

Managed Next Generation Firewall

From Juniper and Powered by Sky ATP, with Integration of Secureworks Threat Intelligence

Effective Deployment Comes with a Heavy Burden

Deploying a next-generation firewall (UTM) to guard against advanced threats is an important part of any company's security defense, but it merely is an initial step. Businesses often lack the in-house expertise to correctly manage security devices. Policies and security configurations must be updated. The amount of alert data can be overwhelming, making it difficult to sort out valid attacks from harmless noise. The inability to update protective measures against the latest threat tactics could leave an organization vulnerable.

How Secureworks Helps

Juniper Next Generation Firewall powered by Sky ATP and Secureworks Threat Intelligence helps clients identify malicious inbound and outbound traffic 24x7, while removing the burden of device or signature management. Experienced firewall and IDS personnel at Secureworks serve as an extension of a client's IT security team. The combination of our device management expertise and our global threat intelligence offers clients protection from threats to sensitive data, and provides comprehensive reporting to demonstrate security control effectiveness.

Secureworks pulls powerful intelligence into the solution via:

Attacker Database: Contains IP addresses and domain names of servers hosting exploits and malware, botnet Command and Control (C&C) servers, and other known malicious activity. Feeds are formatted and updated daily, giving valuable context to your security team.

Powering Advanced Protection with Threat Intelligence

Juniper Next Generation Firewalls perform inline deep packet inspection of inbound and outbound network traffic. The solution uses multiple integrated defense technologies to identify and block real security events requiring a client's attention. The solution provides proactive blocking as a standard configuration, and the client has the option of changing from blocking to monitor/alert-only mode. Our experienced engineers augment a client's staff by providing analysis, configuration, commissioning and management of firewall appliances.

Client Benefits

- Reduce administrative burden and mitigate high-fidelity risk
- Fully managed deployment powered by the Sky ATP threat feed
- Guard data and devices without hiring additional resources
- Powerful, updated intelligence protects against latest threats
- Generate reports in The Secureworks Client Portal to demonstrate compliance

Solution Features

- Sky ATP Juniper new/updated models
- Blocking mode configuration with option for monitor/alert-only mode
- CTU countermeasures and Attacker Database list
- Security and compliance reporting

The powerful Attacker Database provides Juniper clients with incremental Threat Intelligence gathered by The Secureworks Counter Threat Unit™ (CTU™) Research Team. The CTU features more than 70 world-class security experts who produce a globalized view of the rapidly changing threat landscape, integrating human intelligence into a client's Sky ATP connected devices.

Why it Matters

- **Reduce management and monitoring costs:** Our solution removes the burden of the administrative tasks of updating and maintaining a client's Juniper connected appliances, freeing up resources to focus on other business priorities.
- **Protect systems and data 24x7 without increasing in-house headcount:** Secureworks provides around-the-clock support, eliminating the need for clients to hire, train and retain qualified security personnel. With standard blocking configuration, the solution halts malicious traffic before it reaches a client.
- **Defend your network with real-time threat intelligence:** The infusion of CTU intelligence boosts the effectiveness of Juniper connected appliances, increasing the identification rate of suspected malware.
- **Guard against new and emerging threats:** The CTU research team is comprised of experts who understand the latest threat actors' tactics, techniques and procedures. Our holistic view of the global threat landscape gives clients the most updated, valid intelligence possible.
- **Filter out noise and manage valid attacks:** Escalations from CTU rulesets exhibit a superior accuracy rate, meaning what is escalated to a client represents a valid security threat.
- **Satisfy compliance regulations:** Clients easily can generate reports from The Secureworks Client Portal – Powered by the Counter Threat Platform™ (CTP) for technical audiences, management and auditors. Consolidated reports can be generated, providing audit trail documentation.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist. secureworks.com