

TECHNICKÁ SPECIFIKACE

UTM FireWall

- 1. 1 ks - výkonný UTM FireWall (Unified Threat Management)**
- 2. 1 ks – záruka a podpora 24x7 na 1 rok**

Minimální technické parametry:

- Statefull firewall
- Fyzické zařízení, montáž do racku, maximální rozměr 1U
- Propustnost min. 2,5 Gbps
- Podpora IPSec VPN – propustnost min. 1 Gbps (AES256), režimy gw to gw a gw to client
- Možnost vytvořit IPv4 a IPv6 vlan interface
- Podpora IPv4, IPv6
- NAT, PAT
- Podpora SSL VPN, režimy tunel mod a portál mod
- Podpora NTP, SNMPv3, Syslog
- Logování v lokálním režimu a na centrální logovací systém
- Licencování na neomezený počet uživatelů
- Funkcionalita trafic shapingu
- Funkcionalita IPS (propustnost alespoň 900 Mbps)
- Funkcionalita Antivir, Antispyware a antimalware kontroly
- Latence firewallu do 4 mikrosekund
- Funkcionalita rozeznávání aplikací na L7 vrstvě
- Funkcionalita web filteringu
- Funkcionalita routeru – podporováno statické, policy base routing, RIP, OSPF, BGP, IS-IS
- Funkcionalita Web cachingu
- Pravidelné automatické aktualizace signatur od výrobce
- Funkcionalita oddělených kontextů (min. počet šest), s oddělenou konfigurací a správci
- Možnost vytvoření více správcovských účtů, s možností vydefinování rozdílných práv (plný admin, pouze read náhled na konfiguraci, pouze přístup k logům...)
- Dedikovaný port pro management
- Počet konektorů, minimálně 16x GE RJ45, 2x 1GE SFP
- Správa přes minimálně HTTPS, SSH
- Linkový loadbalancer
- Podpora HA módu v režimech active-passive i active-active
- Integrace s AD pro SSO
- Serverový loadbalancing
- Lokální storage min. 60 GB (netočivá technologie)

Záruky a podpora:

- V režimu 24x7 včetně bezpečnostních UTM subskripcí na 1 rok.

Aktivní prvky, UPS a příslušenství

- 3. 2 ks - páteří přepínač do RD1** (požadujeme potvrdit splnění parametrů uvedených níže)
- 4. 2 ks - metalický 10G SFP+ min. 0,5m DAC kabel**

Základní technické parametry:

- Typ přepínače - L3
- Formát přepínače - Standalone, 1U
- Počet 1000/10000 SFP+ portů - 4
- Počet RJ-45 10/100/1000 portů - 24
- Počet rozšiřujících slotů - 1
- Rozšiřitelnost o min. 4x 10G SFP+ port
- Podpora redundantního napájecího zdroje (externí)

Výkonnostní parametry:

- Kapacita směrování / přepínání - 200 Gbps
- Propustnost - 150 Mpps
- Latence (64-byte pakety) - max. 4,1 µs
- Wirespeed na všech portech

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu - 8
- Sestavení stohu přes standardizované síťové rozhraní
- Stoh podporuje distribuované přepínání paketů
- Kterýkoli prvek ve stohu může být řídicím prvkem (1:N redundance)
- Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor)
- Stoh se chová jako jedno L2 zařízení z pohledu spanning tree
- Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu
- Stoh se chová jako jedno L3 zařízení (router, gateway, peer)
- Podpora stohování mezi geograficky odlišnými lokalitami, vzdálenost mezi lokalitami 10km
- Kapacita stohovacího propojení - 20 Gbit/s
- Možnost stohovat PoE/Non-PoE verze přepínačů

Funkční specifikace:

- Podpora 4094 VLAN
- MAC-based VLAN
- IP subnet-based VLAN
- Q-in-Q
- VLAN mapping (one-to-one, many-to-one)
- Podpora Multiple Spanning Tree včetně root guard a BPDU guard
- Podpora pokročilých link-layer služeb OAM dle 802.3ah (služby pro Ethernet první míle) a dle 802.1ag (detekce poruch konektivity)
- LLDP dle 802.1ab včetně rozšíření o LLDP-MED
- 32000 MAC adres dynamicky a 1024 statických záznamů
- 8000 ARP záznamů dynamických, 512 statických
- Min. 512 IP rozhraní pro VLAN (IPv4 i IPv6)
- Min. 4 sekundární IPv4/IPv6 rozhraní
- DHCP Snooping a podpora Option 82
- DNS pro IPv4 i IPv6
- Směrování RIPv2
- Směrování RIPv6
- Směrování OSPFv2
- Směrování OSPFv3
- Směrování IS-IS pro IPv4 i IPv6
- Směrování BGP4 a BGP4+
- IGMP Snooping
- Směrování multicast s PIM-DM, PIM-SM, PIM-SSM
- MLD Snooping
- Směrování multicast s PIM-DM, PIM-SM, PIM-SSM pro IPv6
- Multicast VLAN
- Multicast Source Discovery Protocol
- Podpora tunelování IPv4 over IPv6
- IPv4 i IPv6 PBR
- ECMP routing (min. 4 cesty) pro IPv4 i IPv6
- uRPF
- VRF-Lite (virtualizace směrovacích systémů)
- BFD pro statický i dynamický routing s OSPF a BGP
- 8 hardwarových výstupních front
- Podpora řízení šířky pásma na port (Line-rate) a aplikaci (CAR) na vstupu a výstupu z portu s krokem o minimální velikosti 64kbit
- Podpora vytváření ACL a klasifikace toků na Layer2-Layer4 minimálně na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/v6 adresa, číslo zdrojového/cílového portu, protokol, číslo VLAN
- Podpora přeznačkování 802.1p a DSCP priorit
- Podpora časových úseků pro aplikaci pravidel

- Možnost volby mechanismu pro obsluhu výstupních front minimálně na úrovni Strict Priority, Weighted Fair Queuing a Weighted Deficit Round Robin (SP, WRP, WFQ)
- Podpora mechanismu pro ochranu před zahlcením uvnitř výstupní fronty – Weighted Random Early Detection (WRED)
- Podpora zrcadlení skupin portů
- Podpora zrcadlení provozu na základě přístupového filtru
- Podpora více monitorujících portů současně, minimálně tří - pro připojení rozdílných analyzačních nástrojů
- Port mirroring SPAN, RSPAN, Encapsulated RSPAN
- Podpora ověřování 802.1X, minimálně 1024 ověřených uživatelů na systém
- Podpora ověřování MAC adres, minimálně 1024 ověřených MAC adres na systém
- Podpora Web Based RADIUS authentication
- Podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
- Podpora Private VLAN, Port Security, spojení ověření MAC adresy a 802.1X pro multiple host mode na jednom portu
- Podpora Guest VLAN
- Podpora IP Source Guard
- Podpora Sflow
- Podpora IPFix nebo obdobného z Netflow vycházejícího protokolu
- Podpora DoS/DDoS ochrany CPU systému
- Podpora Virtual Cable Testování a Diagnostiky optických transceiverů

Management:

- CLI formou RJ45 serial konsole port
- Zabezpečený management přepínače - SSH, SSL, SNMPv3, HTTPS
- Syslog
- Podpora RADIUS a TACACS ověřování jak pro LAN hosty, tak pro management systém
- Hierarchický management
- Podpora alarmů pro teplotu a selhání ventilátorů
- Velikost Flash pro minimálně 3 obrazy operačního systému

Záruky:

- Záruka na celý HW ve formátu NBD zajištěná výrobcem zařízení – min. 5 let.
- Přístup k novým verzím Firmware/OS bezplatně – min. pod dobu 7 let.

5. 3 ks - přístupový přepínač do RD1 (požadujeme potvrdit splnění parametrů uvedených níže)

6. 2 ks - metalický 10G SFP+ min. 0,5m DAC kabel

7. 3 ks - metalický 10G SFP+ min. 1,0m DAC kabel

Základní technické parametry:

- Typ přepínače - L2/L3 switch
- Formát zařízení kompaktní do racku
- Velikost 1U
- Počet portů 1 Gbit/s RJ45 - 48x10/100/1000 RJ45
- Počet portů 1/10 Gbit/s SFP+ - 4xSFP+ nezávislé
- Podpora PoE+ dle standardu 802.3at
- Dostupný výkon pro PoE napájení - 370 W
- Podpora redundantního napájecího zdroje (externí)
- Podpora "jumbo rámců"
- Automatické zařazování připojených tel. aparátů do voice VLAN

Výkonnostní parametry:

- Propustnost přepínacího systému - 170 Gbps
- Paketový výkon přepínače - 130 mpps
- Wirespeed (neblokující) na všech portech

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu - 8

- Sestavení stohu přes standardizované síťové rozhraní
- Stoh podporuje distribuované přepínání paketů
- Kterýkoli prvek ve stohu může být řídicím prvkem (1:N redundance)
- Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor)
- Stoh se chová jako jedno L2 zařízení z pohledu spanning tree
- Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu
- Stoh se chová jako jedno L3 zařízení (router, gateway, peer)
- Podpora stohování mezi geograficky odlišnými lokalitami, vzdálenost mezi lokalitami 10km
- Kapacita stohovacího propojení - 20 Gbit/s
- Možnost stohovat PoE/Non-PoE verze přepínačů

Funkční specifikace:

- Podpora IEEE 802.3ad
- Počet LACP skupin/linek ve skupině - 128/8
- Podpora VLAN podle IEEE 802.1Q
- Počet aktivních VLAN - 4 000
- Počet záznamů v tabulce MAC adres - 16 000
- Protokol-based VLAN
- MAC-based VLAN
- Private VLAN
- Protokol pro definici šířených VLAN - MVRP
- IEEE 802.1s - Multiple spanning tree
- IEEE 802.1w - Rapid spanning Tree
- Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení - CDP nebo LLDP
- Podpora LLDP-MED
- Tunelování 802.1Q v 802.1Q
- OAM na Ethernetu - 802.3ah, 802.1ag
- DHCP server pro IPv4 a IPv6
- DHCP relay pro IPv4 a IPv6
- DHCP klient pro IPv4 a IPv6
- DNS klient
- NTP
- Statické směrování IPv4 a IPv6
- RIPv2 a RIPv6
- Policy based routing na základě ACL pro IPv4 a IPv6
- IGMP snooping v2 a v3
- MLD snooping
- IPv4 a IPv6 multicast VLAN
- Hardware podpora IPv4 a IPv6 ACL
- ACL klasifikace na základě zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/v6 adresa, číslo zdrojového/cílového portu, protokol
- BPDU guard
- Root guard
- DHCP snooping pro IPv4 a IPv6
- DHCP paket rate limit
- HW ochrana proti zahlcení (broadcast/multicast/ unicast) nastavitelná na procentuální rychlost portu a množství paketů za vteřinu
- Port mirroring SPAN, RSPAN
- Podpora ověřování 802.1X - 2048 ověřených uživatelů na systém
- Podpora ověřování MAC adres - 1000 ověřených MAC adres na systém
- Podpora zařazování do VLAN, přidělení QoS a ACL na základě 802.1X ověření
- 802.1X s podporou odlišných Guest VLAN, Fail VLAN a Critical VLAN
- IP source Guard pro IPv4 a IPv6
- Podpora Source Address Validation pro IPv6 s využitím informací obsažených v DHCPv6 a SLAAC
- Hardware podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front - 8
- Podpora traffic shaping, GTS a policing
- Podpora Sflow
- Podpora control plane policing (CoPP)

Management:

- CLI formou RJ45 serial konsole port
- Zabezpečený management přepínače - SSH, SSL, SNMPv3, HTTPS
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Syslog
- Podpora RADIUS a TACACS ověřování jak pro LAN hosty, tak pro management systému
- Podpora Netconf
- Podpora OpenFlow v1.3

Záruky

- Záruka na celý HW ve formátu NBD zajištěná výrobcem zařízení - min. 5 let.
- Přístup k novým verzím Firmware/OS bezplatně – min. pod dobu 7 let.

8. 1 ks - přístupový přepínač do RD2 (požadujeme potvrdit splnění parametrů uvedených níže)

9. 4 ks - optický 10G SFP+ LC SR transceiver (2 ks do páteřních prvků)

10. 4 ks - optický propojovací kabel 2m (LC/SC)

Základní technické parametry:

- Typ přepínače - L2/L3 switch
- Formát zařízení kompaktní do racku
- Velikost 1U
- Počet portů 1 Gbit/s RJ45 - 24x10/100/1000 RJ45
- Počet portů 1/10 Gbit/s SFP+ - 4xSFP+ nezávislé
- Podpora PoE+ dle standardu 802.3at
- Dostupný výkon pro PoE napájení - 370 W
- Podpora redundantního napájecího zdroje (externí)
- Podpora "jumbo rámců"
- Automatické zařazování připojených tel. aparátů do voice VLAN

Výkonnostní parametry:

- Propustnost přepínacího systému - 120 Gbps
- Paketový výkon přepínače - 90 mpps
- Wirespeed (neblokující) na všech portech

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu - 8
- Sestavení stohu přes standardizované síťové rozhraní
- Stoh podporuje distribuované přepínání paketů
- Kterýkoli prvek ve stohu může být řídicím prvkem (1:N redundancy)
- Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor)
- Stoh se chová jako jedno L2 zařízení z pohledu spanning tree
- Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu
- Stoh se chová jako jedno L3 zařízení (router, gateway, peer)
- Podpora stohování mezi geograficky odlišnými lokalitami, vzdálenost mezi lokalitami 10km
- Kapacita stohovacího propojení - 20 Gbit/s
- Možnost stohovat PoE/Non-PoE verze přepínačů

Funkční specifikace:

- Podpora IEEE 802.3ad
- Počet LACP skupin/linek ve skupině - 128/8
- Podpora VLAN podle IEEE 802.1Q
- Počet aktivních VLAN - 4 000
- Počet záznamů v tabulce MAC adres -16 000
- Protokol-based VLAN
- MAC-based VLAN
- Private VLAN
- Protokol pro definici šířených VLAN - MVRP
- IEEE 802.1s - Multiple spanning tree
- IEEE 802.1w - Rapid spanning Tree
- Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)

- Detekce protilehlého zařízení - CDP nebo LLDP
- Podpora LLDP-MED
- Tunelování 802.1Q v 802.1Q
- OAM na Ethernetu - 802.3ah, 802.1ag
- DHCP server pro IPv4 a IPv6
- DHCP relay pro IPv4 a IPv6
- DHCP klient pro IPv4 a IPv6
- DNS klient
- NTP
- Statické směrování IPv4 a IPv6
- RIPv2 a RIPv6
- Policy based routing na základě ACL pro IPv4 a IPv6
- IGMP snooping v2 a v3
- MLD snooping
- IPv4 a IPv6 multicast VLAN
- Hardware podpora IPv4 a IPv6 ACL
- ACL klasifikace na základě zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/v6 adresa, číslo zdrojového/cílového portu, protokol
- BPDU guard
- Root guard
- DHCP snooping pro IPv4 a IPv6
- DHCP paket rate limit
- HW ochrana proti zahlcení (broadcast/multicast/ unicast) nastavitelná na procentuální rychlost portu a množství paketů za vteřinu
- Port mirroring SPAN, RSPAN
- Podpora ověřování 802.1X - 2048 ověřených uživatelů na systém
- Podpora ověřování MAC adres - 1000 ověřených MAC adres na systém
- Podpora zařazování do VLAN, přidělení QoS a ACL na základě 802.1X ověření
- 802.1X s podporou odlišných Guest VLAN, Fail VLAN a Critical VLAN
- IP source Guard pro IPv4 a IPv6
- Podpora Source Address Validation pro IPv6 s využitím informací obsažených v DHCPv6 a SLAAC
- Hardware podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front - 8
- Podpora traffic shaping, GTS a policing
- Podpora Sflow a IPFix
- Podpora control plane policing (CoPP)

Management:

- CLI formou RJ45 serial konsole port
- Zabezpečený management přepínače - SSH, SSL, SNMPv3, HTTPS
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Syslog
- Podpora RADIUS a TACACS ověřování jak pro LAN hosty, tak pro management systému
- Podpora Netconf
- Podpora OpenFlow v1.3

Záruky:

- Záruka na celý HW ve formátu NBD zajištěná výrobcem zařízení - min. 5 let.
- Přístup k novým verzím Firmware/OS bezplatně – min. pod dobu 7 let.

11. 1 ks - UPS do RD1

Základní technické parametry:

- UPS o výstupním výkonu min. 2,2 kVA a v provedení on-line s dvojitou konverzí.
- Montáž do racku 19", velikost max. 2U, max. hloubka 700 mm.
- Automatický bypass.
- Baterie vyměnitelné za provozu bez nutnosti demontáže UPS a vypínání systémů.
- Vstup jednofázový 230V, jištění max. 16A (C)
- Vzdálený management, RJ-45 10/100 Base-T, SNMP, Telnet, HTTP.
- Monitorovací a shutdown software pro VMware a Hyper-V, Windows, Linux.

- Výstupní zásuvky 8× IEC C13 (10A) a 1× IEC C19 (16A).

Záruky:

- Záruka na celý HW - min. 2 roky.

12. 1 ks - UPS do RD2

Základní technické parametry:

- UPS o výstupním výkonu min. 1 kVA a v provedení on-line s dvojitou konverzí.
- Montáž do racku 19", velikost max. 2U, max. hloubka 450 mm.
- Automatický bypass.
- Baterie vyměnitelné za provozu bez nutnosti demontáže UPS a vypínání systémů.
- Vstup jednofázový 230V, jištění max. 16A (C).
- Vzdálený management, RJ-45 10/100 Base-T, SNMP, Telnet, HTTP.
- Monitorovací a shutdown software pro VMware a Hyper-V, Windows, Linux.
- Výstupní zásuvky 6× IEC C13 (10A).

Záruky:

- Záruka na celý HW - min. 2 roky.

13. Software pro management a monitoring sítě

Základní technické parametry:

- Management nástroj pro správu sítě s podporou správy produktů výrobce a nejméně jednoho dalšího světového dodavatele networking řešení.
- Správa min.40 síťových zařízení (např. přepínačů).
- Management Multiprotocol Label Switching (MPLS) VPN.
- Manuální a automatické discovery síťových zařízení.
- Možnost tvorby SNMP, TELNET a SSH šablon pro hromadný přístup k zařízením.
- Definice přístupových práv pro jednotlivé operátory na úrovni síťových zařízení a jejich funkcí
- Vizualizace topologie: Layer-2, Layer-3 a spanning tree, možnost tvorby vlastních hierarchických pohledů.
- Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel.
- Performance management síťových zařízení: dostupnost zařízení i linek, vytížení procesoru, využití operační paměti, vytížení linek.
- Performance management pro libovolné SNMP statistiky, dlouhodobou historii i real-time grafy.
- Importování vlastních MIB a kompilátor.
- Podpora SYSLOG.
- VLAN management: změna nastavení, přidávání, přiřazení portů.
- ACL management: ACL šablony, optimalizační nástroje, zálohování a deployment.
- Alarmování, práce se syslog a SNMP trapy včetně vytváření vlastních reakcí na události nebo notifikace ve formě emailu či SMS.
- Audit zařízení: typ zařízení včetně jednotlivých komponent, verze operačního systému, sériová čísla, informace o jednotlivých portech, historický audit jednotlivých zařízení (např. přesuny).
- Vyhledávání a historie zařízení na základě MAC, IP nebo názvu.
- Možnost rozšíření o API postavené na XML volání (RESTful nebo SOAP) pro možnost integrace do aplikací třetích stran.
- Všechny zásuvné moduly musí umožňovat centrální řízení z jedné aplikace.
- Podpora vysoké dostupnosti software, možnost běhu v clusteru.

14. Instalační práce, konfigurace a zprovoznění

Součástí dodávky firewallu, aktivních prvků, UPS a příslušenství je:

- Analýza stávajícího stavu sítě – fyzická a logická topologie, virtuální LAN, IP adresní plán, spanning tree, propojení do sítě operačního střediska ZZS, WAN linky atd.
- Zpracování implementačního dokumentu, který bude obsahovat:
 - Návrh úpravy topologie sítě s novými aktivními prvky.
 - Zadavatelem odsouhlasený návrh změny adresního plánu a logické topologie sítě s cílem dosažení optimální segmentace sítě z pohledu bezpečnosti a zpřehlednění správy sítě.
 - Návrh základní konfigurace redundance v síti včetně nastavení Spanning tree.
 - Návrh propojení s operačním střediskem ZZS odsouhlasený zadavatelem.
 - Zadavatelem odsouhlasený harmonogram implementace, který bude respektovat možnosti zadavatele z pohledu případných odstávek provozu sítě nebo její části.
- Fyzická montáž aktivních prvků, firewallu a napájecích zdrojů do rozvaděčů (LAN prvky, UPS), kabelové propojení.
- Propojení na nově vybudovanou strukturovanou kabeláž zakončenou v nových patchpanelech.
- Základní konfigurace firewallu a oživení.
- Základní implementace firewall politik podle konfigurace stávajícího firewallu Mikrotik zrevidované společně se zadavatelem dle aktuálních požadavků.
- Integrace firewallu do domény (MS AD) zadavatele, aby bylo možné firewall politiky řídit dle skupin a uživatelů
- Případná implementace bezpečného propojení s LAN operačního střediska ZZS.
- Zprovoznění a konfigurace aktivních prvků a jejich plná integrace do stávající infrastruktury zadavatele (včetně L3, ACL, QoS apod.).
- Základní implementace nových aktivních prvků včetně nastavení požadovaných virtuálních clusterů, implementace základních best practices bezpečnostních nastavení.
- Zprovoznění a konfigurace UPS.
- Migrace a úprava stávající konfigurace (stávající přepínače Zyxel – viz schéma v Příloze X).
- Implementaci dílčích změn na úrovni zvýšení redundance propojení serverového segmentu sítě za dvěma Cisco 2960 přepínači připojením druhé redundantní uplink trasy.
- Provedení přepojení stávající LAN a serverové infrastruktury na nově instalovanou v rámci odsouhlaseného okna odstávky provozu.
- Implementace management a monitoring SW, integrace nově dodaných aktivních prvků a stávajících, které to umožňují.
- Provedení funkčních testů a testů redundance, případně doladění firewall pravidel.
- Zpracování dokumentace s uvedením podstatných informací (schéma, IP adresní plán, adresace jednotlivých zařízení, informace k integraci firewallu s doménou, způsoby managementu, atd.).
- Zaškolení obsluhy.