At-a-Glance

Benefits

- **Superior threat defense** with the same industry-leading security technology found in larger Cisco® next-generation firewalls
- **Appropriately sized and affordably priced** for smaller and midsized company budgets, including a low total cost of ownership
- **Simplified on-device management or optional** centralized management for multiple device installations

Cisco ASA with FirePOWER Services

Advanced Security for Small and Midsized Organizations and Distributed Enterprises

Organizations, regardless of their size, face increasingly costly threats that jeopardize customer data, corporate secrets, and intellectual property. The **2013 Information Security Breaches Survey** commissioned by the U.K. government found that 87% of small businesses were compromised in 2012. And large organizations, to enhance their security, are insisting that their partners, such as law firms, improve their own threat defense to reduce the risk of becoming a threat vector.

Both small and midsized businesses and distributed enterprises have advanced threat protection needs. Until now, however, they have been underserved by unified threat management (UTM) products and competing next-generation firewalls (NGFWs). In contrast to these legacy approaches, Cisco NGFWs feature both Advanced Malware Protection (AMP) and next-generation IPS (NGIPS). The newest additions to the Cisco® ASA with FirePOWER™ Services NGFW family are tailor-made for small and medium businesses (SMB) and branch office applications, delivering integrated threat defense, low procurement and operating costs, and simplified security management.

The solution is available in both desktop (5506-X) and 1RU rack-mount (5508-X, 5516-X) form factors. Variants of the desktop model are available with an integrated wireless access point (5506W-X) to simplify SMB networking.

A ruggedized appliance (5506H-X) is specifically designed for industrial control systems and critical infrastructure applications. It features an extended operating temperature range and is available for desktop or DIN rail[1], rack or wall mount deployment.

Superior Value. Superior Threat Protection. Flexible Management Options.

Cisco next-generation firewall solutions feature superior value and leading threat protection capability, including firewall, application control, NGIPS, URL filtering, Cisco Advanced Malware Protection (AMP), and VPN. With exceptional visibility and control and automatic prioritization of threats, false-positive alerts that would otherwise overwhelm staff time can be managed efficiently.

[1] DIN rail - The term derives from the original specifications published by Deutsches Institut für Normung (DIN) in Germany, which have since been adopted as European (EN) and international (ISO) standards.

Proof Points

- Cisco ASA was cited by the 2014 IDC Worldwide Quarterly Security Appliance Track Study as the world's most widely deployed firewall.
- Cisco AnyConnect VPN Client is the world's leading VPN client, with over 100 million deployments, and is fully compatible with Cisco ASA with FirePOWER Services.
- Cisco ASA with FirePOWER Services uses daily threat feeds from Cisco Security Intelligence to provide timely threat detection capability.

Features

Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X, and 5516-X with FirePOWER Services

User/node Support	Unlimited by default
Desktop Form Factor (5506-X, 5506W-X)	7.92" x 8.92" x 1.73"
Rack Mount Form Factor (5508-X, 5516-X)	17.2" x 11.288" x 1.72"
Ruggedized Form Factor (5506H-X)	9.05" x 9.05" x 2.72"
Integrated I/O Ports	8 x 1GE
VPN	
VPN peers	50 - 300
Mobility Support	AnyConnect 4.x; native Apple iOS and Android clients
Throughput	
Max Stateful Firewall	750 Mbps – 1.8 Gbps
Max AVC	250 – 850 Mbps
Max AVC and NGIPS	125 – 600 Mbps
High Availability	Yes: Active/Standby Mode* Active/Active (5508-X and 5516-X only)
NGFW Capabilities	
AVC	Included with SmartNet
Supported applications	More than 3,000
URL Filtering	Subscription
Categories; Total	80+ ; 280+ million
NGIPS	Subscription
Signatures	6000+
AMP - Threat Defense	Subscription
Management	
Integrated On-box Management	Included by default
Centralized Management	Optional License

* Requires Security Plus License

For additional technical specifications, please see the ASA with FirePOWER Services data sheet.

These Cisco security solutions also accelerate incident response, with customers often reporting remediation time shortened from weeks to hours.

While these Cisco NGFW models are purpose-built for SMB and midmarket organizations, they provide the same superior threat protection technologies as other Cisco ASA 5500-X Series Next-Generation Firewalls, including the Cisco ASA 5525-X and 5585-X, which achieved the highest security efficacy rating in the NSS Labs **2014 Next-Generation Firewall Security Value Map**. These Cisco NGFWs include integrated on-device management for single-instance deployments and support centralized management with Cisco FireSIGHT Management System where required.

Cisco ASA with FirePOWER Services Standard Features

- **Granular Cisco Application Visibility and Control (AVC):** Cisco AVC supports more than 3000 application-layer and risk-based controls. For example, you can make popular social media applications read-only to enable compliance with regulations like Financial Industry Regulatory Authority (FINRA) and the Health Insurance Portability and Accountability Act (HIPAA) and to enforce acceptable-use policies.
- **Leading network firewall, and site-to-site and remote access VPN support:** Cisco delivers the world's most trusted and widely deployed firewall and VPN. The optional Cisco AnyConnect® VPN Client can be easily integrated with Cisco ASA with FirePOWER Services. Cisco AnyConnect 4.0 features granular, always-on, application-level VPN. Additionally, Cisco ASA supports Cisco AnyConnect mobile and native Android and iOS VPN clients.

Cisco FirePOWER Services Subscription Options

- **NGIPS** provides industry-leading contextual awareness, full visibility and control for users, devices, applications, and content, and industry-leading threat prevention.
- **AMP** provides industry-leading ability to discover, understand, stop, and when necessary remediate malware and emerging threats missed by other security layers.
- **Reputation-based URL filtering** blocks high risk Web addresses. Spam, URL-based viruses, phishing attacks, and spyware can direct users to malicious URLs. Cisco accurately analyzes URLs and associates a reputation score for each one, enabling users to avoid high-risk web addresses.

Next Steps

Get started by contacting a Cisco partner in your region: Locate a Cisco Partner.

C45-733830-01 03/15