A configuração de NAT e as recomendações ASA para a via expressa-e e a via expressa-C Dual aplicação das interfaces de rede.

Índice

Introdução

Este documento descreve como executar a configuração do Network Address Translation (NAT) exigida na ferramenta de segurança adaptável de Cisco (ASA) para a via expressa-e e interfaces de rede duplas da via expressa-C/aplicação dupla de Network Interface Controller (NIC).

Este desenvolvimento é uma opção recomendada para executar dispositivos da via expressa-e e da via expressa-C um pouco do que usando a reflexão NAT.

Contribuído pelo cristão Hernández e Cesar López Zamarripa, engenheiros de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ASA NAT básico e configuração
- Configuração básica da via expressa-e e da via expressa-C de Cisco

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 8.x e mais recente da via expressa de Cisco.

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.

> Nota: Através do documento inteiro, os dispositivos da via expressa são consultados como a via expressa-e e a via expressa-C. Contudo, a mesma configuração aplica-se à via expressa do server de comunicação de vídeo (VC) e aos dispositivos de controle VC.

Informações de Apoio

Pelo projeto, a via expressa-e de Cisco pode ser colocada ou em uma zona desmilitarizada (DMZ) ou enfrentando a rede pública (Internet) e pode com uma via expressa-C de Cisco em uma rede privada. Contudo, quando a via expressa-e de Cisco é posta em um DMZ, estes são os benefícios adicionais.

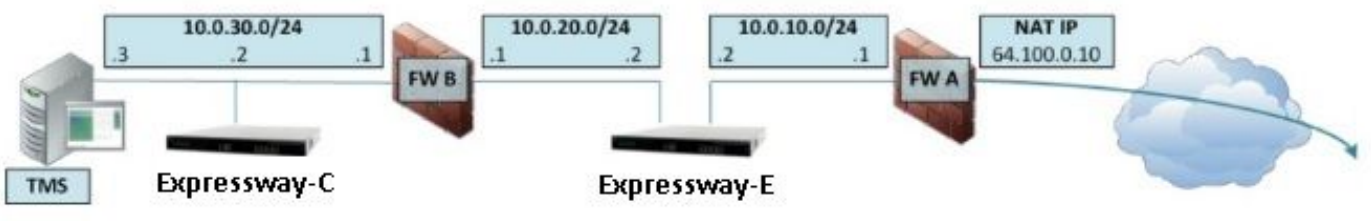
- Na maioria de cenário comum, a via expressa-e de Cisco é controlada da rede privada. Colocando a via expressa-e de Cisco em um DMZ, um Firewall (externo) permietral pode ser usado para obstruir acesso indesejável à via expressa tal como (protocolo de transferência de hipertexto seguro) pedidos HTTPS ou de 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. A via expressa de Cisco pode atuar como esse server 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 a via expressa de Cisco 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 uma comunicação externa para conectar diretamente à rede interna. Isto melhora o macacão da Segurança da rede interna.

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

C da via expressa e E - Aplicação dupla das interfaces de rede/NIC dual

Este diagrama mostra um exemplo de distribuição para uma via expressa-e com interfaces de rede e o NAT estático duplos. Uma via expressa-C que atua como um cliente do traversal e 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 a via expressa-e da interface dupla 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 da via expressa-e LAN2 – 10.0.10.2

Sub-rede DMZ 2 – 10.0.20.0/24

- Interface externa FW B – 10.0.20.1
- Relação da via expressa-e LAN1 – 10.0.20.2

Sub-rede de LAN – 10.0.30.0/24

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

- O FW A é o Firewall externo ou permitetral; é configurado com IP NAT (IP do público) de 64.100.0.10 que é traduzido estaticamente a 10.0.10.2 (a relação da via expressa-e LAN2)

- O FW B é o Firewall interno

- A via expressa-e LAN1 tem o modo do NAT estático desabilitado

- A via expressa-e LAN2 tem o modo do NAT estático permitido com endereço 64.100.0.10 do NAT estático

- A via expressa-C tem uma zona do cliente do traversal que aponte a 10.0.20.2 (a relação da

via expressa-e LAN1)

- Não há nenhum roteamento entre 10.0.20.0/24 e 10.0.10.0/24 sub-redes. A via expressa-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 a via expressa-e configurada com endereço IP 10.0.20.2

Exigências/limitações

sub-redes desobreposição

Se a via expressa-e é configurada para usar ambas as interfaces de LAN, as relações LAN1 e LAN2 devem ser ficadas situadas em sub-redes desobreposição para assegurar-se de que o tráfego esteja mandado à relação correta.

Aglomeração

Quando os dispositivos de aglomeração da via expressa têm a **opção de rede avançada** configurada, cada par do conjunto precisa 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, e o LAN2 é usado como a relação do 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 da via expressa-e da interface de rede, isto pode normalmente ser ajustado à interface de LAN externo da via expressa-e.

Rotas estáticas

A via expressa-e deve ser configurada 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 está traduzindo o tráfego enviado da sub-rede 10.0.30.0/24 à relação da via expressa-e LAN1 (por exemplo, tráfego do cliente do traversal da via expressa-C ou tráfego de gerenciamento do server TMS), este tráfego aparece enquanto vem da interface externa FWB (10.0.20.1) como alcança a via expressa-e LAN1. A via expressa-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 FW B não está fazendo o NAT, o tráfego enviado da via expressa-C à via expressa-e LAN1 mostra enquanto vem de 10.0.30.2. Se a via expressa 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, usando o comando CLI de **RouteAdd do xCommand** através de uma sessão SSH à via expressa.

Neste exemplo particular, a via expressa-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. Isto é realizado usando este comando.

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

> Nota: A configuração da rota estática pode ser aplicada através da interface gráfica de usuário (GUI) da via expressa-e no **/Network > nas relações/rotas estáticas do sistema da** seção.

> Nota: Recomenda-se evitar o uso do NAT em FW-B para a via expressa-C. Isto permite que a via expressa-e alcance a via expressa-C com seu endereço IP real 10.0.30.2. Isto evita determinadas edições dos serviços de telefone. Confirmou-se que a configuração de NAT para a via expressa-C pode fazer com que os dispositivos do móbil e do Acesso remoto (MRA) não venham acima.

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.

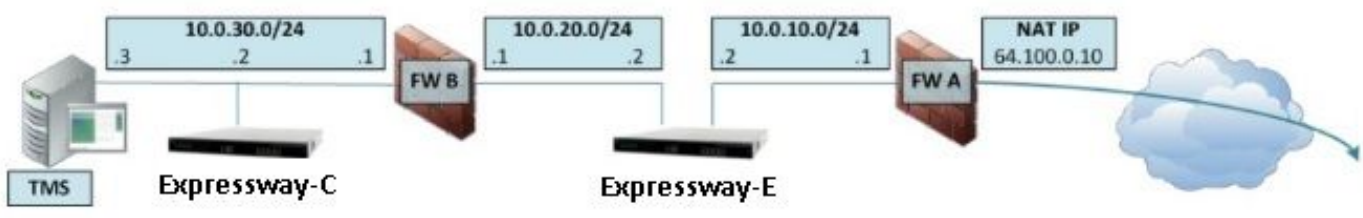
Se o FW B não está fazendo o NAT e a via expressa-e precisa de se comunicar com os dispositivos nas sub-redes diferentes de 10.0.30.0/24 que são ficadas situadas igualmente atrás de FW B tal como o SSH e as conexões de HTTPS do este estações de trabalho de rede ou para serviços de rede como o NTP, o DNS, o LDAP/AD e/ou o Sylog, as rotas estáticas devem ser adicionadas para estes dispositivos/sub-redes.

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

Configuração

Esta seção descreve como configurar o NAT estático exigido para interfaces de rede duplas da via expressa-C e da via expressa-e/aplicação do NIC dual no ASA. Além disso, algumas recomendações de configuração modulares da estrutura de política ASA (MPF) para segurar o tráfego SIP/H323 com o ASA.

C da via expressa e E - Aplicação dupla das interfaces de rede/NIC dual



Neste exemplo o assigment do endereço IP de Um ou Mais Servidores Cisco ICM NT é seguintes.

IP address:10.0.30.2/24 da via expressa-C

Gateway padrão da via expressa-C: 10.0.30.1 (FW-B)

Endereços IP de Um ou Mais Servidores Cisco ICM NT da via expressa-e

No LAN2: 10.0.10.2/24

No LAN1: 10.0.20.2/24

Gateway padrão da via expressa-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 a via expressa-e

Como explicado na seção de **informações de fundo d**este documento, o FW-A tem uma tradução NAT estática para permitir que a via expressa-e seja alcançável do Internet usando o 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 da via expressa-e LAN2, esse que está sendo dito, 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
```

> Nota: Se ao tentar aplicar o PAT estático comanda-o recebem **ERRO do** Mensagem de Erro **": O NAT incapaz de reservar portas" na** interface da linha de comando ASA, então, cancela as entradas do xlate com o comando clear xlate **x.x.x.x local onde** x.x.x.x corresponde ao endereço IP externo ASA. **Este comando cancela todas as traduções associadas a este IP assim que nos ambientes de produção, executa-o com cuidado.**

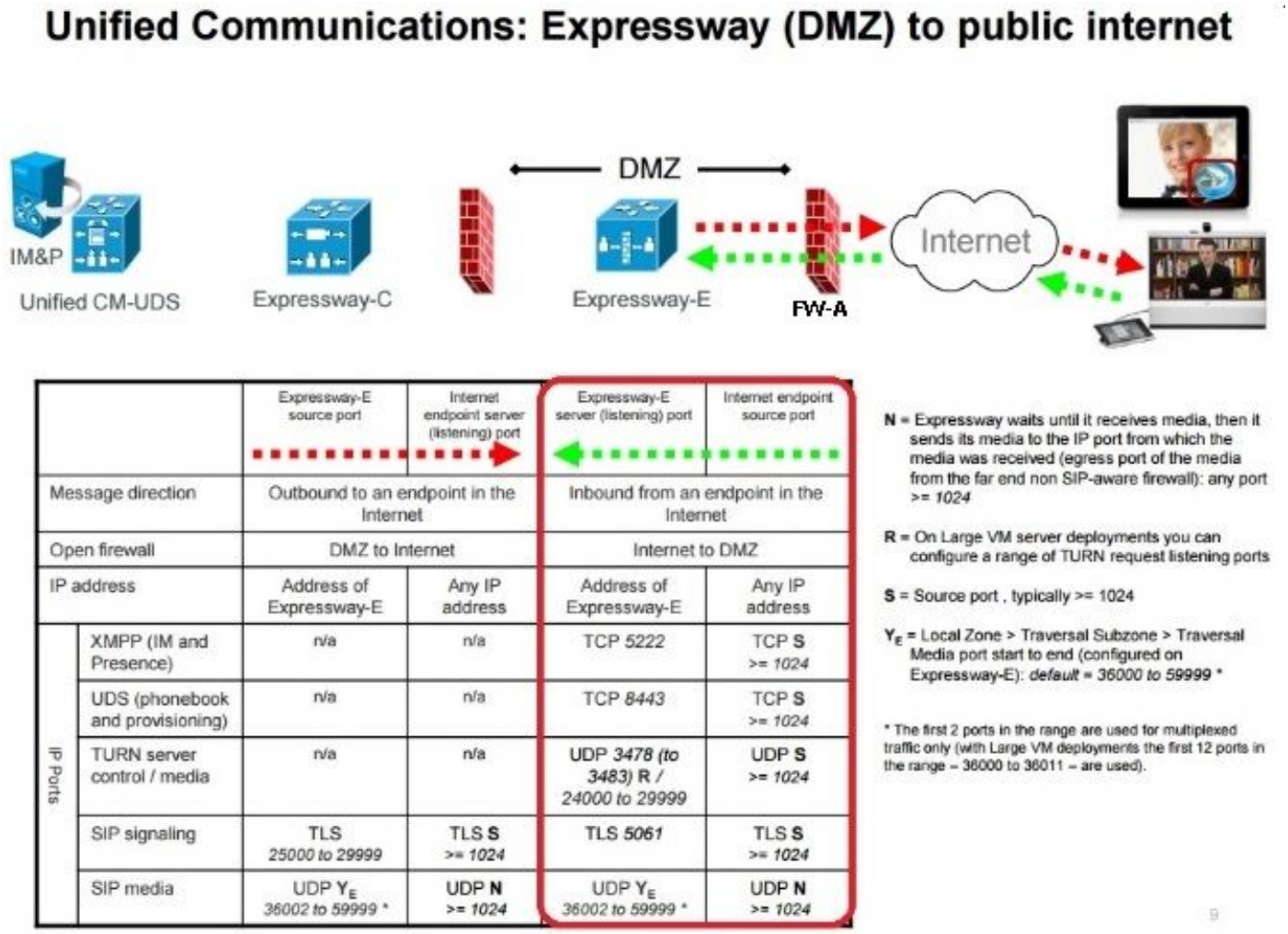
Para as versões ASA 8.2 e mais adiantado:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample 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. Configuração do Access Control List (ACL) para permitir as portas exigidas do Internet à via expressa-e

De acordo com a *comunicação unificada: A via expressa (DMZ) à* documentação do *Internet público*, isto é lista de portas TCP & UDP que a via expressa-e exige para ser permitida em FW-A:



		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.

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

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

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 esample shows only when Static one-to-one NAT is used.

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

Nota: É altamente recomendado desabilitar o SORVO e as inspeçãos de H.323 no tráfego

de rede levando do Firewall a ou de uma via expressa-e, como quando permitidas, isto são encontradas frequentemente para afetar negativamente a funcionalidade incorporado do traversal da via expressa-e firewall/NAT.

Configuração FW-B.

Como explicado na seção de **informações de fundo d**este documento, o FW B apenas exige uma configuração dinâmica NAT ou de PANCADINHA permitir que a sub-rede interna 10.0.30.0/24 seja traduzida ao endereço IP 10.0.20.1 ao sair à interface externa do FW B.

Para as versões ASA 8.3 e mais atrasado.

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

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

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 esample shows only when Static one-to-one NAT is used.

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

Nota: É altamente recomendado desabilitar o SORVO e as inspeçãos de H.323 no tráfego de rede levando do Firewall a ou de uma via expressa-e, as, quando permitida isto é encontrada frequentemente para afetar negativamente a funcionalidade incorporado do traversal da via expressa-e firewall/NAT.

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

Verificar

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

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/5222.

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

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

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/8443.

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

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

Projétil luminoso do pacote para testar 64.100.0.10 em TCP/5061.

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

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

Projétil luminoso do pacote para testar 64.100.0.10 em UDP/24000:

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

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

Projétil luminoso do pacote para testar 64.100.0.10 em UDP/36002.

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

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

Troubleshooting

Etapa 1. Capturas de pacote de informação.

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

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

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

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

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

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

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

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample 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. Capturas de pacote de informação aceleradas da gota do trajeto da Segurança (ASP).

As captações da gota ASA ASP tomam os pacotes que o ASA decidiu deixar cair. A opção **toda** captura todas as razões possíveis pelas quais o ASA deixou cair um pacote. Isto pode ser reduzido para baixo se há alguma razão supected. Para uma lista das razões um uso ASA classificar isto deixa cair, a **gota asp do** comando show pode ser usado.

O buffer do padrão para cada captação ASA é 512 KB. Se há muitos pacotes que estão sendo deixados cair por este ASA, este buffer estará enchido muito rapidamente. Este buffer pode ser incrementado usando o **buffer da** opção.

```
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: Esta captação ASA ASP é muito útil nesta encenação confirmar se as gotas ASA pacotess devido a um ACL ou a um NAT faltante para abrir uma porta específica TCP ou UDP para a via expressa-e.

Recomendações

Assegure-se de que as inspeçãos SIP/H.323 estejam desabilitadas completamente nos Firewall envolvidos

Éaltamente recomendado desabilitar o SORVO e as inspeçãos de H.323 nos Firewall que seguram o tráfego de rede a ou de uma via expressa-e, as, quando permitidos isto são encontrados frequentemente para afetar negativamente a funcionalidade incorporado do traversal da via expressa firewall/NAT.

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

```
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
```

Solução alternativa

Uma solução alternativa em vez de executar a via expressa-e usando interfaces de rede duplas/NIC dual, é executar a via expressa-e usando uma configuração da reflexão NAT nos Firewall, detalhes das mostras deste link mais sobre esta encenação.

ASA: Configuração da reflexão NAT para as aplicações da via expressa VC.

Contudo, como se mencionou no início deste documento, a instalação de rede dupla é recomendada sobre a reflexão NAT.

Links relacionados

Via expressa-e de Cisco e via expressa-C - Guia de distribuição da configuração básica

Colocando uma via expressa de Cisco VC em um DMZ um pouco do que no Internet público

Uso da porta IP da via expressa de Cisco para o Firewall Traversal