

***Projektová dokumentace***

***„Vybudování JCE IB SOŠ INFORMATIKY A SPOJŮ A SOU  
KOLÍN - zpracování projektové dokumentace“***

***TECHNOLOGICKÁ ČÁST JCE IB***

***D.1.4.9. Technologie a řešení JCE IB***

***D.1.4.9.12. VIRTUÁLNÍ FIREWALL (NGFW) PRO  
EXPERIMENTÁLNÍ PROSTŘEDÍ - CYLAB***

**Zpracoval:**

Petr Lacina

## 12 VIRTUÁLNÍ FIREWALL PRO EXPERIMENTÁLNÍ PROSTŘEDÍ ŠKOLY - CYLAB

---

### 12.1 ŘEŠENÍ OCHRANY PERIMETRU V RÁMCI TESTOVACÍCH BEZPEČNOSTNÍCH SCÉNÁŘŮ

S ohledem na IT výuku a cíle vzdělávání studentů je součástí dodávky virtuální firewall (dále jen **NGFW**) sloužící k testování bezpečnostních scénářů experimentálním virtuálním prostředím školy (dále jen **CYLAB**). Z důvodu flexibility řešení je požadována jedna virtuální appliance do virtuálního prostředí dodávaného v rámci tohoto projektu do CYLAB. Na tomto zařízení není vyžadováno použití žádných bezpečnostních funkcí jako URL filtrace, ochrana před malware, IPS atd. Do budoucna je toto, ale nutné předpokládat i s případným požadavkem na variabilní využití subskripcí dle potřeby (např. výměna subskripce URL filtrace za DNS security). Nyní se nepředpokládá ani využití vzdáleného VPN klientského připojení. Virtuální firewall musí být od stejného výrobce jako hardwarové appliance na ochranu perimetru ŠKOLY.

Součástí virtuálního firewallu je podpora aktualizací po dobu 5-ti let včetně instalace a základní konfigurace NGFW.

## 12.2 SPECIFIKACE MINIMÁLNÍCH POŽADAVKŮ TECHNICKÉHO ŘEŠENÍ

### 12.2.1 NGFW – 1 kus

Parametr	Požadovaná hodnota
<b>Základní požadavky</b>	Výrobce FW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls reportu společnosti Gartner v posledním aktuálním reportu a minimálně 5 let v řadě před tímto aktuálním reportem
<b>Požadavky na architekturu</b>	Všechny parametry propustnosti musí dodavatel uvadět v real world mix paketech, tzv. "application mix"
	FW musí být typu SW appliance
	Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídicí modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění
	Virtualni FW musí podporovat AWS, Azure, ESXi, Google Cloud Platform, Hyper-V, KVM, NSX-V, OCI, Alibaba Cloud, Cisco ACI, Cisco CSP, Cisco ENCS, NSX-T
	FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)
<b>Požadavky na High Availability (HA):</b>	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 i v geograficky oddelených lokalitách
	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
<b>Obecné výkonové parametry</b>	Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň 2 Gb/s (app mix)
	Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 1 Gb/s (app mix)
	Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 250 000
	Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 15 000
<b>Síťová funkcionalita:</b>	FW musí plně podporovat IPv4 i IPv6
	FW musí podporovat 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, RIP, 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 (min. TLS v1.2)
	Počet současně připojených uživatelů nesmí být licenčně omezený
	FW musí pro Remote Access VPN poskytovat připojení z klientských operačních systémů Windows a macOS
	Propustnost IPSec musí být alespoň 1 Gb/s
Správa řešení	Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu síťových a bezpečnostních funkcí bez nutnosti používání centrálního management serveru.
	GUI musí podporovat 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 síťových nastavení, bezpečnostních a dalších pravidel, nastavení síťových rozhraní a směrování.
	Jednotlivé HW appliance musí umožňovat automatickou konfiguraci nových FW použitím konfiguračních šablon na připojeném 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 odchyčení provozu
	FW musí být možné spravovat z administrátorských stanic s OS Windows a macOS (včetně HW s čipem Apple Silicon)
	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" při policy lookup
	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 plnohodnotných, uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
<b>Kontrola na úrovni uživatelských identit</b>	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" při policy lookup
	FW musí umožňovat automaticky přesun uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence
	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 kontrolér
	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 prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog
	FW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)
	FW musí podporovat získávání vazby IP adresa-uživatelské jméno přes webový formulář - Captive Portal
	FW musí podporovat získávání vazby IP adresa-uživatelské jméno z VPN agenta
	FW musí podporovat získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)
	FW musí podporovat získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček
	FW musí podporovat kontrolu klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná
<b>Dešifrování</b>	FW musí podporovat dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům

	FW musí podporovat dešifrování příchozího SSL/TLS provozu, za pomoci nainportovaného privátního klíče interního serveru
	FW musí podporovat dešifrování Secure Shell (SSH proxy) a kontrolovat tunelované aplikace
	Dešifrovaný provoz 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 pomoci ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz
	FW musí podporovat dešifrování 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 následně přepośle čistě přefiltrované data zpět do FW. (tzv. decryption broker)
	FW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu.
<b>Sandboxing</b>	Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem 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, Webfiltering, 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 reálném čase, čili s nulovou prodlevou
	FW musí být schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.
	FW musí být schopen detekovat neznámé vzorky přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu.
<b>Bezpečnostní funkcionality</b>	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, HTTP/2, FTP a SMB
	FW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele
	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 podporovat import SNORT signatur
	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 úrovni bezpečnostního pravidla
	FW musí poskytovat možnost zabránit odeslání 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 analýzu DNS dotazu tzv. sinkhole funkcí, která při DNS dotazu na škodlivou doménu vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane.
	FW musí poskytovat možnost rozšíření o funkcionality 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
<b>Ochrana proti DoS</b>	FW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojové a cílové IP adresy a uživatelská identita
<b>QoS</b>	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
<b>URL filtering</b>	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 kategorií 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
<b>Logování a reportování</b>	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)
	FW musí umožňovat vytváření vlastních reportů přímo z grafického rozhraní FW
<b>Servisní podpora a licenční plán</b>	FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů
	Požadovaná délka podpory a platnosti licencí je 5 let od nasazení zařízení do sítě objednatele.