ASA Devices with FirePower Services—Access Control Set Up

Cox Communications Only—version 1.0

<table>
<thead>
<tr>
<th>Corporate Headquarters</th>
<th>Telephone</th>
<th>Fax:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>(408) 526-4000</td>
<td>(408) 526-4100</td>
</tr>
<tr>
<td>170 West Tasman Drive</td>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>San Jose, CA 95134-1706</td>
<td>(800) 553-NETS (6387)</td>
<td>Website:</td>
</tr>
<tr>
<td>U.S.A.</td>
<td></td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
</tbody>
</table>

Change Forecast: Low

This document is under revision control. All printed copies and duplicate soft copies are considered uncontrolled copies; refer to the original online version for the latest information.
This document applies to Cox Communications’ security and firewall setup with ASA and FirePower. It is not intended for any other Cisco client or partner.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW</td>
<td>1</td>
</tr>
<tr>
<td>Additional Information</td>
<td>3</td>
</tr>
<tr>
<td>ACCESS CONTROL WITH ASA AND FIREPOWER SERVICES</td>
<td>4</td>
</tr>
<tr>
<td>FOUNDATION SECURITY</td>
<td>5</td>
</tr>
<tr>
<td>Stateful Firewall</td>
<td>5</td>
</tr>
<tr>
<td>Firewall Types</td>
<td>5</td>
</tr>
<tr>
<td>Reflexive ACL-based Firewalls on ISR</td>
<td>5</td>
</tr>
<tr>
<td>ASA Firewalls</td>
<td>6</td>
</tr>
<tr>
<td>Firewall Services</td>
<td>7</td>
</tr>
<tr>
<td>Firewall Incident Identification and Remediation</td>
<td>7</td>
</tr>
<tr>
<td>VPN</td>
<td>9</td>
</tr>
<tr>
<td>ADVANCED SECURITY</td>
<td>10</td>
</tr>
<tr>
<td>Next Generation Intrusion Prevention Service</td>
<td>10</td>
</tr>
<tr>
<td>IPS Security Settings</td>
<td>11</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>13</td>
</tr>
<tr>
<td>Advanced Malware Protection</td>
<td>14</td>
</tr>
<tr>
<td>File Control</td>
<td>15</td>
</tr>
<tr>
<td>Network-Based AMP</td>
<td>15</td>
</tr>
<tr>
<td>File Information</td>
<td>16</td>
</tr>
<tr>
<td>Application Visibility and Control</td>
<td>17</td>
</tr>
<tr>
<td>Application Visibility</td>
<td>17</td>
</tr>
<tr>
<td>Application Control</td>
<td>18</td>
</tr>
<tr>
<td>Risk-based Control</td>
<td>18</td>
</tr>
</tbody>
</table>
Overview

The Cisco Adaptive Security Appliance (ASA) with FirePower™ services brings distinctive, threat-focused Next-Generation Intrusion Prevention System (NGIPS) to the Cisco ASA 5500 series’ next generation of firewalls.

ASA with FirePower services provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks. The Cisco ASA is the world’s most widely deployed, enterprise-class, stateful firewall. Cisco ASA with FirePower services features the following capabilities:

- Site-to-site and remote VPN access provide secure, high-performance access and high availability to help ensure business continuity.
- Cisco ASA with FirePower’s NGIPS (Next-Generation Intrusion Prevention System) provides highly effective threat prevention so the customer can identify needed changes to security policies based on real-time data, infrastructure, applications, and content to detect multi-vector threats and to automate a defensive response. If changes are needed, please submit a change request.
- Reputation- and category-based URL filtering offer comprehensive alerting and control over suspicious web traffic and enforce policies on millions of URLs in more than 80 categories.
- Advanced Malware Protection (AMP) provides industry-leading, effective breach-detection, a low total cost of ownership, and superior protection—value that helps you discover, understand, and stop malware and emerging threats missed by other security software.
## Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-generation firewall</td>
<td>Threat-focused Next-Generation Firewall (NGFW) provides ASA’s firewall functionality, advanced threat protection, and advanced breach detection and remediation in a single device.</td>
</tr>
<tr>
<td>Proven ASA firewall</td>
<td>Rich-routing, stateful firewall, Network Address Translation, and dynamic clustering for high-performance, secure, reliable access with Cisco AnyConnect® VPN.</td>
</tr>
<tr>
<td>Market-leading Next Generation NGIPS</td>
<td>Threat prevention and mitigation for known threats.</td>
</tr>
<tr>
<td>Advanced malware protection</td>
<td>Detection, blocking, tracking, analysis, and remediation to protect customers against targeted and persistent malware attacks.</td>
</tr>
<tr>
<td>Full contextual awareness</td>
<td>Policy enforcement based on visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats, and URLs.</td>
</tr>
<tr>
<td>URL filtering</td>
<td>Network-based control over websites along with the ability to enforce usage and tailor detection policies based on custom applications and URLs.</td>
</tr>
<tr>
<td>Enterprise-class management</td>
<td>For complete visibility, Cisco provides dashboards and drill-down reports to tell you about discovered hosts, applications, threats, and indications of compromise. Cisco also gets alerts when any security policies are violated, and evaluates the incident to determine whether an incident should be ticketed for resolution.</td>
</tr>
<tr>
<td>Streamlined operations automation</td>
<td>Lower your operating costs and decrease your administrative complexity by using threat correlation, impact assessment, and automated security policy tuning.</td>
</tr>
<tr>
<td>Purpose-built, scalable</td>
<td>Scalable security appliance architecture that performs consistent and robust security for small offices and branch offices; Internet edge; and data centers in physical and virtual environments.</td>
</tr>
<tr>
<td>Remote Access VPN</td>
<td>Extends secure access beyond your corporate network and corporate laptops to personal mobile devices, regardless of physical location. Supports Cisco AnyConnect™ Secure Mobility Solution, with granular, application-level VPN capability, as well as native Apple® iOS and Android™ VPN clients. An AnyConnect license is required.</td>
</tr>
<tr>
<td>Site-to-site VPN</td>
<td>Protect traffic—including VoIP and client–server application data—across the distributed enterprise and branch offices.</td>
</tr>
</tbody>
</table>
Additional Information

For more information, refer to the following documents:

- MSA Portal User Guide
  (https://www.cox.com/business/resources.html#Managed-Router-and-Security)
- FirePower Manager Graph Descriptions for Cox Communications
  (https://www.cox.com/business/resources.html#Managed-Router-and-Security)
- FirePower-System-UserGuide-v601
Access Control with ASA and FirePower Services

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network and pass through your firewall. More simply, an access control policy determines how the system handles traffic on your network.

The simplest access control policy handles all traffic using the policy’s default action—which is set up in the SKA file. For each access control rule, there is an action to take that determines whether your network monitors, trusts, blocks, or allows matching traffic. When you allow traffic, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your hardware assets or exit your network. For more information about what you can configure in the SKA, go to the IPS Security Settings beginning on page 11.

A more complex access control policy can use its access control rules to blacklist traffic based on security intelligence data or to exert control over network traffic logging and handling. These rules can be simple or complex; by matching and inspecting traffic using multiple criteria you can control traffic by security zone, network, geographical location, port, application, and requested URL.

When Cisco sets up access control and filtering, the default is to filter any-to-any traffic using the licensed services on your network.

Note: FirePower services require paid licenses before any intrusion prevention, malware detection, or URL filtering can be activated with a standard filtering policy applied to the device. For any additional filtering, such as by IP address, you must submit a change request because it is not feasible to capture all source and destination pairs in a SKA form.

For access control regarding the Internet, Cox’s firewall is provided by one of the following:

- Foundation Security: ISR (same features as MRS for Internet)
Foundation Security

Stateful Firewall

Each ASA comes with a set of standard functions designed to protect your network and keep operations running smoothly. These include:

- Transmission Control Protocol (TCP) Normalization and TCP Intercept to protect against denial-of-service (DoS) attacks. TCP Normalization is enabled by default; TCP Intercept requires a change service request. For more information, refer to http://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/firewall/asa-95-firewall-config/conns-con limits.html
- IP Option Inspection, IP Fragmentation, and Network Address Translation (NAT), and Routing, ensure that traffic gets to its intended location.

Firewall Types

Reflexive ACL-based Firewalls on ISR

Reflexive Access Control List (ACL) firewalls are based on simple lists that are implemented on Cisco ISR routers. These reflexive access lists are a type of dynamic packet-filtering technology. This packet filtering checks all the packets on the network and screens them against rules defined by ACLs. If a packet does not meet the criteria, then it is dropped from the network. These firewall ACLs can be defined on the basis of address, protocols, or port numbers.

Advantages

Reflexive ACL–based firewalls offer the benefit of lower resource usage and are best suited for smaller networks because they do not support complex, rules–based models.

Disadvantages

- Because reflexive ACLs are very basic, they only look at outgoing traffic and allow the opposite traffic to come back in.
- ACL-based firewalls look only at the source or destination addresses and the ports in the outgoing packet (stateless inspection).
- Reflexive ACLs also don’t address situations where a customer has multiple interfaces on its CPE device and needs multiple inspection policies from one interface to another.
- Reflexive ACLs are vulnerable to spoofing in some cases, and—due to the dynamic nature by which they are created and deleted—reflexive ACLs are much more difficult to pass than other packet filters. One reset packet is all that is required to entirely remove a reflexively generated ACL.
The following graphic shows an ideal implementation of a reflexive ACL-based firewall.

**ASA Firewalls**

With an ASA stateful firewall, a security policy determines what traffic is allowed to pass through a company’s firewall to access another network. This provides a much more reliable and secure firewall compared to a reflexive ACL-based access control running on an ISR.

By default, the ASA device allows traffic to flow freely from an inside network (higher security level) to an outside network (lower security level). You can apply actions to the traffic to customize the security policy. You can apply an access control lists to limit traffic from inside to outside or to allow traffic from outside to inside.

A simple packet filter, such as an ACL, can check for the correct source address, destination address, and ports, but it does not check that the packet sequence or flags are correct. A filter also checks every packet against the filter, which can be a slow process. A stateful firewall like the ASA device, however, takes into consideration the state of a packet:

**Is this a new connection?**

If it is a new connection, the ASA device checks the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the session management path.

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating Network Address Translations (NAT)
- Establishing sessions using the fastest path available
Is this an established connection?

If the connection is already established, the ASA does not need to re-check packets; most matching packets can go through the fastest path in both directions.

Firewall Services

- IOS Updates, patches
- Configuration Backups
- Default Firewall policy design and template creation for all customers. Outside-to-Inside or Outside-to-DMZ-related parameters are blocked by default in the SKA file.

Note: Custom firewall policies are available using a change request for an advanced customer. Customer must contact Cisco through Cox if they have any deviations from the standard policy.

- Firewall Rule/ACL changes
- Provisioning firewall with standard configuration
  - Internet NAT Configuration
  - DHCP Configuration
  - Quality of Service (QoS) Configuration
  - AnyConnect VPN
  - Multicast Configuration
  - Interface configurations (LAN, WAN)
  - Routing configurations

Firewall Incident Identification and Remediation

Monitoring profiles created in the MSA portal will define Key Performance Indicators (KPIs), and any Threshold Crossing Alarms (TCAs) will cause a ticket to be generated.

24 x 7 Monitoring of Security device performance

- Monitor for availability of all security devices, including the following:
  - System statuses
  - Failover
  - Heartbeat loss
  - High resource utilization alerts
  - High load average alerts tracking
24 x 7 Monitoring of real time Firewall events

- Correlate events to enhance the monitoring standard and identify more accurately the possible incidents in the client’s network
- Store the events securely for forensic analysis
- Post event analysis as part of problem management and tracked via CMS ticketing system.

Monthly CPE device performance reports available on Monitoring Portal

- Firewall event reports
  - Alarm based Security events
  - Performance Graphs
  - Event summary for Firewall activity

Note: Additional details about the MSA Portal can be found in the MSA Portal User Guide.

Notify interested parties of Firewall incidents identified, and escalate per customer requirements.

Send electronic notification to the portal for relevant parties to view status. Cox Communications will be notified of the incident so it can contact its end customer.
VPN

Virtual Private Networks (VPN) offer support for a variety of endpoints on both mobile and non-mobile devices, and supports the native Apple iOS and Android VPN clients, even on mobile devices using AnyConnect.

Employees working remotely can send corporate data through the corporate VPN, while personal apps and data can travel a different path. This ensures protection of important information without bogging down network traffic with non-business data.

- VPN capabilities also support split-tunneling information.
- AnyConnect VPN for remote users extends secure corporate network access beyond corporate laptops to personal mobile devices, regardless of physical location.
- Site-to-site VPN protects your traffic, including VoIP and client-server application data, across the distributed enterprises and branch offices.
Advanced Security

FirePower services provide enhanced levels of threat detection and prevention to secure a network. These include:

- Next-generation Intrusion Prevention Service
- URL Filtering (Content Filtering)
- Advanced Malware Protection (AMP)
- Application Visibility Control (AVC)

Next Generation Intrusion Prevention Service

Intrusion detection and prevention is a system’s last line of defense before traffic is allowed on to its destination. Intrusion policies are defined sets of intrusion detection and prevention configurations invoked by your company’s access control policy. Using intrusion rules and other settings, these policies inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic.

If the system-provided policies do not fully address the security needs of your organization, Cisco can help you with custom policies that help your company configure—at a very granular level—how the system processes and inspects traffic on your network for intrusions.

**Note:** Custom intrusion and access control policies must go through the change management process. For more information about what you can configure, go to the IPS Security Settings beginning on page 11.

Here are some ways FirePower’s NGIPS helps your company:

- NGIPS offers granular visibility and threat detection to help protect your network.
- Because it continuously scans your network traffic, NGIPS uses all the information about devices and applications on the network to better analyze intrusion events. By automatically correlating that information, NGIPS can assess each threat and prioritize which intrusion events are impactful and should be immediately investigated.
- The Multi-Vector Correlation feature in FirePower helps address sophisticated, blended threats that combine various evasive methods such as phishing emails, innocuous payloads, stealthy network profiling, infrequent call outs, and much more. It enables easier and earlier identification of infected hosts by correlating and tabulating suspect behaviors across the varied attack planes and integrating network- and file-level activity.
- In addition to protecting the network more effectively, NGIPS can also help reduce the workload of IT staff. By linking asset information with asset vulnerabilities, NGIPS can automatically determine the appropriate intrusion
prevention rules to put in place to defend against risks. This feature not only results in better security, but also enables organizations to do more with the limited resources they have in place.

- NGIPS leverages site reputation, geo-location, and more to determine the risk posed by communications. It then automatically adapts security policies, inspection depth, and controls to better align security with the threat profile of the environment.

### IPS Security Settings

The main metric used to determine a default setting is the Common Vulnerability Scoring System (CVSS) score, which is applied to each vulnerability discovered by the Security team.

The second metric is time-based and concerns the age of a particular vulnerability.

The final metric is the particular area of coverage for the rule. For example, SQL Injection rules are considered to be important enough to have influence when being considered for policy inclusion. The IPS profile settings are:

- No IPS
- Maximum Detection: Maximum Detection policy enables Maximum intrusion detection and will show events about intrusion attempts but will not drop traffic and intrusion attempts. It shows what traffic would have dropped.
- Balanced security and connectivity (default)
  - Common Vulnerability Scoring System (CVSS) Score 9 or greater
  - Age of the vulnerability
    - Current year
    - Last year
    - Year before last
  - Rule Category
    - Malware- Command and Control (CnC)
    - Blacklist
    - SQL Injection
    - Exploit-kit

- Security over connectivity
  - CVSS Score 8 or greater
  - Age of the vulnerability
    - Current year
    - Last year
    - Year before last
    - Year prior
  - Rule Category
    - Malware-CnC
    - Blacklist
    - SQL Injection
    - Exploit-kit
    - App-detect

- Connectivity over security
  - CVSS Score must be 10
  - Age of the vulnerability
    - Current year
    - Last year
    - Year before last
  - Rule Category
    - Not used for this policy
URL Filtering

The ASA and FirePower network-based URL filtering leverages a default reputation filtering policy that can be customized by categories and applied to a network. URL filtering can be enabled based on reputation or by using a manual process. By default, all traffic is allowed and access-policies need to be defined.

For URL filtering, there are over 80 categories to choose from. FirePower uses URL categories from Brightcloud. Click the following link for a list of Brightcloud’s categories and descriptions: [http://www.brightcloud.com/tools/change-request-url-categorization.php#catdescription](http://www.brightcloud.com/tools/change-request-url-categorization.php#catdescription)

URL profiles provide a starting point for filtering in the customer network. As the customer determines that URLs need to be unblocked or blocked these requests are handled through the change management process. (Call from customer to Cox Care, where the customer is validated by a PIN.)

The following profiles are available for URL filtering:

- No URL Filtering—Allows all URLs
- Basic—Blocks all categories that are ethically inappropriate for a business (gambling, pornography, and so on) and allows all leisure sites (social media, health, and so on)
- Balanced (default)—Blocks all categories that are ethically inappropriate and also blocks leisure sites that could be a security risk (games, dating, auctions, and so on)
- Aggressive—Blocks all categories that are ethically inappropriate, blocks all leisure sites

**Note:** You can select URL filtering profiles in the SKA file.
The following graphic shows how you can manage traffic by blocking specific URLs or by using categories.

Advanced Malware Protection

Advanced malware protection (AMP) looks for malware in files by inspecting network traffic for several file types. AMP correlates data and other information to quickly detect and identify malware. Malware protection is set up as part of your FirePower access control configuration. The settings for AMP are:

- No AMP—There is no malware protection installed.
- Detect Files (default)—Detect the malware or suspicious file type, log the detection, allow file transmission.
- Block Files—block specific file types and reset the connection when a file transfer is blocked. File types that can be blocked have been added to the SKA.
- Detect and Block Malware—calculates the SHA-256 hash value, queries the Local Malware Analysis Engine to determine whether the file contains malware, blocks the contaminated file.

Note: AMP settings are configured in the SKA file.
**File Control**

File control detects and blocks users from either sending or receiving specific file types on your network. File control is set up as part of your company’s overall access control configuration; file policies then inspect network traffic to ensure it meets fire control rule conditions as the traffic moves through an ASA.

The File Control list is in the SKA.

**File types monitored for AMP**

- Office documents
- Archive
- Multimedia
- Executables
- PDF Files
- Encoded
- Graphics
- System Files
- Dynamic Analysis Capable
- Local Malware Analysis Capable

**Network-Based AMP**

AMP’s continuous analysis and retrospective security capabilities include:

- Indications of Compromise tracking (IoCs): File events are correlated and prioritized as potential active breaches. AMP automatically correlates multi-source security event data, such as intrusion and malware events, to help connect events to larger, coordinated attacks and to prioritize high-risk events.

- File reputation: Advanced analytics and collective intelligence are gathered to determine whether a file is clean or malicious, allowing for more accurate detection.

- Retrospective detection: Send alerts when a file’s disposition changes after extended analysis, giving you awareness of and visibility into malware that evades initial defenses.

- Custom whitelists: Ensure that safe, custom, or mission-critical applications continue to run no matter what. By Default, no custom whitelist or blacklist will be added, if you want certain traffic to be whitelisted, you will need to submit a change request.

- Device flow correlation: Stops malware call-back communications at the source, especially for remote endpoints outside the corporate network.
**File Information**

On the Analysis tab in FirePower, you can see interactive graphs that give you an overall picture of file and malware events on your monitored network.

Five of the graphs display the file types, file names, and malware impact (disposition) on detected files, along with the IP addresses of the computers sending (uploading) and receiving (downloading) those files. The final graph displays the malware threats detected on your network.

The graphs are:

- Top File Types
- Top File Names
- Top Hosts Sending Malware
- Top Hosts Receiving Files
- Top Malware Detections
- File by Disposition
Application Visibility and Control

AVC provides a solution for setting policy rules for deeper, more precise inspection of network traffic. It discovers applications running on the network and implements control mechanisms to optimize application performance and network resources. AVC enables you to:

- Gain deep visibility into app usage, regardless of port or protocol
- Limit social media to control malware and data leakage
- Reclaim bandwidth from streaming and sharing apps
- Reduce attack surface and inspection requirements

While traditional firewalls enforce policies based on the IP address, port, or protocol alone, AVC identifies each app and allows or blocks it at a network level. It also limits exposure to peer-to-peer file sharing, gaming, chat, or other risky or non-productive apps that often evade traditional firewall protections.

AVC enables users to detect and track custom application signatures to ensure the same enhanced visibility and control over proprietary and custom apps.
Application Control

AVC also offers granular control over both applications and micro-applications. Allow access to certain apps, while restricting micro applications such as videos and chats.

Application conditions in access control rules allow you to perform this application control. Within a single access control rule, there are a few ways you can specify applications whose traffic you want to control:

- You can select individual applications, including custom applications. To do this, look at the list of applications running on your network, then submit a change request for any applications you want to block. To see the list of applications running on your network, look in the FirePower Manager.
- You can use system-provided application filters, which are named sets of applications organized according to the applications’ basic characteristics: type, risk, business relevance, categories, and tags.
- You can create and use custom application filters, which group applications (including custom applications) in any way you choose.

In addition, Cisco frequently updates and adds additional detectors using system and vulnerability-database updates. By using filters based on application characteristics, you can ensure that the system uses the most up-to-date detectors to monitor application traffic. The default restriction level is based on the system-provided application filters.

Risk-based Control

In addition to application controls, AVC supports risk-based controls that can launch tailored threat detection policies to optimize security effectiveness. Cisco will help you with any customizations you need. These changes require a change request.