Ascertain ASA Threat Detection Functionality and Configuration

Contents

Introduction

This document describes the three main components of threat detection functionality and configuration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes the functionality and basic configuration of the Threat Detection feature of the Cisco Adaptive Security Appliance (ASA). Threat Detection provides firewall administrators with the necessary tools to identify, understand, and stop attacks before they reach the internal network infrastructure. In order to do so, the feature relies on a number of different triggers and statistics, which is described in further detail in these sections.

Threat Detection can be used on any ASA firewall that runs a software version of 8.0(2) or later. Although threat detection is not a substitute for a dedicated IDS/IPS solution, it can be used in environments where an IPS is not available to provide an added layer of protection to the core functionality of ASA.

Threat Detection Functionality

The threat detection feature has three main components:

1. Basic Threat Detection
2. Advanced Threat Detection
3. Scanning Threat Detection

Each of these components is described in detail in these sections.

Basic Threat Detection (System Level Rates)

Basic threat detection is enabled by default on all ASAs that run 8.0(2) and later.

Basic threat detection monitors the rates at which packets are dropped for various reasons by the ASA as a whole. This means that the statistics generated by basic threat detection only apply to the entire appliance and are generally not granular enough to provide information on the source or specific nature of the threat. Instead, the ASA monitors dropped packets for these events:

- ACL Drop (acl-drop) - Packets are denied by access lists.
- Bad Pkts (bad-packet-drop) - Invalid packet formats, which includes L3 and L4 headers that do not conform to RFC standards.
- Conn Limit (conn-limit-drop) - Packets that exceed a configured or global connection limit.
- DoS Attack (dos-drop) - Denial of Service (DoS) attacks.
- Firewall (fw-drop) - Basic firewall security checks.
- ICMP Attack (icmp-drop) - Suspicious ICMP packets.
- Inspect (inspect-drop) - Denial by application inspection.
- Interface (interface-drop) - Packets dropped by interface checks.
- Scanning (scanning-threat) - Network/host scanning attacks.
- SYN Attack (syn-attack) - Incomplete session attacks, which includes TCP SYN attacks and unidirectional UDP sessions that have no return data.

Each of these events have a specific set of triggers that are used to identify the threat. Most triggers are tied back to specific ASP drop reasons, though certain syslogs and inspection actions are also considered. Some triggers are monitored by multiple threat categories. Some of the most common triggers are outlined in this table, though it is not an exhaustive list:

Basic Threat	Trigger(s) / ASP Drop Reason(s)
acl-drop	acl-drop

bad-packet-drop	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-matched
conn-limit-drop	conn-limit
dos-drop	sp-security-failed
fw-drop	inspect-icmp-seq-num-not-matched inspect-dns-pak-too-long inspect-dns-id-not-matched sp-security-failed acl-drop
icmp-drop	inspect-icmp-seq-num-not-matched
inspect-drop	Frame drops triggered by an inspection engine
interface-drop	sp-security-failed no-route
scanning-threat	tcp-3whs-failed tcp-not-syn sp-security-failed acl-drop inspect-icmp-seq-num-not-matched inspect-dns-pak-too-long inspect-dns-id-not-matched
syn-attack	%ASA-6-302014 syslog with teardown reason of "SYN Timeout"

For each event, basic threat detection measures the rates that these drops occur over a configured period of time. This period of time is called the average rate interval (ARI) and can range from 600 seconds to 30 days. If the number of events that occur within the ARI exceeds the configured rate thresholds, the ASA considers these events a threat.

Basic threat detection has two configurable thresholds for when it considers events to be a threat: the average rate and the burst rate. The average rate is simply the average number of drops per second within the time period of the configured ARI. For example, if the average rate threshold for ACL drops is configured for 400 with an ARI of 600 seconds, the ASA calculates the average number of packets that were dropped by ACLs in the last 600 seconds. If this number turns out to be greater than 400 per second, the ASA logs a threat.

Likewise, the burst rate is very similar but looks at smaller periods of snapshot data, called the burst rate interval (BRI). The BRI is always smaller than the ARI. For example, building on the previous example, the ARI for ACL drops is still 600 seconds and now has a burst rate of 800. With these values, the ASA calculates the average number of packets dropped by ACLs in 20 seconds, where 20 seconds is the BRI. If this calculated value exceeds 800 drops per second, a threat is logged. In order to determine what BRI is used, the ASA calculates the value of 1/30th of the ARI. Therefore, in the example previously used, 1/30th of 600 seconds is 20 seconds. However, threat detection has a minimum BRI of 10 seconds, so if 1/30th of the ARI is less than 10, the ASA still uses 10 seconds as the BRI. Also, it is important to note that this behavior was different in versions prior to 8.2(1), which used a value of 1/60th of the ARI, instead of 1/30th. The minimum BRI of 10 seconds is the same for all software versions.

When a basic threat is detected, the ASA simply generates syslog %ASA-4-733100 to alert the administrator that a potential threat has been identified. The average, current, and total number of events for each threat category can be seen with the **show threat-detection rate** command. The total number of cumulative events is the sum of the number of events seen in the last 30 BRI samples.

The burst rate in syslog is calculated based on the number of packets dropped so far in the current BRI. The calculation is taken periodically in a BRI. Once a breach happens, a syslog is raised. It is limited that only one syslog is generated in a BRI. The burst rate in â€œshow threat-detection rateâ€ is calculated based on the number of packets dropped in last BRI. The design for the difference is that syslog is time sensitive so if a breach happens in current BRI, it would have a chance to be captured. â€œshow threat-detection rateâ€ is less time sensitive, so the number from last BRI is used.

Basic threat detection does not take any actions in order to stop the deviant traffic or prevent future attacks. In this sense, basic threat detection is purely informational and can be used as a monitoring or reporting mechanism.

Advanced Threat Detection (Object Level Statistics and Top N)

Unlike Basic Threat Detection, Advanced Threat Detection can be used to track statistics for more granular objects. The ASA supports tracking statistics for host IPs, ports, protocols, ACLs, and servers protected by TCP intercept. Advanced Threat Detection is only enabled by default for ACL statistics.

For host, port, and protocol objects, Threat Detection keeps track of the number of packets, bytes, and drops that were both sent and received by that object within a specific time period. For ACLs, Threat Detection keeps track of the top 10 ACEs (both permit and deny) that were hit the most within a specific time period.

The time periods tracked in all of these cases are 20 minutes, 1 hour, 8 hours, and 24 hours. While the time periods themselves are not configurable, the number of periods that are tracked per object can be adjusted with the 'number-of-rate' keyword. See the Configuration section for more information. For example, if 'number-of-rate' is set to 2, you see all statistics for 20 minutes, 1 hour and 8 hours. if 'number-of-rate' is set to 1, you see all statistics for 20 minutes, 1 hour. No matter what, the 20 minute rate is always displayed.

When TCP intercept is enabled, Threat Detection can keep track of the top 10 servers which are considered to be under attack and protected by TCP intercept. Statistics for TCP intercept are similar to Basic Threat

Detection in the sense that the user can configure the measured rate-interval along with specific average (ARI) and burst (BRI) rates. Advanced Threat Detection statistics for TCP intercept are only available in ASA 8.0(4) and later.

Advanced Threat Detection statistics are viewed via the **show threat-detection statistics** and **show threat-detection statistics top** commands. This is also the feature responsible for the population of the "top" graphs on the firewall dashboard of ASDM. The only syslogs that are generated by Advanced Threat Detection are %ASA-4-733104 and %ASA-4-733105, which are triggered when the average and burst rates (respectively) are exceeded for TCP intercept statistics.

Like Basic Threat Detection, the Advanced Threat Detection is purely informational. No actions are taken to block traffic based on the Advanced Threat Detection statistics.

Scanning Threat Detection

Scanning Threat Detection is used in order to keep track of suspected attackers who create connections too many hosts in a subnet, or many ports on a host/subnet. Scanning Threat Detection is disabled by default.

Scanning Threat Detection builds on the concept of Basic Threat Detection, which already defines a threat category for a scanning attack. Therefore, the rate-interval, average rate (ARI), and burst rate (BRI) settings are shared between Basic and Scanning Threat Detection. The difference between the 2 features is that while Basic Threat Detection only indicates that the average or burst rate thresholds were crossed, Scanning Threat Detection maintains a database of attacker and target IP addresses that can help provide more context around the hosts involved in the scan. Additionally, only traffic that is actually received by the target host/subnet is considered by Scanning Threat Detection. Basic Threat Detection can still trigger a Scanning threat even if the traffic is dropped by an ACL.

Scanning Threat Detection can optionally react to an attack by shunning the attacker IP. This makes Scanning Threat Detection the only subset of the Threat Detection feature that can actively affect connections through the ASA.

When Scanning Threat Detection detects an attack, %ASA-4-733101 is logged for the attacker and/or target IPs. If the feature is configured to shun the attacker, %ASA-4-733102 is logged when Scanning Threat Detection generates a shun. %ASA-4-733103 is logged when the shun is removed. The **show threat-detection scanning-threat** command can be used in order to view the entire Scanning Threat database.

Limitations

- Threat Detection is only available in ASA 8.0(2) and later. It is not supported on the ASA 1000V platform.
- Threat Detection is only supported in single context mode.
- Only through-the-box threats are detected. Traffic sent to the ASA itself is not considered by Threat Detection.
- TCP connection attempts that are reset by the targeted server is not counted as a SYN attack or Scanning threat.

Configuration

Basic Threat Detection

Basic Threat Detection is enabled with the **threat-detection basic-threat** command.

```
ciscoasa(config)#
```

```
threat-detection basic-threat
```

The default rates can be viewed with the **show run all threat-detection** command.

```
<#root>
```

```
ciscoasa(config)#
```

```
show run all threat-detection
```

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

In order to tune these rates with custom values, simply reconfigure the **threat-detection rate** command for the appropriate threat category.

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550
```

Each threat category can have a maximum of 3 different rates defined (with rate IDs of rate 1, rate 2, and rate 3). The particular rate ID that is exceeded is referenced in the %ASA-4-733100 syslog.

In the previous example, threat detection creates syslog 733100 only when the number of ACL drops exceeds 250 drops/second over 1200 seconds or 550 drops/second over 40 seconds.

Advanced Threat Detection

Use the **threat-detection statistics** command in order to enable Advanced Threat Detection. If no specific feature keyword is provided, the command enables tracking for all statistics.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics ?

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

In order to configure the number of rate intervals that are tracked for host, port, protocol, or ACL statistics, use the **number-of-rate** keyword.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics host number-of-rate 2

The number-of-rate keyword configures Threat Detection to track only the shortest *n* number of intervals.

In order to enable TCP intercept statistics, use the **threat-detection statistics tcp-intercept** command.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics tcp-intercept

In order to configure custom rates for TCP intercept statistics, use the **rate-interval**, **average-rate**, and **burst-rate** keywords.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100

Scanning Threat Detection

In order to enable Scanning Threat Detection, use the **threat-detection scanning-threat** command.

<#root>

```
ciscoasa(config)#
threat-detection scanning-threat
```

In order to adjust the rates for a scanning-threat, use the same **threat-detection rate** command used by Basic Threat Detection.

```
<#root>
ciscoasa(config)#
threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

In order to allow the ASA to shun a scanning attacker IP, add the **shun** keyword to the **threat-detection scanning-threat** command.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat shun
```

This allows Scanning Threat Detection to create a one hour shun for the attacker. In order to adjust the duration of the shun, use the **threat-detection scanning-threat shun duration** command.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat shun duration 1000
```

In some cases, you can prevent the ASA from shunning certain IPs. In order to do this, create an exception with the **threat-detection scanning-threat shun except** command.

```
<#root>
ciscoasa(config)#
threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255

ciscoasa(config)#
threat-detection scanning-threat shun except object-group no-shun
```

Performance

Basic Threat Detection has very little performance impact on the ASA. Advanced and Scanning Threat Detection are much more resource intensive because they have to keep track of various statistics in memory. Only Scanning Threat Detection with the shun function enabled can actively impact traffic that otherwise would have been allowed.

As the ASA software versions have progressed, the memory utilization of Threat Detection has been significantly optimized. However, care must be taken to monitor the memory utilization of ASA before and after Threat Detection is enabled. In some cases, it would be better to only enable certain statistics (for example, host statistics) temporarily while you actively troubleshoot a specific issue.

For a more detailed view of Threat Detection memory usage, run the **show memory app-cache threat-detection [detail]** command.

Recommended Actions

These sections provide some general recommendations for actions that can be taken when various Threat Detection-related events occur.

When a Basic Drop Rate is Exceeded and %ASA-4-733100 is Generated

Determine the specific threat category mentioned in the %ASA-4-733100 syslog and correlate this with the output of show threat-detection rate . With this information, check the output of show asp drop in order to determine the reasons why traffic is dropped.

For a more detailed view of traffic that is dropped for a specific reason, use an ASP drop capture with the reason in question in order to see all of the packets that are dropped. For example, if ACL Drop threats are logged, capture on the ASP drop reason of acl-drop :

```
<#root>

ciscoasa#

capture drop type asp-drop acl-drop



ciscoasa#

show capture drop



1 packet captured

   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

This capture shows that the dropped packet is a UDP/53 packet from 10.10.10.10 to 192.168.1.100.

If %ASA-4-733100 reports a Scanning threat, it can also be helpful to temporarily enable Scanning Threat Detection. This allows the ASA to keep track of the source and destination IPs involved in the attack.

Since Basic Threat Detection mostly monitors traffic which is already dropped by the ASP, no direct action is required to stop a potential threat. The exceptions to this are SYN Attacks and Scanning threats, which

involve traffic that passes through the ASA.

If the drops seen in the ASP drop capture are legitimate and/or expected for the network environment, tune the basic rate intervals to a more appropriate value.

If the drops show illegitimate traffic, actions must be taken to block or rate limit the traffic before it reaches the ASA. This can include ACLs and QoS on upstream devices.

For SYN attacks, traffic can be blocked in an ACL on the ASA. TCP intercept could also be configured to protect the targeted server(s), but this could simply result in a Conn Limit threat that is logged instead.

For Scanning threats, traffic can also be blocked in an ACL on the ASA. Scanning Threat Detection with the shunoption can be enabled to allow the ASA to proactively block all packets from the attacker for a defined period of time.

When a Scanning Threat is Detected and %ASA-4-733101 is Logged

%ASA-4-733101 must list either the target host/subnet or the attacker IP address. For the full list of targets and attackers, check the output of show threat-detection scanning-threat.

Packet captures on the ASAs interfaces that face the attacker and/or target(s) can also help clarify the nature of the attack.

If the detected scan is a not expected, actions must be taken to block or rate limit the traffic before it reaches the ASA. This can include ACLs and QoS on upstream devices. When the shunoption is added to the Scanning Threat Detection config it can allow the ASA to proactively drop all packets from the attacker IP for a defined period of time. As a last resort, the traffic can also be blocked manually on the ASA via an ACL or TCP intercept policy.

If the detected scan is a false positive, adjust the Scanning Threat rate intervals to a more appropriate value for the network environment.

When an Attacker is Shunned and %ASA-4-733102 is Logged

%ASA-4-733102 lists the IP address of the shunned attacker. Use the show threat-detection shun command in order to view a full list of attackers that have been shunned by Threat Detection specifically. Use the show shun command in order to view the full list of all IPs that are actively shunned by the ASA (this includes from sources other than Threat Detection).

If the shun is part of a legitimate attack, no further action is required. However, it would be beneficial to manually block the traffic of the attacker as far upstream toward the source as possible. This can be done via ACLs and QoS. This ensures that intermediate devices do not need to waste resources on illegitimate traffic.

If the Scanning threat that triggered the shun was a false positive, manually remove the shun with the clear threat-detection shun [IP_address] command.

When %ASA-4-733104 and/or %ASA-4-733105 is Logged

%ASA-4-733104 and %ASA-4-733105 lists the host targeted by the attack that is currently protected by TCP intercept. For more details on the attack rates and protected servers, check the output of show threat-detection statistics top tcp-intercept .

```
ciscoasa#
```

```
show threat-detection statistics top tcp-intercept
```

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

When Advanced Threat Detection detects an attack of this nature, the ASA already protects the targeted server via TCP intercept. Verify the configured connection limits to ensure they provide adequate protection for the nature and rate of the attack. Also, it would be beneficial to manually block the traffic of the attacker as far upstream toward the source as possible. This can be done via ACLs and QoS. This ensures that intermediate devices do not need to waste resources on illegitimate traffic.

If the detected attack is a false positive, adjust the rates for a TCP intercept attack to a more appropriate value with the threat-detection statistics tcp-interceptcommand.

How To Manually Trigger a Threat

To test and troubleshoot, it can be helpful to manually trigger various threats. This section contains tips on how to trigger a few common threat types.

Basic Threat - ACL Drop, Firewall, and Scanning

In order to trigger a particular Basic Threat, refer to the table in the previous Functionality section. Choose a specific ASP drop reason and send traffic through the ASA that would be dropped by the appropriate ASP drop reason.

For example, ACL Drop, Firewall, and Scanning threats all consider the rate of packets dropped by acl-drop. Complete these steps in order to trigger these threats simultaneously:

1. Create an ACL on the outside interface of the ASA that explicitly drops all TCP packets sent to a target server on the inside of the ASA (10.11.11.11):

   ```
   access-list outside_in extended line 1 deny tcp any host 10.11.11.11
   access-list outside_in extended permit ip any any
   access-group outside_in in interface outside
   ```

2. From an attacker on the outside of the ASA (10.10.10.10), use nmap in order to run a TCP SYN scan against every port on the target server:

   ```
   nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
   ```

> **Note**: T5 configures nmap to run the scan as fast as possible. Based on on the resources of the attacker PC, this still is not fast enough to trigger some of the default rates. If this is the case, simply lower the configured rates for the threat you want to see. When you set the ARI and BRI to 0 causes Basic Threat Detection to always trigger the threat regardless of the rate.

3. Notice that Basic Threats are detected for ACL Drop, Firewall, and Scanning threats:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

> **Note**: In this example, the ACL drop and Firewall ARIs and BRIs have been set to 0 so they always trigger a threat. This is why the max configured rates are listed as 0.

Advanced Threat - TCP Intercept

1. Create an ACL on the outside interface that permits all TCP packets sent to a target server on the inside of the ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. If the target server does not actually exist, or it resets the connection attempts of the attacker, configure a fake ARP entry on the ASA to blackhole the attack traffic out the inside interface:

```
arp inside 10.11.11.11 dead.dead.dead
```

3. Create a simple TCP intercept policy on the ASA:

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

From an attacker on the outside of the ASA (10.10.10.10), use nmap to run a TCP SYN scan against every port on the target server:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Note that Threat Detection keeps track of the protected server:

```
<#root>

ciscoasa(config)#

show threat-detection statistics top tcp-intercept


Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

------------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

Scanning Threat

1. Create an ACL on the outside interface that permits all TCP packets sent to a target server on the inside of the ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

Note: In order for Scanning Threat Detection to track the target and attacker IPs, the traffic must be permitted through the ASA.

---

2. If the target server does not actually exist, or it resets the connection attempts of the attacker, configure a fake ARP entry on the ASA to blackhole the attack traffic out the inside interface:

```
arp inside 10.11.11.11 dead.dead.dead
```

Note: Connections that are reset by the target server are not counted as part of the threat.

---

3. From an attacker on the outside of the ASA (10.10.10.10), use nmap to run a TCP SYN scan against every port on the target server:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Note: T5 configures nmap to run the scan as fast as possible. Based on on the resources of the attacker PC, this still is not fast enough to trigger some of the default rates. If this is the case, simply lower the configured rates for the threat you want to see. When you set the ARI and BRI to 0 causes Basic Threat Detection to always trigger the threat regardless of the rate.

---

4. Note that a Scanning threat is detected, the IP of the attacker is tracked, and the attacker is shunned:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
```

```
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Related Information

- **ASA Configuration Guide**
- **ASA Command Reference**
- **Cisco Secure Firewall ASA Series Syslog Messages**
- **Cisco Technical Support & Downloads**