Příloha č. 2 smlouvy o dílo Č.j. R- 04-1/11-2019

Podrobný položkový rozpis nabízeného plnění

Model, P/N	Popis produktu	Množství v 1 kuse	Celkové množství
FlowMon			
Hardware a software			
IFP-4000-CU	Flowmon Probe 4000	1	1
FPC-ADS-S	Flowmon ADS Standard	1	1
FP-APM-S	Flowmon APM Standard	1	1
FC- R5-6000 Pro	DR Collector R5-6000 Pro	1	1
Technical Support Service			
GS-IFP-4000-CU	Gold support 1 rok: IFP-4000-CU	1	5
GS-FPC-ADS-S	Gold Support 1 rok: Flowmon ADS Standard	1	5
GS-FP-APM-S	Gold support 1 rok: Flowmon APM Standard	1	5
GS-FC- R5-6000 Pro	Gold Support 1 rok: Flowmon Collector R5-6000 Pro	1	5
Model, P/N	**Popis produktu**	**Množství v 1 kuse**	**Celkové množství**
Novicom			
Hardware a software			
AN-ES-5K	AddNet Enterprise Server Edition - 5000	1	1
AN-ES-HA-5K	AddNet Enterprise Server Edition HA-5000	1	1
AN-WS	AddNet Work server	1	2
NA-1U-STP	Novicom appliance 1U Standard Plus R18	1	2
NA-1U-STP-EHW	Novicom appliance 1U STP Extended Warranty	1	6
Technical Support Service			
SU-AN-ES-5K	AddNet Enterprise Server Edition - 5000	1	5
SU-AN-ES-HA-5K	AddNet Enterprise Server Edition HA - 5000	1	5
SU-AN-WS	AddNet Work server	1	10
SU-NA-1U-STP	Novicom appliance 1U Standard Plus R18	1	10

7.2.1 Datasheety nabízeného řešení

7.2.2 Flowmon Sonda

Flowmon Sonda

Výkonná autonomní NetFlow/IPFIX sonda

Popis produktu

ÚVOD

Flowmon sonda je výkonné autonomní zařízení, které monitoruje provoz na počítačové síti, vytváří o něm statistiky v podobě IP toků a zasílá (exportuje) je k uložení a další analýze na Flowmon kolektor či jinou kolektorovou aplikaci kompatibilní s NetFlow/IPFIX standardem.

IP toky vytvořené Flowmon sondami obsahují informace o tom, kdo komunikoval, s kým, jak dlouho, jakým protokolem, kolik přenesl dat a řadu dalších informací ze záhlaví paketů (TCP příznaky, ToS, AS). Flowmon sonda podporuje export dat ve fixním formátu NetFlow verze 5 či flexibilních formátech NetFlow verze 9 a IPFIX, u kterých je možné přímo zvolit, jaké informace se mají monitorovat a exportovat.

Flowmon sondy umožňují monitorovat i položky vyšších vrstev (L5-L7), jako jsou HTTP informace (URL, hostname), DNS protokol (DNS dotazy, odpovědi, příznaky, atd.), VoIP statistiky (latence, jitter, ztráty paketů), či přímo provádět detekci aplikací (podpora NBAR2 standardu) a měřit výkonové parametry sítě (NPM – Network Performance Monitoring). Díky tomu přináší nejenom základní přehled o objemu síťového provozu, ale také detailní informace o dění v počítačové síti vhodné pro řešení síťových problémů (troubleshooting), analýzu výkonu sítě (performance monitoring), správu a optimalizaci sítě a v neposlední řadě i pro zvýšení její bezpečnosti.

MOŽNOSTI ZAPOJENÍ FLOWMON SONDY

Flowmon sondy jsou dostupné jako fyzická či virtuální zařízení. Díky tomu jsou vhodné pro monitorování fyzických i virtuálních sítí v rámci virtuálního prostředí.
Sondy obsahují jeden management port pro správu a přístup k webovému rozhraní zařízení a jeden až šest monitorovacích portů, které slouží pro zapojení do těch bodů sítě, ve kterých je monitoring požadován. Sondy jsou zapojovány do sítě zcela pasivně prostřednictvím SPAN/mirror/monitoring portu aktivního centrálního prvku (směrovač, přepínač, vSwitch) nebo TAPu (pasivní rozbočovač/splitter). Díky tomu jsou na monitorované lince nedetekovatelné ani jí nijak neovlivňují.

KLÍČOVÉ VLASTNOSTI

- **Výkonná autonomní NetFlow v5/v9, IPFIX sonda**
- **Podpora pro 10 Mb/s až 100 Gb/s Ethernet**
- **Zpracování dat bez ztráty paketů**
- **Podpora pro IPv4, IPv6, MAC, VLAN a MPLS**
- **HTTP, DNS a VoIP analýza, detekce aplikací (NBAR2)**
- **Monitorování výkonových parametrů sítě (RTT, SRT, retransmise, out-of-order pakety, delay a jitter)**
- **Identifikace zařízení, operačního systému, verze internetového prohlížeče**
- **Dostupné jako fyzické nebo virtuální zařízení**
- **Až 6 monitorovacích portů v jednom zařízení**
- **Jednoduchá správa přes webové rozhraní**
- **Integrovaný kolektor pro zobrazení a analýzu dat**
- **Plně kompatibilní s NetFlow kolektory třetích stran**
- **Zpracování až 16 milionů toků současně**

PORTFOLIO PRODUKTŮ

Portfolio produktů Flowmon sond zahrnuje kompletní řadu modelů pro monitorování fyzických i virtuálních sítí od 10 Mb/s až po 100 Gb/s včetně hardwarové akcelerovaných modelů garantujících zpracování paketů na plné rychlosti linky.

Většina modelů Flowmon sond obsahuje také vestavěnou kolektorovou aplikaci Flowmon Monitorovací Centrum (FMC), která umožňuje uložení a analýzu statistik vytvořených danou sondou.

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhneme projekt monitorování Vaší sítě.

www.flowmon.com

Flowmon Networks

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com

7.2.3 Flowmon Kolektor

Flowmon Kolektor

NetFlow/IPFIX kolektor pro detailní přehled o dění v síti

Popis produktu

ÚVOD

Flowmon kolektor je fyzické či virtuální zařízení určené pro dlouhodobé ukládání, zobrazení a analýzu síťových toků ve formátech NetFlow/IPFIX/sFlow a dalších. Flowmon kolektor umožňuje uživatelům přesně, rychle a efektivně řešit problémy v síti, zvýšit její bezpečnost díky detekci vnitřních i vnějších útoků, předcházet incidentům, optimalizovat síť a snížit provozní náklady.

Flowmon kolektor přináší kompletní přehled o dění v síti ve formě dlouhodobých grafů s možností volby perspektivy, Top statistik o uživatelích, službách a komunikacích, uživatelsky definovatelných profilech, možnosti zobrazení dat až na úrovni jednotlivých komunikací a mnoho dalšího. Poskytuje tak plnou sadu funkcí pro monitorování a reportování o síťovém provozu včetně upozorňování v případě definované události. Funkčnost Flowmon kolektoru je dále možné rozšířit o systém Flowmon ADS (technologie NBA/NBAD) pro automatickou detekci bezpečnostních a provozních incidentů, o Flowmon DDoS Defender pro ochranu proti volumetrickým DDoS útokům, o Flowmon APM (Application Performance Monitoring) pro měření výkonnosti aplikací a Flowmon Traffic Recorder pro záznam kompletní datové komunikace.

HLAVNÍ FUNKCE

Kromě detailního přehledu o komunikaci v počítačové síti Flowmon kolektor poskytuje pokročilé vlastnosti a funkce, mezi které patří:

Analýza položek protokolů vyšších vrstev – podpora pro příjem a analýzu VoIP statistik (zpoždění, ztrátovost, jitter), HTTP informací (URL, hostname), monitorování DNS provozu (DNS dotazy, odpovědi, příznaky, atd.), detekovaných aplikací dle Cisco NBAR2 standardu.

Network Performance Monitoring (NPM) – podpora pro příjem a analýzu výkonových parametrů sítě (RTT, SRT, retransmise, out-of-order pakety, delay a jitter), podpora pro standard Cisco AVC ART.

KLÍČOVÉ VLASTNOSTI

- **Vysoce výkonný kolektor pro analýzu síťových toků**
- **Poskytuje kompletní přehled o dění v síti včetně možnosti zobrazení dat až na úroveň komunikací**
- **Podpora NetFlow v5/v9, IPFIX, sFlow, NetStream, jFlow včetně moderních položek typu NBAR2, NSEL/NEL, MAC adresy, HTTP, VoIP a dalších**
- **Popora pro výkonové parametry sítě (NPM, AVC ART)**
- **Statistiky zobrazovány ve formě grafů a tabulek s možností volby různých perspektiv**
- **Top N statistiky, uživatelsky definované pohledy, automatické reporty, upozornění na email – alerty**
- **Podpora konceptu BYOD (bring-your-own-device) a identifikace zařízení včetně operačního systému**
- **Automatická detekce zdrojů dat**
- **Podpora identity uživatele jako součást flow statistik**
- **Víceuživatelský přístup (multitenancy)**
- **Vysoce výkonný databázový systém optimalizovaný pro velmi rychlou práci s daty**
- **RESTful API pro automatizované získávání a zpracování flow statistik v systémech třetích stran**

PORTFOLIO PRODUKTŮ

Portfolio Flowmon kolektorů zahrnuje řadu modelů ve formě fyzických či virtuálních zařízení, které se liší především diskovou kapacitou a poskytovaným výkonem. Dostupné jsou jak modely vhodné pro menší a střední sítě tak také modely vhodné pro největší sítě či sítě poskytovatelů připojení k internetu.

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhneme projekt monitorování Vaší sítě.

www.flowmon.com

Flowmon Networks

Flowmon Networks, a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com

7.2.4 Flowmon ADS

Flowmon ADS

Systém detekce anomálií pro vnitřní i vnější bezpečnost sítě

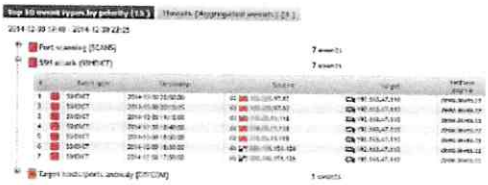
Popis produktu

ÚVOD

Flowmon ADS je řešení přinášející novou dimenzi využití statistik o provozu datové sítě (NetFlow, IPFIX, jFlow, NetStream). Díky unikátní technologii tzv. behaviorální analýzy (Network Behavior Analysis) je možné identifikovat hrozby, které překonaly zabezpečení na perimetru, byly zavlečeny do datové sítě jiným způsobem nebo pro ně dosud neexistuje signatura. Automatická detekce bezpečnostních incidentů, anomálií provozu datové sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.

JEDINEČNÉ SPOJENÍ BEZPEČNOSTI A SPRÁVY SÍTĚ

Flowmon ADS kombinuje funkce důležité pro správce datové sítě, bezpečnostní nebo IT manažery do jediného nástroje schopného poskytovat velmi přesné a spolehlivé informace ve formě událostí. Díky automatickým notifikacím a reportingu je možné systém provozovat jako tzv. standalone řešení. Integrace s dohledovými systémy, incident handling systémy a systémy typu SIEM podporuje nasazení v prostředí rozsáhlých podnikových sítí.



Interaktivní dashboard poskytuje celkový přehled o stavu datové sítě s možností získat okamžitě ke každé události detailní informace o provozu, který danou událost způsobil. Alternativní pohledy na události, včetně jejich vizualizace formou orientovaných grafů, umožňují operátorovi analyzovat příčiny a relevantní okolí události. Samozřejmostí je integrace na síťové služby DNS, WHOIS nebo geolokace a vizualizace na mapě světa. Díky službě **Flowmon Threat Intelligence** získává Flowmon ADS informace z reputačních databází pro přesnější detekci infikovaných stanic nebo odhalení komunikace s botnet command & control centry. Flowmon Threath Intelligence také umožňuje aktualizaci vzorů chování detekčních metod a tím detekovat nejnovější hrozby jako například zranitelnosti nultého dne a další.

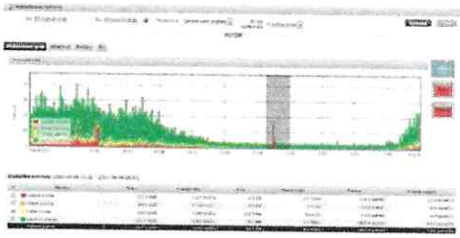
PŘÍNOSY A VÝHODY

- **Automaticky identifikuje hrozby, útoky, incidenty a konfigurační problémy**
- **Vhodně doplňuje nástroje na bázi signatur a zvyšuje bezpečnost**
- **Pracuje na úrovni sítě bez nutnosti cokoliv instalovat na koncové stanice**
- **Odhaluje hrozby, útoky, úniky dat a incidenty, minimalizuje tak jejich finanční dopady**
- **Proaktivně identifikuje možné zdroje a příčiny problémů**
- **Detekuje nežádoucí aktivity uživatelů a zneužívání datové sítě**
- **Plugin pro řešení Flowmon, jednoduchá instalace a zhodnocení stávajících investic**

ANALÝZA SIGNATUR VS. BEHAVIORÁLNÍ ANALÝZA

Systémy typu IDS, IPS nebo antiviry používané pro ochranu perimetru nebo koncových stanic identifikují hrozby a incidenty na základě tzv. signatur. Jedná se o definice známého malware a nežádoucího software.

Oproti tomu behaviorální analýza umožňuje odhalovat dosud neznámé nebo specifické hrozby, pro které signatura neexistuje. Flowmon ADS implementuje desítky pokročilých algoritmů s prvky umělé inteligence, které vyhodnocují chování každého jednotlivého zařízení v síti, dynamicky stanovují profily očekávaného chování a upozorňují na nestandardní odchylky. Díky tomu představuje Flowmon ADS ideální nástroj pro odhalování pokročilých útoků a hrozeb typu APT (Advanced Persistent Threat).



Flowmon Networks

Flowmon Networks, a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com

Flowmon ADS

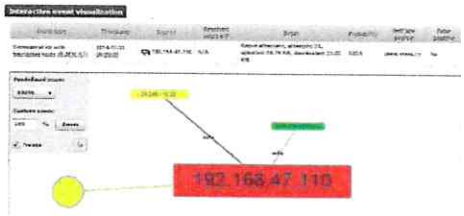
Systém detekce anomálií pro vnitřní i vnější bezpečnost sítě

Popis produktu

DETEKCE INCIDENTŮ A ANOMÁLIÍ CHOVÁNÍ

Flowmon ADS automaticky identifikuje celou řadu bezpečnostních a provozních incidentů, anomálie provozu datové sítě nebo nežádoucí chování uživatelů. Typicky se jedná o:

- **Útoky na síťové služby** s cílem získat neoprávněný přístup k zařízení nebo službě.
- **Infikované stanice** a komunikaci s potenciálně nežádoucími IP adresami, mezi které patří botnet command & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu a malware na základě pokročilých reputačních databází.



- **Anomálie DNS** provozu indikující infikované stanice, nežádoucí software nebo chybné konfigurace síťových služeb.
- **Anomálie DHCP** provozu indikující stanice pokoušející se o odposlech síťové komunikace, podvržené adresy (spoofing) nebo chybné konfigurace.
- **Skenování portů** a obdobné projevy infikovaných stanic nebo nežádoucích aktivit útočníků či interních uživatelů.
- **Potenciálně nežádoucí síťové aplikace** jako jsou P2P sítě nebo on-line komunikátory.
- **Anonymizační služby**, jako např. TOR (The Onion Router) nebo obcházení proxyserveru.
- **Výpadky** nebo špatné konfigurace síťových služeb.
- **Potenciální úniky dat** a využívání služeb pro výměnu dat na internetu.
- **Útoky na internetovou telefonii**, ústředny a přístroje připojené do IP sítě.
- **Nestandardní poštovní komunikace** a šíření spamu.
- **Zneužívání zranitelností serverů** a síťových služeb pro DDoS útoky.

KLÍČOVÉ VLASTNOSTI SYSTÉMU

- **Snadná instalace na sondu nebo kolektor**
- **Podpora NetFlow v5/v9, IPFIX, jFlow, NetStream, sFlow (částečně)**
- **Podpora NBAR2, analýza HTTP informací, MAC adres, VoIP informací**
- **Deduplikace a párování datových toků (RFC 5103)**
- **Multitenance a řízení uživatelských oprávnění pro separaci jednotlivých uživatelů**
- **Notifikace událostí e-mailem (variabilní formáty) a export událostí (syslog, SNMP, CSV)**
- **Modely pro korporátní sítě i rozsáhlé sítě poskytovatelů datové konektivity (ISP)**

SNADNÉ NASAZENÍ A ROZŠÍŘITELNOST

Veškeré metody detekce anomálií jsou dostupné tzv. out-of-box, což umožňuje okamžité nasazení bez nutnosti náročné konfigurace nebo úprav pro dané prostředí.

Flowmon ADS využívá pro analýzu provozu více než 50 různých algoritmů s prvky umělé inteligence (dynamické profilování standardního chování a detekce odchylek, dynamické rozhodovací stromy, strojové učení, prediktivní analýza časových řad, algoritmy shlukové analýzy), které analyzují provoz z různých úhlů pohledu a identifikují podezřelé stanice a události.

Díky integrovanému konfiguračnímu průvodci, šablonám typických konfigurací pro různá prostředí a správě falešných poplachů (false positives) implementace nevyžaduje expertní znalosti.

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhneme projekt monitorování Vaší sítě.

www.flowmon.com

Flowmon Networks

Flowmon Networks, a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com

7.2.5 Flowmon APM

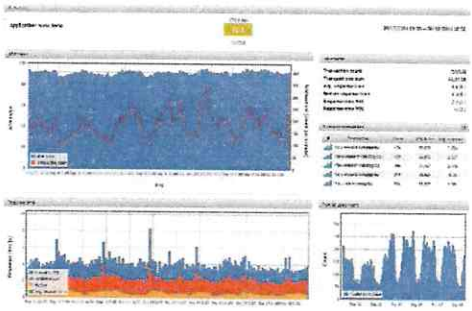
FlowMon APM

Plugin pro monitorování aplikace z pohledu uživatele

Popis produktu

ÚVOD

FlowMon APM (Application Performance Monitoring) je řešení, které bez instalace agentů či rekonfigurace serverů monitoruje aplikace z pohledu jejich uživatelů. Pro všechny uživatele, všechny uživatelské transakce a v reálném čase poskytuje podrobné informace o skutečné výkonnosti aplikací. Díky využití architektury řešení FlowMon je možné APM nasadit v řádu minut a začít transparentně monitorovat kritické podnikové nebo zákaznické aplikace na bázi HTTP/HTTPS.



FLOWMON APM INDEX

FlowMon APM zavádí unikátní koncept tzv. APM indexu, který jediným číslem vyjadřuje výkon aplikace z hlediska plnění definovaného SLA. Transakce mimo stanovenou úroveň SLA snižují APM index váženým průměrem, což umožňuje notifikovat nežádoucí stavy aplikace a následně identifikovat problematické části aplikace nebo skupiny uživatelů. Mezi další unikátní vlastnosti patří:

- Statické (předem definované) i dynamické (na základě struktury aplikace) skupiny, pro které je automaticky sledován APM index a všechny ostatní metriky.
- Předdefinovaná sada reportů s možností uživatelské definice, pravidelné zasílání e-mailem.
- Konfigurace v řádu minut s okamžitým monitoringem všech transakcí.

PŘÍNOSY A VÝHODY

- **Zvyšuje spokojenost zákazníků a interních uživatelů**
- **Omezuje odchod zákazníků ke konkurenci**
- **ROI (return of investment) v řádu jednotek měsíců**
- **Sledování a dokládání úrovně kvality služby (SLA)**
- **Eliminuje prostoje zaměstnanců způsobené špatnou funkčností aplikace**
- **Zkracuje dobu, kterou stráví IT oddělení hledáním příčin aplikačních problémů**
- **Umožňuje identifikovat úzká místa aplikace**
- **Základní nástroj pro oddělení problémů na úrovni infrastruktury a aplikace**
- **Okamžitá notifikace zhoršení výkonu aplikace na základě definovaného SLA**
- **Plugin pro řešení FlowMon, jednoduchá instalace a zhodnocení stávajících investic**
- **Transparentní licencování – počet transakcí za minutu, bez omezení počtu aplikací**
- **Distribuovaná architektura a škálovatelnost**

KLÍČOVÉ VLASTNOSTI A SLEDOVANÉ METRIKY

FlowMon APM monitoruje skutečný aplikační provoz, probíhající mezi uživateli a aplikační infrastrukturou. Z kopie tohoto provozu (zapojení TAPem nebo SPAN portem) zachytává jednotlivé pakety, přiděluje jim časové známky, dekóduje a analyzuje jejich obsah. Na základě naměřených dat zobrazuje přehlednou formou metriky:

- Počet transakcí.
- Doba odezvy monitorované aplikace (maximální, průměrná, medián, percentil).
- Počet uživatelů souběžně pracujících s aplikací.
- Doba přenosu dat na transportní vrstvě a jejich velikost.
- Přehled transakcí v jednotlivých úrovních SLA a jejich rozložení v čase.
- Počet výskytu chybových kódů a jejich rozložení v čase.
- Detaily jednotlivých transakcí.

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhneme projekt monitorování Vaší sítě.

www.invea.com

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@invea.com
www.invea.com

7.2.6 Novicom AddNet

AddNet

novicom

Integrovaný **DDI/NAC nástroj**
pro pokročilou správu IP adresního prostoru
a řízení bezpečnosti přístupů v síti

NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER

AddNet je unikátní nástroj pro řádové zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích. Toho je dosaženo integrací výkonného síťového monitoringu, systému IP adresního plánování (IPAM), základních síťových služeb (DHCP, DNS), řízení přístupu do sítě (NAC) a komunikace s aktivními prvky sítě.

AddNet přináší rovněž robustnost, nadstandardní provozní spolehlivost, bezpečnost a flexibilitu nasazení. To všechno mu dávají originální Novicom technologie, jako je vlastní gridová platforma SGP, komunikační protokol SDP nebo systém appliancí FireBox.

Více informací na 2. stránce >

novicom Novicom, s.r.o.
Praha, Česká republika

www.novicom.cz sales@novicom.cz

7.2.7 Novicom AddNet

Výkonný L2 monitoring

Real-time nástroj pro monitorování výskytu zařízení (IP a MAC adres) v síti a to včetně návaznosti na jeho umístění (port switche / fyzická lokalita). Poskytuje rovněž kompletní historii provozu sítě pro následné auditní činnosti.

Kompletní DDI (DHCP/DNS/IPAM)

Přináší distribuované a spolehlivé základní síťové služby (DHCP a DNS) a jejich snadné ovládání díky integrovanému IPAM nástroji. Integrace s L2 monitoringem umožňuje v reálném čase řešit rozpory mezi realitou a IP adresním plánem a mít vždy adresní plán v souladu s realitou.

> IPAM

Systém správy IP adresního prostoru poskytuje přehledné a pohodlné nástroje adresního plánování s integrovaným řízením všech dalších dílčích částí (DHCP/DNS/NAC). V adresním plánování je tak možné velmi jednoduše přidat nové zařízení nebo změnit síťové parametry stávajících zařízení.

> DHCP

Standardní DHCP služby jsou navržené pro práci v rozsáhlých distribuovaných sítích a tam, kde je zapotřebí maximální provozní spolehlivost nebo výkon. Integrace s L2 monitoringem přináší rozšířené funkční možnosti a flexibilitu použití, včetně zavedení přidělování pevných IP adres pomocí DHCP na základě známých MAC adres.

> DNS

Integrované DNS služby přinášejí možnost spolehlivého provozu v distribuovaných sítích. Je možné využít flexibilní možnost AddNetu řídit rovněž stávající DNS infrastrukturu prostřednictvím dynamických DNS updatů. Je tak zajištěna plná konzistence prostředí IPAM, DHCP a DNS.

Integrovaný NAC (řízení přístupu do sítě)

Výhodou integrovaného NAC řešení AddNetu je možnost snadného nasazení v prostředí rozsáhlé distribuované sítě. Je tak možné zajistit NAC funkcionalitu ve vzdálené lokalitě, která nemá dočasně spojení s centrálou.

> 802.1x/MAC autentizace

AddNet nabízí řízení přístupu do sítě prostřednictvím 802.1x s MAC autentizací. Díky integrovanému monitoringu je MAC adresa vyhodnocována ve více parametrech a AddNet dokáže s vysokou mírou pravděpodobnosti upozornit na podvržené MAC adresy. Výhodou je odpadnutí vysoké pracnosti spojené se zavedením a správou plného 802.1x.

> Autorizace

Po provedení autentizace dojde v rámci procesu autorizace k přidělení zařízení do určené sítě (VLAN). Následně je pak daný port switche dynamicky přenastaven jako přístupový pro danou VLAN. Zařízení tak může komunikovat pouze v dané VLAN.

Podpora krizového plánování

V AddNetu je možné definovat krizové sety, prvky kritické infrastruktury organizace. V případě bezpečnostního incidentu je možné pouhým klikem aktivovat krizový set a zajistit okamžité odpojení od sítě všech zařízení, které nejsou v krizovém setu vyjmenovány.

Síťová správa a řízení přístupu pro BYOD a mobilní zařízení

AddNet podporuje rovněž kompletní IP správu ve wi-fi sítích. Model správy DDI/NAC je doplněn o snadnou správu BYOD a mobilních zařízení. AddNet přináší samoobslužnou zónu pro zaměstnance, kde je možné přidávat pohodlně nové zařízení do sítě. Je možné vytvářet rovněž recepční zóny. Výhodou BYOD modulu je podpora všech typů uživatelských zařízení, bez ohledu na operační systém a prostředí zařízení.

Pokročilá komunikace s aktivními prvky

AddNet poskytuje přehledné informace o aktivních prvcích v síti v přehledovém repository. Díky kontinuálnímu sledování up/down stavu portů je AddNet schopen monitorovat port utilizaci a určit porty aktivních prvků, které nejsou využívány. AddNet obsahuje rovněž funkci automatického zálohování konfigurací aktivních prvků.

Přehledový Dashboard

AddNet poskytuje na jednom místě ty nejdůležitější informace o síti a jejím využívání. Z jednotlivých zobrazovaných informací v dashboardu je možný rychlý proklik na detailní informace v dílčích částech AddNetu. Vedle toho se nabízí možnost poskytnutí dodatečných informací o dané IP nebo MAC adrese kdekoli v aplikaci po zmáčknutí pravého tlačítka myši pro rychlé dohledání informací pomocí drilldown.

Výkonný reporting

AddNet nabízí široké množství pohledů na provoz zařízení v síti. Vedle informací z real-time L2 monitoringu a detailních informací z DHCP provozu poskytuje rovněž informace z aktivních prvků. Kombinace různých zdrojů vstupních informací v jednotném uživatelském prostředí přináší rozsáhlé možnosti při získávání detailních informací o zařízení, například při řešení bezpečnostních incidentů.

KLÍČOVÉ PŘÍNOSY AddNetu

- **Zavedení DDI** – významná úspora práce síťových administrátorů
- Standardizace činností síťových správců a možnost centralizace správy rozsáhlých distribuovaných sítí
- Vysoce výkonný L2 monitoring s možností fyzické lokalizace zařízení – díky integraci s kabelovou knihou
- **Zavedení NAC** – řízení bezpečnosti přístupu do sítě s využitím 802.1x/MAC autentizace a autorizace (přiřazování do VLAN)
- **Plně automatizovaná správa BYOD** a mobilních zařízení a jejich jednoznačná identifikace v síti
- Podstatné zvýšení provozní spolehlivosti a výkonu DNS, DHCP, Radius díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** díky dlouhodobému sledování využití aktivních prvků
- **Plná heterogennost** a bezproblémová spolupráce se síťovými technologiemi Microsoft a Cisco
- **Unikátní podpora distribuovaného modelu sítě – garance zajištění provozu L2 monitoringu/DDI/NAC i ve vzdálené lokalitě** v případě ztráty konektivity s centrální lokalitou
- **Flexibilní nasazení** – vhodné pro centralizované i plně distribuované organizace
- **Snadné nasazení** – díky vlastní implementační metodice a výkonnému iniciačnímu sniffingu
- AddNet jako integrální součást konceptu aktivní bezpečnosti sítě přináší připravené integrace na další prvky (např. Flowmon ADS)

8 PODPORA TECHNOLOGIÍ

8.1 Flowmon Gold Support

Obsahuje následující:

- **Záruka Next Business Day** – v případě hardwarového problému budete mít následující pracovní den na místě certifikovaného technika, který jej řeší.
- **Pravidelné aktualizace a upgrady** produktů zdarma.
- **Podpora v českém jazyce** – zahrnuje přístup k webovému zákaznickému centru, podporu na telefonu a e-mailu, vzdálenou podporu přes SSH a konzultace síťového / bezpečnostního technika v režimu 8/5.
- **Zákaznická školení zdarma** – s Flowmon GS mají zaměstnanci vaší firmy účast zdarma.
- **Prodloužená hardwarová záruka** až na 5 let.
- **Zvýhodněný cyklus obnovy hardware** – po 5 letech přestává být výrobci poskytována záruka na HW. Proto Flowmon nabízí bonusový program určený pouze zákazníkům, kteří si se svými produkty pořídili službu Flowmon Gold Support. Po čtyřech letech Flowmon umožňuje pořízení nového kusu s 50% slevou z koncové ceny (v případě zakoupení Gold Support na celé pětileté období).
- **Flowmon Threat Intelligence pro Flowmon ADS** – Máte nasazen produkt Flowmon ADS? S programem Flowmon Gold Support získáváte navíc stále aktuální reputační databáze pro přesnější detekci infikovaných stanic nebo odhalení komunikace s botnet command & control centry. Flowmon Threat Intelligence také umožňuje aktualizaci vzorů chování detekčních metod, díky čemuž detekujete nejnovější hrozby, jako například zranitelnosti nultého dne a další.

8.2 Podpora Novicomu- AddNet

Obsahuje následující:

- **Službu produktového update** – poskytování bezplatných nových verzí Novicom software
- **Službu poskytování prodloužené záruky** na Novicom softwarové produkty (po dobu placení podpory)
- **Službu helpdesk** – telefonická podpora v pracovní době 9-17 a elektronická podpora 24x7 - příjem požadavků na technickou pomoc (hlášení vad)
- **Základní úroveň SLA podpory** – garantovaný response-time 8 pracovních hodin na zahájení řešení problémů
- **Službu systémového update** – poskytování nových verzí a bezpečnostních update pro hw appliance

8.3 Technická podpora Huatech

Společnost Huatech a.s. poskytuje k dodaným a servisovaným technologickým řešením a poskytovaným ICT službám komplexní technickou podporu. Technická podpora je dostupná registrovaným a autorizovaným uživatelům zákazníků a je poskytována prostřednictvím následujících komunikačních rozhraní.

- Web based helpdesk: support.huatech.cz (dostupnost 24x7)
- Telefonická podpora: Bílá linka 840 11 22 33
- E-mailová podpora: support@huatech.cz

Parametry pro dostupnost jednotlivých komunikačních rozhraní technické podpory jsou dány uzavřenou servisní smlouvou.