PŘÍLOHA č. 5 – Technická specifikace

Zadání:

- náhrada stávajících FW Cisco ASA5585-X, zajišťujících ochranu na vnějším perimetru, včetně rozšíření FW na vnitřní perimetr a náhrada VPN koncentrátorů Cisco ASA5520-X technologií NGFW se závaznými parametry, které nabízené řešení musí splňovat, uvedenými v této příloze (dále v rámci této přílohy také jako „**upgrade systému**“)

Požadovaný stav (podrobně dále v této příloze): (*)

- vnější perimetr (2x 1Gbps Active/Backup na ISP):
  - přenesení stávající konfigurace z FW ASA5585-X
  - zajištění optimalizace pravidel pro instalovanou platformu NGFW
  - zajištění neomezeného počtu VPN s možností lokálního routingu dle aplikací s možností clientless přístupu
- vnitřní perimetr:
  - zajištění filtrování 2x WiFi (Cisco WLC 5515)
  - zajištění filtrování DC x LAN (DC core: 2x Cisco Nexus 93180, LAN aggregation: 2x Cisco Catalyst C6880-X)

(*) údaje v závorkách jsou pro informaci dodavatele, nikoli jako předmět dodávky

Jedná se o dodávku HW, SW, prací, podpory a školení:

- HW a SW tvoří neoddělitelnou dodávku (pro vnější i vnitřní perimetr). Dodaný HW a SW musí splňovat všechny požadavky na výkon a funkčnost uvedené v této příloze.
- Práce jsou spojené s instalací a konfigurací všech dodaných zařízení v prostředí kupujícího. Dále se jedná o migraci stávajících bezpečnostních pravidel a nahrazení stávajících FW a VPN novým systémem.
- Školení – kupující požaduje zaškolení 2 pracovníků. Školení bude vedeno autorizovaným instruktorem, nebo autorizovaným školícím centrem. Školení může probíhat on-line, v prostorách kupujícího nebo prodávajícího, a to dle dohody smluvních stran.
- Dokumentace - kupující požaduje dodání dokumentace nového řešení v českém jazyce a v elektronické formě na vhodném nosiči dat

Časování dodávek:

- D: účinnost smlouvy (zveřejnění v registru smluv)
- D+4w – dodání HW a SW (dodání HW a SW do 4 týdnů od účinnosti smlouvy)
- D+8w – akceptace konfigurace (odevzdání HW, SW, konfigurace, migrace FW a VPN v plně funkčním stavu do prostředí ČRo do 8 týdnů od účinnosti smlouvy)

Akceptace nového systému:

Akceptace proběhne podpisem protokolu o poskytnutí plnění (příloha této smlouvy)
vnější perimetr:
- funkčnost min 1:1 oproti stávajícímu řešení
- napojení dodávaného systému na SIEM (IBM QRadar) pro bezpečnostní monitoring logů
- napojení dodávaného systému na Cisco ISE,
- napojení dodávaného systému na Active Directory (AD WS2016),
- zprovoznění VPN,
- napojení dodávaného systému na interní Certifikační autoritu,
- konfigurace výstupu dat pro provozní monitoring systémem Zabbix

vnitřní perimetr:
- kontrola nad toky dat mezi vnitřními segmenty sítě (mezi LAN a WIFI a mezi LAN DC),
- konfigurace výstupu dat pro provozní monitoring systémem Zabbix

- dodání dokumentace dodaného HW a SW, jejich konfigurace a dokumentace provozních činností (tj. dodržování požadované úrovně podpory, zajištění update nebo upgrade dodaného SW, security patches web, servicedesk, telefonická podpora, přístup do KBase výrobce a konzultace v rozsahu 12 MD za rok, s možností nevyčerpaných dnů do dalších let, příp. s čerpáním dopředu),

Požadovaná úroveň podpory:

- při HW závadě kupující požaduje zaslání náhradního HW následující pracovní den (NBD) po celou dobu trvání podpory
- SLA1: 24x7, po dobu účinnosti smlouvy kritické závady, nefunkčnost řešení, nefunkční část služeb bez možnosti workaround (Kritická závada znemožňuje funkčnost řešení jako celku nebo některých jeho částí a nelze zajistit dočasné náhradní řešení a je přímo ohrožen provoz systémů ČRo). Služby jsou zde chápány jako jednotlivé funkčnosti systému, s požadavky na ně kladenými dle výčtu v připojených požadavcích – systém zajišťuje dohledování, filtraci specifikovaných toků dat mezi specifikovanými sítěmi s vazbou na okolní systémy, ze kterých získává data, nebo kterým data zasílá
- SLA2: 8x9 NBD, po dobu trvání podpory
    - závada, pro niž je zajištěn workaround (tzn. závada, při které, je možno zajistit dočasné náhradní řešení)
- zajištění update/upgrade dodávaného systému security patches po dobu účinnosti smlouvy
- web / servicedesk / telefonická podpora / přístup na KBase výrobce dodávaného řešení
- konzultace v rozsahu 12MD/rok s vykazatelným čerpáním, s možností přenášení nevyčerpaných MD do dalších let (čerpání zpětně), případně s čerpáním dopředu - jde o čerpání MD na konzultace (telefonické, online, příp. osobní, pokud bude nutná přítomnost dodavatele v místě plnění), implementační práce nebo úpravy stávajícího řešení

Společné požadavky na dodávaný systém:

- jednotná správa s možností vzdálené správy z mobilních zařízení (VPN, NB, Tablet, mobil)
- HA, bezvýpadkový upgrade
- zálohy konfigurace do čitelného formátu

Požadavky HW a SW na zařízení pro zajištění vnějšího perimetru:

- kompletní zpracování toku provozu LAN vs ISP
- kompletní zpracování toku LAN vs DMZ
- kompletní zpracování toku DMZ vs DMZ
- kompletní zpracování toku DMZ vs ISP

Požadavky HW a SW na zařízení pro zajištění vnitřního perimetru:

- kompletní zpracování toku WiFi WLC vs LAN
- kompletní zpracování toku DC vs LAN

(uchazeč musí všechny položky vyplnit ANO)	**Splňuje Ano/Ne**
Základní požadavky na FW pro vnější perimetr:	
Bezpečnostní zařízení typu firewall (dále též pouze FW) musí být jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, AS signatur, databází pro URL kategorizaci, sandbox definic apod. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti FW	
Požadavky na HW architekturu:	
Součástí dodávky je dvojice FW, které budou provozovány v režimu HA	
Všechny parametry propustnosti musí dodavatel uvádět v real world mix paketech, tzv. "application mix"	

FW musí být typu HW appliance a musí používat stejný (totožný) operační systém jako FW pro vnitřní perimetr.	
Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění	
FW musí obsahovat alespoň jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	
FW musí obsahovat minimálně 4 SFP+ datové porty o rychlosti 10Gbps	
FW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW	
FW musí být schopen ukládat logové údaje na interní SSD storage o velikosti minimálně 240 GB	
FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	
FW musí být rozměrově kompatibilní s 19“ rozvaděčem	
FW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V, vyměnitelné za běhu zařízení	

Požadavky na High Availability (HA):

FW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení	
FW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	
FW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti	
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 FW	
FW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA a nedostupnosti specifikované IP adresy	

Obecné výkonové parametry:

Propustnost firewallu při aplikační kontrole veškerého procházejícího provozu musí dosahovat hodnoty alespoň 5 Gbps	
Propustnost firewallu při aplikační kontrole veškerého procházejícího provozu a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 2,2 Gbps	
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 1 000 000	
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 55 000	

Síťová funkcionalita:

FW musí plně podporovat IPv4 i IPv6	
FW musí podporovat současné zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	
FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	
FW musí podporovat směrování typu Static route, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	

VPN:

FW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	
FW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (TLS, či DTLS)	
Počet současně připojených uživatelů nesmí být licenčně omezený	
Dodávané řešení musí obsahovat funkcionalitu kontroly připojovaných zařízení, která musí být v souladu s předdefinovanými podmínkami. Např. verze OS, nainstalovaný antivirový nástroj apod.	

FW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows, MacOSX, Linux, Android a iOS	
Propustnost IPSec musí být alespoň 2,5Gbps	

Management:

Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování. GUI musí obsahovat offline kontextovou nápovědu	
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	
Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci všech nastavení, týkajících se bezpečnostních a dalších politik i rozhraní a směrování	
Jednotlivé HW appliance musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash disku	
FW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	
FW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	
FW musí podporovat nativní nástroj pro odchycení provozu	
FW musí být možné spravovat z administrátorských stanic s OS Windows a MacOSX	
V případě použití centrálního managementu musí FW obsahovat funkci, zajišťující opětovné připojení k tomuto managementu v případě jeho neúmyslného odpojení (např. nevhodnou konfigurací bezpečnostního pravidla)	
FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí FW	

Aplikační kontrola:

FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	
Definovaná aplikace musí představovat "match kritérium" v bezpečnostním pravidle	
FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	
FW musí podporovat identifikaci aplikací na nestandardních portech	
Identifikace aplikace musí probíhat přímo ve FW	
FW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	
FW musí podporovat řízení neznámého provozu	
FW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	

Kontrola na úrovni uživatelských identit

FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	
Uživatelská identita musí představovat "match kritérium" v bezpečnostním pravidle	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	

FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	
FW 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)	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	

Dešifrování

FW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	
FW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	
FW musí podporovat dešifrování Secure Shell (SSH) provozu a řídit tunelované aplikace	
Provoz pro dešifrování musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	
FW musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	
FW musí podporovat dekrypci protokolu TLS verze 1.3	
FW 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 FW. (tzv. decryption broker)	
FW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.	

Sandboxing

FW musí obsahovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející minimálně protokoly HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB.	
Sandbox systém musí být od stejného výrobce jako je FW, ale nemusí být HW součástí FW	
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý	
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze, pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	
Sandbox musí poskytovat aktualizace signatur pro AV, URL filtering, DNS, C&C	
Sandbox musí podporovat analýzu vzorku na operačním systému instalovaném přímo na hardwaru, tzn. ne ve virtuálním prostředí	
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní FW	
Aktualizace zero-day signatur musí být instalována do FW v intervalu max. 5 minut	

Bezpečnostní funkcionality

FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	
FW musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	

FW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	
FW musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	
FW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	
FW musí podporovat import SNORT signatur	
FW musí obsahovat funkci blokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	
FW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	
FW 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 úrovní bezpečnostního pravidla	
FW musí poskytovat možnost zabránit odeslání platných doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	
FW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	
FW musí obsahovat funkci analýzy DNS dotazu tzv. Sinkhole funkcí, která na dotaz malware DNS URL vratí podvrženou IP adresu pro detailnejší analýzu a zároveň se stanice na původní malware stránku nedostane.	
FW musí obsahovat funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	
FW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.	
FW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování	

Ochrana proti DoS

FW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a aplikace	

QoS

FW 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.)	
FW musí podporovat prioritizaci provozu na základě DSCP	
FW musí podporovat prioritizaci provozu na základě Identifikované aplikace	

URL filtering

FW musí obsahovat nativní podporu pro využívání databáze URL	
URL databáze musí být od stejného výrobce jako je FW	
FW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	
FW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	

FW musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní FW bez nutnosti kontaktování technické podpory	

Logování

FW musí obsahovat lokální úložiště logů	
FW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	
FW 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	
FW musí podporovat přeposílání logů na zařízení třetích stran	
FW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	
Přeposílané logy z FW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ), zákazník vlastní SIEM IBM QRadar 7.4.	

Servisní podpora a licenční plán

FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	
Požadovaná délka podpory a platnosti licencí je tři roky od nasazení zařízení do sítě kupujícího.	

Migrace, konfigurace, nasazení do provozu

Návrh zapojení FW do současné síťové infrastruktury.	
Prvotní migrace stávajících pravidel FW bude provedena 1:1	
Počet bezpečnostních pravidel určených k migraci je: **370**	
Počet překladových pravidel NAT určených k migraci je: **200**	
Počet migrovaných L3/VLAN interface je: **10**	
Počet Site-To-Site IPsec VPN k migraci: **5**	
Součástí implementace bude úprava stávajících L3/L4 pravidel na pravidla založená na L7 (nejen protokol a port, ale i aplikace)	
Součástí implementace je „hardening“ firewallu do nejvyššího možného zabezpečení s ohledem na nenarušení provozu	
Součástí implementace je vyladění falešných pozitiv systému Threat Prevention, jako je IPS, AV, AntiBot	
Implementace bude provedena s co nejkratšími možnými výpadky provozu, v případě nutnosti mimo pracovní hodiny/pracovní týden	
Návrh a provedení integrace stávajícího řešení VPN koncentrátoru	
Konfigurace napojení na SIEM zadavatele	
Konfigurace napojení na provozní monitoring zadavatele (Zabbix).	
Zálohování konfigurace FW	
Dodavatel zpracuje dokumentaci konfigurace a zapojení FW do síťové infrastruktury	
Veškeré instalační a konfigurační práce budou provedeny osobou s nejvyšší dostupnou certifikací na dodávané řešení	

Základní požadavky pro FW pro vnitřní perimetr:

Bezpečnostní zařízení typu firewall (dále též pouze FW) 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 FW	

Požadavky na HW architekturu:

Součástí dodávky je dvojice FW, které budou provozovány v režimu HA	
Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"	
FW musí být typu HW appliance a musí používat stejný (totožný) operační systém jako FW pro vnější perimetr.	
Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění	
FW musí obsahovat alespoň jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	
FW musí obsahovat minimálně 8 SFP+ datové porty o rychlosti 10Gbps	
FW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW	
FW musí být schopen ukládat logové údaje na interní SSD storage o velikosti minimálně 240 GB	
FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	
FW musí být rozměrově kompatibilní s 19“ rozvaděčem	
FW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V, vyměnitelné za běhu zařízení	

Požadavky na High Availability (HA):

FW musí podporovat režim HA v módu Active-Active složený alespoň ze dvou zařízení	
FW musí podporovat režim HA v módu Active-Standby složený alespoň ze dvou zařízení	
FW musí podporovat režim clusteringu, využitelný pro případné dodatečné zvýšení propustnosti	
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 FW	
FW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy	

Obecné výkonové parametry:

Propustnost firewallu při aplikační kontrole veškerého procházejícího provozu musí dosahovat hodnoty alespoň 6 Gbps	
Propustnost firewallu při aplikační kontrole veškerého procházejícího provozu a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 3 Gbps	
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 2 000 000	
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 70 000	

Síťová funkcionalita:

FW musí plně podporovat IPv4 i IPv6	
FW musí podporovat současné zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	
FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	

FW musí podporovat směrování typu Static route, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	
PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel	

VPN:

FW musí podporovat site-to-site VPN pomocí protokolu IPSec. Počet tunelů nesmí být licenčně omezený	
Propustnost IPSec musí být alespoň 3 Gbps	

Management:

Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování	
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	
Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci všech nastavení, týkajících se bezpečnostních a dalších politik i rozhraní a směrování.	
Jednotlivé HW appliance musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash disku	
FW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	
FW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	
FW musí podporovat nativní nástroj pro odchycení provozu	
FW musí být možné spravovat z administrátorských stanic s OS Windows a MacOSX	
V případě použití centrálního managementu musí FW obsahovat funkci, zajišťující opětovné připojení k tomuto managementu v případě jeho neúmyslného odpojení (např. nevhodnou konfigurací bezpečnostního pravidla).	
FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí FW	

Aplikační kontrola:

FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	
Definovaná aplikace musí představovat "match kritérium" v bezpečnostním pravidle	
FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	
FW musí podporovat identifikaci aplikací na nestandardních portech	
Identifikace aplikace musí probíhat přímo ve FW	
FW musí detekovat a zabránit aplikaci měnit porty, tzv. port-hopping	
FW musí podporovat řízení neznámého provozu	
FW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	

Kontrola na úrovni uživatelských identit

FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	

Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	
Uživatelská identita musí představovat "match kritérium" v bezpečnostním pravidle	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	
FW 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)	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno ze systému Cisco ISE	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	

Dešifrování

FW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	
FW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	
FW musí podporovat dešifrování Secure Shell (SSH) provozu a řídit tunelované aplikace	
Provoz pro dešifrování musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	
FW musí podporovat dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	
FW musí podporovat dekrypci protokolu TLS verze 1.3	
FW 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 FW. (tzv. decryption broker)	
FW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.	

Bezpečnostní funkcionality

FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	
FW musí podporovat, nikoliv obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	
FW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	
FW musí podporovat, nikoliv obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	
FW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	
FW musí podporovat import SNORT signatur	
FW musí podporovat možnost zablokování útoku využívajícího známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci	

FW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	
FW 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 úrovní bezpečnostního pravidla	
FW musí poskytovat možnost zabránit odeslání platných doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	
FW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	
FW musí podporovat, nikoliv obsahovat funkci analýzy DNS dotazu tzv. Sinkhole funkcí, která na dotaz malware DNS URL vratí podvrženou IP adresu pro detailnejší analýzu a zároveň se stanice na původní malware stránku nedostane.	
FW musí podporovat, nikoliv obsahovat funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase.	
FW musí podporovat integraci se systémem Cisco ISE pro zařazení koncové stanice do karantény při detekování nevhodného chování	

Ochrana proti DoS

FW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a aplikace	

QoS

FW 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.)	
FW musí podporovat prioritizaci provozu na základě DSCP	
FW musí podporovat prioritizaci provozu na základě Identifikované aplikace	

URL filtering

FW musí podporovat, nikoliv obsahovat nativní podporu pro využívání databáze URL	
FW musí obsahovat možnost tvorby vlastních URL kategorií	
FW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	
FW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	
FW musí umožňovat požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní FW bez nutnosti kontaktování technické podpory	

Logování

FW musí obsahovat lokální úložiště logů	
FW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	
FW 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	

FW musí podporovat přeposílání logů na zařízení třetích stran	
FW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	
Přeposílané logy z FW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	

Servisní podpora a licenční plán

FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	
Požadovaná délka podpory a platnosti licencí je tři roky od nasazení zařízení do sítě kupujícího.	

Migrace, konfigurace, nasazení do provozu

Návrh zapojení FW do současné síťové infrastruktury.	
Samotné zapojení FW v režimu L3	
Návrh postupu tvorby nových bezpečnostních pravidel	
Součástí implementace je „hardening“ firewallu do nejvyššího možného zabezpečení s ohledem na nenarušení provozu	
Implementace bude provedena s co nejkratšími možnými výpadky provozu, v případě nutnosti mimo pracovní hodiny/pracovní týden	
Konfigurace napojení na SIEM zadavatele	
Konfigurace napojení na provozní monitoring zadavatele (Zabbix).	
Zálohování konfigurace FW	
Dodavatel zpracuje dokumentaci konfigurace a zapojení FW do síťové infrastruktury	
Veškeré instalační a konfigurační práce budou provedeny osobou s nejvyšší dostupnou certifikací na dodávané řešení	

Školení – on- site nebo online (dle dohody smluvních stran)

Školení správců FW formou certifikačního školení pro 2 osoby	
Školení bude vedeno autorizovaným instruktorem, nebo autorizovaným školícím centrem	