# Příloha č. 1

# Základní technické požadavky

* Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, …)
* Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti desktop
* Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem.
* Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality

# **HW parametry**

* Počet síťových rozhraní RJ45 100/1000 - min 8x
* Dedikovaný konzolový port – min 1x
* USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x
* Bluetooth Low Energy (BLE)
* Minimálně 2 x SFP+ port
* Podpora redundantního napájení

# **Výkonnostní parametry**

* Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 27000 Mbps, 27000 Mbps, 25000 Mbps
* Latence firewallu (64 B UDP paket) - max 3,5 mikro sec
* Počet naráz otevřených spojení – min 1 450 000
* Počet nových spojení za sekundu - min. 120 000
* Počet firewall pravidel až 5 000

# **Networking**

* Režim fungování L2 – transparentní režim, L3 – NAT/Router
* Podpora VLAN
* Podopora multicast, vytváření politiky pro multicast routování
* Podpora 802.3ad link aggregation
* Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
* Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
* Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
* Policy-based routing
* Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky)
* Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN).
* Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti.
* Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 200 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu.

# **Funkce IPsec VPN**

* podpora site-to-site VPN
* podpora klientských VPN
* dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek
* funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence.
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 180
* Minimální počet klientských IPSEC VPN tunelů: 2200
* propustnost IPSec VPN min. 23 Gbps (měřeno při AES256-SHA256)
* podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
* podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
* podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
* Podpora VXLAN
* Podpora L2TP, PPTP, GRE
* podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec

# **UTM funkce**

## Funkce detekce aplikací na L7 (Application Control)

* + detekce známých aplikací na základě signatur
  + signaturový database automaticky aktualizované výrobcem
  + alespoň 4 000 podporovaných aplikací
  + pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci)
  + možnost tvorby vlastních signatur
  + detekované aplikace je možné: povolit, monitorovat, blokovat
  + na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
  + funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.

## Funkce detekce a potlačení narušení (IPS/IDS)

* + minimální propustnost IPS inspekce 4,3 Gbps
  + signatury automaticky aktualizované výrobcem
  + alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
  + možnost tvorby vlastních signatur
  + funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
  + funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu

## Funkce antivirové kontroly

* + ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem
  + signatury automaticky aktualizované výrobcem
  + požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
  + možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce
  + deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2100 Mbps
  + funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
  + Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
  + Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací.

## Funkce kategorizace webových stránek

* + založená na centrálně spravované databázi výrobce
  + minimálně 50 filtračních kategorií
  + možnost definice vlastních kategorií
  + možnost definice vlastních seznamů zakázaných URL
  + kategorizace musí zahrnovat I české a slovenské internetové stránky

## Funkce blokování video obsahu portálu YouTube

* + založená na centrálně spravované databázi výrobce
  + minimálně 9 filtračních kategorií
  + možnost definice vlastních kanálů na základně channel ID

## Funkce DNS filtru

* + Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
  + Možnost definovat vlastní tzv. deny-list domén
  + Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
  + Možnost importu seznamu blokovaných domén do DNS filtru
  + Detekce a blokování komunikace do botnet sítí

## Funkce ochrany před únikem citlivých informací (DLP)

* + možností analýzy běžných typů dokumentů a protokolů
  + možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum

## Funkce blokace stahování konkrétních typů souborů

* + možnosti zablokovat stahování souborů s konkrétními typy, jako napři. MSI, EXE…
  + funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.

## Emailový antispamový modul

* + jednoduchá antispamová a antivirová inspekce elektronické pošty

## Podpora SSL dekrypce

* + podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízeních, nebo serverů
  + funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
  + zařízení musí u SSL inspekce dosáhnout min. propustnost 2500 Mbps

## Podpora pravidel pro obranu proti útokům typu DoS

* + zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení.
  + podpora detekce anomálií na 3. a 4. vrstvě
  + podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION
  + funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti

## Explicitní proxy

* + podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
  + podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
  + funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
  + Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém server

# **Firewall**

* Možnost nastavovat firewall politiku na základě geografických údajů
* Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
* Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
* Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
* Viditelnost do provozu na aplikační úrovni
* Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy
* 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 application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
* Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
* Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
* Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
* Podpora funkce reverzní proxy
* Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
* Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření

# **Management**

* FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

# **Příslušenství**

* Součástí dodávky bude rack mount kit

# **Konfigurace**

* Registrace zařízení pro podporu UTM a advanced security
* Instalace stabilní produkční verze
  + Instalace poslední stable verze
* Segmentace sítě + adresace VLAN
  + Segmentace sítě do 5 různých VLAN (MGMT, WIFI žáci+učitelé, LAN žáci+učitelé)
* Inter VLAN routing a pravidla
  + Vytvoření pravidel pro jednotlivé přístupy mezi VLAN
  + Nastavení pravidel pro jednotlivé služby a porty
* SD-WAN
  + Konfigurace interface pro dvě síťové konektivity
  + Vytvoření pravidel provozu
  + Nastavení směřování na jednotlivé IP
  + Nastavení restrikcí
* Konfigurace UTM profilů (bezpečnostní profily)
  + Definování profilů pro jednotlivé VLAN
  + Nastavení definic a přístupů na Weby, aplikace
  + Nastavení DNS ochrany
  + Nastavení antivirových definic
  + Dle provozu, optimalizace pravidel UTM a firewall
* Konfigurace VPN
  + Vytvoření IPSEC VPN
  + Nastavení FW adresace
  + Nastavení FW pravidel a přístupů
  + Případná instalace VPN klienta
* Integrace do Active Directory organizace
  + Namapování AD serveru
  + Synchornizace AD skupin dle potřeb
  + Nastavení AD skupin pro potřeby VPN