Funcionalidade e configuração da detecção da ameaça ASA

Índice

Introdução

Este documento descreve a funcionalidade e a configuração básica da característica Threat Detection do Cisco Adaptive Security Appliance (ASA). A detecção da ameaça fornece administradores de firewall as ferramentas necessárias para identificar, compreender, e parar ataques antes que alcancem a infraestrutura de rede interna. A fim fazer assim, a característica confia em um número disparadores e de estatísticas diferentes, que é descrita em um detalhe mais adicional nestas seções.

A detecção da ameaça pode ser usada em todo o Firewall ASA que executar uma versão de software de 8.0(2) ou mais atrasado. Embora a detecção da ameaça não seja um substituto para uma solução dedicada IDS/IPS, pode ser usada nos ambientes onde um IPS não está disponível para fornecer uma camada adicionada de proteção à funcionalidade do núcleo do ASA.

Funcionalidade da detecção da ameaça

A característica da detecção da ameaça tem três componentes principais:

1. Detecção básica da ameaça
2. Detecção avançada da ameaça
3. Detecção de varredura da ameaça

Cada um destes componentes é descrito em detalhe nestas seções.

Detecção básica da ameaça (taxas do nível de sistema)

A detecção básica da ameaça é permitida à revelia em todo o corredor ASA 8.0(2) e mais atrasado.

A detecção básica da ameaça monitora as taxas em que os pacotes são deixados cair por razões diversas pelo ASA no conjunto. Isto significa que as estatísticas geradas pela detecção básica da ameaça se aplicam somente ao dispositivo inteiro e não se são geralmente granuladas bastante fornecer a informação na fonte ou na natureza específica da ameaça. Em lugar de, o ASA monitora pacotes descartado para estes eventos:

- **Gota ACL (ACL-gota)** - Os pacotes são negados por Listas de acesso
- **Pacotes ruins (ruim-pacote-gota)** - O pacote inválido formata, que inclui os encabeçamentos L3 e L4 que não se conformam aos padrões de RFC
- **Limite conexão (CONN-limite-gota)** - Pacotes que excedem um limite configurado ou da conexão global
- **Ataque DoS (dos-gota)** - Ataque de recusa de serviço (DOS)
- **Firewall (FW-gota)** - Verificações de segurança básicas do Firewall
- **Ataque ICMP (ICMP-gota)** - Pacotes ICMP suspeitos
- **Inspecione (inspecionar-gota)** - Recusa pela inspeção de aplicativo
- **Relação (relação-gota)** - Pacotes deixados cair por verificações de interface
- **Fazer a varredura (exploração-ameaça)** - Ataques da exploração da rede/host
- **Ataque SYN (ataque SYN)** - Ataques incompletos da sessão, que inclui os ataques SYN TCP e as sessões de UDP unidirecionais que não têm nenhum dados do retorno

Cada um destes eventos tem um grupo específico de disparadores que são usados para identificar a ameaça. A maioria de disparadores são amarrados de volta às razões específicas da gota ASP, embora os determinados Syslog e ações da inspeção são considerados igualmente. Alguns disparadores são monitorados por categorias múltiplas da ameaça. Alguns dos disparadores os mais comuns são esboçados nesta tabela, embora não é uma lista exaustiva:

Ameaça básica	Razões da gota dos disparadores/ASP
ACL-gota	ACL-gota
ruim-pacote-gota	inválido-TCP-HDR-comprimento inválido-IP-encabeçamento inspecionar-dns-PAK-demasiado-longo inspecionar-dns-identificação-não-combinado
CONN-limite-gota	CONN-limite
dos-gota	SP-Segurança-falhado
FW-gota	inspecionar-ICMP-segs.-NUM-não-combinado inspecionar-dns-PAK-demasiado-longo

	inspecionar-dns-identificação-não-combinado
	SP-Segurança-falhado
	ACL-gota
ICMP-gota	inspecionar-ICMP-segs.-NUM-não-combinado
inspecionar-gota	Gotas do quadro provocadas por um motor da inspeção
relação-gota	SP-Segurança-falhado
	nenhum-rota
	tcp-3whs-failed
	TCP-não-SYN
	SP-Segurança-falhado
exploração-ameaça	ACL-gota
	inspecionar-ICMP-segs.-NUM-não-combinado
	inspecionar-dns-PAK-demasiado-longo
	inspecionar-dns-identificação-não-combinado
ataque SYN	Syslog %ASA-6-302014 com razão do teardown do “Intervalo de SYN”

Para cada evento, a detecção básica da ameaça mede as taxas que estas gotas ocorrem durante um período configurado de tempo. Este período de tempo é chamado o **intervalo da taxa média (ARI)** e pode variar de 600 segundos a 30 dias. Se o número de eventos que ocorrem dentro do ARI excede os pontos iniciais da taxa configurada, o ASA considera estes eventos uma ameaça.

A detecção básica da ameaça tem dois limiares configurável para quando considera eventos ser uma ameaça: **a taxa média** e a **taxa de intermitência**. A taxa média é simplesmente o número médio de gotas por segundo dentro do período de tempo do ARI configurado. Por exemplo, se o ponto inicial da taxa média para gotas ACL é configurado para 400 com um ARI de 600 segundos, o ASA calcula o número médio de pacotes que foram deixados cair por ACL nos últimos 600 segundos. Se este número despeja ser maior de 400 por segundo, o ASA registra uma ameaça.

Igualmente, a taxa de intermitência é muito similar mas olhares nos períodos menores de dados do instantâneo, chamados o **intervalo da taxa de intermitência (BRI)**. O BRI é sempre menor do que o ARI. Por exemplo, construir no exemplo anterior, o ARI para gotas ACL é ainda 600 segundos e tem agora uma taxa de intermitência de 800. Com estes valores, o ASA calcula o número médio de pacotes deixados cair por ACL nos últimos 20 segundos, onde 20 segundos são o BRI. Se este valor calculado excede 800 gotas por segundo, uma ameaça está registrada. A fim determinar que BRI é usado, o ASA calcula o valor do 1/30th do ARI. Consequentemente, no exemplo usado previamente, o 1/30th de 600 segundos é 20 segundos. Contudo, a detecção da ameaça tem um mínimo BRI dos segundos 10, assim que se o 1/30th do ARI é menos do que o 10, o ASA ainda usa os segundos 10 como o BRI. Também, é importante notar que este comportamento era diferente nas versões antes de 8.2(1), que usou um valor do 1/60th do ARI, em vez do 1/30th. O mínimo BRI dos segundos 10 é o mesmo para todas as versões de software.

Quando uma ameaça básica é detectada, o ASA gerencie simplesmente o Syslog %ASA-4-733100 para alertar o administrador que uma ameaça potencial esteve identificada. A média, a corrente, e o número total de eventos para cada categoria da ameaça podem ser considerados com o **comando rate da ameaça-detecção da mostra**. O número total de eventos cumulativos é a soma do número de eventos vistos nas últimas 30 amostras BRI.

A detecção básica da ameaça não toma nenhuma ações a fim parar o tráfego causador ou impedir os ataques futuros. Neste sentido, a detecção básica da ameaça é puramente informativa e pode ser usada como uma monitoração ou um mecanismo de relatório.

Detecção avançada da ameaça (estatísticas do objeto e parte superior niveladas N)

Ao contrário da detecção básica da ameaça, a detecção avançada da ameaça pode ser usada para seguir estatísticas para uns objetos mais granulados. O ASA apoia o seguimento de estatísticas para o host IPs, as portas, os protocolos, os ACL, e os server protegidos pelo TCP Intercept. A detecção avançada da ameaça é permitida somente à revelia para estatísticas ACL.

Para o host, a porta, e os objetos do protocolo, a detecção da ameaça mantém-se a par do número de pacotes, de bytes, e de gotas que foram enviadas e recebidas por esse objeto dentro de um período de tempo específico. Para ACL, a detecção da ameaça mantém-se a par da parte superior 10 ACE (a licença e nega) que sejam batidos mais dentro de um período de tempo específico.

Os períodos de tempo seguidos em todos estes casos são 20 minutos, 1 hora, 8 horas, e 24 horas. Quando os períodos de tempo eles mesmos não forem configuráveis, o número de períodos que são seguidos pelo objeto pode ser ajustado com a palavra-chave da “número--taxa”. Veja a seção de configuração para mais informação. Por exemplo, se a “número--taxa” é ajustada a 2, você vê todas as estatísticas para 20 minutos, 1 hora e 8 horas. se a “número--taxa” é ajustada a 1, você vê todas as estatísticas por 20 minutos, 1 hora. Não importa o que, a taxa 20 minuto é indicada sempre.

Quando o TCP Intercept é permitido, a detecção da ameaça pode manter-se a par dos server da parte superior 10 que são considerados estar sob o ataque e protegidos pelo TCP Intercept. As estatísticas para o TCP Intercept são similares à detecção básica da ameaça no sentido que o usuário pode configurar o taxa-intervalo medido junto com médio específico (ARI) e estourar as taxas (BRI). As estatísticas avançadas da detecção da ameaça para o TCP Intercept estão somente disponíveis em ASA 8.0(4) e mais atrasadas.

As estatísticas avançadas da detecção da ameaça são vistas através das **estatísticas da ameaça-detecção da mostra** e **mostram comandos top das estatísticas da ameaça-detecção**. Este é igualmente o responsável da característica para povoar os gráficos “superiores” no painel do Firewall do ASDM. Os únicos Syslog que são gerados por detecção avançada da ameaça são %ASA-4-733104 e %ASA-4-733105, que estão provocados quando a média e as taxas de intermitência (respectivamente) são excedidas para estatísticas TCP Intercept.

Como a detecção básica da ameaça, a detecção avançada da ameaça é puramente informativa. Nenhuma ação é tomada para obstruir o tráfego baseado nas estatísticas avançadas da detecção da ameaça.

Detecção de varredura da ameaça

A detecção de varredura da ameaça é usada a fim manter-se a par dos atacantes suspeitados que criam conexões anfitriões demais em uma sub-rede, ou das muitas portas em um host/sub-rede. A detecção de varredura da ameaça é desabilitada à revelia.

Construções de varredura da detecção da ameaça no conceito da detecção básica da ameaça, que já define uma categoria da ameaça para um ataque da exploração. Consequentemente, o taxa-intervalo, a taxa média (ARI), e os ajustes da taxa de intermitência (BRI) são compartilhados entre a detecção básica e da exploração da ameaça. A diferença entre as 2 características é que quando a detecção básica da ameaça indicar somente que a média ou os pontos iniciais da taxa de intermitência estiveram cruzados, a detecção de varredura da ameaça mantém um base de

dados do atacante e dos endereços IP de destino que possa ajudar a fornecer mais contexto em torno dos anfitriões envolvidos na varredura. Adicionalmente, somente o tráfego que é recebido realmente pelo host de destino/sub-rede é considerado fazendo a varredura a detecção da ameaça. A detecção básica da ameaça pode ainda provocar uma ameaça da exploração mesmo se o tráfego é deixado cair por um ACL.

A detecção de varredura da ameaça pode opcionalmente reagir a um ataque evitando o IP do atacante. Isto faz a detecção da ameaça da exploração o único subconjunto da característica da detecção da ameaça que pode ativamente afetar conexões com o ASA.

Quando a detecção de varredura da ameaça detecta um ataque, %ASA-4-733101 está registrado para o atacante e/ou o alvo IPs. Se a característica é configurada para evitar o atacante, %ASA-4-733102 está registrado quando a detecção de varredura da ameaça gerencie evitar. %ASA-4-733103 é registrado quando evitar é removido. O comando da exploração-**ameaça da ameaça-detecção da mostra** pode ser usado a fim ver o base de dados inteiro da ameaça da exploração.

Limitações

- A detecção da ameaça está somente disponível em ASA 8.0(2) e mais atrasada. Não é apoiada na plataforma ASA 1000V.
- A detecção da ameaça é apoiada somente no único modo do contexto.
- Somente as ameaças da através--caixa são detectadas. O tráfego enviado ao ASA próprio não é considerado pela detecção da ameaça.
- As tentativas da conexão de TCP que são restauradas pelo server visado não são contadas como uma ameaça do ataque SYN ou da exploração.

Configuração

Detecção básica da ameaça

A detecção básica da ameaça é permitida com o comando da básico-**ameaça da ameaça-detecção**.

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

As taxas padrão podem ser vistas com a **mostra executam todo o** comando da ameaça-**detecção**.

```
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
```

A fim ajustar estas taxas com valores feitos sob encomenda, reconfigure simplesmente o **comando rate da ameaça-detecção** para a categoria apropriada da ameaça.

```
ciscoasa(config)# threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate
550
```

Cada categoria da ameaça pode ter um máximo de 3 taxas diferentes definidas (com taxa ID da taxa 1, da taxa 2, e da taxa 3). A taxa particular ID que é excedida é provida no Syslog %ASA-4-733100.

No exemplo anterior, a detecção da ameaça cria o Syslog 733100 somente quando o número de gotas ACL excede 250 gotas/em segundo sobre 1200 segundos ou 550 gotas/em segundo sobre 40 segundos.

Detecção avançada da ameaça

Use o **comando statistics da ameaça-detecção** a fim permitir detecção avançada da ameaça. Se nenhuma palavra-chave específica da característica é fornecida, o comando permite o seguimento para todas as estatísticas.

```
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>
```

A fim configurar o número de intervalos da taxa que são seguidos para o host, a porta, o protocolo, ou as estatísticas ACL, use a palavra-chave da número--**taxa**.

```
ciscoasa(config)# threat-detection statistics host number-of-rate 2
```

A palavra-chave da número--taxa configura a detecção da ameaça para seguir somente o número de intervalo o mais curto *n*.

A fim permitir estatísticas TCP Intercept, use o comando das **estatísticas TCP Intercept da ameaça-detecção**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept
```

A fim configurar taxas feitas sob encomenda para estatísticas TCP Intercept, use o taxa-**intervalo**, a **taxa média**, e as palavras-chaves da **taxa de intermitência**.

```
ciscoasa(config)# threat-detection statistics tcp-intercept rate-interval 45
burst-rate 400 average-rate 100
```

Detecção de varredura da ameaça

A fim permitir a detecção da ameaça da exploração, use o comando da exploração-**ameaça da ameaça-detecção**.

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

A fim ajustar as taxas para uma exploração-ameaça, use o mesmo **comando rate da ameaça-detecção** usado pela detecção básica da ameaça.

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

A fim permitir que o ASA evite um IP do atacante da exploração, adicionar a palavra-chave **evitar ao** comando da exploração-**ameaça da ameaça-detecção**.

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

Isto reserva fazer a varredura da detecção da ameaça para criar uma uma hora evita para o atacante. A fim ajustar a duração evitar, use a exploração-**ameaça da ameaça-detecção evitam o** comando da **duração**.

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

Em alguns casos, você pode ainda querer impedir que o ASA evite determinado IPs. A fim fazer isto, crie uma exceção com a exploração-**ameaça da ameaça-detecção evitam o comando except**.

```
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 da ameaça tem o impacto no desempenho muito pequeno no ASA. A detecção avançada e da exploração da ameaça é muito mais repleto de recursos porque têm que se manter a par de várias estatísticas na memória. Somente a detecção de varredura da ameaça com a função evitar permitida pode ativamente impactar o tráfego que seria permitido de outra maneira.

Enquanto as versões de software ASA progrediram, a utilização de memória da detecção da ameaça esteve aperfeiçoada significativamente. Contudo, deve ser tomado para monitorar a utilização de memória do ASA antes e depois de que a detecção da ameaça é permitida. Em alguns casos, pôde ser melhor permitir somente temporariamente determinadas estatísticas (por exemplo, estatísticas do host) ao ativamente pesquisar defeitos uma edição específica.

Para mais vista detalhada da utilização de memória da detecção da ameaça, execute o comando do **[detail] da ameaça-detecção do APP-esconderijo da memória da mostra**.

Ações recomendadas

Estas seções fornecem algumas recomendações gerais para as ações que podem ser tomadas quando os eventos Detecção-relacionados da vária ameaça ocorrem.

Quando uma taxa básica da gota é excedida e %ASA-4-733100 está gerado

Determine a categoria específica da ameaça mencionada no Syslog %ASA-4-733100 e correlacione isto com a saída da **taxa da ameaça-detecção da mostra**. Com esta informação, verifique a saída da **gota asp da mostra** a fim determinar as razões pelas quais o tráfego está sendo deixado cair.

Para mais vista detalhada do tráfego que é deixado cair para uma razão específica, use uma captação da gota ASP com a razão na pergunta a fim ver todos os pacotes que estão sendo deixados cair. Por exemplo, se as ameaças da gota ACL estão sendo registradas, captação na razão da gota ASP da ACL-**gota**:

```
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
```

Esta captação mostra que o pacote que está sendo deixado cair é um pacote UDP/53 de 10.10.10.10 a 192.168.1.100.

Se %ASA-4-733100 relata uma ameaça da exploração, pode igualmente ser útil permitir temporariamente a detecção da ameaça da exploração. Isto permite que o ASA mantenha-se a par da fonte e do ips de destino envolvidos no ataque.

Desde que a detecção básica da ameaça monitora na maior parte o tráfego que está sendo deixado cair já pelo ASP, nenhuma ação direta é exigida para parar uma ameaça potencial. As exceções a esta são as ameaças dos ataques SYN e da exploração, que envolvem o tráfego que passa com o ASA.

Se as gotas consideradas na captação da gota ASP são legítimas e/ou esperadas para o ambiente de rede, ajuste os intervalos da taxa básica a um valor mais apropriado.

Se as gotas mostram o tráfego ilegítimo, as ações devem ser tomadas para obstruir ou limite de taxa o tráfego antes que alcance o ASA. Isto pode incluir ACL e QoS em dispositivos ascendentes.

Para ataques SYN, o tráfego pode ser obstruído em um ACL no ASA. O TCP Intercept poderia igualmente ser configurado para proteger os server visados, mas este poderia simplesmente conduzir a uma ameaça do limite conexão que está sendo registrada pelo contrário.

Para ameaças de varredura, o tráfego pode igualmente ser obstruído em um ACL no ASA. A detecção de varredura da ameaça com a opção **evitar** pode ser permitida de permitir que o ASA obstrua dinamicamente todos os pacotes do atacante por um período de tempo definido.

Quando uma ameaça da exploração é detectada e %ASA-4-733101 está registrado

%ASA-4-733101 deve alistar o host de destino/sub-rede ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante. Para a lista completa dos alvos e dos atacantes, verifique a saída da exploração-**ameaça da ameaça-detecção da mostra**.

As capturas de pacote de informação nas relações ASA que enfrentam o atacante e/ou os alvos podem igualmente ajudar a esclarecer a natureza do ataque.

Se a varredura detectada é não esperada, as ações devem ser tomadas para obstruir ou limite de taxa o tráfego antes que alcance o ASA. Isto pode incluir ACL e QoS em dispositivos ascendentes. Adicionar a opção **evitar à** configuração da detecção da ameaça da exploração pode igualmente permitir que o ASA deixe cair dinamicamente todos os pacotes do IP do

atacante por um período de tempo definido. Como um último recurso, o tráfego pode igualmente ser obstruído manualmente no ASA através de uma política ACL ou TCP Intercept.

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

Quando um atacante é evitado e %ASA-4-733102 está registrado

%ASA-4-733102 alista o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante evitado. Use o **comando shun da ameaça-detecção da mostra** a fim ver uma lista completa dos atacantes que foram evitados pela detecção da ameaça especificamente. Use o **comando show shun** a fim ver a lista completa de todos os IPs que está sendo evitado ativamente pelo ASA (que inclui das fontes diferentes da detecção da ameaça).

Se evitar é parte de um ataque legítimo, nenhuma ação mais adicional está exigida. Contudo, seria benéfico obstruir manualmente tão distante rio acima o tráfego do atacante para a fonte como possível. Isto pode ser feito através dos ACL e do QoS. Isto assegura-se de que os dispositivos intermediários não precisem de desperdiçar os recursos que processam o tráfego ilegítimo.

Se a ameaça da exploração que provocou evitar era um falso positivo, remova manualmente evitar com a ameaça-**detecção clara evitam o** comando do **[IP_address]**.

Quando %ASA-4-733104 e/ou %ASA-4-733105 forem registrados

%ASA-4-733104 e %ASA-4-733105 alistam o host visado pelo ataque que está sendo protegido atualmente pelo TCP Intercept. Para mais detalhes nas taxas de ataque e nos server protegidos, verifique a saída das **estatísticas TCP Intercept superior da ameaça-detecção da mostra**.

```
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 da ameaça detecta um ataque desta natureza, o ASA já está protegendo o server visado através do TCP Intercept. Verifique que os limites configurados da conexão para os assegurar fornecem a proteção adequada para a natureza e a taxa do ataque. Também, seria benéfico obstruir manualmente tão distante rio acima o tráfego do atacante para a fonte como possível. Isto pode ser feito através dos ACL e do QoS. Isto assegura-se de que os dispositivos intermediários não precisem de desperdiçar os recursos que processam o tráfego ilegítimo.

Se o ataque detectado é um falso positivo, ajuste as taxas para um ataque TCP Intercept a um

valor mais apropriado com o comando das **estatísticas TCP Intercept da ameaça-detecção**.

Como provocar manualmente uma ameaça

Para o teste e os propósitos de Troubleshooting, pode ser útil provocar manualmente várias ameaças. Esta seção contém pontas para provocar alguns tipos comuns da ameaça.

Ameaça básica - Gota, Firewall, e exploração ACL

A fim provocar uma ameaça básica particular, refira a tabela na seção precedente da funcionalidade. Escolha uma razão específica da gota ASP e envie o tráfego com o ASA que seria deixado cair pela razão apropriada da gota ASP.

Por exemplo, as ameaças todas da gota ACL, do Firewall, e da exploração consideram a taxa de pacotes que estão sendo deixados cair pela ACL-gota. Termine estas etapas a fim provocar simultaneamente estas ameaças:

1. Crie um ACL na interface externa do ASA que deixa cair explicitamente todos os pacotes de TCP enviados a um servidor de destino no interior 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. De um atacante na parte externa do ASA (10.10.10.10), use o nmap a fim executar uma varredura TCP SYN contra cada porta no servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Nota: O T5 configura o nmap para executar o mais rápido possível a varredura. Segundo os recursos do atacante PC, esta ainda não pode ser rapidamente bastante provocar algumas das taxas padrão. Se este é o caso, abaixe simplesmente as taxas configuradas para a ameaça que você quer ver. Ajustando o ARI e o BRI a 0 detecções básicas da ameaça das causas para provocar sempre a ameaça apesar da taxa.
3. Note que as ameaças básicas estão detectadas para ameaças da gota, do Firewall, e da exploração ACL:`%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`Nota: Neste exemplo, a gota ACL e o Firewall ARI e BRI foram ajustados a 0 assim que provoca sempre uma ameaça. Eis porque as taxas configuradas máximas são alistadas como 0.

Ameaça avançada - TCP Intercept

1. Crie um ACL na interface externa que permite todos os pacotes de TCP enviados a um servidor de destino no interior 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 existe realmente, ou restaura as tentativas de conexão do

atacante, configurar uma entrada de ARP falsificada no ASA ao blackhole o tráfego do ataque para fora a interface interna:`arp inside 10.11.11.11 dead.dead.dead`

3. Crie uma política simples TCP Intercept 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`De um atacante na parte externa do ASA (10.10.10.10), use o nmap para executar uma varredura TCP SYN contra cada porta no servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Note que a detecção da ameaça se mantém a par do server protegido:`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)
```

Ameaça de varredura

1. Crie um ACL na interface externa que permite todos os pacotes de TCP enviados a um servidor de destino no interior 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`Nota: Para que a detecção da ameaça da exploração siga o alvo e o atacante IPs, o tráfego deve ser permitido com o ASA.
2. Se o servidor de destino não existe realmente, ou restaura as tentativas de conexão do atacante, configurar uma entrada de ARP falsificada no ASA ao blackhole o tráfego do ataque para fora a interface interna:`arp inside 10.11.11.11 dead.dead.dead`Nota: As conexões que são restauradas pelo servidor de destino não são contadas como parte da ameaça.
3. De um atacante na parte externa do ASA (10.10.10.10), use o nmap para executar uma varredura TCP SYN contra cada porta no servidor de destino:`nmap -sS -T5 -p1-65535 -Pn 10.11.11.11`Nota: O T5 configura o nmap para executar o mais rápido possível a varredura. Segundo os recursos do atacante PC, esta ainda não pode ser rapidamente bastante provocar algumas das taxas padrão. Se este é o caso, abaixe simplesmente as taxas configuradas para a ameaça que você quer ver. Ajustando o ARI e o BRI a 0 detecções básicas da ameaça das causas para provocar sempre a ameaça apesar da taxa.
4. Note que uma ameaça da exploração está detectado, o IP do atacante é seguido, e o atacante 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

- Manual de configuração ASA

- Referência de comandos ASA
- Guia do Syslog ASA
- Suporte Técnico e Documentação - Cisco Systems