Cisco Firepower NGIPS Series Migration Options

Strengthen Your Network Defenses

It’s no secret that today’s attackers have the resources, expertise, and persistence to compromise any organization at any time. Traditional defenses are no longer effective.

Safeguarding your network assets and data from today’s threats requires detailed visibility into all your network layers and resources. It requires comprehensive, and up-to-date security intelligence. It requires a dynamic approach that uses awareness and automation to adapt to new threats, new vulnerabilities, and everyday network changes.

It requires Cisco Firepower® NGIPS (Next-Generation Intrusion Prevention System) threat appliances.

Many people think that with the adoption of a next-generation firewall (NGFW), that they no longer need a stand-alone intrusion prevention system (IPS). That’s simply not true. A “true” NGIPS can provide visibility, threat detection, threat response, and malware discovery. And it can do all that in areas of your network that remain off-limits to firewall inspection and controls.

The Cisco Firepower NGIPS threat appliance provides industry-leading visibility and threat efficacy against both known and unknown threats.

Cisco Firepower NGIPS stops threats by using:

- More than 30,000 IPS rules that identify and block traffic trying to exploit a vulnerability in your network
- Reputation-based IP, URL, and DNS security intelligence that can shrink the attack surface by identifying malicious sites
- A tightly integrated defense against network-based advanced malware attacks
- An integrated sandboxing technology that uses hundreds of behavioral indicators to spot zero-day attacks
- An Indications of Compromise (IoC) feature that correlates events from multiple sources to identify what may be compromised hosts

Upgrade your customers to Cisco Firepower NGIPS today to help them protect their network, users, applications, and information assets.

It’s as easy as 1…2…3

1. Confirm your current IPS model and refresh needs.
2. Review the recommended migration path.
3. Contact your trusted Cisco Security account manager or partner to get started.

Migration Recommendations for Cisco IPS and FirePOWER (former Sourcefire) Customers

Cisco IDS/IPS 4000 Appliances	Recommendation	Throughput Performance Improvement
Cisco IPS 4270-20	Firepower 4110	2X
Cisco IPS 4360	Firepower 4110	3.2X
Cisco IPS 4510	Firepower 4110	1.33X
Cisco IPS 4520	Firepower 4120	1.6X
Cisco IPS 4520-XL	Firepower 4140	1X

FirePOWER 81xxAppliances	Recommendation	Throughput Performance Improvement
FirePOWER 8120	Firepower 4110	2X
FirePOWER 8130	Firepower 4110	1X
FirePOWER 8140	Firepower 4120	1.33X
Firepower 8xxxx AMP Appliances		
FirePOWER AMP 8050	Firepower 4110 AMP	1.5X
FirePOWER AMP 8150	Firepower 4120 AMP	1.2X
FirePOWER AMP 8150	Firepower 4140 AMP	2X

To learn more about Cisco Firepower NGIPS threat appliances, please visit http://www.cisco.com/go/ngips.

To learn more about the Cisco Advanced Malware Protection capability, please visit http://www.cisco.com/go/amp.

To learn more about Cisco's Talos Security Intelligence and Research team, please visit http://www.talosintelligence.com/.