FirePower Manager
Graph Descriptions
for Cox Communications
CISCO CONFIDENTIAL

This document provides additional descriptive details about the service elements defined in the service description and any addendum documents provided by Cisco. This document does not constitute a written agreement between Cisco and the Customer.

THE SPECIFICATIONS AND INFORMATION REGARDING THE SERVICES IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY SERVICES.

Cisco and the Cisco logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at http://www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The information provided in this document is confidential information of and proprietary to Cisco and is being furnished with the understanding that Customer will keep such information confidential. The information provided in this document may not be used for any purpose other than in connection with Customer’s use of the relevant services provided by Cisco. To that end, this document, and the information contained in it, must not be disclosed to any person other than an employee or advisor of Customer who requires the information in order for Customer to use, or to carry out its responsibilities with respect to, the relevant services provided by Cisco.

© 2016 Cisco Systems, Inc. All rights reserved.
Contents

OVERVIEW .............................................................................................................................................1
  Audience.............................................................................................................................................1
  Scope ..................................................................................................................................................1
  Additional Information ........................................................................................................................1

ASA FEATURES SUPPORTED FOR COX COMMUNICATIONS ..................................................2

FIREPOWER FEATURES SUPPORTED FOR ASA DEVICES ..................................................3
  Anti-Malware ........................................................................................................................................3
    Standard Policies ..............................................................................................................................3
    Supported.........................................................................................................................................4
    Malware Graphs and Widgets ...........................................................................................................4
    Not Covered......................................................................................................................................4

  URL Filtering ....................................................................................................................................5
    Supported.........................................................................................................................................5
    URL Filtering and Reputation Categories ......................................................................................5
    URL Graphs and Widgets ...................................................................................................................5
    Not Covered......................................................................................................................................5

  Application Visibility Control ..........................................................................................................6
    Supported.........................................................................................................................................6
    Application Visibility Graphs and Widgets ......................................................................................6
    Network Information Graphs and Widgets ......................................................................................6
    Security Intelligence Graphs and Widgets .......................................................................................6
    Not Covered......................................................................................................................................6

  Intrusion Prevention ..........................................................................................................................7
    Supported.........................................................................................................................................7
    Intrusion Graphs and Widgets ...........................................................................................................8

FIREPOWER MANAGER TABS, GRAPHS, AND WIDGETS ..................................................9
  Tips ....................................................................................................................................................9
    Hover................................................................................................................................................9
    Double-click.....................................................................................................................................10
    Graph Options.................................................................................................................................10
    Overview Tab—Summary Dashboard ..............................................................................................12
    Network Subtab ..............................................................................................................................12
Overview

As part of access to the Managed Service Activator (MSA) portal, your company or business will be able to view device and user data in the MSA portal and—for even more analytic capability—view access to data tabs in the FirePower Manager.

This document contains a list of features supported in Cox’s golden config file, which is owned by Cox and shared with Cisco. The golden config file serves as the basis for all Cox ASA device implementations.

Additionally, this document contains a list of the FirePower Manager tabs, graphs, and widgets your company or business can see and analyze to ensure that your data and your routers are as secure as possible.

**Note:** Access into FirePower is set up as part of the single-sign-on functionality you use to sign in to the MSA portal. Just sign in to the Cox MyAccount page using your Cox user name and password; click the MSA Portal link; and then click the Display Security Metrics button. FirePower is only available for ASA devices.

Audience

This guide is intended for Cox Business operators. It provides information about the information available in the MSA portal graphs and widgets.

Scope

This document contains information about the MSA portal features and functionality that apply to the Cox Business configuration for MSA and FirePower Manager only. It is not intended for use by any other Cisco client.

Additional Information

For more information, refer to the following documents:

- Managed Service Activator Portal User Guide for Cox Communications
- ASA Devices with FirePower Services—Access Control Set Up
- FirePower-System-UserGuide-v601
ASA Features Supported for Cox Communications

This section lists the features supported by Cisco for ASA devices. These features are part of the golden configuration, which is tested and shared with Cisco by Cox Communications.

- AAA
- Access list Out-To-In
- Anti-Spoofing Configuration
- ASDM Access
- Banner
- BGP Configuration
- DHCP Configuration
- DHCP Relay Configuration
- DMZ Configuration
- Dynamic NAT
- Dynamic Routing - OSPF
- Dynamic Pool NAT
- Failover Active/Standby
- Failover Interface
- FirePower Module Configuration
- ASDM Access
- Hostname Configuration
- HTTP Inspection
- IPv4 Default Route
- IPv6 Default Route
- IPv6 SLAAC
- LAN Configuration
- Logging Configuration
- Multicast Configuration
- Netflow Configuration
- NTP Configuration
- Prioritize VPN Management Traffic
- QoS Configuration
- Route Tracking SLA
- Site to Site VPN Configuration
- Site to Site VPN Management Traffic
- SourceFire Interface
- SourceFire Management Configuration
- SSH Access
- Static NAT
- Static Route
- Telnet Access
- Threat Detection
- WAN Configuration
FirePower Features Supported for ASA Devices

This section lists the supported functionality; graphs and widgets; and non-supported functionality in the FirePower Manager implementation for businesses and companies that purchased the managed router service from Cox Business.

The functionality in this section applies to ASA devices that are being monitored as part of the Managed Router service your company or business purchased from Cox Communications.

Note: Cox Communications and Cisco jointly tested the supported features and functionality in this section.

The FirePower features used for Cox Communications are in the following areas:

- Anti-malware
- URL Filtering
- Application Visibility Control (AVC)
- Intrusion Prevention

Anti-Malware

Advanced Malware Protection (AMP) for FirePower allows you to detect, store and block malware on your network using managed devices.

Standard Policies

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
- 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: Changes to the anti-malware policy must go through the change management process. Anti-malware policies are set in the SKA when you order a service. For more information, refer to the Access Control with ASA and FirePower Services document.
Supported

- Network-based AMP (File transfer traffic passing through ASA device will be analyzed by AMP signature)
- Improved system learning by regularly updating the signature database from the Cisco Cloud.

Malware Graphs and Widgets

If you click through to the FirePower Manager from the MSA portal, the following graphs show you information about malware.

- Top File types
- Top File names
- Malware detected

Not Covered

- End host AMP
- Telemetry and Tejectory reports.
URL Filtering

URL filtering feature allows to determine the traffic that traverses a network based on non-encrypted URL requests.

Supported

- Network-based URL filtering based on categories and reputation.
- There are regular URL database updates from the Cisco Cloud.

**Note:** Changes to the URL filtering policy must go the through the change request process.

URL Filtering and Reputation Categories

- Well known
- Benign site
- Benign site with security risks
- Suspicious site
- High Risk site

URL Graphs and Widgets

- Traffic by URL
- Traffic by Category
- Traffic by Reputation

Not Covered

- User-based URL filtering with integration with end-customer LDAP server
- Captive portal integration with LDAP server
Application Visibility Control

Supported

Network-based Application Visibility Control

Application Visibility
Graphs and Widgets

Application Visibility reports are available for Application Protocol, Client Application, and Web Application

- Traffic by Risk and Application
- Intrusion Events by Risk and Application
- Hosts by Risk and Application
- Application details with risk level, category, and number of hosts.

Network Information
Graphs and Widgets

- Operating Systems
- Traffic by Source IP
- Traffic by Destination IP
- Connections by Access Control Action
- Traffic and Intrusion Events over Time

Security Intelligence
Graphs and Widgets

- Security Intelligence Traffic by Category
- Security Intelligence Traffic by Source IP
- Security Intelligence Traffic by Destination IP

Not Covered

User-based application control
Intrusion Prevention

Supported

Intrusion access policies are configured in the SKA. Your options are:

- No Intrusion Prevention Service
- Maximum Detection: Enables maximum intrusion detection and shows events about intrusion attempts.

**Note** Maximum Detection does not drop traffic and intrusion attempts. Instead, 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

**Note:** Changes to intrusion policies must go through the change management process.

**Intrusion Graphs and Widgets**

**Indication of Compromise**
- Hosts by indications
- Indications by hosts
- Intrusion Events by Priority

**Intrusion Information**
- Top Attackers graph
- Top Targets IP graph
FirePower Manager Tabs, Graphs, and Widgets

This section lists the supported graphs and widgets that you will see in the FirePower Manager. For the Cox Communications implementation of the MSA portal, the FirePower Manager is where you will see security data about your network and ASA devices.

The FirePower Manager aggregates and correlates intrusion, file, malware, discovery, connection, and performance data, and then assesses the impact of events on particular hosts and tagging hosts with indications of compromise. This enables you to monitor the information that your device reports and to assess the overall activity that occurs on your network.

When you click the Detailed Security Metrics button in the MSA portal, the FirePower Manager opens and the following tabs appear:

- Overview tab
- Analysis tab

Each tab contains widgets and graphs that provide you with information about your devices and your firewall security.

Tips
Hover

If you hover over a point on any graph, you will see more information about the specific event.
**Double-click**

If you double-click a graph, you will see a menu of options specific to the graph.

![Graph Options](image)

**Add Filter**

If you select **Add Filter**, a filter bar displays at the top of the “content explorer” in any tab. Select the button to see a list of filters you can apply.

![Filter Options](image)

**Note:** Filter conditions are case-sensitive, so check your entries carefully; all lower-case criteria will not return any results.
Example

To filter application data for risk level, select Application Risk in the Data Type list. In the Filter field, type Medium, High, Very High, and click OK.

Add Exclude Filter

Shows all data not associated with the excluded value. Exclude filters display an exclamation value (!) before the filter value.

Drill into Analysis

Enables you to drill down to the table views of the relevant data if you want to examine graph or list data in more detail than the Context explorer option allows.

View Host Information

Enables you to choose a data point with a specific IP address and view host information of that IP address.

Whois

Allows you to choose a data point with a specific IP address and make a whois search on that address.
Overview Tab—Summary Dashboard

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The first tab you see in the FirePower Manager is the Overview—Summary Dashboard tab, which contains widgets and graphs that together offer a complete overview of FirePower data on your monitored network.

There are four subtabs that give you an at-a-glance picture of recent trends in your network’s activity. The four subtabs are:

- Network
- Threats
- Intrusion Events
- Geolocation

**Note:** This dashboard only displays data for ASA devices.

**Network Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Unique Applications Over Time**

Displays a graph of total unique applications detected on your monitored network over the dashboard time range.
Traffic by Application Risk
Displays estimated risk levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level for the selected time period.

Risk is determined by how likely it is that the application will be used for purposes that violate your organization’s security policy.

Note: The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.

Traffic by Business Relevance
Displays estimated business relevance levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level over the dashboard time range.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance. Business Relevance is assigned by Cisco, by looking into its own vulnerability database.

Note: The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.
Traffic by Application Category
Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.

Top Web Applications Seen
Displays web applications on your monitored network, based on total kilobytes of data transmitted by the web application itself.
Top Server Applications Seen

Displays server applications on your monitored network, based on the number of hosts running the service.

![Top Server Applications Seen](image)

Risky Applications with Low Business Relevance

Displays all application connections on your monitored network that have both high application risk level and low estimated business relevance.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance. Business Relevance is assigned by Cisco, by looking into its own vulnerability database.

Note: The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.
Connections by URL Reputation

Displays all application connections on your monitored network, grouped by URL reputation.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

- Intelligence Feed, which contains several regularly updated collections of IP addresses.
- DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs.

*Intelligence Feeds*

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Top Client Applications Seen
Displays client applications on your monitored network, based on total kilobytes of data transmitted by the client application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Total Bytes (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>2,090,044.59</td>
</tr>
<tr>
<td>Firefox</td>
<td>767,746.47</td>
</tr>
<tr>
<td>Google Toolbar</td>
<td>70,982.66</td>
</tr>
<tr>
<td>PHP</td>
<td>51,137.52</td>
</tr>
<tr>
<td>Yahoo</td>
<td>34,992.15</td>
</tr>
<tr>
<td>Wiki</td>
<td>27,116.94</td>
</tr>
<tr>
<td>ABC</td>
<td>25,986.39</td>
</tr>
<tr>
<td>Links</td>
<td>25,123.07</td>
</tr>
<tr>
<td>Flipboard</td>
<td>23,935.41</td>
</tr>
<tr>
<td>TED</td>
<td>22,055.09</td>
</tr>
<tr>
<td>Twitter</td>
<td>14,424.61</td>
</tr>
<tr>
<td>Facebook</td>
<td>11,227.47</td>
</tr>
<tr>
<td>Advanced Packaging Tool</td>
<td>9,931.36</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>7,406.41</td>
</tr>
<tr>
<td>HeartRadio</td>
<td>3,365.53</td>
</tr>
</tbody>
</table>

Last updated 3 hours, 4 minutes ago
Top Operating Systems Seen
Displays operating systems on your monitored network, based on the number of network hosts with the operating system.

<table>
<thead>
<tr>
<th>OS Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>332</td>
</tr>
<tr>
<td>Mac OSX</td>
<td>175</td>
</tr>
<tr>
<td>Windows</td>
<td>67</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>8</td>
</tr>
<tr>
<td>AIX</td>
<td>3</td>
</tr>
<tr>
<td>ESXi</td>
<td>3</td>
</tr>
<tr>
<td>Android</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 3 hours, 5 minutes ago

Connections by URL Category
Displays all application connections on your monitored network, grouped by URL category.

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>News and Media</td>
<td>23,973</td>
</tr>
<tr>
<td>Computer and Internet Security</td>
<td>3,980</td>
</tr>
<tr>
<td>Social Network</td>
<td>2,808</td>
</tr>
<tr>
<td>Internet Portals</td>
<td>2,276</td>
</tr>
<tr>
<td>Philosophy and Political Advocacy</td>
<td>1,790</td>
</tr>
<tr>
<td>Religion</td>
<td>1,772</td>
</tr>
<tr>
<td>Business and Economy</td>
<td>1,868</td>
</tr>
<tr>
<td>Society</td>
<td>1,507</td>
</tr>
<tr>
<td>Computer and Internet Info</td>
<td>1,216</td>
</tr>
<tr>
<td>Entertainment and Arts</td>
<td>1,131</td>
</tr>
</tbody>
</table>

Last updated 3 hours, 6 minutes ago
**Threats Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Indications of Compromise by Host**

Displays the hosts on your network that are the most likely to be compromised, grouped by associated host IP address. Indicators of Compromise are a quick and easy way to identify which hosts might have been exploited.

**Malware Threats**

Displays the number of malware threats detected in network traffic by the system and grouped by threat name.

**Note:** When a graph contains no data, it means that no malware was found during the selected time period; it does not indicate a problem with the device itself.
New Indications of Compromise Over Time

Displays a graph of new indications of compromise detected over the dashboard time range.
Intrusion Events

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from most severe to least severe. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

Note: All events trigger a notification to technical support to investigate and resolve the event.

- Impact 0: Neither the source or the destination host is on a monitored network.
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- Impact 2: The host is potentially vulnerable.
- Impact 3: The host is currently not vulnerable.
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map.
Intrusion Events Subtab

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Top Attackers**

Displays attacking host IP addresses on your monitored network, based on the number of intrusion events where the listed IP address was the attacker in the connection that caused the event.

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>70.62.115.162</td>
<td>149</td>
</tr>
<tr>
<td>96.10.162.4</td>
<td>103</td>
</tr>
<tr>
<td>97.77.44.5</td>
<td>60</td>
</tr>
<tr>
<td>96.10.39.66</td>
<td>49</td>
</tr>
<tr>
<td>69.75.199.3</td>
<td>41</td>
</tr>
<tr>
<td>98.101.163.122</td>
<td>29</td>
</tr>
<tr>
<td>108.176.89.227</td>
<td>25</td>
</tr>
<tr>
<td>24.106.177.194</td>
<td>23</td>
</tr>
<tr>
<td>173.198.143.98</td>
<td>22</td>
</tr>
<tr>
<td>24.97.220.68</td>
<td>14</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
### Top Targets
Displays destination host IP addresses (where your traffic is going to) on your monitored network, based on the number of intrusion events where the destination host IP address was targeted in the connection that caused the event.

<table>
<thead>
<tr>
<th>Destination IP</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>69.48.211.170</td>
<td>143</td>
</tr>
<tr>
<td>125.209.230.195</td>
<td>56</td>
</tr>
<tr>
<td>185.17.184.11</td>
<td>30</td>
</tr>
<tr>
<td>162.220.223.28</td>
<td>17</td>
</tr>
<tr>
<td>162.220.223.28</td>
<td>14</td>
</tr>
<tr>
<td>46.137.81.66</td>
<td>13</td>
</tr>
<tr>
<td>104.129.204.40</td>
<td>13</td>
</tr>
<tr>
<td>178.77.120.6</td>
<td>12</td>
</tr>
<tr>
<td>52.71.189.2</td>
<td>11</td>
</tr>
<tr>
<td>69.75.199.3</td>
<td>11</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago

### Dropped Intrusion Events
Displays counts for intrusion events, by classification, where the packet was dropped.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Corporate Policy Violation</td>
<td>278</td>
</tr>
<tr>
<td>Attempted Administrator Privilege Gain</td>
<td>253</td>
</tr>
<tr>
<td>A Network Trojan was Detected</td>
<td>84</td>
</tr>
<tr>
<td>Attempted Information Leak</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
All Intrusion Events

Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.
Intrusion Events

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from least severe to most severe. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

Note: All events trigger a notification to technical support to investigate and resolve the event.

- Impact 0: Neither the source or the destination host is on a monitored network.
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- Impact 2: The host is potentially vulnerable.
- Impact 3: The host is currently not vulnerable.
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map.
**Total Events by Application Protocol**

Displays application protocols on your monitored network, based on the number of intrusion events associated with the application protocol.

<table>
<thead>
<tr>
<th>Application</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>1,213</td>
</tr>
<tr>
<td>DynGate</td>
<td>244</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>244</td>
</tr>
<tr>
<td>HTTPS</td>
<td>10</td>
</tr>
<tr>
<td>HL7</td>
<td>8</td>
</tr>
<tr>
<td>Snapchat</td>
<td>8</td>
</tr>
<tr>
<td>Facebook</td>
<td>2</td>
</tr>
<tr>
<td>SSL</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago

**Impact 1 Events by Application Protocol**

The number of events that indicate that the host is vulnerable (impact 1). The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 1 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>84</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
Impact 2 Events by Application Protocol

The number of events that indicate the host is potentially vulnerable (not as serious as impact 1) grouped by application protocol.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 2 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>416</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>95</td>
</tr>
<tr>
<td>DynGate</td>
<td>95</td>
</tr>
<tr>
<td>HTTPS</td>
<td>4</td>
</tr>
<tr>
<td>HL7</td>
<td>4</td>
</tr>
<tr>
<td>Snapchat</td>
<td>3</td>
</tr>
<tr>
<td>SSL</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
**Geolocation Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Intrusion Events by Source Country**

Displays countries where intrusion events originated, based on the number of events originating from each country. The +1 and -1 indicate an increase and a decrease in ranking, respectively.

<table>
<thead>
<tr>
<th>Source Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>550</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>22</td>
</tr>
<tr>
<td>CHN (China)</td>
<td>20</td>
</tr>
<tr>
<td>BRA (Brazil)</td>
<td>6</td>
</tr>
<tr>
<td>DEU (Germany)</td>
<td>4</td>
</tr>
<tr>
<td>ECU (Ecuador)</td>
<td>4</td>
</tr>
<tr>
<td>KAZ (Kazakhstan)</td>
<td>4</td>
</tr>
<tr>
<td>RUS (Russian Federation)</td>
<td>3</td>
</tr>
<tr>
<td>FRA (France)</td>
<td>2</td>
</tr>
<tr>
<td>MEX (Mexico)</td>
<td>2</td>
</tr>
</tbody>
</table>
Intrusion Events by Destination Country

Displays destination countries (where the traffic from your network is going to) targeted by intrusion events. Countries are listed based on the amount of destination traffic where intrusion events were detected.

### Intrusion Events by Destination Country

<table>
<thead>
<tr>
<th>Destination Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>420</td>
</tr>
<tr>
<td>DEU (Germany)</td>
<td>109</td>
</tr>
<tr>
<td>KOR (South Korea)</td>
<td>56</td>
</tr>
<tr>
<td>IRL (Ireland)</td>
<td>25</td>
</tr>
<tr>
<td>BRA (Brazil)</td>
<td>3</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>3</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>3</td>
</tr>
<tr>
<td>AUT (Austria)</td>
<td>2</td>
</tr>
<tr>
<td>DNK (Denmark)</td>
<td>1</td>
</tr>
<tr>
<td>POL (Poland)</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago

Intrusion Events by Source Continent

Displays continents where intrusion events originated (the traffic came to your network), based on the number of events originating from each continent.

### Intrusion Events by Source Continent

<table>
<thead>
<tr>
<th>Source Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>552</td>
</tr>
<tr>
<td>Europe</td>
<td>31</td>
</tr>
<tr>
<td>Asia</td>
<td>25</td>
</tr>
<tr>
<td>South America</td>
<td>10</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago
Intrusion Events by Destination Continent

Displays destination continents (where the traffic from your network is going to) targeted by intrusion events. Continents are listed based on the amount of destination traffic where intrusion events were detected.

<table>
<thead>
<tr>
<th>Destination Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>420</td>
</tr>
<tr>
<td>Europe</td>
<td>145</td>
</tr>
<tr>
<td>Asia</td>
<td>57</td>
</tr>
<tr>
<td>South America</td>
<td>3</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago
Overview Tab—Application Statistics Dashboard

**Note:** This dashboard only displays data for ASA devices.

**Connections Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Allowed Connections by Application**

Displays allowed application connections on your monitored network, grouped by application.

![Allowed Connections by Application Table]

*Last updated less than a minute ago*
Denied Connections by Application

Displays denied connections on your monitored network, grouped by application.

Unique Applications over Time

Displays a graph of total unique applications detected on your monitored network over the dashboard time range.
Allowed Connections by Application Risk

Displays allowed application connections on your monitored network, grouped by application risk level.

Risk is determined by how likely it is that the application will be used for purposes that violate your organization’s security policy.

Note: The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.
**Allowed Connections by Business Relevance**

Displays allowed application connections on your monitored network, grouped by estimated relevance to business activity.

Business Relevance is the likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance. Business Relevance is assigned by Cisco, by looking into its own vulnerability database.

**Note:** The assignment of risk and business relevance are maintained by Cisco's Security Intelligence.

<table>
<thead>
<tr>
<th>Business Relevance</th>
<th>Allowed Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>875</td>
</tr>
<tr>
<td>Medium</td>
<td>810</td>
</tr>
<tr>
<td>Low</td>
<td>425</td>
</tr>
<tr>
<td>High</td>
<td>15</td>
</tr>
<tr>
<td>Very Low</td>
<td>8</td>
</tr>
</tbody>
</table>

Last updated 2 minutes ago
Traffic by Application

Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.

Traffic by Application Category

Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.
Intrusion Events Subtab

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

### Dropped Events by Application

Displays dropped intrusion events, grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Dropped Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>615</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>226</td>
</tr>
<tr>
<td>Web browser</td>
<td>145</td>
</tr>
<tr>
<td>DynGate</td>
<td>121</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>121</td>
</tr>
<tr>
<td>Mobile Safari</td>
<td>74</td>
</tr>
<tr>
<td>Casale</td>
<td>55</td>
</tr>
<tr>
<td>Apple sites</td>
<td>35</td>
</tr>
<tr>
<td>Chrome</td>
<td>30</td>
</tr>
<tr>
<td>Media Stream Daemon</td>
<td>9</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago
### Impact 3 Events by Application
Displays number of events where the host is not vulnerable (impact 3) grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 3 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>14</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>+1</td>
</tr>
<tr>
<td>DynGate</td>
<td>+1</td>
</tr>
<tr>
<td>Web browser</td>
<td>-1</td>
</tr>
<tr>
<td>Media Stream Daemon</td>
<td></td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago

### Impact 1 Events by Application
Displays number of events where the host is vulnerable (impact 1) grouped by application. The source or destination host is potentially compromised by a virus, trojan, or other piece of malicious software.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 1 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>94</td>
</tr>
<tr>
<td>Web browser</td>
<td>62</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>32</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago
Impact 4 Events by Application
Displays number of events of estimated impact level 4 grouped by application.

Impact 4 means either the source or destination host is on a monitored network, but there is no entry for the host in the network map.

Total Events by Application
Displays applications on your monitored network, based on the number of intrusion events generated by the application.
**Impact 2 Events by Application**

Displays number of events where the host is *potentially* vulnerable (impact 2) grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 2 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>416</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>162</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>95</td>
</tr>
<tr>
<td>DynGate</td>
<td>95</td>
</tr>
<tr>
<td>Web browser</td>
<td>72</td>
</tr>
<tr>
<td>Mobile Safari</td>
<td>42</td>
</tr>
<tr>
<td>Chrome</td>
<td>29</td>
</tr>
<tr>
<td>Media Stream Daemon</td>
<td>8</td>
</tr>
<tr>
<td>Safari</td>
<td>5</td>
</tr>
<tr>
<td>HTTPS</td>
<td>4</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago
Impact 0 Events by Application

Displays number of events of estimated impact level 0 grouped by application.

Impact 0 means neither the source nor the destination host is on a network that is monitored by network discovery.

**Note:** When this graph contains no data, it means that no events were detected during the selected time range; it does not indicate a problem with the device itself.
Overview Tab—Connection Summary Dashboard

**Note:** This dashboard only displays data for ASA devices.

**Connections Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Connections by Initiator IP**

Displays host IP addresses on your monitored network, based on the number of connections where that IP address on a host initiated the session.
**Connections by Responder IP**

Displays host IP addresses on your monitored network, based on the number of connections where the responder in that session was that IP address on a host. The output of this widget varies when there is an increase in connections from a specific responder IP.

**Connections Over Time**

Displays a graph of the total number of connections on your monitored network, over the dashboard time range.
Connections by Port

Displays ports on your monitored network, based on the number of detected connections.

Connections by Applications

Displays applications on your monitored network, based on the number of detected connections.
Traffic Subtab

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Traffic by Initiator IP**

Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.
Traffic by Responder IP

Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies when there is an increase in connections from a specific responder IP.

Traffic Over Time

Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.
Traffic by Port

Displays responder ports on your monitored network, based on total kilobytes of data transmitted on your monitored network via each port over the dashboard time range. The output of this widget varies according to your connection logging configuration.

Traffic by Application

Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
Geolocation Subtab

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Connections by Source Country

Displays countries communicating with your monitored network, based on the number of connections initiated from each country.

<table>
<thead>
<tr>
<th>Initiator Country</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1 USA (United States)</td>
<td>88,635</td>
</tr>
<tr>
<td>-1 BRA (Brazil)</td>
<td>5,277</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>43</td>
</tr>
<tr>
<td>AUS (Australia)</td>
<td>31</td>
</tr>
<tr>
<td>EUR (Europe (unknown Country))</td>
<td>31</td>
</tr>
<tr>
<td>IRL (Ireland)</td>
<td>30</td>
</tr>
<tr>
<td>CHN (China)</td>
<td>24</td>
</tr>
<tr>
<td>CZE (Czech Republic)</td>
<td>12</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>9</td>
</tr>
<tr>
<td>ITA (Italy)</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago
Connections by Destination Country
Displays countries communicating with your monitored network (traffic is coming to you), based on the number of connections.

Connections by Source Continent
Displays continents your monitored network is communicating with (you are sending traffic), based on the number of connections initiated from each continent.
Connections by Destination Continent

Displays continents that sent connections to your monitored network (traffic is coming to you), based on the number of connections.

Traffic by Source Continent

Displays continents sending data to your monitored network, based on total kilobytes of data transmitted from each continent during the selected time range.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.
Traffic by Destination Continent

Displays continents contacted from your monitored network (you sent traffic), based on total kilobytes of data transmitted to each continent during the selected time range.

Traffic by Source Country

Displays countries transmitting data to your monitored network (traffic is coming to you), based on total kilobytes of data transmitted from each country during the selected time range.
Traffic by Destination Country

Displays countries contacted from your monitored network, based on total kilobytes of data transmitted on your monitored network to each country over the dashboard time range.
**URL Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Allowed Connections by URL Category**

Displays allowed application connections on your monitored network, grouped by URL category.
Denied Connections by URL Category

Displays denied connections on your monitored network, grouped by URL category.

Traffic by URL Category

Displays application URL categories on your monitored network, based on total kilobytes of data exchanged with URLs of each category over the dashboard time range.
Traffic by URL Reputation

Displays application URL reputation types on your monitored network, based on total kilobytes of data exchanged with URLs of each reputation over the dashboard time range.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

- Intelligence Feed, which contains several regularly updated collections of IP addresses.
- DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs.

Intelligence Feeds

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Allowed connections by URL Reputation

Displays allowed application connections on your monitored network, grouped by URL reputation.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

- Intelligence Feed, which contains several regularly updated collections of IP addresses.
- DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs.

Intelligence Feeds

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.
Denied Connections by URL Reputation

Displays denied connections on your monitored network, grouped by URL reputation.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

- **Intelligence Feed**, which contains several regularly updated collections of IP addresses.
- **DNS and URL Intelligence Feed**, which contains several regularly updated collections of domain names and URLs.

**Intelligence Feeds**

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.

![Denied Connections by URL Reputation](image-url)
Overview Tab—Detailed Dashboard

**Note:** This dashboard only displays data for ASA devices.

**Intrusion Events Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Intrusion Events**

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority from most severe to least severe. This includes statistics on intrusion events with dropped packets.

On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

**Note:** All events trigger a notification to technical support to investigate and resolve the event.

- Impact 0: Neither the source or the destination host is on a monitored network.
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- Impact 2: The host is potentially vulnerable.
- Impact 3: The host is currently not vulnerable.
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map.
All Intrusion Events
Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.

All Intrusion Events (Not Dropped)
Displays the most frequently occurring types of intrusion events, by classification, where the packet was not dropped as part of the event.
Dropped Intrusion Events

Displays counts for intrusion events, by classification, where the packet was dropped.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted Administrator Privilege Gain</td>
<td>962</td>
</tr>
<tr>
<td>Potential Corporate Policy Violation</td>
<td>653</td>
</tr>
<tr>
<td>A Network Trojan was detected</td>
<td>464</td>
</tr>
<tr>
<td>Attempted Information Leak</td>
<td>2</td>
</tr>
<tr>
<td>Web Application Attack</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 7 minutes ago

Intrusion Events Requiring Analysis

Displays a count of intrusion events requiring analysis, based on event classification.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.

Last updated 3 minutes ago
**Context Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Servers**

Displays servers, by number of hosts.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>476</td>
</tr>
<tr>
<td>nginx</td>
<td>324</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>175</td>
</tr>
<tr>
<td>cloudflare-nginx</td>
<td>119</td>
</tr>
<tr>
<td>AmazonS3</td>
<td>103</td>
</tr>
<tr>
<td>CloudFront</td>
<td>25</td>
</tr>
<tr>
<td>Apache-Coyote</td>
<td>26</td>
</tr>
<tr>
<td>Akamai Ghost</td>
<td>23</td>
</tr>
<tr>
<td>BigIP</td>
<td>11</td>
</tr>
<tr>
<td>Sucuri</td>
<td>10</td>
</tr>
</tbody>
</table>

Last updated 4 minutes ago
Operating Systems
Displays operating systems, based on the number of hosts running each operating system within your network.

Clients
Displays clients on your monitored network, by type.
Traffic by Application
Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.

Traffic by Initiator IP
Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.
Traffic by Responder IP

Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies when there is an increase in connections from a specific responder IP.

Traffic Over Time

Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.
Overview Tab—Files Dashboard

**Note:** This dashboard only displays data for ASA devices.

**Malware Subtab**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Hosts Receiving Malware**
Displays the number of malware files received by host IP addresses on your network, grouped by IP address.

![Hosts Receiving Malware](image)

**Hosts Sending Malware**
Displays the number of malware files sent from host IP addresses on your network, grouped by IP address.

![Hosts Sending Malware](image)
Application Protocols Introducing Malware
Displays the number of malware files transmitted over your network, grouped by the application protocol used to transmit the files.

Client Applications introducing Malware
Displays the applications, or parent files, that accessed or created malware detected by the FirePower Advanced Malware protection tool.
Web Applications Introducing Malware
Displays web applications on your monitored network that accessed or created malware detected by the FirePower Advanced Malware protection tool.

Possible Zero Day Malware
Displays the captured files most likely to be zero-day malware, with a file disposition of unknown and either High or Very High threat scores, based on the number of times the file was seen.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.
**Malware Threats**

Displays the number of malware threats detected either in network traffic by the system or by FirePower, grouped by threat name.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.
Threat Detections Over Time
Displays a graph of the total number of malware threats detected either in network traffic by the system or by FirePower, over the dashboard time range.

Top Threats
Displays the distribution of threat scores, based on the number of stored files with that threat score.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.
**Malware Intrusions**
Displays intrusion events, based on the number of intrusion events occurring in connections transmitting malware.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.

**File Types Infected with Malware**
Displays the number of malware detected either in network traffic by the system or by FirePower, grouped by file type.
Processes Introducing Malware

Displays the system processes that accessed or created malware detected by FirePower.

Note: When a graph contains no data, it means that the device did not send any information to FirePower Manager for the time range selected; it does not indicate a problem with the device itself.

Files Subtab

Warning: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Hosts Receiving Files

Displays the number of files received (downloaded) by host IP addresses on your network, grouped by IP address.
Hosts Sending Files
Displays the number of files sent (uploaded) from host IP addresses on your network, grouped by IP address.

Applications Protocols Transferring File
Displays the number of files transmitted over your network, grouped by the application protocol used to transmit the files.
Client Applications Transferring files
Displays the applications, or parent files, that transmitted files over your network.

<table>
<thead>
<tr>
<th>Client</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>3,259</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>80</td>
</tr>
<tr>
<td>Firefox</td>
<td>33</td>
</tr>
<tr>
<td>Web browser</td>
<td>2</td>
</tr>
<tr>
<td>Flipboard</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 19 minutes ago

Web Applications Transferring Files
Displays the number of files transmitted over your network, grouped by the web application used to transmit the files.

<table>
<thead>
<tr>
<th>Web Application</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browsing</td>
<td>3,316</td>
</tr>
<tr>
<td>RealClearPolitics</td>
<td>36</td>
</tr>
<tr>
<td>CNN.com</td>
<td>16</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>2</td>
</tr>
<tr>
<td>C-SPAN</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 20 minutes ago
File Transfers Over Time

Displays a graph of the total number of file transfers detected in network traffic by the system, over the dashboard time range.

File Dispositions

Displays the number of files detected in network traffic as a result of Malware Cloud Lookup file rules, grouped by malware disposition. A local lookup is performed first; then for any unknown files, FirePower performs a cloud lookup and stores the information locally.
File Actions
Displays the number of files transmitted over your network, grouped by the file rule actions used to handle the files.

![File Actions Table]

File Categories
Displays the number of files transmitted over your network, grouped by file category.

![File Categories Table]

File Types
Displays the number of files transmitted over your network, grouped by file type.

![File Types Table]
File Names
Displays the number of files transmitted over your network, grouped by file name.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>.icar.com</td>
<td>3,248</td>
</tr>
<tr>
<td>3bebb2_b53ce6b673c14cdeb9d63832bd7e74cb...</td>
<td>12</td>
</tr>
<tr>
<td>3bebb2_dd69ad4f4af34206959d7de0f07995e2...</td>
<td>8</td>
</tr>
<tr>
<td>2016 Reuters Tracking - Core Political S...</td>
<td>5</td>
</tr>
<tr>
<td>BGGWTarranceGroupLakeResearch.pdf</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 21 minutes ago
Analysis Tab

The Analysis tab in FirePower is divided into sections that show you even more details about events and trends you might see on the dashboards on the Overview tab.

The Analysis tab includes the following subtabs:

- Context Explorer
- Connections
- Intrusions
- Files
- Hosts

**Note:** This tab only displays data for ASA devices.

Context Explorer Tab

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The Context Explorer tab contains details that help you to understand more information and gather data to determine the best needs for your company. This section explains the parts of the Context Explorer and the graphs contained in each section.

**Traffic and Intrusion Events Over Time**

At the top of the Context Explorer is a line chart of traffic and intrusion events over time. The X-axis (horizontal line) plots time intervals, which range from five minutes to one month, depending on the selected time window. The Y-axis (vertical line) plots traffic in kilobytes (blue line) and intrusion event counts (red line).

By default, this section shows all network traffic and all generated intrusion events for the selected time range. If you apply filters, the chart changes to display only traffic and intrusion events associated with the specified filters.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**Indications of Compromise**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Hosts by Indication**

The Hosts by Indication pie chart displays a proportional view of the Indications of Compromise triggered by hosts on your monitored network.

- The inner ring divides by category (such as Command and Control Connected or Malware Detected).
- The outer ring divides data by specific event type.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Indications by Host

Indications by Host bar graph displays the IP addresses and counts of unique Indications of Compromise triggered by the top 15 most active users on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

The other sections are sets of interactive graphs that you can click to see lists that provide greater detail for indications of compromise, network, application, intrusion, file, geolocation, and URL data.

Note: All the sections on the Analysis tab combined together are called the Context Explorer.
Network Information

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

This section contains interactive graphs on monitored network information.

**Operating Systems**

The Operating Systems pie graph shows you the operating systems running on your network.

- Inner ring shows groups of operating systems, such as Windows.
- Outer ring shows details about versions of the operating systems, such as Windows XP.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Source IP

The Traffic by Source IP bar graph shows you the IP addresses of the users on your network who generate the most traffic. Blue bars represent source IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Destination IP

The Traffic by Destination IP bar graph shows you the top destination addresses for traffic leaving your network. Blue bars represent the destination IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Connections by Access Control Action

The Connections by Access Control Action pie graph, displays a proportional view of the access control actions (determined when the security policy is defined) taken the most regarding your network traffic.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Source User

The Traffic by Source User graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source users on your monitored network. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**Application Protocol Information**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The Application Protocol Information section displays application groups together by type. Charts are color-coded to indicate the risk level and business relevance for each type of application.

For example, there can be traffic that is exposing your network to risk, but has little or no business relevance. This could lead to policies and decisions about what types of traffic to keep out of your network.

**Intrusion Events by Risk and Application**

The Intrusion Events by Risk and Application donut graph displays the applications by intrusion events and is arranged by the applications' estimated risk (default) or by estimated business relevance.

- The inner ring represents estimated risk- or business-relevance level (such as Medium or High).
- The outer ring shows you the actual applications that represent the risk.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance. Business Relevance is assigned by Cisco, by looking into its own vulnerability database.

**Note:** The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.
Hosts by Risk and Application

The Hosts by Risk and Application donut graph displays the applications used most by your users and is arranged by the applications’ estimated risk (default) or by estimated business relevance.

- The inner ring represents estimated risk- or business-relevance level (such as Medium or High).
- The outer ring shows you the actual applications that represent the risk.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

Business Relevance is the likelihood that the application is being used within the context of your organization’s business operations, as opposed to recreationally. Example: Gaming applications tend to have a very low business relevance. Business Relevance is assigned by Cisco, by looking into its own vulnerability database.

**Note:** The assignment of risk and business relevance are maintained by Cisco’s Security Intelligence.
**Application Details List**

The Application Detail List displays below the Risk and Application graphs. In this list you can see all the identified applications from each graph with the application’s name, Risk, Business Relevance, Category, and numbers of hosts.

<table>
<thead>
<tr>
<th>Application Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Firefox</td>
</tr>
<tr>
<td>Chrome</td>
</tr>
<tr>
<td>Google Analytics</td>
</tr>
<tr>
<td>Skype</td>
</tr>
<tr>
<td>Microsoft CryptoKit</td>
</tr>
<tr>
<td>Google Apps Authentic</td>
</tr>
<tr>
<td>Adobe Software</td>
</tr>
<tr>
<td>Facebook</td>
</tr>
<tr>
<td>Internet Explorer</td>
</tr>
</tbody>
</table>

**Intrusion Information**

**Warning**: Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Intrusion Events by Impact**

The Intrusion Events by Impact pie chart displays a proportional view of intrusion events on your monitored network, grouped by estimated impact level; 0 is the least impactful and 4 is the most impactful.

- Impact 0: Neither the source or the destination host is on a monitored network.
- Impact 1: The host is vulnerable. The source or destination host is potentially compromised by a virus, Trojan, or other piece of malicious software.
- Impact 2: The host is potentially vulnerable.
- Impact 3: The host is currently not vulnerable.
- Impact 4: The source or the host is on a monitored network, but there is no entry for the host in the network map.
Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

**Top Attackers Graph**

The Top Attackers bar graph shows the IP addresses sorted by the number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Intrusion Events by Priority

The Intrusion Events by Priority graph, in pie form, displays a proportional view of intrusion events on your monitored network, grouped by estimated priority level (such as High, Medium, or Low).

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.
Top Targets Graph

The Top Targets bar graph shows the top 10 target host IP addresses sorted by number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**File Information**

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

**Top File Types**

The Top File Types donut graph displays a view of detected file types associated with malware.

- The outer ring shows file types detected in network traffic.
- The inner ring shows the file types grouped by category.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on information.
Top Hosts Sending Files

The Top Hosts Sending Files or Malware graph shows the top IP addresses of users sending malware or the top users sending files across your network.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Top File Names

The Top File Names bar graph shows the names of the files affected by malware that were detected in network traffic.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Top Hosts Receiving Files

The Top Hosts Receiving Files graph shows the IP addresses of the users who receive the most files.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Files by Disposition

Shows the status of the files that were detected by the network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Top Malware Detections

Shows the Point to a bar in the graph to see detailed information about the malware, such as the threat name and the number of files that contain the selected malware.
**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

Geolocation Information section contains three interactive donut graphs that display an overall picture of countries with which hosts on your monitored network are exchanging data: unique connections by initiator or responder country, intrusion events by source or destination country, and file events by sending or receiving country.

### Connections by Initiator Country

The Connections by Initiator/Responder Country donut graph displays a proportional view of the countries involved in connections on your network as either the initiator (the default) or the responder.

- The inner ring groups the connections by continent.
- The outer ring groups the connections by country.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Intrusion Events by Source Country

The Intrusion Events by Source Country donut graph displays countries targeted by intrusion events, based on the number of events associated with each country.

- The inner ring groups the connections by continent.
- The outer ring groups the connections by country.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
File Events by Sending Country

The File Events by Sending/Receiving Country donut graph displays a proportional view of the countries detected in file events on your network as either sending (the default) or receiving files.

- The inner ring groups the connections by continent.
- The outer ring groups the connections by country.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
URL Information

**Warning:** Do not attempt to delete or add graphs to this tab and its subtabs. When you change a graph, it changes for your entire organization and requires Technical Support intervention to reverse the change.

The URL Information section contains three interactive bar graphs that display an overall picture of the URLs that the hosts on your monitored network use to exchange data.

These graphs show you traffic and unique connections associated with URLs, sorted by:

- Separate URLs
- URL category
- URL reputation

Note: You must have enable URL Filtering for these graphs to include URL category and URL reputation data. Contact Cox Business to set up these filtering options for you.

**Traffic by URL**

The Traffic by URL bar graph shows network traffic in kilobytes per second and unique connections for most-requested URLs on your monitored network. For each URL listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Traffic by URL Category

The Traffic by URL Category bar graph shows network traffic in kilobytes per second and unique connections for the most-requested URL categories on your monitored network. For each URL category listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Traffic by URL Reputation

The Traffic by URL Reputation bar graph shows network traffic in kilobytes per second and unique connections for the most requested URL reputation groups on your monitored network. For each URL reputation listed, blue bars represent traffic data and red bars represent connection data.

The URL reputations are:

- Well known
- Benign site
- Benign with Security Risk
- Suspicious Site
- High Risk

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

URL reputation is determined by how likely a web site is to be used for purposes that might be against your organization’s security policy. Cisco provides feeds which contain IP addresses, domain names, and URLs with poor reputation, as determined by Cisco’s Security Intelligence. The two feeds are:

- Intelligence Feed, which contains several regularly updated collections of IP addresses.
- DNS and URL Intelligence Feed, which contains several regularly updated collections of domain names and URLs.
**Intelligence Feeds**

Because malicious IP addresses, domain names, and URLs that represent security threats (malware, spam, botnets, and phishing) can appear and disappear faster than you can update and deploy new policies, the Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses, and so on. Cisco continually updates its threat intelligence feeds with new URLs, domain names, and IP addresses, as well as new categories and risks for existing URLs, to ensure that our system uses the most up-to-date threat information to filter your network traffic.