Załącznik nr 3 – Wymagane parametry minimalne urządzeń

Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

1 Przełącznik zarządzalny – typ 1, ilość:22 szt.

Cechy produktu:

Porty fizyczne i porty management:

- 24 portów RJ-45 (24 portów PoE)
- 4 porty SFP
- 1 port konsolowy RJ-45
- 1 port EPS (zewnętrzny zasilacz)
- 1 port zasilania AC

Wydajność:

- Możliwość przełączania: 56Gbps
- Rozmiar bufora pakietów: 12 Mb
- Rozmiar tabeli adresacji MAC: 16K
- Pamięć FLASH: 32 MB
- Pamięć DRAM :256 MB
- Szybkość przekazywania: 14,9 Mpps
- Ramka Jumbo: 10K

Cechy QoS:

- Rate Limiting
- Priority Queues Schedule (WRR/Strict Priority/Hybrid QoS)
- Port-Based QoS
- IPv4/IPv6 DSCP
- DiffServ
- Auto VOIP
- Auto Video
- 8 sprzętowych kolejek na port

PoE:

- Wsparcie IEEE 802.3af (15.4W) / IEEE802.3at (30W) na portach RJ-45
- Harmonogram aktywności zasilania PoE definiowany godzinowo
- Dynamiczna alokacja mocy
- Automatyczne wyłączenie po przekroczeniu budżetu mocy
- Budżet mocy 370W z możliwością rozszerzenia do 740W

Zarządzanie:

- System ochrony hasła
- NTP/SNTP
- Dual Image/Configuration
- Configuration upload/download (HTTP/TFTP)
- Firmware upload/download (HTTP/TFTP)
- RMON (groups 1,2,3 and 9)
- SNMP
- SNMP Trap
- SNMP v1/v2/v3
- SNMP Standard/Private MIB
- Management Access (Console/SNMP/Web /Telnet)

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Zapisywanie logów w pamięci FLASH
- Event/Error Log/Syslog
- DHCP v4/v6 Client/Option 82/DHCP Snooping
- DHCP Relay v4
- Port Mirroring (One to One) TX/RX (both)
- DHCP v4 Server

Właściwości warstwy L2:

- Protokół Spanning Tree:
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Rapid Spanning Tree Protocol (MSTP)
  - Wykrywanie Pętli
  - BDPU Filter/Guard
  - BDPU Forward
  - Root Guard

VLAN:

- Wsparcie dla 4K IEEE 802.1Q VLANs
- Port-Based/MAC-Based/Protocol-Based VLANs
- Guest VLAN
- Auto Voice VLAN
- Auto Video VLAN

Agregacja linków:

- Magistrala statyczna
- Protokół IEEE 802.3ad Link Aggregation Control

IGMP Snooping:

- IGMP v1/v2/v3 snooping
- IGMP Proxy reporting
- IGMP Throttling
- IGMP Immediate Leave
- IGMP Querier i Filtering
- MLD Snooping

Zgodność elektromagnetyczna:

- CE Mark
- FCC Klasa A
- CISPR Class A

Cechy mechaniczne:

- Wskaźniki LED: Port, Diagnostyka
- Montaż w szafie rack 19" (uchwyty montażowe w komplecie)

Zasilanie:

- Przewód zasilający: 100 do 240 V, 60 Hz, 1.0A
- Zasilacz wewnętrzny

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Automatycznie zmieniający zakres transformator: 100 do 240 VAC, 50 do 60 Hz
- Pobór mocy:
  - 490W (950W przy budżecie PoE zwiększonym do 740 W)

Bezpieczeństwo:

- Ochrona DDOS
- Ochrona CPU (monitorowanie poziomu eksploatacji)
- Izolacja portu
- Port Mirror (jeden do jednego, jeden do wielu)
- Remote Mirror
- Storm Control
- Broadcast/Multicast/Unknown Storm Control
- IEEE 802.1X
- ACL
- Ingress Only
- L2/L3/L4
- ACL entry :512
- IPv4/IPv6
- TCP/UDP-Based, MAC-Based ACL
- Ochrona portu
- Filtr MAC
- Port max count per port
- Dynamiczne przydzielanie VLAN Assignment
- Dynamiczna kontrola ARP
- AAA (RADIUS/TACACS+)
- IP Source Guard
- SSH v1.5/v2.0
- SSL v1/v2/v3
- SSL IPv4/IPv6
- Przełączniki muszą być objęte gwarancją wieczystą producenta

2 Przełącznik zarządzalny – typ 2 ilość:13 szt.

Cechy produktu:

Porty fizyczne i porty management:

- 48 portów RJ-45 10/100/1000BASE-TX
- 4 porty SFP
- 1 port konsolowy RJ-45
- 1 port zasilania AC

Wydajność:

- Możliwość przełączania: 104 Gbps
- Rozmiar bufora pakietów: 12 Mb

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Rozmiar tabeli adresacji MAC: 16K
- Pamięć FLASH: 32 MB
- Pamięć DRAM :256 MB
- Szybkość przekazywania: 77,4 Mpps
- Ramka Jumbo: 10K

Cechy QoS:

- Rate Limiting
- Priority Queues Schedule (WRR/Strict Priority/Hybrid QoS)
- Port-Based QoS
- IPv4/IPv6 DSCP
- DiffServ
- Auto VOIP
- Auto Video
- 8 sprzętowych kolejek na port

Zarządzanie:

- System ochrony hasła
- NTP/SNTP
- Dual Image/Configuration
- Configuration upload/download (HTTP/TFTP)
- Firmware upload/download (HTTP/TFTP)
- RMON (groups 1,2,3 and 9)
- SNMP
- SNMP Trap
- SNMP v1/v2/v3
- SNMP Standard/Private MIB
- Management Access (Console/SNMP/Web /Telnet)
- Zapisywanie logów w pamięci FLASH
- Event/Error Log/Syslog
- DHCP v4/v6 Client/Option 82/DHCP Snooping
- DHCP Relay v4
- Port Mirroring (One to One) TX/RX (both)
- DHCP v4 Server

Właściwości warstwy L2:

- Protokół Spanning Tree:
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Rapid Spanning Tree Protocol (MSTP)
  - Wykrywanie Pętli
  - BDPU Filter/Guard
  - BDPU Forward
  - Root Guard

VLAN:

- Wsparcie dla 4K IEEE 802.1Q VLANs
- Port-Based/MAC-Based/Protocol-Based VLANs
- Guest VLAN

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Auto Voice VLAN
- Auto Video VLAN

Agregacja linków:

- Magistrala statyczna
- Protokół IEEE 802.3ad Link Aggregation Control

IGMP Snooping:

- IGMP v1/v2/v3 snooping
- IGMP Proxy reporting
- IGMP Throttling
- IGMP Immediate Leave
- IGMP Querier i Filtering
- MLD Snooping

Zgodność elektromagnetyczna:

- CE Mark
- FCC Klasa A
- CISPR Class A

Cechy mechaniczne:

- Wskaźniki LED: Port, Diagnostyka
- Montaż w szafie rack 19" (uchwyty do montażu w komplecie)

Bezpieczeństwo:

- Ochrona DDOS
- Ochrona CPU (monitorowanie poziomu eksploatacji)
- Izolacja portu
- Port Mirror (jeden do jednego, jeden do wielu)
- Remote Mirror
- Storm Control
- Broadcast/Multicast/Unknown Storm Control
- IEEE 802.1X
- ACL
- Ingress Only
- L2/L3/L4
- ACL entry :512
- IPv4/IPv6
- TCP/UDP-Based, MAC-Based ACL
- Ochrona portu
- Filtr MAC
- Port max count per port
- Dynamiczne przydzielanie VLAN Assignment
- Dynamiczna kontrola ARP
- AAA (RADIUS/TACACS+)
- IP Source Guard
- SSH v1.5/v2.0
- SSL v1/v2/v3

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- SSL IPv4/IPv6
- Przełączniki muszą być objęte gwarancją wieczystą producenta

3 Przełącznik zarządzalny – typ 3, ilość: 54 szt.

Cechy produktu:

Porty fizyczne i porty management:

- 24 portów RJ-45 (24 portów PoE)
- 4 porty SFP
- 1 port konsolowy RJ-45
- 1 port zasilania AC

Wydajność:

- Możliwość przełączania: 56Gbps
- Rozmiar bufora pakietów: 12 Mb
- Rozmiar tabeli adresacji MAC: 16K
- Pamięć FLASH: 32 MB
- Pamięć DRAM :256 MB
- Szybkość przekazywania: 14,9 Mpps
- Ramka Jumbo: 10K

Cechy QoS:

- Rate Limiting
- Priority Queues Schedule (WRR/Strict Priority/Hybrid QoS)
- Port-Based QoS
- IPv4/IPv6 DSCP
- DiffServ
- Auto VOIP
- Auto Video
- 8 sprzętowych kolejek na port

PoE:

- Wsparcie IEEE 802.3af (15.4W) / IEEE802.3at (30W) na portach RJ-45
- Harmonogram aktywności zasilania PoE definiowany godzinowo
- Dynamiczna alokacja mocy
- Automatyczne wyłączenie po przekroczeniu budżetu mocy
- Budżet mocy 200W

Zarządzanie:

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- System ochrony hasła
- NTP/SNTP
- Dual Image/Configuration
- Configuration upload/download (HTTP/TFTP)
- Firmware upload/download (HTTP/TFTP)
- RMON (groups 1,2,3 and 9)
- SNMP
- SNMP Trap
- SNMP v1/v2/v3
- SNMP Standard/Private MIB
- Management Access (Console/SNMP/Web /Telnet)
- Zapisywanie logów w pamięci FLASH
- Event/Error Log/Syslog
- DHCP v4/v6 Client/Option 82/DHCP Snooping
- DHCP Relay v4
- Port Mirroring (One to One) TX/RX (both)
- DHCP v4 Server

Właściwości warstwy L2:

- Protokół Spanning Tree:
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Rapid Spanning Tree Protocol (MSTP)
  - Wykrywanie Pętli
  - BDPU Filter/Guard
  - BDPU Forward
  - Root Guard

VLAN:

- Wsparcie dla 4K IEEE 802.1Q VLANs
- Port-Based/MAC-Based/Protocol-Based VLANs
- Guest VLAN
- Auto Voice VLAN
- Auto Video VLAN

Agregacja linków:

- Magistrala statyczna
- Protokół IEEE 802.3ad Link Aggregation Control

IGMP Snooping:

- IGMP v1/v2/v3 snooping
- IGMP Proxy reporting
- IGMP Throttling
- IGMP Immediate Leave
- IGMP Querier i Filtering
- MLD Snooping

Zgodność elektromagnetyczna:

- CE Mark
- FCC Klasa A

Sekcji Informa
WSZ w Koninie
Dawid Górski

- CISPR Class A

Cechy mechaniczne:

- Wskaźniki LED: Port, Diagnostyka
- Montaż w szafie rack 19" (uchwyty montażowe w komplecie)

Zasilanie:

- Przewód zasilający: 100 do 240 V, 60 Hz, 1.0A
- Zasilacz wewnętrzny
- Automatycznie zmieniający zakres transformator: 100 do 240 VAC, 50 do 60 Hz
- Pobór mocy: 260W

Bezpieczeństwo:

- Ochrona DDOS
- Ochrona CPU (monitorowanie poziomu eksploatacji)
- Izolacja portu
- Port Mirror (jeden do jednego, jeden do wielu)
- Remote Mirror
- Storm Control
- Broadcast/Multicast/Unknown Storm Control
- IEEE 802.1X
- ACL
- Ingress Only
- L2/L3/L4
- ACL entry :512
- IPv4/IPv6
- TCP/UDP-Based, MAC-Based ACL
- Ochrona portu
- Filtr MAC
- Port max count per port
- Dynamiczne przydzielanie VLAN Assignment
- Dynamiczna kontrola ARP
- AAA (RADIUS/TACACS+)
- IP Source Guard
- SSH v1.5/v2.0
- SSL v1/v2/v3
- SSL IPv4/IPv6
- Przełączniki muszą być objęte gwarancją wieczystą producenta

Kier...
Sekcji Informat...
WSZ... w Koninie
Dawid Górski

4 Przełącznik zarządzalny – typ 4, ilość: 4 szt.

Cechy produktu:

Porty fizyczne i porty management:

- 48 portów SFP+ 10GE
- 6 portów QSFP 40GE
- 1 x RJ-45 : port konsolowy
- 1 x RJ-45 100/1000BASE-T management port (out of the band)
- 1 x USB Type A storage port

Główne podzespoły

- Chipset: Broadcom BCM56854 Trident II lub podobny z wydajnością nie mniejszą niż 720Gbps
- Procesor: Intel Atom C2538 quad-core 2.4GHz x86 processor
- Pamięć nie mniejsza niż 8 GB SO-DIMM DDR3 RAM with ECC
- 16 MB SPI
- 8 GB NAND flash

Diody LED

- Diody portów 40G QSFP: Status linku, aktywność
- Diody portów 10G SFP+: Status linku, aktywność, szybkość linku
- Dioda portu Ethernet Management: Status linku, aktywność
- Dioda LED portu konsolowego: Status linku, Aktywność
- Diody systemowe: Diagnostyka, Wentylatory, PSU1, PSU2

Zasilanie

- Zasilacze PSU (Power Supply Unit): 2 redundantne zasilacze, load-sharing, hot-swappable, AC lub 48VDC
- Napięcie zasilania: 90 do 264 VAC, 50-60 Hz., -48 do -72 VDC.
- Prąd zasilania: 6A @100/120 VAC, 3 A @200/240 VAC
- Maksymalna konsumpcja mocy: 282W

Kompatybilność elektromagnetyczna

- CE Mark (EN55022 Class A)
- FCC Part 15 Class A
- VCCI

Oprogramowanie

Przełączniki powinien posiadać Open Network Install Environment (ONIE) umożliwiające instalacje systemów operacyjnych : OpenSwitch, Cumulus Linux, Big Mon/Cloud Fabric, PicOS, OcNOS.

Kierow...
Sekcji Informaty...
WSZ w Koninie
Dawid Górski

Funkcje oprogramowania

Warstwa L2 :
• Non-blocking wire speed L2 switching
• Jumbo frames up to 9,216 bytes
• Flow control – IEEE 802.3x for full-duplex mode – Back-pressure flow control in half-duplex mode
• Broadcast, unicast, and multicast storm protection
• IGMP snooping, up to 1K groups
• VLAN support – IEEE 802.1Q VLANs – 4,094 VLANs – Port-based VLANs
• Spanning Tree – IEEE 802.1D STP – IEEE 802.1w RSTP – IEEE 802.1s MSTP – Per-VLAN Spanning Tree (PVST)
• Link aggregation – Up to 48 trunk groups – Up to 8 ports per trunk group – IEEE 802.3ad Link Aggregation & LACP
• Port mirroring (many-to-one)
• Port security
• LLDP
• Q-in-Q
• Multi-chassis Link Aggregation (MLAG)
• MLAG with Spanning Tree support
• VXLAN Tunnel Endpoint (VTEP) support
• 802.1X support

Warstwa L3 (funkcje routingu) :
• ECMP: 32 next hops
• ECMP resilient hashing
• RIPv2
• OSPFv2
• MP-BGP (IPv4, IPv6) – Static MPLS LSP – Labeled BGP (RFC3107)
• VRRP
• DHCP-relay including DHCP option-82 and ARP inspection Layer 3 Multicast
• PIM-SM and PIM-SSM
• IGMPv1/v2/v3
• VXLAN Tunnel Endpoint (VTEP) – VxLAN over mLAG
• 802.1X support – GRE tunneling over LAG interfaces

Warstwa L3 (IPv6) :
• RIPng
• OSPFv3
• MBGP for IPv6 NLRI
• IPv6 routing

Bezpieczeństwo :
• Hasło użytkownika (dostęp do zarządzania)
• L2/L3/L4 ACLs
• TACACS+ AAA
• SSHv1/v2
• SSLv3/TLS v1
• DoS attack protection

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

Quality of Service :
- IEEE 802.1p-based CoS
- 8 priority queues per port
- DSCP-based CoS
- Policy-based DiffServ

Zarządzanie :

- Command line interface (CLI)
- Telnet and SSH remote login
- Centralized control plane policing and filtering
- SNMPv1/v2c
- AAA Radius support
- IPFIX (NetFlow) / sFlow

Protokoły komunikacyjne OpenFlow, CrossFlow i AdvanceFlow :

- Oparte na Open-vSwitch (OVS) 2.3
- Kompatybilność ze specyfikacją OpenFlow 1.4
- Optymalizacja TCAM Flow dla lepszej skalowalności i wydajności
- Interfejs Web / GUI do konfiguracji OVS
- Kompatybilność z OpenDaylight, ONOS, HPE's VAN and RYU
- Enkapsulacja OpenFlow : L2oGRE, L3oGRE, NVGRE, PBB, VXLAN, MPLS
- Network Address Translation (NAT) – Table Type Patterns (TTP) Wsparcie do dwóch milionów przepływów IPv4

Środowisko programowe :

- ONIE
- Auto provisioning (Zero Touch Provisioning)
- Debian 7.0 Linux distribution
- Service daemon for L2/L3 Mode and OVS Mode
- Standard Debian Based package upgrade (apt-get)
- CLI ze skryptami i API
- Configuration Commit / Check / Rollback
- C/C++, Ruby, Python, Perl
- Zarządzanie konfiguracją : Puppet, Chef, CFEngine, Ansible, Salt
- 802.1ag CFM w OVS / tryb OpenFlow

Zgodność ze standardami :

- 802.1D Bridging and Spanning Tree Protocol
- 802.1s Multiple Spanning Tree Protocol
- 802.1w Rapid Spanning Tree Protocol
- 802.1p QOS/COS
- 802.1Q VLAN Tagging
- 802.1X Port-based Network Access Control (PNAC)

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- 802.1ah PBB (MAC in MAC)
- 802.3ad Link Aggregation with LACP
- 802.3ab 1000BASE-T
- 802.3z Gigabit Ethernet
- 802.3ae 10 Gigabit Ethernet
- 802.3by 25/50 Gigabit Ethernet
- 802.3ba 40 Gigabit Ethernet
- 802.3ba 100 Gigabit Ethernet – sygnalizacja błędu linku 10G/40G

- Przełączniki muszą być objęte minimum trzy letnią gwarancją producenta

5 Urządzenia UTM pracujące w klastrze active-passive, ilość: 2 sztuki (1 komplet)

Lp.	Nazwa parametru
1.	Zapora sieciowa typu: DEEP PACKET INSPECTION
2.	Mechanizm pozwalający na dwustronną analizę ruchu bez jego buforowania i proxy
3.	Minimalna ilość interfejsów: 2 interfejsy 10GbE SFP + 4 interfejsy 1 GbE SFP 12 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G 1 interfejs konsoli do zarządzania zaporą 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą
4.	Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
5.	Minimalna ilość stref bezpieczeństwa: 206
6.	Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
7.	Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
8.	Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
9.	Minimalna ilość jednocześnie obsługiwanych sesji: 400,000
10.	Możliwość obsłużenia przynajmniej 40000 nowych sesji w ciągu 1 sekundy.
11.	Przepustowość urządzenia pracującego w trybie stateful firewall: 6 Gbps – dla ramki 1518B zgodnie z RFC 2544
12.	Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 2Gbps
13.	Przepustowość urządzenia pracującego jako koncentrator VPN: 3 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

14.	Przepustowość urządzenia DPI (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS) – 800 Mbps
15.	Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3000
16.	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 500 z możliwością rozszerzenia do przynajmniej 3000
17.	Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
18.	Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
19.	Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)
20.	Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
21.	Wsparcie dla Dynamicznego DNS tzw. DDNS
22.	Zintegrowany mechanizm kontroli zawartości witryn
23.	Zintegrowany mechanizm kontroli ruchu SSL przesyłanego przez urządzenie – licencja nie wymagana
24.	Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL - licencja nie wymagana
25.	Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci
26.	Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego
27.	Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
28.	Kontrola dostępności zestawionych tuneli VPN
29.	Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP
30.	Konfiguracja oparta na pracy grupowej/obiektowej Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty
31.	Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)

Kierownik
Sekcji Informatycznej
WSZ w Goninie
Dawid Górski

32.	Funkcja NAT oparta o reguły bezpieczeństwa
33.	NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
34.	Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp streaming. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych. Bazy antywirusowe oparte o niezależnego producenta oprogramowania antywirusowego (innego niż producent urządzenia firewall)
35.	Zintegrowane system skanowania antyspyware
36.	Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer (możliwość filtrowania usług typu Kaaza, Emule itp.), buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach http
37.	System IPS musi używać algorytmu szeregowego przetwarzania
38.	Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur
39.	Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji Bazy w/w systemów muszą być aktualizowane raz dziennie
40.	System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików
41.	Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między wewnętrznymi strefami bezpieczeństwa
42.	Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi
43.	Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p
44.	Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP
45.	Umożliwia zdalny bezpieczny dostęp do aplikacji webowych, aplikacji typu klient-serwer, poczty oraz musi zapewniać współdzielenie plików poprzez standardową przeglądarkę bez konieczności instalowania dodatkowego oprogramowania z wykorzystaniem technologii SSL VPN
46.	Dodatkowe urządzenie pełniące funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka. Na urządzenie standby nie są wymagane

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

5.1 Wymagane licencje:

Lp.	Nazwa parametru
1.	Subskrypcja pozwalająca na aktualizację sygnatur aplikacji, IPS i wirusów oraz zapewnienie wsparcia technicznego na okres 3 lat

6 Urządzenia UTM– ilość: 1 sztuka

Lp.	Nazwa parametru
1.	Zapora sieciowa typu next generation firewall.
2.	Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
3.	Mechanizm pozwalający na dwustronną analizę ruchu bez potrzeby buforowania i proxy oraz bez ograniczeń na rozmiar skanowanego pliku.
4.	Rozwiązanie musi być zbudowane w oparciu o dedykowaną platformę sprzętową w oparciu o procesory w architekturze MIPS64.
5.	Urządzenie musi być przystosowane do montażu w szafie rack.
6.	Minimalna ilość interfejsów: 8 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa. 2 interfejsy USB do podłączenia modemu 3G/4G 1 interfejs konsoli 1 interfejs do zarządzania
7.	Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa.
8.	Minimalna ilość stref bezpieczeństwa: 32
9.	Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
10.	Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
11.	Minimalna ilość jednocześnie obsługiwanych sesji: 225000
12.	Możliwość obsłużenia przynajmniej 15000 nowych sesji w ciągu 1 sekundy.
13.	Przepustowość urządzenia pracującego w trybie stateful firewall: 1,9 Gbps – dla ramki 1518B zgodnie z RFC 2544
14.	Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 700 Mbps
15.	Przepustowość urządzenia pracującego jako koncentrator VPN: 1,1 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544
16.	Przepustowość urządzenia DPI (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS) – 300 Mbps

Kier...
Sekcji Informatyczn...
WSZ w Koninie
Dawid Górski

17.	Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 250
18.	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostarczonych z urządzeniem: 12 z możliwością rozszerzenia do przynajmniej 250.
19.	Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
20.	Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
21.	Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)
22.	Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
23.	Wsparcie dla Dynamicznego DNS tzw. DDNS
24.	Zintegrowany mechanizm kontroli zawartości witryn
25.	Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
26.	Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL
27.	Możliwość uruchomienia minimum siedmiu łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
28.	Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
29.	Kontrola dostępności zestawionych tuneli VPN
30.	Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
31.	Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty
32.	Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
33.	Funkcja NAT oparta o reguły bezpieczeństwa
34.	NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

	ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
35.	Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych
36.	Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer (możliwość filtrowania usług typu Kaaza, Emule itp.), buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach http
37.	System IPS musi używać algorytmu szeregowego przetwarzania
38.	Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur
39.	System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
40.	Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między wewnętrznymi strefami bezpieczeństwa
41.	Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi.
42.	Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pracującymi w standardzie 802.11ac
43.	Wbudowany kontroler powinien umożliwiać podłączenie i obsługę 32 punktów dostępowych sieci bezprzewodowej pochodzących od tego samego producenta.

6.1 Wymagane licencje:

Lp.	Nazwa parametru
1.	Licencje na aktualizację sygnatur antwirus, antyspyware, IPS, kontrola treści, kontrola aplikacji na okres 3 lat

7 Punkt dostępowy ilość: 220 sztuk

CECHY BEZPRZEWODOWEGO PUNKTU DOSTĘPOWEGO :

Fizyczne porty:

- Dwa porty 10/100/1000BASE-T Gigabit Ethernet (RJ-45), w tym jeden z obsługą PoE 802.3af/at
- Jeden port konsoli ze złączem RJ-45
- Dwie diody LED: Power, System
- Sześć wbudowanych anten omni
- Zgodność ze standardem PoE 802.3at/af

Standardy:

- IEEE 802.11n 2.4 GHz i 5.0 GHz
- IEEE 802.11ac/a 5.0 GHz

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- IEEE 802.11b/g, 2.4 GHz
- IEEE 802.3, IEEE 802.3u, IEEE 802.3ab
- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.11h Regulatory Domain Selection
- IEEE 802.11i
- Wi-Fi Multimedia (WMM)
- System WDS

Częstotliwości pracy:

- 802.11g/n:
  - 2.4 ~ 2.4835 GHz (US, KANADA)
  - 2.4 ~ 2.4835 GHz (ETSI, Japonia)
- 802.11b:
  - 2.4 ~ 2.4835 GHz (US, KANADA)
  - 2.4 ~ 2.4835 GHz (ETSI)
  - 2.4 ~ 2.497 GHz (Japonia)
- 802.11a/n:
  - 5.15 ~ 5.25 GHz (pasmo niskie) US/Kanada, Europa, Japonia
  - 5,25 ~ 5,35 GHz (pasmo średnie) US/Kanada, Europa, Japonia
  - 5,725 ~ 5,825 GHz (pasmo wysokie) US/Kanada
  - 5.50 ~ 5.70 GHz Europa

Bezpieczeństwo:

- WEP 64/128-bits
- Dostęp chroniony do Wi-Fi (WPA/WPA2)
- WPA/WPA2 (PSK) przez WDS
- Secure SSH (Secure Sockets Shell), Telnet
- Secure Sockets Layer (SSL) logowanie do zdalnego zarządzania
- HTTPS
- Lista kontrolna dostępu: 512
- Autentykacja RADIUS
- EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, EAP-SIM i EAP-AKA
- Wyłączenie rozsyłania SSID

Anteny:

- Typ: PCB
- Zysk: 12dBi@5GHz

Zgodność z przepisami:

- FCC Część 15 Klasa B
- CE

Certyfikaty:

- FCC Część 15C 15.247, 15.207 (2.4GHz)
- EN 300 328
- EN 301 489-1
- EN 301 489-17

Funkcje bezprzewodowe:

- Moc wyjściowa: 20dBm
- VAP (Virtual Access Point) z obsługą do 16 SSID
- Tryb pracy: AP, punkt-punkt WDS, punkt do wielu WDS, WDS z AP

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Regulacja mocy transmisji
- IEEE 802.11h DFS/DFS2 i automatyczne TPC
- Kontrola ruchu dla każdego SSID
- Preferencje pasma dla tych samych usług SSID na podwójnym paśmie
- Dynamiczny wybór kanału dla środowisk o dużym zaszumieniu
- Wybór szybkości w celu wyłączenia dostępu przy niskiej prędkości transmisji
- Wywłaszczenie połączenia klienta (n > ag > b) w razie pełnego obciążenia
- Automatyczny wybór kanału

Zarządzanie:

- CLI (Command Line Interface)
- Telnet, SSH
- Web-based Management (HTTP and HTTPS)
- SNMP management v1/v2c/v3
- Aktualizacja oprogramowania z wykorzystaniem serwerów TFTP, FTP i HTTP
- Zapisywanie i przywracanie konfiguracji z wykorzystaniem serwerów TFTP i FTP
- Informacje o systemie – AP status, station status, event logs
- Dual image
- SNTP
- Planowanie restartów urządzenia
- Wsparcie dla RADIUS
- Wsparcie dla IPv4 i IPv6
- Wyłączanie usługi WiFi podczas, gdy port uplink jest nieaktywny

Zasilanie:

- Wejście: 100 lub 240 VAC, 50-60 Hz
- Wyjście: 48 V/ 2A
- Pobór mocy: maksymalnie 14 W

CECHY KONTROLERA SPRZĘTOWEGO :

Porty fizyczne:

- Minimum jeden port konsoli ze złączem RJ45
- Minimum 6 portów Gigabit Ethernet RJ45
- 2xUSB 2.0 (typ A)
- Przycisk reset
- Diody LED: Power/Diag, Ethernet 1, Ethernet 2

Zarządzanie:

- Konfiguracja profilu
- Radio
- VAP
- QoS
- Konfiguracja radia (802.11a/b/g/n, VAP, szybkość transmisji)
- Zarządzanie i sterowanie częstotliwością radiową

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Automatyczne / ręczne przypisywanie planowania kanału AP
- Automatyczna zmiana kanału w celu uniknięcia zakłóceń
- Automatyczne / ręczne ustawienie mocy wyjściowej radia

Właściwości warstwy L2

- Funkcja mostkowania
- Protokół STP
- Cechy L2 ACL
- Izolacja L2 (zapobiega komunikacji STA w ramach jednego
- punktu AP
- DHCP Relay
- Obsługa L2 roaming oraz L3 roaming pomiędzy AC z tej samej grupy (klastra)

VLAN:

- Możliwość konfiguracji VLAN dla każdego SSID

Właściwości QoS:

- Wsparcie dla QoS, CoS, voice
- 802.11e, WMM
- Mapowanie IP DSCP
- 802.1p DSCP - mapowanie bezprzewodowe oparte na priorytetach Reguły ACL
- Client access rate constraint
- Maximum concurrent clients association limit
- Airtime performance protection
- Bandwidth control

System zarządzania siecią:

- IPv4/IPv6 dla SNMP
- Provision
- MAP , heat maps, & status
- Informacja o kanale, szybkość Rx/Tx, ustawienie progu i alarm
- Alarm mailowy i raport
- Statyka ruchu AP dla 2 portów Ethernet
- Lista sąsiednich punktów
- Status radia, zakres pokrycia radia, wydajność radia i raport grupowy
- Kopia zapasowa konfiguracji
- Zapis sesji STA i statystyka
- Statystyka archiwalna
- Zarządzanie grupowe

Bezpieczeństwo:

- Uwierzytelnianie 802.1X

Kierownik
Sekcji Informatycznej
WSZW Koninie
Dawid Górski

- 802.11i, WEP, WPA/WPA2 (enterprise, personal, pre-sharekey).
- Lokalne/zdalne uwierzytelnianie adresów MAC
- Uwierzytelnianie przez Captive portal
- Wykrywanie fałszywych AP, ochrona i raport
- Wykrywanie fałszywych klientów i raport
- Klasyfikacja zagrożeń bezprzewodowych i ich uszkodzenie
- Wykrywanie ataków DOS
- ACL (lista kontroli dostępu).
- Czarna lista/biała lista adresów MAC
- Wykrywanie fałszywych AP, ochrona i raport

CECHY OPROGRAMOWANIA DO ZARZĄDZANIA WLAN :

Centralny system zarządzania użytkownikami dostępny przez przeglądarkę internetową umożliwiający:

Dodawanie i edycję użytkowników sieci bezprzewodowej z możliwością określenia:

- nazwy użytkownika,
- numeru telefonu (w celu wysłania SMS z loginem i hasłem)
- numeru sali,
- daty aktywności dostępu do sieci,
- hasła (z możliwością automatycznego generowania),
- prędkości pobierania (download)
- prędkości wysyłania (upload)
- komentarza

Dodawanie i edycję użytkowników sieci dla personelu z możliwością określenia:

- nazwy użytkownika,
- adresu fizycznego urządzenia sieciowego (MAC)
- prędkość pobierania (download)
- prędkość wysyłania (upload)
- komentarza

- Rejestrację i aktywację urządzeń sieci personelu z możliwością automatycznego odczytania adresu fizycznego (MAC) urządzenia.

- Automatyczną blokadę dostępu do sieci Internet dla użytkownika i wszystkich przypisanych do niego urządzeń po przekroczeniu zdefiniowanego czasu, przekroczeniu wyznaczonej daty.

- Autoryzację użytkownika poprzez wpisanie nazwy użytkownika i hasła w przeglądarce internetowej (Captive Portal) z możliwością zatwierdzenia regulaminu/zgodny na przetwarzanie danych osobowych.

- Walidację wpisywanych danych i wyświetlanie odpowiedniego komunikatu w przypadku podania błędnych/niepełnych danych.

- Blokowanie użytkownikom (lub wybranym urządzeniom użytkownika) dostępu do sieci Internet z możliwością wyświetlenia w przeglądarce internetowej wiadomości z przyczyną tej blokady.

- Informacje o statusie pracy serwera, na którym pracuje oprogramowanie

- Przypisanie adresów IP na podstawie adresów fizycznych (MAC).

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Określenie limitu rejestrowanych urządzeń z wykorzystaniem loginu i hasła/numeru dokumentu tożsamości
- Wysłanie loginu i hasła w postaci wiadomości SMS na podany numer telefonu.
- Rejestrację urządzeń w systemie z możliwością aktywacji przez administratora (personel recepcji, rejestracji).
- Określenie prędkości pobierania oraz wysyłania zarejestrowanego użytkownika.
- Tworzenie spersonalizowanej strony powitalnej Captive Portal (grafika w postaci plików JPG, PNG, BMP oraz animacje flash bez limitu rozmiaru pliku).
- Zapis ruchu sieciowego użytkowników w sieci Internet w postaci dobowych zbiorów danych (oznaczonych datą) z możliwością udostępnienia jedynie organom władzy państwowej w ramach wskazania potencjalnego sprawcy ewentualnego przestępstwa informatycznego (dostęp do raportu zabezpieczony hasłem wysyłanym za pomocą SMS na wskazany w systemie numer telefonu)
- Dynamiczny podział dostępnego łącza polegający na przypisaniu użytkownikowi transferu z równomiernym obniżaniem prędkości pobierania / wysyłania wszystkim użytkownikom
- Monitorowanie ruchu sieciowego – podgląd z możliwością wysyłania powiadomień na SMS w przypadku awarii.
- Monitorowanie działania urządzeń sieciowych – podgląd z możliwością wysyłania powiadomień na SMS w przypadku awarii.
- Autoryzację użytkownika na poziomie punktu dostępowego sieci WLAN zgodnie ze standardem IEEE 802.1X
- Integrację z wybranymi systemami hotelowymi umożliwiającą logowanie do sieci WIFI przy pomocy numeru dokumentu tożsamości użytego podczas zameldowania.
- Wsparcie redundancji przyłącza do sieci Internet (podstawowe i zapasowe) z możliwością automatycznego przełączania w przypadku awarii jednego z nich.
- Moduł konferencji – zarządzanie nazwą i hasłem SSID aktywowanego w trybie ad hoc z poziomu panelu zarządzania oraz dynamiczne zmiany ilości i lokalizacji AP uczestniczących w rozgłaszaniu.
- Obsługa VLAN – poszczególne sieci (personel, pacjenci) pracujące w różnych VLAN-ach
- Access Point-y muszą być objęte 36 miesięczną gwarancją producenta.
- Zamawiający wymaga personalizacji oprogramowania, która ma zapewniać możliwość modyfikacji sposobu prezentacji parametrów systemu tj. statystyki eksploatacji , limity transferu, zakres wyświetlanych danych oraz stopniowanie dostępu do uprawnień , w ramach preferencji poszczególnych użytkowników.

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

8 Oprogramowanie do zarządzania infrastrukturą LAN

NMS – Network Management Software. Oprogramowanie do zarządzania siecią oraz konfiguracji urządzeń.

Funkcje MIB:

- Konfiguracja SNMP urządzenia
- Okno informacyjne i statystyczne dla MIB II
- Tabela informacyjna IF MIB
- Tabela informacyjna MIB jednostki
- Tabela konfiguracji portu oraz informacji Bridge 802.1d
- Tabela konfiguracji portu, informacje Spanning Tree
- Okna statystyki RMON, Zdarzenia oraz Historii
- 802.1p konfiguracja priorytetów wraz z GMRP oraz GARP
- 802.1Q VLAN – informacje i konfiguracja wraz z przekierowaniem / filtrowaniem oraz z unicast/multicast
- Statystyka portu VLAN
- Narzędzia L3 wraz z przekierowaniem IP, RIP2, OSPF, IP multicast, DVMRP oraz konfiguracją PIM

Zarządzanie konfiguracją:

- narzędzia MIB
- kompilator MIB
- przeglądarka MIB
- konfiguracja Web
- narzędzia DIAP
- transfer plików TFTP
- Ping
- IGMP Snooping
- SNTP
- Storm control
- QoS
- MVR
- DHCP
- IP Source Guard
- Aktualizacja masowej konfiguracji
- Masowa aktualizacja oprogramowania typu firmware

Zarządzanie błędem:

- Dziennik trapów
- Filtr trapów
- Edytor trapów

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski

- Dziennik komunikatów
- Ping
- Alarm oraz interwał
- Śledzenie trasy

Zarządzanie wydajnością:

- RMON
- mostek 802.1d
- Liczenie portów
- VLAN
- Statystyka ruchu
- Monitoring centralnego procesora
- Monitoring pamięci
- Funkcja uszczegółowienia
- Zarządzanie progiem
- Monitoring sesji
- Sprawdzanie dostępności procesu

Zarządzanie bezpieczeństwem:

- Konfiguracja SNMP urządzenia
- Konfiguracja SNMP v3
- Konfiguracja ACL
- Konfiguracja HTTPS, SSH, 802.1X itp.
- Konfiguracja autentykacji RADIUS
- Autentykacja TACACS
- Konfiguracja kont

Zarządzanie kontem:

- Aktualizacja informacji o kliencie
- Zamrożenie/odmrożenie połączenia klienta
- Kwerenda rekordu klienta
- Kwerenda klienta on-line
- Nieprawidłowa sytuacja po stronie klienta
- Zarządzanie dostępem użytkownika
- Audyt czynności klienta

Kierownik
Sekcji Informatycznej
WSZ w Koninie
Dawid Górski