

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

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[C de Expressway e E - Aplicação dupla das interfaces de rede/NIC dual](#)

[Exigências/limitações](#)

[sub-redes desobrepõem](#)

[Aglomeração](#)

[Ajustes externos da interface de LAN](#)

[Rotas estáticas](#)

[Configuração](#)

[C de Expressway e E - Aplicação dupla das interfaces de rede/NIC dual](#)

[Configuração FW-A:](#)

[Etapa 1. Configuração do NAT estático para Expressway-e](#)

[Etapa 2. Configuração do Access Control List \(ACL\) para permitir as portas exigidas do Internet a Expressway-e](#)

[Configuração FW-B](#)

[Verificar](#)

[Troubleshooting](#)

[Etapa 1. Compare capturas de pacote de informação.](#)

–

[Etapa 2. Inspeção capturas de pacote de informação aceleradas da gota do trajeto da Segurança \(ASP\).](#)

[Recomendações](#)

[Assegure-se de que a inspeção SIP/H.323 esteja desabilitada completamente nos Firewall envolvidos](#)

[Solução alternativa](#)

[Documentação relacionada](#)

Introdução

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

Este desenvolvimento é a opção recomendada para disposições de dispositivos de Expressway-e e de Expressway-C (um pouco do que o Único-NIC com reflexão NAT).

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

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 documento inteiro, os dispositivos de Expressway são consultados como Expressway-e e Expressway-C. Contudo, a mesma configuração aplica-se ao 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:

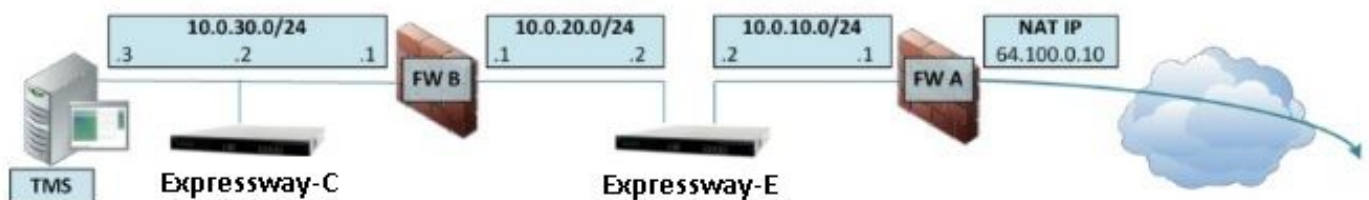
- Na maioria de cenário comum, Cisco Expressway-e é controlado da rede privada. Quando Cisco Expressway-e está em um DMZ, um Firewall (externo) do perímetro pode ser usado para obstruir acesso indesejável a Expressway das redes externas através do protocolo de transferência de hipertexto pedidos seguros (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.

Tip: 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 - Aplicação dupla das interfaces de rede/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 desobrepisição

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

Aglomeración

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 está traduzindo 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 do /Network do sistema da interface gráfica de usuário (GUI) assim como da seção de Expressway-e > 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.

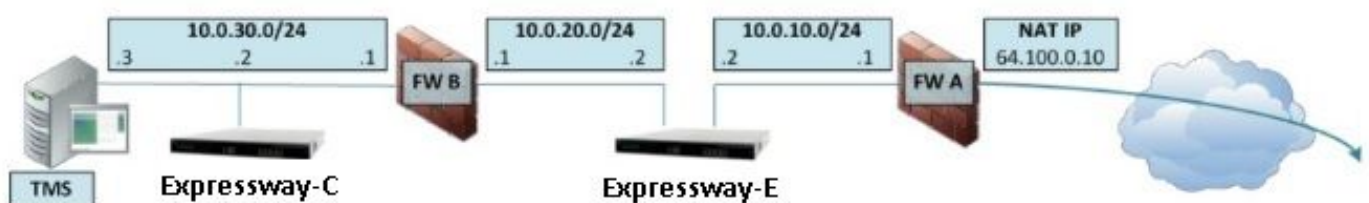
Note: Isto inclui o SSH e as conexões de HTTPS das estações de trabalho de gerenciamento de rede ou para serviços de rede como o NTP, o DNS, o LDAP/AD, ou o Syslog.

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 interfaces de rede duplas de Expressway-C e de Expressway-e/aplicação do NIC dual 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 - Aplicação dupla das interfaces de rede/NIC dual



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

IP address:10.0.30.2/24 de Expressway-C

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 documento, o FW-A tem uma tradução NAT estática para permitir que Expressway-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 de Expressway-e LAN2. Que sendo dito, esta 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
```

Note: Ao tentar aplicar o PAT estático comanda-o recebem este Mensagem de Erro na interface de linha de comando ASA, "ERRO: NAT incapaz de reservar portas". Então claro 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 com este IP, assim que nos ambientes de produção, executa-o com cuidado.

O ### precisa o esclarecimento

Para as versões ASA 8.2 e mais adiantado:

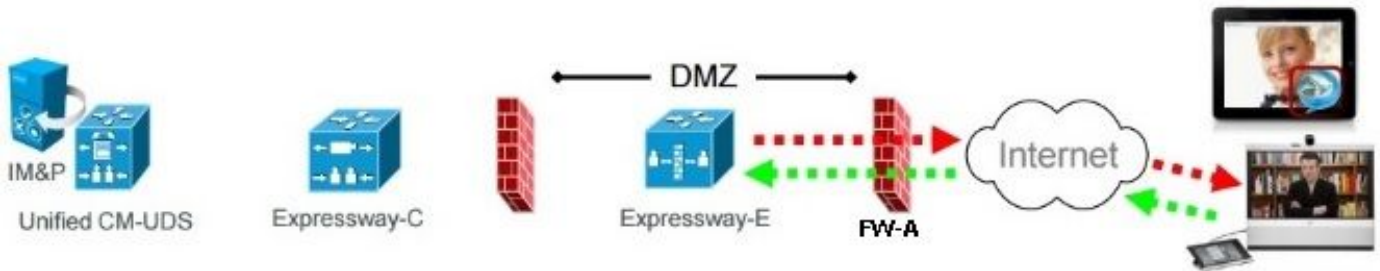
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port. This example shows only when Static one-to-one NAT is used.

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

Etapa 2. Configuração do Access Control List (ACL) para permitir as portas exigidas do Internet a Expressway-e

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

Unified Communications: Expressway (DMZ) to public internet



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

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

Note: É altamente recomendado desabilitar o SORVO e as inspeções de H.323 no tráfego de rede levando do Firewall a ou de Expressway-e, como quando permitidas, isto são encontradas frequentemente para afetar negativamente a funcionalidade incorporado do

traversal de Expressway-e firewall/NAT.

Configuração FW-B

Como explicado na seção de **informações de fundo** deste documento, o FW B pode exigir 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 example 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 example shows only when Static one-to-one NAT is used.
```

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

Note: É altamente recomendado desabilitar o SORVO e as inspeções de H.323 no tráfego de rede levando do Firewall a ou de Expressway-e, como quando permitida isto é encontrada frequentemente para afetar negativamente a funcionalidade incorporado do traversal de Expressway-e firewall/NAT.

Tip: Seja certo que todas as portas exigidas TCP & UDP para permitir que Expressway-C trabalhe corretamente estão abertas no FW B, apenas como especificado neste documento Cisco: [Uso da porta IP de Cisco Expressway para o Firewall Traversal](#)

Verificar

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:

```
! 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
```

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 example 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 example 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 example 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 example 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. Compare 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 example 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 example 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 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. Inspeção 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 suspeitada. Para uma lista de razões que um ASA se usa para classificar estas gotas, execute a **gota asp do** comando show

O buffer do padrão para cada captura 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
```

Tip: Esta captura ASA ASP é muito útil nesta encenação confirmar se o ASA deixa cair pacotes devido a um ACL ou a um NAT faltante (que está precisado de abrir uma porta específica TCP ou UDP para Expressway-e).

Recomendações

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

É altamente 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 inspeções 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 a executar Expressway-e que usa interfaces de rede duplas/NIC dual é executar Expressway-e com um únicos NIC e NAT estático usando a configuração da reflexão NAT nos Firewall. Este link mostra uns detalhes mais adicionais sobre esta encenação:

Note: Enquanto se mencionou no início deste documento, a aplicação do NIC dual é recomendada sobre a reflexão NAT.

Documentação relacionada

[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](#)