

Managed Next Generation Firewall

From Cisco, with Integration of Threat Intelligence from Secureworks and FirePOWER IDS

Next generation firewalls and optional IDS provide organizations with a necessary layer of security, but the ever-evolving threat landscape requires companies to invest time and resources in order to keep security controls up to date and operating effectively.

Effective Deployment Comes with a Heavy Burden

Deploying a next generation firewall and optional IDS solution is an important part of any company's security defense, but it is merely an initial step. Businesses often lack the in-house expertise to correctly manage security devices, especially IDS, which require tuning, resulting in high false-positive and false-negative rates. Policies and security configurations require frequent updates. 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

Cisco Next Generation Firewall with FirePOWER IDS blades and Secureworks Threat Intelligence helps clients eliminate 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 allows clients to protect against threats to sensitive data, and provides comprehensive reporting to demonstrate security control effectiveness.

Secureworks pulls powerful intelligence into the solution via:

Proprietary IDS Signatures: Provide a fully managed and self-service capability to obtain highly targeted IDS signatures to integrate into FirePOWER's Snort IDS engine.

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 for FirePOWER and updated regularly, giving valuable context to your security team.

Client Benefits

- Reduce administrative burden and lower false positives
- Expert IDS tuning
- Guard data and devices without hiring additional resources
- Powerful, updated intelligence protects against latest threats
- Generate reports to demonstrate compliance

Powering Advanced Protection with Threat Intelligence

Cisco FirePOWER 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 does more than just monitor and alert. Our experienced engineers augment a client's staff by providing analysis, configuration, commissioning, management and tuning of FirePOWER appliances. Our service is customized for each client's unique environment. The powerful combination of IDS Signatures and Attacker Database provides Cisco 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 FirePOWER 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 FirePOWER appliances, freeing up resources to focus on other business priorities.

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.™

- **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.
- **Defend your network with real-time threat intelligence:** The infusion of CTU intelligence boosts the effectiveness of FirePOWER devices, 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 true positive/false positive rate, meaning what is escalated to a client represents a valid security threat.
- **Satisfy compliance regulations:** Clients can easily 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.



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
[secureworks.com](https://www.secureworks.com)