ASA 8.2: Redirecionamento de porta (transmissão) com nat, o global, o estático, e comandos access-list que usam o ASDM

Índice

Introdução

Este documento descreve como o redirecionamento de porta funciona no Cisco Adaptive Security Appliance (ASA) usando ASDM. Ele lida com o controle de acesso do tráfego através do ASA e de como as regras de tradução funcionam.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Visão geral de NAT
- PIX/ASA 7.X: Redirecionamento de porta

Componentes Utilizados

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

- Versão ASA 8.2 do Cisco 5500 Series
- Versão ASDM Cisco 6.3

Nota: Esta configuração trabalha muito bem da versão de software 8.0 8.2 de Cisco ASA somente, porque não há nenhuma alteração principal na funcionalidade de NAT.

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.

Convenções

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

Diagrama de Rede

Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Permitir o Acesso de Externo

O acesso externo descreve conexões de uma interface de nível de segurança mais elevado para uma interface de nível de segurança mais baixo. Isso inclui conexões de dentro para fora, dentro de DMZs (Zonas Desmilitarizadas) e DMZs para fora. Isso também pode incluir conexões de uma DMZ para outra, desde que a interface de origem da conexão possua um nível de segurança mais elevado do que a de destino.

Nenhuma conexão pode passar através da ferramenta de segurança sem uma regra de tradução configurada. Esta característica é chamada **controle nat**. A imagem mostrada aqui descreve como desabilitar isto com o ASDM a fim permitir conexões com o ASA sem nenhuma tradução de endereços. Contudo, se você tem qualquer regra de tradução configurada, a seguir desabilitar esta característica não permanece válida para todo o tráfego e você precisará de isentar explicitamente as redes da tradução de endereços.

Permitir o Acesso de Host Internos às Redes Externas via NAT

Você poderia permitir que um grupo de host internos/redes alcance o mundo exterior configurando as regras dinâmicas NAT. A fim realizar isto, você precisa de selecionar o endereço real dos anfitriões/redes para ser dados o acesso e então têm que ser traçados a um pool de endereços IP de Um ou Mais Servidores Cisco ICM NT traduzidos.

Termine estas etapas a fim permitir o acesso dos host internos às redes externas com NAT:

1. Vá à **configuração** > ao **Firewall** > às **regras NAT**, o clique **adiciona**, e escolhe então a opção **dinâmica da regra adicionar NAT** a fim configurar uma regra dinâmica NAT.
2. Escolha o nome da relação a que os anfitriões reais são conectados. Escolha o endereço IP

real dos anfitriões/redes usando o **botão Details Button no** campo de **fonte**.
3. Neste exemplo, a *rede interna* inteira foi selecionada. **APROVAÇÃO do** clique a fim terminar a seleção.
4. O clique **controla** a fim selecionar o pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT a que a rede real será traçada.
5. O clique **adiciona** a fim abrir o indicador do conjunto de endereço global adicionar.
6. Escolha a opção da **escala** e especifique os endereços IP de Um ou Mais Servidores Cisco ICM NT começando e de término junto com a interface de saída. Também, especifique um pool original ID e o clique **adicionam** a fim adicionar estes ao conjunto de endereços. Clique a **APROVAÇÃO** a fim retornar ao indicador do conjunto global do controlo.
7. Clique a **APROVAÇÃO** a fim retornar ao indicador dinâmico da regra adicionar NAT.
8. Clique a **APROVAÇÃO** a fim terminar a configuração dinâmica da regra NAT.
9. O clique **aplica-se** para que as mudanças tomem o efeito.**Nota: O tráfego da possibilidade com o Firewall sem** opção da **tradução de endereços** é desmarcado.

Este é o CLI equivalente output para esta configuração ASDM:

```
nat-control global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192 nat
(inside) 10 172.16.11.0 255.255.255.0
```

Conforme esta configuração, os anfitriões na rede de 172.16.11.0 obterão traduzidos a todo o endereço IP de Um ou Mais Servidores Cisco ICM NT do conjunto NAT, 209.165.200.20-209.165.200.40. Aqui, o conjunto NAT ID é muito importante. Você poderia atribuir o mesmo conjunto NAT a uma outra rede interna/dmz. Se o pool traçado tem menos endereços do que o grupo real, você poderia ser executado fora dos endereços se a quantidade de tráfego é mais do que esperada. Em consequência, você poderia tentar executar a PANCADINHA ou você poderia tentar editar o conjunto de endereços existente para estendê-la.

Nota: Ao fazer toda a alteração à regra da tradução existente, note que você precisa de usar o **comando clear xlate** para que aquelas alterações tomem o efeito. Se não, a conexão existente precedente permanecerá lá na tabela de conexão até elas intervalo. Seja cauteloso ao usar o **comando clear xlate**, porque termina imediatamente as conexões existentes.

Permita o acesso dos host internos às redes externas com PANCADINHA

Se desejar que os host internos compartilhem um único endereço público para a tradução, use o PAT. Se a **declaração global** especificar um endereço, esse endereço terá a porta traduzida. O ASA permite uma tradução de porta por apoios da relação e da essa tradução até 65,535 objetos xlate ativo ao único endereço global.

Termine estas etapas a fim permitir o acesso dos host internos às redes externas com PANCADINHA:

1. Vá à **configuração** > ao **Firewall** > às **regras NAT**, o clique **adiciona**, e escolhe então a opção **dinâmica da regra adicionar NAT** a fim configurar uma regra dinâmica NAT.
2. Escolha o nome da relação a que os anfitriões reais são conectados. Escolha o endereço IP real dos anfitriões/redes usando o **botão Details Button no** campo de **fonte**, e escolha a **rede interna**. O clique **controla** a fim definir a informação de endereço traduzido.
3. Clique em Add.
4. Escolha a **tradução de endereço de porta (PAT) usando o endereço IP de Um ou Mais Servidores Cisco ICM NT da opção de interface**, e o clique **adiciona** a fim adicionar-la ao

conjunto de endereços. Não esqueça atribuir um ID exclusivo para este pool de endereço NAT.
5. Émostrado aqui o pool do endereço configurado com a interface externa como o único endereço disponível nesse pool. Clique a **APROVAÇÃO** a fim retornar ao indicador dinâmico da regra adicionar NAT.
6. Clique em **OK**.
7. A regra dinâmica configurada NAT é mostrada aqui placa na configuração > no Firewall > nas regras NAT.

Este é o CLI equivalente output para esta configuração da PANCADINHA:

```
global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0
```

Restrigir o Acesso de Host Internos a Redes Externas

Quando nenhuma regra do acesso é definida, os usuários de uma interface de segurança mais elevada podem alcançar todos os recursos associados com uma interface de segurança mais baixa. Para restringir usuários determinados de alcançar determinados recursos, use regras do acesso no ASDM. Este exemplo descreve como permitir que um usuário único alcance fora dos recursos (com FTP, S TP, POP3, HTTPS, e WWW) e restrinja todos os outro de alcançar os recursos exteriores.

Nota: Haverá um “implícito nega” a regra na extremidade de cada lista de acesso.

Conclua estes passos:

1. Vá às **regras da configuração** > do **Firewall** > do **acesso**, o clique **adiciona**, e escolhe a opção da **regra do acesso adicionar** a fim criar uma entrada de lista de acesso nova.
2. Escolha o endereço IP de origem que deve ser permitida no campo de **fonte**. Escolha **alguns** como o destino, **dentro** como da relação, e **permita-os** como a ação. Ultimamente, clique o **botão Details Button no** campo do serviço a fim criar um grupo de serviço TCP para as portas exigidas.
3. O clique **adiciona**, e escolhe então a opção do **grupo de serviço TCP**.
4. Dê entrada com um nome para este grupo. Escolha cada um das portas exigidas, e o clique **adiciona** a fim movê-las para os membros no campo do grupo.
5. Você deve ver todas as portas selecionada no campo à direita. Clique a **APROVAÇÃO** a fim terminar as portas do serviço que selecionam o processo.
6. Você pode ver o grupo de serviço configurado TCP aqui. Clique em **OK**.
7. **APROVAÇÃO do** clique a fim terminar a configuração.
8. A regra do acesso configurado pode ser considerada sob a **interface interna na** placa das regras da configuração > do Firewall > do acesso.
9. Para a acessibilidade, você poderia igualmente editar o grupo de serviço TCP diretamente no painel direito na aba dos **serviços**. O clique **edita** a fim alterar diretamente este grupo de serviço.
10. Reorienta outra vez ao indicador de grupo de serviço da edição TCP. Execute as alterações baseadas em suas exigências, e clique a **APROVAÇÃO** a fim salvar as mudanças.
11. Émostrada aqui uma vista completa do ASDM:

Esta é a configuração de CLI equivalente:

```
object-group service Permit-172.16.10.100 TCP port-object eq ftp port-object eq ftp-data port-
object eq www port-object eq https port-object eq pop3 port-object eq smtp ! access-list
inside_access_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 !
access-group inside_access_in in interface inside !
```

Para obter informações completas sobre de executar o controle de acesso, consulte para adicionar ou alterar uma lista de acessos com o ASDM GUI.

Permita o tráfego entre relações com o mesmo nível de segurança

Esta seção descreve como permitir o tráfego dentro das relações que têm os mesmos níveis de segurança.

Estas instruções descrevem como permitir uma comunicação da intra-relação.

Isto será útil para o tráfego VPN que incorpora uma relação, mas é distribuído então para fora a mesma relação. O tráfego VPN pôde ser unencrypted neste caso, ou pôde re-ser cifrado para uma outra conexão de VPN. Vai à **configuração** > a **instalação de dispositivo** > **relações**, e escolhe o **tráfego da possibilidade entre dois ou mais anfitriões conectados à mesma opção de interface**.

Estas instruções descrevem como permitir uma comunicação da inter-relação.

Isto é útil permitir uma comunicação entre relações com os níveis de segurança iguais. Vai à **configuração** > a **instalação de dispositivo** > **relações**, e escolhe o **tráfego da possibilidade entre dois ou mais relações que são configuradas com a mesma** opção dos **níveis de segurança**.

Este é o CLI equivalente para both of these ajustes:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

Permita o acesso dos hosts não confiáveis aos hosts em sua rede confiável

Isto pode ser conseguido com da aplicação de uma tradução NAT estática e de uma acesso-regra para permitir aqueles anfitriões. Você exige para configurar este sempre que um usuário externo gostaria de alcançar todo o server que se sentar em sua rede interna. O server na rede interna terá um endereço IP privado que não seja roteável no Internet. Em consequência, você precisa de traduzir esse endereço IP privado a um endereço IP público com uma regra do NAT estático. Supõe que você tem um servidor interno (172.16.11.5). A fim fazer este trabalho, você precisa de traduzir este IP de servidor privado a um IP do público. Este exemplo descreve como executar o NAT estático bidirecional para traduzir 172.16.11.5 a 209.165.200.5.

A seção em permitir que o usuário externo alcance este servidor de Web executando uma regra do acesso não é mostrada aqui. Um breve snippet CLI é mostrado aqui para sua compreensão:

```
access-list 101 permit TCP any host 209.165.200.5
```

Para mais informação, consulte para adicionar ou alterar uma lista de acessos com o ASDM GUI.

Nota: Especificar a palavra-chave “” permite que todo o usuário do mundo exterior alcance este

server. Também, se não se especifica para nenhuma portas do serviço, o server pode ser alcançado em toda a porta do serviço enquanto aquele estada aberta. Use o cuidado quando você implementar, e você são recomendados limitar a permissão ao usuário externo individual e igualmente à porta exigida no server.

Termine estas etapas a fim configurar o NAT estático:

1. Vá à **configuração** > ao **Firewall** > às **regras NAT**, o clique **adiciona**, e escolhe **adiciona a regra do NAT estático**.
2. Especifique o endereço IP original e o endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido junto com suas relações associadas, e clique a **APROVAÇÃO**.
3. Você pode ver a entrada NAT estática configurada aqui. O clique **aplica-se** a fim enviar este ao ASA.

Este é um breve exemplo CLI para esta configuração ASDM:

```
! static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !
```

Desabilitar o NAT para Hosts/Redes Específicos

Quando você precisa de isentar anfitriões ou redes específicas do NAT, adicionar uma regra isenta NAT para desabilitar a tradução de endereços. Isto reserva traduzido e host remotos para iniciar conexões.

Conclua estes passos:

1. Vá à **configuração** > ao **Firewall** > às **regras NAT**, o clique **adiciona**, e escolhe **adiciona a regra isenta NAT**.
2. Aqui, a rede interna 172.18.10.0 foi isentada da tradução de endereços. Certifique-se de que a opção **isenta** esteve selecionada. O sentido isento NAT tem duas opções:Tráfego de saída às interfaces de segurança mais baixaTráfego de entrada às interfaces de segurança mais elevadaA opção padrão é para o tráfego de saída. **APROVAÇÃO do** clique a fim terminar a etapa.**Nota:** Quando você escolhe **não isente a** opção, esse host particular não será isentado do NAT e uma regra separada do acesso será adicionada com “nega” a palavra-chave. Isto é útil em evitar anfitriões específicos do NAT por mais isenta que a sub-rede completa, com exclusão destes anfitriões, seja NAT isentado.
3. Você pode ver a regra isenta NAT para a direção externa aqui. O clique **aplica-se** a fim enviar a configuração ao ASA.Este é o CLI equivalente output para sua referência:
```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```
4. Aqui você pode ver como editar a regra isenta NAT para seu sentido. Clique a **APROVAÇÃO** para que a opção tome o efeito.
5. Você pode agora ver que o sentido esteve mudado a *de entrada*.O clique **aplica-se** a fim enviar este CLI output ao ASA:
```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```
Nota: Disto, você pode ver que uma palavra-chave nova (fora) esteve adicionada para terminar do **comando nat 0**. Esta característica é chamada um **NAT exterior**.
6. Uma outra maneira de desabilitar o NAT é com a aplicação da identidade NAT. A identidade

NAT traduz um host ao mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT. Está aqui um exemplo de NAT estático regular da identidade, onde o host (172.16.11.20) esteja traduzido ao mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT quando é alcançado da parte externa.Isto é o CLI equivalente output:

```
! static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255 !
```

Redirecionamento de Portas (Encaminhamento) com Statics

A transmissão ou o redirecionamento de porta da porta são uns recursos úteis onde os usuários externos tentem alcançar um servidor interno em uma porta específica. A fim conseguir isto, o servidor interno, que tem um endereço IP privado, será traduzido a um endereço IP público que seja permitido por sua vez o acesso para a porta específica.

Neste exemplo, o usuário externo quer alcançar o servidor SMTP, 209.165.200.15 na porta 25. Isto é realizado em duas etapas:

1. Traduza o servidor de e-mail interno, 172.16.11.15 na porta 25, ao endereço IP público, 209.165.200.15 na porta 25.
2. Permita o acesso ao mail server público, 209.165.200.15 na porta 25.

Quando o usuário externo tenta alcançar o server, 209.165.200.15 na porta 25, este tráfego estará reorientado ao servidor de e-mail interno, 172.16.11 15 na porta 25.

1. Vá à **configuração >** ao **Firewall >** às **regras NAT**, o clique **adiciona**, e escolhe **adiciona a regra do NAT estático**.
2. Especifique a fonte original e o endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido junto com suas relações associadas. Escolha **permitem a tradução de endereço de porta (PAT)**, especificam as portas a ser reorientadas, e clicam a **APROVAÇÃO**.
3. A regra configurada do PAT estático é considerada aqui:Isto é o CLI equivalente output:
   ```
   ! static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
   !
   ```
4. Esta é a regra do acesso que permite que o usuário externo alcance o server smtp do público em 209.165.200.15:**Nota:** Certifique-se usar anfitriões específicos em vez de usar **toda a** palavra-chave na fonte da regra do acesso.

Limitar Sessão de TCP/UDP Usando Static

Você pode especificar o número máximo de conexões TCP/UDP usando a regra estática. Você pode igualmente especificar o número máximo de conexões embriônica. Uma conexão embriônica é uma conexão que seja um estado entreaberto. Um número maior destes afetará o desempenho do ASA. Limitar estas conexões impedirá determinados ataques como o DoS e o SYN em certa medida. Para a mitigação completa, você precisa de definir a política na estrutura MPF, que é além do alcance deste documento. Para obter informações adicionais sobre deste assunto, refira o abrandamento dos ataques de rede.

Conclua estes passos:

1. Clique a aba das **configurações de conexão**, e especifique os valores para as conexões máxima para esta tradução estática.
2. Estas imagens mostram os limites da conexão para esta tradução estática específica:Isto é

o CLI equivalente output:!

```
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
TCP 100 50 !
```

Lista de Acessos Baseada em Tempo

Esta seção trata a aplicação de listas de acesso baseada em tempo usando o ASDM. As regras do acesso podem ser aplicadas baseadas no tempo. A fim executar isto, você precisa de definir uma tempo-escala que especifique os sincronismos no dia/semana/mês/ano. Então, você precisa de ligar esta tempo-escala à acesso-regra exigida. a Tempo-escala pode ser definida em duas maneiras:

1. Absoluto - Define um período de tempo com horas inicial e tempo do término.
2. Periódico - Igualmente sabido como o retorno. Define um período de tempo que ocorra em intervalos especificados.

Nota: Antes que você configure a tempo-escala, certifique-se de que o ASA esteve configurado com as configurações de data/hora corretas enquanto esta característica usa os ajustes do relógio de sistema para executar. Ter o ASA sincronizado com o servidor de NTP renderá resultados muito melhores.

Termine estas etapas a fim configurar esta característica com o ASDM:

1. Ao definir a regra do acesso, clique o **botão Details Button no** campo do intervalo de tempo.
2. O clique **adiciona** a fim criar uma tempo-escala nova.
3. Defina o nome do intervalo de tempo, e especifique as horas inicial e o tempo do término. Clique em **OK**.
4. Você pode ver o intervalo de tempo aqui. Clique a **APROVAÇÃO** a fim retornar ao indicador da regra do acesso adicionar.
5. Você pode agora ver que o intervalo de tempo do Restringir-uso esteve limitado a esta regra do acesso.Conforme esta configuração da regra do acesso, o usuário em 172.16.10.50 foi restringido de usar todos os recursos de 05/Feb/2011 2 PM a 06/Feb/2011 4.30 PM. Isto é o CLI equivalente output:

   ```
   time-range Restrict-Usage absolute start 14:00 05 February 2011 end 16:30 06 February 2011
   ! access-list inside_access_out extended deny ip host 172.16.10.50 any time-range Restrict-
   Usage ! access-group inside_access_out in interface inside
   ```
6. Está aqui um exemplo em como especificar um intervalo de tempo de retorno. O clique **adiciona** a fim definir um intervalo de tempo de retorno.
7. Especifique os ajustes baseados em suas exigências, e clique a **APROVAÇÃO** a fim terminar.
8. Clique a **APROVAÇÃO** a fim retornar de volta ao indicador do intervalo de tempo.Conforme esta configuração, o usuário em 172.16.10.50 foi negado o acesso a todos os recursos de 3 PM a 8 PM em todos os dias úteis exceto sábado e domingo.

   ```
   ! time-range Restrict-Usage absolute start 00:00 05 February 2011 end 00:30 06 March 2011
   periodic weekdays 15:00 to 20:00 ! access-list inside_access_out extended deny ip host
   172.16.10.50 any time-range Restrict-Usage ! access-group inside_access_out in interface
   inside
   ```

   Nota: Se um **comando time-range** tem valores absolutos e periódicos especificados, a seguir os **comandos periodic** estão avaliados somente depois que as horas inicial absolutas são alcançadas, e não são mais adicionais avaliados depois que o tempo absoluto do fim é alcançado.

Informações Relacionadas

- Página de documentação de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems