Juniper Networks SRX Firewalls

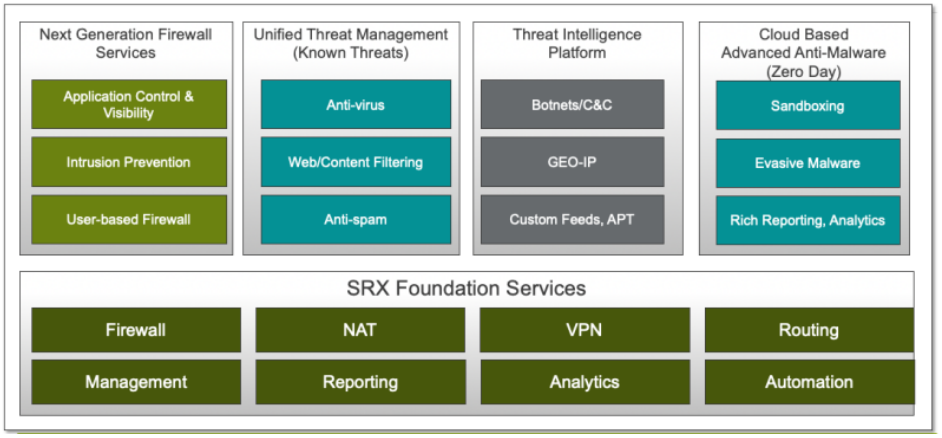
Silné zabezpečení kontroly přístupu, ověřování uživatele a ochrana před útokem na úrovni sítě i aplikace

Protože ohrožení sítě roste, jej stále častější a destruktivnější, k udržení životaschopnosti podniku je kriticky důležité odpovídající zabezpečení infrastruktury. Útoky přicházejí z několika zdrojů a v různých podobách. Podniky a poskytovatelé potřebují komplexní, spolehlivé a integrované bezpečnostní řešení opírající se o špičkové technologie ve svém oboru.

Bezpečnostní zařízení Juniper Networks® jsou speciálně navržena tak, aby zajišťovala všechny důležité funkce bezpečnosti sítě. Základ zařízení, která jsou optimalizována k maximálnímu výkonu a integraci funkcí, tvoří robustní síťový a bezpečnostní operační systém JUNOS® . Tento operační systém, navržený od základu tak, aby poskytoval vynikající síťové a bezpečnostní schopnosti

S širokou nabídkou specializovaných vysoce výkonných platforem, které poskytují integrovanou bezpečnost a LAN/WAN směrování prostřednictvím LAN/WAN rozhraní s vysokou hustotou, se integrovaná bezpečnostní zařízení Juniper Networks zaměřují na potřeby malých i středních podniků, ale také na velké korporace, poskytovatele služeb a velká datová centra. Tato integrovaná zařízení nabízejí ochranu sítě před všemi typy útoků a škodlivého softwaru, a současně zajišťují bezpečnou mezifiremní komunikaci (B2B).

JUNIPER SECURITY SERVICES OVERVIEW



Charakteristika produktové řady:

- Kompletní sada bezpečnostních funkcí UTM (Unified Threat Management) zahrnující stavový firewall, aplikační bezpečnost, prevenci proti průnikům antivirus

(vč. Anti-spyware, anti-adware, anti-phishing), antispam a filtrování webů zabraňuje průnikům spyware, trojských koní, malwaru a dalších nově se objevujících typů útoků.

- Centralizovaná správa založená na zásadách minimalizuje možnost, že dojde k přehlédnutí děr v zabezpečení a zjednodušuje rozšiřování sítě a aktualizaci na síťové vrstvě.

- Technologie virtualizace usnadňují správcům rozdělit síť do bezpečných segmentů a poskytuje tak další vyšší stupeň ochrany.

- Různé volby pro vysokou dostupnost nabízejí nejlepší redundantní schopnosti pro jakoukoliv danou síť.

SRX300

SRX320

SRX340

SRX345

odkaz na datasheet SRX3XX series

SRX4100

odkaz na datasheet SRX4x00 series

Obrana perimetru začíná ochranou na úrovní sítě

Pro ochranu proti útokům na síťové úrovní používají zařízení Juniper Networks metodu dynamického filtrování paketů známou jako důkladnou kontrolu, jež je schopna odhalit nežádoucí provoz v síti. Díky této metodě mohou firewally shromažďovat informace, která jsou obsažena v záhlaví paketů včetně zdrojových a cílových IP adres, zdrojových a cílových čísel portů a pořadových čísel paketů. Pokud dorazí paketová odpověď, firewall porovnává obrazce obsažené v jeho záhlaví se stavem související relace. Jestliže se údaje neshodují, firewall provede akci specifikovanou v bezpečnostní politice, což obvykle znamená, že je paket zahozen a akce se zaznamená do protokolu (logu).

Stavová inspekce poskytuje vyšší úroveň bezpečnosti než jiné technologie firewallů (například filtrování paketů), protože provoz se kontroluje v kontextu spojení a nikoliv jako soubor různých paketů. Ve výchozím stavu odmítá Juniper Networks firewall veškerý provoz ve všech směrech. Díky centralizované správě založené na zásadách pak mohou podniky vytvořit vlastní zásady zabezpečení, které definují parametry síťového provozu, který smí procházet ze specifikovaných zdrojů do specifikovaných cílů.

Bezpečné a spolehlivé spojení WAN také hraje důležitou roli při ochraně na úrovni sítě. Při zavedení robustních VPN sítí lze vzdálená místa bezpečně připojit k jiným vzdáleným místům a k centralizovaným datům a aplikacím za využití sdílených vysokorychlostních médií jako je Internet. Funkce jako je Auto Connect VPN, které jsou u vybraných modelů k dispozici, usnadňují administraci a správu sítí VPN, zejména v topologiích typu hub-and-spoke, a tak umožňují automaticky nastavovat bezpečná spojení bez nutnosti manuální konfigurace.

odkaz na datasheet SRX1500

Ochrana Day-Zero proti útokům na úrovni aplikaci

Za účelem blokování škodlivých útoků na úrovni aplikací lze využít technologii prevence proti průnikům na všech produktech SRX Juniper Networks. U centrálních pracovišť podniků, v prostředí datových center a v sítích servisních poskytovatelů s velkými objemy přenášených dat lze využívat pro ochranu na úrovni aplikací technologii IPS a řadu servisních SRX gateway Juniper Networks. Zařízení SRX mají v sobě integrován stejný software, který se nachází v zařízeních řady Juniper Networks MX (routery).

Bezkonkurenční výkon při zajišťování bezpečnosti a funkce segmentace sítě chrání kriticky důležité vysokorychlostní sítě proti průniku a šíření existujících i vznikajících hrozeb na úrovni aplikací. Pomocí několika mechanismů detekce útoků, včetně stavových podpisů a nástrojů detekce anomálií protokolu, provádí servisní gateweje řady SRX hloubkovou analýzu souborů (odeslaných přes internetový protokol http/https, případně emailovou komunikací), aplikačních protokolů, kontextu, stavu a chování. Kontrolu a analýzu provádí ve virtuálním sandboxu, kde sledují chování potencionálně nebezpečných souborů, čímž zajišťují ochranu proti Zero Day útokům.

Správci bezpečnosti sítě mohou implementovat funkce Juniper Network AppSecure, a tak blokovat útoky na úrovni aplikací dříve, než infikují síť a způsobí nějaké škody. Technologie AppSecure využívá pokročilé vysoce výkonné detekční mechanismy integrované do firewallu stavové inspekce a zároveň několik inspekčních enginů, které fungují paralelně, takže je zajištěno dokonalé odhalování i pokročilých odolných hrozeb, včetně takových, které se nalézají v aplikacích uvnitř dalších aplikací.

odkaz na datasheet SRX4600

Integrovaný antivirový program chrání vzdálená místa

Pro vzdálené kanceláře nebo menší pobočky, které mají omezený počet pracovníků IT, je u jakéhokoliv řešení bezpečnosti absolutní nutností integrace a jednoduchost. Juniper Networks v současnosti poskytuje integrovanou antivirovou ochranu na bázi souborů od Sophos a Avira v produktech SRX. Tyto produkty kombinují funkce firewallu a VPN s antivirovým skenovacím enginem, který zahrnuje anti-phishing, anti-spyware a anti-adware, a tak poskytují komplexní bezpečnostní řešení v jediném zařízení.
Tato integrovaná zařízení vyhledávají viry, které se šíří elektronickou poštou i webovým provozem, a to tak, že kontrolují protokoly IMAP, SMTP, FTP, POP3 a http/https. Poskytují nejpokročilejší ochranu před dnešními rychle se šířícími červy, viry, trojskými koni, spyware a dalším malware poškozujícím síť. Díky schopnosti dekomprimovat soubory používající běžné protokoly skenuje tento engine hloubkově přílohy a detekuje i hrozby skryté v několika úrovních komprese.

Řízení přístupu ke známým webovým stránkám obsahujícím malware a phishing

Zaměstnanci, kteří mají ze sítě společnosti přístup k nevhodným webovým stránkám, riskují, že do organizace pronikne škodlivý software. A co hůř, jejich chyby v úsudku mohou vystavit společnost hrozbě soudních sporů nedostatečné ochrany. Integrovaná bezpečnostní zařízení Juniper Networks jsou ideálním řešením, které pomáhá organizacím navrhnout a prosadit zásady odpovědného využívání webu.

Možné jsou dva přístupy: externí a integrované filtrování webu. Externí filtrování webu, které je k dispozici na všech zařízeních Juniper Networks firewall/VPN, provádí přesměrování síťového provozu ze zařízení na dedikovaný server filtrování webu Websense, kde se prosazují stanovené bezpečnostní zásady společnosti. Integrované filtrování webu, které je k dispozici na zařízeních Juniper Networks řady SRX (Service Gateway), umožňuje podnikům vytvořit vlastní zásady přístupu k webu na základě selektivního blokování přístupu k webům uvedeným v průběžně aktualizované databázi. Tato databáze, kterou udržuje společnost Websense, alianční partner společnosti Juniper Networks, obsahuje více než 20 milionů adres URL uspořádaných do více než několika stovek kategorií potenciálně problematického obsahu.
Zákazníci mohou rychle zavádět integrované nebo externí filtrování webu pomocí výchozí konfigurace založené na databázi Websense. Profily filtrování webu lze upravovat pomocí seznamů vylučujících použití stránek (black lists), seznamů povolujících využití stránek (white lists) a celé řady předdefinovaných a uživatelem definovaných kategorií.

Blokování příchozích spamů a útoků typu phishing

Společnost Juniper Networks úzce spolupracuje se společností Sophos a využívá její antispamové řešení, které má vynikající tržní pozici a podporu, pro menší a středně velké kancelářské platformy Juniper za účelem zbrždění záplavy nevyžádaných mailů a potenciálních útoků, které mohou tyto e-maily obsahovat. Antispamový engine, který je nainstalován na Juniper Networks FW/VPN gateway, filtruje příchozí e-maily odstraněním známých spamových a phishing uživatelů, a tak funguje jako první linie obrany. Když do sítě přijde známý škodlivý e-mail, je zablokován a/nebo označen, jako první linie obrany. Když do sítě přijde známý škodlivý e-mail, je zablokován a/nebo označen, tak aby poštovní server mohl podniknout příslušné kroky. Integrovaný antispam je k dispozici na všech zařízeních řady SRX pro pobočky.

Virtualizace zvyšuje úroveň zabezpečení rozdělením sítě do několika segmentů

Technologie virtualizace u integrovaných firewall/VPN a směrovacích bezpečnostních řešení Juniper Networks umožňuje uživatelům rozdělit síť do mnoha samostatných částí a řídit je všechny prostřednictvím jediného zařízení. Správci mohou jednoduše rozdělit provoz v síti určený pro různé účely nebo mohou rozdělit síť do samostatných bezpečných segmentů s vlastními firewally a vlastními zásadami zabezpečení.

Zařízení firewall/VPN podporují následující technologie virtualizace:

- **Bezpečnostní zóny – Security Zones:** Podporované všemi produkty. Bezpečnostní zóny představují virtuální části sítě segmentované do logických celků. Bezpečnostním zónám lze přiřadit fyzické rozhraní nebo v případě větších zařízení i virtuální systém. Je-li přiřazen virtuální systém, může několik zón sdílet jedno fyzické rozhraní, které snižuje náklady na pořízení a

- **Logical systems (LSYS):** Dostupné na zařízeních řady SRX. Výsledkem je několik nezávislých virtuálních prostředí, každé s vlastní množinou uživatelů, firewallů, VPN, bezpečnostními zásadami a správou. Správci mají možnost rychle segmentovat síť do několika bezpečných prostředí spravovaných jediným zařízením. Díky tomu umožňují logické systémy provozovatelům sítě vytvářet řešení pro řadu zákazníků s menším počtem fyzických firewallů a sníženým dohledem správců. Tím se snižují investiční i provozní náklady.

- Virtuální směrovače Virtual Router (VR): Podporované všemi produkty. Virtuální směrovače umožňují správcům rozdělit jedno zařízení tak, aby fungovalo jako několik fyzických směrovačů. Každý VR může podporovat vlastní domény a zaručovat, že nebude docházet k výměně informací s doménami zavedenými na jiných VR. Díky tomu může jediné zařízení podporovat více zákaznických prostředí a tím se snižují celkové náklady na pořízení a provoz.
- Virtuální sítě LAN (VLAN): Podporované na všech platformách. Jde o logické – nikoliv fyzické – rozdělení podsítí, které umožňují správcům identifikovat a segmentovat provoz již na L2. Bezpečnostní zásady mohou specifikovat, jak bude provoz směrován z jednotlivých sítí VLAN do bezpečnostních zón, virtuálních systémů nebo fyzických rozhraní. Díky tomu mohou správci snadno identifikovat a organizovat provoz z několika oddělení a definovat, které zdroje mají být přístupné jednotlivým uživatelům.

Komplexní řešení s vysokou dostupností zaručují velkou provozuschopnost

Bezpečnostní systém je dobrý jen v případě, že je spolehlivý a provozuschopný. Řešení bezpečnosti od Juniper Networks zahrnují spolehlivé a vysoce dostupné systémy založené na protokolu Juniper Services Redundancy Protocol (JSRP) u produktů na bázi operačního systému JUNOS. Firewally, VPN tunely a IPS toky lze vzájemně synchronizovat, takže v případě výpadku či selhání jednoho zařízení nedojde ke kolapsu celé sítě. Mezi možnosti konfigurace patří:

- Aktivní/pasivní: Hlavní (master) zařízení sdílí informace o síti, její nastavení, vlastní konfigurace a informace o aktuální relaci se záložním zařízením, takže v případě selhání může záložní zařízení hladce převzít funkci.

- Aktivní/aktivní: Obě zařízení jsou konfigurována tak, aby byla aktivní, data v síti proudí oběma. Pokud by některé zařízení selhalo, druhé zařízení se stane hlavním (master) a pokračuje v řízení veškerého provozu. Redundantní fyzické cesty zaručují maximální pružnost a provozuschopnost.

Snadná integrace zařízení

Dnešní LAN/WAN sítě nejsou nikdy statické. Stále se objevují potenciálně nákladné a časově náročné změny a doplňky. Jestliže se změní topologie sítě nebo jsou do sítě přidány nové kanceláře, obchodní partneři nebo zákazníci, je otázka schopnosti síťových systémů spolupracovat mimořádně důležitá. Ke zjednodušení síťové integrace a minimalizaci administrativního úsilí v případě požadovaných změn mohou integrovaná řešení zabezpečení společnosti Juniper Network pracovat ve třech různých režimech:

- Transparentní režim nabízí nejsnadnější způsob zvýšení bezpečnosti sítě.
V transparentním režimu mohou organizace využívat integrovaná zařízení firewall/VPN od Juniper Networks bez jakýchkoliv změn v síti: firewall, VPN, IPS a funkce omezující útoky DoS pracují bez IP adresy a zařízení je díky tomu pro uživatele „neviditelné“.
- Režim směrování umožňuje bezpečnostnímu zařízení účastnit se aktivně ve směrování v síti za podpory statických a dynamických protokolů směrování včetně BGP, OSPF, RIPv1, RIPv2 a ECMP. Režim směrování umožňuje správcům rychle zavádět strukturované řešení zabezpečení s minimem ruční konfigurace.

- Režim NAT automaticky překládá IP adresy nebo skupiny IP adres na jednu adresu a skrývá soukromé adresy organizací před pohledem z vnějšku.

Integrované bezpečnostní systémy Juniper Networks podporují statické i dynamické přidělování adres DGCP nebo PPPoE, což umožňuje nasazení Juniper Networks řešení v jakémkoli síťovém prostředí.

Neomezená škálovatelnost

Jak se rozvíjejí požadavky sítě, zvyšují se i požadavky na výkon a na I/O možnosti různých síťových zařízení. Pro uspokojení stále se měnících a rostoucích síťových požadavků využívá řada servisních gatewejí SRX5000 architekturu dynamických služeb (DSA).

Architektura DSA (Dynamic Services Architecture) umožňuje vytvářet flexibilní konfigurace, co se týče I/O a výkonu zpracování, neboť stejný slot lze používat jak pro kartu servisního procesoru tak pro kartu I/O, takže high-end servisní gateweje SRX lze nakonfigurovat buď jako řešení pro intenzivní výkon nebo řešení pro intenzivní I/O, nebo kdekoliv mezi tím. U řady SRX5000 lze výkon škálovat téměř lineárně pomocí přídavných síťových a servisních karet, a to s velmi malými režijními náklady. Tato rozsáhlá škálovatelnost v oblasti I/O a výkonu zpracování, kterou poskytuje architektura DSA od Juniper Network, je k dispozici pouze u servisních gatewejí řady SRX třídy datových center.

Efektivní správa sítě a bezpečnosti pomocí centrálního managementu

Na rozdíl od řešení, která vyžadují, aby administrátoři sítě používali při řízení jednoho zařízení více správních nástrojů, umožňuje produkt Junos Space Platform oddělením IT řídit zařízení po celou dobu jeho životního cyklu prostřednictvím jediného centralizovaného ovládacího panelu. Tento správní nástroj je určen specificky k podpoře týmové práce mezi techniky IT, síťovými administrátory a správci bezpečnosti.

Produkt Junos Space Security Director využívá nový přístup ke správě bezpečnosti. Poskytuje oddělením IT snadno použitelné řešení, které kontroluje všechny aspekty zařízení firewall/VPN včetně konfigurace zařízení, síťových nastavení a pravidel bezpečnosti. Pomocí tohoto produktu/aplikace lze z jednoho místa spravovat a konfigurovat SRX firewall z grafického rozhraní, včetně nastavení všech advance bezpečnostních funkcí (AppSecure, IPS, Sandboxing, UTM).

Produkt/aplikace Juniper Networks Log Collector poskytuje možnost sběru logů a následného reportingu zjištěných informací. Volbou vhodných management nástrojů mohou síťoví administrátoři docílit efektivní implementace, správy a řešení problémů u rozsáhlých síťových instalací.

SRX5400
Services Gateway

SRX5600
Services Gateway

SRX5800
Services Gateway

odkaz na SRX5x00 series

Pokročilé nástroje řady Juniper Networks **JSA (Juniper Secure Analytics)** poskytují funkce SIEM (Security Information and Event Management) pro řízení informací o bezpečnosti a řízení událostí, včetně pokročilého monitorování zařízení různých dodavatelů, korelace událostí a sofistikovaného řízení protokolů (logů).

K rychlému zavedení s nízkými náklady zasílejte zařízení – neposílejte správce

Aby nevznikaly vysoké náklady na dopravu správců, aby nakonfigurovali systémy na vzdálených pracovištích, zařízení Juniper Networks lze nainstalovat na vzdálených místech, kde nejsou techničtí uživatelé. S funkcemi ZTP (Zero touch provisioning) lze vzdáleně nastavit dané zařízení a poté spravovat.

Na vzdáleném pracovišti je třeba nové zařízení pouze připojit kabely a načíst malý konfigurační soubor, který do místa instalace zašle správce elektronickou poštou nebo na USB disku. Počáteční konfigurační soubor naváže zabezpečené spojení se správcem, který poté zašle novému zařízení kompletní konfigurační soubory.

O společnosti Juniper Networks

Juniper Networks, Inc. je vedoucí společnost na trhu vysoce výkonných sítí. Zákazníkům nabízí vysoce výkonnou síťovou infrastrukturu, která vytváří zabezpečené prostředí pro urychlené nasazení služeb a aplikací v síti, což podporuje podnikatelské aktivity náročné na vysoký výkon. Další informace můžete najít na stránkách www.juniper.net.

Kontakty
Juniper Networks, Inc. | **www.juniper.net**
Arrow ECS, a.s. |28. října 3390/111a | 702 00 Moravská Ostrava | Tel: 587 488 811 | **www.arrow.com/ecs/cz**