Kernun Clear Web
Příručka administrátora

Trusted Network Solutions, a.s.

1. listopadu 2018

Obsah

Kapitola 1

Kernun Clear Web

Webový filtr Kernun Clear Web monitoruje, kontroluje a řídí přístup uživatelů interní počítačové sítě k webu na základě konfigurovatelné politiky. Jeho hlavní funkce jsou:

Kategorizace webových serverů Díky automatické kategorizaci pomocí vyškolených operátorů dosahuje databáze kategorizovaných webů vysoké míry úspěšnosti. To v kombinaci s rychlou reakcí na změny a pravidelnou aktualizací databáze zajišťuje konzistentně vysokou kvalitu.

Autentizace uživatelů Kernun Clear Web umí identifikovat jednotlivé uživatele a skupiny uživatelů v prostředí Microsoft Active Directory a Samba.

Politika přístupu k webu Pro jednotlivé klientské počítače, uživatele a skupiny uživatelů lze definovat přístupové profily určující, ke kterým kategoriím webových serverů může daný počítač, uživatel nebo skupina přistupovat. Z profilů je možné definovat výjimky pro jednotlivé webové servery.

Inspekce HTTPS provozu Kernun Clear Web umožňuje průběžně dešifrovat, zkontrolovat a znovu zašifrovat komunikaci protokolem HTTPS.

Antivirová ochrana Soubory stahované z webu jsou volitelně kontrolovány antivirem před odesláním do počítačů uživatelů.

Monitoring provozu Kernun Clear Web monitoruje právě probíhající spojení mezi klienty a webovými servery. Vytváří detailní provozní záznamy obsahující informace o webovém provozu na úrovni HTTP požadavku a o zdraví systému.

Statistiky a analýza provozu Z provozních záznamů se pravidelně nebo na požádání vytvářejí přehledné statistické reporty zachycující aktivitu uživatelů. Kernun Clear Web lze rozšířit o modul Kernun Business Intelligence určený pro interaktivní analýzu informací o webové komunikaci a tvorbu reportů.

Uživatelská přívětivost Produkt se ovládá pomocí webového rozhraní s různými úrovněmi nápovědy a kontroly funkčnosti.

Flexibilita nasazení Zařízení Kernun Clear Web zpracovává jak transparentní, tak netransparentní webové požadavky. To umožňuje jej nasadit různými způsoby podle omezení sítě, například jako Proxy nebo Router.

Škálovatelnost a robustnost Kernun Clear Web se dodává jako hardwarové zařízení v několika variantách podle výkonu, které je možné nasadit také v režimu cluster, nebo jako virtuální zařízení do prostředí Oracle VirtualBox, VMware vSphere nebo Microsoft Hyper-V. Systém Kernun, jakožto bezpečnostní zařízení, je vyvíjen se zřetelem na odolnost vůči chybám.

Kapitola 2

Uvedení do provozu

Kapitola obsahuje informace potřebné pro nasazení a zprovoznění zařízení Kernun Clear Web ve vaší síti. Zejména se jedná o nároky kladené na kompatibilitu prostředí, parametry pro prvotní konfiguraci nebo samotný režim nasazení jako Proxy nebo Router.

2.1 Předpoklady kompatibility prostředí

Pro zaručení správné funkčnosti a dosažení nejlepších výsledků produktu Kernun Clear Web je nutné, aby se vlastnosti prostředí vaší sítě, kde má být Kernun Clear Web nasazen, pokud možno co nejlépe shodovaly s níže uvedenými předpoklady. Odchylky od těchto předpokladů nemusí nutně znamenat celkovou nefunkčnost zařízení, mohou však značně omezit některé jeho možnosti využití.

- Pro správné fungování zařízení Kernun Clear Web je nutné zajistit na mezilehlých prvcích vaší síťové infrastruktury (např. firewall) povolení následující komunikace ze zařízení Kernun Clear Web:

    1. porty 80 (HTTP), 443 (HTTPS) a jiné na všechny servery v internetu pro obsluhu požadavků klientů
    2. port 22 (SSH) nebo 443 (HTTPS) na server `callhome.kernun.com` pro službu vzdálené pomoci
    3. port 22 (SSH) na server `feedback.kernun.com` pro službu automatické kategorizace
    4. port 443 (HTTPS) na server `download.kernun.com` pro aktualizaci databáze i systému Kernun Clear Web

- Z důvodu správného fungování autentizace uživatelů a jiných částí systému, musí interní DNS servery vaší sítě obsahovat záznamy pro dopředný i zpětný převod mezi hostitelským jménem a IP adresou, zvolenou pro zařízení Kernun Clear Web. Dále pro využití automatické detekce proxy pomocí WPAD je nutné zajistit překlad jména počítače `wpad` ve vaší doméně na IP adresu, zvolenou pro zařízení Kernun Clear Web.

- Zařízení Kernun Clear Web podporuje autentizaci uživatelů v síti. Předpokladem je funkční Microsoft Active Directory. Podporovány jsou také Active Directory postavené nad Sambou 4 a Microsoft Windows doména nad Sambou 3. Standardně podporované autentizační metody jsou:

  1. Kerberos v prostředí Active Directory
  2. NTLM

- Pro praktické nasazení inspekce HTTPS provozu je nutné zajistit distribuci certifikátu certifikační autority systému Kernun Clear Web do webových prohlížečů klientů nebo na systém Kernun Clear Web importovat klíč a certifikát interní certifikační autority vaší společnosti.

- Pro antivirovou ochranu v režimu ICAP server v produktu Kernun Clear Web lze využít specializovaných antivirových řešení renomovaných výrobců. Komunikace mezi Kernun Clear Web a antivirem probíhá pomocí protokolu ICAP v módu RESPMOD. Seznam ověřených spolupracujících antivirových produktů:

  1. Kaspersky Anti-Virus Suite for Gateway 5.5
  2. ESET Gateway Security 4

     V grafickém rozhraní ESET GS4 je nutné povolit položku Performance Agent. Položka se nachází v sekci Configuration/ICAP.
  3. eScan for NAS 5.1-0
  4. McAfee Email and Web Security 5.6
  5. Symantec Scan Engine 5
  6. Sophos SAVUL 4 + SAVDI 2

  Je možné použít i integrovaný antivirus Kaspersky nebo jiná antivirová řešení podporující ICAP protokol. V současné době není kompatibilní antivirové řešení DrWeb přes ICAP.

- Preferovaný způsob nasazení do sítě je v režimu Proxy s jedním síťovým rozhraním. V tomto režimu je nutné nastavit klientské počítače tak, aby pro přístup k webu používaly Kernun Clear Web. K tomu lze využít technologii WPAD nebo GPO v prostředí Microsoft Active Directory. Druhou variantou nasazení je režim Router se dvěma sítovými rozhraními.

- Virtuální zařízení Kernun Clear Web může běžet na následujících platformách:

  1. VirtualBox 4.3 a vyšší
  2. VMware vSphere ESXi 5.5 a vyšší
  3. Microsoft Hyper-V Windows Server 2012 R2
  4. Citrix XenServer 6.5

- Požadavky na virtuální zařízení:

  – Do 150 uživatelů – 2 CPU 4 GB RAM 120 GB HDD

- Do 750 uživatelů – 4 CPU 8 GB RAM 240 GB HDD
- Do 2 000 uživatelů – 6 CPU 16 GB RAM 360 GB HDD
- Nad 2 000 uživatelů – 8 CPU 24 GB RAM 480 GB HDD

2.2 Příprava

Před zprovozněním systému Kernun Clear Web je potřeba provést několik kroků:

1. Zvolte si hostitelské jméno (včetně domény, tzn. FQDN), kterým bude Kernun Clear Web identifikován ve vaší síti. Příklad: `kernun.example.com`.
2. Zvolte si unikátní IP adresu z vaší sítě (včetně masky), na které bude Kernun Clear Web komunikovat.
3. Zvolte si nové heslo pro administrátorský účet.
4. Zjistěte si IP adresu výchozí brány vaší sítě pro přístup do Internetu.
5. Zjistěte si IP adresu primárního (i sekundárního) doménového serveru pro překlad doménových jmen na IP adresy.
6. Připravte si platný licenční soubor produktu Kernun Clear Web.
7. Připravte si počítač s webovým prohlížečem (Mozilla Firefox, Microsoft Internet Explorer nebo Google Chrome) a ethernetovým síťovým kabelem.
8. Nastavte záznam typu A (pro převod hostitelského jména na IP adresu) a záznam typu PTR (pro zpětný převod IP adresy na jméno počítače) na svých interních DNS serverech pro hostitelské jméno a IP adresu z kroků 1 a 2. Vynechání A nebo PTR záznamu způsobí nefunkčnost autentizace uživatelů.
9. Nastavte váš firewall a případné mezilehlé prvky vaší síťové infrastruktury tak, aby neblokovaly komunikaci z IP adresy z bodu 2 na porty 80 (HTTP) a 443 (HTTPS) serverů z internetu (obsluha požadavků klientů) a na port 22 (SSH) serverů `callhome.kernun.com` (služba vzdálené pomoci), `feedback.kernun.com` (služba automatické kategorizace) a port 443 (HTTPS) serveru `download.kernun.com` (aktualizace databáze a systému).
10. Připravte si hardware nebo v případě instalace jako virtuální zařízení pro VMware vSphere a Oracle VirtualBox OVF šablonu (např.: *kernun_clear_web-040102h00.201502050824.amd64.ova*) a pro Microsoft Hyper-V soubor VHD (např.: *kernun_clear_web-040102h00.201502050824.amd64.vhd*).

2.3 Zapojení

Jakmile máte vše potřebné připraveno, můžete přistoupit ke zprovoznění systému Kernun Clear Web.

1. Jestliže instalujete hardwarové zařízení, propojte ho pomocí ethernetového síťového kabelu přímo s vaším počítačem. Počáteční IP adresa systému Kernun Clear Web nastavená z výroby je `192.168.1.2`. Jestliže je tato IP adresa použitelná ve vaší síti, můžete zařízení alternativně připojit rovnou do vaší sítě.

2. Zapněte zařízení Kernun Clear Web.

3. Pokud jste propojili Kernun Clear Web přímo s vaším počítačem, nastavte na vašem počítači IP adresu `192.168.1.3` a masku sítě `255.255.255.0`.

Jestliže instalujete virtuální zařízení, naimportujte tuto OVF šablonu do vašeho virtualizačního prostředí a nastavte virtuální síť tak, abyste z vašeho počítače mohli přistupovat k systému Kernun Clear Web používajícímu výchozí IP adresu (`192.168.1.2`). Podrobnější návod importu virtuální šablony do nejběžnějších virtualizačních platforem lze nalézt na `http://www.kernun.cz/podpora/navody-kernun/`.

2.4 První přihlášení

V tuto chvíli by měl systém Kernun Clear Web běžet a být dostupný po síti z vašeho počítače. Před zahájením běžného používání je potřeba se přihlásit do webového grafického rozhraní a systém nakonfigurovat.

1. Otevřete webový prohlížeč a do adresního řádku napište výchozí adresu zařízení `https://192.168.1.2`.

2. Zobrazí se informace o nedůvěryhodném spojení, protože prohlížeč nedůvěřuje certifikační autoritě, která certifikát podepsala. Akceptujte spojení s tímto certifikátem, například přidáním výjimky pro tento certifikát ve vašem prohlížeči. Pro zvýšení bezpečnosti lze ověřit otisk certifikátu v prohlížeči s otiskem certifikátu na systémové konzoli zařízení pomocí připojeného monitoru nebo virtuální obrazovky.

3. Objeví se přihlašovací obrazovka, viz obr. 2.1. Zadejte uživatelské jméno `admin` a heslo `admin`.

4. Po úspěšném přihlášení se objeví uvítací obrazovka. Jako první krok je potřeba nastavit nové heslo administrátora. Zvolte vhodné heslo, které nelze snadno uhodnout, a zapamatujte si ho nebo si ho zapište na bezpečné místo.

2.5 Počáteční konfigurace

Po nastavení hesla administrátora je nutné dokončit počáteční konfiguraci systému zadáním základních parametrů nastavení sítě. V konfiguračním dialogu (obr. 2.2) se nastavují dříve zvolené hodnoty, viz kap. 2.2:

- hostitelské jméno
- IP adresa a maska síťového rozhraní (ve formátu počet bitů masky 0–32)

Obrázek 2.1: Přihlašovací obrazovka

- výchozí brána pro přístup do Internetu
- primární DNS server
- licenční soubor

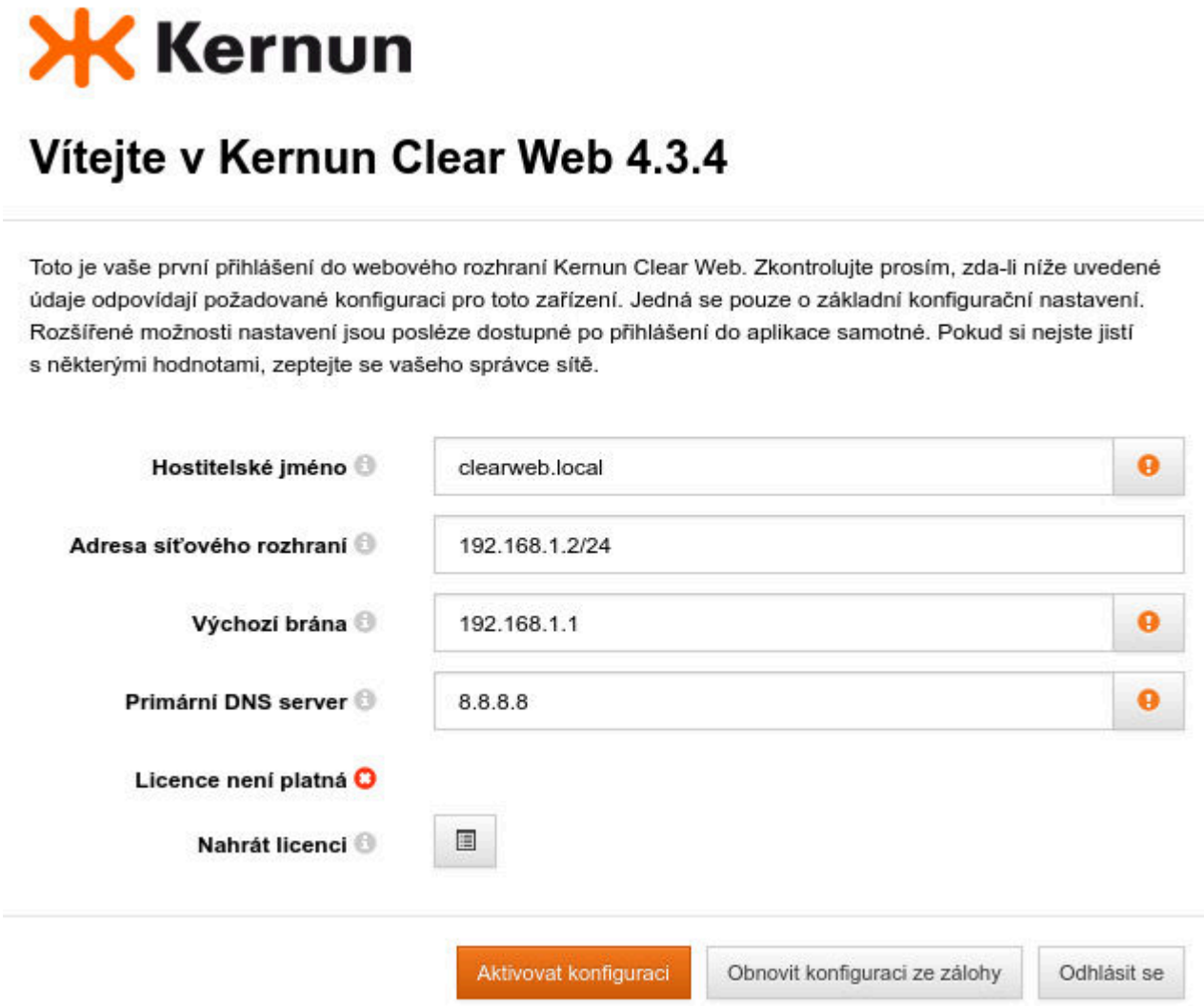
Aby fungovalo DNS i bez nutnosti nastavovat adresy serverů, je ve výchozím nastavení jako primární DNS server nastavena adresa Google Public DNS `8.8.8.8`.

Po zadání hodnot klikněte na tlačítko Aktivovat konfiguraci. Nová konfigurace zařízení se uloží a aplikuje. Poté je vyžadováno nové přihlášení, tentokrát přímo do grafického uživatelského rozhraní produktu Kernun Clear Web. Jeho možnosti jsou popsány v následující kapitole.

Při novém přihlášení po aplikaci nastavení je nutné v prohlížeči zadat nově nastavené hostitelské jméno nebo IP adresu zařízení Kernun Clear Web.

2.6 Nastavení klientských stanic

Pro správnou funkčnost zařízení Kernun Clear Web v režimu Proxy ve vaší síti je potřeba, aby prohlížeče na jednotlivých uživatelských stanicích používaly zařízení jako webovou proxy. To lze nastavit manuálně na každé stanici zvlášť, což se hodí spíše pro menší sítě s malým množstvím klientských stanic nebo pro testovací účely. V případě větších sítí lze využít buď možnost automatické detekce proxy WPAD, případně konfigurace přes zásady skupiny GPO v doméně Microsoft Active Directory. Lze také využít nasazení Kernun Clear Web v režimu Router.



Obrázek 2.2: Počáteční konfigurace

2.6.1 Automatická detekce proxy

Zařízení Kernun Clear Web podporuje automatickou detekci proxy pomocí technologie Web Proxy Auto-Discovery Protocol (WPAD), ve které vystupuje v roli WPAD serveru. Tato technologie umožňuje klientům v síti automaticky detekovat a nastavit proxy. Pro mobilní uživatele připojující se k různým sítím (práce, hotel, domov) zajišťuje správné nastavení připojení k webu bez nutnosti manuálních změn v nastavení prohlížeče. Pro úspěšné využití této funkčnosti je nutné provést následující kroky:

- Na interních DNS serverech přidat záznamy typu A pro převod jmen `wpad` a `wpad.example.com` na IP adresu, na které běží Kernun Clear Web. V případě používání více domén je nutné zajistit odpovídající DNS záznamy i pro tyto domény.

- Zajistit, aby příslušný webový prohlížeč měl nastavenou automatickou detekci proxy. Toto nastavení je výchozí pro systémy Windows a většinu webových prohlížečů. Změnu tohoto nastavení lze také pomocí Group Policy v Microsoft Active Directory doméně.

> **Poznámka**
>
> Pokud jako interní DNS server používáte Microsoft Windows Server 2008 a novější, ujistěte se, že nejsou požadavky na WPAD blokovány, viz `http://technet.microsoft.com/en-us/library/cc995158.aspx`.

Automatická detekce proxy pomocí WPAD funguje tak, že webový prohlížeč se při spuštění pokusí získat konfigurační soubor z adresy `http://wpad.example.com/wpad.dat`, případně `http://wpad/wpad.dat`. Tento soubor určuje, kterou proxy má prohlížet použít. Pokud se soubor nepodaří získat, prohlížeč bude k webu přistupovat přímo přes výchozí bránu.

Generovaný konfigurační soubor `wpad.dat` na zařízení Kernun Clear Web způsobuje následující chování webového prohlížeče: pokud je proxy dostupná přes odpovídající hostitelské jméno nebo alespoň přes IP adresu, webový prohlížeč ji použije pro přístup do Internetu. V opačném případě se klient pokusí připojit k Internetu přímo bez využití proxy. Přímo bez proxy se klient připojuje, i pokud přistupuje k samotnému webovému rozhraní systému Kernun Clear Web nebo k serverům ze seznamu, definovaném v pokročilých možnostech sekce Síťové nastavení aktivity Správa.

2.6.2 Nastavení proxy pomocí GPO

Pro nastavení proxy do webových prohlížečů klientů lze v prostředí Microsoft Active Directory využít nástroj Správy zásad skupiny (Group Policy Management Tool). Více informací o Zásadách skupiny a jejích použití lze najít na `http://technet.microsoft.com/`.

Pro nastavení parametrů prohlížeče Internet Explorer lze v Zásadách skupiny využít sekci Konfigurace uživatele / Předvolby / Nastavení ovládacích panelů / Nastavení internetu (User Configuration / Preferences / Control Panel Settings / Internet Settings), kde lze nastavit konkrétní parametry pro vybrané verze prohlížeče Internet Explorer.

Pro nastavení parametrů prohlížeče Firefox pomocí Šablon zásad skupiny (Group Policy Templates) doporučujeme použít FirefoxADM. Více informací na `http://sourceforge.net/projects/firefoxadm/`.

2.6.3 Režim Router

Kernun Clear Web je možné provozovat v režimu Router (bez nutnosti nastavení proxy v prohlížeči uživatele). Transparentní režim má oproti standardnímu zapojení následující omezení:

- Politiku pro koncová zařízení lze řídit jen podle jejich IP adresy

Režim nasazení lze zvolit v aktivitě Správa v sekci Síťové nastavení po kliknutí na tlačítko Pokročilé možnosti.

V režimu Router zařízení Kernun Clear Web v síti vystupuje jako síťový router. Zařízení stojí na perimetru sítě, a odděluje vnitřní síť od vnější. Používá dvě síťová rozhraní. Jedno je připojeno do interní sítě (stejné rozhraní, které je použito v režimu Proxy). Druhé je připojeno do Internetu. Ostatní zařízení ve vnitřní síti by měla mít nastaven Kernun Clear Web jako výchozí bránu.

HTTP/HTTPS požadavky

Kernun Clear Web má v tomto režimu spuštěnu transparentní proxy, která automaticky zpracovává webový provoz. Ve výchozím nastavení proxy zpracovává požadavky na portech 80 (HTTP) a 443 (HTTPS). Porty, na kterých transparentní proxy zpracovává požadavky, lze upravit ve stejné sekci.

I v režimu Router Kernun Clear Web provozuje netransparentní HTTP/HTTPS proxy (ve výchozím nastavení na portu 3128). Požadavky realizované netransparentně fungují stejně, jako v režimu nasazení Proxy (tj. včetně HTTPS inspekce a autentizace).

Ostatní protokoly

Pro provoz ostatních protokolů je možné vytvořit pravidla paketového filtru. Pro přístup z vnější sítě ke službám ve vnitřní síti lze přidat pravidla pro přesměrování portů (viz kap. 4.1).

Interní síť, DHCP server

Zařízení může provozovat pro vnitřní síť DHCP server. Rozsah IP adres, které bude zařízení poskytovat klientům, lze nastavit v téže sekci. Seznam klientů, kterým bude poskytována pevná IP adresa, lze zadat v Tabulce doménových jmen v sekci Parametry systému.

Externí síť, DHCP klient

Adresu používanou pro přístup k Internetu je možno zadat buď přímo, nebo nastavit autokonfiguraci pomocí DHCP protokolu. Je-li automatická konfigurace na externím síťovém rozhraní zapnuta, je možno zvolit automatické nastavení DNS serverů, nebo je explicitně vyjmenovat.

2.6.4 Nasazení v transparentním režimu

Tato kapitola je počínaje verzí 4.3.1 považována za zastaralou. Pro transparentní nasazení je preferován režim nasazení Router, viz kap. 2.6.3.

Kernun Clear Web je možné provozovat v transparentním režimu (bez nutnosti nastavení proxy v prohlížeči uživatele). Transparentní režim má oproti standardnímu zapojení následující omezení:

- Politiku pro koncová zařízení lze řídit jen podle jejich IP adresy

Podporovány jsou dvě varianty zapojení.

Kernun Clear Web jako výchozí brána

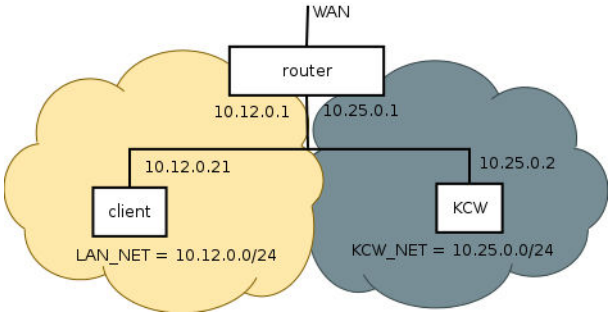
Kernun Clear Web může fungovat jako výchozí brána pro přístup do Internetu. V tomto zapojení zařízení propouští pouze HTTP a HTTPS komunikaci na portech, definovaných v příslušných polích podsekce Pokročilé možnosti v aktivitě Správa, sekci Síťové nastavení. Provoz HTTPS na specifikovaných portech nelze omezit ani monitorovat.

Ostatní typy požadavků (např. DNS, IMAP, SSH, apod.) nejsou propouštěny. Servery obsluhující tyto požadavky by proto měly být dostupné v místní síti a používat pro přístup do internetu jinou výchozí bránu.

Přesměrování HTTP požadavků z výchozí brány na Kernun Clear Web

Toto zapojení lze použít v případě, že brána používaná pro přístup k internetu dokáže přesměrovat všechny HTTP požadavky na Kernun Clear Web (funkce DNAT).

Schéma transparentního nasazení je znázorněno na obr. obr. 2.3. Klienti jsou umístěni v síti LAN_NET, zařízení Kernun Clear Web je umístěno do své vlastní IP sítě KCW_NET. Sítě nemusí být fyzicky odděleny (mohou sdílet jeden ethernetový segment).



Obrázek 2.3: Zapojení v transparentním režimu

Brána přesměrovává HTTP požadavky klientů na zařízení Kernun Clear Web. V zařízení typu IP TABLES lze použít následující pravidlo:

```
#!/bin/sh
KCW_IP=10.25.0.2
```

```
KCW_PORT=3128
LAN_NET="10.12.0.0/24"
KCW_NET="10.25.0.0./24"
LAN_DEV="eth0"

# presmerovat HTTP provoz z LAN_NET na KCW:3128 (s vyjimkou provozu uvnitr LAN_NET)
iptables -t nat -A PREROUTING -i $LAN_DEV -s $LAN_NET ! -d $LAN_NET \
        -p tcp  -dport 80 -j DNAT -to $KCW_IP:$KCW_PORT
```

Tip

Pro přístup k rozhraní Kernun Clear Web je vhodné na administrátorské stanici vytvořit síťový alias v síti KCW_NET.

Kapitola 3

Uživatelské rozhraní

Kapitola popisuje webové grafické rozraní pro administraci systému Kernun Clear Web společně se strukturou aktivit a sekcí rozhraní. S prvním přístupem k rozhraní vám pomůže návod pro přihlášení.

3.1 Přihlášení

Do grafického uživatelského rozhraní systému Kernun Clear Web se přistupuje pomocí webového prohlížeče (Mozilla Firefox, Microsoft Internet Explorer nebo Google Chrome). Přihlášení probíhá obdobně, jako první přihlášení po zapojení systému, viz kap. 2.4:

1. Otevřete webový prohlížeč a do adresního řádku napište hostitelské jméno zadané v konfiguraci zařízení, např. `https://kernun.example.com`. Jestliže jméno nebylo zavedeno do DNS, je potřeba místo jména zadat IP adresu síťového rozhraní systému Kernun Clear Web, např. `https://192.168.1.2`.

2. Zobrazí se informace o nedůvěryhodném spojení, protože prohlížeč protože prohlížeč nedůvěřuje certifikační autoritě, která certifikát podepsala. Akceptujte spojení s tímto certifikátem, například přidáním výjimky pro tento certifikát ve vašem prohlížeči. Pro zvýšení bezpečnosti lze ověřit otisk certifikátu v prohlížeči s otiskem certifikátu na systémové konzoli zařízení pomocí připojeného monitoru nebo virtuální obrazovky.

   Nutnosti akceptovat certifikát se lze vyhnout importováním certifikační autority do prohlížeče, která je dostupná na adrese `http://kernun.example.com/ca`. Také lze na Kernun Clear Web importovat vaši certifikační autoritu, viz kap. 5.3, případně pouze certifikát serveru rozhraní, který lze nastavit v pokročilých možnostech sekce Správa a aktualizace aktivity Správa.

3. Objeví se přihlašovací obrazovka, viz obr. 2.1. Zadejte uživatelské jméno `admin` a heslo.

4. Po chvíli se objeví přehled systému Kernun Clear Web, viz obr. 3.1.

3.2 Popis uživatelského rozhraní

Grafické uživatelské rozhraní produktu Kernun Clear Web je rozděleno do několika částí (aktivit). V této kapitole stručně popíšeme jednotlivé aktivity. Podrobnější vysvětlení klíčových aktivit a s nimi souvisejících funkcí produktu bude následovat v dalších kapitolách.

Po přihlášení se zobrazí Přehled (obr. 3.1), který podává základní informace o stavu systému.

Úspěšnost databáze Úspěšnost (procento nalezených serverů) databáze pro kategorizace webových serverů. Graf progrese zachycuje rozdíl mezi aktuální úspěšností a historickou úspěšností v době nasazení zařízení Kernun Clear Web do provozu. Tlačítko Statistiky zobrazí podrobné statistiky provozu.

Síťový provoz Grafy objemu data přenášených po síti. Je možné se přepínat mezi pohledy za poslední měsíc, týden, den nebo hodinu. Tlačítko Monitoring vede na zobrazení právě probíhajících HTTP spojení od klientů.

Licence Informace o platnosti licence a také o počtu unikátních uživatelů a zařízení v síti za poslední týden. Okno obsahuje čas od poslední úspěšně aktualizace databáze pro kategorizaci webových serverů.

Povolené kategorie, Bypass kategorie, Blokované kategorie Přehled nejčastějších kategorií stránek podle akce pravidel politiky (Povolit, Bypass, Blokovat). Grafy je možné zobrazit za poslední den, týden nebo měsíc. Tlačítko Statistiky zobrazí podrobné statistiky provozu.

Rizikové kategorie Přehled uživatelů nebo klientů s největším počtem zachycených virů a přístupů na servery, které jsou zařazené do kategorií považovaných za bezpečnostní riziko.

Antivirová ochrana Platnost licence, statistiky a poslední aktualizace databáze modulu antivirus.

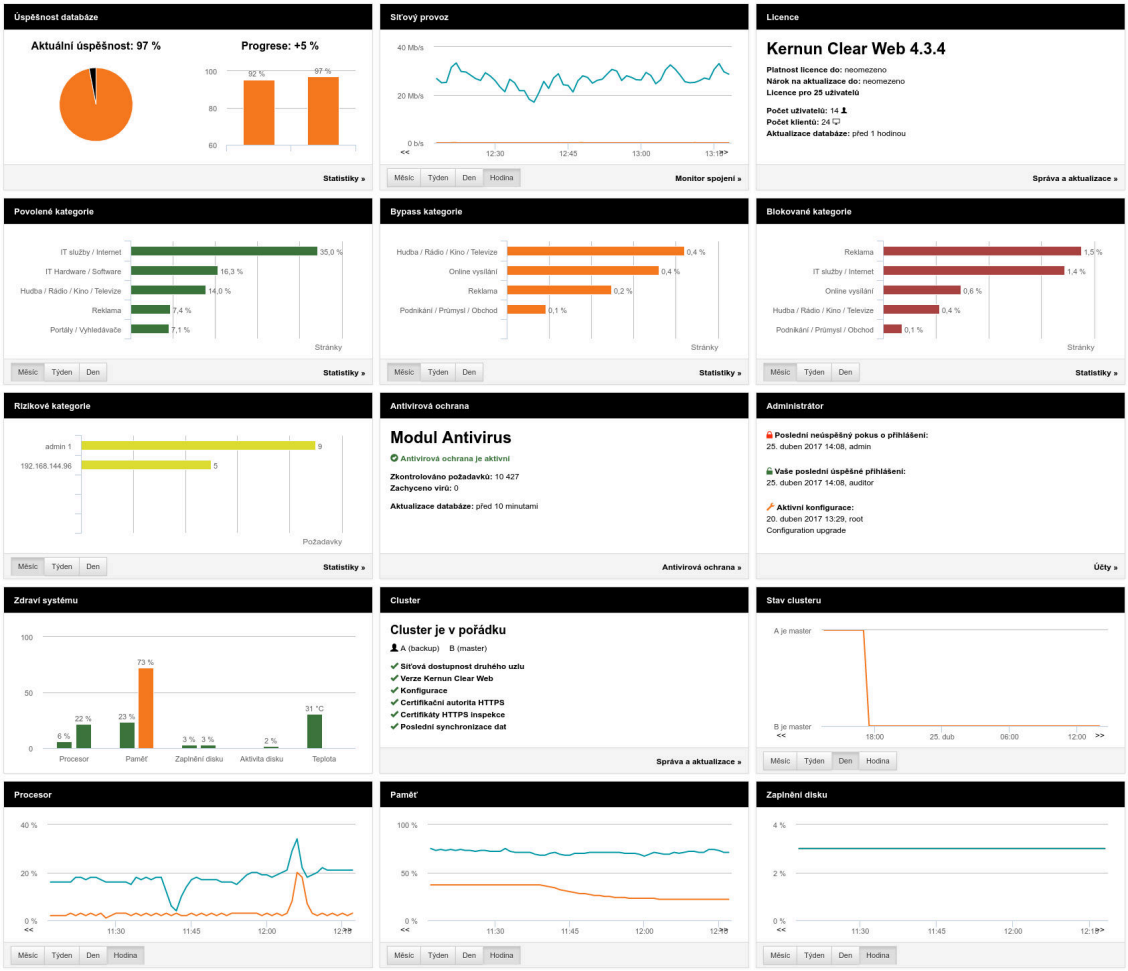
Administrátor Informace o posledním přihlášení administrátora a o poslední změně konfigurace.

Zdraví systému Aktuální hodnoty vybraných důležitých parametrů systému Kernun Clear Web.

Cluster, Stav clusteru Informace o dostupnosti a stavu synchronizace obou uzlů clusteru.

Procesor, Paměť, Kapacita disku Vývoj naměřených hodnot vybraných důležitých parametrů systému za poslední hodinu, den, týden nebo měsíc.

V horní části obrazovky je navigační lišta (obr. 3.2). V jejím levém rohu se nachází tlačítko Clear Web sloužící pro přepnutí do rozhraní modulu Kernun Business Intelligence. Následně jsou zobrazeny jednotlivé aktivity rozhraní se zvýrazněnou právě zobrazenou aktivitou. V pravé části lišty se zobrazují ikony upozorňující na nestandardní stav systému. V pravém rohu lišty je menu, kterým je možné uložit systémovou konfiguraci nebo uživatelské nastavení, zapomenout veškeré provedé změny, změnit heslo a odhlásit se.



Obrázek 3.1: Přehled

Obrázek 3.2: Navigační lišta

3.3 Struktura uživatelského rozhraní

Struktura dostupných aktivit v uživatelském rozhraní má dvě úrovně. První úroveň (nazývaná aktivity) se vybírá pomocí ikon na navigační liště. Názvy druhé úrovně (nazývané sekce) jsou v levém panelu.

- *Přehled*
- *Provoz*
  - *Statistiky* — Statistiky webového provozu generované každý den, týden, měsíc, nebo na požádání
  - *Monitor spojení* — Přehled aktuálně probíhajících HTTP spojení od klientů
  - *Záznamy* — Prohlížení provozních záznamů (logů) obsahujících detailní informace o všech uskutečněných HTTP požadavcích
- *Politika* — Bude podrobně vysvětleno v kap. 4.
  - *Výchozí profil*
  - *Profily*
  - *Výjimky z profilů*
  - *Výjimky z inspekce HTTPS* — při zapnuté inspekci HTTPS
  - *Výjimky z autentizace* — při zapnuté autentizaci
  - *Politika obsahu*
  - *Paketový filtr* — v režimu Router
  - *Přesměrování portů* — v režimu Router
- *Správa*
  - *Síťové nastavení* — Hostitelské jméno, parametry sítě, režim nasazení, ...
  - *Parametry systému* — Nastavení času, interní servery, zasílání zpráv, tabulka doménových jmen a správa záznamů.
  - *Zdraví systému* — Grafy stavu systému
  - *Správa a aktualizace* — Správa verzí a aktualizace systému, licence, zálohování konfigurace a obnova ze zálohy, restart a vypnutí zařízení, služba vzdálené pomoci, HTTPS certifikát administračního rozhraní, SNMP monitoring, systémové komponenty
  - *Globální nastavení provozu* — Konfigurace bezpečného vyhledávání, jazyka chybových hlášek a nadřazené webové proxy.
  - *Proxy autentizace* — Bude podrobně vysvětleno v kap. 5.2.
  - *Inspekce HTTPS* — Bude podrobně vysvětleno v kap. 5.3.
  - *Antivirová ochrana* — Konfigurace antivirové kontroly — Bude podrobně vysvětleno v kap. 5.4.

  - *Účty* — Správa administrátorských účtů

- *Nápověda*
  - *Příručka administrátora* — Zobrazí tuto příručku administrátora
  - *Poznámky k vydání*
  - *Seznam změn*
  - *O aplikaci*

Kapitola 4

Politika

Kapitola představuje možnosti pro nastavení a testování politiky přístupu k webu. Popisuje koncept profilů a výjimek pro definování politiky, způsob vyhodnocení politiky a také pokročilé funkce pro řízení provozu. Pro nastavení pravidel politiky slouží aktivita Politika administračního rozhraní.

Politika přístupu definuje, kteří uživatelé nebo klienti mohou přistupovat na webové servery, a za jakých podmínek. Každý uživatel je identifikován uživatelským jménem a jmény skupin, jejichž je členem. Jestliže je vypnuta autentizace, viz kap. 5.2, lze uživatele rozlišovat podle IP adresy nebo hostitelského jména klienta. Politika přístupu se skládá z pravidel řídících přístup na web nebo na internet obecně. Pravidlo může být profil nebo výjimka, případně pravidlo paketového filtru.

Webové servery jsou v databázi Kernun Clear Web řazeny do kategorií podle typu obsahu. Aktuální příslušnost webové stránky do kategorií lze zjistit v katalogu kategorií dostupném na `http://www.kernun.cz/cwdb`. Kromě základních pevně daných kategorií v databázi lze v aktivitě Správa v sekci Parametry systému definovat servery ve speciální kategorii `Interní servery`, kam jsou implicitně zařazeny také servery s privátními IP adresami podle RFC 1918 ze sítí `10.0.0.0/8`, `172.16.0.0/12` a `192.168.0.0/16`. Pro definování politiky přístupu na základě kategorií webového obsahu slouží pravidla typu profil. V případě potřeby lze definovat pomocí výjimky z profilů pravidlo politiky přístupu také pro jednotlivé servery podle jejich jména.

Pokročilé funkce pravidel politiky jsou:

Bypass Pomocí funkce Bypass lze na uživatele delegovat rozhodnutí, zda na stránku z dané kategorie přistoupí. Uživatel je upozorněn, že na danou kategorii by neměl přistupovat, ale umožní mu v případě potřeby po kliknutí na aktivační tlačítko zobrazit obsah po administrátorem definovanou dobu. Po uplynutí této doby se mu znovu zobrazí upozornění. Doba aktivace funkce Bypass se nastavuje v aktivitě Správa, v sekci Globální nastavení provozu. Pro HTTP metody CONNECT a POST se požadavky povolí bez upozornění.

Nadřazené proxy servery Požadavky se pro uplatněné pravidlo posílají na cílové servery pres vybranou nadřazenou webovou proxy nebo přímo. Seznam nadřazených webových proxy serverů lze definovat v aktivitě Správa, v sekci Globální nastavení provozu.

Rizikové tunelování Umožňuje blokovat šifrované spojení na servery, pro které klient neuvedl doménové jméno, ale pouze IP adresu. Tato funkce blokuje některé aplikace, např. Skype, Tor a TeamViewer. Jedná se o metodu CONNECT s IP adresou v hlavičce Host pro netransparentní provoz a TLS bez vyplněného SNI pro transparentní provoz.

Čas Pro většinu pravidel lze nastavit časový interval, kdy se mají uplatňovat.

4.1 Pravidla politiky

Politika přístupu se skládá z pravidel řídících přístup na web. Pravidlo může být profil nebo výjimka. V případě že je Kernun Clear Web nasazené jako router, lze řídit politiku přístupu na internet také pomocí pravidel paketového filtru.

Politika přístupu se definuje v aktivitě Politika, která je rozdělena do více sekcí v závislosti na využívané funkcionalitě systému Kernun Clear Web:

Výchozí profil Pomocí akcí (Povolit, Bypass, Blokovat) přiřazených ke všem tematickým kategoriím webového obsahu a nastavením pokročilých funkcí lze vytvořit pravidlo politiky přístupu na web nazvané profil. Výchozí profil definuje implicitní pravidlo politiky přístupu na web pro celou síť, které se uplatní na veškerý webový provoz, na který se neuplatnil žádný jiný profil nebo výjimka z profilů.

Profily V případě, že chceme nějakému uživateli nebo skupině uživatelů nastavit jinou politiku přístupu na web, než jak definuje výchozí profil, je potřeba vytvořit nový profil v sekci profily.

Pomocí akcí (Povolit, Bypass, Blokovat) přirazených ke všem tematickým kategoriím webového obsahu a nastavením pokročilých funkcí lze vytvořit pravidlo politiky přístupu na web nazvané profil. Profilu lze přiřadit seznam uživatelů, skupin nebo zdrojových adres, na které se má uplatnit.

Profily definují pravidla politiky přístupu na web pro vybrané zdroje komunikace. Na provoz se uplatní první profil ze seznamu obsahující alespoň jednu identifikaci zdroje komunikace (uživatel, skupina, zdrojová adresa), za předpokladu, že se na provoz neuplatnila žádná výjimka z profilů.

Prázdný seznam zdrojových adres znamená libovolnou zdrojovou adresu. Prázdný seznam uživatelů a skupin při zapnuté autentizaci znamená libovolného autentizovaného uživatele. V případě vypnuté autentizace se uživatel ani skupina nekontrolují.

Příklad: Pomocí výchozího profilu blokujeme přístup na sociální sítě. Ale zaměstnanci obchodního a marketingové oddělení potřebují sociální sítě pro komunikaci se zákazníky, proto jim vytvoříme samostatný profil a v něm sociální sítě povolíme.

Profily jsou zobrazeny v tabulce uspořádané podle priority a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazované sloupce tabulky a také filtrovat profily podle hodnot obsažených ve sloupcích. Nově přidaný profil má nastavené hodnoty z výchozího profilu, jakožto základní politiky přístupu. Nový profil lze vytvořit také duplikováním již existujícího. Profil je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu na web.

Výjimky z profilů Někdy je potřeba pro konkrétní webový server nebo doménu nastavit přístup jinak, než vyplývá z kategorie obsahu serveru a odpovídajícím profilům. V tom případě lze definovat výjimku z profilů, která povolí nebo blokuje přístup k vybraným serverům nebo doménám.

Výjimky z profilů definují pravidla politiky přístupu na web, které umožnují povolit nebo blokovat komunikaci se servery nezávisle na jejich kategoriích obsahu pro vybrané zdroje komunikace. Uplatní se první ze seznamu výjimek z profilů obsahující zároveň identifikaci zdroje komunikace (uživatel, skupina, zdrojová adresa) a příslušnou adresu serveru.

Prázdný seznam adres serverů znamená libovolný server. Prázdný seznam zdrojových adres znamená libovolná zdrojová adresa. Prázdný seznam uživatelů a skupin při zapnuté autentizaci znamená libovolný autentizovaný uživatel. V případě vypnuté autentizace se uživatel a skupina nekontrolují.

Pomocí výchozího profilu blokujeme přístup na sociální sítě. Zaměstnancům obchodního oddělení a oddělení lidských zdrojů povolíme pomocí výjimky z profilů přístup pro pracovní účely na LinkedIn.

Výjimky z profilů jsou zobrazeny v tabulce uspořádané podle priority a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat výjimky podle hodnot obsažených ve sloupcích. Novou výjimku lze vytvořit duplikováním již existující nebo přidáním prázdné. Výjimku je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu na web.

Výjimky z inspekce HTTPS V sekci Inspekce HTTPS aktivity Správa lze zapnout funkci inspekce obsahu šifrované HTTPS komunikace. Výjimky z inspekce HTTPS definují webový provoz, na kterém není vynucena inspekce HTTPS komunikace. Provoz lze identifikovat pomocí zdrojové adresy klienta, cílové adresy serveru nebo podle kategorie obsahu.

Výjimky z inspekce HTTPS jsou zobrazeny v tabulce a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat pravidla podle hodnot obsažených ve sloupcích. Novou výjimku lze vytvořit duplikováním již existující nebo přidáním prázdné. Výjimku je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu na web.

Výjimky z autentizace V sekci Proxy autentizace aktivity Správa lze zapnout funkci autentizace uživatelů, která pro přístup k webu vyžaduje platné uživatelské autentizační údaje. Většina nejčastěji používaných aplikací v prostředí Windows, zejména prohlížečů, se dokáží vůči proxy autentizovat bez nutnosti zásahu uživatele. Některé aplikace nebo klienti z interní sítě však nemusí podporovat zvolený mechanizmus autentizace. Můžou to být proprietární aplikace pro elektronické bankovnictví, aplikace Java nebo některé aktualizace softwaru. Pomocí výjimek z autentizace lze takovéto klientské aplikaci povolit přístup na web bez vynucení autentizace.

Výjimky z autentizace definují webový provoz, na kterém není vynucena autentizace uživatelů. Provoz lze identifikovat pomocí zdrojové adresy klienta, cílové adresy serveru

nebo podle klientského programu z HTTP hlavičky User-Agent. Prázdný seznam User agentů znamená chybějící hlavičku User-Agent.

Výjimky z autentizace jsou zobrazeny v tabulce a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat výjimky podle hodnot obsažených ve sloupcích. Novou výjimku lze vytvořit duplikováním již existující nebo přidáním prázdné. Výjimku je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu na web.

Politika obsahu V sekci Politika obsahu je možné řídit přístup k jednotlivým typům obsahu. Pravidla v této sekci se uplatní na požadavky, které byly povoleny pravidly v sekcích Výchozí profil, Profily a Výjimky z profilů. Provoz lze identifikovat pomocí zdroje komunikace (adresa klienta, uživatel, skupina), cílové adresy serveru a typu obsahu. Typ obsahu je určen z odpovědi serveru, viz `http://www.iana.org/assignments/media-types/media-types.xhtml`).

Prázdný seznam adres serverů znamená libovolný server. Prázdný seznam zdrojových adres znamená libovolná zdrojová adresa. Prázdný seznam uživatelů a skupin při zapnuté autentizaci znamená libovolný autentizovaný uživatel. V případě vypnuté autentizace se uživatel a skupina nekontrolují.

Je-li v pravidle uveden celý MIME typ (např. `image/jpeg`), bude se pravidlo vztahovat právě na tento typ obsahu. Je-li v pravidle uveden pouze název skupiny (např. `image`), uplatní se pravidlo pro všechny typy obsahu z této skupiny (tj. např. `image/jpeg`, ale i `image/gif`, a podobně). Obsahuje-li pravidlo více MIME typů, pak se uplatní, jestliže typ obsahu odpovídá alespoň jednomu z vyjmenovaných.

Pravidla politiky obsahu jsou zobrazena v tabulce a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat výjimky podle hodnot obsažených ve sloupcích. Nové pravidlo lze vytvořit duplikováním již existujícího nebo přidáním prázdného. Pravidlo je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu na web.

Paketový filtr V případě nasazení Kernun Clear Web v režimu router lze také využít pravidla paketového filtru pro řízení komunikace z interní sítě na internet. Tato pravidla jsou na úrovni jednotlivých paketů, je tedy možné jimi řídit provoz libovolného síťového protokolu. Provoz je možné identifikovat na základě zdrojové adresy klienta, cílové adresy a portu klienta, a použitého protokolu transportní vrstvy.

Pravidla paketového filtru jsou zobrazena v tabulce a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat výjimky podle hodnot obsažených ve sloupcích. Nové pravidlo lze vytvořit duplikováním již existujícího nebo přidáním prázdného. Pravidlo je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu.

Přesměrování portů V případě nasazení Kernun Clear Web v režimu router lze komunikaci přicházející na vybrané porty rozhraní zapojeného do internetu přesměrovat na vybrané porty klientů z interní sítě. Tato pravidla jsou na úrovni jednotlivých paketů, je tedy možné

jimi řídit provoz libovolného síťového protokolu. Provoz je možné identifikovat na základě zdrojové adresy klienta, cílové adresy a portu klienta, a použitého protokolu transportní vrstvy.

Tato funkce slouží pro zpřístupnění interních síťových služeb z internetu. Příkladem může být přesměrování komunikace z portu 25 nebo 465 na interní mailový server nebo z portu 80 a 443 na webovou prezentaci společnosti.

Pravidla přesměrování portů jsou zobrazena v tabulce a jejich pořadí lze měnit tažením za ikonu na konci každého řádku. V horní části tabulky lze zvolit zobrazené sloupce tabulky a také filtrovat výjimky podle hodnot obsažených ve sloupcích. Nové pravidlo lze vytvořit duplikováním již existujícího nebo přidáním prázdného. Pravidlo je možné dočasně vypnout, což po aktivaci konfigurace způsobí, že se neuplatní při řízení přístupu.

V případě nasazení v režimu cluster jsou pravidla přesměrování portů aplikována na všechny tři adresy externích síťových rozhraní clusteru, komunikace je tedy přesměrovávána jak ze společné adresy, tak z adres obou uzlů. Pokud je jako cíl přesměrování zvolena adresa některého uzlu, je veškerý provoz přesměrován na tuto adresu. Pokud je jako cíl přesměrování zvolena společná adresa (ať už externího či interního rozhraní), je provoz přicházející na uzel A zpracován uzlem A a provoz přicházející na uzel B je zpracován uzlem B.

4.2 Vyhodnocení politiky

Pro každý HTTP požadavek se vybere jeden profil nebo výjimka z profilů a rozhodne se o povolení nebo zamítnutí požadavku, popř. se nastaví další parametry zpracování požadavku. Výběr profilu nebo výjimky probíhá v několika krocích:

1. Jestliže je Kernun Clear Web nasazen v režimu Router (viz též kap. 2.6.3) a existuje-li pravidlo paketového filtru nebo pravidlo pro přesměrování portů, které vyhovuje danému požadavku, použije se toto pravidlo.

2. Jestliže je zapnutá autentizace uživatelů, požadavek neobsahuje autentizační informace uživatele a neplatí pro něj ani žádná výjimka z autentizace, je požadavek zamítnut pomocí výzvy k autentizaci.

3. Prochází se postupně seznam výjimek z profilů v pořadí, jak jsou zapsané v tabulce. Když se najde výjimka odpovídající požadavku, požadavek se podle jejího obsahu povolí nebo blokuje. Výjimka odpovídá požadavku, jestliže platí současně:

   - cílový server je vyjmenovaný mezi adresami serverů ve výjimce, nebo je seznam serverů ve výjimce prázdný (platí pro libovolný server) a
   - adresa klienta je obsažena v seznamu zdrojových adres ve výjimce, nebo je jméno uživatele nebo skupiny obsažené v seznamu uživatelů, resp. skupin, ve výjimce, nebo jsou seznamy zdrojových adres, uživatelů i skupin prázdné.

4. Jestliže se na požadavek neuplatní žádná výjimka z profilů, hledá se profil. Prochází se postupně seznam profilů v pořadí, jak jsou zapsané v tabulce. Když se najde profil odpovídající

požadavku, rozhodne se o povolení nebo zákazu požadavku podle nastavení kategorií ve vybraném profilu. Profil odpovídá požadavku, jestliže je adresa klienta obsažena v seznamu zdrojových adres v profilu, nebo je jméno uživatele nebo skupiny obsažené v seznamu uživatelů, resp. skupin, v profilu, nebo jsou seznamy zdrojových adres, uživatelů i skupin prázdné.

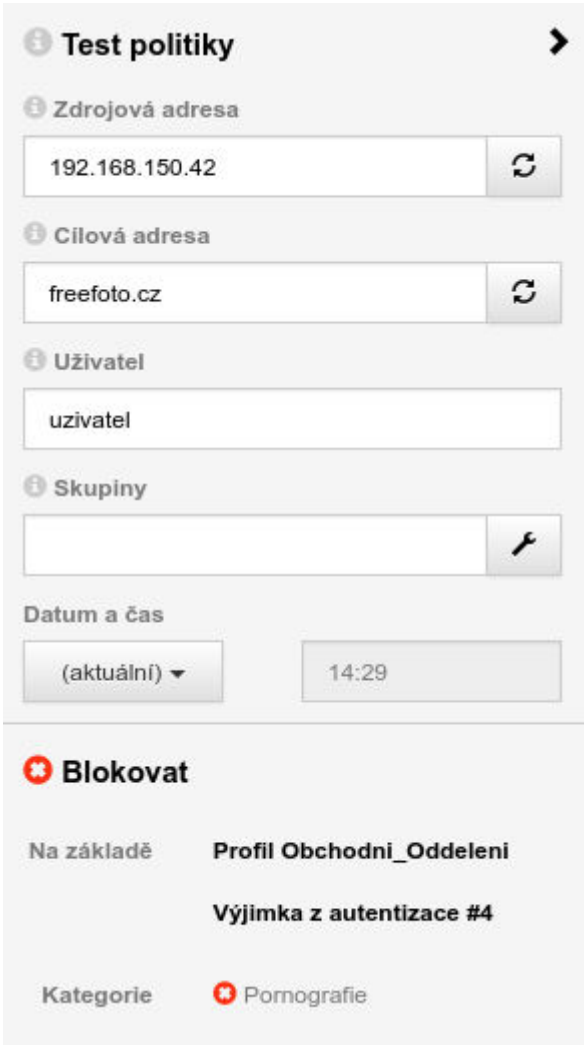
5. Jestliže se na požadavek neuplatní žádná výjimka z profilů, ani žádný profil z tabulky profilů, použije se výchozí profil.

Jestliže je požadavek v některém z předchozích kroků povolen (přímo nebo prostřednictvím funkce Bypass), je požadavek odeslán na cílový server. Na základě typu obsahu odpovědi se použije první vyhovující pravidlo obsahu. Nevyhovuje-li žádné pravidlo obsahu (nebo pokud není žádné pravidlo obsahu zadáno), odpověď serveru je zaslána klientovi. Na odpovědi je vykonána kontrola podle nastavení antivirové ochrany.

4.3 Testování politiky

Test politiky slouží k testování změn při úpravách konfigurace ještě před její aktivací. Nachází se v pravém panelu Politika. Po zadání webového provozu (zdrojové adresy, adresy serveru, času, popř. i jména uživatele nebo skupiny) informuje o akci, která bude provedena, a na základě jakého pravidla politiky. Kliknutí na název pravidla způsobí přesměrování na konfiguraci daného pravidla.

V případě, že byly v konfiguraci politiky provedeny změny a konfigurace nebyla aktivována, mohou se výsledky testování lišit od skutečného chování zařízení Kernun Clear Web. Nástroj test politiky nebere v úvahu pravidla paketového filtru, přesměrování portů a politiku obsahu, protože tato pravidla neřídí provoz na úrovni HTTP požadavku. Test politiky také zatím nepodporuje IPv6 adresy, rozsahy IPv4 adres a odkazy na pojmenované síťové objekty.



Obrázek 4.1: Test politiky

Kapitola 5

Správa

Kapitola vysvětluje důležité a složitější funkce systému Kernun Clear Web z aktivity Správa. Jedná se zejména o autentizaci uživatelů přistupujících k webu, inspekci šifrovaného HTTPS protokolu nebo antivirovou kontrolu.

5.1 Správa a aktualizace

Systém Kernun Clear Web periodicky kontroluje dostupnost nových verzí a aktualizací. V případě zaškrtnuté možnosti Příprava aktualizací se automaticky, bez nutnosti zásahu administrátora, stáhne dostupná aktualizace a připraví se lokálně na zařízení. Tím se čas samotné aktualizace zařízení zkrátí na co nejkratší možnou dobu. V případě nepovedené aktualizace je možné se vždy vrátit k předešlé funkční verzi pomocí tlačítka Obnovit.

Platnost licence je možné zkontrolovat jak na Přehledu, tak v sekci Správa a aktualizace aktivity Správa, kde je navíc možnost nahrát do zařízení novou licenci. V této sekci se také nachází funkce pro zálohování a obnovu konfigurace, restart a vypnutí zařízení Kernun Clear Web.

Pro rychlejší analýzu a řešení nekonzistentností systému lze spustit službu vzdálené pomoci, která umožní přímý přístup technikům výrobce na konkrétní zařízení Kernun Clear Web. Pro fungování této služby nastavte váš firewall a případné mezilehlé prvky vaší síťové infrastruktury tak, aby neblokovaly komunikaci ze zařízení na port 22 (SSH) serveru `callhome.kernun.com`.

V této sekci je možné změnit HTTPS certifikát administračního rozhraní. Ve výchozím nastavení je certifikát vygenerován automaticky a je vždy podepsán certifikační autoritou pro akceptované certifikáty, která je nastavena v sekci kap. 5.3. Při změně této certifikační autority nebo při změně hostitelského jména systému je výchozí certifikát vygenerován nově a může být nezbytné znovu pro něj přidat výjimku v prohlížeči. Lze zadat vlastní certifikát, který se použije namísto výchozího certifikátu.

Dále lze v této sekci zapnout nastavit SNMP server pro umožnění monitorování stavu systému. SNMP používá verzi 3 pomocí UDP protokolu na portu 161 vybraného síťového rozhraní pro přístup v read-only režimu.

5.2 Autentizace uživatelů

Kernun Clear Web podporuje autentizaci uživatelů v prostředí Microsoft Active Directory a Samba. Dokáže zjistit jméno uživatele přihlášeného do domény a jemu příslušející skupiny. Tyto informace využívá k nalezení správného profilu nebo výjimky pro řízení přístupu uživatele k webu podle nastavené politiky kap. 4. Uživatelé a skupiny se následně objevují v monitoru spojení, v záznamech, ve statistikách a lze jich využít i v testu politiky.

Autentizace uživatelů je podporována pro veškerý HTTP a FTP provoz, a pro HTTPS v netransparentním režimu.

Doporučený způsob autentizace je pomocí mechanismu Kerberos, zejména z důvodu efektivnější síťové komunikace a podpoře autentizace uživatelů na terminálových serverech. Protokol NTLM je podporován jako záložní možnost pro případy, kdy klientské aplikace nepodporují Kerberos nebo při použití serveru Samba verze 3 a vyšší v doméně Windows NT.

Ke konfiguraci autentizace slouží podsekce Proxy autentizace v aktivitě Správa. Po nastavení parametrů autentizace a aktivaci konfigurace je nutné provést inicializaci autentizačního mechanismu pomocí tlačítka Inicializovat připojení k doméně. Funkčnost autentizace lze ověřit pomocí tlačítka Otestovat autentizaci v doméně. Obě tlačítka se zobrazí po zapnutí autentizace a aktivaci konfigurace.

> **Poznámka**
>
> Prohlížeč Google Chrome nepodporuje autentizaci uživatelů ve FTP provozu, viz `https://bugs.chromium.org/p/chromium/issues/detail?id=310456`.

Pro úspěšnou inicializaci autentizace je nutné splnit následující předpoklady:

- **Adresa a jméno doménového řadiče musí být správně nastaveny na všech DNS serverech,** používaných zařízením Kernun Clear Web. Musí správně fungovat převod jména doménového řadiče na IP adresu i zpětný převod IP adresy na jméno, kdy jako první prvek seznamu musí vracet jméno uvedené v konfiguraci autentizace.
- **Hodiny na doménovém řadiči a na systému Kernun Clear Web musí být synchronizované.** To lze zajistit pomocí protokolu NTP, kdy se jako primární časový server pro Kernun Clear Web nastaví hlavní časový server interní sítě, což je většinou doménový řadič. Doménové řadiče jsou automaticky používány jako NTP servery a jsou předřazeny NTP serverům ze sekce Parametry systému.

5.2.1 Autentizace metodou Kerberos

Před zahájením konfigurace se ujistěte, že prostředí vaší sítě splňuje všechny předpoklady uvedené v kap. 5.2.

Pro Kerberos autentizaci je nutné nakonfigurovat pouze dva parametry:

- **jméno domény** Active Directory ve tvaru např. `example.com`
- **jméno řadiče domény** ve tvaru např. `ad.example.com`

Lze zadat několik redundantních řadičů domén pro zajištění autentizace i v případě výpadku některého z nich.

Poznámka

Při konfiguraci proxy ve webovém prohlížeči se ujistěte, že zadáváte přesně stejné jméno zařízení Kernun Clear Web, které bylo použito při vytváření souboru keytab. Pro správnou funkčnost autentizace totiž nestačí, nastavíte-li IP adresu, zkrácené jméno (bez domény), nebo alternativní jméno, i když se převede na stejnou IP adresu.

V rámci inicializace Kerberos autentizace je potřeba vytvořit soubor keytab, který obsahuje kryptografické klíče sdílené systémem Kernun Clear Web a řadičem domény. Volba jedné ze dvou podporovaných metod vytvoření souboru keytab se provádí při zahájení inicializace připojení k Active Directory.

Nahrát keytab soubor Vytvořte v doméně nový uživatelský účet. Nastavte účet tak, aby mu nikdy nevypršela platnost hesla. Účet musí mít dostatečná práva na čtení informací o uživatelích a skupinách uživatelů v Active Directory (standardně stačí příslušnost do skupiny `Domain Users`). Poté vytvořte soubor keytab ručně na doménovém radiči jako administrátor zadáním příkazu (příkazový řádek musí být spuštěn jako správce):

```
C:\> ktpass /out KEYTAB /princ HTTP/proxy@AD_DOMAIN
/mapuser USER@AD_DOMAIN /pass * /crypto All
/ptype KRB5_NT_PRINCIPAL
```

kde *KEYTAB* je libovolně zvolené jméno souboru keytab, *proxy* je hostitelské jméno zařízení Kernun Clear Web (včetně jména domény, tzn. FQDN), které se bude nastavovat do konfigurace proxy ve webovém prohlížeči, *AD_DOMAIN* je jméno domény Active Directory a *USER* je jméno vytvořeného uživatele. V hostitelském jméně *proxy* je nutné používat malá písmena, ve jménu domény Active Directory *AD_DOMAIN* je nutné používat velká písmena. Ve jménu souboru keytab a ve jménu uživatele na velikosti písmen nezáleží. Vytvořený soubor keytab nahrajte na Kernun Clear Web prostřednictvím dialogu pro inicializaci autentizace.

Přidat do domény Tento způsob inicializace autentizace z technických důvodů nefunguje v režimu cluster. Po případném nakonfigurování clusteru bude nutné reinicializovat autentizaci nahráním keytabu. S pomocí jména a hesla uživatele ze skupiny `Domain Admins` se systém Kernun Clear Web automaticky přidá do domény a vygeneruje potřebný keytab soubor na hostitelské jméno zařízení Kernun Clear Web. Zkontrolujte, zda vytvořený účet v doméně má dostatečná práva na čtení informací o uživatelích a jejich skupinách v Active Directory.

5.2.2 Autentizace metodou NTLM a NTLM (Samba 3)

Před zahájením konfigurace se ujistěte, že prostředí vaší sítě splňuje všechny předpoklady uvedené v kap. 5.2.

Pro autentizaci metodou NTLM a NTLM (Samba 3) je nutné nakonfigurovat tyto parametry:

- **jméno domény** Active Directory nebo Windows NT
- **jméno pracovní skupiny**, standardně je to první komponenta jména domény (před první tečkou)
- **jméno řadiče domény** ve tvaru `ad.example.com`
- **adresa sítě** (IP adresa s maskou ve tvaru `192.168.1.0/24`), ve které je umístěn řadič domény
- **LDAP URL** ve tvaru `ldap://ad.example.com` pro server LDAP používaný pro zjišťování, do kterých skupin uživatel patří; standardně se jako LDAP server používá řadič domény
- **jméno uživatele** používané pro přihlášení k serveru LDAP.
  - pro NTLM ve tvaru distinguished name (DN), např. `cn=kernun,cn=Users,dc=example,dc=com`
  - pro NTLM (Samba 3) ve tvaru distinguished name (DN), např. `cn=kernun,ou=users,dc=example,dc=com`
- **heslo uživatele** používané pro přihlášení k serveru LDAP
- (pouze NTLM Samba 3) **jméno uzlu LDAP**, pod kterým jsou umístěné informace o uživatelích; zadává se ve tvaru distinguished name (DN), např. `ou=users,dc=example,dc=com`
- (pouze NTLM Samba 3) **jméno uzlu LDAP**, pod kterým jsou umístěné informace o skupinách uživatelů; zadává se ve tvaru distinguished name (DN), např. `ou=groups,dc=example,dc=com`

Při inicializaci NTLM autentizace je nutné zadat jméno a heslo uživatele ze skupiny `Domain Admins`. Následně se systém Kernun Clear Web automaticky přidá do domény a nastaví si připojení používané pro ověřování uživatelů na doménovém řadiči.

5.3 Inspekce HTTPS

Inspekce HTTPS provozu umožňuje průběžně dešifrovat, zkontrolovat, a znovu zašifrovat komunikaci protokolem HTTPS. Inspekci HTTPS provozu lze zapnout v aktivitě Správa v sekci Inspekce HTTPS.

Jestliže je inspekce HTTPS provozu vypnuta, Kernun Clear Web se rozhoduje pouze podle domény cílového počítače. Není možné řídit ani logovat jednotlivé HTTP požadavky.

Jestliže je inspekce HTTPS provozu zapnuta, Kernun Clear Web se pro HTTPS požadavky rozhoduje obdobně jako pro HTTP požadavky.

Protokol HTTPS používá certifikáty jako prostředek k ověření identity serveru. Inspekce HTTPS (z principu věci) vstupuje do komunikace mezi klientem a serverem, což by za normálních okolností webový prohlížeč na straně klienta detekoval a hlásil uživateli jako „Nedůvěryhodné spojení“. Kernun Clear Web tomu předchází: generuje vlastní certifikát serveru, který kopíruje obsah originálního certifikátu serveru. Tento vygenerovaný certifikát je vydán certifikační autoritou (CA) provozovanou na systému Kernun Clear Web.

Kernun Clear Web používá pro komunikaci s klientem serverové certifikáty podepsané jednou ze dvou CA.

CA pro akceptované certifikáty Jestliže HTTPS server používá certifikát, který Kernun Clear Web úspěšně ověří, Kernun Clear Web vygeneruje a pošle klientovi certifikát podepsaný touto CA. Certifikát této CA by měl být importován v prohlížeči uživatele, aby prohlížeč akceptoval certifikát serveru.

Certifikát CA pro akceptované certifikáty je dostupný ke stažení na adrese `kernun.example.com/ca` nebo ve webovém rozhraní Správa v sekci Inspekce HTTPS.

Certifikátu je třeba nastavit v prohlížeči důvěryhodnost tak, aby daný certifikát mohl identifikovat webové stránky.

CA pro odmítnuté certifikáty Jestliže HTTPS server používá certifikát, který Kernun Clear Web neověří, Kernun Clear Web vygeneruje a pošle klientovi certifikát podepsaný touto CA. Certifikát této CA by naopak NEMĚL být importován v prohlížeči uživatele, aby prohlížeč zobrazil varování o nedůvěryhodném spojení.

Certifikáty serveru ověřuje Kernun Clear Web pomocí seznamu důvěryhodných certifikačních autorit. Doporučuje se používat standardní seznam důvěryhodných certifikačních autorit, který je součástí produktu Kernun Clear Web. Je-li potřeba, je možno přidat další důvěryhodné certifikační autority.

Kernun Clear Web umožňuje definovat výjimky z inspekce HTTPS. Výjimky se zadávají v aktivitě Politika v sekci Výjimky z inspekce HTTPS. Výjimky je možno zadat na základě adresy klienta, adresy serveru nebo seznamu Clear Web kategorií. Kernun Clear Web do provozu vyjmutého z inspekce HTTPS nevstupuje a chová se k němu stejně, jako by byla HTTPS inspekce zcela vypnuta.

5.4 Antivirová ochrana

Zařízení Kernun Clear Web poskytuje ochranu před viry, trójskými koňmi a jinými druhy škodlivých programů ve webovém obsahu přenášeném z internetu do interní sítě organizace. Pro dosažení vysoké bezpečnosti podle konceptu obrany do hloubky doporučujeme využít tuto funkci jako doplňkovou vrstvu ochrany k antivirům na koncových stanicích a serverech. Ochrana je implementována pomocí specializovaných antivirových řešení renomovaných výrobců.

Pro nastavení a správu antivirové ochrany se používá sekce Antivirová ochrana aktivity Správa. Lze zvolit režim integrovaný antivirus nebo ICAP server, nastavit maximální velikost kontrolovaných dokumentů nebo úroveň zabezpečení. Pro antivirovou ochranu dat přenášených pomocí HTTPS spojení je nutné mít zapnutou inspekci HTTPS provozu. Funkčnost antivirové ochrany lze zkontrolovat pomocí série testů spustitelných z administračního rozhraní.

Režim integrovaný antivirus využívá antivirové řešení a databázi společnosti Kaspersky přímo na zařízení Kernun. Nutností je zakoupení platné licence pro modul antivirus a její nahrání na systém Kernun Clear Web pomocí administračního rozhraní.

Aktualizace databáze vzorků virů je prováděná automaticky minimálně jednou za hodinu. Aktualizaci lze také spustit manuálně z administračního rozhraní.

Režim ICAP server umožnuje zasílání webového obsahu za účelem antivirové kontroly na dedikovaný antivirový server pomocí síťového protokolu ICAP. Kernun Clear Web v komunikaci vystupuje jako ICAP klient a s ICAP serverem komunikuje v módu RESPMOD. Pro fungování je nutné nastavit správné URI pozůstávající z IP adresy a portu ICAP serveru (většinou port 1344) a z cesty ke službě. Byla ověřena spolupráce systému Kernun Clear Web s následujícími antivirovými produkty, pro které je přednastavena výchozí cesta ke službě:

1. Kaspersky Anti-Virus Suite for Gateway 5.5
2. ESET Gateway Security 4

   V grafickém rozhraní ESET GS4 je nutné povolit položku Performance Agent. Položka se nachází v sekci Configuration/ICAP.
3. eScan for NAS 5.1-0
4. McAfee Email and Web Security 5.6
5. Symantec Scan Engine 5
6. Sophos SAVUL 4 + SAVDI 2

Je možné použít i jiná antivirová řešení podporující ICAP protokol pomocí položky jiný a zadáním odpovídající cesty pro službu antiviru podle jeho konfigurace (v současné době není podporováno antivirové řešení DrWeb).

5.5 Cluster pro vysokou dostupnost

Cluster slouží k zajištění vysoké dostupnosti služeb poskytovaných systémem Kernun Clear Web. Umožnuje snížit na minimum čas výpadku v případě poruchy hardwarového zařízení. Předpokladem je redundantní zapojení dvou stejných hardwarových zařízení Kernun Clear Web (tzv. uzlů) za použití clusterové licence. Jeden uzel clusteru je hlavní (master) a druhý záložní (slave). V případě výpadku hlavního uzlu dojde bez potřeby administračního zásahu správce k automatickému převzetí provozu záložním uzlem. Vysokou dostupnost služeb pro virtuální zařízení Kernun Clear Web doporučujeme zajistit pomocí funkcí konkrétního virtualizačního prostředí.

Pro správné fungování clusteru je nutné mít oba uzly v synchronizovaném stavu. K synchronizaci interního stavu uzlů dochází automaticky a průběžně v řádu jednotek minut. K synchronizaci konfigurace mezi uzly dochází při aktivaci konfigurace na jednom z uzlů nebo při použití funkce Spárovat uzly clusteru.

Celkový stav clusteru:

V pořádku Oba uzly clusteru jsou zapnuté, jsou navzájem dostupné po síti a jsou v synchronizovaném stavu.

Rozpojený Uzly clusteru nejsou navzájem dostupné po síti například z důvodu výpadku jednoho z nich nebo chyby v síti.

Degradovaný Oba uzly jsou zapnuté, jsou navzájem dostupné po síti, ale nelze je synchronizovat.

Možné důvody:

Liší se verze systému na uzlech clusteru. Pomocí aktualizace systému sjednoťte verze Kernun Clear Web na obou uzlech.

Liší se obsah konfigurace na uzlech clusteru. Pomocí funkce Spárovat uzly clusteru sjednoťte soubor s konfigurací.

Liší se výchozí CA pro HTTPS inspekci na uzlech clusteru. Pomocí funkce Spárovat uzly clusteru sjednoťte CA.

Liší se aktivní CA pro HTTPS inspekci na uzlech clusteru. Pomocí funkce Spárovat uzly clusteru sjednoťte certifikáty serverů.

5.5.1 Aktivace clusteru

Zprovoznit cluster je možné s pomocí clusterové licence na dvou stejných hardwarových zařízeních Kernun Clear Web se stejnou verzí systému. Jedno ze zařízení, dále označované jako uzel A, může být aktuálně používáno, druhé, označované jako uzel B, musí být nově nainstalováno. Obě zařízení se musí nacházet ve stejném ethernetovém segmentu jedné sítě. Každý z uzlů má pro svá síťová rozhraní vlastní adresu a hostitelské jméno zavedené do interních DNS serverů. Také existuje sdílená adresa a hostitelské jméno pro celý cluster.

Pro nasazení Kernun Clear Web v clusteru v režimu Proxy se tedy celkově jedná o tři síťové adresy a tři hostitelská jména. Pro nasazení Kernun Clear Web v clusteru v režimu Router se celkově jedná o šest síťových adres a šest hostitelských jmen.

Typické je použití aktuální adresy a hostitelského jména uzlu A, jakožto sdílené adresy a hostitelského jména celého clusteru a vytvoření dvou nových adres a hostitelských jmen pro uzly v konfiguraci.

Samotná aktivace clusteru probíhá následovně:

1. V administračním rozhraní uzlu A v Správa / Síťové nastavení / Pokročilé možnosti aktivovat funkci Nakonfigurovat cluster. Vyplnit, případně upravit, hodnoty síťových adres, hostitelských jmen a MAC adres. Ujistěte se, že veškeré stávající úpravy mezilehlých prvků vaší síťové infrastruktury jsou platné i pro nové adresy zařízení, viz kap. 2.1. Aktivujte konfiguraci. Z důvodu změn síťových adres dojde k odhlášení správce z rozhraní.

2. Přihlásit se do rozhraní uzlu A (adresa uzlu nebo sdílená adresa clusteru). Upozornění na nedostupnost uzlu B ignorujte. V sekci Správa / Síťové nastavení / Pokročilé možnosti nebo Správa / Správa a aktualizace použijte funkci Uložit konfiguraci pro vytvoření clusteru. Odhlašte se z rozhraní, jinak bude rozhraní na tomto uzlu v dalších krocích zobrazovat hlášky, které mohou působit matoucím dojmem.

3. Přihlásit se do rozhraní uzlu B. V sekci Správa / Síťové nastavení / Pokročilé možnosti nebo Správa / Správa a aktualizace použijte funkci Připojit ke clusteru a konfigurační soubor z předchozího kroku. Aktivujte konfiguraci. Z důvodu změn síťových adres dojde k odhlášení správce z rozhraní.

4. Přihlásit se do rozhraní uzlu B na adrese tohoto uzlu. Po automatickém ustanovení spojení mezi uzly A a B (které může trvat i minutu) se zobrazí okno Počáteční spárování clusteru, které způsobí prvotní synchronizaci clusteru.

V případě nastavené autentizace pomocí metody Kerberos je nutné v kroku 1 a 3 použít pro inicializaci autentizace v procesu aktivace konfigurace existující keytab podle kap. 5.2.1.

5.5.2 Aktualizace systému v clusteru

Aktualizace clusteru na novější verzi systému Kernun Clear Web probíhá postupně. Nejdříve je potřeba aktualizovat záložní (slave) uzel clusteru, poté přepnout provoz přepnut na aktualizovaný uzel, a nakonec aktualizovat druhý uzel. Po aktualizaci zařízení je cluster v degradovaném stavu, takže je nutné Spárovat uzly clusteru. Pro přepnutí provozu na druhý uzel slouží funkce Přesunout roli mastera v sekci Správa / Správa a aktualizace.

Funkce v sekci Správa / Správa a aktualizace týkající se aktualizace systému (kontrola nejnovější verze, aktualizace, obnova předchozí verze) jsou prováděna pouze na zařízení, do jehož rozhraní je uživatel právě přihlášen.

5.6 Účty

Vytvoření a správu účtů pro přístup k administračnímu rozraní Kernun Clear Web lze provádět v sekci Účty aktivity Správa. Vlastník účtu využívá pro autentizaci do administračního rozhraní název účtu a heslo. Úspěšně autentizovanému uživateli rozhraní jsou přidělena oprávnění k manipulaci s funkcemi rozraní podle nastavené role. Vytvořenému účtu lze změnit heslo nebo role, avšak pro změnu názvu nebo celého jména vlastníka je potřebné vytvořit účet nový. Z bezpečnostních důvodů je vyžadována změna výchozího hesla každého účtu po prvním úspěšném přihlášení.

Jednotlivým rolím jsou přidělena následující oprávnění:

Administrátor Má neomezená práva pro manipulaci s funkcemi rozhraní.

Auditor Má přístup do všech aktivit pouze pro čtení. Tato role je určena zejména pro kontrolu správného nastavení systému, politiky přístupu a vyhodnocování záznamů.

Správce systému Může provádět změny pouze v aktivitě Správa. Tato role je určena zejména pro správu, zajištění funkčnosti a integraci zařízení Kernun Clear Web do počítačové sítě.

Správce politiky Může provádět změny pouze v aktivitě Politika. Tato role je určena zejména pro nastavení, vyhodnocování a správu politiky přístupu uživatelů k webu.

Uživatel KBI Má přístup pouze k funkcím modulu Kernun Business Intelligence. Tato role je určena pro analýzu záznamů nebo tvorbu reportů a sestav v modulu Kernun Business Intelligence.

5.7 Single Sign-on

Pro přihlášení do webového rozhraní bez nutnosti zadávat uživatelské jméno a heslo lze použít funkcionalitu Single Sign-on (SSO). Ta v prostředí Microsoft Active Directory využívá protokol Kerberos a LDAP.

Podmínkou funkčnosti SSO je správně nakonfigurovaná proxy autentizace pomocí metody Kerberos: kap. 5.2.1 a správně nastavené prostředí klienta.

Microsoft Internet Explorer a Google Chrome:

- V nastaveních Možnosti Internetu, v záložce "Zabezpečení", v sekci "Důvěryhodné weby"přidat hostitelské jméno KCW (např. https://kernun.example.com) do seznamu "Weby".
- Nastavit ve "Vlastní úroveň...", v sekci "Ověření uživatele", v podsekci "Přihlášení"možnost "Automatické přihlášení pod aktuálním uživatelským jménem a heslem".

Mozilla Firefox:

- Zobrazit pokročilá nastavení zadáním adresy about:config do adresního řádku prohlížeče.
- Hodnotu položky s názvem "network.negotiate-auth.trusted-uris"nastavit na hostitelské jméno KCW (např. https://kernun.example.com).

Single Sign-on lze nastavit v sekci "Účty": kap. 5.6. Poté lze do webového rozhraní autentizovat dvěma způsoby:

Pomocí účtu v Active Directory: Konkrétnímu lokálnímu účtu lze nastavit jeden AD účet z domény. Tento AD účet lze následně využít pro přihlášení pomocí SSO k tomuto lokálnímu účtu.

Pomocí skupin v Active Directory: V tabulce mapování AD skupin na role je možné k jednotlivým rolím přiřadit AD skupiny, jejichž členové po přihlášení pomocí SSO obdrží oprávnění dané role bez nutnosti vytvářet lokální účet. Jestliže je možné uživateli přiřadit více rolí, použije se role s nejvyššími oprávněními.

Kapitola 6

Provoz

Kapitola obsahuje informace a funkce dostupné v sekcích aktivity Provoz. Popisuje dva typy uchovávaných provozních záznamů a z nich generované statistiky společně s nástrojem pro monitorování aktivní komunikace Kernun Clear Web.

6.1 Statistiky

Webový provoz kontrolovaný a řízený zařízením Kernun Clear Web lze jednoduše analyzovat pomocí statistik. Statistiky systému jsou generované periodicky za každý ukončený den, týden nebo měsíc. Mimo to lze vytvořit vlastní statistiku za zvolené období z dostupných záznamů a s vybraným filtrem na klienta, uživatele, skupinu, server, pravidlo nebo kategorii. Takto vytvořené statistiky lze filtrovat podle data, zobrazit, smazat nebo stáhnout jako jeden soubor ve formátu HTML.

Každá statistika se skládá ze tří graficky oddělených částí. Mimo hlavičky s názvem, specifikací období a filtru obsahuje Souhrnné informace, Časový histogram a Top X hitparády.

Souhrnné informace V této části statistiky lze zjistit, kolik bylo za sledované období vyřízeno stránek nebo požadavků protokolu HTTP a staženo nebo odesláno dat. Tyto údaje jsou členěny podle akce, která byla vykonána na povolené nebo blokované a zda byl detekován virus nebo použita funkce Bypass. Výsečový graf zobrazuje poměr jednotlivých akcí a také lze zjistit úspěšnost databáze Kernun Clear Web za sledované období. Kliknutí do tabulky slouží k nastavení filtru pro zbylé dvě části statistiky.

Časový histogram Zobrazuje vývoj webového provozu v čase (hodina, den v týdnu, den v měsíci) pro stránky, požadavky, stažená nebo odeslaná data podle filtru z první části statistik. Názvy akcí v legendě grafu slouží pro úpravu zobrazovaných dat.

Top X hitparád Poslední část statistik obsahuje tříúrovňovou interaktivní hitparádu pro vybraných top X položek. První úroveň tvoří akce, druhou úroveň klient, server, uživatel, skupina, kategorie nebo pravidlo. Třetí úroveň tvoří smysluplné položky pro prvek vybraný v druhé úrovni. Lze přepínat mezi sloupcovým a výsečovým zobrazením grafu.

6.2 Monitor spojení

Přehled právě probíhajících spojení je dostupný v sekci Monitor spojení v aktivitě Provoz.

Každý řádek této tabulky reprezentuje jedno právě probíhající spojení klienta. Pro každé spojení jsou mimo jiné zobrazeny informace o klientovi, uživateli, počtu a rychlosti stažených a odeslaných dat a času, kdy spojení začalo. Jestliže skrze spojení právě probíhá nějaký požadavek, zobrazuje se též informace o cíli, URL a kategoriích.

6.3 Záznamy

Kernun Clear Web vytváří a ukládá základní a podrobné provozní záznamy. Oba typy jsou uchovávané v textové podobě, která je komprimovaná po dnech. Tyto záznamy jsou uložené na zařízení standardně po dobu 31 dní. Dobu uložení lze změnit v aktivitě Správa, sekci Parametry systému. Nastavení příliš vysokého limitu může vést k zaplnění disku a k omezení funkčnosti zařízení. V režimu cluster jsou z důvodu šetření systémových prostředků synchronizovány pouze záznamy z předchozích dnů, pro analýzu záznamů z dnešního dne je nutné se přihlásit do rozhraní uzlu clusteru, který analyzujeme.

Základní logy jsou importovány do databáze, která je používána pro generování statistik a využívána modulem Kernun Business Intelligence pro tvorbu reportů. Více o správě databáze lze nalézt v administrační příručce modulu Kernun Business Intelligence

Pro práci s provozními záznamy je určena sekce Záznamy v aktivitě Provoz. Před samotných zobrazením záznamů je nutno upřesnit omezující parametry, jako je typ záznamů nebo hledaný výraz. Pro urychlení práce doporučujeme co nejvíce omezit období prohledávaných záznamů, zadáním časového rozmezí. Zobrazení záznamů za dnešní den je rychlejší, protože data není nutné dekomprimovat. Při nevyplnění konce časového intervalu se budou postupně zobrazovat nově vznikající záznamy. Hledaný výraz lze upřesnit v pokročilém nastavení filtru. Zobrazené záznamy lze filtrovat v levém panelu.

Záznamy se zobrazují ve formě tabulky. V záhlaví tabulky se nachází řádek s filtry, které omezují zobrazované záznamy. Sloupce lze skrýt pomocí tlačítka Zobrazit sloupce, kde je kliknutím a tažením možné upravit pořadí sloupců. Po dvojitém kliknutí na řádek se zobrazí detailní informace obsažené v záznamu.

6.3.1 Základní záznamy

Jedná se o záznamy, které by měly ve většině případů stačit ke zjištění požadovaných informací. Obsahují informace pro statistiky a reporty. Naopak neobsahují informace týkající se funkcí systému samotného. K tomuto účelu slouží Podrobné záznamy, viz níže. Každý HTTP požadavek, HTTPS nebo TCP spojení vytvoří jeden základní záznam.

Ve výchozím nastavení se zobrazují pouze záznamy, kdy byla na požadavek vrácena odpověď v podobě webové stránky. Pro zobrazení záznamů, jejichž odpověď obsahovala obrázky, skripty, archivy nebo TCP a HTTPS spojení, je nutné vypnout možnost Pouze stránky. Po vyplnění hledaného výrazu se zobrazí pouze záznamy, které ho v některém z textových sloupců obsahují.

Každý záznam obsahuje informace, které jsou v detailu záznamu rozděleny do čtyř skupin.

První skupina obsahuje čas vytvoření záznamu a identifikátor TCP spojení či HTTP požadavku. Druhá skupina identifikuje zdroj komunikace pomocí IP adresy a portu. V případě zapnuté autentizace i identifikaci uživatele a skupin, do kterých uživatel patří. Třetí skupina určuje cíl, server, doménu, IP adresu, port a kategorii obsahu. Poslední skupina obsahuje ostatní informace, jako například pravidlo politiky, URL adresu, typ obsahu odpovědi a množství odeslaných a stažených dat. Z detailu záznamu je možné se překliknout na adresu cíle, nebo analyzovat server pomocí služeb GeoIP, Whois, Alexa a katalogu kategorií Kernun Clear Web.

6.3.2 Podrobné záznamy

Oproti základním záznamům obsahují podstatně více informací, protože obsahují detailní informace o průchodu jednotlivými komponentami. Jsou proto vhodné pro analýzu problémů síťové komunikace i samotného systému Kernun Clear Web.

Vzhledem k jejich rozsáhlé velikosti je v grafickém rozhraní omezen přístup pouze po zadání odpovídajícího identifikátoru TCP spojení či HTTP požadavku (session ID), který administrátor získá buď v základních záznamech, případně se session ID zobrazuje v chybových a Bypass stránkách generovaných systémem Kernun Clear Web.

Každý podrobný záznam obsahuje jednoznačný identifikátor session ID spolu s časem, kdy záznam vznikl, a službou, která záznam vytvořila. Zejména obsahuje zprávu a její strukturovaný identifikační kód.

6.4 Řešení problémů

Pro řešení problémů v systému Kernun Clear Web lze využít následující možnosti:

- Příručka administrátora dostupná v aktivitě Nápověda nebo na stránkách výrobce.
- Popisky v samotném administračním rozhraní a to jako tooltip nebo ikona Více informací.
- Test funkčnosti autentizace a test politiky.
- Statistiky, monitoring, záznamy a grafy stavu systému.
- Služba vzdálené pomoci.
- Reset zařízení do továrního nastavení, viz kap. 5.1) nebo z příkazové řádky spuštěním **kernun factory_reset -r**.