Česká školní inspekce

Příloha č. 1

Technická specifikace předmětu plnění

1. HW a související služby

Požadují se zařízení (2 totožná, redundantní pro zajištění režimu vysoké dostupnosti viz dále) typu firewall/router. Soubor zařízení nahradí soubor stávajících zařízení Sonicwall SuperMassive 9200 v ostrém produkčním prostředí.

Firewall bude dodán v provedení hardwarového clusteru z důvodu zajištění redundance, a to v podobě dvou kusů stejných modelů zařízení, které budou identicky zapojeny do infrastruktury a budou tak zajišťovat vysokou dostupnost v režimu active/passive. Obě zařízení musí být vybavena redundantními napájecími zdroji. Je požadováno, aby pasivní zařízení automaticky respektovalo konfiguraci aktivního zařízení a v případě konfigurační změny v aktivním firewallu došlo automaticky bez prodlení a bez zásahu administrátora k aktualizaci konfigurace i v pasivním zařízení. Současně musí obě zařízení detekovat dostupnost, funkčnost a konektivitu druhého zařízení a v případě jeho selhání či nedostupnosti musí převzít vedoucí úlohu nejpozději do max. 20 sekund od výpadku aktivního zařízení. Totéž se týká plánovaných odstávek, např. během aktualizace firmwarů. Obě zařízení si mezi sebou musí průběžně vyměňovat informace o otevřených spojeních, aby v případě přenosu aktivní role mezi zařízeními nedošlo k resetování probíhajících spojení.

Firewall bude sloužit k ochraně perimetru sítě, stejně jako k ochraně provozu mezi vnitřními zónami sítě (LAN, DMZ, MPLS, Guest WiFi, CMS apod.). S ohledem na to jsou požadovány následující min. výkonové parametry propustnosti (platí pro každé ze dvou zařízení):

- stateful firewall min. 25 Gbps,
- aplikační firewall min. 15 Gbps,
- antivirová kontrola min. 15 Gbps,
- ochrana IPS min. 15 Gbps
- VPN min. 5 Gbps
- počet souběžných spojení kontrolovaných technologií DPI min. 2 000 000, se schopností zpracovávání nárůstu počtu spojení min. 200 000 za sekundu.

Firewall bude zároveň sloužit jako hraniční router. Vzhledem k možnosti zřízení autonomního systému („AS“) je požadována i případná licence (pokud je pro zajištění funkčnosti nutná) umožňující routování pomocí protokolů OSPF, RIP a zejména BGP. Firewall musí být schopen zajistit i funkci vysoké dostupnosti konektivity poskytované nezávislými dodavateli (ISP), tj. musí být schopen detekovat provozuschopnost těchto připojení (testováním dostupnosti ICMP a TCP vůči stanoveným vzdáleným destinacím), v případě výpadku primárního spojení přepnout na záložní bez zásahu administrátora a po zotavení primárního spojení opět zajistit přepnutí provozu zpět na primární. Současně je požadována schopnost vynucení určitého spojení pouze prostřednictvím záložní linky (např. hostovský HTTP/S provoz), aby jím nebyla zatěžována primární konektivita nutná k zajištění plynulého běhu kritických služeb a aplikací.

Z důvodu vysoké dostupnosti a rozložení zátěže musí být firewall schopen přijímat příchozí připojení na všech veřejných konektivitách souběžně.

Minimální parametry konektivity (platí pro každé ze dvou zařízení):

- min. 6x 10Gb SFP+,
- min. 12x 1G Base-T
- mimo výše uvedených provozních portů je požadován oddělený 1GbE management port
- pro případ servisních činností CLI rozhraní spravované pomocí protokolu SSH na management portu, identické rozhraní dostupné pomocí portu pro připojení sériové konzole

Dále jsou požadovány tyto vlastnost/funkčnosti (platí pro každé ze dvou zařízení):

- hloubková inspekce paketů („DPI“),

- včetně licencí opravňujících k použití funkcí zahrnující funkce aplikační firewall, antivirová kontrola síťových spojení, intrusion prevention system, filtr URL a webového obsahu

- kromě standardních DPI funkcí možnost definovat Geo-IP filtr a filtr sítí botnet, tj. omezení příchozí a odchozí komunikace s nežádoucími zeměmi a s botnet sítěmi centrálně řízených počítačů za účelem provádění kybernetické kriminality. Firewall musí být schopen aktualizovat databáze a signatury funkcí DPI průběžně a automaticky, bez jakéhokoli zásahu administrátora. Je požadováno, aby byl firewall schopen zároveň fungovat jako pasivní DPI sonda, která analyzuje provoz přiváděný z kritických segmentů technologií Port mirroring („SPAN“).
- k dosažení efektivní komunikace je požadována schopnost prioritizace provozu nejen dle TCP portů, ale zejména na základě detekovaných aplikací.
- na úrovni L2/L3:
    - ochrana před (D)DoS útoky v podobě vynucení standardů TCP (RFC 1122, RFC 793),
    - aktivní ochrana (blokováním) při překročení max. počtu spojení v případě L2 útoku typu SYN/RST/FIN/TCP flood,
    - aktivní ochrana (blokováním) při překročení max. počtu spojení v případě L3 útoku typu SYN flood,
    - aktivní ochrana (blokováním) při překročení max. počtu spojení v případě UDP a ICMP flood útoku a schopností SYN proxy v případě podezření z útoku typu SYN flood nastavením horní hranice počtu spojení, od kterého je SYN proxy aktivní.
- z důvodu prevence připojení nežádoucích zařízení funkce MAC-IP anti-spoofingu se schopností detekovat, reportovat a aktivně blokovat zařízení, která nejsou uvedena v anti-spoof cache. Dále musí být anti-spoof cache schopna „uzamčení“ vazby mezi MAC a IP, aby předešla případným man-in-the-middle útokům pomocí technik typu ARP poisoning.
- možnost personifikace datových toků, tj. schopnost detekovat nejen zdrojové/cílové adresy ve vnitřní síti, ale zároveň i detekovat konkrétní přihlášené uživatele na pracovních stanicích ve vnitřní síti, kteří datový tok iniciovali. Detekce těchto uživatelů musí probíhat buď na základě dotazu směrovaného konkrétní pracovní stanici nebo zjištění přihlášení/odhlášení uživatele ze Security logů doménových řadičů (uživatelé i počítače jsou zařazeny do doménové struktury Microsoft Active Directory).

- možnost definování platnosti standardních i aplikačních firewallových pravidel pouze pro vyjmenované uživatele, případně pro vyjmenované skupiny uživatelů, přičemž firewall musí umožňovat vytváření lokálních skupin přímo ve firewallu a ruční přiřazování uživatelů do nich, a zároveň musí umožňovat načítání skupin a členství uživatelů v nich přímo z Active Directory.
- možnost hloubkové inspekce šifrovaných SSL spojení („DPI-SSL“) pro zajištění ochrany před útoky a dalšími nežádoucími toky na veřejně poskytované služby využívající protokol HTTPS, ať už umístěné v místním prostředí nebo na internetu.
- ochrana proti škodlivým DNS dotazům a rizikovým doménám, přičemž kategorizaci rizika musí průběžně zajišťovat výrobce firewallu a mezi kategorie by měly patřit min. anonymizační proxy, hostování nevhodného nebo rizikového obsahu, zaparkované (nepoužívané) domény apod.
- dostupné metody správy, monitoringu a auditu, konkrétně:
    - správa pomocí sériového a SSH terminálu,
    - podpora monitoringu protokoly SNMPv2 a v3, IPFIX, NetFlow
    - zasílání provozních událostí od informativních po kritické protokolem Syslog ve strojově zpracovatelným formátu zpráv, tj. s rozlišením čísla události, popisu události, zdrojové/cílové IP adresy a portu a případně dalších relevantních metainformací (jméno uživatele, webová URL, zdrojová/cílová země)
- funkce pro kompletní správu emailové komunikace s těmito požadavky:
    - kontrola příchozí i odchozí pošty
    - podpora běžných zabezpečení – SPF, DKIM, DMARC
    - obsahuje vestavěný antispam, anti-phishing, antivir
    - vlastní pravidla na příjem i odesílání pošty
    - komunikace jak s onprem řešeními, tak MS365
    - propojení s Active Directory
- funkce VPN s parametry:
    - schopnost (včetně licence, pokud je nutná) pro připojení poboček a případných dalších vzdálených lokalit v počtu min. 100
    - VPN spojení na bázi protokolu IPsec
    - při vyjednávání spojení a následném šifrování provozu podpora kryptografické metody (IKEv2), protokolů AH, ESP, šifrovacích algoritmů AES-256 a 512, hashe SHA-256 a 512, výměny Diffie-Hellman s použitím bezpečných klíčů (min. 2048 bitů a eliptických křivek o délkách 256, 384 a 521 bitů), dopředné šifrování (forward secrecy, s použitím DH a bezpečných klíčů již uvedených parametrů) a ověřování pomocí sdíleného klíče a digitálního certifikátu.
- funkce softwarově definované konektivity (tzv. SD-WAN), která vzdáleným pobočkám umožní více souběžných VPN tunelů do centrálního firewallu.
  Požadována je schopnost realizace dvou základních scénářů:
  1) Pobočka nedisponuje záložní konektivitou, je připojena dvěma souběžnými VPN tunely do dvou konektivit centrálního firewallu.
  2) Pobočka disponuje záložní konektivitou, je připojena primární konektivitou do primární konektivity centrály a sekundární konektivitou do sekundární konektivity centrály.

  V obou případech je pak vyjmenovaný business-critical provoz na obou stranách routovaný pouze po těch VPN tunelech, které splňují administrátorem stanovené QoS, tedy předem stanovenou kvalitu definovanou pomocí latence a ztrátovosti. Pokud ani jedna z linek parametry QoS nesplňuje, pak musí být routou s nižší prioritou stanovena

alternativní cesta více tolerantním QoS. Běžný provoz bude mít stanovený vlastní více tolerantní QoS. Nekritický provoz (např. zálohování, synchronizace aktualizací aplikací) musí být možné routovat pouze po záložním spojení, aby nebyla ovlivněna primární linka, a to jen pokud je primární linka dostupná. Pokud není, musí být nekritický provoz automaticky přerušen, aby nezatěžoval záložní linku.

V rámci dodávky firewallu (platí pro obě zařízení) je vyžadována technická podpora výrobce 24x7, hardwarová záruka a případné předplatné/licence výše uvedených požadovaných funkcionalit a bezpečnostních služeb, pokud je pro jejich plnou požadovanou funkčnost nutné, v délce trvání min. 60 měsíců.

Součástí plnění je dodávka, instalace, parametrizace a konfigurace do ostrého produktivního provozu kupujícího. Součástí těchto služeb je pak také konfigurace všech stávajících pravidel (firewall, NAT, VLAN atd.) a nastavení, které kupující využívá na stávajícím nahrazovaném řešení. Dále pak také nastavení logování veškerých síťových aktivit do SIEM systému Logmanager (včetně případné výroby odpovídajících parserů).

2. SW pro správu a monitoring provozu firewallů a související služby

Požadován je administračně-analytický SW nástroj pro centrální správu a monitoring (včetně reportingu) firewallů podle bodu 1. a dále s možností správy a monitoringu dalších firewallů Sonicwall TZ470 a NSA 2700 již implementovaných v prostředí kupujícího.

Funkční požadavky pro oblast centrální správy:

- Komplexní plnohodnotná správa všech zařízení v jednotném rozhraní
- Správa konfiguračních možností jednotlivých firewallů samostatně, ale i hromadně formou administrátorem definovatelných šablon, min. v tomto rozsahu nastavení:
    - firewallových, routovacích a NAT pravidel,
    - adresních a portových objektů,
    - webových a aplikačních pravidel,
    - antivirových výjimek,
    - Geo a botnet filtrů,
    - VPN tunelů,
    - dalších nastavení jako jsou např. lokální účty ve firewallu za účelem konfigurace správců pro případ ztráty spojení s centrálním LDAP
- Šablony musí umožňovat uvést u IP adres v objektech i konfiguraci VPN (autentikace protistran) určitou formu a syntaxi zástupných symbolů, které budou vyhodnoceny pro konkrétní firewall. Například IP adresa 10.<CisloPobocky>.100.1 by měla zástupný symbol CisloPobocky, který by se pro příklad v konkrétním firewallu pobočky č. 5 přeložil a reprezentoval v něm odpovídající IP adresu, tedy např. 10.5.100.1. Obdobný způsob musí být použitelný pro konfiguraci identifikátorů protistran při vyjednávání VPN.

Funkční požadavky pro oblast monitoringu (včetně reportingu)

- agregace, sumarizace a reporting e-mailem ve vhodném formátu (např. PDF)
- statistiky využívání sítě, s možností reportování nejvíce využívaných typů provozu seskupovaných dle detekovaných aplikací, dle zdrojových a cílových IP adres, dle blokovaných a detekovaných virů, útoků a dalších hrozeb, dle konkrétních uživatelů apod., minimálně však v tomto rozsahu.

- rozhraní, ve kterém je možné dohledávat konkrétní provoz filtrováním dle zemí původu, uživatelů, aplikací atd., s případným dohledáváním až na úroveň jednotlivých spojení a případných otevíraných URL
- zpětně musí být možné dohledat provoz za dobu min. 12 měsíců
- jednotné rozhraní s možností sledovat provoz napříč všemi firewally i pro konkrétní zvolený firewall

K SW je vyžadována technická podpora výrobce a případné předplatné/licence výše uvedených požadovaných funkcionalit, pokud je to uvedenou plnou požadovanou funkčnost nutné, v délce trvání min. 60 měsíců.