Požadované technické parametry dodávky

Předmětem plnění veřejné zakázky je dodávka **vysoce dostupné sestavy firewallu nové generace (NGFW) a systému pro zpracování a korelaci logů** dle technických podmínek uvedených níže.

Tabulka povinných požadavků pro firewall nové generace (požadovány 2 ks)

Požadavky na funkcionalitu	**Minimální požadavky**
Typ zařízení	NGFW (Next-Generation Firewall) – pravidla a politiky musí být možné vytvářet jednoduše a intuitivně v grafickém prostředí využíváním objektů aplikace, uživatel/skupina, počítač apod.
Formát zařízení	Hardwarová appliance
Vysoká dostupnost/High Availability	V režimech active/passive i active/active na L2 vrstvě bez dalších nákladů
Minimální počet a typ rozhraní 40/100G	4, QSFP+/QSFP28
Minimální počet a typ rozhraní 1/10/25G	8, SFP/SFP+/SFP28
Minimální počet a typ rozhraní pro vzájemné propojení zařízení v režimu vysoké dostupnosti	2, SFP+
Minimální počet a typ rozhraní vyhrazených pro vzdálený management	2, RJ45
Požadovaný počet a typ 100G transceiverů	2, 100G QSFP28 aktivní optický kabel (AOC), délka 7 m, kompatibilní s dodaným hardware i s přímo připojeným stávajícím zařízením
Požadovaný počet a typ 25G transceiverů	2, 25G SFP28 aktivní optický kabel (AOC), délka 7 m, kompatibilní s dodaným hardware i s přímo připojeným stávajícím zařízením 4, 25GBase-LR, SFP28, 10 km, DDM
Požadovaný počet a typ 25G transceiverů pro přímo připojená stávající zařízení	4, 25GBase-LR, SFP28, 10 km, DDM
Redundantní napájecí AC zdroje	ano
Napájecí zdroje vyměnitelné za chodu	ano
Podporované funkce	
Provoz zařízení v režimu L3 (směrování)	ano
Provoz zařízení v režimu L2 (přepínání nebo transparentní) při zachování všech relevantních kontrol provozu	ano
Podpora stateful failover	ano
Směrování pro IPv4 a IPv6 s akcelerací v hardware	ano
Statické i dynamické směrování pro IPv4 (OSPF, BGP)	ano
Statické i dynamické směrování pro IPv6 (OSPFv3, MP-BGP)	ano
Podpora multicast PIM (dense i sparse mód), Source-Specific Multicast (SSM), IGMPv2/3	ano

Podpora multicast IPv6 (dense i sparse mód), Source-Specific Multicast (SSM), MLDv1/2	ano
Podpora Policy-based routing	ano
Podpora vytváření logicky oddělených instancí virtuálních směrovacích tabulek (obdoba VRF-Lite), může být nahrazena funkcionalitou virtuálních instancí firewallů	ano
Podpora virtuálních instancí firewallu – plná funkcionalita jednotlivých virtuálních firewallů	ano
Počet virtuálních instancí firewallu	10
Podpora překladu adres Static/Dynamic NAT, PAT, Source/Destination NAT	ano
Podpora protokolu IPv6 pro management, IPv6 tunnelling, firewalling, NAT46, NAT64, IPv6 IPSec VPN	ano
Podpora minimálně 1000 VLAN	ano
Podpora IEEE 802.1Q	ano
Podpora QoS pro IPv4 a IPv6	ano
Podpora prioritizace provozu na aplikační úrovni (7. vrstva)	ano
Podpora Link Aggregation IEEE 802.3ad/LACP	ano
Vytváření bezpečnostních zón (Zone-based firewall)	ano
Integrace s Active Directory – řízení, monitoring a reporting dle uživatelů nezávisle na využívané stanici (IP)	ano
VPN koncentrátor	
Vytváření LAN-to-LAN IPSec VPN v transportním i tunelovacím módu	ano
Podpora tunelování provozu pomocí technologie GRE	ano
Podpora vzdáleného přístupu pro uživatele pomocí IPSec VPN a SSL VPN	ano
Podpora SSL VPN vzdáleného přístupu na platformách MS Windows, Apple macOS, Linux a mobilních platformách Android, Apple a Windows	ano
Podpora autentizace a autorizace uživatelů pomocí MS Active Directory/LDAP, RADIUS, lokální databáze	ano
Ověřování VPN uživatelů jménem a heslem	ano
Ověřování VPN uživatelů osobním certifikátem	ano
Aplikační firewall	
Funkce rozpoznávání populárních síťových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, aplikace rozděleny do přehledných kategorií	ano
Pravidelná automatická aktualizace signatur aplikací výrobcem bez nutnosti upgrade OS	ano
Možnost vytvářet signatury pro vlastní aplikace	ano
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů	ano
Možnost současného provozu aplikačního firewallu a IDP/IPS	ano

Rekognoskace aplikací za provozu	ano
Detekce a blokování Botnet komunikace	ano
Podpora inspekce SSL spojení (MITM) včetně podpory TLSv1.3	ano
DoS/DDoS ochrana	
Dekódovaní DNS, HTTP	ano
Identifikace útočících stanic – prahové hodnoty pro dotazy za časovou jednotku	ano
Akce blokace požadavků, akce snížení počtu požadavků za časovou jednotku	ano
Podpora antispoofingové kontroly RPFC (Reverse Path Forwarding Check) pro IPv4 i IPv6	ano
Ochrana centrálního procesoru (Control Plane)	ano
Správa a monitoring	
Centralizované grafické rozhraní pro kompletní správu firewallu, resp. HA clusteru jako celku, a online monitorování aktuálního stavu	ano
Textově orientované konfigurační rozhraní (CLI)	ano
Možnost povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Přístup pomocí protokolu SSHv2	ano
Podpora protokolů SNMPv2, SNMPv3	ano
DNS klient	ano
Podpora synchronizace času protokolem NTPv3	ano
Podpora netflow, sflow nebo ekvivalentních exportů statistik datových toků/flow	ano
Export statistik datových toků/flow selektivně na více kolektorů	ano
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
Ověřování přístupu k zařízení pomocí RADIUS nebo TACACS+ protokolu	ano
Lokální logování na zařízení	ano
Kapacita lokálního úložiště logů	2 TB
Vzdálené logování na syslog server	ano
Podpora podrobného logování a reportování událostí na síti, aktivit a tendencí v reálném čase	ano
Korelace logů a událostí	ano
Vynucení potvrzení změn nastavení	ano
Systémový rollback konfigurace	ano
Správa revizí konfigurací	ano
Výkonnostní parametry firewallu	
Agregovaná propustnost aplikačního firewallu při plném zatížení (provoz IPv4/IPv6)	120/120 Gb/s
Maximální zpoždění při požadované propustnosti firewallu	5 µs

Počet souběžných TCP spojení	10 miliónů
Počet nových spojení	500 tisíc/s
Propustnost IPSec VPN (AES256 + SHA256)	50 Gb/s
Propustnost SSL VPN	10 Gb/s
Počet současně připojených VPN uživatelů	8000
Agregovaná propustnost IPS při plném zatížení	20 Gb/s
Agregovaná propustnost aplikační kontroly při plné zatížení	30 Gb/s

Tabulka povinných požadavků pro systém na zpracování a korelaci logů z firewallu (požadován 1 ks)

Požadavky na funkcionalitu	**Minimální požadavky**
Typ zařízení	Hardwarová appliance
Redundantní napájecí AC zdroje	ano
Napájecí zdroje vyměnitelné za chodu	ano
Hot-swap disky	ano
Minimální využitelná kapacita disků pro uložení logovacích záznamů	20 TB
Celkový počet záznamů uložitelných za 1 den	500 GB
Minimální počet nových záznamů	20 tisíc/s
Minimální počet nových záznamů pro analýzu	10 tisíc/s
Minimální počet a typ rozhraní 1G/10G	2, SFP/SFP+
Minimální počet rozhraní RJ45	2
Podpora Link Aggregation IEEE 802.3ad/LACP	ano
Generování reportů podle šablon	ano
Vytváření vlastních šablon pro reporty	ano

Další požadavky

- Zadavatel požaduje převod konfigurace ze stávajícího zařízení na dodané bez ztráty funkcionality.
- Všechny poptávané aktivní síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě zadavatele kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě specifikovanými níže.

Požadavky na záruku a servis dodávky

Zadavatel požaduje další související plnění:

- Dodávka Zboží do místa plnění.
- Technická dokumentace v elektronické podobě.
- Uživatelská příručka.
- Dodavatel poskytne Zadavateli po dobu trvání záruky všechny relevantní verze operačního software nabízené výrobcem tak, aby dodané řešení fungovalo bez závad. Dodavatel se současně zavazuje informovat Zadavatele o nových softwarových verzích a funkčnostech, které mohou rozšiřovat dodané řešení. Dodavatel se zavazuje získat potřebné softwarové produkty legálním způsobem za podmínek stanovených výrobcem zařízení,
- Dodavatel zajistí Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, pokud ji výrobce v rámci své podpory koncovým uživatelům poskytuje.
- Veškeré zákonem vyžadované dokumenty potřebné pro provoz nabízených zařízení na území České republiky (prohlášení o shodě apod.).

- Dodavatel je povinen zajistit dostupnost nových originálních náhradních dílů od výrobce pro dodané řešení za podmínek specifikovaných Zadavatelem v režimu 8h x 5d x NBD (počet hodin dostupnosti servisu uchazeče x počet dní v týdnu dostupnosti servisu dodavatele x doba pro odeslání náhradního dílu Zadavateli do místa plnění).

Výše specifikovanou záruční lhůtu, servis a dostupnost náhradních dílů Zadavatel požaduje po dobu 60 měsíců.

Popis prostředí počítačové sítě ZČU

Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování šíření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).
- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

Popis současného stavu

ZČU v současné době používá jako centrální firewall dvojici zařízení Fortinet Fortigate 3700D v režimu active/standby. Aktivní i záložní firewall je připojen do dvojice zařízení Cisco Nexus 93180YC-EX využívající technologii vPC (Virtual Port Channel). Použitým typem optického rozhraní je v obou případech QSFP28. Interně je pro rozkládání zátěže využíván clustering. Některé virtuální domény (VDOM) jsou aktivní na primárním firewallu, jiné na sekundárním firewallu. Připojení do sítě ZČU je realizováno na úrovni L3 pomocí MP-BGP pro každý VDOM separátně. Páteřní síť ZČU používá technologii EVPN/VXLAN. Plánuje se přechod na VXLAN L2VPN technologii i v prostředí firewallu. Na firewallu jsou ukončeny VPN spojení vzdálených lokalit využívající technologii IPSec a GRE.
Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované z firewallu se zpracovávají pomocí software FTAS[1]. Přístup na firewall je centrálně řízen pomocí protokolu TACACS+.

[1] http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/,
http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/,
http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf