Online] 2013. [Citace: 19. Duben 2015.] https://books.google.cz/books?id=VRQLAAAAQBAJ&pg=PA224&lpg=PA224&dq=network+idps&source=bl&ots=FRXcqRPKmn&sig=J5ZvO21VufjcgfPJ8yM9dHflBsI&hl=cs&sa=X&ei=Gk4yVZznA4O5sQG1rIAo&ved=0CFcQ6AEwBTgK#v=onepage&q&f=false. 978-0-8400-2422-0.

Příloha A – Přiložené CD

Přiložené CD obsahuje konfigurační soubory agentů a management serveru nekomerčního HIDPS řešení OSSEC. Adresáře jsou pojmenovány podle OS, na kterém byl agent nasazen. Adresář s konfiguračním souborem serveru je pouze z OS Linux, jelikož dané řešení management server pro OS Windows nepodporuje.

Co se týče komerčního řešení Deep Security. Management server je kompatibilní pouze s OS Windows a jednotliví agenti se spravují přímo z jeho webového rozhraní. Konfigurační soubory, které by mělo smysl přikládat, tedy toto řešení neobsahuje.