

Threat Detection

The following topics describe how to configure threat detection statistics and scanning threat detection.

- Detecting Threats, on page 1
- Guidelines for Threat Detection, on page 4
- Defaults for Threat Detection, on page 4
- Configure Threat Detection, on page 5
- Monitoring Threat Detection, on page 9
- History for Threat Detection, on page 13

Detecting Threats

Threat detection on the ASA provides a front-line defense against attacks. Threat detection works at Layer 3 and 4 to develop a baseline for traffic on the device, analyzing packet drop statistics and accumulating "top" reports based on traffic patterns. In comparison, a module that provides IPS or Next Generation IPS services identifies and mitigates attack vectors up to Layer 7 on traffic the ASA permitted, and cannot see the traffic dropped already by the ASA. Thus, threat detection and IPS can work together to provide a more comprehensive threat defense.

Threat detection consists of the following elements:

- Different levels of statistics gathering for various threats.

  Threat detection statistics can help you manage threats to your ASA; for example, if you enable scanning threat detection, then viewing statistics can help you analyze the threat. You can configure two types of threat detection statistics:

  - Basic threat detection statistics—Includes information about attack activity for the system as a whole. Basic threat detection statistics are enabled by default and have no performance impact. See Basic Threat Detection Statistics, on page 2.
  - Advanced threat detection statistics—Tracks activity at an object level, so the ASA can report activity for individual hosts, ports, protocols, or ACLs. Advanced threat detection statistics can have a major performance impact, depending on the statistics gathered, so only the ACL statistics are enabled by default. See Advanced Threat Detection Statistics, on page 3.

- Scanning threat detection, which determines when a host is performing a scan. You can optionally shun any hosts determined to be a scanning threat. See Scanning Threat Detection, on page 3.

- Threat Detection for VPN Services, which you can use to protect against the following types of VPN attack from IPv4 addresses:
  - Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning.
  - Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host.
  - Access attempts to invalid VPN services, that is, services that are for internal use only.

  These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service. See Configure Threat Detection for VPN Services, on page 7.

Basic Threat Detection Statistics

Using basic threat detection statistics, the ASA monitors the rate of dropped packets and security events due to the following reasons:

- Denial by ACLs.
- Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
- Connection limits exceeded (both system-wide resource limits, and limits set in the configuration).
- DoS attack detected (such as an invalid SPI, Stateful Firewall check failure).
- Basic firewall checks failed. This option is a combined rate that includes all firewall-related packet drops in this list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.
- Suspicious ICMP packets detected.
- Packets failed application inspection.
- Interface overload.
- Scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
- Incomplete session detection such as TCP SYN attack detected or UDP session with no return data attack detected.

When the ASA detects a threat, it immediately sends a system log message (733100). The ASA tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst rate interval is 1/30th of the average rate interval or 10 seconds, whichever is higher. For each received event, the ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA sends two separate system messages, with a maximum of one message for each rate type per burst period.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Advanced Threat Detection Statistics

Advanced threat detection statistics show both allowed and dropped traffic rates for individual objects such as hosts, ports, protocols, or ACLs.

Caution Enabling advanced statistics can affect the ASA performance, depending on the type of statistics enabled. Enabling host statistics affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Port statistics, however, has modest impact.

Scanning Threat Detection

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, ASA threat detection scanning maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

If the scanning threat rate is exceeded, then the ASA sends a syslog message (733101), and optionally shuns the attacker. The ASA tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst event rate is 1/30th of the average rate interval or 10 seconds, whichever is higher. For each event detected that is considered to be part of a scanning attack, the ASA checks the average and burst rate limits. If either rate is exceeded for traffic sent from a host, then that host is considered to be an attacker. If either rate is exceeded for traffic received by a host, then that host is considered to be a target.

The following table lists the default rate limits for scanning threat detection.

Table 1: Default Rate Limits for Scanning Threat Detection

Average Rate	Burst Rate
5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 120 second period.

Caution The scanning threat detection feature can affect the ASA performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

Guidelines for Threat Detection

Security Context Guidelines

Except for advanced threat statistics and VPN services, threat detection is supported in single mode only. In Multiple mode, TCP Intercept statistics are the only statistic supported.

Types of Traffic Monitored

- For statistics, only through-the-box traffic is monitored; to-the-box traffic is not monitored.
- Traffic that is denied by an ACL does not trigger scanning threat detection; only traffic that is allowed through the ASA and that creates a flow is affected by scanning threat detection.
- For VPN services, only to-the-box traffic from IPv4 addresses is monitored.

Defaults for Threat Detection

Basic threat detection statistics are enabled by default.

The following table lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command in Tools > Command Line Interface.

For advanced statistics, by default, statistics for ACLs are enabled.

For VPN service threat detection, all services are disabled by default.

Table 2: Basic Threat Detection Default Settings

Packet Drop Reason	Trigger Settings	
	Average Rate	**Burst Rate**
• DoS attack detected • Bad packet format • Connection limits exceeded • Suspicious ICMP packets detected	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 20 second period.
	80 drops/sec over the last 3600 seconds.	320 drops/sec over the last 120 second period.
Scanning attack detected	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
	4 drops/sec over the last 3600 seconds.	8 drops/sec over the last 120 second period.

Packet Drop Reason	Trigger Settings	
	Average Rate	Burst Rate
Incomplete session detected such as TCP SYN attack detected or UDP session with no return data attack detected (combined)	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 20 second period.
	80 drops/sec over the last 3600 seconds.	160 drops/sec over the last 120 second period.
Denial by ACLs	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	640 drops/sec over the last 120 second period.
• Basic firewall checks failed • Packets failed application inspection	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	1280 drops/sec over the last 120 second period.
Interface overload	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 20 second period.
	1600 drops/sec over the last 3600 seconds.	6400 drops/sec over the last 120 second period.

Configure Threat Detection

Basic threat detection statistics are enabled by default, and might be the only threat detection service that you need. Use the following procedure if you want to implement additional threat detection services.

Procedure

Step 1 Configure Basic Threat Detection Statistics, on page 5.

Basic threat detection statistics include activity that might be related to an attack, such as a DoS attack.

Step 2 Configure Advanced Threat Detection Statistics, on page 6.

Step 3 Configure Scanning Threat Detection, on page 7.

Step 4 Configure Threat Detection for VPN Services, on page 7.

Configure Basic Threat Detection Statistics

Basic threat detection statistics is enabled by default. You can disabled it, or turn it on again if you disable it.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Threat Detection**.

Step 2 Select or deselect **Enable Basic Threat Detection** as desired.

Step 3 Click **Apply**.

Configure Advanced Threat Detection Statistics

You can configure the ASA to collect extensive statistics. By default, statistics for ACLs are enabled. To enable other statistics, perform the following steps.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Threat Detection**.

Step 2 In the Scanning Threat Statistics area, choose one of the following options:

- **Enable All Statistics**.
- **Disable All Statistics**.
- **Enable Only Following Statistics**.

Step 3 If you chose **Enable Only Following Statistics**, then select one or more of the following options:

- **Hosts**—Enables host statistics. The host statistics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
- **Access Rules** (enabled by default)—Enables statistics for access rules.
- **Port**—Enables statistics for TCP and UDP ports.
- **Protocol**—Enables statistics for non-TCP/UDP IP protocols.
- **TCP-Intercept**—Enables statistics for attacks intercepted by TCP Intercept (to enable TCP Intercept, see Protect Servers from a SYN Flood DoS Attack (TCP Intercept)).

Step 4 For host, port, and protocol statistics, you can change the number of rate intervals collected. In the Rate Intervals area, choose **1 hour**, **1 and 8 hours**, or **1, 8 and 24 hours** for each statistics type. The default interval is **1 hour**, which keeps the memory usage low.

Step 5 For TCP Intercept statistics, you can set the following options in the TCP Intercept Threat Detection area:

- **Monitoring Window Size**—Sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.
- **Burst Threshold Rate**—Sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.

- **Average Threshold Rate**—Sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.

Click **Set Default** to restore the default values.

Step 6 Click **Apply**.

Configure Scanning Threat Detection

You can configure scanning threat detection to identify attackers and optionally shun them.

You can configure the ASA to send system log messages about an attacker or you can automatically shun the host. By default, the system log message 730101 is generated when a host is identified as an attacker. Be sure to except addresses from shunning when you expect a lot of messages from the host. For example, if you have enabled PIM multicast, exempt the PIM routers or PIM messages will be dropped.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Threat Detection**.

Step 2 Select **Enable Scanning Threat Detection**.

Step 3 (Optional) To automatically terminate a host connection when the ASA identifies the host as an attacker, select **Shun Hosts detected by scanning threat** and fill in these options if desired:

- To exempt host IP addresses from being shunned, enter an address or the name of a network object in the **Networks excluded from shun** field. You can enter multiple addresses or subnets separated by commas. To choose a network from the list of IP address objects, click the **...** button.
- To set the duration of a shun for an attacking host, select **Set Shun Duration** and enter a value between 10 and 2592000 seconds. The default length is 3600 seconds (1 hour). To restore the default value, click **Set Default**.

Step 4 Click **Apply**.

Configure Threat Detection for VPN Services

You can enable threat detection for VPN services to help prevent denial of service (DoS) attacks from IPv4 addresses. There are separate services available for the following types of attack:

- Remote access VPN login authentication. By repeatedly starting login attempts in a password-spray attack, the attacker can consume resources used for authentication attempts, thus preventing real users from logging into the VPN.
- Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. Like the password-spray attack, this attack can consume resources and prevent valid users from connecting to the VPN.

- Attempts to connect to an invalid VPN service, that is, services that are for internal use only. An IP address that attempts this connection is immediately shunned.

When you enable these services, the system automatically shuns hosts that exceed thresholds to prevent further attempts. You can manually remove the shun using the **no shun** command for the address.

To manually reset the counters for the services to 0, use the **clear threat-detection service** command.

Before you begin

When deciding on appropriate hold-down and threshold values, consider the use of NAT in your environment. If you use PAT, so that many requests can come from the same IP address, then you should consider higher values for the authentication failure and client initiation services, to ensure valid users have enough time to complete their connections. For example, a hotel, where many customers might try connecting within very short time periods.

Procedure

Step 1 Enable threat detection for remote access VPN authentication failures.

threat-detection service remote-access-authentication hold-down *minutes* **threshold** *count*

Where:

- **hold-down** *minutes* defines the hold-down period from the last failure. The threshold count of consecutive failures must be met within the hold-down period of the previous failure to trigger a shun for the attacker's IPv4 address. For example, if the hold-down period is 10 minutes and the threshold is 20, and if there are 20 consecutive authentication failures from a single IPv4 address, and if the timespan between any two consecutive failures does not exceed 10 minutes, then the source IPv4 address will be shunned. You can specify a time between 1 and 1440 minutes.
- **threshold** *count* defines the number of failed attempts that must occur within the hold-down period to trigger the shun. You can specify a threshold between 1 and 100.

To disable the service, use the following command:

no threat-detection service remote-access-authentication

Example:

The following example sets a metric of 10 failures within 20 minutes.

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

Step 2 Enable threat detection for remote access VPN client initiations.

threat-detection service remote-access-client-initiations hold-down *minutes* **threshold** *count*

Where:

- **hold-down** *minutes* defines the hold-down period from the last initiation. The threshold count of consecutive initiations must be met within the hold-down period of the previous initiation to trigger a shun for the client's IPv4 address. For example, if the hold-down period is 10 minutes and the threshold is 20, and if there are 20 consecutive initiations from a single IPv4 address, and if the timespan between

any two consecutive initiations does not exceed 10 minutes, then the source IPv4 address will be shunned. You can specify a time between 1 and 1440 minutes.

- **threshold** *count* defines the number of initiations that must occur within the hold-down period to trigger the shun. You can specify a threshold between 5 and 100.

To disable the service, use the following command:

no threat-detection service remote-access-client-initiations

Example:

The following example sets a metric of 10 initiations within 20 minutes.

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

Step 3 Enable threat detection for attempts to connect to invalid VPN services.

threat-detection service invalid-vpn-access

To disable the service, use the following command:

no threat-detection service invalid-vpn-access

Example:

The following example enables the Invalid VPN Access service.

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

Monitoring Threat Detection

The following topics explain how to monitor threat detection and view traffic statistics.

Monitoring Basic Threat Detection Statistics

Choose **Home > Firewall Dashboard > Traffic Overview** to view basic threat detection statistics.

Monitoring Advanced Threat Detection Statistics

You can monitor advanced threat statistics using the following dashboards:

- **Home > Firewall Dashboard > Top 10 Access Rules**—Displays the most hit access rules. Permits and denies are not differentiated in this graph. You can track denied traffic in the **Traffic Overview > Dropped Packets Rate** graph.
- **Home > Firewall Dashboard > Top Usage Statistics**—The **Top 10 Sources** and **Top 10 Destinations** tabs show statistics for hosts. Due to the threat detection algorithm, an interface used as a combination failover and state link could appear in the top 10 hosts; this is expected behavior, and you can ignore this IP address in the display.

The **Top 10 Services** tab shows statistics for both ports and protocols (both must be enabled for the display), and shows the combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.

- **Home > Firewall Dashboard > Top Ten Protected Servers under SYN Attack**—Shows the TCP Intercept statistics. Click the **Detail** button to show history sampling data. The ASA samples the number of attacks 30 times during the rate interval, so for the default 30 minute period, statistics are collected every 60 seconds.

Monitoring Threat Detection for VPN Services

You can monitor threat detection for VPN services using syslog and show commands, as explained in the following topics.

Syslog Monitoring for Threat Detection VPN Services

You might see the following syslog messages related to these services:

- %ASA-6-733200: Threat-detection Info: *message*

  This message reports general informational events for threat detection.

- %ASA-4-733201: Threat-detection: Service[*service*] Peer[*peer*]: threshold of *threshold-value* was exceeded. Adding shun to interface *interface*. *Additional_message*

  This message shows that the threat detection service shunned an IP address due to suspicious activity for the specified service. The message might contain additional information. For example, for RA VPN client initiation attempts, the additional information might be “SSL (or IKEv2): RA excessive client initiation requests.”

  You can see the list of shunned hosts using the **show shun** command. If you know the IP address is not an attacker, you can remove the shun using the **no shun** command.

Show Command Monitoring for Threat Detection for VPN Services

To display statistics for threat detection VPN services, use the following command:

show threat-detection service [*service*] [**entries** | **details**]

You can optionally limit the view to a particular service (**remote-access-authentication**, **remote-access-client-initiations**, or **invalid-vpn-access**). You can limit the view further by adding these parameters:

- **entries**—Display only the entries being tracked. For example, the IP addresses that have had failed authentication attempts.
- **details**—Display both service details and service entries.

Based on selected options, the display output shows the following:

- The name of the service
- The state of the service: enabled or disabled

- The service hold-down setting
- The service threshold setting
- Service action statistics
  - Failed—A failure occurrence when processing the reported occurrence.
  - Blocking—The reported occurrence is within the hold-down period and the threshold was met or exceeded. As a result, the service automatically installed a shun to block the mischievous peer.
  - Recording—The reported occurrence is outside of the hold-down period, or the threshold was met or exceeded. As a result, the service will record the occurrence.
  - Unsupported—The reported occurrence does not currently support automatic shunning.
  - Disabled—An occurrence was reported; but the service has been disabled.

Examples

The following example shows that all services are enabled, and potential attackers are being tracked for the remote-access-authentication service.

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

The following is an example of the **show threat-detection service entries** command.

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

The following is an example of the **show threat-detection service details** command.

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Removing Shuns Applied for VPN Service Violations

You can monitor shuns applied for VPN services, and remove shuns, using the following commands. Note that shuns applied by threat detection for VPN services do not appear in the **show threat-detection shun** command, which applies to scanning threat detection only.

- **show shun** [*ip_address*]

  Shows shunned hosts, including those shunned automatically by threat detection for VPN services, or manually using the **shun** command. You can optionally limit the view to a specified IP address.

- **no shun** *ip_address* [**interface** *if_name*]

  Removes the shun from the specified IP address only. You can optionally specify the interface name for the shun, if the address is shunned on more than one interface and you want to leave the shun in place on some interfaces.

- **clear shun**

  Removes the shun from all IP addresses.

History for Threat Detection

Feature Name	Platform Releases	Description
Basic and advanced threat detection statistics, scanning threat detection	8.0(2)	Basic and advanced threat detection statistics, scanning threat detection was introduced. The following screens were introduced: **Configuration > Firewall > Threat Detection**, **Home > Firewall Dashboard > Traffic Overview**, **Home > Firewall Dashboard > Top 10 Access Rules**, **Home > Firewall Dashboard > Top Usage Status**, **Home > Firewall Dashboard > Top 10 Protected Servers Under SYN Attack**.
Shun duration	8.0(4)/8.1(2)	You can now set the shun duration, The following screens was modified: **Configuration > Firewall > Threat Detection**.
TCP Intercept statistics	8.0(4)/8.1(2)	TCP Intercept statistics were introduced. The following screens were introduced or modified: **Configuration > Firewall > Threat Detection**, **Home > Firewall Dashboard > Top 10 Protected Servers Under SYN Attack**.
Customize host statistics rate intervals	8.1(2)	You can now customize the number of rate intervals for which statistics are collected. The default number of rates was changed from 3 to 1. The following screen was modified: **Configuration > Firewall > Threat Detection**.
Burst rate interval changed to 1/30th of the average rate.	8.2(1)	In earlier releases, the burst rate interval was 1/60th of the average rate. To maximize memory usage, the sampling interval was reduced to 30 times during the average rate.
Customize port and protocol statistics rate intervals	8.3(1)	You can now customize the number of rate intervals for which statistics are collected. The default number of rates was changed from 3 to 1. The following screen was modified: **Configuration > Firewall > Threat Detection**.
Improved memory usage	8.3(1)	The memory usage for threat detection was improved.

Feature Name	Platform Releases	Description
Threat Detection for VPN services	9.20(3)	You can configure threat detection for VPN services to protect against the following types of VPN attack from IPv4 addresses: • Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning. • Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. • Access attempts to invalid VPN services, that is, services that are for internal use only. These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service. The following commands were introduced or changed: **clear threat-detection service**, **show threat-detection service**, **shun**, **threat-detection service**.