Požadované technické parametry dodávky

Předmětem dodávky jsou **VPN koncentrátory (požadovány 2 ks)** dle technických podmínek uvedených níže.

Tabulka povinných požadavků pro VPN koncentrátor (požadovány 2 ks)

Požadovaná funkcionalita	**Minimální požadavky**
Základní vlastnosti	
Typ zařízení	Stavový firewall / VPN koncentrátor
Vysoká dostupnost/High Availability	V režimech active/passive i active/active
Formát zařízení	samostatné zařízení
Počet a typ rozhraní 1/10G dedikovaných pro management	1, SFP+
Počet a typ rozhraní 1/10/25G	8, SFP+/SFP28
Možnost rozšíření o moduly rozhraní s rychlostí 40 Gb/s	ano
Požadovaný počet a typ transceiverů	4 ks, 25GBase AOC, 7 m
Redundantní napájecí AC zdroj	ano
Napájecí zdroje vyměnitelné za chodu	ano
Výkonnostní parametry	
Počet současně otevřených spojení	5 miliónů
Počet nových spojení za vteřinu	600 tisíc
Agregovaná propustnost firewallu	35 Gb/s
Agregovaná propustnost VPN koncentrátoru (šifrování AES256)	9 Gb/s
Agregovaná propustnost IPSec VPN	12 Gb/s
Podporované funkce	
Stateful failover	V režimech active/active i active/passive
Počet VLAN	700
Provoz zařízení v režimu L3 (směrování)	ano
Provoz zařízení v režimu L2 (přepínání nebo transparentní)	ano
Seskupování portů IEEE 802.3ad	ano
Statické i dynamické směrování pro IPv4 (OSPF, BGP)	ano
Statické i dynamické směrování pro IPv6 (OSPFv3, MP-BGP)	ano
NAT64 a DNS64	ano
Policy based Routing	ano
Kontrola paketů TCP provozu s ochranou před útoky, jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	ano
Filtrace IPv4 a IPv6 provozu	ano
Inspekce IPv4 a IPv6 provozu	ano
Filtrace podle identity uživatele nebo jeho skupiny definované v AD	ano
Filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	ano
Bezpečnostní pravidla se zohledněním i identity uživatele	ano
Bezpečnostní pravidla se zohledněním informací o koncovém zařízení (typ, stav, apod.)	ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	ano

RADIUS klient pro AAA (autentizace, autorizace, accounting)	ano
DHCP relay	ano
Správa	
CLI rozhraní	ano
Přístup pomocí protokolu SSHv2	ano
Omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
Protokoly SNMPv2, SNMPv3	ano
Ověřování přístupu k zařízení pomocí RADIUS anebo TACACS+ protokolu	ano
Řízení přístupu na zařízení podle rolí administrátorů	ano
Vzdálené logování na syslog server	ano
Export statistik datových toků pomocí netflow, sflow nebo ekvivalentních	ano
Vzdálené správa konfigurace přes grafické rozhraní bez nutnosti instalace zvláštního SW	ano
Přehledy a statistiky na dohledové konzoli s filtrací podle času, typů incidentů, aplikací, koncových stanic	ano
Centrální dohledová konzole s vytvářením reportů manuálně a podle časového harmonogramu	ano
Centrální dohledová konzole s korelací událostí s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu apod.	ano
Funkcionalita VPN	
Počet souběžných šifrovaných spojení	10000
Definice specifických přístupových oprávnění (bezpečnostní politiky, ACL, atd.) podle identity nebo skupiny uživatele (např. v AD)	ano
Autentizace uživatelů pomocí lokální databáze	ano
Autentizace uživatelů pomocí RADIUS serveru	ano
Autentizace uživatelů pomocí Kerberos serveru	ano
Autentizace uživatelů pomocí digitálních certifikátů X. 509	ano
Autentizace uživatelů pomocí SmartCard	ano
Autentizace uživatelů pomocí RSA softID a RSA securID	ano
Podpora veřejných CA včetně možnosti zprovoznit CA přímo na firewallu	ano
Současná autentizace AAA a certifikátem	ano
CRL a OCSP pro kontrolu revokace certifikátu	ano
Přiřazení IPv6 adres klientům	ano

Další požadavky

- Součástí nabídky musí být samostatná položka **povýšení základních funkčních vlastností VPN koncentrátoru**, které bude zahrnovat plnou podporu provozu v režimu vysoké dostupnosti (HA režim active/active i active/standby včetně statefull switchover) a podpora šifrování AES.
- Zadavatel požaduje převod konfigurace a licencí klientského VPN software používaného VPN koncentrátoru na dodané zařízení 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.

..

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 síření 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 VPN koncentrátor dvojici zařízení Cisco ASA 2130 v režimu active/standby. Aktivní i záložní VPN koncentrátor je připojen do dvojice zařízení Cisco Nexus 93180YC-EX využívající technologii vPC (Virtual Port Channel). Použitým typem optického rozhraní je v obou případech SFP+/SFP28. Jako klientský VPN software je použit Cisco Secure VPN Client

licencovaný pro 800 klientů. Pro autentizaci uživatelů je použit Kerberos anebo klientský certifikát vydaný certifikační autoritou ZČU a GEANT, dostupný buď ve formě souboru, nebo USB tokenu. Pro autorizaci uživatelů je použita dvojice RADIUS serverů, která slouží pro přidělování pevné IPv4 a IPv6 adresy, masky sítě a přístupových práv formou access-listu vybraným uživatelům.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů, linuxových firewallů (kolejní extranet) a specializované FlowMon[1] sondy (kolejní intranet) se zpracovávají pomocí IPv4/IPv6 software FTAS[2].

AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

[1] http://www.invea.cz/produkty-sluzby/flowmon/flowmon-sondy

[2] 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