# Cisco Next Generation Firewalls



## Features and Capabilities:

### Superior Multilayered Threat Protection

Cisco ASA with FirePOWER Services brings distinctive, threat-focused, next-generation security services to the ASA 5500-X Series and ASA 5585-X firewall products. It provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks.

Cisco ASA with FirePOWER Services provides several advanced capabilities, listed below.

### Industry-Leading Network Visibility

Feature highlights include:

- World's most deployed ASA stateful firewall with remote access VPN and advanced clustering
- Granular Application Visibility and Control to support over 3000 application-layer and risk-based controls
- Cisco FirePOWER Next-Generation IPS appliances, which provide threat prevention and contextual awareness
- Filters on hundreds of millions of URLs in over 80 categories
- Discovery and protection against advanced malware and threats
- Proactively protect against Internet threats using Talos Security Intelligence
- Enforce differentiated policies based on the user, device, role, application type, and threat profile

You can centrally manage Cisco ASA with FirePOWER Services with the Cisco FireSIGHT Management Center. Gain comprehensive visibility into users, mobile devices, client-side apps, virtual machine (VM)-to-VM communications, vulnerabilities, threats, and URLs. Also, gain control over activity within the network and across next-generation firewall (NGFW) deployments.

Cisco FireSIGHT Management Center provides holistic, actionable indications of compromise (IoCs) that correlate detailed network and endpoint event information. It gives you further visibility into malware infections. And it also provides content awareness with malware file trajectory, which aids infection scoping and root-cause determination to speed time to remediation.

Cisco ASA Next-Generation Firewall Services add new capabilities, including Application Visibility and Control (AVC), Intrusion Prevention (IPS), and Web Security Essentials (WSE), to the ASA 5500-X Series. You can easily scale and manage these next-generation services with the Cisco Prime Security Manager, a centralized management application



This table shows the next-generation firewall capabilities and capacities of the Cisco ASA with FirePOWER Services for Cisco ASA 5500-X Series.

| Feature | ASA 5512-X | ASA 5515-X | ASA 5525-X | ASA 5545-X | ASA 5555-X |
|---|---|---|---|---|---|
| Maximum application control (AVC) throughput | 300 Mbps | 500 Mbps | 1100 Mbps | 1500 Mbps | 1750 Mbps |
| Maximum AVC and IPS throughput | 150 Mbps | 250 Mbps | 650 Mbps | 1000 Mbps | 1250 Mbps |
| Maximum concurrent sessions | 100,000 | 250,000 | 500,000 | 750,000 | 1,000,000 |
| Maximum new connections per second | 10,000 | 15,000 | 20,000 | 30,000 | 50,000 |
| AVC or IPS sizing throughput [440-byte HTTP]* | 100 Mbps | 150 Mbps | 375 Mbps | 575 Mbps | 725 Mbps |
| Supported applications | More than 3000 | | | | |
| URL categories | 80+ | | | | |
| Number of URLs categorized | More than 280 million | | | | |
| Centralized configuration, logging, monitoring, and reporting | Multidevice Cisco Security Manager and Cisco FireSIGHT Management Center | | | | |

\* Activating more features will change performance

## Safeguard your business by supporting threat prevention capabilities using IPS

Using Cisco Talos, ASA Next-Generation Firewall Services gather threat intelligence feeds from nearly two million Cisco security devices worldwide, giving you near-real-time protection from zero-day threats. Cisco ASA Next-Generation Firewall Services uses these same feeds to enable reputation-based web security and IPS policies.



## Many Devices, Total Control

With ASA Next-Generation Firewall Services, you can now confidently allow employees to use their personal mobile devices while maintaining high levels of network protection and control. Using Cisco AnyConnect, ASA Next-Generation Firewall Services identify the specific type of device attempting to gain access to the network, whether it is local or remote, and supports differentiated access policies based on this information.