

確定ASA威脅檢測功能和配置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[威脅檢測功能](#)

[基本威脅檢測 \(系統級速率\)](#)

[高級威脅檢測 \(對象級別統計資訊和前N個\)](#)

[掃描威脅檢測](#)

[限制](#)

[組態](#)

[基本威脅檢測](#)

[高級威脅檢測](#)

[掃描威脅檢測](#)

[效能](#)

[建議的操作](#)

[超出基本丟棄速率並生成%ASA-4-733100時](#)

[檢測到掃描威脅並記錄%ASA-4-733101時](#)

[迴避Attacker並記錄%ASA-4-733102時](#)

[記錄%ASA-4-733104和/或%ASA-4-733105時](#)

[如何手動觸發威脅](#)

[基本威脅 — ACL丟棄、防火牆和掃描](#)

[高級威脅 — TCP攔截](#)

[掃描威脅](#)

[相關資訊](#)

簡介

本檔案介紹威脅檢測功能和配置的三個主要組成部分。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔介紹思科自適應安全裝置(ASA)的威脅檢測功能的功能和基本配置。威脅檢測為防火牆管理員提供了必要的工具，以便在攻擊到達內部網路基礎架構之前識別、瞭解和阻止攻擊。為此，該功能依賴於許多不同的觸發器和統計資訊，這將在這些部分中進一步詳述。

威脅檢測可以在運行8.0(2)或更高版本軟體的任何ASA防火牆上使用。雖然威脅檢測不能替代專用的IDS/IPS解決方案，但是可以在IPS不可用的環境中使用，為ASA的核心功能提供額外的保護層。

威脅檢測功能

威脅檢測功能有三個主要元件：

1. 基本威脅檢測
2. 高級威脅檢測
3. 掃描威脅檢測

以下各節將詳細介紹所有這些元件。

基本威脅檢測（系統級速率）

運行8.0(2)及更高版本的所有ASA預設啟用基本威脅檢測。

基本威脅檢測監控由於各種原因而丟棄資料包的速率（ASA作為一個整體）。這意味著基本威脅檢測生成的統計資訊僅應用於整個裝置，並且通常不夠精細，不足以提供有關威脅的源或特定性質的資訊。相反，ASA會監控丟棄的資料包是否存在以下事件：

- ACL Drop(acl-drop) — 存取清單拒絕封包。
- Bad Pkts(bad-packet-drop) — 無效的資料包格式，包括不符合RFC標準的L3和L4報頭。
- Conn Limit(conn-limit-drop) — 超過已配置或全域性連線限制的資料包。
- DoS攻擊(dos-drop) — 拒絕服務(DoS)攻擊。
- 防火牆-fw-drop) — 基本防火牆安全檢查。
- ICMP攻擊(icmp-drop) — 可疑ICMP資料包。
- Inspect(inspect-drop) — 通過應用程式檢查拒絕。
- Interface(interface-drop) — 介面檢查丟棄的資料包。
- 掃描（掃描 — 威脅） — 網路/主機掃描攻擊。
- SYN攻擊（syn攻擊） — 不完整的會話攻擊，包括沒有返回資料的TCP SYN攻擊和單向UDP會話。

每個事件都有一組特定觸發器，用於識別威脅。大多數觸發器都關聯回特定的ASP丟棄原因，儘管某些系統日誌和檢查操作也會被考慮。某些觸發器受多個威脅類別監控。下表中列出了一些最常見的觸發器，不過它並不是一個詳盡的清單：

基本威脅	觸發器/ASP丟棄原因
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	由檢查引擎觸發的幀丟棄
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攻擊	%ASA-6-302014系統日誌，其拆卸原因為「SYN超時」

對於每種事件，基本威脅檢測都會測量這些丟棄在配置的時間段內的發生率。這段時間稱為平均速率時間間隔(ARI)，範圍從600秒到30天。如果ARI內發生的事件數超過配置的速率閾值，ASA會將這些事件視為威脅。

基本威脅檢測具有兩個可配置的閾值，當它將事件視為威脅時：平均速率和突發速率。平均速率只是已配置ARI的時間週期內每秒的平均丟棄數。例如，如果將ACL丟棄的平均速率閾值配置為400，且ARI為600秒，則ASA將計算過去600秒內ACL丟棄的資料包的平均數量。如果此數字大於每秒400，則ASA會記錄威脅。

同樣，突發速率非常相似，但會檢視快照資料的較小週期，稱為突發速率間隔(BRI)。BRI始終小於ARI。例如，在上一個範例的基礎上，ACL捨棄的ARI仍然是600秒，現在的突發速率是800。使用這些值，ASA計算ACL在20秒內丟棄的資料包的平均數量，其中20秒是BRI。如果此計算值超過每秒800個丟包，則會記錄威脅。為了確定使用BRI，ASA計算ARI的1/30的值。因此，在先前使用的範例中，600秒的第1/30秒為20秒。但是，威脅檢測的最小BRI為10秒，因此，如果ARI的1/30小於10，則ASA仍使用10秒作為BRI。此外，必須注意的是，在8.2(1)之前的版本中，此行為是不同的，8.2(1)使用的值是ARI的1/60，而不是1/30。對於所有軟體版本，最低BRI為10秒。

當檢測到基本威脅時，ASA僅生成系統日誌%ASA-4-733100，以提醒管理員已識別出潛在威脅。可以使用show threat-detection rate命令檢視每個威脅類別的平均事件、當前事件和事件總數。累積事件總數是指在最近30個BRI樣本中看到的事件總數。

系統日誌中的突發速率根據當前BRI中到目前為止丟棄的資料包數量計算。該計算在BRI中定期進行。一旦發生漏洞，就會生成系統日誌。限制在BRI中僅生成一個系統日誌。「show threat-detection rate」中的突發速率根據上一個BRI中丟棄的資料包數量計算。不同之處在於，系統日誌具有時間敏感性，因此，如果當前BRI中發生漏洞，將有機會捕獲該漏洞。「show threat-detection rate」對時間不太敏感，因此使用來自上一個BRI的數字。

基本威脅檢測不會採取任何操作來停止異常流量或防止未來攻擊。從這個意義上講，基本威脅檢測純粹是資訊性的，可以用作監控或報告機制。

高級威脅檢測 (對象級別統計資訊和前N個)

與基本威脅檢測不同，高級威脅檢測可用於跟蹤更精細對象的統計資訊。ASA支援主機IP、埠、協定、ACL和受TCP攔截保護的伺服器的跟蹤統計資訊。高級威脅檢測僅預設啟用ACL統計資訊。

對於主機、埠和協定對象，威脅檢測會跟蹤該對象在特定時間段內傳送和接收的資料包、位元組數和丟棄數。對於ACL，威脅檢測會跟蹤在特定時間段內點選率最高的前10個ACE (包括允許和拒絕)。

在所有這些案例中，跟蹤的時間段分別為20分鐘、1小時、8小時和24小時。雖然時段本身不可配置，但每個對象跟蹤的時段數量可以使用「number-of-rate」關鍵字進行調整。如需詳細資訊，請參閱組態一節。例如，如果將「number-of-rate」設定為2，則可以檢視20分鐘、1小時和8小時的所有統計資訊。如果將「number-of-rate」設定為1，則可以檢視20分鐘、1小時的所有統計資訊。無論發生什麼情況，始終顯示20分鐘速率。

啟用TCP攔截後，威脅檢測可以跟蹤被視為受攻擊並受TCP攔截保護的前10台伺服器。TCP攔截的統計資訊與基本威脅檢測類似，使用者可以將測量的速率間隔與特定的平均(ARI)和突發(BRI)速率一起配置。TCP攔截的高級威脅檢測統計資訊僅在ASA 8.0(4)及更高版本中可用。

高級威脅檢測統計資訊通過show threat-detection statistics和show threat-detection statistics top命令檢視。此功能也負責填充ASDM防火牆控制面板上的「頂部」圖形。高級威脅檢測生成的唯一系統日誌是%ASA-4-733104和%ASA-4-733105，當超出了TCP攔截統計資訊的平均和突發速率（分別為）時觸發這些系統日誌。

與基本威脅檢測類似，高級威脅檢測也是純資訊性的。根據高級威脅檢測統計資訊，不採取任何操作來阻止流量。

掃描威脅檢測

掃描威脅檢測用於跟蹤可疑攻擊者，這些攻擊者會在子網中建立過多主機或主機/子網中許多埠的連線。掃描威脅檢測預設處於禁用狀態。

掃描威脅檢測基於基本威脅檢測的概念，基本威脅檢測已經定義了掃描攻擊的威脅類別。因此，基本威脅檢測和掃描威脅檢測之間共用速率間隔、平均速率(ARI)和突發速率(BRI)設定。這兩個功能之間的區別在於，雖然基本威脅檢測僅表示平均或突發速率閾值已超過，但掃描威脅檢測會維護一個包含攻擊者和目標IP地址的資料庫，這有助於為掃描所涉及的主機提供更多情景。此外，掃描威脅檢測僅考慮目標主機/子網實際接收的流量。即使流量被ACL捨棄，基本威脅檢測仍可以觸發掃描威脅。

掃描威脅檢測可以通過避開攻擊者IP選擇性地對攻擊做出反應。這使得掃描威脅檢測成為威脅檢測功能中唯一可以通過ASA主動影響連線的子集。

當掃描威脅檢測檢測到攻擊時，將為攻擊者733101/或目標IP記錄%ASA-4-。如果該功能配置為避開攻擊者，則當掃描威脅檢測生成shun時，會記錄%ASA-4-733102。刪除shun時733103錄%ASA-4-XL。show threat-detection scanning-threat命令可用於檢視整個掃描威脅資料庫。

限制

- 威脅檢測僅在ASA 8.0(2)及更高版本中可用。ASA 1000V平台不支援該功能。
- 僅在單情景模式下支援威脅檢測。
- 僅檢測到直通式威脅。威脅檢測不考慮傳送到ASA本身的流量。
- 由目標伺服器重置的TCP連線嘗試不計為SYN攻擊或掃描威脅。

組態

基本威脅檢測

基本威脅檢測是使用threat-detection basic-threat命令啟用的。

```
<#root>
```

```
ciscoasa(config)#
```

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

可以使用show run all threat-detection命令檢視預設速率。

```
<#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
```

若要使用自訂值調整這些速率，只需為適當的威脅類別重新配置threat-detection rate命令。

```
<#root>
```

```
ciscoasa(config)#
```

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

每個威脅類別最多可以定義3個不同的速率（速率ID為速率1、速率2和速率3）。在%ASA-4-733100系統日誌中引用了超出的特定速率ID。

在上一個示例中，只有當在1200秒內ACL丟棄數超過250個丟包/秒或在40秒內550個丟包/秒時，威脅檢測才會建立系統日誌733100。

高級威脅檢測

使用threat-detection statistics命令以啟用高級威脅檢測。如果未提供特定的feature關鍵字，該命令將啟用對所有統計資訊的跟蹤。

```
<#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>
```

要配置主機、埠、協定或ACL統計資訊跟蹤的速率間隔數，請使用number-of-rate關鍵字。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection statistics host number-of-rate 2
```

number-of-rate關鍵字將配置威脅檢測以僅跟蹤最短n個時間間隔。

要啟用TCP攔截統計資訊，請使用threat-detection statistics tcp-intercept命令。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection statistics tcp-intercept
```

要配置TCP攔截統計資訊的自定義速率，請使用rate-interval、average-rate和burst-rate關鍵字。

```
<#root>
```

```
ciscoasa(config)#
```

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

掃描威脅檢測

若要啟用掃描威脅檢測，請使用threat-detection scanning-threat命令。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat
```

要調整掃描威脅的速率，請使用基本威脅檢測所用的threat-detection rate命令。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

為了允許ASA避開掃描攻擊者IP，請將shun關鍵字新增到threat-detection scanning-threat命令中。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun
```

這樣，掃描威脅檢測可為攻擊者建立一小時的迴避。要調整shun的持續時間，請使用threat-detection scanning-threat shun duration命令。

```
<#root>
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun duration 1000
```

在某些情況下，您可以防止ASA規避某些IP。為此，請使用threat-detection scanning-threat shun except命令建立異常。

```
<#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
```

效能

基本威脅檢測對ASA的效能影響很小。高級和掃描威脅檢測會佔用更多的資源，因為它們必須跟蹤記憶體中的各種統計資訊。只有啟用了shun功能的掃描威脅檢測才能主動影響本來會允許的流量。

隨著ASA軟體版本的進展，威脅檢測的記憶體利用率已顯著最佳化。但是，必須注意在啟用威脅檢測之前和之後監控ASA的記憶體利用率。在某些情況下，最好在主動排查特定問題的同時暫時啟用某些統計資訊（例如，主機統計資訊）。

有關威脅檢測記憶體使用情況的更詳細檢視，請運行show memory app-cache threat-detection [detail]命令。

建議的操作

這些部分針對發生各種威脅檢測相關事件時可以採取的操作提供一些一般建議。

超出基本丟棄速率並生成%ASA-4-733100時

確定%ASA-4-X系統日誌中提及的特定威733100類別，並將其與 show threat-detection rate .使用此資訊，請檢查 show asp drop 以確定流量遭捨棄的原因。

要獲得因特定原因丟棄的流量的更詳細檢視，請使用包含問題原因的ASP丟棄捕獲，以便檢視所有被丟棄的資料包。例如，如果記錄了ACL Drop威脅，則在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
```

此擷取顯示捨棄的封包是從10.10.10.10到192.168.1.100的UDP/53封包。

如果%ASA-4-733100報告掃描威脅，則臨時啟用掃描威脅檢測也非常有用。這允許ASA跟蹤攻擊中涉及的源和目標IP。

由於基本威脅檢測主要監視已被ASP丟棄的流量，因此不需要直接操作來阻止潛在威脅。例外情況是SYN攻擊和掃描威脅，這些威脅涉及通過ASA的流量。

如果ASP丟棄捕獲中顯示的丟棄是合法的，並且/或者對於網路環境是預期的，請將基本速率間隔調

整為更合適的值。

如果丟棄顯示非法流量，則必須在流量到達ASA之前採取措施對其進行阻止或速率限制。這可能包括上游裝置上的ACL和QoS。

對於SYN攻擊，可以阻止ASA上的ACL中的流量。也可以將TCP攔截配置為保護目標伺服器，但這只會導致記錄的Conn Limit威脅。

對於掃描威脅，也可以在ASA上的ACL中阻止流量。掃描威脅檢測 `shun` 可以啟用該選項，以允許ASA在定義的時間段內主動阻止來自攻擊者的所有資料包。

檢測到掃描威脅並記錄%ASA-4-733101時

%ASA-4-733101必須列出目標主機/子網或攻擊者IP地址。有關目標和攻擊者的完整清單，請檢視 `show threat-detection scanning-threat`。

在面向攻擊者和/或目標的ASA介面上捕獲資料包也有助於澄清攻擊的性質。

如果檢測到的掃描不是預期掃描，則必須在流量到達ASA之前採取措施阻止流量或限制流量。這可能包括上游裝置上的ACL和QoS。當 `shun` 選項被新增到掃描威脅檢測配置中，它允許ASA在定義的時間段內主動丟棄來自攻擊者IP的所有資料包。作為最後手段，還可以通過ACL或TCP攔截策略在ASA上手動阻止流量。

如果檢測到的掃描是誤報，請將掃描威脅率間隔調整為更適合網路環境的值。

躲避攻擊者並記錄%ASA-4-733102時

%ASA-4-733102列出迴避的攻擊者的IP地址。使用 `show threat-detection shun` 命令，以便檢視威脅檢測專門避開的攻擊者的完整清單。使用 `show shun` 命令，以檢視ASA主動避開的所有IP的完整清單（這包括來自威脅檢測以外的來源）。

如果shun是合法攻擊的一部分，則無需執行進一步操作。但是，最好手動阻止攻擊者的流量，使其儘可能向上游到源位置。這可透過ACL和QoS完成。這可確保中間裝置無需非法流量上浪費資源。

如果觸發shun的掃描威脅為誤報，請使用 `clear threat-detection shun [IP_address]` 指令。

記錄%ASA-4-733104和/或%ASA-4-733105時

%ASA-4-733104和%ASA-4-733105列出當前受TCP攔截保護的攻擊所針對的主機。有關攻擊率和受保護伺服器的詳細資訊，請檢視 `show threat-detection statistics top tcp-intercept`。

```
<#root>
```

```
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)
```

當高級威脅檢測檢測到此類攻擊時，ASA已經通過TCP攔截保護目標伺服器。檢驗配置的連線限制，以確保它們為攻擊的性質和速率提供充分的保護。此外，最好手動阻止攻擊者的流量，使其流向源裝置的上游儘可能遠。這可透過ACL和QoS完成。這可確保中間裝置無需在非法流量上浪費資源。

如果檢測到的攻擊為誤報，請將TCP攔截攻擊的速率調整為更合適的值，並使用 `threat-detection statistics tcp-intercept` 指令。

如何手動觸發威脅

要測試和排除故障，手動觸發各種威脅非常有用。本節包含有關如何觸發幾種常見威脅型別的提示。

基本威脅 — ACL丟棄、防火牆和掃描

要觸發特定基本威脅，請參閱上一功能部分中的表。選擇特定的ASP丟棄原因，並通過相應的ASP丟棄原因丟棄的ASA傳送流量。


例如，ACL Drop、防火牆和掃描威脅都會考慮acl-drop丟棄的資料包的速率。完成以下步驟，以同時觸發這些威脅：

1. 在ASA的外部介面上建立一個ACL，該ACL顯式丟棄傳送到ASA(10.11.11.11)內部目標伺服器的所有TCP資料包：

```
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. 在ASA(10.10.10.10)外部的攻擊者中，使用nmap對目標伺服器上的每個埠運行TCP SYN掃描：

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

 **注意:** T5配置nmap以儘快運行掃描。根據攻擊者PC的資源，這仍不足以觸發某些預設速率。如果是這種情況，只需降低您想要看到的威脅的已配置速率。當您將ARI和BRI設定



為0時，基本威脅檢測將始終觸發威脅，無論其速率如何。

3. 請注意，檢測到ACL丟棄、防火牆和掃描威脅的基本威脅：

```
%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
```



注意：在此示例中，ACL丟棄和防火牆ARI和BRI已設定為0，因此它們始終會觸發威脅。這就是最大配置速率列為0的原因。

高級威脅 — TCP攔截

1. 在外部介面上建立ACL，以允許所有傳送到ASA(10.11.11.11)內部目標伺服器的TCP資料包：

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

2. 如果目標伺服器實際上並不存在，或者它重置了攻擊者的連線嘗試，請在ASA上配置一個虛假ARP條目，以便將攻擊流量從內部介面挖空：

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

3. 在ASA上建立簡單的TCP攔截策略：

```
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
```

從ASA(10.10.10.10)外部的攻擊者那裡，使用nmap對目標伺服器上的每個埠運行TCP SYN掃描：

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

請注意，威脅檢測會跟蹤受保護的伺服器：

```
<#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)
```

掃描威脅


1. 在外部介面上建立ACL，以允許所有傳送到ASA(10.11.11.11)內部目標伺服器的TCP資料包：

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

 注意：為了讓掃描威脅檢測跟蹤目標和攻擊者IP，必須允許通過ASA的流量。


2. 如果目標伺服器實際上並不存在，或者它重置了攻擊者的連線嘗試，請在ASA上配置一個虛假ARP條目，以便將攻擊流量從內部介面挖空：

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

 注意：由目標伺服器重置的連線不計為威脅的一部分。

3. 從ASA(10.10.10.10)外部的攻擊者那裡，使用nmap對目標伺服器上的每個埠運行TCP SYN掃描：

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

 注意：T5配置nmap以儘快運行掃描。根據攻擊者PC的資源，這仍不足以觸發某些預設速率。如果是這種情況，只需降低您想要看到的威脅的已配置速率。當您將ARI和BRI設定為0時，基本威脅檢測將始終觸發威脅，無論其速率如何。

4. 請注意，檢測到掃描威脅，跟蹤攻擊者的IP，並避開攻擊者：

```
%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
```

相關資訊

- [ASA配置指南](#)
- [ASA命令參考](#)
- [Cisco安全防火牆ASA系列系統日誌消息](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。