Capturas de pacote de informação ASA com CLI e exemplo da configuração ASDM

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Produtos Relacionados
Informações de Apoio
Configurar
Diagrama de Rede
Configurações
Configurar a captura de pacote de informação com o ASDM
Configurar a captura de pacote de informação com o CLI
Tipos disponíveis da captação no ASA
Defaults
Veja os pacotes capturados
No ASA
Transferência do ASA para a análise off-line
Cancele uma captação
Pare uma captação
Verificar
Troubleshooting

Introdução

Este documento descreve como configurar o Firewall adaptável da próxima geração da ferramenta de segurança de Cisco (ASA) a fim capturar os pacotes desejados com o Cisco Adaptive Security Device Manager (ASDM) ou o CLI.

Pré-requisitos

Requisitos

Este documento supõe que o ASA é plenamente operacional e está configurado a fim permitir que Cisco ASDM ou o CLI faça alterações de configuração.

Componentes Utilizados

Este documento não é restringido ao hardware ou às versões de software 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com este Produtos da Cisco:

- Versões ASA de Cisco 9.1(5) e mais atrasado
- Versão ASDM Cisco 7.2.1

Informações de Apoio

O processo da captura de pacote de informação é útil quando você pesquisa defeitos problemas de conectividade ou monitora a atividade suspeita. Além, você pode criar capturas múltiplas a fim analisar tipos de tráfego diferentes em interfaces múltiplas.

Configurar

Esta seção fornece a informação que você pode usar a fim configurar as características da captura de pacote de informação que são descritas neste documento.

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

> Nota: Os esquemas de endereçamento de IP que são usados nesta configuração não são legalmente roteável no Internet. São os endereços do RFC 1918 que são usados em um ambiente de laboratório.

Configurar a captura de pacote de informação com o ASDM

Nota: Este exemplo de configuração é usado a fim capturar os pacotes que são transmitidos durante um sibilo do **usuário1** (rede interna) ao **roteador1** (rede externa).

Termine estas etapas a fim configurar a característica da captura de pacote de informação no ASA com o ASDM:

1. Navegue aos **assistentes > ao assistente da captura de pacote de informação** a fim começar a configuração da captura de pacote de informação, como mostrado:

2. O assistente da captação abre. Clique em Next.

3. Na nova janela, forneça os parâmetros que são usados a fim capturar o **tráfego de ingresso**. Selecione o **interior** para a **interface de ingresso** e forneça a fonte e os endereços IP de destino dos pacotes a ser capturados, junto com sua máscara de sub-rede, no espaço respectivo fornecido. Também, escolha o tipo de pacote a ser capturado pelo ASA (o IP é o tipo de pacote escolhido aqui), como mostrado:

   Clique em Next.

4. Selecione a **parte externa** para a **interface de saída** e forneça a fonte e os endereços IP de destino, junto com sua máscara de sub-rede, nos espaços respectivos fornecidos. Se o Network Address Translation (NAT) é executado no Firewall, tome isto na consideração também.

   Clique em Next.

5. Incorpore o **tamanho do pacote** apropriado e o **tamanho de buffer ao** espaço respectivo fornecido, como estes dados são exigidos para que a captação ocorra. Também, recorde verificar a caixa de verificação **circular do buffer do uso** se você quer usar a opção circular do buffer. Os bufferes circulares nunca enchem-se acima. Porque o buffer alcança seu tamanho máximo, uns dados mais velhos são rejeitados e a captação continua. Neste exemplo, o buffer circular não é usado, assim que a caixa de verificação não é verificada.

   Clique em Next.

6. Este indicador mostra as **listas de acesso** que devem ser configuradas no ASA de modo que os pacotes desejados sejam capturados, e mostra o tipo de pacotes a ser capturados (os pacotes IP são capturados neste exemplo). Clique em Next.

7. Clique o **começo** a fim começar a captura de pacote de informação, como mostrado aqui:

8. Como a captura de pacote de informação é começada, tente sibilar a rede externa da rede interna de modo que os pacotes que fluem entre a fonte e os endereços IP de destino sejam capturados pelo buffer da captação ASA.

9. O clique **consegue o buffer da captação** a fim ver os pacotes que são capturados pelo buffer da captação ASA.

10. Os pacotes capturados são mostrados neste indicador para o **ingresso** e o **tráfego de saída**. **A salvaguarda do** clique **captura** a fim salvar a informação da captação.

11. Do indicador das **captações da salvaguarda**, escolha o formato exigido em que o buffer da captação deve ser salvar. Este é **ASCII** ou **PCAP**. Clique o botão de rádio ao lado dos nomes do formato. Então, a **captação do ingresso da salvaguarda do** clique ou a **saída da salvaguarda capturam** como necessário. Os arquivos PCAP podem ser abertos com analisadores da captação, tais como Wireshark, e é o método preferido.

12. Do indicador do **arquivo de captura da salvaguarda**, forneça o nome de arquivo e o lugar a onde o arquivo de captura deve ser salvar. Clique em Salvar.

13. Clique em Finish.

    Isto termina o procedimento da captura de pacote de informação.

Configurar a captura de pacote de informação com o CLI

Termine estas etapas a fim configurar a característica da captura de pacote de informação no ASA com o CLI:

1. Configurar as interfaces internas e externas como ilustrado no diagrama da rede, com o endereço IP de Um ou Mais Servidores Cisco ICM NT e os níveis de segurança corretos.

2. Comece o processo da captura de pacote de informação com o comando capture no modo de exec privilegiado. Neste exemplo de configuração, a captação nomeada **capin** é definida. Ligue-a à **interface interna**, e especifique-o com a palavra-chave do **fósforo** essa somente os pacotes que combinam o tráfego do interesse são capturados:

```
ASA# capture capin interface inside match ip 192.168.10.10 255.255.255.255
203.0.113.3 255.255.255.255
```

3. Similarmente, a captação nomeada **capout** é definida. Ligue-a à **interface externa**, e especifique-o com a palavra-chave do **fósforo** essa somente os pacotes que combinam o tráfego do interesse são capturados:

```
ASA# capture capout interface outside match ip 192.168.10.10 255.255.255.255
203.0.113.3 255.255.255.255
```

   O ASA começa agora a capturar o fluxo de tráfego entre as relações. A fim parar a qualquer hora a captação, não inscreva nenhum comando capture seguido pelo nome da captação.

   Aqui está um exemplo:

```
no capture capin interface inside
no capture capout interface outside
```

Tipos disponíveis da captação no ASA

Esta seção descreve os tipos diferentes de captações que estão disponíveis no ASA.

- **asa_dataplane** - Captura os pacotes no backplane ASA que passam entre o ASA e um módulo que use o backplane, tal como o ASA CX ou módulo ips.

```
ASA# cap asa_dataplace interface asa_dataplane
ASA# show capture
capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]
```

- *gota-código da ASP*-**gota** - Captura os pacotes que são deixados cair pelo trajeto acelerado da Segurança. *O gota-código* especifica o tipo de tráfego que é deixado cair pelo trajeto acelerado da Segurança.

```
ASA# capture asp-drop type asp-drop acl-drop
ASA# show cap
ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown

ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
```

```
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown
```

- *tipo do* **tipo de Ethernet** - Seleciona um tipo de Ethernet para capturar. Os tipos de Ethernet apoiados incluem 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, e VLAN.

  Esta mostra do exemplo como capturar o **tráfego ARP**:

```
ASA# cap arp ethernet-type ?

exec mode commands/options:
 802.1Q
 <0-65535>  Ethernet type
 arp
 ip
 ip6
 ipx
 pppoed
 pppoes
 rarp
 vlan

cap arp ethernet-type arp interface inside


ASA# show cap arp

22 packets captured

1: 05:32:52.119485 arp who-has 10.10.3.13 tell 10.10.3.12
 2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
3: 05:32:52.481878 arp who-has 192.168.10.50 tell 192.168.100.10
4: 05:32:53.409723 arp who-has 10.106.44.135 tell 10.106.44.244
5: 05:32:53.772085 arp who-has 10.106.44.108 tell 10.106.44.248
6: 05:32:54.782429 arp who-has 10.106.44.135 tell 10.106.44.244
7: 05:32:54.784695 arp who-has 10.106.44.1 tell 11.11.11.112:
```

- **exibições em tempo real os** pacotes capturados continuamente no tempo real. A fim terminar uma captura de pacote de informação do tempo real, pressione o **Ctrl-c**. A fim remover permanentemente a captação, não use **nenhum** formulário deste comando. Esta opção não é apoiada quando você usa o **comando capture do executivo do conjunto**.

```
ASA# cap capin interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture
```

- **Traço** - Segue os pacotes capturados de um modo similares à característica do projétil luminoso do pacote ASA.

```
ASA#cap in interface Webserver trace match tcp any any eq 80

// Initiate Traffic

1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S
2322784363:2322784363(0) win 8192
```

```
<mss 1460,nop,wscale 2,nop,nop,sackOK>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 0.0.0.0 0.0.0.0 outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group any in interface inside
access-list any extended permit ip any4 any4 log
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.0.0.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type:
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 9
Type: ESTABLISHED
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 41134, packet dispatched to next module

Phase: 14
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.1 using egress ifc outside
adjacency Active
next-hop mac address 0007.7d54.1300 hits 3170

Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

- **ikev1/ikev2** - Informação de protocolo 1 (IKEv1) ou IKEv2 somente do intercâmbio de chave de Internet das captações da versão.

- **isakmp** - Tráfego do Internet Security Association and Key Management Protocol (ISAKMP) das captações para conexões de VPN. O subsistema ISAKMP não tem o acesso aos protocolos de camada superior. A captação é uma captação pseudo-, com o exame, as camadas IP, e UDP combinados junto a fim satisfazer um parser PCAP. Os endereços de

peer são obtidos da troca SA e armazenados na camada IP.

- **lacp** - Tráfego do protocolo link aggregation control das captações (LACP). Se configurado, o nome da relação é o nome da interface física. Isto pôde ser útil quando você trabalha com EtherChannéis a fim identificar o comportamento atual do LACP.

- **TLS-proxy** - As captações decifraram dados de entrada e de partida do proxy do Transport Layer Security (TLS) em umas ou várias relações.

- **webvpn** - Dados das captações WebVPN para uma conexão VPN da Web específica. Cuidado: Quando você permite a captação WebVPN, afeta o desempenho da ferramenta de segurança. Assegure-se de que você desabilite a captação depois que você gerencie os arquivos de captura que estão precisados a fim pesquisar defeitos.

Defaults

Estes são os valores de padrão de sistema ASA:

- O tipo padrão é **dados brutos**.
- *O tamanho de buffer do* padrão é **512 KB**.
- *O tipo de Ethernet do* padrão é **pacotes IP**.
- *O comprimento do pacote do* padrão é **1,518 bytes**.

Veja os pacotes capturados

No ASA

A fim ver os pacotes capturados, inscreva o [comando capture da mostra] seguido pelo nome da captação. Esta seção fornece os **show command outputs (resultado do comando show) dos** índices do buffer da captação. O comando do **capin da captação da mostra** mostra os índices do buffer da captação nomeado **capin**:

```
ASA# show cap capin

8 packets captured

1: 03:24:35.526812 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527224 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528247 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528582 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529345 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529681 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:57.440162 192.168.10.10 > 203.0.113.3: icmp: echo request
8: 03:24:57.440757 203.0.113.3 > 192.168.10.10: icmp: echo reply
```

O comando do **capout da captação da mostra** mostra os índices do buffer da captação nomeado **capout**:

```
ASA# show cap capout

8 packets captured
```

```
1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request
8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

Transferência do ASA para a análise off-line

Há um par maneiras de transferir off line as capturas de pacote de informação para a análise:

1. Navegue a https:// <ip_of_asa>/admin/capture/<capture_name>/pcap em todo o navegador. Dica: Se você deixa para fora a palavra-chave do **pcap**, a seguir somente o equivalente da saída do comando do **<cap_name> da captação da mostra** está fornecido.
2. Incorpore o comando capture da cópia e seu protocolo de transferência de arquivo preferido a fim transferir a captação:

```
ASA# show cap capout

8 packets captured

1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request
8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

Dica: Quando você pesquisa defeitos uma edição com o uso das capturas de pacote de informação, Cisco recomenda que você transfere as captações para a análise off-line.

Cancele uma captação

A fim cancelar o buffer da captação, incorpore o comando **claro do <capture-name> da captação**:

```
ASA# show capture
capture capin type raw-data interface inside [Capturing - 8190 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 11440 bytes]
match icmp any any

ASA# clear cap capin
ASA# clear cap capout

ASA# show capture
capture capin type raw-data interface inside [Capturing - 0 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 0 bytes]
match icmp any any
```

Incorpore o comando **claro de /all da captação** a fim cancelar o buffer para todas as captações:

```
ASA# clear capture /all
```

Pare uma captação

A única maneira de parar uma captação no ASA é desabilitá-la completamente com este comando:

```
no capture <capture-name>
```

A identificação de bug Cisco CSCuv74549 esteve arquivada para adicionar a capacidade para parar uma captação sem completamente desabilitá-la e para controlá-la quando uma captação começa capturar o tráfego.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.