McAfee Network Security Platform (IPS)

Síťová IPS/IDS sonda nové generace s multigigabitovou propustností

IPS/IDS síťové sondy McAfee Network Security Platform preventivně chrání vnitřní síť před známými/ neznámými/ spyware, malware, botnety, DoS/DDoS útoky, VoIP hrozbami, atd. Kombinuje několik stupňů detekce narušení od rozpoznání útoků na základě signatur přes pravidla chování, anomálií provozu, rozpoznání aplikací a „Zero Day Attack" ochran. Poskytuje snadný přechod z detekce na prevenci, precizně a rychle blokuje hrozby bez zastavení legitimního provozu, a tím šetří celkové náklady na ochranu a obnovu systémů.

Klíčové charakteristiky

- ⇒ Kombinace detekce na základě signatur, aplikací i pravidel chování chrání vnitřní síť před známými i neznámými útoky, jako jsou např. DoS útoky, spyware, malware, botnets, VoIP hrozby, tunelování a různé šifrované a kombinované útoky.
- ⇒ Flexibilní definice politik pro síťový segment, skupinu stanic, VLAN či konkrétní systém.
- ⇒ Integrace IPS a interního stavového firewallu chrání veškerá zařízení připojená v síti.
- ⇒ Inovovaná technologie Virtual IDS umožňuje definovat více politik na applianci, přičemž každá politika může chránit specifické prostředí.
- ⇒ Odlišné politiky na základě směru provozu.
- ⇒ Nepřetržitá aktualizace systému díky globální síti laboratoří McAfee.
- ⇒ 4 různé možnosti, jak umístit sondu do topologie konkrétní LAN.
- ⇒ Schopnost kontrolovat SSL šifrovaný provoz.
- ⇒ Velké množství předdefinovaných reportů.
- ⇒ Management konzole dostupná prostřednictvím webového prohlížeče.
- ⇒ Detekce a granulární filtrování aplikací používajících pro komunikaci protokol http.
- ⇒ Škálovatelné řešení s propustností od 150 Mbps do 80 Gbps, podpora Fast a Gigabit Ethernet.
- ⇒ Podpora IPv6, MPLS, GRE, Q-in-Q Double.
- ⇒ Možnost integrace služby cloudového sandboxu CTD

Přínosy

- ⇒ Vhodné i pro nasazení do sítě, kde není legitimní provoz z počátku přesně definován – plynulý přechod od detekce k prevenci.
- ⇒ Snadno nasaditelná forma appliance na proprietární hardwarové platformě vhodná pro všechny typy organizací.
- ⇒ Možnost maximalizovat efektivitu integrací s dalšími bezpečnostními systémy McAfee pro dosažení jednotné a snadno spravovatelné bezpečnostní infrastruktury:
  - McAfee Host IPS - řešení s desktop firewallem pro ochranu koncových stanic a serverů,
  - McAfee ePolicy Orchestrator – společná centrální správa pro všechna McAfee řešení,
  - McAfee Network Security Threat Behavior Analysis – monitorování a analýza síťového provozu

Snadné nasazení a správa v každé síti

K dispozici je vestavený průvodce, který zajistí bezproblémové nasazení. Jednoduchá stále dostupná (redundantní) správa vlastní sondy i bezpečnostních politik je dostupná prostřednictvím webového prohlížeče. Zahrnuje předdefinované okamžitě použitelné bezpečnostní politiky, integrovanou podporu pro autentizaci uživatelů do externí databáze, automatizovaný „failover" a „fail-back" a systém obnovy kritických konfiguračních dat. Pro rozsáhlejší implementace sond je k dispozici nástroj poskytující hierarchizovanou správu s centrální kontrolou. Nastavení pro vysokou dostupnost umožňuje transparentní, Stateful, L7 Fail-over, L2 Fail-open a hardware Fail-open pro odstranění rizika představujícího nefunkčnost prvku v síti.

Hlavní pilíře ochrany

Pokročilá prevence narušení sítě

- Stavová kontrola datového toku
- Detekce anomálií
- Detekce na základě signatur
- Detekce na základě reputace (McAfee GTI)
- Heuristická detekce Botnetů
- Korelace útoků
- Detekce protokolů 7. síťové vrstvy
- Hloubkové filtrování http
- Karanténa nakažených strojů

Granulární kontrola

- Přehled nad aplikacemi
- ACL pravidla založená na geolokaci
- Connection limiting
- Host karanténa prostřednictvím IPS

Prevence DoS a DDoS útoků

- Heuristická a prahová detekce
- Connection limiting na základě geolokace a reputace
- Detekce na základě učení

Přehled o stavu sítě

- Systémové informace
- Přehled o využívaných aplikacích
- Korelace zranitelností
- Spolupráce s Host IPS
- Inspekce virtuálního prostředí

McAfee Global Threat Inteligence

- IP reputace
- Reputace souborů
- Aplikační a protokolová reputace
- Geolokace

Gartner NSS LABS

Integrace s McAfee Endpoint Intelligence Agent

Jedná se o doplněk, který je zdarma součástí licence a přináší analytikovi širší kontext, zejména:

- Sběr informací o procesech na koncových strojích, které komunikují po síti (potenciálně se může jednat o malware)
- Metadata o procesech jsou srovnávána s antimalware cloudovou službou McAfee Global Threat Intelligence
- Známý malware je označen a infikovaný stroj může být zařazen do síťové karantény (dvojnásobná antimalware kontrola bez nutnosti dokupovat další licence a prakticky bez dopadu na výkon)
- Neznámý software, který generuje podezřelý provoz, může být cílem další analýzy, zatímco Důvěryhodný software je označen a jeho analýza nepřidělává analytikovi práci

Integrace s McAfee Cloud Threat Detection

Tato cloudová služba efektivně chrání proti pokročilým hrozbám, ransomware a zero-day útokům. Neznámý soubor tzv. „grey file" sonda odešle do cloudového sandboxu, kde je nejdříve zkoumán statickou analýzou a poté spuštěn ve virtuálním prostředí, kde se uplatňuje behaviorální analýza. Vše, co se malware pokusí udělat je nahráváno, prošetřeno a vyhodnoceno. Po vyhodnocení škodlivosti souboru pošle CTD informaci zpět do sondy, která jej buď propustí nebo odstraní.

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

Funkce / vlastnosti / modelová řada / McAfee Network Security Portfolio

McAfee NS Series

McAfee přichází s IPS nové generace, které nabízí propustnost až 70Gbps. Nové modely dále nabízí až 16 pevných portů (se zabudovaným fail-open kitem) a možnost osadit zařízení dalšími síťovými I/O moduly. Byla zvýšena propustnost při zapnuté kontrole šifrovaného provozu a navýšena podpora pro současná spojení a připojení za sekundu. Tyto modely nabízí i 40GE QSFP+ porty a až 16 10GE SFP+ portů.

Virtual Network Security Platform

Jedná se o IPS sensory přímo určené pro ochranu virtuálního prostředí. Tomu odpovídají i možnosti nasazení sondy pro: inspekci uvnitř virtuálního prostředí, inspekci na rozhraní fyzického a virtuálního prostředí, ale i inspekci mezi fyzickými rozhraními a na SPAN portu. Virtuální sonda nabízí podobnou funkcionalitu jako hardwarové modely a navíc dovoluje aplikovat bezpečnostní politiky pro virtualizovaná prostředí. Virtuální IPS sonda VM1000-CLD je určena pro cloudové platformy – privátní i veřejné (např. Amazon Web services (AWS), OpenStack Midokura Midonet, VMware NSX)

Modely	VM100	VM600	VM1000-CLD
Maximální propustnost	500 Mbps	1 Gbps	700 Mbps
Reálná propustnost	200 Mbps	600 Mbps	200 Mbps
Max. počet souč. spojení	56 000	367 000	56 000
Navázaná spojení / sec	6 000	20 000	6000
Podporované UDP toky	39 000	254 000	39 000
Počet monit. párů portů	2	3	1
Virtuální rozhraní / sonda	32	100	32
DoS profily	100	300	100
Přizpůsobitelné signatury	20 000	100 000	20 000
Virtuální platforma	VMware ESX 5.0, 5.1, 5.5		ESXi5.5

Integrace s McAfee Network Security Threat Behavior Analysis

Analyzuje síťový provoz a slouží k odhalení a následnému nahlášení hrozeb na základě jejich chování v síti. Dodává ucelené analytické informace o provozu v síti včetně informací získaných z IPS a může aktivně skenovat stroje v síti. Navíc obsahuje antivirus, který dokáže kontrolovat provoz na IPS sondě. Součástí McAfee Network Security Platform je licence McAfee NTBA pro nasazení do virtuálního prostředí a pro 2 zdroje logů.

Specifikace modelové řady NS-series

Modely	NS9300/NS9200	NS9100	NS7300	NS7200	NS7100	NS5200	NS5100	NS3200	NS3100
Maximální propustnost	70 / 35 Gbps	30 Gbps	15 Gbps	10 Gbps	5 Gbps	3 Gbps	1,5 Gbps	1 Gbps	600 Mbps
Reálná propustnost	40 / 20 Gbps	10 Gbps	5 Gbps	3 Gbps	1,5 Gbps	1 Gbps	600 Mbps	200 Mbps	100 Mbps
Max. počet souč. spojení	32 / 16 mil	13 mil	10 mil	5 mil	3 mil	1 350 000	750 000	80 000	40 000
Spojení za vteřinu	1 mil/575 000	450 000	225 000	200 000	135 000	45 000	40 000	20 000	15 000
Propustnost se SSL dešifrací	40 / 20G bps	10 Gbps	5 Gbps	3 Gbps	1,5 Gbps	1 Gbps	600 Mbps	-	-
SYN cookie rate per second	13,5 / 9 mil	5 mil	3,3 mil	1,8 mil	1,4 mil	800 000	600 000	-	-
Importovaný SSL klíč	1024	1024	1024	1024	1024	1024	1024	-	-
Porty									
Gigabit ethernet – pevné porty	16 / 8*	8*	8	8	8	8	8	8	8
Gigabit - SFP porty	32** / 16**	16**	2**	2**	2	12	12	-	-
10 Gigabit ethernet	32 / 16	16	18	18	18	2	2	-	-
Vyhrazené "response" porty	1	1	1	1	1	1	1	1	1
Vyhrazené "management" porty	1	1	1	1	1	1	1	1	1
Vestavěné Porty s „Fail-Open“	16 / 8	8	8	8	8	8	8	-	-
Externí "Fail-Open" kontrol. porty	- / -	-	1	1	1	6	6	-	-
Konzolové a "aux" porty	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Fail-close	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Způsoby nasazení									
Span port monitoring	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Tap mode	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
In-line mode	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Port clustering	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Počet virtuálních IPS systémů	1 000 / 1 000	1 000	1 000	1 000	1 000	1000	100	32	16
Monitorování active-active linek	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Monitorování active-pasive linek	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Monitorování asymetr. provozu	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Qos	ne/ne	ne	ne	ne	ne	ne	ne	ne	ne
Vysoká dostupnost (HA)									
Redundantní zdroj	ano / ano	volitelně	volitelně	volitelně	volitelně	volitelně	volitelně	-	-
Detekce poruchy zařízení	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano
Detekce výpadku linky	ano / ano	ano	ano	ano	ano	ano	ano	ano	ano

* obsahuje navíc 2 pevné 40 Gigabit porty; ** možnost osadit zařízení dvěma moduly, které obsahují 8 portů (SFP+ / SFP) 10 GigE / 10 GigE nebo 2 port (QSFP+) 40 GigE

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz