Kernun
INTERNET SECURITY

Kernun Adaptive Firewall

Adaptujte na vyšší bezpečnost

Účinná ochrana před probíhajícím kyberútokem

Kernun Adaptive Firewall je bezpečnostní aktivní síťový prvek, který efektivně chrání síťovou infrastrukturu před kybernetickými útoky, které jsou v danou chvíli skutečnou aktivní hrozbou. Využívá k tomu unikátní databázi hrozeb, obsahující charakteristiky útoků, díky níž dokáže na aktuální bezpečnostní situaci rychle reagovat a útoky automaticky blokovat.

Se znalostí aktivních hrozeb

Expertním způsobem tvořená databáze je unikátní a nemá v ČR obdoby. Tvůrcem i správcem databáze je bezpečnostní tým KERNUN CSIRT, který je při analýze a identifikaci hrozeb, plně zapojen do spolupráce a výměny těchto informací s národními bezpečnostními autoritami a CSIRT týmy komerčních firem i státní správy.

Kernun Adaptive Firewall

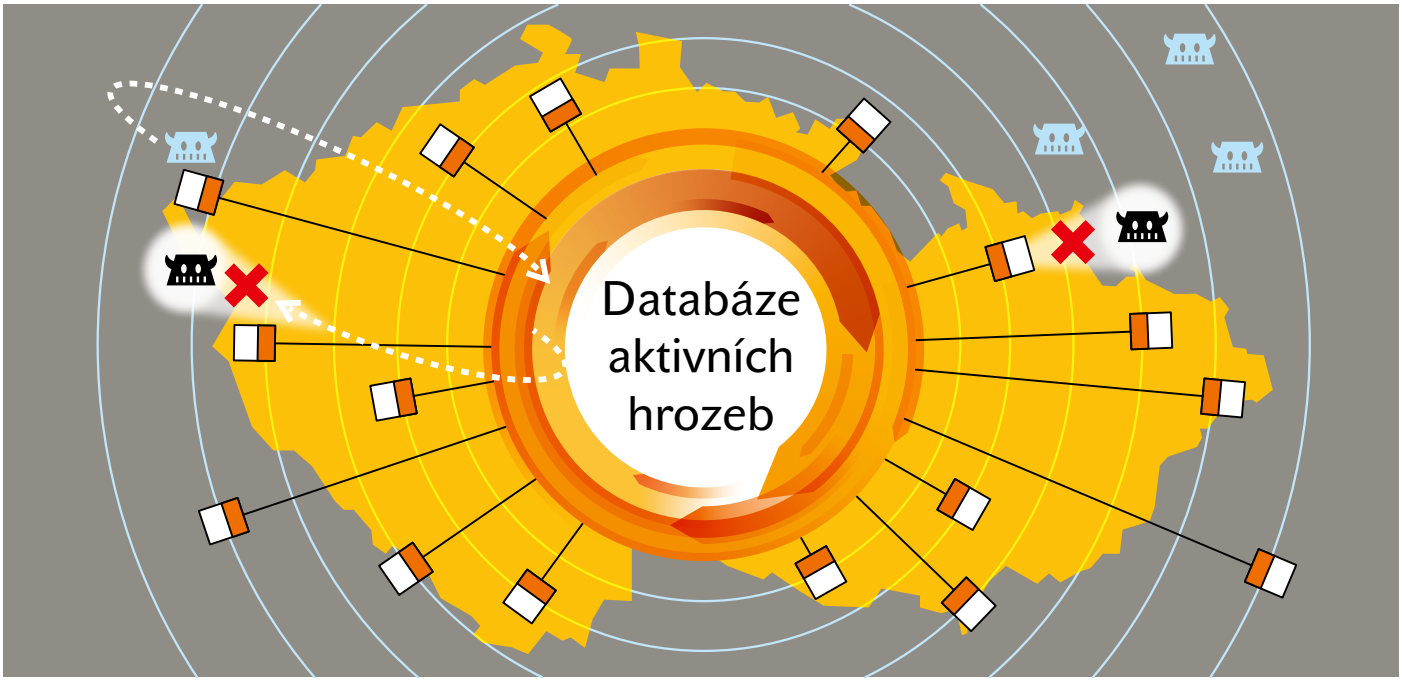
Chrání před kyberútoky právě teď

- Moderní koncepce adaptivního firewallu
- Automatická bezpečnostní reakce a blokace útoků
- Unikátní databáze aktivních hrozeb v České republice
- Mimořádná účinnost a udržitelnost zabezpečení sítě
- Zjednodušení procesů při správě a obsluze řešení
- Český produkt s technickou podporou výrobce
- Záruka a důvěryhodnost zdrojového kódu

Proč adaptivní firewall

Klíčová otázka je stále stejná: jak rozpoznat útočníka?

Řešením je adaptivnost založená na analýze internetového provozu a kolektivní inteligenci. Tým KERNUN CSIRT je správcem unikátní databáze aktivních hrozeb, které nás skutečně ohrožují. Pokud v českém internetu probíhá cílený útok, Kernun Adaptive Firewall se o něm záhy dozví a může tak rychle a efektivně reagovat.



Nastává doba neviditelná

V současné době pozorujeme jednoznačný trend uzavírat veškerou komunikaci do šifrovaných kanálů. Dříve používané protokoly, jako je HTTP, SMTP nebo DNS, jsou vytlačovány svými šifrovanými variantami. Uživatelé stále častěji využívají vzdálená připojení (VPN), v nichž je veškerá komunikace okolnímu světu nedostupná. Objevují se nové standardy jako TLS verze 1.3 nebo HTTP/3, které velmi znesnadňují nebo přímo znemožňují jejich inspekci. Praktika známá jako rozlamování HTTPS se tak dříve či později stane neproveditelnou. **Bezpečnostní správce má už jen málo technických možností pro účinné vynucení bezpečnostní síťové politiky.**

Jak rozpoznat útočníka?

Jakkoliv může být obsah komunikace skryt v šifrovaném kanálu, stále ještě zůstává mnoho informací, které známe. Jsou to tzv. meta informace. Známe především adresy: kdo a s kým komunikuje. Známe kdy, jak, jak často, a kolik dat prochází. Kdybychom znali adresy útočníků nebo dokázali poznat, jestli je komunikující adresa nebezpečná, mohli bychom taková spojení jednoduše nepovolit. Jenže jak je poznat?

Řešením je adaptivnost a znalost prostředí

Pro získání informací o tom, kdo je nebo může být útočník, je potřeba aktivně sledovat a analyzovat širší síťový kontext. Posouzení nelze provádět na jednom místě nebo na jednom firewallu. Musí probíhat kontinuálně nad co možná největším množstvím dat příslušné lokality, v našem případě českého internetu.

To, co na jednom místě, na jednom firewallu, neuvidíme, s oddálením pozorovacího okna na širší síťový kontext už spatříme. Například na několika krátkých spojení na SSH portu lokálně nepoznáme mnoho. Ale pokud vidíme, že jedna adresa provádí několik malých SSH spojení na velké množství různých IP adres, bude se nejspíš jednat o útočníka, který se snaží prolomit heslo na SSH přístupu.

Tvoříme unikátní databázi aktivních hrozeb

Výsledkem takové analýzy je databáze hrozeb, které nás ohrožují v našem prostředí. Lokální databáze je rychlá, efektivní a mimořádně účinná.

Jakmile je útočník ve sledovaném prostředí poprvé zachycen a identifikován, databáze hrozeb je aktualizována a případný pokus o útok je na všech připojených zařízeních Kernun automaticky zablokován. A to bez nutnosti zásahu administrátora.

Jestliže tedy v českém internetu probíhá nějaký cílený útok, Kernun Adaptive Firewall se o něm záhy dozví a může tak rychle a efektivně reagovat.

Kernun Adaptive Firewall

Výkonný bezpečnostní nástroj

Čtyři hlavní bezpečnostní komponenty v jednom řešení poskytují vysokou úroveň ochrany a zabezpečení infrastruktury sítě.

Adaptivní firewall

Bezpečnostní síťová komponenta vyhledávající v síťovém provozu spojení, která představují hrozbu. Pracuje s unikátní databází aktivních hrozeb, která vzniká na základě sofistikovaných metod a stálého vyhodnocování síťových provozů, a to ve spolupráci s důvěryhodnými národními autoritami českého internetu. Rozšiřuje tak běžné signatury útoků (IPS/IDS) navíc o unikátní signatury hrozeb, které jsou právě aktivní v České republice.

Webový filtr

Kvalitní technologie řízení webového provozu, přesná filtrace obsahu a flexibilní nastavení pravidel, to jsou klíčové vlastnosti webového filtru Kernun Clear Web, který v reálném provozu dosahuje až 95% úspěšnost. Systém umožňuje s vysokou přesností blokovat stránky s nebezpečným či nevhodným obsahem a nastavit účinná pravidla bezpečného přístupu a chování uživatelů na internetu. Navíc preventivně chrání počítačovou síť před zavirováním, generuje detailní statistiky a poskytuje ucelený přehled o webové komunikaci pro odpovědné řízení a nastavení bezpečnostní politiky.

Stavový firewall

Uživatelsky přívětivé administrační rozhraní umožňuje snadnou a intuitivní obsluhu. Všechna výchozí nastavení jsou připravena podle principu Best practices, aby poskytovala co nejvyšší možnou míru zabezpečení při co nejmenším snížení propustnosti sítě. Pokročilá nastavení pak umožňují detailní ladění pravidel dle specifických požadavků bezpečnostní politiky.

VPN server

Zajišťuje bezpečnou šifrovanou komunikaci pro režimy Site-to-Site, tedy bezpečné propojení poboček, tak i pro režimy Remote Access Server, které jsou určeny pro bezpečné připojení mobilních klientů.

Ryze český produkt

Kernun Adaptive Firewall je ryze český produkt. Za produktem stojí český tým, který může pomoci s řešením implementačních i provozních záležitostí. Celý produkt je vytvářen jako crystal box, který lze auditovat až na úroveň zdrojových kódů. Garantuje absenci „zadních vrátek" a zbavuje tak obavy z defraudace informací.

Produkt a licence

Kernun Adaptive Firewall je dodáván jako samostatné hardwarové zařízení dle požadovaného výkonu nebo jako virtuální zařízení (VirtualBox, vSphere, Hyper-V, XenServer a další). Řešení je licencováno (per box) dle propustnosti s nárokem na nové verze včetně pravidelné aktualizace filtrační databáze. Lze jej navíc pořídit formou jednorázové investice nebo formou služby, což umožňuje hradit náklady z investičních nebo provozních finančních prostředků.

Svěřená správa a servis

Jako český výrobce s vlastním vývojem garantujeme maximální dostupnost technické podpory s možností svěřené správy až 24×7, servisní zásah v místě instalace a bezkonkurenční záruku na českém trhu v podobě opravy softwaru do smluvně stanoveného počtu dní od nalezení bezpečnostní chyby.

Vyšší bezpečnost díky znalosti českého internetu

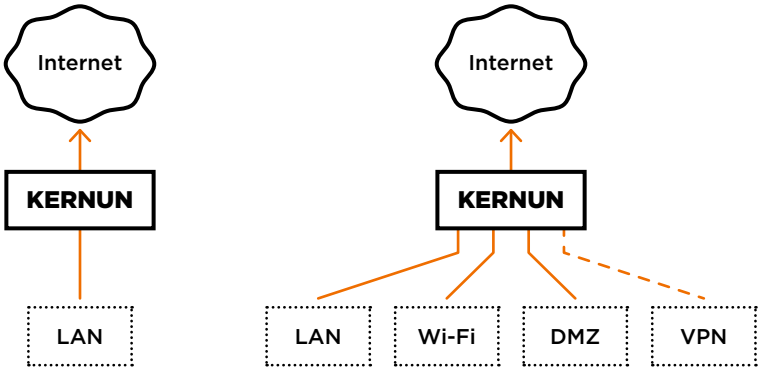
- **Přesné a cílené zaměření na prostředí českého internetu a jeho páteřní sítě**
- **Spolupráce s národními bezpečnostními autoritami a CSIRT týmy**
- **Rozsáhlá síť zapojených zařízení KERNUN ve státním i komerčním sektoru**
- **Jakmile je útočník poprvé zachycen, databáze hrozeb je aktualizována**
- **Další pokus o útok je na všech připojených zařízeních automaticky zablokován**
- **Rychlá efektivní bezpečnostní reakce bez nutnosti zásahu administrátora**
- **Systém aplikované kolektivní inteligence chrání konkrétní cíle**

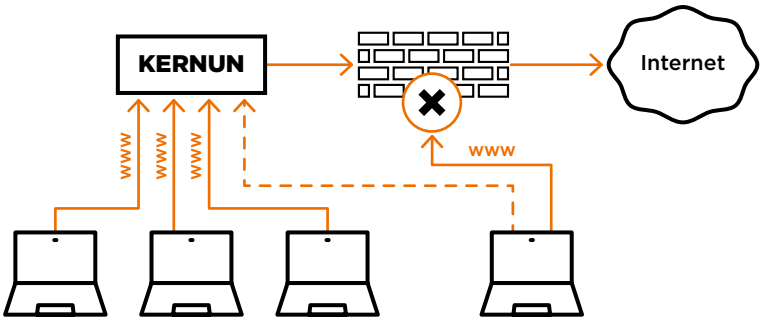
Režimy nasazení

Kernun Adaptive Firewall nabízí flexibilní možnosti nasazení do síťové infrastruktury

Perimetrový firewall

Základní koncepce implementace firewallu. Typicky se jedná o připojení privátní sítě k internetu. V tomto režimu jsou plně funkční všechny bezpečnostní komponenty, tedy Adaptivní firewall, Webový filtr, Stavový firewall i VPN server. Při pokročilejším zapojení zařízení odděluje od sebe více sítí, z nichž každá má jinou úroveň důvěryhodnosti. Režim umožňuje také zapojení dvou uzlů do klastru.



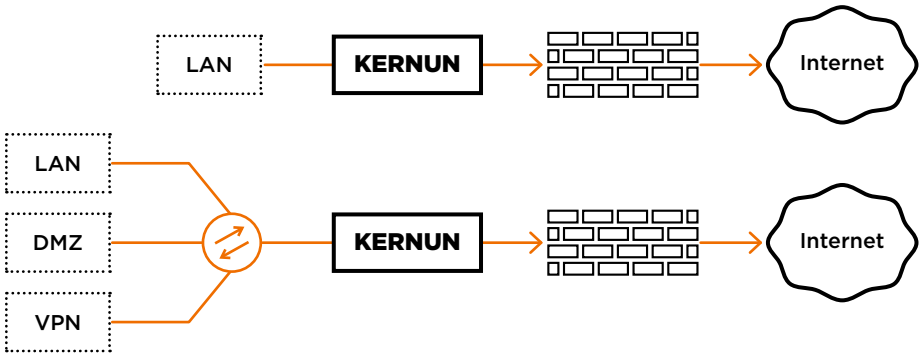


Webová proxy brána

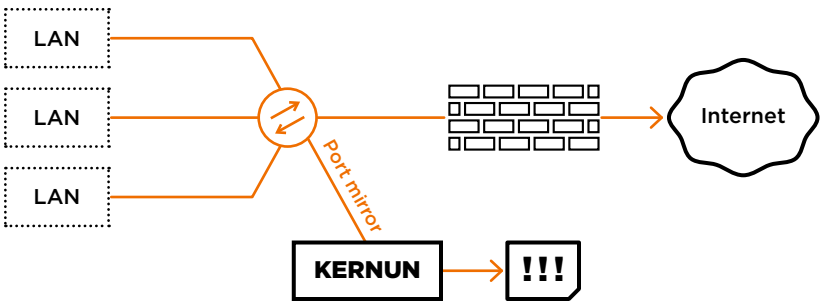
Zařízení je připojeno jako další stanice nebo server a poskytuje pro vnitřní síť službu přístupu na webové stránky internetu, tzv. HTTP proxy. Umožňuje filtrovat webový provoz, vyžadovat autentizaci uživatelů, provádět TLS inspekci, nebo zakazovat rizikové tunelování.

Transparentní firewall

Zařízení lze do sítě nasadit v režimu transparentní firewall, z technického pohledu jako síťový bridge, a to bez nutnosti změny topologie sítě. Veškerý provoz, který přes něj prochází, monitoruje, vyhledává v něm nebezpečné anomálie a ty blokuje.



* V režimu Transparentní firewall nelze využít bezpečnostní komponenty Webový filtr a VPN server. Stavový firewall lze využít omezeně.



Sonda

Jedná se o pasivní způsob zapojení do síťové infrastruktury. Zařízení je nainstalováno do sítě jako odposlechové zařízení, typicky na zrcadlený port (Port mirror). Pasivně přijímá kopii síťového provozu a provádí jeho analýzu. Nebezpečný provoz neblokuje, ale pouze reportuje nebo vyvolává jinou adekvátní reakci, např. poplach.

* V režimu Sonda nelze využít bezpečnostní komponenty Webový filtr, Stavový firewall a VPN server.