Specifikace požadavků na perimetrický firewall

| **ID** | **Požadavek na vlastnost řešení** |
| --- | --- |
| **HW-1** | Předmětem dodávky jsou dva firewally s identickou HW konfigurací a identickými licencemi určené pro provoz v clusteru. |
| **HW-2** | Každý uzel firewallu má celkem minimálně 8 síťových rozhraní využitelných pro datový provoz. Do tohoto počtu se nezapočítávají síťová rozhraní určená pro správu/dohled firewallu, ani síťová rozhraní, která slouží pro výměnu stavových informací v rámci clusteru. Minimální počet síťových rozhraní určených pro datový provoz je dosažen bez použití externího přepínače. |
| **HW-3** | Každý uzel firewallu má minimálně 4 síťová rozhraní pro datový provoz s metalickým výstupem, která podporují rychlost 1 Gbit/s. Může být řešeno kombinací SFP slotu a SFP modulu s metalickým rozhraním. |
| **HW-4** | Každý uzel firewallu má minimálně 4 síťová rozhraní pro datový provoz typu SFP, která podporují rychlost 10 Gbit/s. Součástí dodávky budou 4 SFP moduly pro 10G Multimode optické připojení pro každý uzel firewallu. |
| **HW-5** | Každý uzel firewallu má redundantní napájení. Výpadek poloviny napájecích zdrojů neovlivní činnost uzlu. |
| **HW-6** | Jednotlivé komponenty systému jsou uzpůsobené pro montáž do 19" racku. |
| **HW-7** | Střední doba mezi poruchami jednotlivých uzlů firewallu je alespoň 10 let. |
| **SYS-1** | Firewall je redundantní. Výpadek síťového rozhraní, selhání HW ani pád některého z procesů na jednom z uzlů nezpůsobí takovou ztrátu paketů, která by donutila hosty komunikující přes firewall znovu navázat TCP spojení. |
| **SYS-2** | Firewall není řešen pomocí kombinace hardwaru od jednoho dodavatele a virtuálního firewallu od jiného dodavatele.  |
| **SYS-3** | Firewall podporuje ISSU (In-Service Software Upgrade). |
| **SYS-4** | Firewall podporuje clustering v režimu active/active i active/passive. V režimu active/active je možné synchronizovat relace mezi více než dvěma uzly.  |
| **NET-1** | Firewall podporuje dynamické směrovací protokoly OSPF i BGP. |
| **NET-2** | Firewall podporuje NAT64. |
| **SEC-1** | Firewall podporuje stavovou inspekci datového provozu. |
| **SEC-2** | Firewall podporuje analýzu aplikačních dat u následujících protokolů za účelem povolení komunikace na vyjednaných portech a změny IP adresy při provádění NATu: SIP, SCCP, FTP, RPC.  |
| **SEC-3** | Firewall podporuje vytváření prostupů na základě uživatelské identity / rolí.  |
| **SEC-4** | Firewall podporuje vyčítání identit ze systému Active Directory. |
| **SEC-5** | Firewall podporuje vyčítání identit ze systému Cisco ISE. |
| **SEC-6** | Firewall implementuje API pro předávání identit / rolí ze systémů třetích stran. K popisu API mají zákazníci bezplatný přístup, využití API nevyžaduje licenci nebo je příslušná licence součástí dodávky. |
| **SEC-7** | Firewall podporuje rozlišení identit uživatelů, kteří jsou souběžně přihlášení na stejný Microsoft Terminal Server. |
| **SEC-8** | Firewall podporuje identifikaci aplikací na základě aplikačních dat. Příslušná licence na aktualizaci detekčního enginu a signatur je součástí dodávky. |
| **SEC-9** | Správce může definovat vlastní aplikace, které bude firewall rozpoznávat na základě dat aplikační vrstvy. |
| **SEC-10** | Firewall podporuje tvorbu politik, které pracují s aplikačními metadaty (např. zahazuj provoz všech aplikací jejichž rizikovost je rovna nebo větší než stanovené skóre). V rámci jedné politiky je možné aplikovat více kritérií současně (např. zahazuj provoz peer-to-peer aplikací jejichž rizikovost je rovna nebo větší než stanovené skóre). |
| **SEC-11** | Firewall podporuje dekrypci TLS provozu včetně verze 1.3. Příslušná licence je součástí dodávky. |
| **SEC-12** | Firewall obsahuje výrobcem předdefinovaný seznam známých hostů, pro které nefunguje dekrypce. |
| **SEC-13** | Při dekrypci TLS umí firewall použít odlišný CA certifikát pro podpis certifikátu jehož předobraz na cílovém serveru je validní a jiný CA certifikát pro podpis certifikátu jehož předobraz na cílovém serveru není validní (např. self-signed). |
| **SEC-14** | Firewall podporuje site-to-site IPsec VPN. Součástí dodávky je licence nejméně pro 5 tunelů. |
| **SEC-15** | Firewall podporuje client-to-gateway VPN. Součástí dodávky je licence nejméně pro 100 současně připojených uživatelů, podporující alespoň desktopové klienty (MS Windows 10/11). |
| **SEC-16** | Firewall podporuje předávání a vyhodnocování informací o desktopovém zařízení VPN uživatele, minimálně v následujících oblastech: operační systém, firewall, antivirový program, šifrování disku. Příslušná licence nemusí být součástí dodávky. |
| **SEC-17** | Firewall podporuje detekci malwaru v datech přenášených protokoly: FTP, HTTP, SMTP, IMAP. Příslušná licence je součástí dodávky. |
| **SEC-18** | Firewall podporuje funkci IPS. Příslušná licence na aktualizaci IPS enginu a signatur je součástí dodávky. |
| **SEC-19** | Firewall podporuje nastavení různých IPS profilů / politik pro různé skupiny serverů a uživatelů. |
| **SEC-20** | Firewall podporuje dynamické vyčítání skupin adres z externích zdrojů a jejich automatickou aplikaci v bezpečnostních politikách. |
| **SEC-21** | Firewall obsahuje systém kategorizace URL a umožňuje jeho využití v bezpečnostních politikách. Příslušná licence je součástí dodávky. |
| **SEC-22** | Firewall podporuje automatické blokování komunikace na známé škodlivé adresy, jejichž seznam je dodáván výrobcem. Příslušná licence je součástí dodávky. |
| **SEC-23** | Firewall podporuje detekci 0-day malwaru pomocí analýzy chování ve virtualizovaném prostředí (sandboxing). Příslušná licence je součástí dodávky. |
| **SEC-24** | Firewall podporuje logování informací o svém stavu, o přístupu a činnosti administrátorů i o procházejícím provozu protokolem syslog. |
| **SEC-25** | Pro syslog zprávy firewallu je dostupný parser, který lze implementovat do systému ArcSight Logger. |
| **SEC-26** | Funkce pro správu firewallu i bezpečnostní funkce pro logování a kontrolu provozu zmíněné v tomto dokumentu fungují i pro IPv6 protokol. U RPC ALG není podpora IPv6 požadována. |
| **SEC-27** | Bezpečnostní politiky podporují skupiny uživatelů, jejichž členství vzniká a zaniká dynamicky na základě přiřazení a odebrání atributů danému uživateli jak pomocí vnějšího API (bez nutnosti manuální intervence), tak přes rozhraní pro správu firewallu. Změna členství se musí projevit bez nutnosti úpravy bezpečnostních politik na firewallu. |
| **SEC-28** | Firewall podporuje stažení a instalaci zero-day signatur v reálnem čase (spuštění aktualizačního procesu bez prodlevy od jejího vydání, mimo pevně definované časové intervaly). Příslušná licence musí být součástí dodávky. |
| **SEC-29** | Firewall je schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod. |
| **PWR-1** | Firewall je dostatečně dimenzován na souběžnou TLS dekrypci, IPS, Anti-Virus a Web-Filtering inspekci HTTPS datových toků o celkové šířce pásma minimálně 2 Gbit/s pro velikost paketů 64 KB. |
| **PWR-2** | Firewall je dostatečně dimenzován pro souběžné VPN připojení 200 uživatelů, jejichž souhrnný datový tok dosáhne 1 Gbit/s. |
| **MGMT-1** | Informace o stavu firewallu je možné vyčíst pomocí SNMP protokolu ve verzích 2c a 3. Příslušné MIB jsou volně k dispozici nebo jsou součástí dodávky. |
| **MGMT-2** | Firewall je podporován v systému Tufin SecureTrack. |
| **MGMT-3** | Firewall je podporován v systému AlgoSec FireFlow. |
| **MGMT-4** | Oprávnění pro správu jsou řešena pomocí rolí. Role mohou mít různé úrovně přístupu (čtení/zápis) pro různé části konfigurace (firewall politiky, IPS politiky apod.). |
| **MGMT-5** | Firewall podporuje dvoufaktorovou autentizaci správců. |
| **MGMT-6** | Firewall umožňuje krátkodobý odchyt procházejícího provozu do souboru, který lze následně analyzovat v programu WireShark. |
| **MGMT-7** | V téže bezpečnostní politice mohou být objekty s IPv4 i IPv6 adresami. |
| **MGMT-8** | Bezpečnostní politiky je možné spravovat prostřednictvím webového rozhraní i příkazové řádky bez potřeby instalace separátního management serveru. |
| **SUP-1** | Dodavatel zajistí kompletní přechod na nový firewall, včetně převodu stávajících NAT pravidel a bezpečnostních politik ze současného řešení (Check Point). |
| **SUP-2** | Dodavatel zajistí implementaci TLS dekrypce uživatelského provozu do Internetu i provozu navazovaného z Internetu na podnikové servery v DMZ.  |
| **SUP-3** | Dodavatel navrhne mechanismus, kterým budou uživatelé hlásit nedostupnost vybraných služeb (např. z důvodu nefunkční dekrypce TLS), mechanismus schvalování potřebných výjimek z inspekce i mechanismus jejich implementace.  |
| **SUP-4** | Dodavatel otestuje funkčnost klientského softwaru v prostředí ŘLP. V případě kolize se stávajícím SW vybavením zajistí nápravu do 3 měsíců od dodání systému. |
| **SUP-5** | Součástí dodávky je podpora HW ze strany výrobce v režimu NBD (Next Business Day) po dobu 5 let od podpisu akceptačních testů. |
| **SUP-6** | Součástí dodávky je podpora SW ze strany výrobce po dobu 5 let od podpisu akceptačních testů, zahrnující:* kontakt na technickou podporu (zakládání servisních lístků přes webový portál i telefonické konzultace),
* reakční čas odpovědi při řešení kritických závad SW (firewall je nefunkční) do 1 hodiny od nahlášení,
* asistence při šetření útoků – analýzy logů, doporučení úprav nastavení,
* předplatné (subscription) nezbytné pro zajištění všech požadovaných funkcionalit (např. aktualizace signatur),
* nárok na aktualizace SW nezbytné pro zachování funkčnosti a bezpečného provozu dodaného řešení.
 |
| **SUP-7** | Součástí dodávky jsou veškeré potřebné licence na dobu 5 let od podpisu akceptačních testů. |