

Uživatelská příručka

Kernun Security Appliance

Obsah

1	Úvod.....	3
2	GUI konfigurační rozhraní.....	3
2.1	Monitoring.....	3
2.2	Konfigurace.....	3
2.2.1	Rozhraní.....	3
2.2.2	Rezolvování.....	4
2.2.3	Směrování.....	4
2.2.4	QOS.....	4
2.3	Služby sítě.....	4
2.3.1	OpenVPN.....	4
2.3.2	IPSec.....	5
2.3.3	DHCP Server.....	5
2.3.4	DNS server.....	5
2.3.5	Vzdálená správa.....	5
2.3.6	Zpětná vazba.....	5
2.3.7	NTP klient.....	6
2.3.8	SNMP.....	6
2.3.9	Proměnné.....	6
2.4	Ochrana.....	7
2.4.1	Stavový firewall.....	7
2.4.2	Proxy.....	7
2.4.3	Reverzní proxy.....	9
2.4.4	Adaptivní firewall.....	9
2.4.5	IPS.....	9
2.4.6	Honeypot.....	9
2.5	System.....	10
2.5.1	Správa.....	10
2.5.2	Autentizace.....	11
2.5.3	Databáze.....	11
2.5.4	Administrační rozhraní.....	11
2.6	Uživatelé.....	11
2.6.1	Seznam uživatelů.....	11
3	Doporučené nastavení KSA.....	12
3.1	Výchozí nastavení KSA.....	12
3.2	Doporučení k nastavení bezpečnosti a provozu.....	12
3.2.1	Bezpečnostní funkce.....	12
3.2.2	Řízení provozu.....	13
3.2.3	Konfigurační GUI.....	13
3.2.4	Služby sítě.....	14
3.2.5	Upgrade KSA.....	14
4	Pokročilé funkce.....	15
4.1	Multihoming.....	15
4.2	Cluster.....	15
5	Poznámky.....	16

1 Úvod

Kernun Security Appliance (KSA) je moderní bezpečnostní řešení v oblasti kyberbezpečnosti. Umožní vám nejen nastavení síťování a zabezpečený přístup do interní sítě, také zvyšuje síťovou bezpečnost využitím pokročilé adaptivní databáze hrozeb i blokováním nevhodných webových stránek.

2 GUI konfigurační rozhraní

Kernun Security Appliance (KSA) se ovládá pomocí webového rozhraní - GUI. V každé scéně konfiguračního rozhraní je k dispozici kontextová nápověda s vysvětlením jednotlivých konfiguračních položek a dále tooltipsy.

2.1 Monitoring

V menu Monitoring se nachází grafické znázornění parametrů systému, grafy využití systémových prostředků, datový provoz, počty blokováných/povolených spojení.

V záložce Systémové záznamy lze vyhledávat konkrétní spojení např podle zdrojové/cílové ip adresy, času nebo služby.

2.2 Konfigurace

Menu Konfigurace obsahuje všechna nastavení serveru Kernun i služeb, které na něm běží.

2.2.1 Rozhraní

Konfigurace ip adres jednotlivých síťových rozhraní, lze definovat VLAN rozhraní, případně agregované linky (LACP, bonding) a bridge rozhraní.

Přidání virtuálních rozhraní se provádí najetím myši mezi existující řádky, kde se zobrazí ikonka pro volbu nového rozhraní.

Označení WAN, LAN slouží uživateli k lepší orientaci v rozhraních a dále pak se toto označení využije v předdefinovaných proměnných (viz Proměnné), které se mohou použít v konfiguraci řízení provozu (viz Řízení provozu).

Pokud chcete ve vaší síti používat ipv6, je nutno zapnout podporu ipv6 příslušným přepínačem.

Síťová rozhraní, které v systému fyzicky existují, ale nepoužívají se, lze skrýt.

2.2.2 Rezolvování

Rezolvování specifikuje, jakým způsobem zařízení Kernun překládá doménová jména na IP adresy. Toto nastavení se týká zejména provozu http proxy a stahování aktualizací. Kromě toho můžete nakonfigurovat DNS server na Kernunu a tento pak použít pro klienty vaší interní sítě (viz Služby sítě).

Tabulka doménových jmen: Lokální seznam pro převod jména počítače na IP adresu a pro zpětný převod IP adresy na jméno počítače nezávisle na záznamech DNS serverů. Tento seznam má přednost před službou DNS.

2.2.3 Směrování

Nastavuje se Výchozí brána systému Kernun, případně další směrovací záznamy (routy).

Směrování klientů: Určuje, zda směrovat provoz klientů. Pokud je zapnuté, zařízení se chová jako router. Pokud je server používán pouze jako aplikační proxy, lze směrování klientů vypnout.

Multihoming je pokročilá funkce, která umožňuje nakonfigurovat 2 konektivity (viz Pokročilé funkce).

2.2.4 QoS

QoS (quality of service) je služba, pomocí které lze konfigurovat kvalitu spojení. Umožňuje vytváření QoS stromů na rozhraní a definuje jim garantovanou a maximální použitelnou šířku pásma.

2.3 Služby sítě

2.3.1 OpenVPN

Služba OpenVPN umožňuje nastavit VPN připojení v režimu Remote Access Server a v režimu Klient.

Remote Access Server (RAS, server pro vzdálený přístup) umožňuje různým klientům připojit se k podnikové síti nebo intranetu tak, jako kdyby byli přímo připojeni na místě. Klienty mohou být různá mobilní zařízení, jako například notebooky nebo mobilní telefony, nebo PC s připojením k internetu.

Klient se připojuje k nějakému VPN serveru, typicky Remote Access Serveru. Parametry nastavení jsou určené obvykle serverovou stranou.

2.3.2 IPsec

používá se pro spojení protokolem IPsec, parametry jsou obvykle určeny protější stranou spojení.

2.3.3 DHCP Server

DHCP server lze provozovat přímo na zařízení Kernun, je možno definovat více DHCP oborů. Obor představuje jeden rozsah IP adres na vybraném síťovém rozhraní. V oboru je pak možné vytvářet fondy adres, které jsou dynamicky přidělovány klientům, a rezervace, které klientovi se zadanou MAC adresou přiřadí vždy stejnou IP adresu.

Přenosový agent: Pokud již máte vlastní DHCP server a chcete ho poskytnout klientům v jiné síti, můžete využít přenosového agenta DHCP (DHCP relay), který požadavky klientů přepošle na zadaný DHCP server.

2.3.4 DNS server

Na serveru Kernun může běžet služba DNS server, která snižuje datovou zátěž internetové konektivity tím, že provádí kešování dotazů.

Předávat dotazy nadřazeným DNS serverům získaných pomocí DHCP klienta: DNS server je nerekurzivní, adresy nadřazených DNS serverů získává pomocí DHCP klienta na vnějším rozhraní.

Provádět rekurzivní dotazy: DNS server je rekurzivním serverem.

Předávat dotazy níže uvedeným nadřazeným DNS serverům: DNS server je nerekurzivní, adresy nadřazených DNS serverů má specifikovány seznamem IP adres.

Odchytávání DNS dotazů: DNS provoz ze zvolených klientských adres je odchytáván a předáván lokálnímu DNS serveru na zařízení Kernun. Toto je doporučeno zapnout v případě zapnuté funkce bezpečné vyhledávání.

Bezpečné vyhledávání: Bezpečné vyhledávání vyčistí nevhodné výsledky vyhledání.

Povolit dotazy z jakékoliv adresy: Používá se k řízení přístupu k DNS záznamům v kešovací paměti.

2.3.5 Vzdálená správa

Nastavení vzdáleného přístupu k zařízení Kernun pomocí SSH spojení.

Služba vzdálené pomoci: Služba vzdálené pomoci dovolí pracovníkům technické podpory firmy Kernun přímý přístup na SSH terminál zařízení bez nutnosti dalších zásahů uživatele. Pro využití této služby je potřeba se nejprve domluvit s příslušným technikem firmy Kernun.

2.3.6 Zpětná vazba

Nastavení zaslání zpětné vazby o tomto zařízení.

2.3.7 NTP klient

Nastavení a synchronizace času zařízení Kernun podle protokolu NTP.

2.3.8 SNMP

Monitoring zařízení prostřednictvím protokolu SNMP verze 3.

2.3.9 Proměnné

Na základě označení interfaců tagem WAN/LAN systém Kernun automaticky vytvoří předdefinované proměnné.

Kromě toho administrátor může vytvářet vlastní proměnné. Pojmenované hodnoty a Pojmenované seznamy slouží pro zpřehlednění konfigurace v Řízení provozu.

2.4 Ochrana

V sekci Ochrana se konfiguruje bezpečnostní funkce a také řízení uživatelského provozu.

2.4.1 Stavový firewall

Stavový firewall (SF) je základním místem pro řízení uživatelského síťového provozu. Slouží jako první linie obrany Kernun Security Appliance, tudíž prochází veškerý síťový provoz, který se pak předává dalším bezpečnostním prvkům, jako je Proxy a Adaptivní firewall.

Stavový firewall se skládá z pravidel. Pravidla se vyhodnocují směrem shora dolů, na pořadí tedy záleží. Pro lepší přehled je možné mezi pravidla přidat hlavičky.

Ve Stavovém firewallu jsou nakonfigurována výchozí pravidla, která povolují provoz vzájemně mezi interními sítěmi (interfacy s označením LAN) a také veškerý provoz z interních sítí do internetu, včetně webového provozu.

Uživatelské úpravy konfigurace se provádí zakomentováním výchozích pravidel a konfigurací vlastních pravidel, při čemž lze využít upravené kopie již existujících pravidel.

Přidání položek do seznamu se provádí najetím myši na spodní okraj řádku, kde chci nové pravidlo přidávat a tam vyberu požadovanou položku.

Pořadí pravidel lze měnit přetažením myši při uchopení symbolu teček na začátku řádku pravidla.

Další doporučení k úpravě konfigurace najdete v kapitole Doporučené nastavení KSA.

2.4.2 Proxy

Služba Proxy řídí uživatelský provoz na weby, obvykle na portu 80 a 443. Využívá bezpečnostní databázi ClearWeb, která webovým stránkám přiřazuje kategorie podle obsahu. Administrátor tak může nastavovat pravidla podle kategorií ClearWebu.

Proxy lze použít buď v netransparentním režimu (proxy v prohlížeči) a nebo v transparentním režimu.

2.4.2.1 Proxy | Profily

V menu Proxy lze definovat více Profilů proxy.

Provoz je na tyto profily předáván pomocí Stavového firewallu, použitím pravidel webového provozu, kde se zadává název webového profilu. Toto se týká transparentní proxy.

Provoz přes netransparentní proxy se nastavuje přímo v Profilu proxy, kde se zadává **Síťový socket proxy serveru**, tedy kombinace IP adresy a portu pro netransparentní proxy. Pokud je tato položka vypnutá, profil bude fungovat pouze v transparentním režimu, pokud je správně nastaveno pravidlo SF pro webový provoz s tímto profilem.

Nastavení netransparentní proxy lze klientům distribuovat buď ručně, nebo prostřednictvím souboru wpaad, nebo pomocí politiky MSAD (gpo).

Profily | Nastavení profilu

Autentizace: Pro profil je možné zapnout autentizaci. Pro všechna pravidla následující za hlavičkou Autentizace bude vyžadována autentizace. V případě použití autentizace na proxy protokolem Kerberos je nutno u klientů http proxy zadávat názvem proxy, nikoli ip adresou.

TLS (Transport Layer Security): Pro profil je možné zapnout TLS inspekci pro všechna pravidla následující za hlavičkou TLS inspekce bude zapnuta TLS inspekce. TLS inspekce provozu může na méně výkonných strojích způsobovat významné snížení datové propustnosti serveru.

Nezobrazovat chybovou stránku proxy: V případě nezobrazování chybové stránky proxy se ve spojení, o kterém se ví, že bude zakázáno nebude provádět rozlamování. Při zakázání spojení tak uživatel uvidí chybu prohlížeče.

Profily - Řízení provozu

Profil se skládá z globálních položek a pravidel. Pravidla se vyhodnocují směrem shora dolů, na pořadí tedy záleží. Pro lepší přehled je možné mezi pravidla přidat hlavičky. U pravidel se mohou definovat tyto vstupní podmínky:

Uživatel: Pravidlo se aplikuje na vyjmenované uživatele, pokud je zapnutá autentizace profilu. Prázdný seznam znamená libovolný autentizovaný uživatel.

Skupina: Pravidlo se aplikuje na vyjmenované skupiny, pokud je zapnutá autentizace profilu. Prázdný seznam znamená libovolná skupina.

Klient: Pravidlo se aplikuje na vyjmenované adresy klientů. Prázdný seznam znamená libovolnou ip adresu.

Server: Pravidlo se aplikuje na vyjmenované adresy serverů. Prázdný seznam znamená libovolnou ip adresu.

Časové intervaly: Seznam časových intervalů od 0:00 do 23:59, kdy se pravidlo uplatní. Časové intervaly se vztahují pouze na vyjmenované dny v týdnu.

Dny v týdnu: Dny, kdy se pravidlo uplatní.

Kategorie: Pravidlo se aplikuje na servery patřící do vyjmenovaných kategorií.

Přidání položek do seznamu se provádí najetím myši na spodní okraj řádku, kde chci nové pravidlo přidávat a tam vyberu požadovanou položku.

Pořadí pravidel lze měnit přetažením myši při uchopení symbolu teček na začátku řádku pravidla.

2.4.2.2 Proxy | Antivirus

Antivirus je služba zajišťující kontrolu veškerých souborů procházejících skrz proxy. Pomocí nastavení Úrovně ochrany lze říci, které typy souborů se mají kontrolovat. Antivirová kontrola souborů může na méně výkonných strojích způsobit zpomalení provozu.

Pokud není zapnutá TLS inspekce, kontrolují se pouze soubory http provozu.

2.4.3 Reverzní proxy

Reverzní proxy slouží pro přístup z internetu na webové služby v interní síti na základě doménového jména v URL požadavku.

Přidání položek do seznamu se provádí najetím myši na spodní okraj řádku, kde chci nové pravidlo přidávat a tam vyberu požadovanou položku.

Pořadí pravidel lze měnit přetažením myši při uchopení symbolu teček na začátku řádku pravidla.

2.4.4 Adaptivní firewall

Adaptivní firewall je služba, která vyhodnocuje, jestli se v komunikaci neobjevila některá z adres uvedených v databázi této služby. Taková komunikace je blokována, pokud není nastavena explicitní výjimka.

2.4.5 IPS

IPS je další z bezpečnostních služeb, využívá vlastní databázi hrozeb. Služba je náročná na zdroje serveru, doporučujeme ji zapínat pouze na vyšších modelech serveru Kernun.

2.4.6 Honeypot

Honeypot je služba pro detekci útočníků. Poslouchá na definovaných adresách a portech, na kterých neposlouchá žádná nakonfigurovaná služba Kernunu. V případě, že se na tyto adresy a porty někdo připojí, je prohlášen za útočníka a zařazen na blocklist na definovanou dobu.

2.5 Systém

2.5.1 Správa

2.5.1.1 Správa | Zařízení

Informace o základních nastaveních systému.

Zařízení lze vypnout/restartovat, nahrát novou licenci a nastavit časovou zónu.

Zálohovat/obnovit konfiguraci: server se automaticky zálohuje do cloudu (viz Konfigurace | Zpětná vazba), ale je možné vyrobit si vlastní zálohu.

Cluster: Cluster slouží k zajištění vysoké dostupnosti služeb poskytovaných systémem Kernun Security Appliance. Umožňuje snížit na minimum čas výpadku v případě poruchy hardwarového zařízení. Předpokladem je redundantní zapojení dvou stejných hardwarových zařízení Kernun Security Appliance (tzv. uzlů) za použití clusterové licence. Jeden uzel clusteru je hlavní (master) a druhý záložní (backup). V případě výpadku hlavního uzlu dojde bez potřeby administračního zásahu správce k automatickému převzetí provozu záložním uzlem.

Nastavení Clusteru: viz Pokročilé funkce

2.5.1.2 Správa | Aktualizace

Aktualizace systému se provádí ručně na požadavek administrátora systému.

Vyžadovat potvrzení aktualizace uživatelem: Uživatel potvrdí aktualizaci systému přihlášením do Kernun Security Appliance, pokud toto potvrzení nenastane v daný čas, systém se restartuje do předchozí verze. Doporučujeme tuto volbu mít vždy zapnutou.

Čekání na potvrzení: Při aktualizaci se systém restartuje a následně čeká po dobu nastaveného času na uživatelské potvrzení úspěšné aktualizace. Pokud uživatel během tohoto časového úseku úspěch aktualizace nepotvrdí, restartuje se systém do původní verze a po přihlášení vyzve uživatele k opakování aktualizace nebo zahoezení nové verze.

2.5.1.3 Správa | Systémové služby

Přehledová tabulka všech služeb a komponent, které běží v systému Kernun Security Appliance.

2.5.2 Autentizace

Autentizace je služba pro autentizaci uživatelů v prostředí Microsoft Active Directory protokolem Kerberos. V síti je potřeba používat netransparentní proxy (proxy v prohlížeči). Na základě zjištěného uživatelského jména a členství ve skupinách AD lze řídit přístup uživatele k webům podle nastavených pravidel v Profilech proxy. Pro použití autentizace je nutné ji zapnout v jednotlivých Profilech proxy.

2.5.3 Databáze

Databáze systému obsahuje statistické údaje systému, využívá se pro zobrazení grafů a statistik v menu Monitoring.

2.5.4 Administrační rozhraní

Konfigurace přístupu k Administračnímu rozhraní. Lze definovat, na kterých rozhraních bude služba dostupná, případně lze nahrát certifikát vlastní autority a přistupovat potom na server Kernun jeho názvem.

2.6 Uživatelé

2.6.1 Seznam uživatelů

V seznamu uživatelů jsou uvedeni uživatelé s oprávněním přístupu na server Kernun.

3 Doporučené nastavení KSA

3.1 Výchozí nastavení KSA

Pro první přihlášení do GUI použijte username *admin* a heslo *admin*. Důrazně doporučujeme toto nastavení co nejdříve změnit.

Ve výchozím stavu (nový KSA) nejsou zapnuty žádné bezpečnostní funkce a je povolen veškerý provoz vzájemně mezi interními sítěmi (všechna rozhraní s označením LAN) a také veškerý provoz z interních sítí do internetu.

3.2 Doporučení k nastavení bezpečnosti a provozu

Pro optimální využití pokročilé funkcionality serveru Kernun Security Appliance doporučujeme zapnout / nakonfigurovat minimálně následující komponenty:

3.2.1 Bezpečnostní funkce

Kernun Security Appliance má několik bezpečnostních funkcí, které přispívají ke zvýšení bezpečnosti a ochrany. Bezpečnostní funkce se nacházejí v sekci **Ochrana**

1. **Adaptivní firewall.** automaticky aktualizovaná databáze ip adres, které jsou známé nebezpečným provozem. Pokud dojde k pokusu o navázání spojení s takovou adresou, je tato komunikace automaticky zablokována. Lze přidat výjimky jak povolovací (Allowlist), tak i zakazovací (Blocklist).
2. **Honeypot** pokud je váš server ve funkci perimetrového firewallu, zapněte tuto funkci na WAN interface a vyberte vámi nepoužívané, ale útočníky často vyhledávané porty, např 23(telnet), 445(smb sdílení) 1433(mysql), čas blokování doporučujeme 15 minut. Pokud útočník z internetu zkusí spojení na vaši veřejnou adresu a některý z definovaných portů, bude dočasně zablokován.
3. **IPS** automaticky aktualizovaná databáze bezpečnostních pravidel, Služba analyzuje síťový provoz a pokud najde bezpečnostní incident, pak provoz buďto blokuje nebo jen posílá varování, podle konfigurace. Služba je velmi náročná na systémové zdroje a způsobuje snížení datové propustnosti serveru z důvodu podrobné analýzy paketů.

3.2.2 Řízení provozu

Řízení uživatelského provozu se nastavuje v sekci **Ochrana: Stavový firewall** a **Proxy**

Ve výchozím stavu je povolen provoz vzájemně mezi interními sítěmi (interfacy s označením LAN) a také veškerý provoz z interních sítí do internetu.

Webový provoz (provoz typu http/https) je řízen Proxy, ve výchozím stavu je také vše povoleno.

Pravidla se vyhodnocují vždy principem **First_match**, tedy použije se první pravidlo, kde jsou splněny vstupní podmínky a další pravidla se pak již nevyhodnocují.

V řízení provozu doporučujeme tyto úpravy:

1. Stavový firewall

- pokud chcete omezit provoz navzájem mezi interními sítěmi, zakomentujte pravidlo `ALLOW_LAN_TO_LAN` a nahraďte ho vlastními pravidly
- pokud chcete omezit provoz z interních sítí do internetu, zakomentujte pravidlo `ALLOW_LAN` a nahraďte ho vlastními pravidly

2. Proxy http/https

pokud chcete nastavit omezení přístupu na webové kategorie a servery v sekci Proxy | Profily změňte výchozí pravidlo na Zakazovací (kliknutím na ikonku před názvem pravidla) a před něj přidejte vlastní pravidla.

Je možno definovat pravidla:

- Povolovací: Povolí pouze vybrané kategorie
- Zakazovací: Zakáže vybrané kategorie
- Podle kategorií: na jedné stránce definujete povolené i zakázané kategorie
- V případě zapnuté autentizace v profilu je autentizace vyžadována ve všech pravidlech, která jsou umístěna níže pod hlavičkou Autentizace.
- V případě zapnuté TLS inspekce v profilu je TLS inspekce prováděna ve všech pravidlech, která jsou umístěna níže pod hlavičkou TLS inspekce.
- Výjimky z autentizace a/nebo z TLS inspekce se vytváří přidáním pravidla výše nad hlavičku těchto funkcí.

3.2.3 Konfigurační GUI

Ve výchozím stavu je GUI dostupné na všech interfacech, doporučujeme ho omezit pouze na interní ip adresy a z internetu přistupovat k serveru Kernun pomocí VPN klienta.

Toto nastavení se provádí v sekci Správa | Administrační rozhraní.

3.2.4 Služby sítě

Kernun Security Appliance obsahuje i různé systémové služby, které lze využít v interní síti nebo pro zabezpečený přístup do interní sítě. Konfigurace těchto služeb je popsána v kapitole 2.3 Služby sítě

- DHCP server, DHCP Relay
- DNS server
- OpenVPN server
- Konfigurační GUI
- SSH server

3.2.5 Upgrade KSA

Doporučujeme pravidelně aktualizovat OS Kernun Security Appliance, kontrola nových verzí i průvodce instalací jsou k dispozici v sekci Správa | Aktualizace.

4 Pokročilé funkce

4.1 Multihoming

Konfigurační utilita **Multihoming** umožňuje připojení do Internetu pomocí dvou konektivit, primární a záložní.

Zadávají se konfigurační údaje pro obě konektivity (ipadresa/maska a výchozí brána) a dále servery pomocí nichž se testuje dostupnost každé konektivity.

Preemptivní timeout: Je-li v systému aktuálně nastavena sekundární výchozí brána a zároveň už je alespoň jeden server pro kontrolu primární konektivity dostupný po dobu tohoto timeoutu, je výchozí brána změněna zpět na primární.

Timeout pro testování konektivity: Timeout, po který musí být všechny servery pro testování primární konektivity nedostupné, aby došlo ke změně výchozí brány na sekundární.

4.2 Cluster

Cluster slouží k zajištění vysoké dostupnosti služeb poskytovaných systémem Kernun Security Appliance. Umožňuje snížit na minimum čas výpadku v případě poruchy hardwarového zařízení.

Zprovoznit cluster je možné po aktivaci licence pro cluster na dvou stejných hardwarových zařízeních Kernun Security Appliance se stejnou verzí systému.

Jedno ze zařízení, v průvodci označované jako uzel A, může být aktuálně používáno, např. při migraci z režimu Single. Druhé ze zařízení, v průvodci označované jako uzel B, musí být nově nainstalováno. Obě zařízení se musí nacházet ve stejném ethernetovém segmentu jedné sítě.

Administrátor si připraví ip adresy síťových rozhraní pro oba uzly a ip sdílenou adresu pro cluster. V DNS serveru v LAN nakonfiguruje názvy serverů (A záznamy) pro oba uzly a také sdílený název pro celý cluster.

Cluster se vytváří pomocí funkce průvodce, který ve spolupráci s administrátorem postupně provádí jednotlivé kroky konfigurace.

5 Poznámky