# Bezpieczeństwo sieciowe z Juniper Networks

Przemysław Krzywiec

Sales Support Engineer

Przemyslaw.Krzywiec@ingrammicro.com

tel. 601-536-379

23-24.09.25, v.1

# SRX Firewalls Hardware

Juniper Networks | Driven by Experience™

# JUNIPER SRX SERIES PORTFOLIO

## Branch

SRX300

SRX320

SRX340

SRX345

SRX380

## Campus & Scale-Out DC/Cloud/SP

SRX1500

SRX4100

SRX4200

SRX4600


SRX1600


SRX2300


SRX4300


SRX4700

## Scale-Up DC/Cloud/SP

SRX5800

SRX5600

SRX5400

## Cloud Firewalls

vSRX

cSRX

Secure Edge


Cyberratings
"**AAA**" **Rating**


Secure Edge
"**2022 Product of the Year**" by CRN

Gartner

Enterprise Firewall Magic Quadrant
**CHALLENGERS**


3-time Cybersecurity **Channel Champions** by Canalys

# SRX Quick Reference











| | SRX300 | SRX320 | SRX320-POE | SRX340 | SRX345 | SRX345-2AC | SRX380 | SRX1500 | SRX4100 | SRX4200 | SRX4600 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| On-board Ports | 8xGbE | 8xGbE | 8xGbE | 16xGbE | 16xGbE | 16xGbE | 16x1GbE + 4x10GbE | 16x1GE + 4x10GbE | 8x10GbE | 8x10GbE | 8x10GbE+ 4x40GbE/ 100GbE |
| DSL/LTE cards | 0 | 2xMPIMs | 2xMPIMs | 4xMPIMs | 4xMPIMs | 4xMPIMs | 4xMPIMs | 0 | 0 | 0 | 0 |
| Stateless* | 800 Mbps | 820 Mbps | 820 Mbps | 1.6 Gbps | 2.3 Gbps | 2.3 Gbps | 5 Gbps | 5 Gbps | 28 Gbps | 57 Gbps | 92 Gbps |
| Stateful* | 500 Mbps | 500 Mbps | 500 Mbps | 1 Gbps | 1.5 Gbps | 1.5 Gbps | 4 Gbps | 5 Gbps | 20 Gbps | 40 Gbps | 71 Gbps |
| IPSec VPN* | 150 Mbps | 150 Mbps | 150 Mbps | 250 Mbps | 330 Mbps | 330 Mbps | 1 Gbps | 1.3 Gbps | 5 Gbps | 9.6 Gbps | 16 Gbps |
| Dual PSU | N/A | N/A | N/A | N/A | N/A | YES | YES | YES | YES | YES | YES |
| Max PoE Ports | 0 | 0 | 6 | 0 | 0 | 0 | 16 | 0 | 0 | 0 | 0 |

**Stateless = Routing = Packet mode**
**Stateless**: urządzenie nie śledzi stanu połączenia — każdy pakiet jest przetwarzany niezależnie.
**Routing**: klasyczny tryb pracy routera — decyzje są podejmowane na podstawie nagłówków pakietów (np. adresów IP).
**Packet mode**: inna nazwa dla tego podejścia — pakiety są analizowane osobno, bez kontekstu „flowów".
**Zalety**: szybsze przetwarzanie, mniejsze obciążenie CPU
**Wady**: brak możliwości kontroli stanu połączeń (np. dla zapory sieciowej)

**Stateful = Firewall = Flow mode**
**Stateful: u**rządzenie śledzi stan połączenia — np. które pakiety są częścią tej samej sesji.
**Firewall**: tryb ten umożliwia kontrolę i filtrowanie połączeń na poziomie sesji (np. TCP handshake).
**Flow mode**: pakiety są przypisywane do przepływów (flows) i przetwarzane jako część kontekstu.
**Zalety**: lepsze bezpieczeństwo, kontrola
**Wady**: większe zużycie zasobów, niższa wydajność niż w packet mode

# NEW ADDITIONS TO THE SRX SERIES FAMILY

## Compact, High-performance fixed form-factor firewall appliances


**SRX1600**

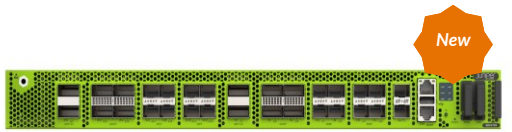
9G FW
7.5G NGFW
5G IPsec


**SRX2300**

25G FW
15G NGFW
12G IPsec


**SRX4300**

50G FW
45G NGFW
30G IPsec




**SRX4700**

1.4T FW
110G NGFW
90G IPsec PMI

### High-Performance

- FW IMIX: 9Gbps to 1.4Tbps
- Industry highest security efficacy
- 400GE interface support

### Built-in Zero Trust

- Supply chain security
- TPM 2.0 w/ cryptographically signed Device ID
- Tamper-proof
- Wirespeed MACsec

### EVPN-VXLAN

- No need to break the tunnel and simpler config
- Better Together: Juniper Security Director Cloud & NSX-T & Apstra

### AI-Predictive Threat Prevention

- AI-generated custom signatures
- Line-rate anti-malware performance
- More customizable URL filtering

# SRX1600 (SPECTRE)
## FIXED ENTRY SCALE FIREWALL FOR LARGE BRANCH OR ENTERPRISE EDGE


### Use Cases
- Enterprise edge FW
- DC edge FW
- Roaming FW
- SD-WAN secure branch

### Modular Interfaces
- 16x 1G-T (Cu)
- 4x 1/10G (SFP+)
- 2x 1/10/25G (SFP28)
- 2 Dedicated HA Control Ports (SFP)
- Dedicated OOB Mgmt (1xGE)
- MACsec supported on SFP ports

### Storage & Dimensions
- 1x 100G SSD
- Dual Power Supply (AC / DC)
- Size: 1RU
- Front to Back Airflow
- FIPS 140-3, CC

### Projected Performance
- Firewall (IMIX) : 8G
- NGFW 7.5G
- IPsec VPN (IMIX) : 5G
- **IPS Recommended :** 8G
- NAT (IMIX) : 8G

# SRX2300 (MOONRAKER)
## FIXED LOW PERFORMANCE FIREWALL FOR LARGE BRANCH OR ENTERPRISE EDGE

## Use Cases

- Enterprise edge FW
- DC edge FW
- Roaming FW
- SD-WAN secure branch
- SD-WAN secure hub

## Modular Interfaces

- 8x 1/10G-T (Cu)
- 8x 1/10G (SFP+)
- **4x 1/10/25G (SFP28)**
- 2x 40/100G (QSFP28)
- 2 Dedicated HA Control Ports (SFP)
- Dedicated OOB Mgmt (1xGE)
- **MACsec supported**

## Storage & Dimensions

- **1x 100G SSD**
- **1x 200G SSD**
- Dual Power Supply (AC / DC)
- Size: 1RU
- Front to Back Airflow
- **FIPS 140-3, CC**

## Projected Performance

| | |
|---|---|
| Firewall (IMIX) : | 25G |
| NGFW : | 15G |
| IPsec VPN (IMIX) : | 12G |
| **IPS Recommended :** | 15G |
| NAT (IMIX) : | 25G |

# SRX4300 (SKYFALL)
## FIXED MEDIUM PERFORMANCE FIREWALL FOR ENTERPRISE DATA CENTER

## Use Cases

- Enterprise Edge FW
- Enterprise Core FW
- DC edge FW
- DC core FW
- Roaming FW
- SD-WAN secure hub

## Modular Interfaces

- 8x 1/10G-T (Cu)
- 8x 1/10G (SFP+)
- 4x 1/10/25G (SFP28)
- 6x 40/100 G (QSFP28)
- 2 Dedicated HA Control Ports (SFP)
- Dedicated OOB Mgmt (1xGE)
- **MACsec supported**

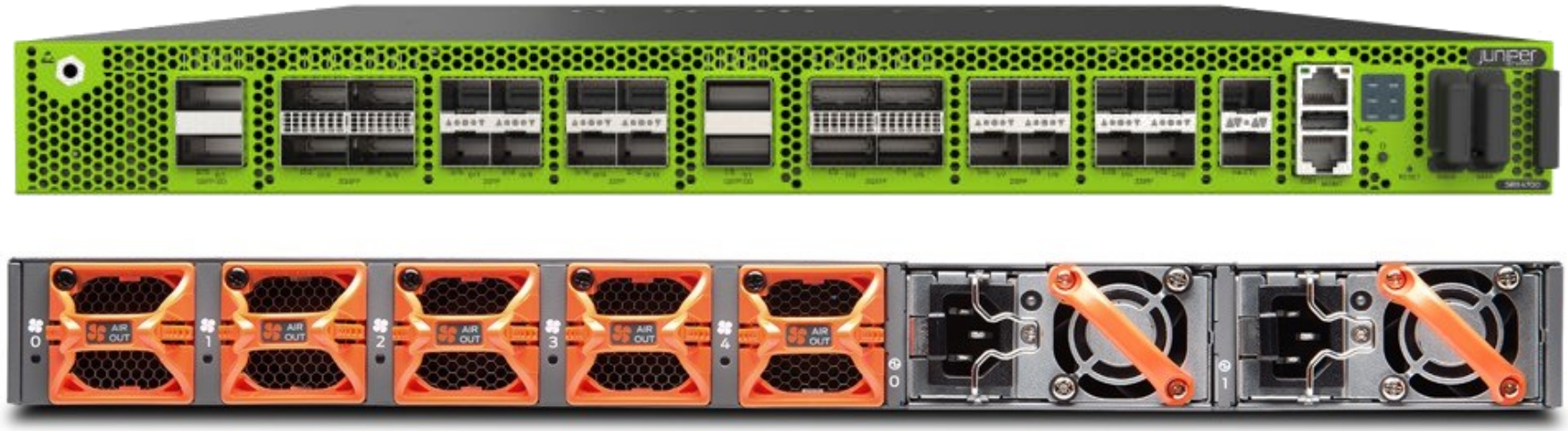
## Storage & Dimensions

- 1x 100G SSD
- 1x 1TB SSD
- Dual Power Supply (AC / DC)
- Size: 1RU
- Front to Back Airflow
- **FIPS 140-3, CC**

## Projected Performance

| | |
|---|---|
| Firewall (IMIX) : | 50G |
| NGFW : | 45G |
| IPsec VPN (IMIX) : | 30G |
| **IPS Recommended :** | 45G |
| NAT (IMIX) : | 50G |

# SRX4700 (CASINO ROYALE)
## FIXED HIGH-PERFORMANCE FIREWALL FOR DATA CENTER EDGE AND CORE



## Use Cases

- Enterprise Edge FW
- Enterprise Core FW
- DC edge FW
- DC core FW
- **Security Gateway** New
- CGNAT / Gi/N6 firewall
- Roaming FW
- SD-WAN secure hub

## Interface options

- 4 configurable modes:
  - 2x400G + 4x100G + 4x50G OR
  - 2x400G + 2x100G + 8x50G OR
  - 12x100G + 4x50G (SFP56) OR
  - 6x100G + 16x50G (SFP56)
- Dedicated OOB Mgmt (1G)
- MACsec on all ports

## Storage & Dimensions

- 2x 1TB or 2x 2TB SSD
- Dual Power Supply (AC / DC)
- Size: 1RU
- Front to Back Airflow
- FIPS 140-3, CC

## Projected Performance

- Firewall (IMIX) : 800G
- IPsec VPN (IMIX) : 90G
- IPS Recommended : 150G
- NAT (IMIX) : 150G
- NGFW : 110G

# Junos Security Feature Comparison

| | JSB / JB | JSE / JE |
|---|---|---|
| Management (CLI, JWEB, SNMP) and Automation | ● | ● |
| L2 Switching, LACP, L2TM & Secure Wire | ● | ● |
| Routing, Multicast Protocols, Virtual Router, PBR | ● | ● |
| Packet Mode & Overlay (GRE, IP-IP) | ● | ● |
| Network Services (DHCP, Jflow, QOS, BFD, RPM) | ● | ● |
| Stateful Firewall, Screen, NAT, ALG, UserFW, SSL FP | ● | ● |
| IPSec VPN (Site-Site, Auto, AD, Group) | ● | ● |
| Remote Access VPN | L | L |
| Chassis Cluster, VRRP, ISSU / ICU | ● | ● |
| MPLS, LDP, RSVP, L3 VPN, pseudo-wires, VPLS | ● | ● |
| Application Security (AppID, AppFW, AppQOS, AppRoute) | | ● |

L = per user license based (2 user free licenses included in JB or JE packages)

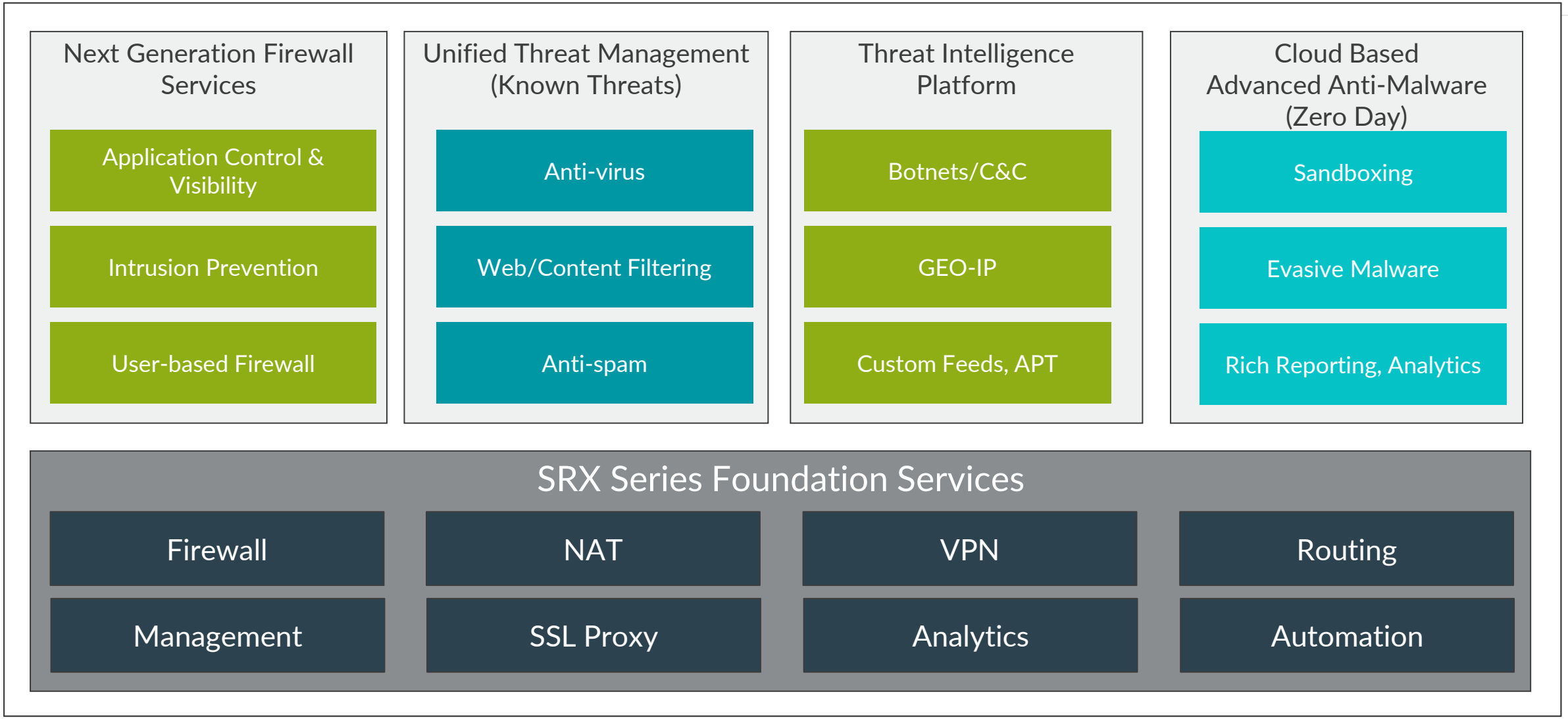
# Junos Security Feature

Juniper Networks | Driven by Experience™

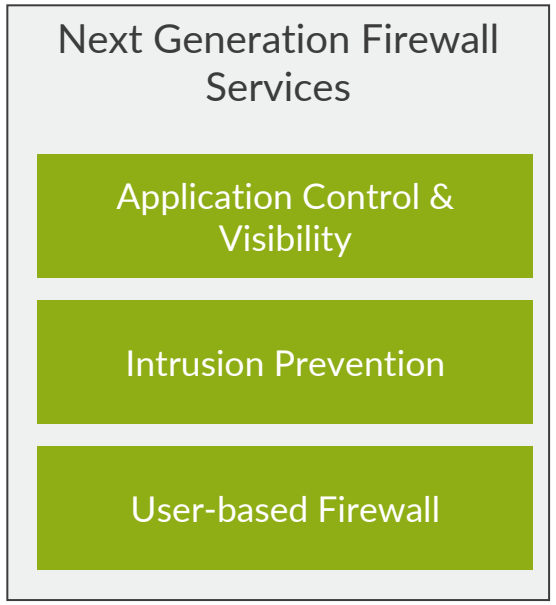
# JUNIPER CONNECTED SECURITY

## Network must take an active role in securing itself

# JUNIPER SECURITY SERVICES OVERVIEW



# JUNIPER SECURITY SERVICES OVERVIEW

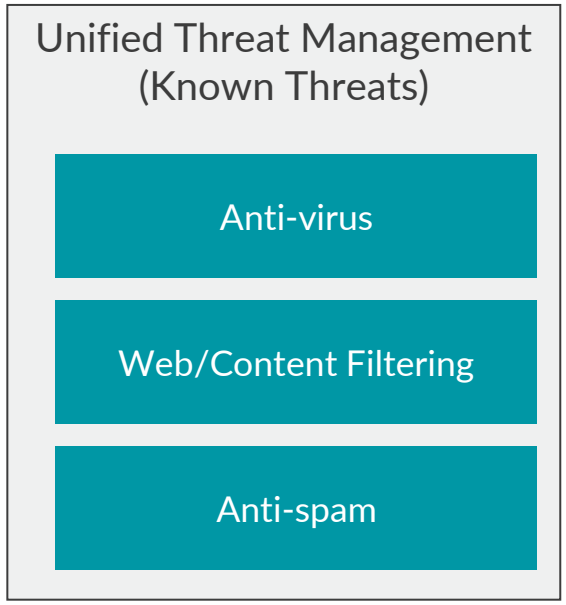



**Application Control & Visibility** – kontrola i widoczność aplikacji, czyli możliwość identyfikowania, monitorowania i zarządzania ruchem aplikacyjnym w sieci.

**Intrusion Prevention** – zapobieganie włamaniom, czyli wykrywanie i blokowanie podejrzanych działań oraz znanych zagrożeń w czasie rzeczywistym.

**User-based Firewall** – zapora oparta na użytkownikach, czyli możliwość stosowania polityk bezpieczeństwa w oparciu o tożsamość użytkownika, a nie tylko adres IP.

# JUNIPER SECURITY SERVICES OVERVIEW



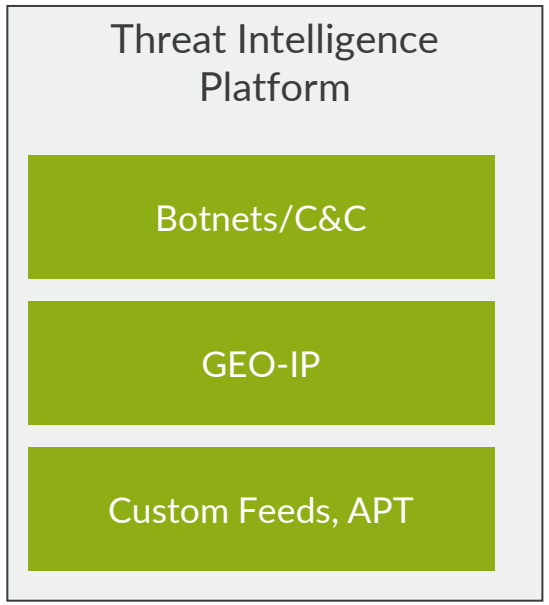

**Unified Threat** Management skupia się na zabezpieczeniach przed zagrożeniami, które są już znane i sklasyfikowane.

**Anti-virus** – ochrona przed znanym złośliwym oprogramowaniem, wykrywanie i usuwanie wirusów, trojanów, robaków itp.

**Web/Content Filtering** – filtrowanie treści internetowych, blokowanie dostępu do niebezpiecznych lub niepożądanych stron oraz kontrola nad tym, jakie treści mogą być przeglądane.

**Anti-spam** – ochrona przed niechcianą pocztą elektroniczną, wykrywanie i blokowanie wiadomości spamowych oraz potencjalnie złośliwych e-maili.

# JUNIPER SECURITY SERVICES OVERVIEW



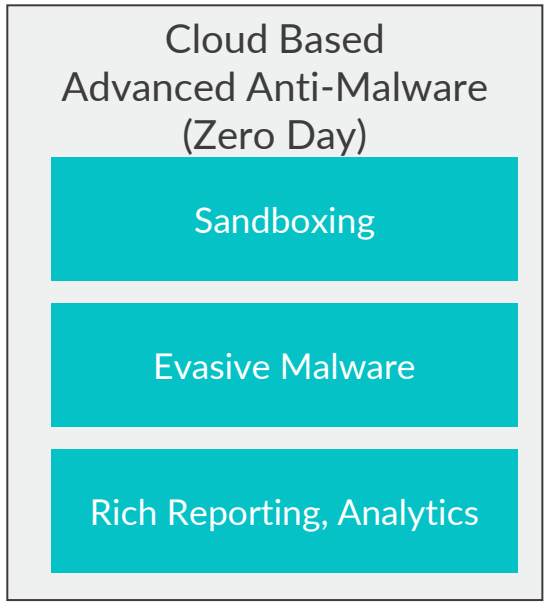

**Threat Intelligence** integruje różnorodne źródła informacji, aby umożliwić skuteczne wykrywanie i reagowanie na zagrożenia.

**Botnets/C&C** – informacje o botnetach i serwerach Command & Control, które są wykorzystywane przez cyberprzestępców do zdalnego sterowania zainfekowanymi urządzeniami.

**GEO-IP** – dane geolokalizacyjne adresów IP, umożliwiające identyfikację lokalizacji źródła zagrożenia lub podejrzanego ruchu.

**Custom Feeds, APT** – niestandardowe źródła danych oraz informacje o zaawansowanych trwałych zagrożeniach (Advanced Persistent Threats), które są dostosowane do specyficznych potrzeb organizacji.

# JUNIPER SECURITY SERVICES OVERVIEW




**Cloud Based Advanced Anti-Malware (Zero Day) to** kluczowe elementy nowoczesnych rozwiązań antymalware działających w chmurze, skoncentrowanych na zagrożeniach typu Zero Day. Rozwiązania chmurowe mogą skutecznie chronić przed nowymi, nieznanymi wcześniej zagrożeniami.

**Sandboxing** – technika izolowania i uruchamiania podejrzanych plików w kontrolowanym środowisku, aby bezpiecznie obserwować ich zachowanie i wykrywać złośliwe działania.

**Evasive Malware** – wykrywanie złośliwego oprogramowania, które próbuje ukryć się przed tradycyjnymi mechanizmami bezpieczeństwa, np. poprzez szyfrowanie, polimorfizm czy wykrywanie środowisk testowych.

**Rich Reporting, Analytics** – zaawansowane raportowanie i analityka, które dostarczają szczegółowych informacji o zagrożeniach, ich źródłach, sposobie działania i potencjalnym wpływie.

# AI-PREDICTIVE THREAT PREVENTION

## Speed and Security. No Need to Compromise.

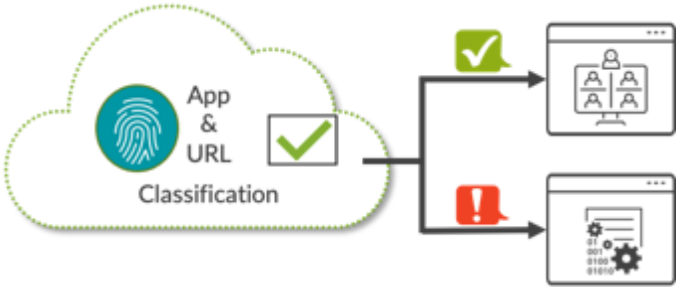
### AI-generated custom signatures

Automatyczne tworzenie sygnatur dostosowanych do specyfiki środowiska klienta.

### Even more effective malware prevention at line rate

Architektura bez proxy wspierana przez sztuczną inteligencję umożliwia wykrywanie zagrożeń już na podstawie pierwszych pakietów, bez potrzeby analizy całego pliku.

### Even more customizable web filtering




Skuteczna ochrona przed atakami sieciowymi oraz rozszerzona kontrola dzięki klasyfikacji w ponad 200 kategoriach.

# SECURITY INTELLIGENCE (SECINTEL) REVIEW


**Korzyści:**
Odciążenie zespołów bezpieczeństwa – mogą skupić się na analizie zagrożeń nieznanych, zamiast reagować na znane.

Zwiększenie skuteczności ochrony – według raportu CyberRatings.org, Juniper osiągnął **99,7% skuteczności blokowania exploitów** przy zerowej liczbie fałszywych alarmów.

**Główne cechy Juniper SecIntel:**

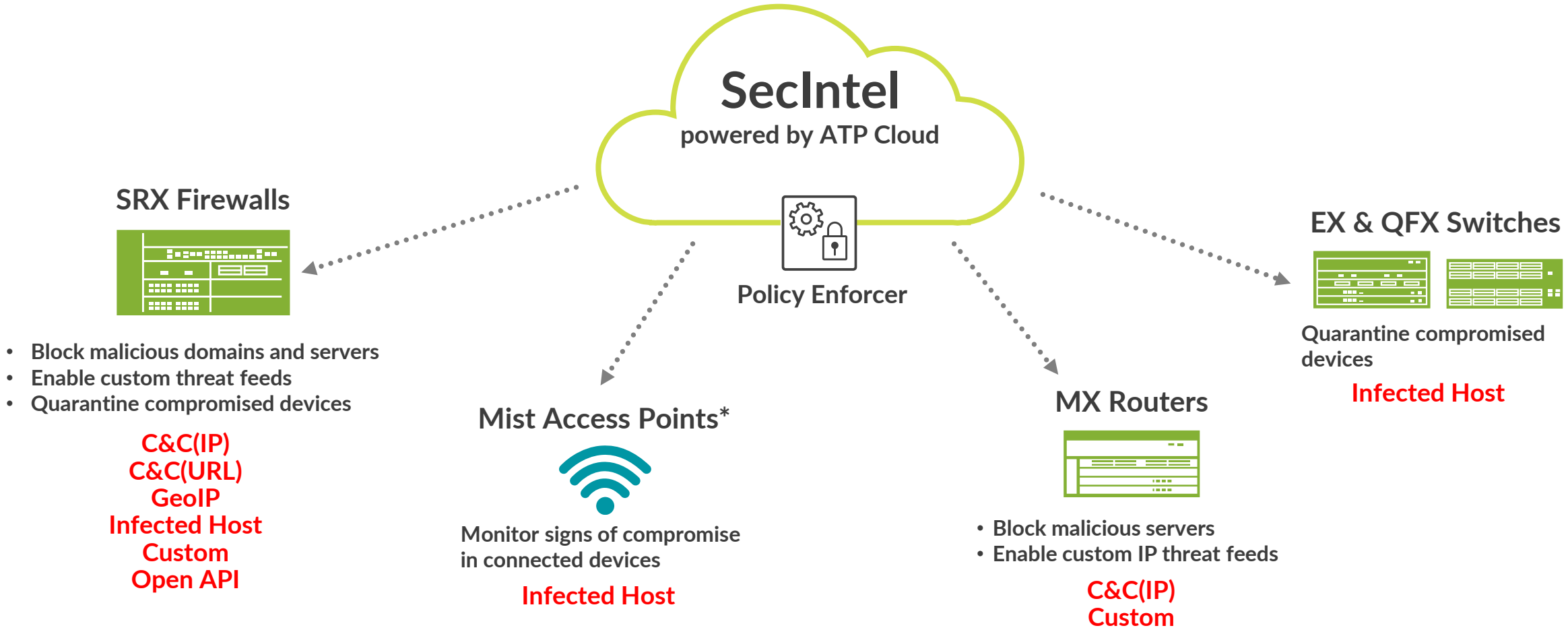
**Zautomatyzowane wykrywanie i blokowanie** zagrożeń w czasie rzeczywistym. Wsparcie dla urządzeń Juniper (np. zapór SRX, routerów MX, przełączników EX/QFX, punktów dostępowych) danymi o:

- złośliwych adresach IP,
- podejrzanych URL-ach,
- haszach certyfikatów,
- domenach wykorzystywanych przez cyberprzestępców.

**Integracja z zewnętrznymi źródłami danych** – umożliwia dodawanie niestandardowych feedów, np. branżowych lub specyficznych dla klienta.

**Współpraca z systemami SIEM** – dane o zagrożeniach mogą być przekazywane do Juniper Secure Analytics lub innych systemów zarządzania logami.

# SECURITY INTELLIGENCE (SECINTEL) REVIEW



# ENCRYPTED TRAFFIC ANALYSIS

## Looking for threats without breaking encryption

**Encrypted Traffic Analysis** ma na celu odzyskanie części widoczności utraconej wskutek szyfrowania, bez konieczności obciążającego procesu odszyfrowywania ruchu. Zbiera istotne dane o połączeniach SSL/TLS z urządzenia SRX, w tym:

- używane certyfikaty,
- negocjowane zestawy szyfrów (cipher suites),
- czas i częstotliwość połączeń.

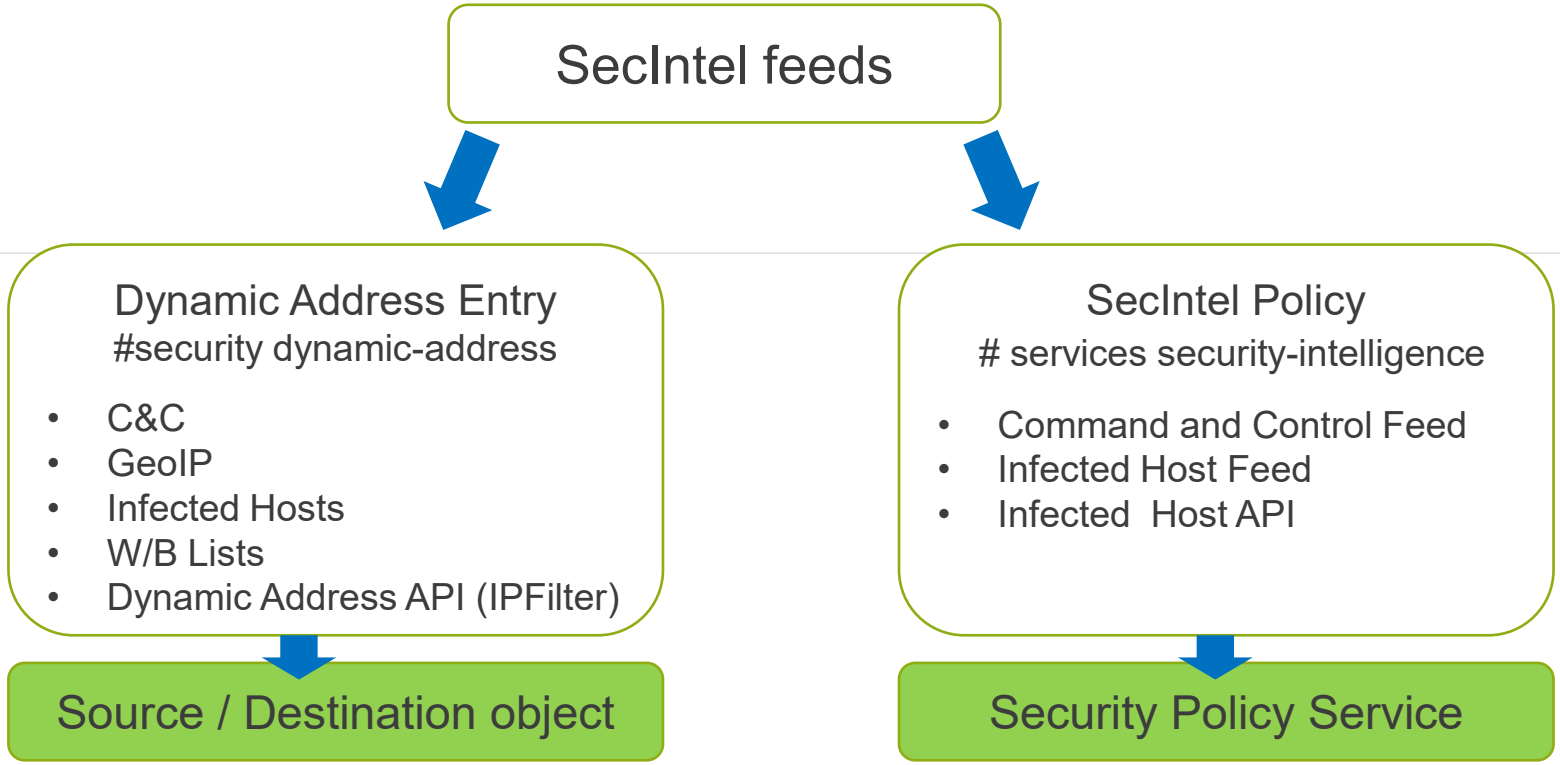
Wykorzystuje analizę zachowań sieciowych oraz uczenie maszynowe w chmurze ATP Cloud, aby określić, czy dane połączenie jest **bezpieczne (benign)** czy **złośliwe (malicious)**.


### Metadata

- Znane złośliwe certyfikaty
- Szczegóły połączenia podczas uzgadniania SSL (SSL handshake)

### Connection Patterns

- Połączenia na sekundę
- Zachowanie typu beaconing (czyli regularne, powtarzalne próby komunikacji z serwerem – często spotykane w przypadku złośliwego oprogramowania lub botnetów)




**Dynamic Address Entry:**
Ta część odpowiada za tworzenie dynamicznych obiektów adresowych na podstawie danych z feedów SecIntel:

#security dynamic-address – konfiguracja dynamicznych adresów w systemie.
C&C – adresy serwerów Command & Control (sterujących botnetami).
GeoIP – lokalizacje geograficzne adresów IP.
Infected Hosts – adresy zainfekowanych urządzeń.
W/B Lists – listy dozwolonych (white) i zablokowanych (black) adresów.
Dynamic Address API (IPFilter) – interfejs API do filtrowania adresów IP.

Wszystkie te dane trafiają do obiektu **Source / Destination**, który może być używany w politykach bezpieczeństwa.

**SecIntel Policy:**
Ta część odpowiada za wykorzystanie danych wywiadowczych w politykach bezpieczeństwa:

#services security-intelligence – konfiguracja usług inteligencji bezpieczeństwa.
Command and Control Feed – feed z adresami C&C.
Infected Host Feed – feed z adresami zainfekowanych hostów.
Infected Host API – API do integracji danych o zainfekowanych urządzeniach.

Te dane są wykorzystywane przez **komponent Security Policy Service**, który egzekwuje zasady bezpieczeństwa.

# THIRD PARTY FEED (IP ONLY)


## Obsługa filtrowania adresów IP dla Office 365:

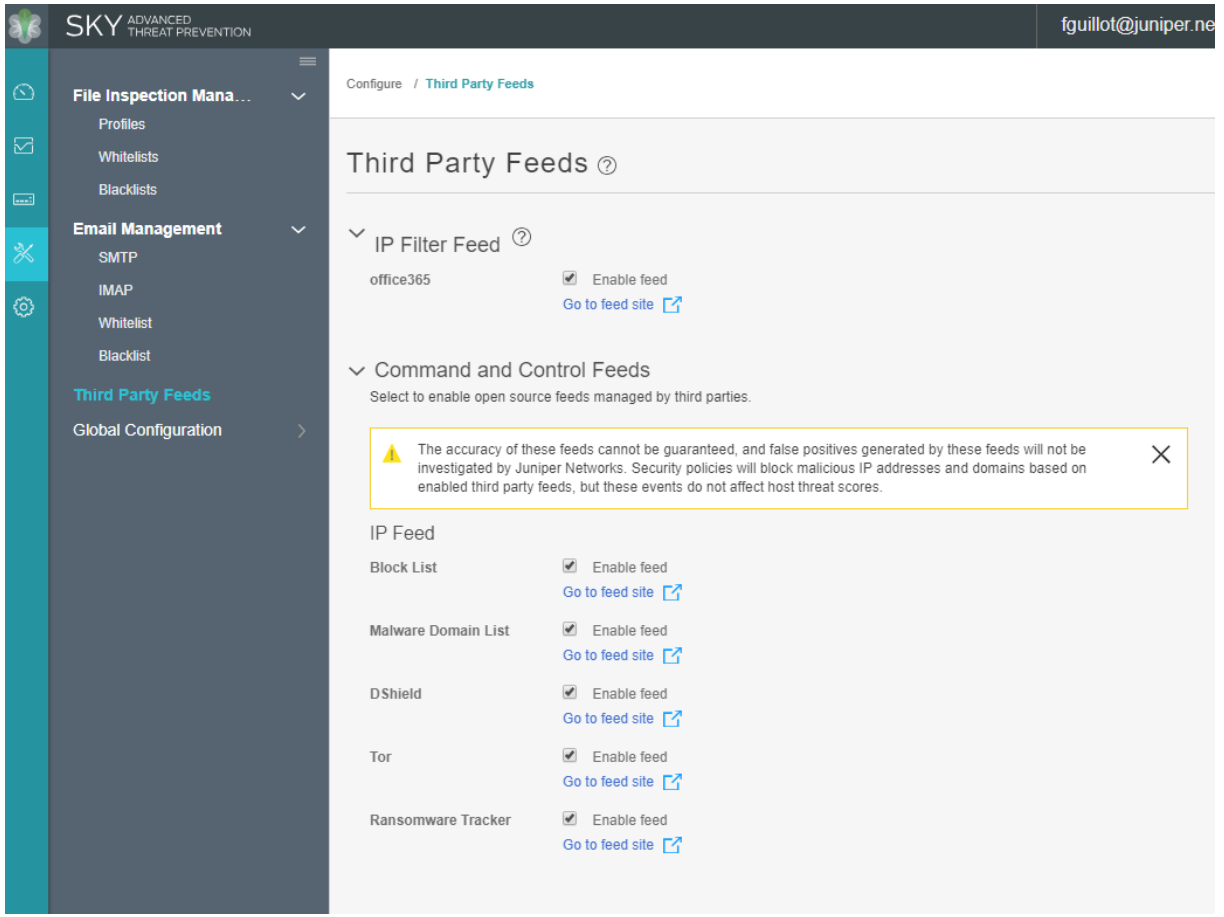
- **Filtrowanie ruchu** – system może analizować połączenia do/z adresów IP używanych przez O365 i np. zezwalać na nie, blokować lub monitorować.
- **Unikanie fałszywych alarmów** – dzięki znajomości adresów O365, system nie oznaczy ich błędnie jako złośliwe.
- **Lepsza kontrola dostępu** – administratorzy mogą tworzyć reguły bezpieczeństwa, które np. zezwalają tylko na dostęp do O365 z określonych lokalizacji lub urządzeń.

To szczególnie ważne w środowiskach korporacyjnych, gdzie O365 jest intensywnie wykorzystywany, a jednocześnie trzeba zachować wysoki poziom bezpieczeństwa.

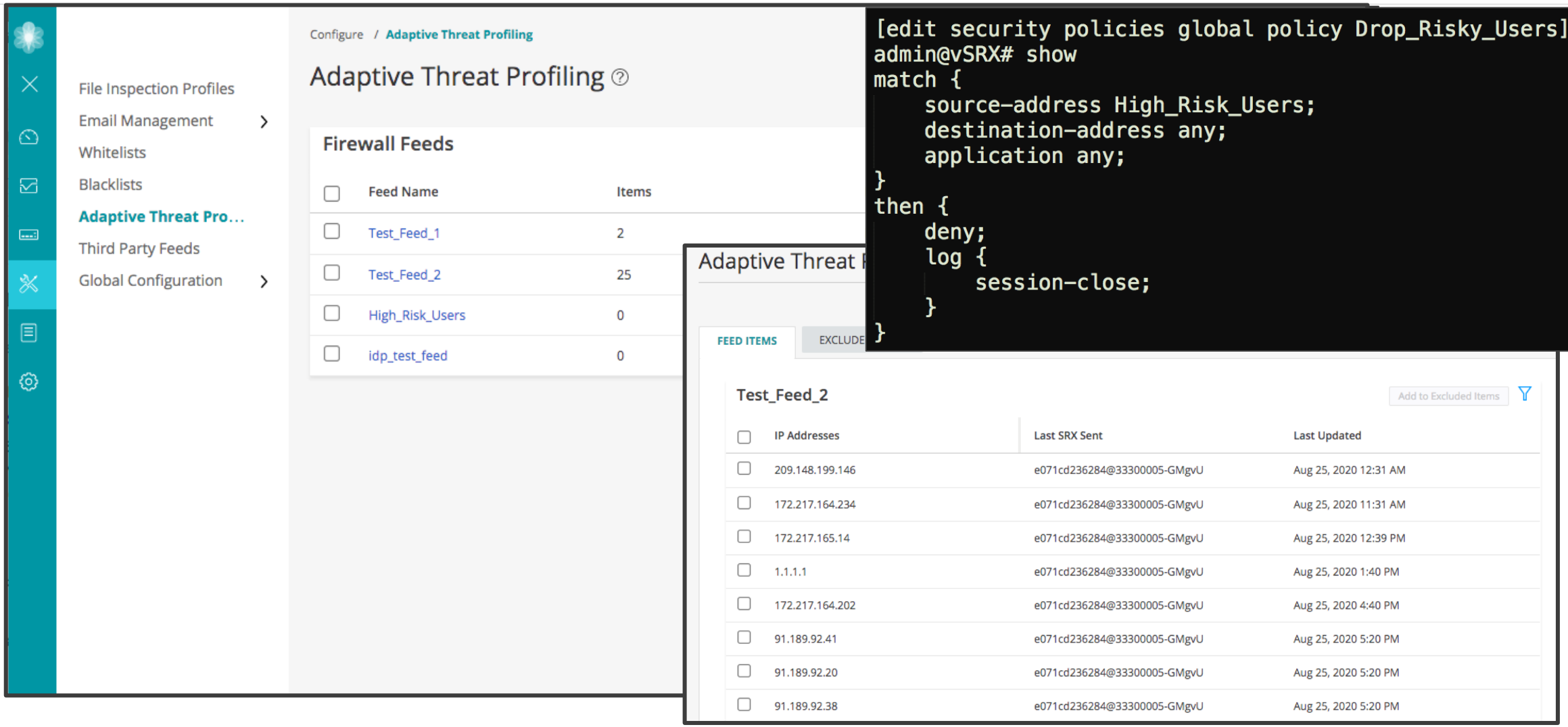
## Źródeł zagrożeń (threat feeds):

- **Blocklist.de** – specjalista ds. oszustw i nadużyć
- **Malware Domain List** – lista wielu domen złośliwego oprogramowania
- **Dshield** – 20 najczęściej atakujących klas C
- **Ransomware Tracker** – wiele źródeł dotyczących ransomware
- **TOR** – anonimowa i szyfrowana ścieżka sieciowa

Dodatkowe źródła danych mogą być dodawane za pomocą dostępnego **otwartego API.**



# ADAPTIVE THREAT PROFILING – PRZYKŁAD



# MANAGEMENT EXPERIENCE FIRST.

## ZERO TRUST SINGLE POLICY FRAMEWORK & UNIFIED VISIBILITY

Juniper
Security Director Cloud

### SECURITY DIRECTOR CLOUD

**Zero Trust**

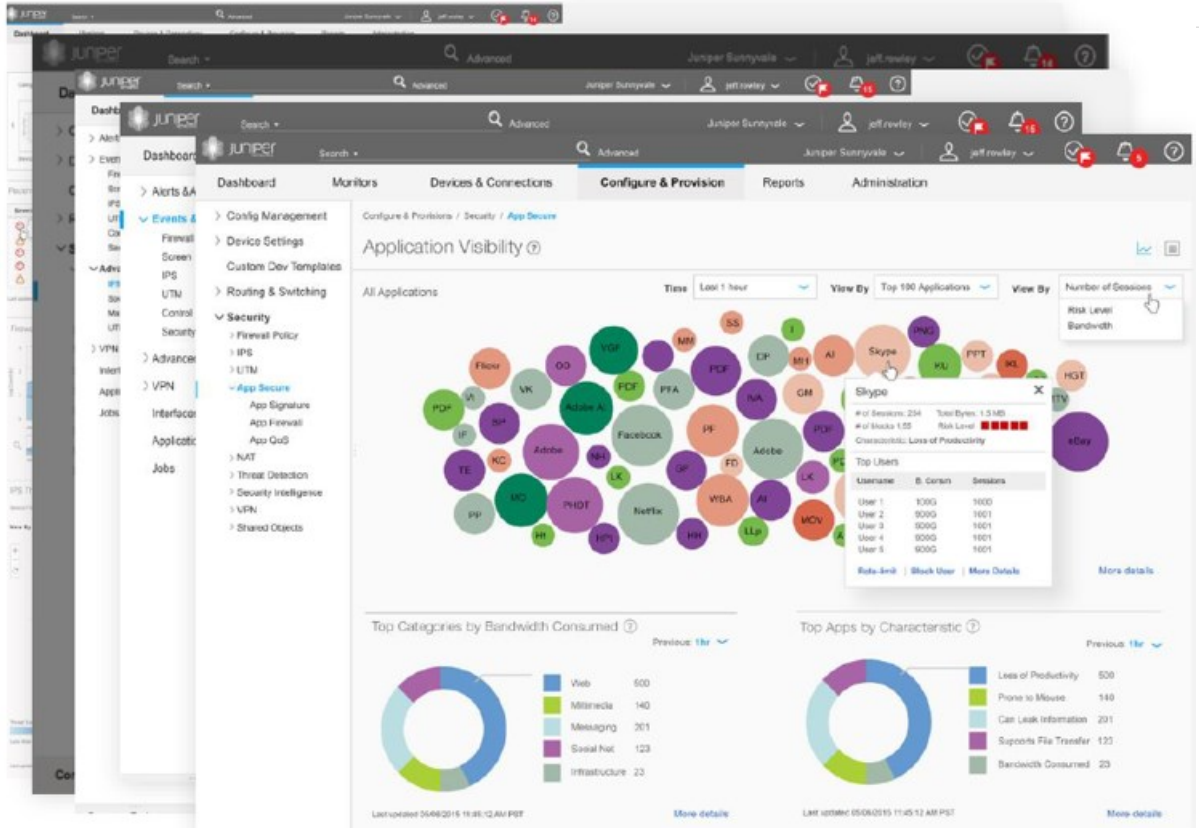
Jednolity system polityki bezpieczeństwa, niezależnie od lokalizacji użytkownika czy urządzenia.

**Unified Visibility**

Wgląd w dane i zdarzenia w całej infrastrukturze IT niezależnie od lokalizacji, urządzenia czy typu systemu. Pomaga to w szybszym wykrywaniu zagrożeń, analizie incydentów i zarządzaniu bezpieczeństwem.

# MANAGEMENT EXPERIENCE FIRST

## ZERO TRUST SINGLE POLICY FRAMEWORK & UNIFIED VISIBILITY




**Dashboard** – Panel główny

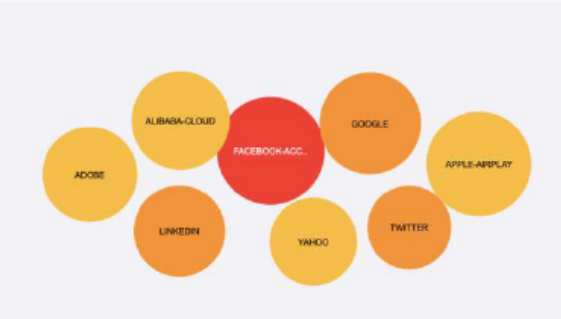
**Firewall Policy** – Polityka zapory sieciowej

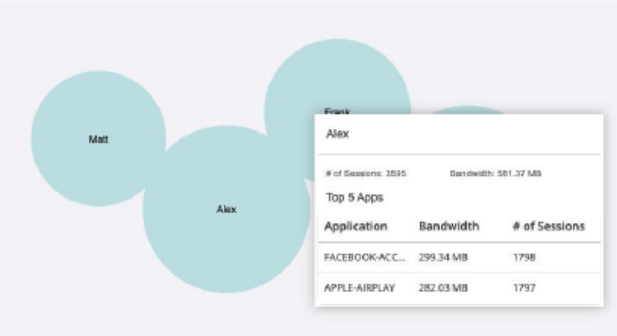
**Threat Map** – Mapa zagrożeń

**Events and Logs** – Zdarzenia i logi

**Application Visibility** – Widoczność aplikacji

# Unified Consistent Policy






Application


Users


IPS


Antivirus


Anti Spam


Content Filtering


URL Filtering

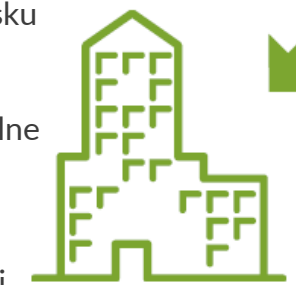

SecIntel


ATP Cloud

Policy

**Pełna kontrola lokalna** – dane i zarządzanie pozostają w środowisku klienta.

Brak zależności od chmury – idealne dla organizacji z restrykcyjnymi wymaganiami bezpieczeństwa.
Skalowalność – możliwość zarządzania dużą liczbą urządzeń i reguł.

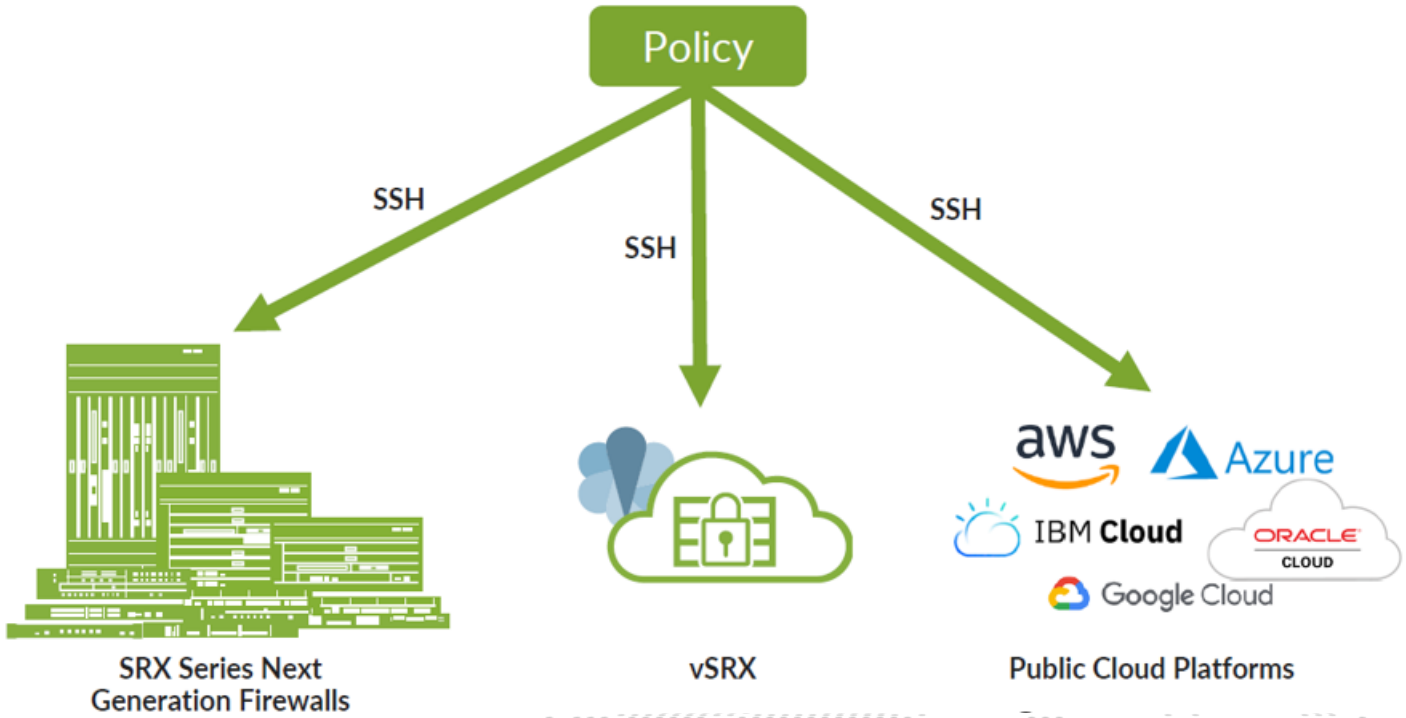

On-premises


On Cloud

**Bezpieczeństwo w chmurze:**

- Jednolita polityka bezpieczeństwa
- Gotowość do architektury SASE
- Centralne zarządzanie i widoczność
- Automatyzacja zadań bezpieczeństwa
- Ochrona niezależnie od lokalizacji
- Obsługa różnych typów zapór

# Security Anywhere Everywhere




**Jedna polityka zarządzania urządzeniami zabezpieczającymi Juniper – niezależnie od miejsca wdrożenia.**

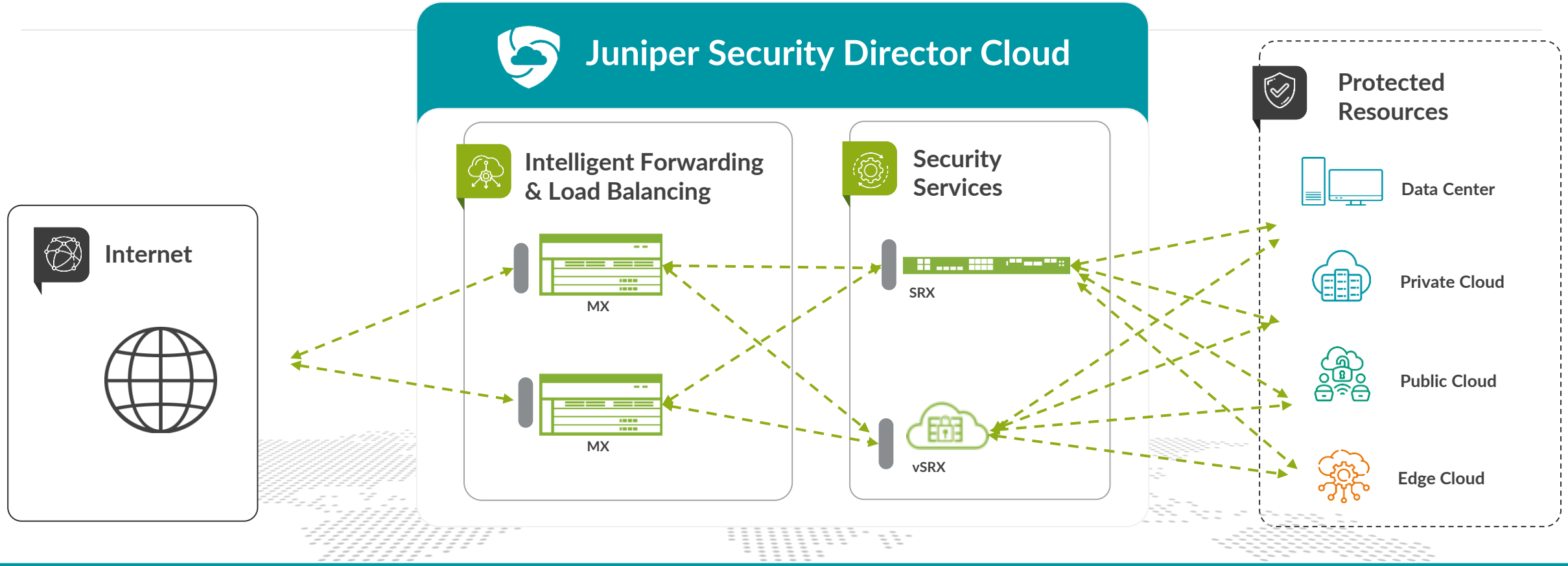
Wszystkie obsługiwane wersje i modele zapór sieciowych Juniper mogą być zarządzane za pomocą jednej, spójnej polityki.

**Obsługiwane technologie komunikacji:**
**Połączenie TLS/SSH** – bezpieczne kanały komunikacji

**Netconf** – protokół zarządzania konfiguracją sieci

INTRODUCING JUNIPER

# CONNECTED SECURITY DISTRIBUTED SERVICES ARCHITECTURE




**Unlimited scale-out** while operate as one logical device

**Independently scale** forwarding performance and services scale

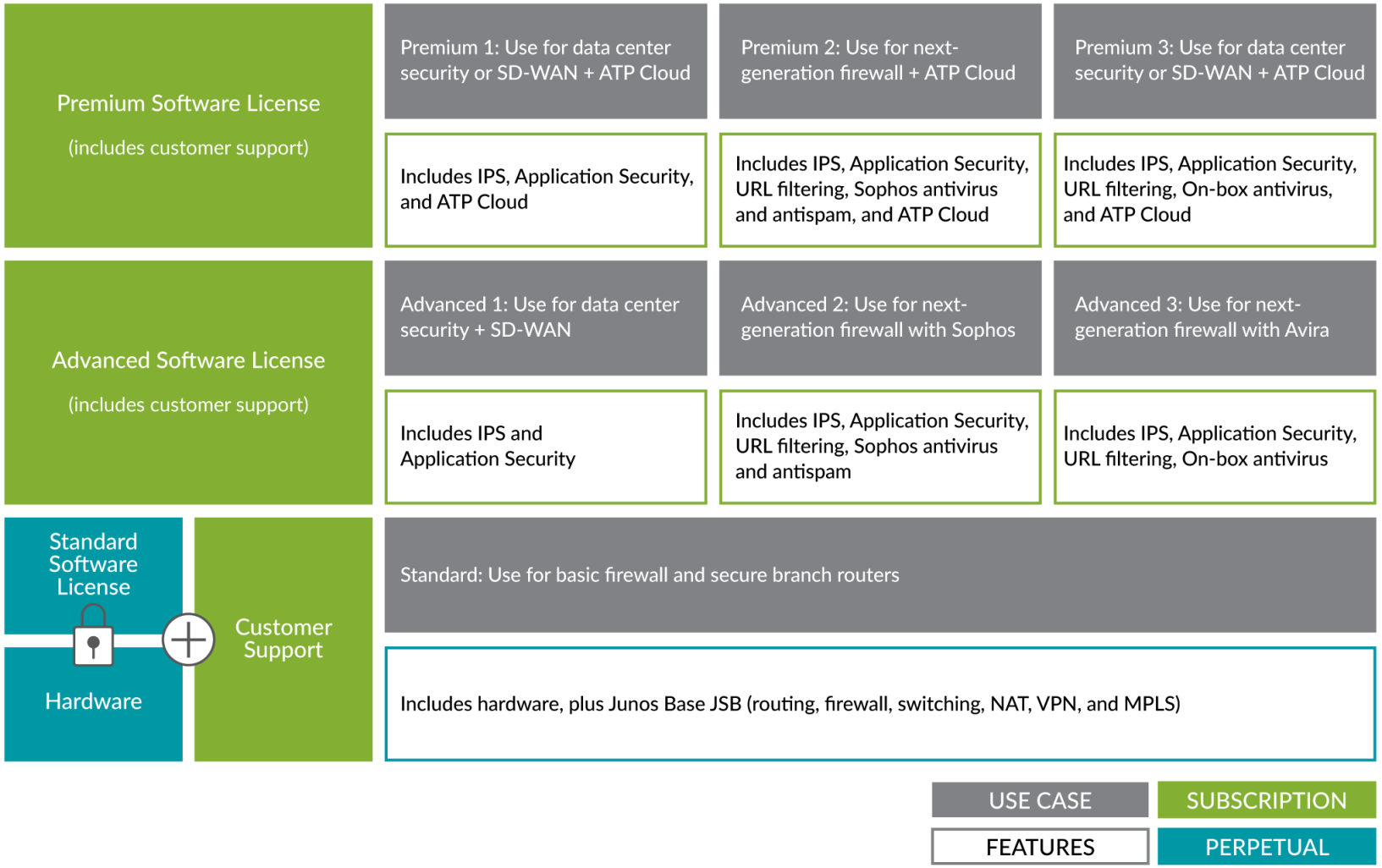
**Automated Resilience**, no single point of failure

**Leverage Existing Devices,** save cost

# SRX Security Subscriptions

Juniper Networks | Driven by Experience™

# Junos Security Feature Comparison



# Product Mapping to Security Subscriptions

| | A1 | A2 | A3 | P1 | P2 | P3 |
|---|---|---|---|---|---|---|
| SRX300/320 | ● | ● | – | ● | – | – |
| SRX340/345 | ● | ● | – | ● | ● | – |
| SRX380 | ● | ● | – | ● | ● | – |
| SRX1500 | ● | ● | ● | ● | ● | ● |
| SRX4100/4200 | ● | ● | ● | ● | ● | ● |
| SRX4600 | ● | ● | ● | ● | ● | ● |
| SRX5400/5600/5800 | ● | ● | ● | ● | ● | ● |

Bezpieczeństwo aplikacji obejmuje widoczność i kontrolę aplikacji poprzez jednolitą politykę dla funkcji nowoczesnej zapory sieciowej (Next-Gen Firewall). Dodatkowo umożliwia funkcje SD-WAN dzięki:

- zaawansowanemu routingu opartemu na politykach (APBR)
- monitorowaniu jakości działania aplikacji (AppQoE – Application Quality of Experience)

# SRX SKU Definition – Flex License


| Flex Tier | Software Features | License SKU |
|---|---|---|
| ADVANCED 1<br>DC Security / SD-WAN | IPS and AppSec | Example:<br>S-SRX380-A1-1 |
| ADVANCED 2<br>NG Firewall/SD-WAN w/Sophos | IPS, AppSec, URL Filtering, Sophos Anti-Virus and Anti-Spam | Example:<br>S-SRX380-A2-1 |
| ADVANCED 3<br>NG Firewall/SD-WAN w/Avira | IPS, AppSec, URL Filtering, on-box Anti-Virus and Anti-Spam | Example:<br>S-SRX380-A3-1 |
| PREMIUM 1<br>DC Security/SD-WAN + ATP Cloud | IPS, AppSec and ATP Cloud | Example:<br>S-SRX380-P1-1 |
| PREMIUM 2<br>NG Firewall/SD-WAN + ATP Cloud | IPS, AppSec, URL Filtering, Sophos Anti-Virus. Anti-Spam and ATP Cloud | Example:<br>S-SRX380-P2-1 |

# Security Subscription Bundles

| | A1 | A2 | P1 | P2 |
|---|---|---|---|---|
| IDP | ● | ● | ● | ● |
| AppSecure | ● | ● | ● | ● |
| SecIntel | ● | ● | ● | ● |
| Anti-malware Flow AV / AI-Predictive Threat Prevention (24.2) | ● | ● | ● | ● |
| Security Director Cloud | ● | ● | ● | ● |
| Content Filtering | — | ● | — | ● |
| NG URL Filtering (Junos 23.4) | — | ● | — | ● |
| ATP Cloud Sandbox | — | — | ● | ● |
| Encrypted Traffic Insights & DNS Security | — | — | ● | ● |
| Adaptive Threat Profiling | — | — | ● | ● |
| IoT Security | — | — | ● | ● |

**All licenses include Security Director Cloud**