Příloha č. 1 smlouvy

Technická specifikace předmětu plnění

1 Popis celkového řešení

Cílem dodávky zabezpečení kritické informační infrastruktury NÚKIB, zejména:

- ochrana před škodlivým kódem mezi vnější a vnitřní sítí,
- integrita mezi vnější a vnitřní sítí,
- řízení bezpečného přístupu mezi vnější a vnitřní sítí,
- segmentace sítí, bezpečnost a dostupnost služeb z vnější sítě,
- vzdálený přístup s možností vzdálené správy z důvodu zajištění provozu dle interních požadavků,
- odstranění nebo blokování přenášených dat, která nesplňují požadavky na ochranu integrity.

2 Komponenty systému ochrany síťového perimetru

2.1 Komponenta „Centrální management“

Požadavky na komponentu:

- Možnost centrální správy prvků (firewally, sandbox) včetně existujících HW prvků zadavatele (Fortinet 310B).
- Podpora pro správu min. 10 HW boxů a min. 30 virtuálních kontextů. Možnost rozšíření na min. 15 HW boxů a 50 virtuálních kontextů.
- Dodání v podobě virtuální appliance na technologii VMware.
- Podpora na 5 let v režimu 24x7xFix-time 8 h.

2.2 Komponenta *„Firewall“*

Obecné požadavky na komponentu:

- Konzolový a management port.
- Podpora VLAN, podpora LACP.
- Virtualizace v HW/OS pro min. 10 virtuálních kontextů, s možností definování maximálních povolených zdrojů (při překročení přidělených zdrojů bude ovlivněn pouze daný virtuální kontext).
- Podpora izolovaných administrátorských účtů pro jednotlivé virtuální kontexty.
- Možnost funkce v L2 režimu (transparentní inspekční režim) nebo v L3 režimu (router).
- Funkce SSL VPN v tunelovém režimu a režimu přístupu ke vnitřním službám přes webovou proxy s podporou aplikací RDP, SSH a HTTP; součástí nabídky VPN klient pro neomezený počet uživatelů, podpora dvoufaktorové autentizace uživatelů; jsou-li funkce SSL VPN licencovány na počet uživatelů, součástí nabídky v současné době musí být licence pro 500 uživatelů s možností rozšíření na 5000 uživatelů.
- Požadované bezpečnostní funkce (pokryté licencí): antivirová inspekce, kategorizace webu/web filtering, L7 analýza aplikací, detekce narušení (IPS/IDS), ochrana před únikem citlivých dat (DLP), DNS filtr, vše s podporou výrobce na 5 let.
- Podpora antivirové inspekce: signatury automaticky aktualizované výrobcem, s možností rozšíření o inspekci tzv. sandbox technikou, která nesmí být poskytována formou cloud služby, ale jako lokální VM/HW appliance.
- Funkce rozlišování aplikací pomocí L7 charakteristiky, možnost definovat vlastní aplikace pomocí signatur, automatická aktualizace od výrobce.
- Funkce kategorizace webových stránek a web filtering s podporou českých a slovenských stránek.
- Funkce ochrany úniku citlivých dat (DLP).
- Funkce Loadbalancingu provozu.

- Funkce transparentního ověřování uživatelů komunikujících skrz NGFW pomocí domény (MS Active Directory).
- Funkce ověřování uživatelů pomocí LDAP, RADIUS, SSO, Kerberos... s možností práce se skupinami uživatelů.
- Funkce GEO IP databáze, možnosti definování politiky pomocí geolokační databáze.
- Funkce reputační databáze IP adress a blokace známých botnet C&C center.
- Funkce překladu IP adres (NAT).
- Musí splňovat požadavky na logování podle vyhlášky 316/2014 §21 jako kritický informační systém. Pro logování podporovat Syslog protokol s podporou TCP a TLS (podle RFC 5425) s možností volby cíle pro logy.
- Logy musí být ve strukturovaném, zdokumentovaném tvaru.
- Funkce hloubkové analýzy provozu (packet capture) pro případ řešení problému v provozu (Debug mod).
- Funkce přeposílání dešifrovaného provozu, který prošel SSL inspekcí na externí IP adresu.
- FW cluster musí být možné v případě nedostupnosti centrálního managementu plnohodnotně spravovat pomocí lokálního GUI a CLI provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici.
- Funkce explicitní proxy přímo na firewallu (včetně autentizace uživatelů, proxy-chainingu, podpora inspekčních mechanismů a bezpečnostních funkcí (AV, IPS, Webfilter) s kapacitou pro 1000 uživatelů.
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce rozlišování aplikací dle L7 charakteru (AppControl), nikoliv pouhý TCP/UDP port), resp. kategorie URL filteringu (nikoliv jako AppControl resp. URL filtering profil aplikovaný na dané pravidlo).
- Funkce reverzní proxy (publikování webových serverů) s funkcionalitou WAF (detekce Cross Site Scripting, SQL injection, generických útoků, detekce Information Disclosure a známých exploitů, detekce Bad Botů, možnost definice a omezení parametrů (Constraint) u tolerované délky hlavičky či těla, počtu URL parametrů, Cookie), podpora manipulace s HTTP metodami (get/put/post/head/connect/options) včetně funkce Load Balancingu (round robin, static, váha, nejkratší odezva, nejmenší počet spojení) a funkce SSL offloadingu (včetně definice použitého certifikátu).
- Podpora režimu redundatní IPSEC VPN se statickým routingem (bez nutnosti použití dynamického routingu).
- Podpora vytváření virtuálních sítových propojů mezi jednotlivými virtuálními kontexty firewallu a to včetně akcelerace HW moduly.

Komponenta bude složena z UTM/NG firewall geo cluster HW appliance:

- Pracují v režimu vysoké dostupnosti v módu Active-Active/Active-Pasive/Cluster.
- Redundantní napájení s funkcí Hotswap.
- Min. 8x 10 GE SFP+ rozhraní na každém firewallu.
- Min. 10x 1 GE SFP rozhraní na každém firewallu.
- Min. 10x 1 GE RJ45 rozhraní na každém firewallu.
- Propustnost firewallu min. 50 Gbps pro IPv4 (UDP pakety 64 B) i IPv6 (UDP pakety 86B).
- Počet spojení na firewallu minimálně 10 miliónů celkem v jeden okamžik, min. 280 000 nových spojení za sekundu (nárůst).
- Propustnost IPSEC VPN min. 40 Gbps.
- Propustnost funkce IPS min. 12 Gbps.
- Podpora funkce inspekce SSL provozu s propustností min. 10 Gbps v rámci jedné lokality.
- Řešení stavového firewallu a celého šifrování na HW modulech (hlavní šifrování a dešifrování provádí zabudované nebo dodané HW moduly).
- Osazení všech rozhraní moduly (konektory) tj. 16xSFP SR, 8xSFP+ SR, a zbytek RJ45 pomocí originálních komponent.

- Splňovat minimální požadavky na všechny kryptografické funkcionality podle zákona 181/2014 a jeho platných vyhlášek.
- Podpora na 5 let v režimu 24x7xFix-time 8 h.

a UTM/NG firewall HW appliance:

- Pracují v režimu vysoké dostupnosti v módu Active-Active/Active-Pasive/Cluster.
- Redundantní napájení součástí nabídky včetně všech napájecích a propojovacích napájecích kabelů.
- Min. 2x 10 GE SFP+ rozhraní na každém firewallu.
- Min. 8x 1 GE SFP rozhraní na každém firewallu.
- Min. 8x 1 GE RJ45 rozhraní na každém firewallu.
- Propustnost firewallu min. 24 Gbps pro IPv4 (UDP pakety 64 B) i IPv6 (UDP pakety 86B).
- Počet spojení firewallu minimálně 5,5 miliónů celkem v jeden okamžik, min. 250 000 nových spojení za sekundu (nárůst).
- Propustnost IPSEC VPN min. 15 Gbps.
- Propustnost funkce IPS min. 5 Gbps.
- Podpora funkce inspekce SSL provozu s propustností min. 3,5 Gbps.
- Latence firewallu < 8 µs (udp pakety 64 B).
- Řešení stavového firewallu a celého šifrování na HW modulech (hlavní šifrování a dešifrování provádí zabudované nebo dodané HW moduly).
- Osazení všech rozhraní moduly (konektory), tj. 8xSFP SR, 2xSFP+ SR a zbytek RJ45 pomocí originálních komponent.
- Splňovat minimální požadavky na všechny kryptografické funkcionality podle zákona 181/2014 a jeho platných vyhlášek.
- Podpora na 5 let v režimu 24x7xFix-time 8 h.

2.3 Komponenta „Sandbox“

- Analýza podezřelých souborů formou sandboxingu (spuštění, otevření podezřelého souboru v izolovaném prostředí příslušného operačního systému s reálným vyhodnocením chování daného souboru).
- Plnohodnotná a obousměrná integrace s nabízenou firewall platformou, informace o výsledcích kontrol na sandboxu dostupné v centrálním managementu.
- Dodání formou virtuální appliance nasazené v existujícím prostředí zadavatele (vSphere verze 6.5).
- Požadovaná VM appliance s možností škálování výkonu licenčním navyšováním počtu běžících instancí sanboxovaného OS.
- Podpora skenování souborů v režimu online nebo na span portu.
- Funkce reportingu nalezených problémů.
- Podporované OS MS Windows 10.
- Podpora Android (výhodou, volitelně).
- Počet instancí MS Windows 10 – 8x (Licenci pro OS může dodat zadavatel).
- Počet instancí pro inspekci MS Office dokumentů – 4x (Licence může dodat zadavatel).
- Podpora inspekce minimálně: spustitelných souborů, MS Office souborů, Adobe Flash souborů, PDF, JAR souborů, skriptů (nap. vbs) a multimediálních soborů a to včetně podpory běžně používaných archivů.
- Zařízení disponuje API, pomocí kterého lze obousměrně propojit sandboxovací inspekci s aplikací zákazníka za účelem zkoumání potencionálně nebezpečných vzorků, počet takto připojených aplikací nesmí být omezován.
- Součástí nabídky musí být provázání sandbox zařízení s portálem elektronické podatelny za účelem analýzy vkládaných souborů včetně potřebné implementace.
- Podpora v režimu 24x7 na dobu 5 let.
- Podpora automatizovaného scannování potencionálně nebezpečných souborů na sdílených síťových discích přes protokol CIFS/SMB a NFS.

- Podpora zákazníkem připravené verze OS (custom VM image) - možnost importovat do sandbox prostředí image pracovní stanice (OS Windows XP, 7, 8, 8.1 a 10 + další používané aplikace) či serveru (OS Windows Server 2008,2012 a 2016).
- V případě identifikace škodlivého kódu, sandbox okamžitě vytváří lokální AV/URL databázi, kterou okamžitě sdílí s NGFW platformou.
- Možnost integrace sandboxu s endpoint SW, který funguje jako Sandbox Agent.
- Možnost navýšení kapacity sandboxingu rozšířením o další appliance.

2.4 Komponenta „End-point software pro pracovní stanice“

Software pro koncové pracovní stanice zaměstnanců NÚKIB:

- Zabezpečení pracovní stanice formou antivirové inspekce, webového filtru s funkcí kategorizace, aplikační firewall.
- Podporované systémy (end-point security): MS Windows 7, 8/8.1, 10, Server 2008, 2012 a 2016; Mac OSX.
- Management software pro Windows Server 2008, 2012 a 2016.
- VPN připojení s funkcí ověřování uživatele personálním certifikátem a dvoufaktorovou autentizací.
- Obousměrná spolupráce s nabízenou UTM/NG firewall platformou.
- Podpora výrobce a subskripce na 5 let.

2.5 Komponenta „Token“

Generátory jednorázových hesel – obecné požadavky:

- OTP se skládá z min. šesti číslic, OATH TOTP (RFC6238).
- Integrace s nabízenou UTM/NG firewall platformou a end-point softwarem pro VPN připojení uživatel (např. Radius server nebo integrovaná podpora).

Tokeny budou jak ve formě mobilní softwarové aplikace, tak ve formě hardwarového tokenu:

- Mobilní aplikace pro SW token musí být podporována systémy Windows Mobile, Android, iOS,
- HW token musí mít dobře čitelný LCD displej a životnost baterie min. 2 roky.

3 Počty nakupované techniky

komponenta	počet
Centrální management	1
Firewall - UTM/NG firewall geo cluster HW appliance	6
Firewall - UTM/NG firewall HW appliance	1
Sandbox	2
End-point software pro pracovní stanice	400
Tokeny – softwarové	200
Tokeny – hardwarové	50

4 Seznam některých zkratek

zkratka	význam

CIFS/SMB	Common Internet File System / Server Message Block
CLI	command-line interface
GUI	graphical user interface
HTTP(S)	Hypertext Transfer Protocol (Secure)
HW	hardware
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NFS	Network File System
NGFW	Next-Generation Firewall
OATH	Initiative for Open Authentication
OS	operační systém
RDP	Remote Desktop Protocol
SFP	Small Form-factor Pluggable
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	single sign-on
SW	software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOTP	Time-based One-Time Password
UDP	User Datagram Protocol
UTM/NG	Unified Threat Management / Next Generation
VPN	virtuální privátní síť