



AFCEA Konference Kybernetická
bezpečnost KB12

Jak snadno zavést a řídit segmentaci sítí

Jindřich Šavel

CEO

24.9. 2024

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

S čím se setkáváme u zákazníků

Prostředí a legislativa

- V souvislosti s vnímáním legislativních změn na úrovni NIS-2 se začínají podrobněji diskutovat dílčí oblasti kyberbezpečnosti v organizacích
- Nová legislativa významněji poukazuje i na jiné oblasti kyberbezpečnosti než jsou dnes běžně aplikované
 - ochrana perimetru, ochrana klientů, kryptování, zálohování a obnova apod.



S čím se setkáváme v sítích zákazníků

Technologie

- Jsou implementované ochrany na úrovni perimetrů (FW), klientů (EDR) a částečně v oblasti monitoringu infrastruktury a sítí (NDR)

Lidské zdroje

- Zásadní problém – většina organizací nemá dedikované zdroje pro kyberbezpečnosti
- Organizace má často svého guru síťáře, před kterým chodí šéf po špičkách...
 - těžko se prosazují změny, chybí dokumentace a zastupitelnost
 - provádění reakcí při kybernetických útocích je na nich osobně závislá

Procesy

- Začínají se vylepšovat procesy v oblasti detekce, pokulhávají v oblasti investigace a reakce
- Nutno akceptovat stav, kdy zásadní výkon kyberbezpečnosti bude outsourcován
 - **SOC – Security operation center**

Oblast správy sítí

- **Převládá provozní pohled**

- IT je odměňováno za rychlý a spolehlivý provoz
- nejsou chváleni za překážky, které přináší bezpečnost

- **Bezpečnost pokulhává – často shledáme**

- není L2 monitoring, který ověřuje výskyt zařízení v síti
- DHCP jsou často nastavené genericky - bez rezervací
- DNS provozovány bez filtrování provozu
- často chybí řízení přístupu do sítí - NAC
- pokročilé síťové politiky jsou aplikovány výjimečně

- **Není návaznost na další oblasti**

- CDB
- monitoring
- reakční nástroje



Jedna oblast v detailu – segmentace sítí

- Zavedení segmentace je velmi různorodé
- Setkáváme se dvěma extrémy:
- *Bez segmentace – plochá síť*
 - **Problémy bezpečnosti**
 - velmi rychlé šíření škodlivého kódu
 - možnost nežádoucího monitoringu sítě
 - **Problémy výkonnosti**
 - degradace výkonu díky vysokému množství zařízení v síti

- **Segmentované sítě**

- **Intenzivní**

- VLAN jsou nastavené nejenom podle logického členění organizace a technologií, ale i podle lokalit
- V důsledku stovky VLAN s komplikovanou správou

- **Natvrdo nastavené**

- Na switchích jsou nastavené porty natvrdo, kdy se předpokládá že dané zařízení má přístup do konkrétní VLAN
- Bývá často kombinované s přístupem přes MAC adresu

- **Problém síťové správy**

- Vysoká pracnost pro realizaci změn v síti – často ruční konfigurace switchů
- Nedostatečná dokumentace stavu po změnách

Jak zavést rychle segmentaci?

- **S využitím nástroje pro řízení přístupu do sítě – NAC**
- **Lépe s využitím integrovaného DDI/NAC řešení**
 - DDI (DNS, DHCP, IPAM), včetně kontinuálního L2 monitoringu
 - NAC – Autentizace a Autorizace síťových zařízení
- **Předání vstupních informací o stavu sítě**
 - Potřebných pro nastavení NAC řešení
 - Je k dispozici aktuální síťová dokumentace
- **Alternativní zjištění stavu sítě s využitím služby Novicom NADS**
 - Ověření stavu síťového prostředí a připravenosti na zavedení NAC
 - Ověření zavedení a organizace stávajících VLAN
 - **Vytvoření dokumentace o stavu síťové infrastruktury a stavu síťových služeb**
- **Nastavení DDI/NAC řešení**
 - Ověření stavu sítě (sniffing)
- **Nastavení switchů**
 - Vyčítání switchů pro L2 monitoring, případně nezávislé zálohování
 - Nastavení komunikace s NAC infrastrukturou
- **Přístupové politiky**
 - Zvolení optimálního módu pro autentizaci
- **MAC based s ochranou**
 - Funguje pro všechny zařízení
- **Full 802.1x**
 - Flexibilní možnosti
- **Integrace s prostředím MS Active Directory**
- **Kombinovaný model**
 - **Co je v doméně** (a podporuje suplikanty), ověřuje se s využitím informací z prostředí MS AD
 - **Co není v doméně**, ověřuje se s využitím informací z interní databáze ADDNETu

Dynamické softwarové řízení síťových služeb



NAC

DDI

BYOD

Integrace

**Dashboard
& reporting**

**Pokročilé
síťové
politiky**

DACL

**Alert
Centrum**

**L2
monitoring**

**Switch
Interoperability**

**Síťová
viditelnost**

**Aktivní
SOC**

Když chybí dokumentace...

- **Potřeba instalace ADDNET**
 - Jaké jsou switche, VLAN, Fyzická topologie, ...
- **Vyplnění implementačních tabulek pro nastavení...**
 - Není čas
 - To ví Arnošt.
 - Arnošt už tu 2 roky nepracuje
- **OK. Tak si dokumentaci si vyrobíme sami**
- **Cílem služby**
 - je poskytnout znalosti v oblasti síťového konzultingu, které výrazně zvýší provozní spolehlivost a bezpečnost sítě
 - Vytvoření aktuální dokumentace o stavu sítě
 - síťový HW, jeho konfigurace a síťové služby
- **Komu určeno je určen služba NADS?**
 - Zákazníkům, kteří nemají specifické dovednosti nebo čas



Network Assessment and Documentation Service

- **NADS – Cílem služby je**
 - neinvazivním způsobem zmapovat stav síťové infrastruktury
 - poskytnout základní dokumentaci síťové infrastruktury, základních síťových služeb
 - a poskytnout vrcholový návrh na zlepšení zjištěného stavu
- **Služba je koncipována na 3 až 6 týdnů, podle velikosti organizace**
- **Zahrnuje následující základní činnosti**
 - Vstupní workshop
 - Instalace analytických nástrojů
 - Scan sítě
 - Vyhodnocení scanu
- **Příprava hodnotící zprávy**
 - Network devices list
 - Low level design
 - Top anomaly
 - Top performance issues
 - Top security issues
 - NAC readiness / top issues
 - Segmentation (VLAN)
 - Advanced network policies (DAACL)
 - Core net services (DHCP/DNS)
 - IPAM
 - Monitoring (IP, L2, DHCP, netflow/ipfix, syslog)
- **Prezentace pro management (Workshop)**
- **Následný 14-ti denní provoz analytických nástrojů**
- **Závěrečný workshop**

Shrnutí přínosů služby NADS

- Služba se zaměřuje na dosažení rychlých výsledků za pevně danou cenu
- Vytváří objektivní pohled na síť a síťovou infrastrukturu
- Vytváří/aktualizuje dokumentaci sítě
- Přináší nezávislý pohled a vrcholová doporučení pro další rozvoj sítě
- Služba je nezávislá na výrobcích síťové infrastruktury



Pokročilé síťové politiky

- **Pokročilý NAC je možné využít i pro nastavení pokročilých síťových politik**
- **Cílem je zásadní omezení nevhodné komunikace v síti**
- **Modelový stav - Příklad účetní**
 - Povolená komunikace: SAP, intranet, internet, pošta
 - Ostatní komunikace: zakázaná (zahození paketů)
- **Jak realizováno**
 - Pomocí DACL generátoru
 - Alternativně pomocí řízení relací na nahrané ACL ve switchích

- **Ukázka nastavení**

- Dashboard
- ACL nastavení
- Switche - heterogenita
- DACL nastavení
- Jednotlivé pravidla
- Editace DACL

- **Přínosy pokročilých síťových politik**

- **Dynamické řízení komunikačních politik v rámci jednotlivých VLAN**
- De-facto z běžných switchů se stávají **distribuované firewally** a je ochráněná lokální komunikace bez nutnosti zavádění/zatěžování centrálních firewallů
- **Je aplikováno automaticky** v rámci zařazení zařízení/uživatele v organizaci
- **Zásadně omezí šíření škodlivého kódu** (např. nemožnost použít RDP mezi zařízení kolegů v jedné VLAN) – co není povoleno je zakázáno



1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

Začít editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MSAD Radius DNS Switche DHCP Adresní plánování Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

Konfigurace dashboardu

Top 24 sítě podle využití IP [%]

Zobrazit vše



Jméno sítě	DHCP	MAC/24h	Využití IP v %
Quarantine_Bonn-10.201.27.192/26	0	0	48.4%
Quarantine_Dublin-10.201.27.128/26	0	0	48.4%
Print_Dublin-10.201.15.128/27	1	9	36.3%
Print_Bonn-10.201.15.192/27	1	6	26.3%
PrivPC_A-10.201.7.0/24	1	40	23.6%
PC_Dublin-10.201.8.0/23	1	58	16.5%
PC_Bonn-10.201.12.0/23	1	58	16.5%

Rychlé hledání



IP adresa IP adresa MAC Hledat

☆ Oblíbené



Servery DHCP klienti Sítě DHCP události DNS servery Switche Pravidla Dílčí monitor Monitor Radius uživatelé IP

Top 11 nejvytíženějších switčů

Zobrazit vše



Jméno switče	Porty využité po celou dobu posledních 7 dní
A1-C3560X-48-1	78.7%
Dublin1-C3560X-24-1	60.6%
Bonn1-C3560X-24-1	54.5%
A2-C2960G-24-2	12%
A2-C2960G-24-1	12%

Posledních 100 událostí Alert centra za posledních 7 dní

Zobrazit vše



Jméno	Modul	Závažnost	Čas
Test modul	Test input module	Nizká	24.09.2024 02:13:15
New device	New device input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15

Top 14 sítě s nejvíce požadavky Discover za posledních 7 dní

Zobrazit vše



Celkem požadavků: 54046, Unikátních požadavků: 253

Jméno sítě	Discover / Unikátní Discover
PC_A-10.201.0.0/22	17042
PC_Bonn-10.201.12.0/23	12328
PC_Dublin-10.201.8.0/23	11376
PC_A-10.201.0.0/22	79
PC_Bonn-10.201.12.0/23	56
PC_Dublin-10.201.8.0/23	53

Top 5 sítě s neznámými zařízeními



Jméno sítě	Počet nových zařízení
MNG_A-10.201.16.0/24	5
PC_A-10.201.0.0/22	1
PrivPC_A-10.201.7.0/24	1
Guest_A-10.201.24.0/24	1
Guest_Bonn-10.201.26.0/24	1

Top 14 sítě s nejvíce požadavky Request za posledních 7 dní

Zobrazit vše



Top 1 síť se zařízeními v rozporu s pravidly



1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

Začít editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Přístup Protokol Uživatelský radius **DACL** Přihlašovací čas Alert centrum Kabelová kniha

DACL / Typové skupiny switchů

Hledat...

Hledat



Stav záznamů:

Editované

Zobrazeny záznamy 1 - 5 z 5

50 na stránku



#	Název	Typ generátoru	Směr OUT	Filter SRC	Rozsah portů	Multi port	IPv6	Podpora IPv6 zakázáno	
1	Cisco	Cisco	Ne	Ne	Ano	Ne	Ne	Ne	Detail
2	Cisco-inverted-mask	CiscoInv	Ne	Ne	Ano	Ne	Ne	Ne	Detail
3	HPE	HPE	Ne	Ne	Ano	Ano	Ano	Ano	Detail
4	Huawei	Huawei	Ne	Ne	Ne	Ne	Ne	Ne	Detail
5	Standard	Standard	Ne	Ne	Ano	Ano	Ne	Ne	Detail

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

Začít editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

DACL / Typové skupiny switchů / Detail skupiny

ID	2	
Název	Cisco	
Typ generátoru	Cisco	
Směr OUT	Ne	
Filter SRC	Ne	
Rozsah portů	Ano	
Multi port	Ne	
IPv6	Ne	
Podpora IPv6 zakázáno	Ne	
Atribut IPv6 zakázáno		
Protokoly	icmp ip tcp udp	
RAD atributy	Filter-Id Port-Limit Cisco-AVPair	
ICMP zprávy	IPv4 Communication Administratively Prohibited Communication with Destination Host is Administratively Prohibited Communication with Destination Network is Administratively Prohibited Destination Host Unknown Destination Host Unreachable for Type of Service Destination Network Unknown Destination Network Unreachable for Type of Service Destination unreachable (all) Echo reply Echo request Fragmentation Needed Host Precedence Violation Host Unreachable ICMP redirects (all) Net Unreachable Port Unreachable Precedence cutoff in effect Protocol Unreachable Redirect Datagram for the Host Redirect Datagram for the Network (or subnet) Redirect Datagram for the Type of Service and Host Redirect Datagram for the Type of Service and Network Source Host Isolated Source Route Failed	

1. Nastavení pokročilých politik

- Typové skupiny switchů
- Typy šablon
- DAACL šablony**
- ACL

DAACL / DAACL šablony

+ Nová DAACL šablona Přidat ke skupině switchů ?

Hledat... Hledat ? Typ šablony: -- Vše -- Stav záznamů: Editované

Zobrazeny záznamy 1 - 12 z 12 50 na stránku < 1 >

#	Jméno	Guest síť	IPv6 zakázáno	Typová skupina switchů	Typ šablony	Počet pravidel	
1	Guest-Cisco	Ano	Ne	Cisco	GUEST	6 Editovat	Editovat Kopie
2	Guest-HPE	Ano	Ne	HPE	GUEST	6 Editovat	Smazat Editovat Kopie
3	Guest-Huawei	Ano	Ne	Huawei	GUEST	6 Editovat	Smazat Editovat Kopie
4	Quarantine-Cisco	Ne	Ne	Cisco	Quarantine	4 Editovat	Editovat Kopie
5	Quarantine-HPE	Ne	Ne	HPE	Quarantine	4 Editovat	Editovat Kopie
6	Quarantine-Huawei	Ne	Ne	Huawei	Quarantine	4 Editovat	Editovat Kopie
7	Server-Cisco	Ne	Ne	Cisco	Server-all-accept	1 Editovat	Editovat Kopie
8	Server-HPE	Ne	Ne	HPE	Server-all-accept	1 Editovat	Editovat Kopie
9	Server-Huawei	Ne	Ne	Huawei	Server-all-accept	1 Editovat	Editovat Kopie
10	User-Cisco	Ne	Ne	Cisco	USER	14 Editovat	Editovat Kopie
11	User-HPE	Ne	Ne	HPE	USER	13 Editovat	Editovat Kopie
12	User-Huawei	Ne	Ne	Huawei	USER	13 Editovat	Editovat Kopie

Zobrazeny záznamy 1 - 12 z 12 50 na stránku < 1 >

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

[Přestat editovat](#)

[jindra@10.201.16.120](#)



[Různé](#) [Topologie](#) [DHCP Volby](#) [MS AD](#) [Radius](#) [DNS](#) [Switche](#) [DHCP](#) [Adresní plánování](#) [Importy](#) [Přístup](#) [Protokol](#) [Uživatelský radius](#) [DACL](#) [Přihlašovací čas](#) [Alert centrum](#) [Kabelová kniha](#)

DACL / DACL šablony / Změna šablony

Pro šablonu jsou již definována pravidla. Lze editovat pouze pole, která nemají vliv nastavení pravidel.

Jméno

Guest síť

IPv6 zakázáno [?](#)

Typová skupina switchů

Typ šablony

[Uložit](#)

[Uložit a zpět](#)

[Uložit jako nový](#)

[Zpět](#)

Pravidla zobrazit raw formát

[Editovat pravidla](#)

[Export do CSV](#)

#	RAD atribut	Typ	Směr	Protokol	Zdrojová IP/sít'	Port	Cílová IP/sít'	Port	ICMP zpráva	Vlastní hodnota
1	Cisco-AVPair	Deny	IN	TCP			any	445	NULL	
2	Cisco-AVPair	Deny	IN	TCP			any	139	NULL	
3	Cisco-AVPair	Deny	IN	TCP			any	3389	NULL	
4	Cisco-AVPair	Deny	IN	UDP			any	137	NULL	
5	Cisco-AVPair	Deny	IN	UDP			any	138	NULL	
6	Cisco-AVPair	Permit	IN	IP			any		NULL	

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Nezvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

Přestat editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

DACL / DACL šablony / Změna šablony / Změna pravidel

DACL šablona - **Guest-Cisco**

Jméno	Guest-Cisco
Guest síť	Ano
IPv6 zakázáno	Ne
Typová skupina switchů	Cisco
Typ šablony	GUEST

Pravidla (6/32 možných)

	RAD atribut	Typ	Směr	Protokol	Zdrojová IP/síť a port	Cílová IP/síť a port	ICMP zpráva	
↑↓ □	Cisco-AVPair	Deny	IN	tcp	Zdrojová IP/síť Port	any 445	---	🗑️
↑↓ □	Cisco-AVPair	Deny	IN	tcp	Zdrojová IP/síť Port	any 139	---	🗑️
↑↓ □	Cisco-AVPair	Deny	IN	tcp	Zdrojová IP/síť Port	any 3389	---	🗑️
↑↓ □	Cisco-AVPair	Deny	IN	udp	Zdrojová IP/síť Port	any 137	---	🗑️
↑↓ □	Cisco-AVPair	Deny	IN	udp	Zdrojová IP/síť Port	any 138	---	🗑️
↑↓ □	Cisco-AVPair	Permit	IN	ip	Zdrojová IP/síť Port	any Port	---	🗑️

+ Přidat pravidlo

Uložit

Uložit a zpět

Zpět

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

Přestat editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius **DACL** Přihlašovací čas Alert centrum Kabelová kniha

DACL / ACL

+ Nový ACL

Hledat...

Hledat



Stav záznamů:

Editované

Zobrazeny záznamy 1 - 3 z 3

50

na stránku

< 1 >

#	Jméno	Počet šablon	Přiřazené sítě	Přiřazené IP adresy	
1	QURANTINE	3	3	0	Editovat
2	SERVER	3	0	68	Editovat
3	USER	3	6	0	Editovat

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

Přestat editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

DACL / ACL / Změna ACL

Jméno

DACL šablony

Vybrané šablony ?

- Quarantine-Cisco
- Quarantine-Huawei
- Quarantine-HPE



Dostupné šablony

- Guest-Cisco
- Guest-HPE
- Guest-Huawei
- Server-Cisco
- Server-HPE
- Server-Huawei
- User-Cisco

Sítě Přřazené k tomuto ACL

Quarantine_Bonn-10.201.27.192/26
Quarantine_Dublin-10.201.27.128/26
Quarantine_A-10.201.27.0/25



Dostupné

Byod A-10.201.28.0/23
Byod Bonn-10.201.31.0/24
Byod Dublin-10.201.30.0/24
Demo-10.201.0.0/19
Guest_A-10.201.24.0/24
Guest_Bonn-10.201.26.0/24

Dostupné kolekce

IP adresy Přřazené k tomuto ACL



Dostupné

10.201.0.1 (Přřazena k: SERVER)
10.201.0.2 (Přřazena k: SERVER)
10.201.0.24 (Přřazena k: SERVER)
10.201.0.25 (Přřazena k: SERVER)
10.201.0.26 (Přřazena k: SERVER)
10.201.0.27 (Přřazena k: SERVER)

Uložit

Uložit a zpět

Uložit jako nový

Zpět

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Nezvoleno - v

Profil: -- Všechny povolené sítě -- v

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

Přestat editovat

jindra@10.201.16.120 v



Různé Topologie DHCP Volby MS AD Radius DNS Switche DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

Sítě: Demo-10.201.0.0/19

10.201.0.0/19 (10.201.0.0-10.201.31.255)

Demo office A

Vlastních podsítí: 21,

Všech podsítí: 21

Počet bloků: 0

Počet IP: 0 / 8190 (4.7%)

Vlastních pravidel: 0,

Všech pravidel: 386

Sítě - Výpis

Vypsáné záznamy: 1-21/21

Na stránku: 50 v

Strana: 1 / 1

Fulltextové hledání

Hledat

Strana: 1 (1 - 1) Zobrazit

Editovaný stav v

Navigace v sítích: Kořen - Demo-10.201.0.0/19

#	JMÉNO	PODSÍŤ	IP/MASKA	POPIS	POČET BLOKŮ	POČET DEF. IP	NADŘAŽENÁ SÍŤ	VOLBY	VLAN	BYOD	ACL	ŠABLONA PŘIHLAŠOVACÍHO ČASU			
1.	Byod A-10.201.28.0/23	10.201.28.0 / 23		BYOD net A	0	0	Demo-10.201.0.0/19	Byod A-10.201.28.0/23 + 0 voleb	2021	Ano					
2.	Byod Bonn-10.201.31.0/24	10.201.31.0 / 24		BYOD net Bonn	0	0	Demo-10.201.0.0/19	Byod Bonn-10.201.31.0/24 + 0 voleb	2023	Ano					
3.	Byod Dublin-10.201.30.0/24	10.201.30.0 / 24		BYOD net Dublin	0	0	Demo-10.201.0.0/19	Byod Dublin-10.201.30.0/24 + 0 voleb	2022	Ano					
4.	Guest A-10.201.24.0/24	10.201.24.0 / 24		Guest building A	1 (1 dynamický)	0	Demo-10.201.0.0/19	Guest_A-10.201.24.0/24 + 0 voleb	2011	Ne					
5.	Guest Bonn-10.201.26.0/24	10.201.26.0 / 24		Guest branch office Bonn	1 (1 dynamický)	0	Demo-10.201.0.0/19	Guest_Bonn-10.201.26.0/24 + 0 voleb	2013	Ne					
6.	Guest Dublin-10.201.25.0/24	10.201.25.0 / 24		Guest branch office Dublin	1 (1 dynamický)	0	Demo-10.201.0.0/19	Guest_Dublin-10.201.25.0/24 + 0 voleb	2012	Ne					
7.	MNG A-10.201.16.0/24	10.201.16.0 / 24		MNG building A	4	29	Demo-10.201.0.0/19	MNG_A-10.201.16.0/24 + 0 voleb	2070	Ne					
8.	MNG Bonn-10.201.18.0/24	10.201.18.0 / 24		MNG branch office Bonn	4	15	Demo-10.201.0.0/19	MNG_Bonn-10.201.18.0/24 + 0 voleb	2010	Ne					
9.	MNG Dublin-10.201.17.0/24	10.201.17.0 / 24		MNG branch office Dublin	4	20	Demo-10.201.0.0/19	MNG_Dublin-10.201.17.0/24 + 0 voleb	2009	Ne					
10.	PC A-10.201.0.0/22	10.201.0.0 / 22		Stations building A	7 (1 dynamický)	104	Demo-10.201.0.0/19	PC_A-10.201.0.0/22 + 0 voleb	2000	Ne	USER				
11.	PC Bonn-10.201.12.0/23	10.201.12.0 / 23		Stations branch office Bonn	6	63	Demo-10.201.0.0/19	PC_Bonn-10.201.12.0/23 + 0 voleb	2006	Ne	USER				
12.	PC Dublin-10.201.8.0/23	10.201.8.0 / 23		Stations branch office Dublin	7 (1 dynamický)	63	Demo-10.201.0.0/19	PC_Dublin-10.201.8.0/23 + 0 voleb	2003	Ne	USER				
13.	Print A-10.201.15.0/26	10.201.15.0 / 26		Printers building A	3	6	Demo-10.201.0.0/19	Print_A-10.201.15.0/26 + 0 voleb	2002	Ne					
14.	Print Bonn-10.201.15.192/27	10.201.15.192 / 27		Printers branch office Bonn	3	6	Demo-10.201.0.0/19	Print_Bonn-10.201.15.192/27 + 0 voleb	2008	Ne					
15.	Print Dublin-10.201.15.128/27	10.201.15.128 / 27		Printers branch office Dublin	3	9	Demo-10.201.0.0/19	Print_Dublin-10.201.15.128/27 + 0 voleb	2005	Ne					
16.	PrivPC A-10.201.7.0/24	10.201.7.0 / 24		Privileged PC building A	6	39	Demo-10.201.0.0/19	PrivPC_A-10.201.7.0/24 + 0 voleb	2001	Ne	USER				
17.	PrivPC Bonn-10.201.14.0/24	10.201.14.0 / 24		Privileged PC branch office Bonn	6	11	Demo-10.201.0.0/19	PrivPC_Bonn-10.201.14.0/24 + 0 voleb	2007	Ne	USER				
18.	PrivPC Dublin-10.201.10.0/24	10.201.10.0 / 24		Privileged PC branch office Dublin	6	17	Demo-10.201.0.0/19	PrivPC_Dublin-10.201.10.0/24 + 0 voleb	2004	Ne	USER				
19.	Quarantine Bonn-10.201.27.192/26	10.201.27.192 / 26		Quarantine Net Bonn	1	0	Demo-10.201.0.0/19	Quarantine_Bonn-10.201.27.192/26 + 0 voleb	2053	Ne	QUARANTINE				
20.	Quarantine Dublin-10.201.27.128/26	10.201.27.128 / 26		Quarantine Net Dublin	1	0	Demo-10.201.0.0/19	Quarantine_Dublin-10.201.27.128/26 + 0 voleb	2052	Ne	QUARANTINE				
21.	Quarantine A-10.201.27.0/25	10.201.27.0 / 25		Quarantine Net A	1	0	Demo-10.201.0.0/19	Quarantine_A-10.201.27.0/25 + 0 voleb	2051	Ne	QUARANTINE				

Vypsáné záznamy: 1-21/21

Na stránku: 50 v

Strana: 1 / 1

1. Nastavení pokročilých politik



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

[Přestat editovat](#)

jindra@10.201.16.120



Různé Topologie DHCP Volby MSAD Radius DNS Switche DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

Sítě: Demo-10.201.0.0/19

10.201.0.0/19 (10.201.0.0-10.201.31.255)

Demo office A

Vlastních podsítí: 21,

Všech podsítí: 21

Počet bloků: 0

Počet IP: 0 / 8190 (4.7%)

Vlastních pravidel: 0,

Všech pravidel: 388



Sítě - Editace

ID:	16 (platné od změny 568 do současnosti)
Jméno:	Demo-10.201.0.0/19
IP adresa/Maska:	10.201.0.0 / 19 10.201.0.1 - 10.201.31.254 Síť Maska Broadcast
Popis:	Demo office A
Výchozí VLAN:	- Ne zvoleno -
Cisco voice:	<input type="checkbox"/>
BYOD síť:	<input type="checkbox"/>
Skupina DNS serverů:	DNS internal
Výchozí doména (dns origin):	novicom.demo.
Skupina radius serverů:	Radius main
ACL:	- Ne zvoleno -
Šablona přihlašovacího času:	- Ne zvoleno -
Nouzová VLAN:	- Ne zvoleno - (pro nefunkční supplicant)
ACL pro nouzovou VLAN:	
Šablona přihlašovacího času pro nouzovou VLAN:	
Brána pro generování voleb k sítím:	- Ne zvoleno - Je nutné provést generování skupin voleb k sítím, aby sejevilo.

Volby	Volba	Politika	Pokud volba	Reg. výraz	Nový typ	Hodnota
	---					+
Skupina voleb:	-					

Sítě nemůže mít bloky, protože obsahuje podsítě.

2. Přidání neznámého zařízení do sítě

Top 24 sítě podle využití IP [%]

[Zobrazit vše](#)

Jméno sítě	DHCP	MAC/24h	Využití IP v %
Quarantine_Bonn-10.201.27.192/26	0	0	48.4%
Quarantine_Dublin-10.201.27.128/26	0	0	48.4%
Print_Dublin-10.201.15.128/27	1	9	36.3%
Print_Bonn-10.201.15.192/27	1	6	26.3%
PrivPC_A-10.201.7.0/24	1	40	23.6%
PC_Dublin-10.201.8.0/23	1	58	16.5%
PC_Bonn-10.201.12.0/23	1	58	16.5%

Rychlé hledání

IP adresa IP adresa MAC Hledat

☆ Oblíbené

Servery DHCP klienti Sítě DHCP události DNS servery Switche Pravidla Dílčí monitor Monitor Radius uživatelé IP

Top 11 nejvytíženějších switčů

[Zobrazit vše](#)

Jméno switče	Porty využité po celou dobu posledních 7 dní
A1-C3560X-48-1	78.7%
Dublin1-C3560X-24-1	60.6%
Bonn1-C3560X-24-1	54.5%
A2-C2960G-24-2	12%
A2-C2960G-24-1	12%

Posledních 100 událostí Alert centra za posledních 7 dní

[Zobrazit vše](#)

Jméno	Modul	Závažnost	Čas
Test modul	Test input module	Nizká	24.09.2024 02:13:15
New device	New device input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15
MSAD NAC users difference	Radius input module	Střední	24.09.2024 02:12:15

Top 14 sítě s nejvíce požadavky Discover za posledních 7 dní

[Zobrazit vše](#)

Celkem požadavků: 54046, Unikátních požadavků: 253

Jméno sítě	Discover / Unikátní Discover
PC_A-10.201.0.0/22	17042
PC_Bonn-10.201.12.0/23	12328
PC_Dublin-10.201.8.0/23	11376
PC_A-10.201.0.0/22	79
PC_Bonn-10.201.12.0/23	56
PC_Dublin-10.201.8.0/23	53

Top 5 sítě s neznámými zařízeními

Jméno sítě	Počet nových zařízení
MNG_A-10.201.16.0/24	5
PC_A-10.201.0.0/22	1
PrivPC_A-10.201.7.0/24	1
Guest_A-10.201.24.0/24	1
Guest_Bonn-10.201.26.0/24	1

Top 14 sítě s nejvíce požadavky Request za posledních 7 dní

[Zobrazit vše](#)

Top 1 síť se zařízeními v rozporu s pravidly

2. Přidání neznámého zařízení do sítě



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

[Přestat editovat](#)

[jindra@10.201.16.120](#)



[Různé](#) [Topologie](#) [DHCP Volby](#) [MS AD](#) [Radius](#) [DNS](#) [Switche](#) [DHCP](#) [Adresní plánování](#) [Importy](#) [Přístup](#) [Protokol](#) [Uživatelský radius](#) [DACL](#) [Přihlašovací čas](#) [Alert centrum](#) [Kabelová kniha](#)

Díčí monitor - Výpis

Vypsání záznamy: 1-5/5

Na stránku: 50

Strana: 1 / 1

Fulltextové hledání

[Hledat](#)

Strana: 1 (1 - 1) [Zobrazit](#)

[Export do CSV](#)

Filtr (Kliknutím ukázat)

#	MAC	POPIS MAC	IP	POPIS IP	PŘIDAT	STATUS	SOUČ. STATUS	PŘÍDĚLENÍ	JMÉNO SWITCHE	INTERFACE	ZDROJ	JMÉNO SERVERU	PORTY	SÍŤ ADR. PLÁN.	OD	DO	AUDIT
1.	00:50:56:8D:D9:7C+	<input type="checkbox"/>	10.201.16.63		F S I	Neznámý	Neznámý	Nepřifazeno		eth1	ARP	work1-A		MNG_A-10.201.16.0/24	26.10.2023 14:20:01	24.09.2024 02:23:26	
2.	00:50:56:8D:00:3C+	<input type="checkbox"/>	10.201.16.64		F S I	Neznámý	Neznámý	Nepřifazeno		eth1	ARP	work1-A		MNG_A-10.201.16.0/24	26.10.2023 14:20:02	24.09.2024 02:23:26	
3.	00:50:56:8D:94:A2+	<input type="checkbox"/>	10.201.16.65		F S I	Neznámý	Neznámý	Nepřifazeno		eth1	ARP	work1-A		MNG_A-10.201.16.0/24	05.01.2024 11:35:07	24.09.2024 02:20:07	
4.	0C:C4:7A:DA:21:E9+	<input type="checkbox"/>	10.201.16.1	gwa01.novicom.demo	F S I	Neznámý	Neznámý	Nepřifazeno		eth1	ARP	work1-A		MNG_A-10.201.16.0/24	23.09.2024 02:42:36	24.09.2024 02:09:27	
5.	E8:1C:BA:BE:1D:4B+	<input type="checkbox"/>	10.201.16.126		F S I	Neznámý	Neznámý	Nepřifazeno		eth1	ARP	work1-A		MNG_A-10.201.16.0/24	23.09.2024 15:18:30	23.09.2024 15:18:30	

Vypsání záznamy: 1-5/5


Na stránku: 50

Strana: 1 / 1

2. Přidání neznámého zařízení do sítě

Zjednodušené vkládání MAC - IP

IP adresa Zapsat ručně Vybrat blok Volné IP ze sítě Žádná

Sítě: Byod A-10.201.28.0/23 (IP mimo bloky) 510 volných adres 

MAC: 0C:C4:7A:DA:21:E9

Nepovinné údaje:

VLAN ID: - Ne zvoleno -

Autentikace v nativní síti: MAC Seznam NAC uživatelů MAC + Seznam NAC uživatelů

Zvolte uživatele

Autentikace mimo nativní síť: Ne MAC Seznam NAC uživatelů MAC + Seznam NAC uživatelů

Povoleno: Ano

Povoleno do: 

Typ pravidla: DHCP přiřazení

Krizový set: Ne

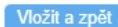
DNS: gwa01 novicom.demo

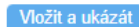
Popis IP: gwa01.novicom.demo

Popis MAC:

Skupina voleb: -









2. Přidání neznámého zařízení do sítě



Dashboard

Lokalita: - Ne zvoleno -

Profil: -- Všechny povolené sítě --

AddNet Enterprise edition, Novicom s.r.o. ()

[jindra edituje]

Přestat editovat

jindra@10.201.16.120



Různé Topologie DHCP Volby MS AD Radius DNS Switch DHCP Adresní plánování Importy Přístup Protokol Uživatelský radius DACL Přihlašovací čas Alert centrum Kabelová kniha

Zjednodušené vkládání MAC - IP

IP adresa Zapsat ručně Vybrat blok Volné IP ze sítě Žádná

Sít: Byod A-10.201.28.0/23 (IP mimo bloky) 510 volných adres [Provéřit](#)

MAC 0C:C4:7A:DA:21:E9

Nepovinné údaje:

VLAN ID: - Ne zvoleno -

Autentikace v nativní síti: MAC Seznam NAC uživatelů MAC + Seznam NAC uživatelů

Autentikace mimo nativní síti:

- valid
- valid_computer_certificate (AD)**
- valid_user_certificate (AD)
- ken.ivanhoe (Nativní AD)
- tonda.svatek (Nativní AD)

Povoleno: Ano

Povoleno do:

Typ pravidla: DHCP přiřazení

Krizový set: Ne

DNS: gwa01 novicom.demo

Popis IP: gwa01.novicom.demo

Popis MAC:

Skupina voleb: -

Vložit

Vložit a zpět

Vložit a ukázat

Zpět

Shrnutí konceptu Novicomu a kam patří ADDNET

• Řízení integrovaných síťových služeb

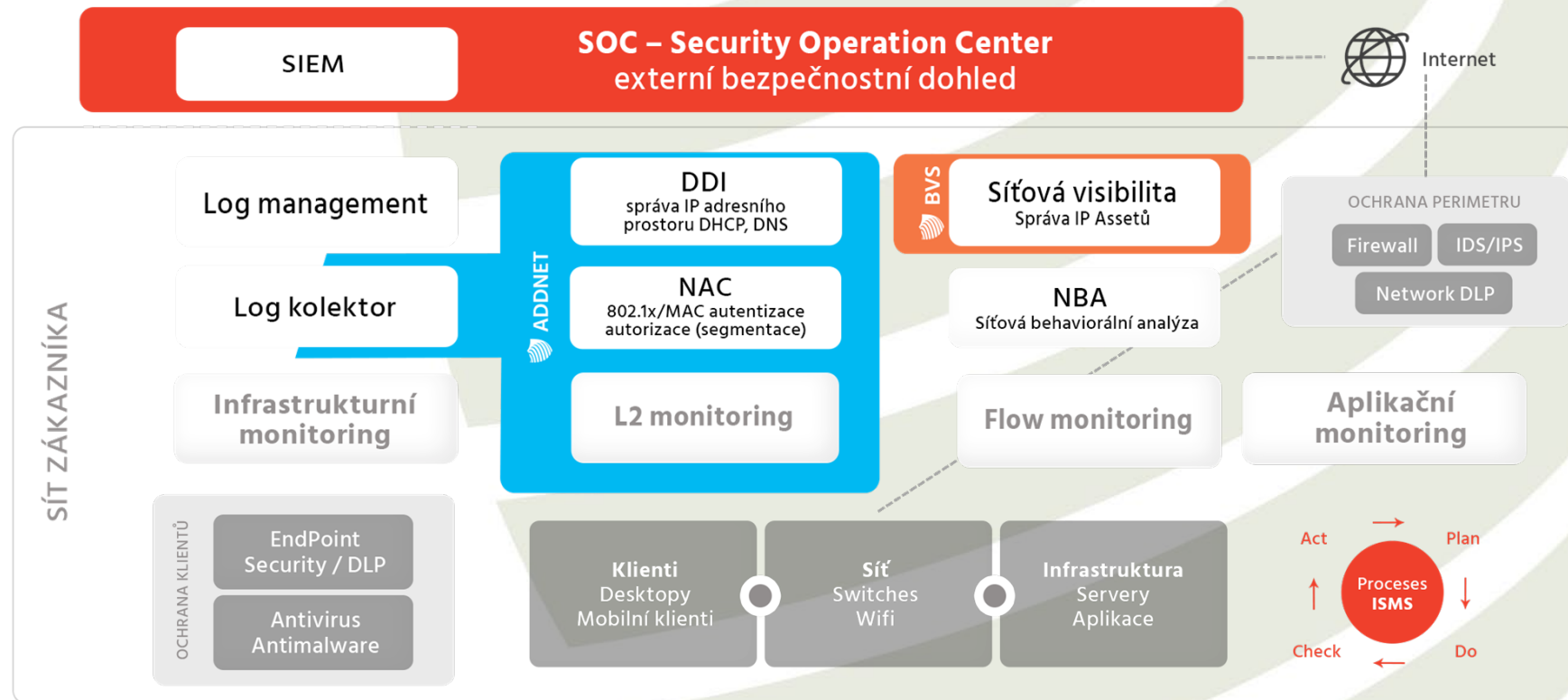
- L2 monitoring
- DDI
- NAC (segmentace)

• Sběr dat pro monitoring

- L2 monitoring
- DDI/NAC
- Syslog
- Síťové toky

• Provádění reakčních opatření

- Uživatelsky
- S využitím rest api



Je zavedení NAC mrtvou záležitostí?

- **Cloud computing**
 - Ale já mám všechno v cloudu – opravdu?
- **Principy Zero trust**
 - Funguje na všem, kde je nainstalován klient...
 - Co tiskárny, kamery, OT?
- **Komplikovanost 802.1x**
 - Nemám na všechno suplikant, nezvládneme výjimky, všechny MAC based zařízení dáme do whitelistu...
 - A co takhle DDI/NAC, a MAC based s ochranou?
- **Ne – segmentace, sběr síťových dat, aktivní reakce – je aktuálnější než kdykoliv před tím**
- **Jak chcete reagovat**
 - když nevíte co se děje v síti?
 - když nevíte, jak mají být nastavená pravidla síťových služeb?
 - když aktivně neřídíte svoji síť?



Shrnutí výhod přístupu Novicomu

- **Výrazné zvýšení bezpečnosti**
 - Řízení přístupu do sítě
 - Zavedení pokročilých síťových politik
 - Zvýšení dostupnosti síťových služeb
- **Zásadní zjednodušení síťové správy**
 - Integruje všechny významné síťové služby – DDI/NAC
 - Vysoce kvalifikovaní síťáři nastaví politiky
 - Provozní správci aplikují připravené politiky
 - Veškerá činnost je auditovaná
- **Připraveno na snadné začlenění do stávající sítě organizace**
 - Připravené integrace pro všechny zásadní oblasti
- **Je navrženo pro spolupráci s aktivním SOC**
 - Sběr dat a zajištění reakcí v prostředí interní sítě
- **Je připraveno na budoucí zařízení, bez ohledu na výrobce**
- **Zavádí moderní princip SD LAN**
- **Je úspěšně ověřeno na desítkách rozsáhlých sítí u zákazníků v ČR i zahraničí**





novicom

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER



ADDNET



BVS



APPLIANCE

Další informace?

Sledujte nás na

- www.novicom.cz
- [LinkedIn](#)
- [Facebook](#)

Kontaktujte nás na

- Email: sales@novicom.cz
- Tel. +420 271 777 231

Adresa

- Na schodech 65/1
- 140 00 Praha 4 - Michle