

KERNUN Security Appliance (KSA)

stručný průvodce pro spuštění serveru

Obsah

KERNUN Security Appliance (KSA).....	1
Nový server KSA a výchozí hodnoty nastavení.....	1
Kontrola / úprava výchozí konfigurace KSA z konzoly.....	2
Přihlášení do GUI.....	2
Základní nastavení KSA po instalaci.....	2
výchozí stav.....	2
Základní doporučení k nastavení bezpečnosti a provozu.....	2
Bezpečnostní funkce.....	3
Řízení provozu.....	3
Služby.....	4
Další informační zdroje.....	4

Nový server KSA a výchozí hodnoty nastavení

Server je dodán s nainstalovaným OS KERNUN Security Appliance, ve výchozí konfiguraci jsou připraveny 2 síťové interfacery:

1. WAN: má nakonfigurovaný dhcp-klient, tedy pokud je v této síti DHCP server, přiřadí se mu ip adresa automaticky
2. LAN: má přiřazenou pevnou ip adresu 192.168.1.2/24

Pokud toto nastavení nevyhovuje, můžete konfiguraci změnit z konzoly serveru, viz dále.
Další úpravy provedete po přihlášení do GUI.

Kontrola / úprava výchozí konfigurace KSA z konzoly

1. přihlásíte se do konzoly systému
U: sysadmin
P: sysadmin
2. příkazem **ip a** zjistíte, jaké ip adresy byly přiřazeny interfacům
první z interfaců (WAN) má nakonfigurovaný dhcp-klient, tedy pokud je v této síti DHCP server, přiřadí se mu ip adresa automaticky
druhý z interfaců (LAN) má přiřazenou pevnou ip adresu 192.168.1.2/24
3. pokud tyto adresy nechcete použít pro přihlášení do GUI, můžete je změnit tímto postupem :
 - a) změna ip adresy
připravte si ip adresy zařízení pro oba interfaci LAN/WAN a ip adresy gw (na WAN iface)
spusťte konfigurační utilitu a vyplňte požadované údaje
admin
zde vyberete druhou volbu
Reinitialize configuration a potom **Firewall**
je nutno vyplnit všechny hodnoty správně , utilita je nekontroluje
ip adresa interfaců se zadává s maskou (např /24 nebo /255.255.255.0)
ostatní hodnoty: dns server, gateway se zadávají bez masky
 - b) po dokončení zadávání adres a potvrzení zadaných změn
je nutno počkat cca 5 minut pro dokončení aktivace
dokončení procesu lze zkontrolovat příkazem
ip a
který začne vypisovat nově nakonfigurované ip adresy interfaců

Přihlášení do GUI

1. přihlásíte se do GUI na vaší ip adrese (viz předchozí krok)
U: admin
P: admin
při prvním přihlášení je nutná změna hesla.
2. další konfigurace se provádí v GUI

Základní nastavení KSA po instalaci

výchozí stav

po instalaci je KSA ve výchozím stavu a nejsou zapnuty žádné bezpečnostní funkce a je povolen veškerý provoz vzájemně mezi interními sítěmi (interfaci s označením LAN) a také veškerý provoz z interních sítí do internetu

Základní doporučení k nastavení bezpečnosti a provozu

Pro optimální využití funkcionality KERNUN Security Appliance doporučujeme zapnout / nakonfigurovat minimálně následující komponenty:

Bezpečnostní funkce

KERNUN Security Appliance má několik bezpečnostních funkcí, tyto byste měli zapnout pro 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.
2. **Honeypot** pokud je váš server ve funkci perimetrového firewallu, zapněte tuto funkci na WAN interface a vámi nepoužívaném, ale útočníky vyhledávaném portu, 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, je dočasně zablokován.

Řízení provozu

Řízení 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 .

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 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 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

Služby

KERNUN Security Appliance obsahuje i různé systémové služby, které lze využít v interní síti nebo pro zabezpečený přístup do interní sítě.

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

Další informační zdroje

podrobnější informace ke konfiguraci, uživatelský manuál KSA a další dokumenty najdete na webu společnosti KERNUN:

<https://www.kernun.cz/pro-zakazniky/kernun-security-appliance/>