Troubleshooting de Conexões via PIX e ASA

Índice

Introdução

Este documento fornece ideias de troubleshooting e sugestões para quando o Cisco ASA 5500 Series Adaptive Security Appliance (ASA) e o Cisco PIX 500 Series Security Appliance forem usados. A maior parte da vezes, quando os aplicativos ou os origens de rede quebram ou não estão disponíveis, os Firewall (PIX ou ASA) tendem a ser um alvo preliminar e responsabilizado como a causa das indisponibilidade. Com alguns testes no ASA ou no PIX, um administrador pode determinar mesmo se o ASA/PIX causa o problema.

Refira o PIX/ASA: Estabeleça e pesquise defeitos a Conectividade através do dispositivo do Cisco Security a fim aprender mais sobre o Troubleshooting relativo relação nas ferramentas de segurança de Cisco.

Nota: Este documento focaliza no ASA e no PIX. Uma vez que pesquisar defeitos está completa no ASA ou no PIX, é provável que o Troubleshooting adicional pôde ser necessário com outros dispositivos (Roteadores, Switches, server, e assim por diante).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em Cisco ASA 5510 com OS 7.2.1 e 8.3.

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

Este documento pode igualmente ser usado com estes versão de hardware e software:

- ASA e PIX OS 7.0, 7.1, 8.3, e mais tarde
- Módulo de serviços de firewall (FWSM) 2.2, 2.3, e 3.1

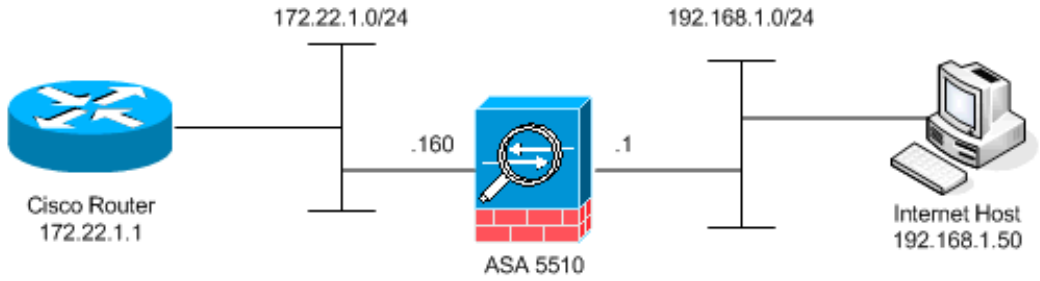
Nota: Os comandos e a sintaxe específicos podem variar entre versões de software.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O exemplo supõe que o ASA ou o PIX estão na produção. A configuração ASA/PIX pode ser relativamente simples (somente linhas dos 50 pés de configuração) ou o complexo (centenas aos milhares de linhas de configuração). Os usuários (clientes) ou os server podem estar em uma rede segura (para dentro) ou em uma rede inseguro (DMZ ou parte externa).



Os começos ASA com esta configuração. A configuração é pretendida dar ao laboratório um o ponto de referência.

Configuração inicial ASA

```
ciscoasa#show running-config : Saved : ASA Version
7.2(1) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 172.22.1.160
255.255.255.0 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet0/2 nameif dmz security-level 50 ip
address 10.1.1.1 255.255.255.0 ! interface Management0/0
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www access-list inside_acl extended
permit icmp 192.168.1.0 255.255.255.0 any access-list
inside_acl extended permit tcp 192.168.1.0 255.255.255.0
any eq www access-list inside_acl extended permit tcp
192.168.1.0 255.255.255.0 any eq telnet pager lines 24
mtu outside 1500 mtu inside 1500 mtu dmz 1500 no asdm
history enable arp timeout 14400 global (outside) 1
172.22.1.253 nat (inside) 1 192.168.1.0 255.255.255.0 !-
-- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
```

```
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Problema

Um usuário contacta o departamento TI e relata que o aplicativo X já não trabalha. O incidente escala ao administrador ASA/PIX. O administrador tem pouco conhecimento deste aplicativo particular. Com o uso do ASA/PIX, o administrador descobre que usos do aplicativo X das portas e protocolo assim como o que pôde ser a causa do problema.

Solução

O administrador ASA/PIX precisa de recolher tanta informação do usuário como possível. A informação útil inclui:

- Endereço IP de origem — Este é tipicamente a estação de trabalho ou o computador do usuário.
- Endereço IP de destino — O endereço IP do servidor que o usuário ou o aplicativo tentam conectar.
- Portas e protocolo os usos do aplicativo

Frequentemente o administrador é afortunado se capaz de obter uma resposta a uma destas perguntas. Para este exemplo, o administrador não pode recolher nenhuma informação. Uma revisão de mensagens do syslog ASA/PIX é ideal mas é difícil encontrar o problema se o administrador não conhece o que procurar.

Etapa 1 - Descubra o endereço IP de Um ou Mais Servidores Cisco ICM NT do usuário

Há muitas maneiras de descobrir o endereço IP de Um ou Mais Servidores Cisco ICM NT do usuário. Este documento é sobre o ASA e o PIX, assim que este exemplo usa o ASA e o PIX para descobrir o endereço IP de Um ou Mais Servidores Cisco ICM NT.

O usuário tenta comunicar-se ao ASA/PIX. Esta comunicação pode ser ICMP, telnet, SSH, ou HTTP. O protocolo escolhido deve ter limitado a atividade no ASA/PIX. Neste exemplo específico, o usuário sibila a interface interna do ASA.

O administrador precisa de estabelecer umas ou várias destas opções e então de mandar o usuário sibilar a interface interna do ASA.

- SyslogO registro Make sure é permitido. O nível do log deve ser definido como **debug**. Registrar pode ser enviado aos vários lugar. Este exemplo usa o buffer de registro ASA. Você pôde precisar um servidor de logging externo nos ambientes de produção.`ciscoasa(config)#`**`logging enable`** `ciscoasa(config)#`**`logging buffered debugging`** O usuário sibila a interface interna do ASA (sibilo 192.168.1.1). Esta saída é indicada.`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-6-302020: Built ICMP connection for faddr` **`192.168.1.50`**`/512 gaddr 192.168.1.1/0 laddr 192.168.1.1/0 %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512 gaddr 192.168.1.1/0 laddr 192.168.1.1/0` *`!--- The user IP address is 192.168.1.50.`*
- **Característica da captação ASA**O administrador precisa de criar uma lista de acesso que defina que tráfego o ASA precisa de capturar. Após a definição da lista de acesso, o

comando **capture** incorpora a lista de acesso e a aplica a uma interface.`ciscoasa(config)#`**`access-list inside_test permit icmp any host 192.168.1.1`**
`ciscoasa(config)#`**`capture inside_interface access-list inside_test interface inside`** O usuário sibila a interface interna do ASA (sibilo 192.168.1.1). Esta saída é indicada.`ciscoasa#`**`show capture inside_interface`** `1: 13:04:06.284897` **`192.168.1.50`** `> 192.168.1.1: icmp: echo request` *`!--- The user IP address is 192.168.1.50.`* **Nota:** A fim transferir o arquivo de captura a um sistema tal como etéreo, você pode fazê-lo enquanto esta saída mostra.
`!--- Open an Internet Explorer and browse with this https link format:`
`https://[<pix_ip>/<asa_ip>]/capture/<capture name>/pcap` Refira ASA/PIX: Pacote que captura usando o CLI e o exemplo da configuração ASDM a fim saber mais sobre o pacote que captura no ASA.
- Debug**O comando debug icmp trace** é usado capturar o tráfego ICMP do usuário.`ciscoasa#`**`debug icmp trace`** O usuário sibila a interface interna do ASA (sibilo 192.168.1.1). Esta saída é indicada no console.`ciscoasa#`
`!--- Output is suppressed.` `ICMP echo request from` **`192.168.1.50`** `to 192.168.1.1 ID=512 seq=5120 len=32 ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32` *`!--- The user IP address is 192.168.1.50.`* A fim desabilitar **debugar o traço ICMP**, usam um destes comandos:**nenhum debugar o traço ICMPtraço ICMP do undebugundebug todos**, **Undebug todos**, ou **un todos**

Cada um destas três opções ajuda o administrador a determinar o endereço IP de origem. Neste exemplo, o endereço IP de origem do usuário é 192.168.1.50. O administrador está pronto para aprender mais sobre o aplicativo X e para determinar a causa do problema.

Etapa 2 - Encontre a causa do problema

Com referência à informação alistada na seção de etapa 1 deste documento, o administrador conhece agora a fonte de uma sessão do aplicativo X. O administrador está pronto para aprender mais sobre o aplicativo X e para começar a encontrar onde as edições puderam estar.

O administrador ASA/PIX precisa de preparar no mínimo o ASA um destas sugestões listadas. Uma vez que o administrador está pronto, o usuário inicia o aplicativo X e limita toda atividade restante desde que a atividade adicional do usuário pôde causar a confusão ou enganar no administrador ASA/PIX.

- **Monitore mensagens do syslog.**Procure o endereço IP de origem do usuário que você identificou no Passo 1. O usuário inicia o aplicativo X. O administrador ASA emite o **comando show logging** e vê a saída.`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound` **`TCP`** `connection 90 for` **`outside:172.22.1.1/80`** `(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)` Os logs revelam que o endereço IP de destino é 172.22.1.1, o protocolo são TCP, a porta do destino é HTTP/80, e que o tráfego está enviado à interface externa.
- **Altere os filtros da captação.**O comando **o mais inside_test da lista de acesso** foi usado e é usado previamente aqui.`ciscoasa(config)#`**`access-list inside_test permit ip host 192.168.1.50 any`** *`!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the ASA.`* `ciscoasa(config)#`**`access-list inside_test permit ip any host 192.168.1.50 any`** *`!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.`*
`ciscoasa(config)#`**`no access-list inside_test permit icmp any host 192.168.1.1`**
`ciscoasa(config)#`**`clear capture inside_interface`** *`!--- Clears the previously logged data. !--- The`* ***`no capture inside_interface`*** *`removes/deletes the capture.`* O usuário inicia o aplicativo X. O administrador ASA então emite o comando do **inside_interface da captação da mostra** e vê a saída.`ciscoasa(config)#`**`show capture inside_interface`** `1: 15:59:42.749152 192.168.1.50.1107`

`> **172.22.1.1**.80: S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK> 2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.**80**: S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK> 3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80: **S** 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>` O tráfego capturado fornece o administrador diversas partes de informação valiosa:Endereço de destino — 172.22.1.1Número de porta — 80/httpProtocolo — TCP (observe o “S” ou a bandeira do syn)Além, o administrador igualmente sabe que o tráfego de dados para o aplicativo X chega no ASA.Se a saída tinha sido esta saída do comando do **inside_interface da captação da mostra**, a seguir o tráfego de aplicativo ou nunca alcançou o ASA ou o filtro da captação não foi ajustado para capturar o tráfego:`ciscoasa#**show capture inside_interface** 0 packet captured 0 packet shown` Nesse caso, o administrador deve considerar investigar o computador do usuário e qualquer roteador ou dispositivo de rede no caminho entre esse computador e o ASA.**Nota:** Quando o tráfego chega em uma relação, o **comando capture** grava os dados antes que todas as políticas de segurança ASA analisem o tráfego. Por exemplo, uma lista de acesso nega todo o tráfego de entrada em uma relação. O comando **capture** ainda registra o tráfego. A política de segurança ASA analisa então o tráfego.
- DebugO administrador não é familiar com o aplicativo X e consequentemente não conhece qual dos serviços debugar a permitir para a investigação do aplicativo X. Debug não pôde ser a melhor opção do Troubleshooting neste momento.

Com a informações recolhidas em etapa 2, o administrador ASA ganha diversos bit da informação valiosa. O administrador sabe que o tráfego chega na interface interna do ASA, do endereço IP de origem, do endereço IP de destino e dos usos do aplicativo de serviço X (TCP/80). Dos Syslog, o administrador igualmente sabe que a comunicação esteve permitida inicialmente.

Etapa 3 - Confirme e monitore o tráfego de aplicativo

O administrador ASA quer confirmar que o tráfego do aplicativo X saiu do ASA assim como monitorar todo o tráfego de retorno do server do aplicativo X.

- **Monitore mensagens do syslog.**Filtre mensagens do syslog para o endereço IP de origem (192.168.1.50) ou o endereço IP de destino (172.22.1.1). Da linha de comando, os mensagens do syslog de filtração olham como o **registro da mostra | inclua 192.168.1.50** ou **mostre o registro | inclua 172.22.1.1**. Neste exemplo, o **comando show logging** é usado sem filtros. A saída é suprimida a fim fazer a leitura fácil.`ciscoasa#**show logging** *!--- Output is suppressed.* %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025) **%ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80 to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout** %ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30 %ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 duration 0:01:00 %ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00` O mensagem do syslog indica a conexão fechada porque do Intervalo de SYN. Isto diz ao administrador que nenhuma resposta de servidor do aplicativo X esteve recebida pelo ASA. As razões da terminação do mensagem do syslog podem variar.O Intervalo de SYN obtém registrado devido a um fim de conexão forçado após 30 segundos que ocorra após a conclusão do cumprimento de três vias. Esta edição ocorre geralmente se o server não responde a um pedido de conexão, e, na maioria dos casos, não é relacionada à configuração no PIX/ASA.A fim resolver esta edição, refira esta lista de verificação:Certifique-se que o comando static está inscrito corretamente e isso que não sobrepõe com outros comandos static, por exemplo,`static (inside,outside)`

```
x.x.x.x  y.y.y.y netmask 255.255.255.255
```

O NAT estático em ASA 8.3 e mais atrasado pode ser configurado como mostrado aqui:

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

Certifique-se de que uma lista de acessos existe a fim permitir o acesso ao endereço IP global do exterior e de que está limitada à relação:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

Para uma conexão bem sucedida com o server, o gateway padrão no server deve apontar para a relação DMZ do PIX/ASA.Consulte Mensagens de Sistema do ASA para obter mais informações sobre as mensagens do Syslog.

- **Crie um filtro novo da captação.**De um tráfego e de uns mensagens do syslog capturados mais adiantados, o administrador sabe que o aplicativo X deve deixar o ASA através da interface externa.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80 !--- When you leave the source as 'any', it allows !--- the administrator to monitor any network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any !--- When you reverse the source and destination information, !--- it allows return traffic to be captured. ciscoasa(config)#capture outside_interface access-list outside_test interface outside
```

O usuário precisa de iniciar uma sessão nova com aplicativo X. Depois que o usuário iniciou uma sessão do aplicativo novo X, o administrador ASA precisa de emitir o comando do **outside_interface da captação da mostra no** ASA.

```
ciscoasa(config)#show capture outside_interface 3 packets captured 1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80: S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK> 2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80: S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK> 3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80: S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK> 3 packets shown
```

O tráfego das mostras da captação que sae da interface externa mas não mostra nenhum tráfego da resposta do server de 172.22.1.1. Esta captação mostra os dados enquanto sae do ASA.

- **Uso da opção packet-tracer**.Das seções anterior, o administrador ASA aprendeu bastante informação usar a opção do pacote-**projétil luminoso no** ASA.**Nota:** O ASA apoia o comando do pacote-**projétil luminoso que** começa na versão 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http !--- This line indicates a source port of 1025. If the source !--- port is not known, any number can be used. !--- More common source ports typically range !--- between 1025 and 65535. 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: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0 255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group inside_acl in interface inside access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www Additional Information: Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 7 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: NAT Subtype: Result: ALLOW Config: nat (inside) 1 192.168.1.0 255.255.255.0 match ip inside 192.168.1.0 255.255.255.0 outside any dynamic translation to pool 1 (172.22.1.254) translate_hits = 6, untranslate_hits = 0 Additional Information: Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028 using netmask 255.255.255.255 Phase: 9 Type: NAT Subtype: host-limits Result: ALLOW Config: nat (inside) 1 192.168.1.0 255.255.255.0 match ip inside 192.168.1.0 255.255.255.0 outside any dynamic translation to pool 1 (172.22.1.254) translate_hits = 6, untranslate_hits = 0 Additional Information: Phase: 10 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 11 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 12 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 13 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: Phase: 14 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 94, packet dispatched to next module Phase: 15 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional
```

```
Information: found next-hop 172.22.1.1 using egress ifc outside adjacency Active next-hop
mac address 0030.a377.f854 hits 11 !--- The MAC address is at Layer 2 of the OSI model. !---
This tells the administrator the next host !--- that should receive the data packet. Result:
input-interface: inside input-status: up input-line-status: up output-interface: outside
output-status: up output-line-status: up Action: allow
```

A saída a mais importante do comando do pacote-**projétil luminoso** é a última linha, que é `ação: reserve`.

As três opções em etapa 3 mostram cada ao administrador que o ASA não é responsável para as edições do aplicativo X. O tráfego do aplicativo X sae do ASA e o ASA não recebe uma resposta do server do aplicativo X.

Que é seguinte?

Há muitos componentes que permitem o aplicativo X trabalhar corretamente para usuários. Os componentes incluem o computador do usuário, o cliente do aplicativo X, roteamento, políticas de acesso e o servidor do aplicativo X. No exemplo anterior, provamos que o ASA recebe e encaminha o tráfego do aplicativo X. O server e os administradores do aplicativo X devem agora obter involvidos. Os administradores devem verificar se os serviços do aplicativo estão em execução, examinar os logs no servidor e verificar se o tráfego do usuário é recebido pelo servidor e pelo aplicativo X.

Problema: Terminando a mensagem de erro de conexão do TCP-proxy

Você recebe este Mensagem de Erro:

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

Solução

Explicação: Este exibições de mensagem quando o limite de buffer de remontagem for excedido durante a montagem de segmentos TCP.

- *source_address/source_port* - O endereço IP de origem e a porta de origem do pacote que inicia a conexão.
- *dest_address/dest_port* - O endereço IP de destino e a porta do destino do pacote que inicia a conexão.
- *interface_inside* - O nome da relação em que o pacote que iniciou a conexão chega.
- *interface_outside* - O nome da relação em que o pacote que iniciou a conexão retira.
- *limite* - O limite configurado da conexão embriônica para a classe de tráfego.

A definição para esta edição é desabilitar como mostrado a inspeção RTSP na ferramenta de segurança.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

Refira a identificação de bug Cisco CSCsl15229 (clientes registrados somente) para mais detalhes.

Problema: "%ASA-6-110003: Distribuição não são encontrados o salto seguinte para o protocolo Mensagem de Erro da relação do src"

O ASA deixa cair o tráfego com o `error:%ASA-6-110003: Distribuir não é encontrada o salto seguinte para o protocolo do src conecta: porta do src IP/src à relação dest:` mensagem de `erro de porta dest IP/dest.`

Solução

Este erro ocorrer quando as tentativas ASA para encontrar o salto seguinte em uma tabela de roteamento da relação. Tipicamente, esta mensagem está recebida quando o ASA tem uma tradução (xlate) construída a uma relação e a uma rota que indica uma relação diferente. Verifique para ver se há um misconfiguration nas declarações NAT. A definição do misconfiguration pode resolver o erro.

Problema: Conexão obstruída pelo ASA com o "%ASA-5-305013: Regras assimétricas NAT combinadas para Mensagem de Erro dianteiro e dos fluxos reversos o"

A conexão é obstruída pelo ASA, e este Mensagem de Erro é recebido:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

Solução

Quando o NAT é executado, o ASA igualmente tenta inverter o pacote e verifica se este bate qualquer tradução. Se não bate alguns ou uma tradução NAT diferente, a seguir há uma má combinação. Você vê o mais geralmente este Mensagem de Erro quando há umas regras diferentes NAT configuradas para de partida e o tráfego de entrada com a mesma fonte e destino. Verifique a declaração NAT para ver se há o tráfego interessado.

Problema: Receba o erro - %ASA-5-321001: O limite conns do recurso dos "de 10000 alcançados para o sistema

Solução

Este erro significa que as conexões para um server situado através de um ASA alcançaram seu limite máximo. Esta podia ser uma indicação de um ataque DoS a um server em sua rede. Use o MPF no ASA e reduza o limite das conexões embriônica. Também, permita a detecção inoperante da conexão (DCD). Refira este snippet de configuração:

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

Problema: Receba o erro %PIX-1-106021: Negue a verificação do caminho reverso TCP/UDP do src_addr ao dest_addr no int_name da relação

Solução

Este mensagem de registro é recebido quando a verificação do caminho reverso é permitida. Emita este comando a fim resolver o problema e desabilitar a verificação do caminho reverso:

no ip verify reverse-path interface *<interface name>*

Problema: Interrupção da conectividade de Internet devido à detecção da ameaça

Este Mensagem de Erro é recebido no ASA:

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

Solução

Esta mensagem está gerada pela detecção da ameaça devido à configuração padrão quando um comportamento de tráfego anômalo é detectado. A mensagem focaliza em Miralix Licen 3000 que é uma porta TCP/UDP. Encontre o dispositivo que está usando a porta 3000. Verifique nas estatísticas gráficas ASDM para ver se há a detecção de ameaça e verifique os ataques superiores para ver se mostra a porta 3000 e o endereço IP de origem. Se é um dispositivo legítimo, você pode incrementar a taxa básica da detecção da ameaça no ASA a fim resolver este Mensagem de Erro.

Informações Relacionadas

- Referência de comandos de Cisco ASA
- Referência de comando PIX de Cisco
- Erro e mensagens de sistema de Cisco ASA
- Erro e mensagens de sistema de Cisco PIX
- Apoio do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Apoio do Dispositivos de segurança Cisco PIX série 500
- Suporte Técnico e Documentação - Cisco Systems