

Opis predmetu zákazky - Next Generation Firewall v hardwarovom prevedení

- 2x Next Generation Firewall v hardwarovom prevedení a nasadenie do IKT infraštruktúry

Technické požiadavky

- Hardwarové prevedenie Next Generation Firewall (NGFW). Priepustnosť Firewall pre IPv4 minimálne 195/195/130 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B)
- Priepustnosť Firewall pre IPv6 minimálne min. 195/195/130 Gbps (merané na UDP paketoch s veľkosťou 1518B)
- Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, NGFW a zapnutým logovaním minimálne 17 Gbps
- Firewall Throughput (packet per second - počet spracovaných paketov za 1 sekundu) minimálne 205 Mpps
- Počet súčasných TCP spojení firewallu - Concurrent Sessions (TCP) minimálne 12 Milion
- Počet nových TCP spojení za sekundu (setup-rate) minimálne 730000
- Latencia firewallu maximálne 4 μ s (merané na malých UDP paketoch (64B))
- Firewall policies minimálne 75 000
- Priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response) minimálne 33 Gbps
- Priepustnosť funkcie IPS vrátane logovania minimálne 22 Gbps
- Priepustnosť SSL dešifrovania/SSL inšpekcie minimálne 11 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)
- Počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom minimálne 11000
- Detekcia známych aplikácií na základe signatúr minimálne 4000 preddefinovaných aplikácií/signatúr
- Funkcia detekcie aplikácií na L7 (Application Control)
- Podpora SSL VPN
- Podpora TLS verzie 1.3
- Priepustnosť SSL VPN minimálne 11Gbps
- Podpora IPSEC VPN v režime site-2-site aj client-2-site
- Priepustnosť IPSEC VPN (AES256-SHA256, packet size 512B) minimálne 52 Gbps
- Podpora minimálne 50 izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod. Ak je pre túto funkcionality potrebná licencia, súčasťou ponuky musí byť pokryté minimálne 10 kontextov.
- Podpora minimálne 3600 VLAN
- Podpora LACP

- Rozhrania na firewalle využiteľné pre spracovanie komunikácie minimálne 12 x 25 GE SFP28/10 GE SFP+ port (plno osadené duplex MM SFP+ modulmi súčasťou dodávky)
- Rozhrania na firewalle využiteľné pre spracovanie komunikácie minimálne 4 x 40 GE QSFP+ port
- Rozhrania na firewalle využiteľné pre spracovanie komunikácie minimálne 14 x GE RJ45 port
- Rozhrania na firewalle využiteľné pre spracovanie komunikácie minimálne 8 x GE SFP port
- Rozhrania na firewalle využiteľné na clustrovanie okrem komunikačných rozhraní minimálne 2 x 10GE SFP+
- Rozhrania na firewalle využiteľné pre management minimálne 1 x Console port (CLI)
- Rozhrania na firewalle využiteľné pre management minimálne 1 x GE RJ45 Management port
- Minimálne 1 x USB Management port
- Podpora centrálnej správy firewallov prostredníctvom management nástrojov objednávateľa a to: FortiManager- (všetky potrebné rozširujúce licencie súčasťou dodávky). Dodané zariadenia musia byť plne integrovateľné a spravované uvedeným centrálnym managementom.
- Požiadavky na napájanie minimálne 2x AC zdroj 100-250VAC, 50/60 Hz, zdroje vymeniteľné za chodu (HOT-SWAP)
- Interné úložisko pre logy a konfigurácie minimálne 2 x 900 GB SSD
- Prevedenie HW appliance do racku s veľkosťou maximálne 2RU; Kompletne príslušenstvo (montážne prvky) pre montáž do RACKU
- Požiadavky na vysokú dostupnosť - HA minimálne v režime Active / Active , Active / Passive, georedundantné clustrovanie min. dvoch clustrov (potrebné licencie súčasťou dodávky)
- Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Požadované zapojenie vysokej dostupnosti v režime dactive-passive. Ak funkcie klastrovania vyžadujú licenciu, tak táto musí byť súčasťou dodávky.
- Podpora statických ale aj dynamických smerovacích protokolov minimálne BGP, OSPF (potrebné licencie súčasťou dodávky)
- Podpora integrácie na MS Active directory pre potreby riadenia prístupov ACL na základe identít AD (napr. Username, computer, ...) potrebné licencie a komponenty súčasťou dodávky
- Podpora funkcie transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri (potrebné licencie súčasťou dodávky)
- Pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii). Aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu
- Podpora použitia Application control aj formou profilov priradených k pravidlám

- Požiadavky na funkčnosť - možnosť definície FW pravidiel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je minimálne zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.
- Požiadavky na funkčnosť - podpora použitia Application control aj formou profilov priradených k pravidlám. Ak funkcie vyžadujú licenciu, tak táto musí byť súčasťou dodávky.
- Požiadavky na funkčnosť - Funkcie detekcie a zamedzenia narušení (IPS/IDS), funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám. Ak funkcie vyžadujú licenciu, tak táto musí byť súčasťou dodávky.
- Požiadavky na funkčnosť - možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS
- Požiadavky na funkčnosť - Funkcie antivírovej kontroly, Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom. Ak funkcie vyžadujú licenciu, tak táto musí byť súčasťou dodávky.
- Požiadavky na funkčnosť - podpora AV kontroly o rozšírenie o inšpekciu tzv. sandbox technikou. Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky
- Požiadavky na funkčnosť - Podpora služby výrobcu umožňujúca detegovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov
- Požiadavky na funkčnosť - Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky
- Požiadavky na funkčnosť - Funkcia DNS filtra, Možnosť blokovat' DNS dotazy na základe príslušnosti k URL kategórii,... (potrebné licencie súčasťou dodávky)
- Požiadavky na funkčnosť - Možnosť definovať vlastný tzv. blacklist domén, Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL
- Požiadavky na funkčnosť - Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos
- Požiadavky na funkčnosť - FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu
- Požiadavky na funkčnosť - Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky bez nutnosti samostatnej inštalácie politik
- Požiadavky na funkčnosť - Podpora SNMP vrátane SNMP MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete. Požadovaná verzia minimálne SNMPv3.
- Požiadavky na funkčnosť - Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať.
- Požiadavky na funkčnosť - Možnosť kombinovať akcie pre automatizačné pravidlá minimálne v rozsahu webhook s definovateľnými parametrami, CLI script, Email, MS-

TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy

- Požiadavky na funkčnosť - Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel minimálne schopnosť parsovať vstupy z logov a z predchádzajúcich vykonaných akcií
- Podpora otvoreného API pre ďalšie možnosti integrácie
- Požiadavky na rozsah prevádzkových teplôt 0 - 40°C
- Požiadavky na chladenie - predná strana nasávanie, vyfukovanie dozadu

Licenčné a záručné požiadavky

Všetky potrebné licencie s platnosťou na 1 rok a záruka 1 rok od dátumu akceptácie. Podpora výrobcu v režime 24x7. Vlastníctvo Supportného kontraktu a licencií priamo objednávateľom. Prístup na supportný portál vo vlastníctve objednávateľa, otváranie, správa supportných ticketov priamo objednávateľom.