A configuração de NAT e as recomendações ASA para Expressway-e Dual aplicação das interfaces de rede

Índice

Introdução

Este original descreve como executar a configuração do Network Address Translation (NAT) exigida na ferramenta de segurança adaptável de Cisco (ASA) para a aplicação dupla das

interfaces de rede de Expressway-e.

> Dica: Este desenvolvimento é a opção recomendada para a aplicação de Expressway-e, um pouco do que a aplicação Único-NIC com reflexão NAT.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração básica e configuração de NAT de Cisco ASA
- Configuração básica de Cisco Expressway-e e de Expressway-C

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivos do 5500 e 5500-X Series de Cisco ASA que executam a versão de software 8.0 e mais atrasado.
- Versão X8.0 de Cisco Expressway e mais tarde.

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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

> **Note**: Através do original inteiro, os dispositivos da via expressa são referidos como Expressway-e e Expressway-C. Contudo, a mesma configuração aplica-se para o server de comunicação de vídeo (VCS) Expressway e dispositivos de controle do VCS.

Informações de Apoio

Pelo projeto, Cisco Expressway-e pode ser colocado em uma zona desmilitarizada (DMZ) ou com uma relação da face Internet, quando puder se comunicar com Cisco Expressway-C em uma rede privada. Quando Cisco Expressway-e é colocado em um DMZ, estes são os benefícios adicionais:

- Na maioria de cenário comum, Cisco Expressway-e é controlado pela rede privada. Quando Cisco Expressway-e está em um DMZ, um Firewall (externo) do perímetro pode ser usado para obstruir acesso indesejável a Expressway das redes externas através do protocolo de transferência de hipertexto pedidos seguros (HTTPS) ou do Shell Seguro (ssh).
- Se o DMZ não permite conexões direta entre interno e redes externas, os servidores dedicados estão exigidos para segurar o tráfego que atravessa o DMZ. Cisco Expressway pode atuar como um servidor proxy para o Session Initiation Protocol (SIP) e/ou a Voz e o tráfego de vídeo de H.323. Neste caso, você pode usar a opção de interfaces de rede dupla

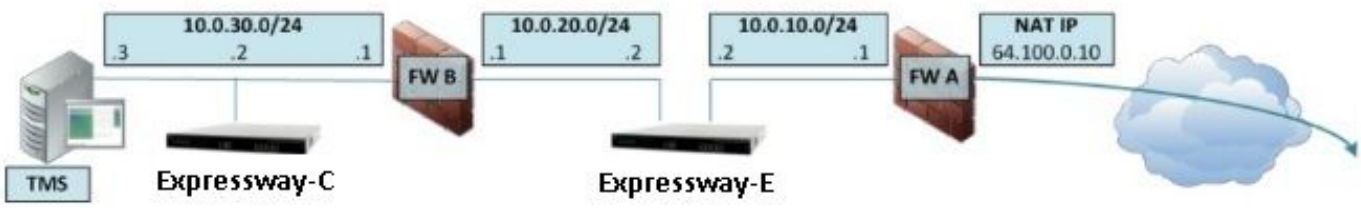
que permite que Cisco Expressway tenha dois endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes, um para o tráfego para/desde o firewall externo, e uma para o tráfego para/desde o Firewall interno.

- Esta instalação impede conexões direta da rede externa à rede interna. Isto melhora o macacão da Segurança da rede interna.

  Dica: A fim obter mais detalhes sobre a aplicação do TelePresence, refira Cisco Expressway-e e Expressway-C - guia de distribuição da configuração básica e colocação de um VCS Expressway de Cisco em um DMZ um pouco do que no Internet público.

C de Expressway e E - Interfaces de rede/aplicação duplas do NIC dual

Esta imagem mostra um exemplo de distribuição para Expressway-e com interfaces de rede e o NAT estático duplos. Expressway-C atua como o cliente do traversal. Há dois Firewall (FW A e FWB). Tipicamente, nesta configuração DMZ, o FW A não pode distribuir o tráfego a FW B, e os dispositivos tais como Expressway-e são exigidos para validar e enviar o tráfego da sub-rede FW a à sub-rede FW b (e vice-versa).



Este desenvolvimento consiste nestes componentes.

Sub-rede DMZ 1 – 10.0.10.0/24

- Interface interna FW A – 10.0.10.1
- Relação de Expressway-e LAN2 – 10.0.10.2

Sub-rede DMZ 2 – 10.0.20.0/24

- Interface externa FW B – 10.0.20.1
- Relação de Expressway-e LAN1 – 10.0.20.2

Sub-rede de LAN – 10.0.30.0/24

- Interface interna FW B – 10.0.30.1
- Relação de Expressway-C LAN1 – 10.0.30.2
- Relação de rede de servidor da suite de gerenciamento do Cisco TelePresence (TMS) – 10.0.30.3

Específicos desta aplicação:

- O FW A é o Firewall externo ou do perímetro; é configurado com IP NAT (IP do público) de 64.100.0.10 que é traduzido estaticamente a 10.0.10.2 (a relação de Expressway-e LAN2)
- O FW B é o Firewall interno
- Expressway-e LAN1 tem o modo do NAT estático desabilitado
- Expressway-e LAN2 tem o modo do NAT estático permitido com endereço 64.100.0.10 do

NAT estático
- Expressway-C tem uma zona do cliente do traversal que aponte a 10.0.20.2 (a relação de Expressway-e LAN1)
- Não há nenhum roteamento entre 10.0.20.0/24 e 10.0.10.0/24 sub-redes. Expressway-e constrói uma ponte sobre estas sub-redes e atua como um proxy para a sinalização SIP/H.323 e os media do Real-Time Transport Protocol (RTP)/Protocolo de Controle RTP (RTCP).
- Cisco TMS tem Expressway-e configurado com endereço IP 10.0.20.2

Exigências/limitações

sub-redes desobreposição

Se Expressway-e é configurado para usar ambas as interfaces de LAN, as relações LAN1 e LAN2 devem ser ficadas situadas em sub-redes NON-sobrepostas para assegurar-se de que o tráfego esteja mandado à relação correta.

Aglomeração

Ao aglomerar dispositivos de Expressway com a opção de rede avançada configurada, cada par do conjunto precisa de ser configurado com seu próprio endereço da relação LAN1. Além, aglomerar-se deve ser configurada em uma relação que não tenha o modo do NAT estático permitido. Consequentemente, recomenda-se que você usa o LAN2 como a interface externa, em que você pode aplicar e configurar o NAT estático onde aplicável.

Ajustes externos da interface de LAN

Os ajustes de configuração externos da interface de LAN no controle da página da configuração IP que a interface de rede usa a utilização Transversal retransmitem em torno de NAT (VOLTA). Em uma configuração dupla de Expressway-e da interface de rede, isto é ajustado normalmente à interface de LAN externo de Expressway-e.

rotas estáticas

Expressway-e deve ser configurado com um endereço de gateway padrão de 10.0.10.1 para esta encenação. Isto significa que todo o tráfego mandado através do LAN2, está enviado à revelia ao endereço IP 10.0.10.1.

Se o FW B traduz o tráfego enviado da sub-rede 10.0.30.0/24 à relação de Expressway-e LAN1 (por exemplo, tráfego do cliente do traversal de Expressway-C ou tráfego de gerenciamento do server TMS), este tráfego aparece enquanto vem da interface externa FWB (10.0.20.1) como alcança Expressway-e LAN1. Expressway-e pode então responder a este tráfego através de sua relação LAN1 desde que a fonte aparente desse tráfego é ficada situada na mesma sub-rede.

Se o NAT é permitido em FW B, o tráfego enviado de Expressway-C a Expressway-e LAN1 mostra enquanto vem de 10.0.30.2. Se Expressway não tem uma rota estática adicionada para a sub-rede 10.0.30.0/24, envia as respostas para este tráfego a seu gateway padrão (10.0.10.1) para fora do LAN2, porque não está ciente que a sub-rede 10.0.30.0/24 está ficada situada atrás do Firewall interno (FW B). Consequentemente, uma rota estática precisa de ser adicionada,

executa o comando CLI de **RouteAdd do xCommand** através de uma sessão SSH a Expressway.

Neste exemplo particular, Expressway-e deve saber que pode alcançar a sub-rede 10.0.30.0/24 atrás do FW B, que é alcançável através da relação LAN1. Para realizar isto, execute o comando:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Note**: A configuração da rota estática pode ser aplicada através de Expressway-e GUI assim como do **/Network do sistema da** seção **> das relações/rotas estáticas**.

Neste exemplo, o parâmetro da relação pode igualmente ser ajustado ao **automóvel** porque o endereço de gateway (10.0.20.1) é somente alcançável através do LAN1.

Se o NAT não é permitido em FW B e em necessidades de Expressway-e se comunicar com os dispositivos nas sub-redes (a não ser 10.0.30.0/24) que são ficadas situadas igualmente atrás de FW B, as rotas estáticas devem ser adicionadas para estes dispositivos/sub-redes.

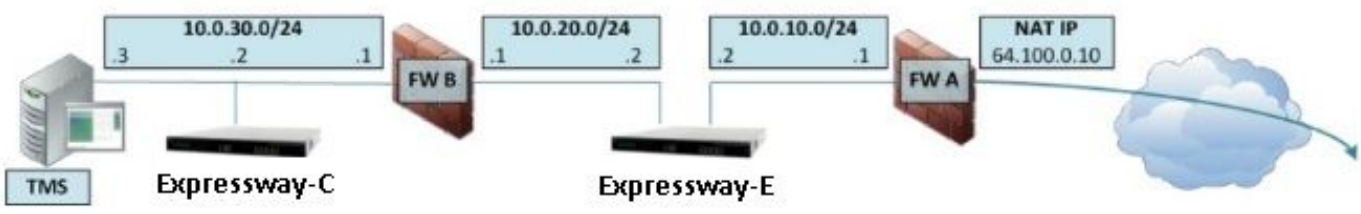
> **Note**: Isto inclui o SSH e as conexões de HTTPS das estações de trabalho de gerenciamento de rede ou para serviços de rede como o NTP, o DNS, o LDAP/AD, ou o Syslog.

O comando e a sintaxe de **RouteAdd do xCommand** são descritos no detalhe completo no guia do administrador do VCS.

Configuração

Esta seção descreve como configurar o NAT estático exigido para a aplicação dupla da interface de rede de Expressway-e no ASA. Algumas recomendações de configuração modulares adicionais da estrutura de política ASA (MPF) são incluídas para segurar o tráfego SIP/H323.

C de Expressway e E - Interfaces de rede/aplicação duplas do NIC dual



Neste exemplo, a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT é seguinte.

Endereço IP de Um ou Mais Servidores Cisco ICM NT de Expressway-C: 10.0.30.2/24

Gateway padrão de Expressway-C: 10.0.30.1 (FW-B)

Endereços IP de Um ou Mais Servidores Cisco ICM NT de Expressway-e:

No LAN2: 10.0.10.2/24

No LAN1: 10.0.20.2/24

Gateway padrão de Expressway-e: 10.0.10.1 (FW-A)

Endereço IP de Um ou Mais Servidores Cisco ICM NT TMS: 10.0.30.3/24

Configuração FW-A

Etapa 1. Configuração do NAT estático para Expressway-e.

Como explicado na seção de informações de fundo deste original, o FW-A tem uma tradução NAT estática para permitir que Expressway-e seja alcançável do Internet com endereço IP público 64.100.0.10. Este último é NATed ao endereço IP de Um ou Mais Servidores Cisco ICM NT 10.0.10.2/24 de Expressway-e LAN2. Aquela dita, isto é a configuração exigida do NAT estático FW-A.

Para as versões ASA 8.3 e mais atrasado:

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
(inside,outside) static interface
```

> Cuidado: Quando você se aplica o PAT estático comanda-o recebe este Mensagem de Erro na interface de linha de comando ASA, "**ERRO: NAT incapaz de reservar portas"**. Após isto, continua cancelar as entradas do xlate no ASA, para esta, executa o comando **x.x.x.x clearxlatelocal, o fromwhere** x.x.x.x corresponde ao endereço IP externo ASA. Este comando cancela todas as traduções associadas com este endereço IP de Um ou Mais Servidores Cisco ICM NT, executa-o com cuidado nos ambientes de produção.

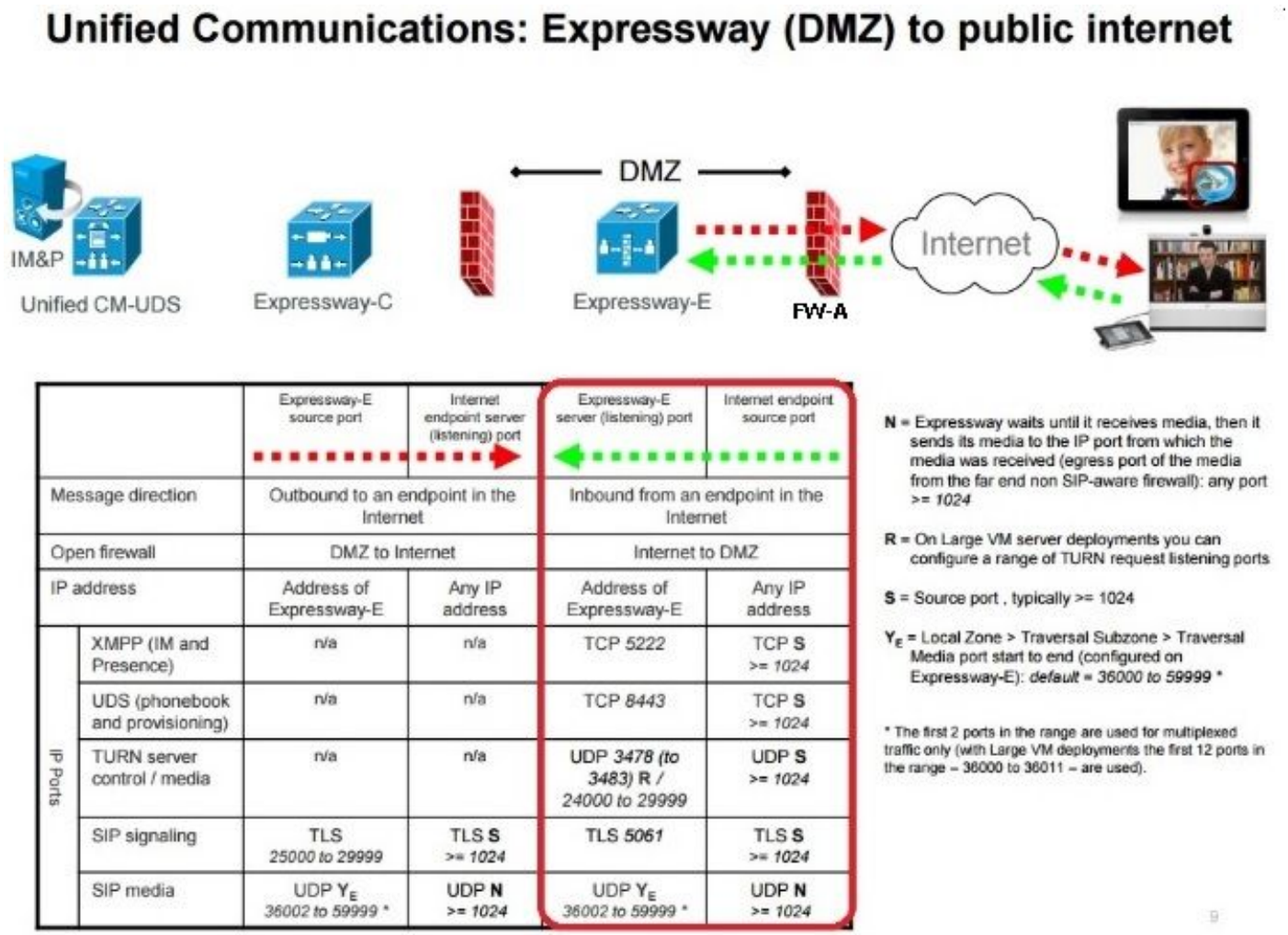
Para as versões ASA 8.2 e mais adiantado:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Etapa 2. A configuração do Access Control List (ACL) permite as portas exigidas do Internet a Expressway-e.

De acordo com a comunicação unificada: Expressway (DMZ) à documentação do Internet público, a lista de portas TCP e UDP que Expressway-e exige permitir em FW-A, é segundo as indicações da imagem:



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Esta é a configuração ACL exigida como de entrada na interface externa FW-A.

Para as versões ASA 8.3 e mais atrasado:

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

Para as versões ASA 8.2 e mais adiantado:

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
```

```
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

Configuração FW-B

Como explicado na seção de informações de fundo deste original, o FW B pode exigir uma configuração dinâmica NAT ou de PANCADINHA permitir que a sub-rede interna 10.0.30.0/24 esteja traduzida ao endereço IP 10.0.20.1 quando vai à interface externa do FW B.

Para as versões ASA 8.3 e mais atrasado:

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

Para as versões ASA 8.2 e mais adiantado:

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> Dica: Seja certo que todas as portas exigidas TCP e UDP permitem que Expressway-C trabalhe corretamente e estão abertas no FW B, apenas como especificado neste documento Cisco: Uso da porta IP de Cisco Expressway para o Firewall Traversal

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O projétil luminoso do pacote pode ser usado no ASA para confirmar que os trabalhos de tradução NAT estática de Expressway-e como necessário.

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
```

```
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 13, packet dispatched to next module

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

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
```

```
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 14, packet dispatched to next module

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

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 15, packet dispatched to next module

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

Projétil luminoso do pacote para testar 64.100.0.10 em UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 16, packet dispatched to next module

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

Projétil luminoso do pacote para testar 64.100.0.10 em UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
```

```
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 17, packet dispatched to next module

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

Troubleshooting

Etapa 1. Compare capturas de pacote de informação.

As capturas de pacote de informação podem ser tomadas no ingresso e nas interfaces de saída ASA.

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

Capturas de pacote de informação para 64.100.0.10 em TCP/5222:

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

Capturas de pacote de informação para 64.100.0.10 em TCP/5061:

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

Etapa 2. Inspecione capturas de pacote de informação aceleradas da gota do trajeto da Segurança (ASP).

As quedas de pacote de informação por um ASA são capturadas pela captação ASA ASP. **Toda a** opção, captura todas as razões possíveis pelas quais o ASA deixou cair um pacote. Isto pode ser reduzido para baixo se há alguma razão suspeitada. Para uma lista de razões que um ASA se usa para classificar estas gotas, execute a **gota asp do** comando show.

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

> Dica: A captação ASA ASP é usada nesta encenação para confirmar se as gotas ASA pacotess devido a um ACL ou a uma configuração de NAT faltada, que exijam para abrir uma porta específica TCP ou UDP para Expressway-e.

Dica: O tamanho de buffer do padrão para cada captação ASA é 512 KB. Se pacotes demais são deixados cair pelo ASA, o buffer está enchido rapidamente. O tamanho de buffer pode ser aumentado com a opção do **buffer**.

Recomendações

Assegure-se de que a inspeção SIP/H.323 esteja desabilitada completamente nos Firewall envolvidos.

Éaltamente recomendado desabilitar o SORVO e a inspeção de H.323 nos Firewall que seguram o tráfego de rede a ou de Expressway-e. Quando permitida, a inspeção SIP/H.323 é encontrada frequentemente para afetar negativamente a funcionalidade incorporado do traversal de Expressway firewall/NAT.

Este é um exemplo de como desabilitar o SORVO e as inspeçãos de H.323 no ASA:

```
policy-map global_policy
 class inspection_default
  no inspect h323 h225
  no inspect h323 ras
  no inspect sip
```

Aplicação alternativa de Expressway do VCS

Uma solução alternativa para executar Expressway-e com interfaces de rede duplas/NIC dual é executar Expressway-e mas com configuração de uma única reflexão NIC e NAT nos Firewall. O link seguinte mostra que uns detalhes mais adicionais sobre esta aplicação configuram a reflexão NAT no ASA para dispositivos do TelePresence de Expressway do VCS.

Dica: A aplicação recomendada para o VCS Expressway é as interfaces de rede/a aplicação duplas de Expressway VCS do NIC dual descrita neste original.

Informações Relacionadas

- Configurar a reflexão NAT no ASA para dispositivos do TelePresence de Expressway do VCS
- **Suporte Técnico e Documentação - Cisco Systems**
- Cisco Expressway-e e Expressway-C - Guia de distribuição da configuração básica
- Colocando um VCS Expressway de Cisco em um DMZ um pouco do que no Internet público
- Uso da porta IP de Cisco Expressway para o Firewall Traversal