Cisco ASA with FirePOWER Services
For SMB, Distributed Enterprises, and Industrial Control Systems

Featured products: 5506-X | 5506W-X | 5506H-X | 5508-X | 5516-X
## Key Enhancements Over ASA 5505

<table>
<thead>
<tr>
<th>Category</th>
<th>5505</th>
<th>5506-X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NGFW</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Visibility &amp; Control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>FirePOWER Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMP, NGIPS, URL Filtering Subscriptions</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Hardware Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACT 2 Hardware Anti-Tamper</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Simplified Purchase Experience</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlimited User (node) Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced mobility support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Additional Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>→ Over 2X Firewall Throughput</td>
<td></td>
</tr>
<tr>
<td>Integrated Wireless Access Point</td>
<td>No</td>
<td>Yes (5506W-X variant)</td>
</tr>
</tbody>
</table>

**5506-X**
- More Secure
- More Scaleable
- More Flexible
Limited options made it difficult to get the protection you need

Unified Threat Management (UTM)  Stateful Firewall

OR

Multiple Point Solutions

- Email Security
- Network Control
- Malware Analysis
- Remote Access
- Web Security

Less Effective
- UTMs are often less effective than components-based systems
- Legacy firewalls and UTM solutions were never designed for protecting against advanced threats

Difficult to Integrate
- Point solutions are difficult to integrate and configure
- Incorrect or incomplete solutions can increase risk

Costly and Time Consuming
- Legacy NGFWs and point solutions are costly and may be impractical to administer
- Multiple vendors result in multiple support calls, increasing overall costs
## Until now

### Cisco ASA with FirePOWER services

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Cisco ASA" /></td>
<td><img src="image2" alt="Adaptive Security Device Manager (ASDM)" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Services</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-Generation IPS (NGIPS)</td>
<td>FireSIGHT Management Center</td>
</tr>
<tr>
<td>Application Visibility and Control (AVC)</td>
<td><img src="image3" alt="Advanced Malware Protection (AMP)" /></td>
</tr>
<tr>
<td>URL Filtering</td>
<td><img src="image4" alt="FireSIGHT Management Center" /></td>
</tr>
</tbody>
</table>

And Other Next-Generation Firewall Capabilities

---

Copyright © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.

Cisco ASA for SMB and Distributed Enterprise Presentation | © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 4

---

![Image](image5)
Hardware
## Start with the right appliance

### ASA 5506-X

- **Desktop Model**
  - 100% NGFW; best for ASA 5505-X refreshes

### ASA 5506W-X

- **Integrated Wireless AP:** Wireless can be managed locally or through WLC

### ASA 5506H-X

- **Ruggedized**
  - For industrial control and critical infrastructure

### ASA 5508-X / ASA 5516-X

- **Higher Performance**
  - Value-focused price; 5516 is best for 5512 & 5515

### Form Factor

<table>
<thead>
<tr>
<th></th>
<th>Desktop</th>
<th>Desktop</th>
<th>Rack Mount or Wall Mount</th>
<th>1RU</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Multicore @ 1.25GHz</td>
<td>Multicore @ 1.25GHz</td>
<td>Multicore @ 1.25GHz</td>
<td>5508: Multicore @ 2GHz</td>
</tr>
<tr>
<td>Memory – RAM</td>
<td>4GB</td>
<td>4GB</td>
<td>4GB</td>
<td>5516: Multicore @ 2.4GHz</td>
</tr>
<tr>
<td>Storage</td>
<td>50GB mSata</td>
<td>50GB mSata</td>
<td>50GB mSata tested for heat</td>
<td></td>
</tr>
<tr>
<td>Flash</td>
<td>8GB</td>
<td>8GB</td>
<td>8GB</td>
<td>8GB</td>
</tr>
<tr>
<td>Integrated I/O</td>
<td>8x1G (all L3 interfaces)</td>
<td>8 External, 1 AP</td>
<td>4x1G</td>
<td>8x1G (all L3 interfaces)</td>
</tr>
<tr>
<td>Security Context</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>FirePOWER Services</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Cisco Trust Anchor validates the source of the image file and protects against hardware tampering and counterfeiting.
To get the performance you need

<table>
<thead>
<tr>
<th>Features</th>
<th>ASA 5506-X</th>
<th>ASA 5508-X</th>
<th>ASA 5516-X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max stateful inspection throughput</td>
<td>750 Mbps</td>
<td>1 Gbps</td>
<td>1.8 Gbps</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>100 Mbps</td>
<td>175 Mbps</td>
<td>250 Mbps</td>
</tr>
<tr>
<td>Max AVC throughput</td>
<td>250 Mbps</td>
<td>450 Mbps</td>
<td>850 Mbps</td>
</tr>
<tr>
<td>Max AVC and NGIPS throughput</td>
<td>125 Mbps</td>
<td>250 Mbps</td>
<td>450 Mbps</td>
</tr>
<tr>
<td>AVC or IPS sizing throughput [440B]</td>
<td>90 Mbps</td>
<td>180 Mbps</td>
<td>300 Mbps</td>
</tr>
<tr>
<td>Max concurrent sessions</td>
<td>50,000</td>
<td>100,000</td>
<td>250,000</td>
</tr>
<tr>
<td>Max connections per second (CPS)</td>
<td>5,000</td>
<td>10,000</td>
<td>20,000</td>
</tr>
</tbody>
</table>

~1.5x to 2x

~1.5x to 2x

~1.5x to 2x

Cisco ASA for SMB and Distributed Enterprise Presentation | © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 7
Security Services
Add security services to help defend your network

**FirePOWER Services**
Subscription services that run on the ASA and provide enhanced levels of threat protection and network visibility

- URL Filtering
- Next-Generation Intrusion Prevention System
- Advanced Malware Protection
- Application Visibility and Control

**Foundational Functionality**
Built-in firewall services to provide base protection and connect with other security solutions

- Stateful Firewalling
- VPN Capabilities
- Policy Enforcement Point for ISE

Included by default
Minimize your exposure to web-based threats

**Services**
- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

**Block specific URLs**
- bad_url.com
- office365.com

**Restrict categories of URLs**
- Gambling
- Social Media
- Health
- Gaming
- Drug Use

Filter out over 280 million URLs based on any of the 80+ categories into which they are grouped; new URLs are added daily.

**Change policies easily**

Use the refined user interface to make additions or changes with just a few clicks.
Gain unmatched visibility and threat detection

**Protect the network more effectively**

NGIPS automatically correlates information from intrusion events with network assets to prioritize threat investigation.

- Priority 1
- Priority 2
- Priority 3

Blended threats and attacks coming through multiple vectors are quickly identified.

**Reduce IT management burden**

Policies can be updated automatically based on vulnerabilities and previous intrusion events.

Admins can make adjustments to policies and system settings across locations from a single location, even offsite.

---

**Services**

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

---

Cisco ASA for SMB and Distributed Enterprise Presentation | © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Protect against the most advanced forms of malware and remediate after a breach

**Services**

- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

**Point-in-time Protection**

Identify malware that other solutions miss by analyzing files based on reputation or suspicious behavior. AMP is continuously updated to ensure that it can stop the latest and most advanced forms of malware.

**Continuous Protection**

Defend against attacks even after a file passes the perimeter. AMP tracks files as they move around network; if they turn out to be malicious, you can quickly determine areas of impact and remediate quickly.
Reduce attack surfaces by controlling application access

Control port- and protocol-hopping apps that evade traditional firewalls

Enforce acceptable use policies with granular control over applications and micro-applications

Limit the exposure created by social media applications

Use custom application detectors / Open App ID

Services
- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

Capabilities
- Filters
- NGIPS
- AMP
- Stateful
- Firewalling
- AVC
- VPN
- AV
- URL
- Filtering
- AVC
- Stateful
- Firewalling
- VPN

Social Media Applications
- Facebook
- Google+
- Twitter
- LinkedIn
Leverage the proven ASA Firewall capabilities

**Standard Functions**
- TCP Normalization
- TCP Intercept
- IP Option Inspection
- IP Fragmentation
- NAT
- Routing
- ACL

**New ASA Features**
- Clientless tagging, WebVPN support for OWA2013 and XenDesktop7.5
- TLS 1.2
- ECMP Support, IPV6 BGP
- Std. based IKEv2 support. Citrix HTML5 browser support
- VPN Clients Win7, 8.1, 8.1 phone client, iOS8, Knox and Strong Swan
- Full VX LAN support
- Policy-based Routing
Extend protection to off-site users

**Services**
- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

**Diverse Endpoint Support**
- Mobile and non-mobile devices
- Cisco and non-Cisco devices

**Broad VPN Deployment**
- AnyConnect 4.0 and 3rd-party VPNs
- Single- and Multi-site deployments

**Split Tunneling Capabilities**
- Corporate and sensitive information
- Personal and generic information

**VPN Capabilities**
- Threat Protection
- Data-loss Prevention
- Acceptable Use
- Access Control

**Services**
- URL Filtering
- NGIPS
- AMP
- AVC
- Stateful Firewalling
- VPN Capabilities

**Diverse Endpoint Support**
- Mobile and non-mobile devices
- Cisco and non-Cisco devices

**Broad VPN Deployment**
- AnyConnect 4.0 and 3rd-party VPNs
- Single- and Multi-site deployments

**Split Tunneling Capabilities**
- Corporate and sensitive information
- Personal and generic information

**VPN Capabilities**
- Threat Protection
- Data-loss Prevention
- Acceptable Use
- Access Control
No other firewall offers extensive contextual visibility

The more infrastructure you see, the better protection you get
Or is supported by the largest security intelligence and research group

Identify advanced threats quickly with industry-leading threat research

Get industry-specific threat intelligence tailored to your business

Catch advanced threats endpoints miss with Cisco’s reverse engineers and threat analysts

Stay protected against the latest threats with regular updates pushed automatically

Talos

- Monitors 35% of the world’s email traffic
- Receives 1.1 million incoming malware samples daily
- Performs 4.9 billion AV and web filtering blocks per month
- Processes 100 terabytes of security intelligence daily

Email
Endpoints
Web
Networks
NGIPS
Devices

Threat Intelligence

Research Response

600+ Researchers
24 • 7 • 365 Operations
Management
Cisco offers multiple management solutions

Adaptive Security Device Manager (ASDM) on-box manager

FireSIGHT Management Center
Including integrated, on-box management through Adaptive Security Device Manager

ASDM 7.3.X+ combines control of Access Policy and Advanced Threat Defence Functions

The enhanced UI provides quick views on trends and the ability to drill-down for details

ASDM consolidates management of all stateful and Next-Generation Firewall functions for ease of use
And centralized management for greater control

FireSIGHT Management Center and Cisco Security Management (CSM)

- CSM is for ASA, and FireSIGHT Management Center is for FirePOWER Services
- They offer management capabilities across multiple devices
- Centralized management delivers comprehensive visibility and control over the network
- They provide optimal remediation through infection scoping and root cause determination
- FireSIGHT Management Center is offered as a physical appliance or a virtual appliance
With unmatched visibility for accurate threat detection and adaptive defense

Threats
Users
Web Applications
Application Protocols
File Transfers
Malware
Command & Control
Client Applications
Network Servers
Operating Systems
Mobile Devices

FirePOWER Services

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Linux</td>
<td>2.6</td>
</tr>
<tr>
<td>Google</td>
<td>Android</td>
<td>2.2, 2.3.4, 2.3.7</td>
</tr>
</tbody>
</table>

Operating Systems (2)
Cisco provides the best protection at a competitive price
NSS Labs:
Next-Generation Firewall Security Value Map

The NGFW Security Value Map shows the placement of Cisco® ASA with FirePOWER Services and the FirePOWER™ 8350 as compared to other vendors. All products achieved 99.2 percent in security effectiveness. Now customers can be confident they'll get the best protections possible, regardless of deployment.

Source: NSS Labs 2014
NSS Labs:
Intrusion Prevention Systems Security Value Map

Based on individual and comparative testing of vendors in the IPS market Cisco FirePOWER™ NGIPS* leads the Security Value Map and provides the best protection possible while also leading the class in total cost of ownership.

* Formerly Sourcefire FirePOWER

Source: NSS Labs 2014
Cisco® Advanced Malware Protection (AMP) has the lowest TCO of any product tested. It is also a leader in security effectiveness, achieving detection of 99 percent of all tested attacks. AMP excelled in time to detection, catching threats faster than competing breach detection systems.

Source: NSS Labs 2014
Cisco offers multiple deployment options
Options include clustering for linear scalability.

**Deployment Options**
- Linear Scalability Clustering
- Multi-context Mode
- High Availability

**Supported on 5516-X for 2 node clustering**
- Eliminates asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently
Multi-context mode for policy flexibility

Deployment Options
- Linear Scalability Clustering
- Multi-context Mode
- High Availability

Supported on both the 5508-X and 5516-X models

Each interface appears separately to FirePOWER Services module

Allows for granular policy enforcement on both ASA and FirePOWER Services

Supported on both the 5508-X and 5516-X models

Each interface appears separately to FirePOWER Services module

Allows for granular policy enforcement on both ASA and FirePOWER Services

Context B

Context A

Outside

Inside
And high availability for increased redundancy

Deployment Options

- Linear Scalability
- Clustering
- Multi-context Mode
- High Availability

Redundancy and state sharing (A/S and A/A pair)

L2 and L3 designs
FirePOWER can be deployed with ASA in 3 modes

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | **Fail-open**  
When FirePOWER services is deployed in fail-open mode, the traffic will not be blocked in case FirePOWER fails. |
| 2 | **Fail-closed**  
When FirePOWER services is deployed in fail-closed mode, the traffic will be blocked in case FirePOWER fails. |
| 3 | **Monitor Only**  
When FirePOWER services deployed in monitor only mode, the traffic from ASA will be copied to FirePOWER services. The FirePOWER services will not block any traffic. This is usually used for visibility. This mode is also known as “Passive Mode” or “IDS mode.” |
With the option to deploy in SPAN port mode (Interface Monitor-only mode)

Considerations for deployment:
- ASA running in transparent mode and single-context mode
- No failover or clustering setup
- SPAN traffic going to FirePOWER Services module in monitor-mode (CLI command: ‘traffic-forward sfr monitor-only’)
- Traffic forwarding interface must be a physical interface
- Traffic forwarding interface cannot be used for ASA traffic
- ASA version 9.4.1 and FirePOWER version 5.4.1.X
- Other ASA inline interfaces are running ASA functions, but are not forwarding any traffic FirePOWER services module
The default configuration offers easy, first-time setup

Default Configuration Provides easy Internet connectivity

1. **WAN connection**

2. **Manage ASA using Data port**

3. **Manage Firepower using management port**

There are three steps to provide internet connectivity to laptops

The WAN port, inside port and management port are already configured

The WAN port is the outside port that runs DHCP client, the inside port is configured for ASDM management, and the Management port will only be used to manage FirePOWER

FirePOWER Services can get internet connectivity using L2 switch, L3 switch is not required for SMB deployment
Deploy at the Internet Edge
And protect remote locations

Distributed Enterprises, Remote location/SMB Branch Deployment

All protected by Cisco ASA with FirePOWER Services
Receive this comprehensive protection today
Get started now

1. Identify your current and expected needs, paying attention to:
   a. Amount of traffic
   b. Other branches or locations and roaming users
   c. Management needs and resource availability

2. Work with a Cisco partner representative to determine the best hardware, services, and management solution for your needs

3. Deploy the appliance and subscribe to FirePOWER Services
Check out these additional resources

At-a-Glance

Data Sheet:

Cisco Talos Security Intelligence & Research:
Backup Slides
Packet Processing Order of Operations

1. ASA Module processes all ingress packets against ACL, Connection tables, Normalization and CBAC before traffic is forwarded to the FirePOWER Services module.

2. ASA provides flow normalization and context-aware selection/filtering to the FirePOWER Services.

3. Clustered ASA provides flow symmetry and HA to the FirePOWER Services.

4. Packets and flows are not dropped by FirePOWER Services.
   - Packets are marked for Drop or Drop with Reset and sent back to ASA.
   - This allows the ASA to clear the connection from the state tables and send resets if needed.
## Key Enhancements Over ASA 5505

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>5505</th>
<th>New ASA with FirePOWER Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGFW — FirePOWER Services</td>
<td>Application Visibility &amp; Control</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AMP, NGIPS, URL Filtering Subscriptions</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Security</td>
<td>Trust Anchor Module</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Hardware Anti-Tamper</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Purchase Experience</td>
<td>Unlimited User (node) Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN</td>
<td>Enhanced mobility support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Additional Features</td>
<td>Throughput</td>
<td>→</td>
<td>Over 2.5X Steeteful Performance</td>
</tr>
<tr>
<td></td>
<td>Integrated Wireless Access Point</td>
<td>No</td>
<td>Yes (5506W-X variant)</td>
</tr>
<tr>
<td></td>
<td>Ruggedized Option</td>
<td>No</td>
<td>Yes (5506H-X variant)</td>
</tr>
<tr>
<td></td>
<td>POE</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Stay focused on what’s important

**Impact Assessment**

Correlates all intrusion events with an impact of the attack against the target

<table>
<thead>
<tr>
<th>Impact Flag</th>
<th>Administrator Action</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Act Immediately; Vulnerable</td>
<td>Event corresponds with vulnerability mapped to host</td>
</tr>
<tr>
<td>2</td>
<td>Investigate; Potentially Vulnerable</td>
<td>Relevant port open or protocol in use, but no vulnerability mapped</td>
</tr>
<tr>
<td>3</td>
<td>Good to Know; Currently Not Vulnerable</td>
<td>Relevant port not open or protocol not in use</td>
</tr>
<tr>
<td>4</td>
<td>Good to Know; Unknown Target</td>
<td>Monitored network, but unknown host</td>
</tr>
<tr>
<td>5</td>
<td>Good to Know; Unknown Network</td>
<td>Unmonitored network</td>
</tr>
</tbody>
</table>
FirePOWER Services support all current ASA deployment models

- Up to 16x ASA in cluster
- Eliminates Asymmetrical traffic issues
- Each FirePOWER Services module inspects traffic independently

- Each ASA Interface appears as a separate interface to FirePOWER Services module
- Allows for granular policy enforcement on both ASA and FirePOWER services

- Redundancy and state sharing (A/S & A/A pair)
- L2 and L3 designs

*State sharing does not occur between FirePOWER Services Modules*