



Cisco ASA with FirePOWER Services

Evolution Beyond Traditional “Defense in Depth” Security

Traditional “defense in depth” architectures typically force organizations to buy multiple security solutions – such as firewalls, VPN gateways, web filters, and other appliances – from different vendors. This approach increases complexity, as the products don’t always work well together. The lack of unified protection creates multiple blind spots. Attackers exploit these gaps, leaving organizations vulnerable and too often unaware of threats and attacks. Enterprises usually need to hire several dedicated teams to install and manage these disconnected security solutions. These security teams try to compensate for gaps in visibility and threat protection with manual processes that are inefficient, unreliable, and costly. This environment prevents rapid responses to the fast-changing threat landscape.

With Cisco ASA with FirePOWER Services, you consolidate multiple security layers in a single platform, eliminating the cost of buying and managing multiple solutions. This integrated approach combines best-in-class security technology with multilayer protection integrated in a single device that’s less costly than piecemeal security solutions. You also get much greater visibility into what’s going on in your network, far beyond what’s available with traditional solutions. With full contextual awareness you will see all the resources you are charged with protecting. Blinds spots that are avenues for exploit are eliminated. Full visibility lets you better detect and prioritize threats based on their risk. Their possible impact is assessed and prioritized by an automated system. Meanwhile, the number of events associated with monitoring and response is reduced. The time between detection and cure quickly shrinks in a streamlined operation.

Unprecedented Network Visibility

Cisco ASA with FirePOWER Services is centrally managed through the Cisco Firepower Management Center which provides security teams with comprehensive visibility into and control over activity within the network. This capability includes users, devices, communications between virtual machines, vulnerabilities, threats, client-side applications, files, and websites. Holistic, actionable indications of compromise (IoCs) correlate detailed network and endpoint event information and provide further visibility into malware infections.

Features and Benefits

Cisco ASA with FirePOWER Services provides:

- **Precise application visibility and control (AVC).** More than 3000 application-layer and risk-based controls can invoke tailored IPS threat-detection policies to improve security effectiveness.
- **Industry-leading Cisco ASA with FirePOWER NGIPS.** Highly effective threat prevention and a full contextual awareness of users, infrastructure, applications, and content help you detect multivector threats and automate the defense response.
- **Reputation - and category-based URL filtering.** This filtering provides comprehensive alerting and control over suspect web traffic. It enforces policies on hundreds of millions of URLs in more than 80 categories.
- **Advanced malware protection.** Effective breach detection with low TCO offers protection value. Discover, understand, and stop malware and emerging threats missed by other security layers.

Meet the industry's first adaptive, threat-focused next-generation firewall (NGFW) designed for a new era of threat and advanced malware protection. Cisco® ASA with FirePOWER™ Services delivers an integrated threat defense across the entire attack continuum – before, during, and after an attack. It combines the proven security capabilities of the Cisco ASA Firewall with industry-leading Sourcefire® threat and advanced malware protection features in a single device. The solution uniquely extends the capabilities of the Cisco ASA 5500-X Series beyond what other NGFW solutions are capable of.

Now we've integrated the next-generation intrusion prevention system (NGIPS) and advanced malware protection capabilities from Sourcefire with the industry's most trusted ASA firewall. This solution is available on the Cisco ASA 5500-X Series and ASA 5585-X NGFW platforms.

Cisco Firepower Management Center also provides content awareness with malware file trajectory. It helps you track an infection and determine the root cause to speed time to remediation.

Cisco Security Manager can help you manage a scalable and centralized network operations workflow. It integrates a powerful suite of capabilities, including policy and object management, event management, reporting, and troubleshooting for Cisco ASA Firewall functions. For small-scale and simple deployments, the Cisco Adaptive Security Device Manager (ASDM) can provide on-device, GUI-based firewall network operations management.

Cisco's enterprise-class management tools help administrators reduce complexity with excellent visibility and control across NGFW deployments.

Next Steps

To learn more about the Cisco ASA Firewall with FirePOWER Services, visit www.cisco.com/go/asafps.