| Popis parametrů | Požadavek | Ano/Ne |
|---|---|---|
| Výrobce zařízení | Uvedení výrobce | [redacted] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla | |
| Odkaz na WWW stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu | |
| **Základní požadavky:** | | |
| Bezpečnostní zařízení typu next-generation firewall (dále též pouze NGFW) musí být jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic a pod.. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW | ano | Ano |
| **Požadavky na HW architekturu:** | | |
| NGFW musí být typu HW appliance | ano | Ano |
| Všechny parametry propustnosti musí dodavatel uvádět v real world mix paketech, tzv. "application mix" | ano | Ano |
| Modul pro zpracování dat musí být v architektuře firewallu oddělen alespoň na úrovni CPU jader od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění | ano | Ano |
| NGFW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI | ano | Ano |
| NGFW musí obsahovat minimálně 2 optické datové rozhraní QSFP28 o rychlosti 100Gb/s | ano | Ano |
| NGFW musí obsahovat minimálně 1x datové rozhraní SFP+ pro vzájemné propojení FW mezi lokalitami (resp. všechna rozhraní vč. SFP modulů pro zajištění HA dle výrobce | ano | Ano |
| NGFW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu NGFW | ano | Ano |
| NGFW musí být schopen ukládat logové údaje na interní storage o velikosti minimálně 460 GB | ano | Ano |
| NGFW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP) | ano | Ano |
| NGFW musí být rozměrově kompatibilní s 19" rozvaděčem | ano | Ano |
| NGFW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V, vyměnitelné za běhu zařízení | ano | Ano |
| **Požadavky na High Availability (HA):** | | |
| NGFW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení | ano | Ano |
| NGFW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení | ano | Ano |
| NGFW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti i v geograficky oddělených lokalitách | ano | Ano |
| V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes NGFW | ano | Ano |
| NGFW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého NGFW v HA, nedostupnosti specifikované IP adresy | ano | Ano |
| **Obecné výkonové parametry:** | | |
| Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň (app mix) | 34 Gb/s | Ano |
| Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň (app mix) | 19 Gb/s | Ano |
| Minimální počet souběžných spojení musí dosahovat hodnoty alespoň | 2800000 | Ano |
| Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň | 260000 | Ano |
| **Síťová funkcionalita:** | | |
| NGFW musí plně podporovat IPv4 i IPv6 | ano | Ano |
| NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP | ano | Ano |
| NGFW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64 | ano | Ano |
| NGFW musí podporovat persistentní NAT pro DIPP (Dynamic IP and Port) | ano | Ano |
| NGFW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing) | ano | Ano |
| NGFW musí podporovat MSDP (Multicast Source Discovery Protocol) pro pokročilé směrování. | ano | Ano |
| NGFW musí podporovat BFD (Bidirectional Forwarding Detection) pro tradiční i pokročilé směrování. | ano | Ano |
| NGFW musí podporovat nástroj pro pokročilé směrování (Advanced Routing Engine) | ano | Ano |
| PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel. | ano | Ano |
| NGFW musí umožnit nakonfigurovat expirační dobu cookies na 1 až 5 let | ano | Ano |
| NGFW musí podporovat web proxy a umožnit migraci proxy na NGFW beze změny architektury. | ano | Ano |
| NGFW musí podporovat stateful DHCPv6 klienta k získání IPv6 adresy a jiných parametrů | ano | Ano |
| NGFW musí umožnit nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty. | ano | Ano |
| NGFW musí umožnit nakonfigurovat IPSec tunnel s podporou post-quantum šifrování přímo na NGFW bez nutnosti použití třetích stran. | ano | Ano |
| NGFW musí podporovat výměnu hybridních post quantových klíčů založených na RFC 9242 a RFC 9370 v rámci IKEv2 a IPsec rekey. | ano | Ano |
| NGFW musí podporovat vytváření hybridních post quantových klíčů použitím kryptografických sad NIST round 3 a round 4. | ano | Ano |
| NGFW musí podporovat na současně na jednom zařízení na úrovni síťového rozhraní konfigurace Span, Transparent, Layer 3 a Layer 2 | ano | Ano |
| **VPN:** | | |
| NGFW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený | ano | Ano |
| NGFW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (min. TLS v1.2) | ano | Ano |
| Počet současně připojených uživatelů nesmí být licenčně omezený | ano | Ano |
| NGFW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS | ano | Ano |
| Propustnost IPSec musí být alespoň | 14 Gb/s | Ano |
| **Správa řešení:** | | |
| Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru. | ano | Ano |
| GUI musí podporovat čtení logových záznamů bez nutnosti používání centrálního management serveru. | ano | Ano |
| Připojení ke GUI musí podporovat šifrování TLSv1.3 | ano | Ano |
| GUI musí obsahovat offline kontextovou nápovědu. | ano | Ano |
| Jednotlivé HW appliance musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování | ano | Ano |
| Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování. | ano | Ano |
| Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových NGFW použitím konfiguračních šablon na připojeném USB flash disku. | ano | Ano |
| NGFW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát | ano | Ano |
| NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu | ano | Ano |
| NGFW musí podporovat nativní nástroj pro odchycení provozu | ano | Ano |
| NGFW musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon) | ano | Ano |
| NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem | ano | Ano |
| Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí NGFW | ano | Ano |
| NGFW s novějšími verzemi OS musí umožnit při upgrade/downgrade přeskočit až o 3 (major) softwarové verze naráz. | ano | Ano |
| **Aplikační kontrola:** | | |
| NGFW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu | ano | Ano |
| Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla | ano | Ano |
| Definovaná aplikace musí představovat "match kritérium" při policy lookup | ano | Ano |
| NGFW musí podporovat identifikaci aplikací napříč všemi porty/protokoly | ano | Ano |
| NGFW musí podporovat identifikaci aplikací na nestandardních portech | ano | Ano |
| Identifikace aplikace musí probíhat přímo v NGFW | ano | Ano |
| NGFW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping | ano | Ano |
| NGFW musí podporovat řízení neznámého provozu | ano | Ano |
| NGFW musí umožňovat tvorbu plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele | ano | Ano |
| NGFW musí umožnovat zakázat instalaci nových signatur aplikací z aktualizací poskytovaných vendorem | ano | Ano |
| **Kontrola na úrovni uživatelských identit:** | | |
| NGFW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit | ano | Ano |
| Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla | ano | Ano |
| Uživatelská identita musí představovat "match kritérium" při policy lookup | ano | Ano |
| NGFW musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins) | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta) | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta | ano | Ano |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API) | ano | Ano |

| | | |
|---|---|---|
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček | ano | Ano |
| NGFW musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná | ano | Ano |
| **Dešifrování:** | | |
| NGFW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům | ano | Ano |
| NGFW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru | ano | Ano |
| NGFW musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace | ano | Ano |
| Dešifrovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita | ano | Ano |
| NGFW musí podporovat dešifrování za pomoci ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz | ano | Ano |
| NGFW musí podporovat dešifrování protokolu TLS verze 1.3 | ano | Ano |
| NGFW musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následne přepošle čistě přefiltrované data zpět do NGFW. (tzv. decryption broker) | ano | Ano |
| NGFW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu. | ano | Ano |
| NGFW musí podporovat OCSP (Online Certificate Status Protocol) pro zkontrolování platnosti SSL/TLS certifikátů v síťové architektuře obsahující web proxy | ano | Ano |
| **Ochrana proti DoS:** | | |
| NGFW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita | ano | Ano |
| **QoS:** | | |
| NGFW musí poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.) | ano | Ano |
| NGFW musí podporovat prioritizaci provozu na základě DSCP | ano | Ano |
| NGFW musí podporovat prioritizaci provozu na základě Identifikované aplikace | ano | Ano |
| **Logování a reportování:** | | |
| NGFW musí obsahovat lokální úložiště logů | ano | Ano |
| NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI | ano | Ano |
| NGFW musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL | ano | Ano |
| NGFW musí podporovat přeposílání logů na zařízení třetích stran | ano | Ano |
| NGFW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla | ano | Ano |
| NGFW musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní NGFW | ano | Ano |
| **Servisní podpora a licenční plán:** | | |
| NGFW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů | ano | Ano |
| **Bezpečnostní funkcionality:** | | |
| NGFW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu | ano | Ano |
| NGFW musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve NGFW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla | ano | Ano |
| NGFW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele | ano | Ano |
| NGFW musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve NGFW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla | ano | Ano |
| Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích - SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB | ano | Ano |
| NGFW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele | ano | Ano |
| NGFW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci | ano | Ano |
| NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; NGFW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů | ano | Ano |
| NGFW musí podporovat import SNORT signatur manuálně a přes API. | ano | Ano |
| NGFW musí pro přístup ke kritickým aplikacím, poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci; tato vlastnost musí být konfigurovatelná na úrovni bezpečnostního pravidla | ano | Ano |
| NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu | ano | Ano |
| NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu | ano | Ano |
| NGFW musí podporovat analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane. | ano | Ano |
| NGFW musí umět zabránit neznámým injekčním útokům jako je SQLi a Command Injection útoky pomocí strojového učení. | ano | Ano |
| NGFW musí podporovat Local Deep Learning, který poskytuje mechanismus pro provádění rychlé, lokální analýzy zero-day a dalších vyhýbavých hrozeb založené na hlubokém učení. | ano | Ano |
| NGFW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování | ano | Ano |
| NGFW musí umožnit tvorbu uživatelsky definovaných signatur pro hrozby založené na L3 a L4 hlavičkách. | ano | Ano |
| NGFW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele | ano | Ano |
| Řešení musí podporovat rozšíření funkcionality NGFW o bezpečnost IoT nativní (automatizovaná identifikace zařízení a jejich zranitelností, automatizovaná bezpečnostní pravidla pro IoT) bez nutnosti integrace s třetími stranami. | ano | Ano |
| Řešení musí podporovat rozšíření funkcionality NGFW o bezpečnost IoT nativní bez nutnosti instalace agentů nebo síťových sond. | ano | Ano |
| **Sandboxing:** | | |
| Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB. | Možnost rozšíření | Ano |
| Sandbox systém musí být od stejného výrobce jako je NGFW, ale nemusí být HW součástí NGFW | Možnost rozšíření | Ano |
| Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý; | Možnost rozšíření | Ano |
| Sandbox musí být schopen automaticky upravit kategorie používané URL databáze pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL | Možnost rozšíření | Ano |
| Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C. | Možnost rozšíření | Ano |
| Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android | Možnost rozšíření | Ano |
| Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní NGFW | Možnost rozšíření | Ano |
| Aktualizace zero-day signatur musí být instalována do NGFW v reálnem čase, čili s nulovou prodlevou | Možnost rozšíření | Ano |
| NGFW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod. | Možnost rozšíření | Ano |
| NGFW musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu. | Možnost rozšíření | Ano |
| NGFW musí podporovat sandboxing v cloudu, který využívá umělou inteligenci k ochraně před sofistikovanými útoky. | Možnost rozšíření | Ano |
| Sandbox musí umět používat introspekci VM (Virtual Machine) a paměťovou analýzu, aby odhalil vysoce sofistikovaný malware. Zároveň umí předcházet tomu, aby malware rozpoznal, že se nachází ve virtuálním prostředí. | Možnost rozšíření | Ano |
| Sandbox musí používat inteligentní analýzu běžící paměti a zachycuje snímky v době, kdy probíhá podezřelá aktivita. | Možnost rozšíření | Ano |
| Sandbox musí rozpoznat, které závisloti malware potřebuje k tomu, aby se spustil a umí je nasimulovat. | Možnost rozšíření | Ano |
| **Centrální management:** | | |
| Řešení musí obsahovat virtuální platformu pro centrální správu všech dodaných firewallů do VMware ESXi prostředí | ano | Ano |
| Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat všechny dodané HW appliance včetně všech virtuálních kontextů | ano | Ano |
| Centrální management musí podporovat zběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci | ano | Ano |
| Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu | ano | Ano |
| Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní NGFW a zároveň přes grafické rozhraní centrálního managementu | ano | Ano |
| Administrátor musí mít možnost importovat NGFW konfiguraci do centrálního managementu | ano | Ano |
| Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat se grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami | ano | Ano |
| Řešení musí obsahovat podporu statických Security Group Tags pro Cisco TrustSec | ano | Ano |
| Administrátor musí mít možnost zapsat změny i při čekajících změnách od ostatních administrátorů. | ano | Ano |
| Centrální management musí umět v reálném čase zkontrolovat plánovéné změny v konfiguraci při zápisu a zablokovat ty, které neodpovídají předepsaným pravidlům. | ano | Ano |
| Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu. | ano | Ano |
| Centrální management musí podporovat uložení alespoň 30 GB logů za den. | ano | Ano |
| Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na webovém rozhraní centrálního managementu. | ano | Ano |