Technická specifikace

Požadovaný budoucí stav

Navržený budoucí stav sítě reflektuje požadavky na modernizaci, zajištění provozní stability a rozšíření funkcionality síťové infrastruktury. Klíčové charakteristiky zahrnují:

- Navýšení propustnosti sítě - Infrastruktura bude navržena s důrazem na dostatečnou kapacitu páteřních i přístupových prvků tak, aby byla zajištěna rezervní kapacita pro růst provozu, náročnější aplikace a minimalizace latencí.
- Podpora stávajícího dohledového systému HPE IMC - Nové síťové prvky budou plně kompatibilní se systémem HPE Intelligent Management Center (IMC) včetně podpory SNMP, CLI skriptování a integrace s existující topologií a sledováním dostupnosti.
- Podpora exportu síťových toků (flow) - Síť bude podporovat technologie typu NetFlow/sFlow/IPFIX pro export síťových toků do nástroje pro analýzu provozu. Tato funkcionalita umožní efektivní identifikaci anomálií, neobvyklého provozu a kybernetických hrozeb.
- Podpora vysoké dostupnosti - Architektura sítě bude navržena s ohledem na eliminaci single points of failure. Pomocí redundance síťových prvků, záložních napájecích zdrojů a vícecestného směrování bude zajištěna vysoká dostupnost služeb a odolnost vůči výpadkům.

Potvrzení o pětileté záruce

Součástí předávacích protokolů bude písemné potvrzení od výrobce dodávaných technologií, že na předmět plnění byla u výrobce zakoupena minimálně 5 letá rozšířená záruka výrobce s dobou opravy/výměny následující pracovní den s možností hlásit závadu 8 hodin denně v pracovní dny (označovaná zpravidla jako 8x5xNBD) platná od data zahájení implementace. Tato záruka musí být poskytována na místě instalace pracovníky výrobce nebo dodavatele.

Potvrzení o určení zboží pro koncového zákazníka

V databázi výrobce dodávaných technologií musí být zadavatel veden jako první uživatel dodávaného zboží a souvisejících licencí/subskripcí/operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh. Před převzetím zboží si zadavatel vyhrazuje právo kontroly dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než zadavatel, bude se jednat o porušení podmínky originálního a nového zařízení. Za účelem ověření těchto parametrů vybraný dodavatel na vyžádání před dodáním zboží předloží prohlášení výrobce dodávaného zařízení či jeho oficiálního zastoupení o tom, že na dodávané zboží zadavateli jako koncovému zákazníkovi bude poskytnuta k dodávanému zařízení záruka výrobce v plném výrobcem poskytovaném rozsahu. Účastník do své nabídky vloží **čestné**

prohlášení deklarující, že: „*veškeré dodávané HW a SW produkty budou získány legálně, zadavatel jako koncový zákazník bude prvním uživatelem dodaného zboží a licencí/subskripcí/operačních systémů v souladu s distribučními a licenčními podmínkami výrobce zařízení a na tyto produkty bude umožněna záruka a podpora výrobce v plném rozsahu jménem zadavatele - zadavatel jako koncový zákazník nesmí být nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaného zařízení a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje*“.

Minimální požadavky na záruku a služby

Na všechny části dodávané síťové infrastruktury je vyžadována záruka a záruční servisní podpora následujícího rozsahu (pokud není u konkrétního prvku uvedeno jinak):

Požadované parametry
Záruka a záruční podpora výrobce v úrovni 8x5xNBD – Minimálně 5 let
Součástí záruky musí být přímý přístup zadavatele k technické podpoře výrobce zařízení – Minimálně 5 let
Přístup k bezpečnostním opravám SW a HW po dobu životnosti dodaných prvků – Minimálně 5 let.
Přístup k aktualizaci software a firmware pro dodané prvky po dobu životnosti dodaných prvků – Minimálně 5 let.

Minimální technické požadavky

Distribuční MAN přepínač 4 kusy

Požadavek na funkcionalitu
Základní vlastnosti
Typ zařízení: L3 přepínač- modulární chassis
Maximální velikost zařízení: 7U
Počet slotů pro linkové karty: 5
Minimálně 96x 1/10/25Gbps portů s volitelným fyzickým rozhraním
Minimálně 48x 10/100/1000Mbit RJ45 metalických portů s podporou PoE Class 4
Možnost rozšíření o linkové karty s podporou 10GBASE-T SFP+ portů
Všechny dostupné ethernet interface jsou plně propustné – neblokující porty

Interní redundantní AC hot-swap napájecí zdroje
Možnost rozšíření o další napájecí zdroje pro vyšší míru redundance nebo vyšší PoE výkon (nebo výměna za silnější zdroje)
Redundantní management jednotku/supervisor
Redundantní hot-swap ventilátory
Podpora PoE+ dle standardu 802.3at a Enhanced PoE dle standardu 802.3bt
Minimální dostupný výkon pro PoE+ napájení 1440W s možností rozšíření minimálně na 7200W
Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače
Podpora Energy Efficient Ethernet (802.3az)
Minimální přepínací výkon: 14 Tbps
Minimální paketový výkon: 5,7 Bpps
Minimální paketový buffer: 16 MB per linková karta
Podporovaný počet přepínačů ve stohu: 2
Minimální kapacita stohovacího propojení: 50 Gbps
Stoh podporuje distribuované přepínání paketů
Libovolný prvek stohu může být řídícím prvkem (1:1 redundance)
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)
Podpora upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade)
Podpora automatizace upgrade OS ve stohu bez narušení provozu přes REST API
KeepAlive mezi členy stohu přes OOB port
Funkce a protokoly
Podpora jumbo rámců včetně velikosti 9198 Byte
Podpora linkové agregace IEEE 802.1AX
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
Minimální počet LACP skupin/linek ve skupině: 256/8
Minimální počet záznamů v tabulce MAC adres: 32 000
Minimální počet záznamů v tabulce ARP: 49 000
Protokol pro definici šířených VLAN: MVRP
Minimálně 4000 aktivních VLAN podle IEEE 802.1Q
Tunelování 802.1Q v 802.1Q
VLAN translace - swap 802.1Q tagů na trunk portu

Podpora zařazování do VLAN podle standardu 802.1v
Private VLAN včetně primary, secondary a community VLAN
Podpora VLAN-group pro rozkládání klientů přes více VLAN ID
IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích
Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port
Podpora LLDP-MED
Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)
DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF
Podpora zapouzdření: GRE over IPv4
Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
Podpora NTP server
Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety
Podpora L3 routed port včetně L3 sub-interface - nadřazené L3 rozhraní lze rozdělit
Podpora forward error correction (FEC)
Statické směrování IPv4 a IPv6
Minimální počet IPv4 záznamů ve směrovací tabulce: 61 000
Minimální počet IPv6 záznamů ve směrovací tabulce: 61 000
Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP
Funkce BGP konfederace a route reflector pro IPv4 a IPv6
Podpora BGP MD5 autentizace a BGP TTL security
Podpora police based routing
Podpora VRRPv2 a VRRPv3
Podpora route map
ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4
Podpora minimálně 100 virtuálních směrovacích instancí (VRF)
IGMP v2 a v3, IGMP snooping
MLD v1 a v2, MLD snooping
Směrování multicast: PIM-DM, PIM-SM, PIM-BIDIR, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP

Možnost zadávat statické multicast routy
PIM-SSM source group mapping
Hardware podpora IPv4 a IPv6 ACL
ACL definice na základě skupiny fyzických portů
IN a OUT ACL aplikovatelný na interface, LAG, VLAN
DHCP snooping pro IPv4 a IPv6
HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps
IEEE 802.1p – Minimálně 8 front
Předcházení zahlcení pomocí mechanismu WRED
802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN
Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely
Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace
Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace
Tunelování uživatelského provozu - schopnost izolovat více koncových zařízení na jednom portu
Přiřazení koncového zařízení do tunelu/Overlay na základě výsledku autorizace
Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL
Monitoring síťových otisků DHCP, HTTP, CDP, LLDP zařízení a jejich přenos na RADIUS server
Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard
IP source guard / dynamic IP lockdown
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
BPDU guard a Root guard
Podpora statických a dynamických VXLAN s využitím BGP-EVPN
Podpora Group based policy pro VXLAN (VXLAN GBP)
Podpora VXLAN přes IPv6 (underlay)
Podpora MPLS L3 VPN

Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači
Možnost instalace vlastního certifikátu včetně podpory automatizované instalace např. Enrollment over Secure Transport (EST)
TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem
Podpora Radius over TLS (RadSec)
Možnost nastavit různou skupinu RADIUS serverů na různé porty
Podpora autentizace z Cloud prostředí včetně RadSec pro Cloud autentizaci
Podpora RADIUS CoA (RFC3576)
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5
Možnost rozšíření o rozpoznávání aplikací, podpora pro rozpoznávání minimálně 3000 aplikací
Možnost rozšíření o monitorování konkrétního provozu přímo na přepínači
Možnost rozšíření o zobrazení minimálně 10 nejvíce komunikujících klientů přímo na přepínači
Podpora Containeru na přepínači
Možnost rozšíření o monitorování zpoždění klientské komunikace: autentizace, DNS a DHCP
Management
CLI formou console port
Konfigurace zařízení v člověku čitelné textové formě
OoB management formou portu RJ45 s podporou ethernetu
USB port pro přenos konfigurace a firmware
Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient
Možnost nastavit vlastní port pro SSHv2 server
Podpora RSA s délkou klíče minimálně 4096 bitů
Podpora SNMPv2c a SNMPv3
Podpora filtrování SNMP trap
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
Lokálně vynucené RBAC na úrovni přepínače
Podpora aktualizací běžícího software bez nutnosti restartovat systém - Hot-Patching
Dvou-faktorová autentizace minimálně pro přihlášení na ssh a WebGUI

Dualní flash image - podpora dvou nezávislých verzí operačního systému
Možnost využití přepínače jako lokálního distribučního zdroje operačního systému na další přepínače v síti
Podpora upgrade OS přepínače bez narušení provozu (ISSU/Live upgrade)
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)
Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů - možnost vynášení stavu monitorovaných metrik do grafů atp.
Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 30 GB
Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress
Export síťového provozu formátem IPFIX
Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
IP SLA pro měření dostupnosti a zpoždění provozu VoIP - režim responder i probe
Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
Podpora REST API v režimech read-only a read-write pro automatizaci nastavení
Podpora Cloud based management
Podpora Zero Touch Provisioning (ZTP)

Distribuční a Centrální LAN přepínač 4 kusy

Požadavek na funkcionalitu
Základní vlastnosti
Typ zařízení: L3 přepínač
Maximální velikost zařízení: 1U
Minimálně 24x 1/10Gbps portů s volitelným fyzickým rozhraním

Minimálně 4 porty s volitelným fyzickým rozhraním s podporou minimálních rychlostí 1/10/25/50Gbps
Podpora originálních transceiverů výrobce: 10GBASE-T SFP+
Redundantní interní AC napájecí zdroj za běhu vyměnitelný
Minimální přepínací výkon: 780 Gbps
Minimální paketový výkon:580 Mpps
Minimální paketový buffer: 16 MB
Minimální počet přepínačů ve stohu: 2
Minimální kapacita stohovacího propojení: 200 Gbps
Stoh podporuje distribuované přepínaní paketů
Podpora stohu na delší vzdálenost minimálně 100m
Redundance řídícího prvku v rámci stohu
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)
Podpora jumbo rámců včetně velikosti 9198 Byte
Podpora linkové agregace IEEE 802.1AX
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
Minimální počet LACP skupin/linek ve skupině: 54/8
Podpora LACP Fallback (např. pro PXE boot)
Minimální počet záznamů v tabulce MAC adres: 32 000
Minimální počet záznamů v tabulce ARP: 49 000
Protokol pro definici šířených VLAN: MVRP
Minimálně 1024 aktivních VLAN podle IEEE 802.1Q
Tunelování 802.1Q v 802.1Q
VLAN translace - swap 802.1Q tagů na trunk portu
Podpora zařazování do VLAN podle standardu 802.1v
Private VLAN včetně primary, secondary a community VLAN
IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích
Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port
Podpora LLDP-MED

Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)
DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF
Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
Podpora NTP server
Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety
Podpora L3 routed port a IP unnumbered interface
Statické směrování IPv4 a IPv6
Minimální počet IPv4 záznamů ve směrovací tabulce: 24 000
Minimální počet IPv6 záznamů ve směrovací tabulce: 12 000
Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP
Funkce BGP konfederace a route reflector pro IPv4 a IPv6
Podpora police based routing
Podpora VRRPv2 a VRRPv3
Podpora route map
ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4
Podpora minimálně 60 virtuálních směrovacích instancí (VRF)
Podpora BFD pro: OSFP,OSPFv3, BGP IPv4, BGP IPv6, PIM, PIM6
IGMP v2 a v3, IGMP snooping
MLD v1 a v2, MLD snooping
Směrování multicast: PIM-DM, PIM-SM, PIM-SSM, PIM BIDIR, PIMv6-SM, PIMv6-SSM, MSDP
Hardware podpora IPv4 a IPv6 ACL včetně podpory object group pro IP adresy a porty
ACL definice na základě skupiny fyzických portů
IN a OUT ACL aplikovatelný na interface, LAG, VLAN, SVI
DHCP snooping pro IPv4 a IPv6
HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps
802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN

802.1X a MAC ověřování pomocí odlišných RADIUS serverů aplikované na různé skupiny portů
Podpora persistentní paměti pro 802.1x kritické role
Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely
Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace
Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace
Tunelování uživatelského provozu - schopnost izolovat více koncových zařízení na jednom portu
Přiřazení koncového zařízení do tunelu/Overlay na základě výsledku autorizace
Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL
Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard
IP source guard / Dynamic IP lockdown
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
BPDU guard a Root guard
HW a SW podpora VXLAN
Podpora Group based policy pro VXLAN (VXLAN GBP)
Podpora static a dynamic VXLAN s využítím BGP-EVPN
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači
Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST)
TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem
Podpora Radius over TLS (RadSec)
Možnost nastavit různou skupinu RADIUS serverů na různé porty
Podpora RADIUS CoA (RFC3576)
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5
QoS ochrana před zahlcením WRED
Minimálně 8 front pro IEEE 802.1p
Podpora Forward Error Correction
Možnost rozšíření o monitorování zpoždění klientské komunikace: autentizace, DNS a DHCP

CLI formou console port
Podpora bluetooth sériové konzole
Konfigurace zařízení v člověku čitelné textové formě
Konfigurace interfaců pomocí šablon
OoB management formou portu RJ45 s podporou ethernetu
USB port pro přenos konfigurace a firmware
Přepínač je možné nastavit jako distribuční bod pro upgrade OS
Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient
Dvou-faktorová autentizace pro SSH a WebGUI přihlášení
Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DH s klíčem 3072bit a vyšší
Podpora SNMPv2c a SNMPv3
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
Možnost nastavit vlastní SSH server port
Lokálně vynucené RBAC na úrovni přepínače pro administrátory
Podpora aktualizací běžícího software bez nutnosti restartovat systém - Hot-Patching
Podpora pro bezvýpadkový upgrade přepínačů ve stacku (ISSU)
Dualní flash image - podpora dvou nezávislých verzí operačního systému
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
Podpora SYSLOG over TLS
Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači
Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)
Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů - možnost vynášení stavu monitorovaných metrik do grafů atp.
Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 30 GB
Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress

Analýza síťového provozu IPFIX
Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
IP SLA pro měření dostupnosti a zpoždění provozu VoIP - režim responder i probe
Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů
Podpora Cloud i On-Premise management software výrobce zařízení
Podpora Zero Touch Provisioning (ZTP)

Firewall nové generace (1. Cluster)

Parametr	**Požadovaná hodnota (minimální)**
Provedení	1U rack
Min počet portů (s podporou HW akcelerace)	8x 10G SFP+, 10x 1G RJ45, 6x 1G SFP, dedikované 2x HA porty, 1x mgmt port, 1x konzolový port
Propustnost FW pro packet velikosti 512B UDP protokol	120 Gbps
IPS propustnost	12 Gbps
NGFW propustnost	10 Gbps
Počet souběžných session (TCP)	7 Milionů
Počet nových session /sekundu (TCP)	500 000
Počet FW pravidel	20 000
Propustnost IPSEC	50 Gbps
Propustnost SSLVPN	4 Gbps
Souběžní uživatelé u SSLVPN	2 000

Podpora linkové agregace	Min. 4 LACP
TPM	Integrované řešení
Napájení	2x AC napájení, redundantní zdroj je součástí
Počet boxů	2

Firewall nové generace (2. Cluster)

Parametr	**Požadovaná hodnota (minimální)**
Provedení	1U rack
Min počet portů (s podporou HW akcelerace)	2x 10G SFP+, 4x 1G SFP, 10x 1G RJ45, dedikované 2x HA porty, 1x mgmt port, 1x konzolový port
Propustnost FW pro packet velikosti 512B UDP protokol	12 Gbps
IPS propustnost	2 Gbps
NGFW propustnost	1,5 Gbps
Počet souběžných session (TCP)	1 Milion
Počet nových session /sekundu (TCP)	50 000
Počet FW pravidel	8 000
Propustnost IPSEC	10 Gbps
Propustnost SSLVPN	1 Gbps
Souběžní uživatelé u SSLVPN	400
Podpora linkové agregace	Min. 4 LACP
Napájení	2x AC napájení, redundantní zdroj je součástí
Počet boxů	2

Společné funkce pro oba FW clustery

Parametr	Požadovaná hodnota (minimální)
Podpora standardů	802.1Q, s-flow
Podpora VLAN	Min. 1024 VLAN
Režimu clusteru	Active-Active, Active-Standby
Konfigurační rozhraní	Konfigurační rozhraní je integrované do nabízeného NGFW zařízení a to jak v grafické podobě dostupné pomocí HTTPS, tak i SSH CLI bez licenčního omezení na počet administrátorů. SSH CLI rozhraní umožňuje plnou administraci zařízení.
Virtualizace firewallu	Možnost logické segmentace zařízení s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.
IPv6	Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46
Identita uživatelů	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
Identita uživatelů	Možnost předávání známých identit mezi oběma NGFW clustery
VPN	Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.
Management a vzdálená správa	SSH, webmanagement, console
2FA	Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů
Dynamický Routing	Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6

Policy based routing	Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)
Dodávané transceivery	4x 10G MM BiDi (1330nm TX/ 1270mm RX)
Security funkce	IPS/IDS, WebFilter, Antivirus, hloubková inspekce
Antivirus	Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
Antimallware	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení, detekce komunikace do sítí typu botnet, podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu
IPS	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury
Webfilter	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy, GeoIP databáze, data a času
DDOS	funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně zpracovávat před jeho zahozením
SSL inspekce	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
Podpora security funkcí	Na 5 let
Podpora HW boxu	5 let na nabízené zařízení funguje v režimu 24/7 a je součástí nabízeného zařízení

Uložiště pro logy z obou FW clusterů

Parametr	**Požadovaná hodnota (minimální)**
provedení	Fyzický box nebo VM

účel	Musí se jedna o centrální logovací prvek pro všechny NGFW firewally
kompatibilita	Možnost nativní integrace s poptávaným zařízením typu NGFW viz. FW clustery, které bude sloužit jako zdroj dat pro analýzu
GUI	Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy
Náhledy logů	Realtime a historický náhled do logů
Náhledy logů	Obsahuje náhledy pro zobrazení IP adres s největším objemem přenesených dat, nejčastěji používané cílové IP adresy a aplikace
Reporting	Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF
Reporting	Generování reportů v pravidelných intervalech
Počet GB logů za den	10 GB
Celková velikost uložiště	Alokovatelná disková kapacita je alespoň 1TB
Podporovaná virtualizační platforma	VmWare
Uživatelská přístupnost	Plnohodnotná správa pomocí grafického rozhraní a CLI
Podpora u výrobce	5 let v režimu 24x7 na systém i konfiguraci je součástí nabídky