Verificar a funcionalidade e a configuração da detecção de ameaças do ASA

Contents

Introdução

Este documento descreve os três principais componentes da funcionalidade e configuração da detecção de ameaças.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer

comando.

Informações de Apoio

Este documento descreve a funcionalidade e a configuração básica da característica Threat Detection do Cisco Adaptive Security Appliance (ASA). A Detecção de Ameaças fornece aos administradores de firewall as ferramentas necessárias para identificar, entender e interromper ataques antes que eles alcancem a infraestrutura de rede interna. Para fazer isso, o recurso conta com vários disparadores e estatísticas diferentes, que são descritos em mais detalhes nestas seções.

A Detecção de Ameaças pode ser usada em qualquer firewall ASA que execute uma versão de software 8.0(2) ou posterior. Embora a detecção de ameaças não substitua uma solução de IDS/IPS dedicada, ela pode ser usada em ambientes em que um IPS não esteja disponível para fornecer uma camada adicional de proteção à funcionalidade principal do ASA.

Funcionalidade de detecção de ameaças

O recurso de detecção de ameaças tem três componentes principais:

1. Detecção básica de ameaças
2. Detecção avançada de ameaças
3. Verificando a detecção de ameaças

Cada um desses componentes é descrito em detalhes nestas seções.

Detecção Básica de Ameaças (Taxas no Nível do Sistema)

A detecção básica de ameaças é ativada por padrão em todos os ASAs que executam o 8.0(2) e posterior.

A detecção básica de ameaças monitora as taxas nas quais os pacotes são descartados por vários motivos pelo ASA como um todo. Isso significa que as estatísticas geradas pela detecção básica de ameaças só se aplicam a todo o equipamento e geralmente não são suficientemente granulares para fornecer informações sobre a origem ou a natureza específica da ameaça. Em vez disso, o ASA monitora pacotes descartados para esses eventos:

- Descarte de ACL (acl-drop) - Os pacotes são negados pelas listas de acesso.
- Pacotes inválidos (queda de pacote inválida) - Formatos de pacote inválidos, que incluem cabeçalhos L3 e L4 que não estão em conformidade com os padrões RFC.
- Limite de conexão (conn-limit-drop) - Pacotes que excedem um limite de conexão global ou configurado.
- Ataque de DoS (dos-drop) - ataques de negação de serviço (DoS).
- Firewall (fw-drop) - Verificações básicas de segurança de firewall.
- Ataque ICMP (queda icmp) - Pacotes ICMP suspeitos.
- Inspect (inspect-drop) - Negação por inspeção de aplicativo.
- Interface (interface-drop) - Pacotes eliminados por verificações de interface.
- Varredura (varredura-ameaça) - Ataques de varredura de rede/host.
- Ataque SYN (ataque SYN) - Ataques de sessão incompletos, o que inclui ataques SYN TCP e sessões UDP unidirecionais que não têm dados de retorno.

Cada um desses eventos tem um conjunto específico de acionadores que são usados para identificar a ameaça. A maioria dos acionadores está vinculada a motivos específicos de descarte de ASP, embora determinados syslogs e ações de inspeção também sejam considerados. Alguns acionadores são monitorados por várias categorias de ameaças. Alguns dos acionadores mais comuns estão descritos nesta tabela, embora

não seja uma lista exaustiva:

Ameaça básica	Gatilho(s) / Motivo(s) de queda ASP
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	Quedas de quadros disparadas por um mecanismo de inspeção
queda de interface	sp-security-failed no-route
ameaça de varredura	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
ataque SYN	Syslog %ASA-6-302014 com motivo de encerramento de "SYN Timeout"

Para cada evento, a detecção básica de ameaças mede as taxas em que esses descartes ocorrem durante um período de tempo configurado. Esse período é chamado de intervalo de taxa média (ARI) e pode variar de 600 segundos a 30 dias. Se o número de eventos que ocorrem dentro do ARI exceder os limites de taxa configurados, o ASA considerará esses eventos uma ameaça.

A detecção básica de ameaças tem dois limites configuráveis para quando considera eventos como uma ameaça: a taxa média e a taxa de intermitência. A taxa média é simplesmente o número médio de quedas por segundo dentro do período de tempo do ARI configurado. Por exemplo, se o limite de taxa média para quedas de ACL estiver configurado para 400 com um ARI de 600 segundos, o ASA calculará o número médio de pacotes que foram descartados pelas ACLs nos últimos 600 segundos. Se esse número for superior a 400 por segundo, o ASA registrará uma ameaça.

Da mesma forma, a taxa de intermitência é muito semelhante, mas observa períodos menores de dados de instantâneo, chamados de intervalo de taxa de intermitência (BRI, burst rate interval). A BRI é sempre menor que a ARI. Por exemplo, baseando-se no exemplo anterior, o ARI para quedas de ACL ainda é de 600 segundos e agora tem uma taxa de intermitência de 800. Com esses valores, o ASA calcula o número médio de pacotes descartados pelas ACLs em 20 segundos, onde 20 segundos é a BRI. Se esse valor calculado exceder 800 quedas por segundo, uma ameaça será registrada. Para determinar qual BRI é usada, o ASA calcula o valor de 1/30 do ARI. Portanto, no exemplo usado anteriormente, 1/30 de 600 segundos é 20 segundos. No entanto, a detecção de ameaças tem uma BRI mínima de 10 segundos, portanto, se 1/30 do ARI for menor que 10, o ASA ainda usará 10 segundos como BRI. Além disso, é importante observar que esse comportamento era diferente nas versões anteriores à 8.2(1), que usava um valor de 1/60 do ARI, em vez de 1/30. A BRI mínima de 10 segundos é a mesma para todas as versões de software.

Quando uma ameaça básica é detectada, o ASA simplesmente gera o syslog %ASA-4-733100 para alertar o administrador que uma possível ameaça foi identificada. O número médio, atual e total de eventos para cada categoria de ameaça pode ser visto com o comando **show threat-detection rate**. O número total de eventos cumulativos é a soma do número de eventos observados nas últimas 30 amostras BRI.

A taxa de intermitência no syslog é calculada com base no número de pacotes descartados até agora na BRI atual. O cálculo é feito periodicamente em uma BRI. Quando ocorre uma violação, um syslog é acionado. É limitado que apenas um syslog seja gerado em uma BRI. A taxa de intermitência em "show threat-detection rate" é calculada com base no número de pacotes descartados na última BRI. O design da diferença é que o syslog é sensível ao tempo, portanto, se uma violação acontecer na BRI atual, ela teria uma chance de ser capturada. "show threat-detection rate" é menos sensível ao tempo, portanto, o número da última BRI é usado.

A detecção básica de ameaças não realiza nenhuma ação para interromper o tráfego desviante ou impedir ataques futuros. Nesse sentido, a detecção básica de ameaças é puramente informativa e pode ser usada como um mecanismo de monitoramento ou relatório.

Detecção Avançada de Ameaças (Estatísticas em Nível de Objeto e Principais N)

Diferentemente da Detecção Básica de Ameaças, a Detecção Avançada de Ameaças pode ser usada para rastrear estatísticas de objetos mais granulares. O ASA suporta estatísticas de rastreamento para IPs de host, portas, protocolos, ACLs e servidores protegidos por interceptação TCP. A detecção avançada de ameaças só é habilitada por padrão para estatísticas de ACL.

Para objetos de host, porta e protocolo, a Detecção de Ameaças rastreia o número de pacotes, bytes e descartes que foram enviados e recebidos por esse objeto dentro de um período de tempo específico. Para ACLs, a detecção de ameaças monitora as 10 principais ACEs (de permissão e de negação) que foram as mais atingidas em um período de tempo específico.

Os períodos de tempo rastreados em todos esses casos são 20 minutos, 1 hora, 8 horas e 24 horas. Embora os

períodos de tempo em si não sejam configuráveis, o número de períodos rastreados por objeto pode ser ajustado com a palavra-chave 'número da taxa'. Consulte a seção Configuração para obter mais informações. Por exemplo, se 'número da taxa' estiver definido como 2, você verá todas as estatísticas para 20 minutos, 1 hora e 8 horas. se 'número da taxa' estiver definido como 1, você verá todas as estatísticas para 20 minutos, 1 hora. Não importa o que aconteça, a taxa de 20 minutos é sempre exibida.

Quando a interceptação de TCP está habilitada, a Detecção de Ameaças pode controlar os 10 principais servidores que são considerados sob ataque e protegidos pela interceptação de TCP. As estatísticas de interceptação de TCP são semelhantes à Detecção Básica de Ameaças, no sentido de que o usuário pode configurar o intervalo de taxa medido juntamente com as taxas médias específicas (ARI) e de intermitência (BRI). As estatísticas de detecção avançada de ameaças para interceptação TCP estão disponíveis apenas no ASA 8.0(4) e posterior.

As estatísticas avançadas de detecção de ameaças são visualizadas através dos comandos **show threat-detection statistics** e **show threat-detection statistics top**. Esse também é o recurso responsável pelo preenchimento dos gráficos "principais" no painel de firewall do ASDM. Os únicos syslogs gerados pela Detecção avançada de ameaças são %ASA-4-733104 e %ASA-4-733105, que são acionados quando as taxas média e de intermitência (respectivamente) são excedidas para estatísticas de interceptação TCP.

Assim como a Detecção básica de ameaças, a Detecção avançada de ameaças é puramente informativa. Nenhuma ação é tomada para bloquear o tráfego com base nas estatísticas de detecção avançada de ameaças.

Verificando a detecção de ameaças

A detecção de ameaças de varredura é usada para rastrear suspeitos de ataque que criam conexões em excesso de hosts em uma sub-rede ou em muitas portas em um host/sub-rede. A varredura da detecção de ameaças é desativada por padrão.

A varredura da detecção de ameaças baseia-se no conceito de detecção básica de ameaças, que já define uma categoria de ameaça para um ataque de varredura. Portanto, as configurações de intervalo de taxa, taxa média (ARI) e taxa de intermitência (BRI) são compartilhadas entre a detecção básica e a detecção de ameaças de varredura. A diferença entre os dois recursos é que, enquanto a Detecção Básica de Ameaças indica apenas que os limites da taxa média ou de intermitência foram ultrapassados, a Detecção de Ameaças de Varredura mantém um banco de dados de endereços IP do invasor e do alvo que pode ajudar a fornecer mais contexto sobre os hosts envolvidos na varredura. Além disso, somente o tráfego realmente recebido pelo host/sub-rede de destino é considerado pela Varredura de Detecção de Ameaças. A Detecção Básica de Ameaças ainda pode disparar uma ameaça de Varredura, mesmo que o tráfego seja descartado por uma ACL.

A varredura da detecção de ameaças pode, opcionalmente, reagir a um ataque evitando o IP do invasor. Isso torna a detecção de ameaças de varredura o único subconjunto do recurso de detecção de ameaças que pode afetar ativamente as conexões por meio do ASA.

Quando a detecção de ameaças de varredura detecta um ataque, o %ASA-4-733101 é registrado para o invasor e/ou IPs de destino. Se o recurso estiver configurado para evitar o invasor, o %ASA-4-733102 será registrado quando a Varredura da Detecção de Ameaças gerar um bloqueio. %ASA-4-733103 é registrado quando o shun é removido. O comando **show threat-detection scanning-threat** pode ser usado para exibir todo o banco de dados de ameaças de varredura.

Limitações

- A Detecção de Ameaças só está disponível no ASA 8.0(2) e posterior. Ele não é suportado na plataforma ASA 1000V.
- A Detecção de Ameaças só é suportada no modo de contexto único.

- Somente ameaças diretas são detectadas. O tráfego enviado ao próprio ASA não é considerado pela Detecção de ameaças.
- As tentativas de conexão TCP que são redefinidas pelo servidor de destino não são contadas como um ataque SYN ou uma ameaça de Varredura.

Configuração

Detecção básica de ameaças

A Detecção Básica de Ameaças é ativada com o comando **threat-detection basic-threat**.

```
<#root>

ciscoasa(config)#

threat-detection basic-threat
```

As taxas padrão podem ser visualizadas com o comando **show run all threat-detection**.

```
<#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
```

Para ajustar essas taxas com valores personalizados, basta reconfigurar o comando **threat-detection rate** para a categoria de ameaça apropriada.

```
<#root>

ciscoasa(config)#
```

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

Cada categoria de ameaça pode ter no máximo 3 taxas diferentes definidas (com IDs de taxa 1, taxa 2 e taxa 3). A ID de taxa específica que é excedida é referenciada no syslog %ASA-4-733100.

No exemplo anterior, a detecção de ameaças cria 733100 de syslog somente quando o número de quedas de ACL excede 250 quedas/segundo em 1200 segundos ou 550 quedas/segundo em 40 segundos.

Detecção avançada de ameaças

Use o comando **threat-detection statistics** para habilitar a Detecção Avançada de Ameaças. Se nenhuma palavra-chave de recurso específica for fornecida, o comando ativará o rastreamento de todas as estatísticas.

```
<#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>
```

Para configurar o número de intervalos de taxa que são rastreados para estatísticas de host, porta, protocolo ou ACL, use a palavra-chave **number-of-rate**.

```
<#root>

ciscoasa(config)#

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

A palavra-chave number-of-rate configura a Detecção de Ameaças para rastrear apenas o menor *n* número de intervalos.

Para habilitar as estatísticas de interceptação TCP, use o comando **threat-detection statistics tcp-intercept**.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept
```

Para configurar taxas personalizadas para estatísticas de interceptação TCP, use as palavras-chave **rate-**

interval, **average-rate** e **burst-rate**.

```
<#root>

ciscoasa(config)#

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

Verificando a detecção de ameaças

Para habilitar a detecção de ameaças de varredura, use o comando **threat-detection scanning-threat**.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat
```

Para ajustar as taxas de uma ameaça de varredura, use o mesmo comando **threat-detection rate** usado pela Detecção Básica de Ameaças.

```
<#root>

ciscoasa(config)#

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

Para permitir que o ASA evite um IP do invasor de verificação, adicione a palavra-chave **shun** ao comando **threat-detection scanning-threat**.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

Isso permite que a Detecção de ameaças à varredura crie um shun de uma hora para o invasor. Para ajustar a duração do shun, use o comando **threat-detection scanning-threat shun duration**.

```
<#root>

ciscoasa(config)#

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

Em alguns casos, você pode impedir que o ASA evite determinados IPs. Para fazer isso, crie uma exceção

com o comando **threat-detection scanning-threat shun except**.

```
<#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
```

Desempenho

A detecção básica de ameaças tem pouco impacto no desempenho do ASA. A detecção avançada e a detecção de ameaças de varredura consomem muito mais recursos, pois precisam controlar várias estatísticas na memória. Somente a Varredura de Detecção de Ameaças com a função shun ativada pode impactar ativamente o tráfego que, de outra forma, teria sido permitido.

À medida que as versões do software ASA progrediram, a utilização de memória da Detecção de ameaças foi significativamente otimizada. No entanto, deve-se tomar cuidado para monitorar a utilização de memória do ASA antes e depois que a Detecção de ameaças for ativada. Em alguns casos, seria melhor ativar apenas algumas estatísticas (por exemplo, estatísticas de host) temporariamente enquanto você soluciona ativamente um problema específico.

Para obter uma visão mais detalhada do uso de memória da Detecção de ameaças, execute o comando **show memory app-cache threat-detection [detail]**.

Ações recomendadas

Estas seções fornecem algumas recomendações gerais para ações que podem ser tomadas quando ocorrem vários eventos relacionados à Detecção de ameaças.

Quando uma taxa de queda básica é excedida e o %ASA-4-733100 é gerado

Determine a categoria de ameaça específica mencionada no syslog %ASA-4-733100 e correlacione isso com a saída de `show threat-detection rate` . Com essas informações, verifique a saída de `show asp drop` para determinar os motivos pelos quais o tráfego é descartado.

Para obter uma visão mais detalhada do tráfego que é descartado por um motivo específico, use uma captura de queda ASP com o motivo em questão para ver todos os pacotes que são descartados. Por exemplo, se as ameaças de queda de ACL forem registradas, capture a razão de queda de ASP de `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
```

Essa captura mostra que o pacote descartado é um pacote UDP/53 de 10.10.10.10 a 192.168.1.100.

Se o %ASA-4-733100 relatar uma ameaça à Varredura, também poderá ser útil habilitar temporariamente a Detecção de Ameaças à Varredura. Isso permite que o ASA acompanhe os IPs de origem e destino envolvidos no ataque.

Como a Detecção Básica de Ameaças monitora principalmente o tráfego que já é descartado pelo ASP, nenhuma ação direta é necessária para interromper uma ameaça potencial. As exceções a isso são Ataques SYN e Ameaças de varredura, que envolvem o tráfego que passa pelo ASA.

Se as quedas observadas na captura de quedas do ASP forem legítimas e/ou esperadas para o ambiente de rede, ajuste os intervalos de taxa básica para um valor mais apropriado.

Se os descartes mostrarem tráfego ilegítimo, devem ser tomadas medidas para bloquear ou limitar a taxa do tráfego antes que ele chegue ao ASA. Isso pode incluir ACLs e QoS em dispositivos upstream.

Para ataques SYN, o tráfego pode ser bloqueado em uma ACL no ASA. A interceptação de TCP também pode ser configurada para proteger os servidores de destino, mas isso pode simplesmente resultar em uma ameaça de Limite de Conn que é registrada.

Para verificar ameaças, o tráfego também pode ser bloqueado em uma ACL no ASA. Fazendo a varredura da detecção de ameaças com o shunpode ser ativada para permitir que o ASA bloqueie proativamente todos os pacotes do invasor por um período de tempo definido.

Quando uma ameaça de verificação é detectada e o %ASA-4-733101 é registrado

%ASA-4-733101 deve listar o host/sub-rede de destino ou o endereço IP do invasor. Para obter a lista completa de alvos e invasores, verifique a saída de show threat-detection scanning-threat.

Capturas de pacotes nas interfaces do ASA que enfrentam o invasor e/ou o(s) alvo(s) também podem ajudar a esclarecer a natureza do ataque.

Se a varredura detectada não for esperada, devem ser tomadas medidas para bloquear ou limitar a taxa do tráfego antes que ele atinja o ASA. Isso pode incluir ACLs e QoS em dispositivos upstream. Quando o comando shuné adicionada à configuração Scanning Threat Detection, permitindo que o ASA remova proativamente todos os pacotes do IP do invasor por um período de tempo definido. Como último recurso, o tráfego também pode ser bloqueado manualmente no ASA por meio de uma política de interceptação de ACL ou TCP.

Se a varredura detectada for um falso positivo, ajuste os intervalos da taxa de ameaças de varredura para um valor mais apropriado para o ambiente de rede.

Quando um invasor é removido e o %ASA-4-733102 é registrado

%ASA-4-733102 lista o endereço IP do invasor ignorado. Use o show threat-detection shun para exibir uma lista

completa de invasores que foram evitados especificamente pela Detecção de ameaças. Use o show shun para exibir a lista completa de todos os IPs que são ativamente evitados pelo ASA (isso inclui fontes diferentes da Detecção de ameaças).

Se o shun for parte de um ataque legítimo, nenhuma ação adicional será necessária. No entanto, seria útil bloquear manualmente o tráfego do invasor o mais a montante possível em direção à origem. Isso pode ser feito via ACLs e QoS. Isso garante que os dispositivos intermediários não precisem desperdiçar recursos em tráfego ilegítimo.

Se a ameaça de verificação que disparou o shun for um falso positivo, remova manualmente o shun com o comando clear threat-detection shun [IP_address] comando.

Quando %ASA-4-733104 e/ou %ASA-4-733105 estiver registrado

%ASA-4-733104 e %ASA-4-733105 lista o host de destino do ataque que está atualmente protegido pela interceptação TCP. Para obter mais detalhes sobre as taxas de ataque e os servidores protegidos, verifique a saída de 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)
```

Quando a Detecção Avançada de Ameaças detecta um ataque dessa natureza, o ASA já protege o servidor de destino através da interceptação TCP. Verifique os limites de conexão configurados para garantir que eles forneçam proteção adequada para a natureza e a taxa do ataque. Além disso, seria benéfico bloquear manualmente o tráfego do invasor o mais a montante possível em direção à origem. Isso pode ser feito via ACLs e QoS. Isso garante que os dispositivos intermediários não precisem desperdiçar recursos em tráfego ilegítimo.

Se o ataque detectado for um falso positivo, ajuste as taxas de um ataque de interceptação TCP para um valor mais apropriado com o comando threat-detection statistics tcp-interceptcomando.

Como disparar manualmente uma ameaça

Para testar e solucionar problemas, pode ser útil disparar manualmente várias ameaças. Esta seção contém dicas sobre como acionar alguns tipos comuns de ameaças.

Ameaça básica - Queda de ACL, firewall e varredura

Para disparar uma determinada Ameaça Básica, consulte a tabela na seção anterior Funcionalidade. Escolha um motivo de queda de ASP específico e envie o tráfego pelo ASA que seria descartado pelo motivo de queda de ASP apropriado.

Por exemplo, as ameaças de queda de ACL, firewall e varredura consideram a taxa de pacotes descartados por queda de ACL. Conclua estas etapas para disparar essas ameaças simultaneamente:

1. Crie uma ACL na interface externa do ASA que descarte explicitamente todos os pacotes TCP enviados a um servidor de destino na parte interna do 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. A partir de um invasor fora do ASA (10.10.10.10), use nmap para executar uma verificação TCP SYN em cada porta no servidor de destino:

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

> **Observação**: o T5 configura o nmap para executar a verificação o mais rápido possível. Com base nos recursos do PC do invasor, isso ainda não é rápido o suficiente para disparar algumas das taxas padrão. Se esse for o caso, simplesmente reduza as taxas configuradas para a ameaça que você deseja ver. Quando você define o ARI e o BRI como 0, o Basic Threat Detection sempre aciona a ameaça, independentemente da taxa.

---

3. Observe que as ameaças básicas são detectadas para as ameaças de queda de ACL, firewall e varredura:

```
%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
```

> **Observação**: neste exemplo, as ARIs e BRIs de queda de ACL e de firewall foram definidas como 0, de modo que sempre acionam uma ameaça. É por isso que as taxas máximas configuradas são listadas como 0.

Ameaça avançada - Interceptação de TCP

1. Crie uma ACL na interface externa que permita todos os pacotes TCP enviados a um servidor de destino na parte interna do 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. Se o servidor de destino não existir de fato, ou se ele redefinir as tentativas de conexão do invasor, configure uma entrada ARP falsa no ASA para bloquear o tráfego de ataque na interface interna:

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

3. Crie uma política de interceptação TCP simples no 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
```

A partir de um invasor fora do ASA (10.10.10.10), use o nmap para executar uma verificação TCP SYN em cada porta no servidor de destino:

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

Observe que a detecção de ameaças rastreia o servidor protegido:

<#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)
```

Varredura de ameaças

1. Crie uma ACL na interface externa que permita todos os pacotes TCP enviados a um servidor de destino na parte interna do 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
```

Observação: para que a Detecção de ameaças de varredura rastreie os IPs do alvo e do invasor,

---

o tráfego deve ser permitido através do ASA.

2. Se o servidor de destino não existir de fato, ou se ele redefinir as tentativas de conexão do invasor, configure uma entrada ARP falsa no ASA para bloquear o tráfego de ataque na interface interna:

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

Observação: as conexões redefinidas pelo servidor de destino não são contadas como parte da ameaça.

3. A partir de um invasor fora do ASA (10.10.10.10), use o nmap para executar uma verificação TCP SYN em cada porta no servidor de destino:

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

Observação: o T5 configura o nmap para executar a verificação o mais rápido possível. Com base nos recursos do PC do invasor, isso ainda não é rápido o suficiente para disparar algumas das taxas padrão. Se esse for o caso, simplesmente reduza as taxas configuradas para a ameaça que você deseja ver. Quando você define o ARI e o BRI como 0, o Basic Threat Detection sempre aciona a ameaça, independentemente da taxa.

4. Observe que uma ameaça de Varredura é detectada, o IP do invasor é rastreado e o invasor é evitado:

```
%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
```

Informações Relacionadas

- **Guia de configuração do ASA**
- **Referência de comando do ASA**
- **Mensagens do Syslog do Cisco Secure Firewall ASA Series**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.