



Top Use Cases: ASA with FirePOWER Services

Customer characteristics or requirements 	Relevant features or capabilities 
<p>1 Customer has experienced a breach and/or is highly concerned about security efficacy (e.g. financial, healthcare, government verticals) and needs protection against malware</p>	<ul style="list-style-type: none"> • Advanced Malware Protection (AMP) for Networks and AMP for Endpoints delivers integrated malware protection • AMP is managed centrally and provides sophisticated file detection, analysis, traceability and other forensics capabilities that enables a customer to remove malware from their system
<p>2 Customer is highly distributed and needs the ability to consolidate reports from multiple branches</p>	<ul style="list-style-type: none"> • Cisco FireSIGHT Management Center provides role-based, centralized device, license, event and policy management. It provides a dashboard with custom and template-based reports and alerts • FireSIGHT provides industry-leading visibility and insight into trends and high-level statistics to track security posture and event details to support compliance and forensics
<p>3 Customer has multiple overseas locations and requires automation to control access to the network</p>	<ul style="list-style-type: none"> • Sourcefire Snort engine delivers Next-Gen Intrusion Prevention System (NGIPS) with deep contextual awareness that provides important details about users and applications, such as identity, origin of access attempts, and device type • Security automation capabilities enable security administrators to design policies that permit or deny access based on certain attributes, including the ability to adjust many aspects of pre-defined rulesets and create custom rulesets
<p>4 Customer needs a faster way to cut through the network noise and wants alerts to identify which indicators of compromise (IoC) are relevant</p>	<ul style="list-style-type: none"> • Advanced Malware Protection (AMP) Threat Grid provides automated sandboxing of unknown files as they attempt to enter the network, including inspecting encrypted traffic • AMP helps customers understand malware – what it's doing or attempting to do, how large a threat it poses, and how to defend against it
<p>5 Customer has a dedicated security team or requires the services of an IT specialist to have granular control over security policy configuration and enforcement</p>	<ul style="list-style-type: none"> • The ASA's extensive database supports over 3,500 apps and micro-apps and provides granular control and deep configuration options for each • BrightCloud database supports URL and category filtering. It includes extensive configuration and management capabilities, Web reputation capabilities like risk and business relevance classifications, customizable block notification pages, and (via FireSIGHT Management Center syslog) reporting on URLs accessed
<p>6 Customer currently uses an older version of the ASA and other Cisco gear and wants to fortify their network security solution</p>	<ul style="list-style-type: none"> • The ASA with FirePOWER Services is a NGFW that has additional features and functionality that provide the customer greater deeper visibility and control over their network • ASA solutions work in unison with other Cisco network elements to provide cohesive security and excellent IT and business value