

MyNetScope® je špičkovou českou technologií pro monitorování a analýzu k zajištění bezpečnosti počítačové sítě. MyNetScope® je výsledkem úspěšného inovačního procesu včetně transferu technologií, na kterém se podílela přední vědecko-výzkumná pracoviště (např. sdružení CESNET) ve spolupráci s komerčními subjekty.

Implementací MyNetScope® zákazník zvýší bezpečnost datové sítě, sníží provozní náklady ICT infrastruktury a její obsluhu a získá permanentní dohled nad kvalitou služeb od svých dodavatelů.

MyNetScope® shromažďuje na jediné univerzální platformě důležité provozní informace o zařízeních, aplikacích a službách v síti bez ohledu na jejich původ. Tato vlastnost je založena na technologii NetFlow – průmyslovém standardu pro měření datových toků v síti (viz <http://cs.wikipedia.org/wiki/Netflow>).

Konkurenční výhodou MyNetScope® je vynikající poměr cena/výkon, technologie sběru provozních dat, podrobnější a přesnější informace o síti, rozšiřitelnost, možnost efektivního doplnění detekčních metod bezpečnostních incidentů relevantních pro danou počítačovou síť nebo propojení na specifické datové zdroje v organizaci. Díky těmto vlastnostem MyNetScope® chrání stávající i budoucí ICT investice zákazníka.

Řešení MyNetScope® podporuje síť všech velikostí (od 10Mbps do 10 Gbps) a je připraveno na zvýšení zátěže sítě i počtu monitorovaných míst. Monitoring sítě je navíc z pohledu monitorované sítě zcela transparentní (neviditelný).

Dodávka řešení MyNetScope® zahrnuje monitorování sítě z bezpečnostního a provozního hlediska, dlouhodobé uložení statistik o provozu na síti, centrální zpracování statistik, nástroje pro analýzu chování sítě a zařízení v síti, nástroje pro dohled nad provozní infrastrukturou a administrativně-organizační prostředí pro dokumentaci infrastruktury a efektivní práci IT týmu.

Typická implementace řešení MyNetScope® vyžaduje v iniciační fázi projektu udělení mandátu dodavateli vrcholovým managementem zákazníka k provedení před-implementační analýzy anebo auditu sítě. Na základě zjištění prezentovaných dodavatelem jsou vyzvány příslušné odborné útvary k oponentuře výsledků a odsouhlasení plánu pro implementaci řešení MyNetScope®, případně plánu úprav stávajících vztahů s dodavateli ICT infrastruktury. Po dohodě se zákazníkem je ustanoven projektový manažer zodpovědný za dodávku a konfiguraci řešení MyNetScope®, včetně implementace prostředí pro dokumentaci infrastruktury, sdílení metodik a pracovních postupů a řešení bezpečnostních incidentů. V

závěrečné fázi projektu zákazník nominuje tým, který bude zajišťovat obsluhu řešení a dodavatel provede školení.

### Konkrétní přínosy řešení MyNetScope®

#### 1. Analýza chování sítě a zařízení v síti

Na základě dlouhodobých statistik o provozu na síti poskytuje řešení MyNetScope® statistiky objemů provozu na jednotlivých linkách, vytížení serverů, profily typického chování zařízení v síti nebo přehled o aktivních aplikacích v síti. Tyto informace je možné použít pro sestavení mapy využití sítě a serverů, kontrolu dodržování SLA nebo optimalizaci síťové infrastruktury a snížení nákladů. Klíčové přínosy:

- Kontrola dohod o kvalitě služeb (SLA) a uplatnění nároků za jejich neplnění.
- Optimalizace síťové infrastruktury a aplikací v síti, zvýšení kvality služeb, snížení provozních nákladů.

Client/Server behavior

#	Client (%)	Server (%)	Unclassified (%)
1	48.84	23.38	27.78

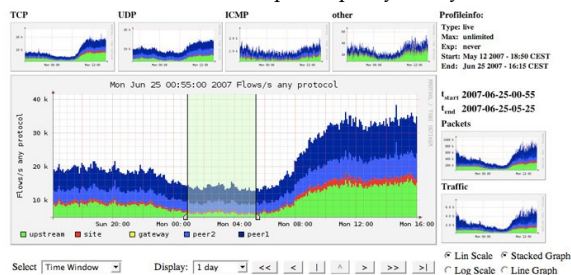
Traffic structure

#	General device role	Flow pair kind	Port	Protocol	Transferred (B)	Packets	Flows
1	unclassified	single flow	25	TCP	959,254	1,404	81
2	client	request	25	TCP	182,232	639	45
3	client	reply	25	TCP	64,044	522	45

#### 2. Dohled nad rutinním provozem sítě

Řešení MyNetScope® monitoruje počítačovou síť v reálném čase a je schopné upozornit na potenciální problémy v provozní infrastruktuře dříve, než skutečně vzniknou. Kombinace moderní metody měření datových toků v síti a klasického dohledu na bázi SNMP představuje nejrobustnější způsob monitorování provozní infrastruktury. Klíčové přínosy:

- On-line přehled o stavu celé provozní infrastruktury v jediné aplikaci umožňuje správci sítě rychlé odhalení aktuálních či potenciálních problémů, a tak minimalizuje eskalování problémů.
- Upozorňování na potenciální problémy v reálném čase, např. nadměrná zátěž serveru, nedostupnost služby, zdroj nežádoucího provozu, apod.
- Předcházení nespokojenosti uživatelům a souvisejícím nákladům s nedostupností poskytovaných IT služeb.



### 3. Prostředí pro spolupráci a dokumentaci

Součástí řešení MyNetScope® je komfortní prostředí pro dokumentaci infrastruktury, vedení bezpečnostní dokumentace a řešení bezpečnostních incidentů. Zajištění bezpečnosti a spolehlivosti je dlouhodobý proces, proto součástí řešení MyNetScope® ve větších organizacích může být rovněž vybudování bezpečnostního týmu a zavedení metodik a ověřených pracovních postupů bezpečnostních týmů. Samozřejmostí jsou následné konzultace v oblasti bezpečnosti. Klíčové přínosy:

- Součástí řešení jsou moderní metody a v praxi ověřené postupy, které je možné při řešení bezpečnostních incidentů rovnou aplikovat.
- Přípravenost na certifikaci oficiálního bezpečnostního týmu organizace. Certifikace organizací Trusted Introducer zaručuje zvýšení důvěryhodnosti vůči ostatním sítím a obchodním partnerům.

### 4. Dohled nad využíváním sítě zaměstnanci

Řešení MyNetScope® umožňuje dohled nad činností správců sítě a počítačových systémů, jejichž činnost běžně bezpečnostnímu auditu nepodléhá. Dle nezávislých průzkumů tráví zaměstnanci až 20% času zábavou. Řešení MyNetScope® je schopné upozornit na využívání nežádoucích služeb (např. sdílení dat, on-line hry, instant messaging) nebo nadměrné datové přenosy. Klíčové přínosy:

- Zvýšení produktivity práce díky eliminaci nepracovních aktivit.
- Dohledem nad správci IT infrastruktury.
- Zvýšení bezpečnosti firemních dat

Events

#	Event source	Type	Details	Timestamp	Data source	Event targets
1	31.169	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 14:29:38	PIF	200.2
2	67.229	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 14:01:22	PIF	49.10
3	67.229	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 12:59:52	PIF	52.194
4	35.9	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 11:25:05	PIF	169.135
5	5.166	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 10:24:39	PIF	52.199
6	67.206	BITTORRENT	Bittorrent downloads, unique sources: 1	2009-09-18 09:57:16	PIF	121.243

### 5. Detekce a prevence anomálií

Anomáliemi souhrnně označujeme výjimečné, typicky nežádoucí, stavy v síti. Mezi anomálie zahrnujeme rovněž cílené útoky nebo šíření počítačových virů nebo červů. Řešení MyNetScope® disponuje pokročilými prostředky pro odhalování a prevenci anomálií. Nabízí jak automatické budování profilů chování zařízení na síti, tak i odhalování explicitně definovaných nežádoucích vzorů chování. Klíčové přínosy:

- Včasné odhalení výskytu nežádoucích vzorů chování v síti, např. využívání nežádoucích služeb nebo rozpoznání útoku.
- Včasné rozpoznání změny v chování zařízení na síti, upozornění a reakce dříve, než změna v chování způsobí skutečné problémy spojené s náklady nebo poškozením pověsti organizace.

SSH Attacks

Successful attacks in result: 0  
Non-successful attacks in result: 11

#	Timestamp	Attacker	Victim	Attack status	Certainty (%)
1	2009-09-16 20:07:37	144.16.112.114	65.2	non-success	100.00
2	2009-09-16 20:07:32	144.16.112.114	65.55	non-success	100.00
3	2009-09-16 20:06:37	144.16.112.114	90.252	non-success	100.00
4	2009-09-16 20:06:12	144.16.112.114	57.136	non-success	100.00
5	2009-09-16 20:06:53	144.16.112.114	57.230	non-success	100.00
6	2009-09-16 19:54:08	144.16.112.114	31.135	non-success	100.00
7	2009-09-16 19:53:31	144.16.112.114	27.143	non-success	100.00
8	2009-09-16 19:53:01	144.16.112.114	27.199	non-success	100.00
9	2009-09-16 19:52:53	144.16.112.114	27.177	non-success	100.00
10	2009-09-16 19:52:51	144.16.112.114	27.189	non-success	100.00
11	2009-09-16 19:52:22	144.16.112.114	24.201	non-success	100.00

### 6. Monitoring služeb v síti

MyNetScope® disponuje prostředky pro odhalování serverů a klientů v síti a rozpoznávání nových/nežádoucích služeb v počítačových sítích. Pro jednotlivá zařízení v síti nabízí strukturované profily chování obsahující informace o rolích zařízení v síti, využívaných a poskytovatelských službách a komunikačních partnerech. Formou pravidelného reportingu je možné získávat přehled o serverech a klientech v síti, dostupných službách a míře jejich využívání. Klíčové přínosy:

- Snížení provozních a investičních nákladů sítě optimalizací poskytování a využívání služeb v síti na základě znalosti aktuálního stavu.
- Zvýšení celkové bezpečnosti sítě vyplývající se ze znalosti chování klíčových serverů v síti a struktury poskytovaných/využívaných služeb.

### Audit sítě

Řešení MyNetScope® je možné využít rovněž pro jednorázový audit síťové infrastruktury a inventuru síťového provozu. Prostřednictvím našeho auditu zjistíte skutečné parametry vaší infrastruktury i způsob jejího využití. Klíčové přínosy:

- Kontrola dodržování SLA ze strany dodavatelů a partnerů.
- Získání podkladů jako je vytížení linek nebo serverů využitelných pro optimalizaci ICT infrastruktury.

### Kontaktujte nás

Rádi Vám připravíme nabídku řešení MyNetScope® na míru vašim potřebám, navrhne projekt auditu sítě nebo zodpovíme jakékoli dotazy.

## Přehled vlastností řešení MyNetScope<sup>®</sup>

### Monitorování toků v síti

- Vysoce výkonné autonomní řešení NetFlow v5/v9 monitoringu v reálném čase
- Podpora linek od 10Mbps do 10Gbps
- Podpora pro IPv4, IPv6, VLAN a MPLS
- Neviditelné na L2 a L3 vrstvě
- Poskytuje primární data pro další aplikace:
  - Analýza síťového provozu
  - Sledování uživatelů a služeb
  - Dohled nad přístupem k Internetu
  - Plánování kapacity sítě a datových linek
  - Kontroly peeringu a SLA
  - Dodržování zákona o elektronických komunikacích a souvisejících předpisů
  - Detekce nežádoucích vzorů chování
  - Detekce anomálií
  - Průzkum bezpečnostních incidentů

### Centrální uložení statistik o provozu na síti

- Vysoce výkonný kolektor pro sběr NetFlow statistik z libovolného počtu monitorovaných bodů v síti
- Dostupná kapacita od 1TB do 50TB
- Centrální databáze pro dlouhodobé uchování statistik o provozu na síti
- Platforma pro analýzu a další vyhodnocování statistik
- Platforma pro dohled nad dostupností a výkonností síťových prostředků

### Centrální vyhodnocování statistik o provozu na síti

- Implementace standardu Bidirectional Flows
- Předdefinovaná sada nežádoucích vzorů chování
- Předdefinovaná sada pravidel detekce anomálií
- Připraveno na rozšíření o další vzory nežádoucího chování a pravidla detekce anomálií
- Zvýšení bezpečnosti sítě a možnost odhalení vnějších i vnitřních útoků
- Detekce slovníkových útoků
- Budování dlouhodobých profilů chování zařízení
- Odhalování skrytých/nežádoucích služeb v síti
- Klasifikace bezpečnostních incidentů dle druhů a závažnosti
- Historie bezpečnostních incidentů

### Behaviorální analýza

- Vysoce výkonná analýza chování v reálném čase:

- uživatelů
- síťových zařízení
- jednotlivých aplikací
- sítě jako celku

- Detekce nežádoucích vzorů chování
- Monitorování aktivit uživatelů a využívání služeb
- Korelace událostí na úrovni sítě s aplikačními logy

### Dohled nad provozem na síti a prvky síťové infrastruktury

- Přehled o dění v síti v reálném čase
- Monitoring provozního stavu síťových prvků (SNMP)
- Pravidelný a souhrnný reporting
- Analýza dlouhodobých statistik s rozlišením na jednotlivé počítače a uživatele, aplikace a konverzace

### Pokročilá analýza provozu na síti

- Automatická integrace s DNS s inteligentní cache
- Filtrování dle různých kritérií
- Překlad čísel portů na názvy odpovídajících služeb. Doplňkové informace o službách, informace o známých hrozbách.
- Integrace nástrojů síťové diagnostiky (ping, tracer, nmap) a dalších informací (WHOIS)
- Průzkum bezpečnostních incidentů
- Rychlé a přesné řešení problémů na síti
- Detailní průzkum chování vybraného zařízení nebo uživatele na síti
- Pohled na celkovou situaci na síti

### Administrativně-organizační zázemí bezpečnostního týmu

- Ukládání textů ve standardu dokuwiki
- Přístup ke změnám ve formátu RSS
- Ticketovací systém, automatický mailing změn
- Centralizace bezpečnostního know-how v organizaci
- Evidence bezpečnostních incidentů/úkolů
- Sledování postupu řešení bezpečnostních incidentů
- Metodiky a pracovní postupy bezpečnostních týmů

### Technická podpora a aktualizace SW

- Telefonická a e-mailová podpora 8x5
- Vzdálená asistence a konfigurace zařízení
- Bezpečnostní konzultace
- Aktualizace software a firmware zařízení
- Nové vzory chování/aktualizace vzorů chování

