STOP ATTACKERS IN THEIR TRACKS

SecIntel extends security intelligence across all points of connection across the network

Challenges

The goals of the network and security organizations are not aligned: one focuses on connectivity while the other focuses on securing the business. This limits where security can be deployed for identification and enforcement across the network.

Solution

SecIntel verifies threat intelligence at all network connection points to block malicious traffic. SecIntel can also be deployed at the network edge and across wired and wireless LANs, increasing visibility and creating enforcement points where threats can be blocked.

Benefits

- *Quickly identify risk and take action*
- *Increase the number of threat identification and network enforcement points*
- *Reduce the time required to curate and deploy threat intelligence*
- *Enable the security group to identify and block threats on unmanaged devices such as BYOD and IoT devices*

SecIntel curates threat intelligence to Juniper Networks® SRX Series Services Gateways, MX Series 5G Universal Routing Platforms, EX Series Ethernet Switches, and QFX Series Switches, allowing malicious traffic and/or hosts to be quickly identified and blocked.

The Challenge

As enterprises, applications, and users become more and more distributed, multilayer security becomes increasingly important. In fact, traditional security technologies and the infrastructure are converging, meaning Juniper's portfolio of standards-based security, routing, switching, and wireless products are well positioned to detect and enforce policies on their own as well as on third-party devices.

Customers can begin replacing their infrastructure as it ages out and complete their amortization cycle on legacy security and infrastructure products while pivoting their business to a lower risk profile. That is the power of creating a threat-aware network with Juniper Connected Security.

The Juniper Networks SecIntel Solution

At Juniper, we believe that a secure network must be threat-aware. Threat-aware networks require both deep network visibility and the ability to enforce policy at every connection point across the network. Automated policy orchestration across firewalls, switches, and routers is one example of a simple management option that allows administrators to safeguard users, applications, and infrastructure by automating the creation and distribution of policies that can monitor, block, or quarantine traffic down to the port level. That is the power of Juniper Security Intelligence (SecIntel).

SecIntel Overview

Relying on a single device at the network edge to identify and block threats leaves other points within the network vulnerable, lacking the necessary visibility and enforcement. After all, threats can and do emerge behind the organizational perimeter, and perimeter-only defenses leave gaps in security coverage. Securing the WAN edge and network against today's threats requires both deep network visibility and the ability to enforce policies at every connection point.

SecIntel addresses these challenges and constraints by aggregating threat data from multiple sources to deliver curated, consolidated, actionable intelligence. Our threat intelligence feeds include threat information curated by Juniper Threat Labs and accessed via Juniper Advanced Threat Prevention (ATP) cloud-based service and distributed to Juniper products through Policy Enforcer, a feature on Junos Space®

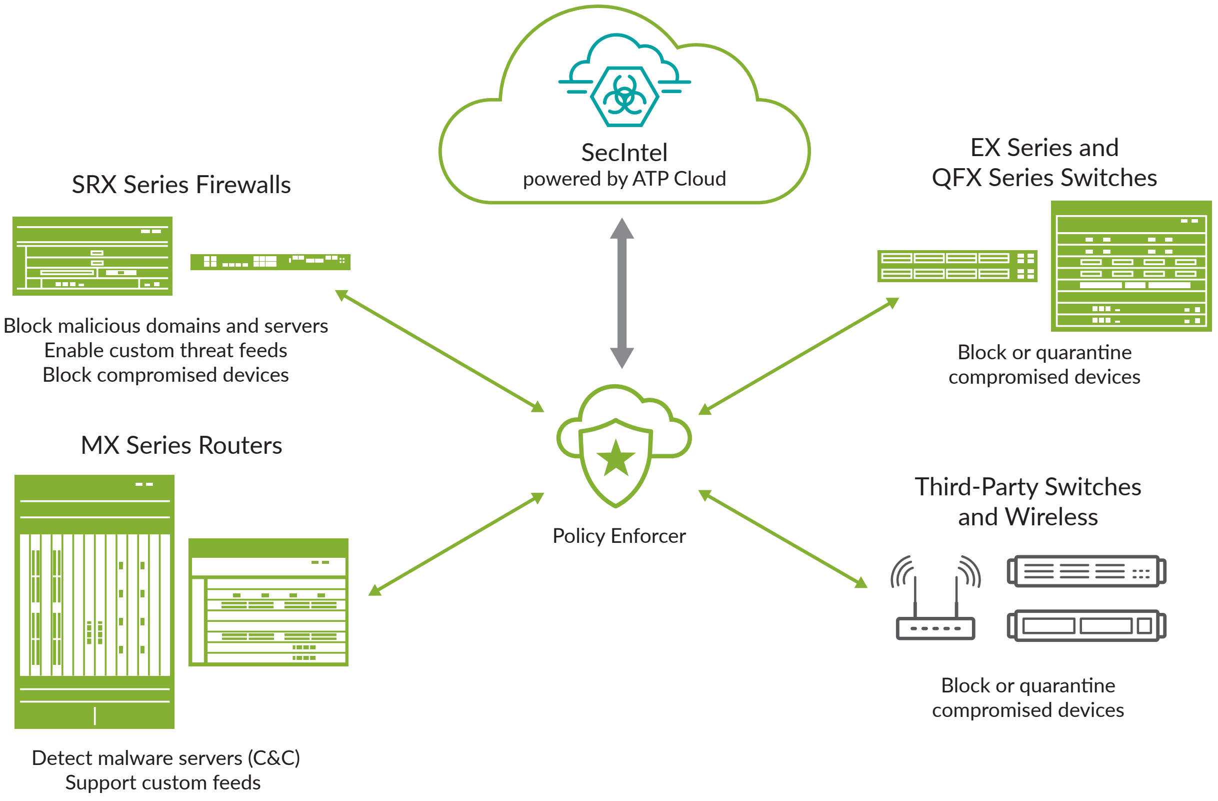

Figure 1: Juniper SecIntel used to build a threat-aware network

Security Director. These feeds also include third-party data and information that customers can integrate covering industry-specific threats.

Enforcing security at all connection points is more critical than ever. SecIntel allows you to enforce policies on SRX Series Services Gateways, MX Series 5G Universal Routing Platforms, EX Series and QFX Series switches, and even on third-party networking devices. You can selectively apply policies to individual devices, specific network segments, groups of devices, or push to all sites.

Features and Benefits

- Quickly identify risk and take necessary action across your network
- Block threats at any network connection point
- Leverage Juniper-curated as well as custom and third-party threat feeds
- Automate responses to threats

The SecIntel feature enables EX Series and QFX Series switches, SRX Series firewalls, and MX Series routers to consume threat feed data through Policy Enforcer and automate actions to block or quarantine threats. Threat feeds can be provided by Juniper ATP Cloud, third-party feeds, or custom feeds.

The infected host feed, provided by ATP Cloud through Policy Enforcer, can be automatically blocked or quarantined throughout the network, all the way down to the switch port or wireless access point level. Juniper's infected host threat feed is part of SecIntel.

In addition to the Juniper Threat Labs-supplied feeds offered through ATP Cloud, SecIntel allows IT teams to use custom threat feeds supplied by a third-party or based on detection events from the SRX Series' core, non-ATP feature set: application identification, intrusion prevention system (IPS), and Web filtering. These feeds, aggregated across multiple SRX Series firewalls in the ATP Cloud, can be used by admins as blacklists or as dynamic address groups in security policies across the network.

When used in combination with Juniper ATP, SecIntel threat feeds not only allow customer-provided rules and policies to be pushed to devices, they also allow threat responses to be automated. Policies can be applied to individual devices, specific network segments, groups of devices, or pushed to all sites, protecting the organization's entire network fabric, from the endpoint to the edge, and across every cloud in between.

Simplified Operations

SecIntel threat feeds allow IT teams to respond to threats in an automated fashion. By working closely with our customers, Juniper has ensured that the management experience, policy consistency, and security workflow are preserved. Juniper's Connected Security strategy is about protecting users, applications, and infrastructure—both physical and virtual—and this is why many of the largest companies in the world depend on Juniper to support their enterprise and cloud environments today.

Juniper has always been an industry-leading proponent of network automation and orchestration, both considered table stakes by our customers and partners. Juniper does not, however, take a proprietary approach to product automation. For example, in addition to many native Juniper automation capabilities, we also support third-party automation, enabling customers to take full advantage of their prior infrastructure investments. With Policy Enforcer, we provide third-party connectors for industry-leading network access control (NAC) technologies, including Forescout CounterACT and other third-party switches. These connectors provide the most common configuration for automating policy enforcement across non-Juniper products and help improve security.

Through Security Director and Policy Enforcer, Juniper provides a simple management option that allows administrators to detect threats, applications, and users and then automatically create and distribute firewall policies via metadata. Insightful visualizations enable administrators to quickly assess their network security environment. Administrators can interact with these visualizations, allowing them to take swift action.

Architectural Examples

When used in combination with Juniper ATP, Juniper's centralized network management products orchestrate rule changes to any combination of supported devices, enabling an automated threat response. This integration enables IT teams to block threats at any network connection point and, ultimately, is what enables the diversity of architectures that Juniper Connected Security supports.

When connecting distributed locations to the corporate WAN fabric, there are three possible approaches. The classic approach is to funnel all local traffic through a VPN or WAN connection, effectively backhauling it to the corporate data center. There, data flows are examined by centralized information security resources, and Internet traffic can exit the corporate network.

In a traditional split-tunnel approach, Internet-bound traffic leaves the distributed site using that site's Internet connectivity, reducing the load on the VPN and centralized IT resources. This method is predominantly employed to improve the experience for distributed users, as backhauling all traffic across the VPN can introduce significant latency.

The third option is to funnel Internet-bound traffic through a second tunnel to a cloud-based Internet hub. Here, data flowing from multiple distributed sites can be examined centrally with a less significant latency impact.

Application Policy-Based Routing (APBR) is critical in security as well as SD-WAN. By taking advantage of APBR and SecIntel, organizations can use any combination of these approaches on a per-application or per-user basis, providing automated information security protection to all data flows regardless of destination or origin. This ability to steer applications provides organizations with north-south protection, regardless of the WAN architecture.

Looking at this from a WAN core perspective, SecIntel's support for MX Series routers—which are not traditionally considered security devices—allows those routers to block many data flows before they reach the SRX Series firewalls. This layered approach reduces load on these more computationally expensive firewalls while protecting any corporate data flows transiting the router to access other network segments. Combined with SecIntel's support for the Juniper Networks vSRX Virtual Firewall and Juniper switches, SecIntel gives organizations the ability to block the lateral movement of threats, providing east-west protection as well.

About Juniper Threat Labs

Juniper Threat Labs provide dynamic and automatic updates for SecIntel. With a large global presence of honeypots, security researchers, and analysts, our dedicated team provides rapid and actionable insights about emerging threats, and new protection techniques.

Juniper Threat Labs also maintain and integrate our threat intelligence ecosystem by working with many other security vendors, alliances, and partnerships. SecIntel threat feeds can be used to filter traffic and drive automated incident response orchestration. These threat feeds are an important component of a threat-aware network, allowing IT teams to improve visibility and security while continuing to reduce risk. For the latest information on Juniper Threat Labs, please visit www.juniper.net/us/en/threat-labs/.

Summary—Enable a Threat-Aware Network and Stop Attackers in Their Tracks

Juniper SecIntel provides threat intelligence to all connection points across the network, blocking malicious traffic and strengthening network defenses. To reduce risk, SecIntel can be deployed on all firewalls, at the WAN edge, and across wired and wireless LANs to increase threat visibility and strengthen enforcement points. This allows IT teams to quickly identify risks and take effective action. It also enables the security group to identify and block threats on unmanaged devices such as BYOD and IoT devices.

Juniper's Connected Security strategy is about reducing the attack surface, unifying all network elements into a threat-aware network. Open and extensible, it enables IT teams to protect users, applications, and infrastructure—both physical and virtual—and this is why many of the largest companies in the world depend on Juniper to support their enterprise and cloud environments today.

Next Steps

For more information about Juniper's security solutions, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Engineering
Simplicity