Uso da indicação NAT e de PANCADINHA no exemplo seguro da configuração de firewall de Cisco ASA

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar - Instruções NAT múltipla com o NAT manual e auto
Diagrama de Rede
Versão ASA 8.3 e mais atrasado
Configurar - Conjuntos globais múltiplos
Diagrama de Rede
Versão ASA 8.3 e mais atrasado
Configurar - Misture indicações NAT e de PANCADINHA
Diagrama de Rede
Versão ASA 8.3 e mais atrasado
Configurar - Instruções NAT múltipla com indicações manuais
Diagrama de Rede
Versão ASA 8.3 e mais atrasado
Configurar - Use a política NAT
Diagrama de Rede
Versão ASA 8.3 e mais atrasado
Verificar
Conexão
Syslog
Traduções NAT (xlate)
Troubleshooting

Introdução

Este documento fornece configurações do Network Address Translation (NAT) e da tradução de endereço de porta (PAT) dos exemplos básicos no Firewall adaptável seguro da ferramenta de segurança de Cisco (ASA). Este documento igualmente fornece diagramas de rede simplificada. Consulte a documentação ASA para sua versão de software ASA para mais informação detalhada.

Este documento oferece análise personalizada do seu dispositivo Cisco.

Refira a configuração de NAT no ASA em ferramentas de segurança do 5500/5500-X Series ASA para mais informação.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do Firewall seguro de Cisco ASA.

Componentes Utilizados

A informação neste documento é baseada na versão 8.4.2 e mais recente segura do software de firewall de Cisco ASA.

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.

Configurar - Instruções NAT múltipla com o NAT manual e auto

Diagrama de Rede

Neste exemplo, o ISP fornece a gerente de rede um bloco 209.165.201.0/27 do endereço IP de Um ou Mais Servidores Cisco ICM NT que varie de 209.165.201.1 a 209.165.201.30. A gerente de rede decide atribuir 209.165.201.1 à interface interna no roteador de Internet, e 209.165.201.2 à interface externa do ASA.

O administrador de rede já tem um endereço do C da classe atribuído à rede, 198.51.100.0/24, e tem algumas estações de trabalho que usam estes endereços a fim alcançar o Internet. Estas estações de trabalho não exigem nenhuma tradução de endereços porque já têm endereços válidos. Contudo, as novas estações de trabalho são atribuídas endereços na rede 10.0.0.0/8 e precisam de ser traduzidas (porque 10.x.x.x é um dos espaços de endereços não-roteável pelo RFC 1918.

A fim acomodar este projeto de rede, o administrador de rede deve usar duas declarações NAT e um conjunto global na configuração ASA:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Esta configuração não traduz o endereço de origem de nenhum tráfego de saída da rede 198.51.100.0/24. Traduz um endereço de origem na rede 10.0.0.0/8 em um endereço da escala 209.165.201.3 com 209.165.201.30.

Nota: Quando você tem uma relação com uma política de NAT e se não há nenhum

conjunto global a uma outra relação, você precisa de usar 0 nat a fim estabelecer a exceção NAT.

Versão ASA 8.3 e mais atrasado

Está aqui a configuração.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configurar - Conjuntos globais múltiplos

Diagrama de Rede

Neste exemplo, a gerente de rede tem duas escalas dos endereços IP de Um ou Mais Servidores Cisco ICM NT que são registrados no Internet. A gerente de rede deve converter todos os endereços internos, que estão na escala 10.0.0.0/8, em endereços registrados. As escalas dos endereços IP de Um ou Mais Servidores Cisco ICM NT que a gerente de rede deve usar são 209.165.201.1 com 209.165.201.30 e 209.165.200.225 com 209.165.200.254. A gerente de rede pode fazer esta com:

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30
```

```
object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Nota: Um esquema de endereçamento de wildcard é usado na declaração NAT. Esta indicação diz o ASA para traduzir todo o endereço de fonte interna quando sai ao Internet. O endereço nesse comando pode ser mais específico, se desejado.

Versão ASA 8.3 e mais atrasado

Está aqui a configuração.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurar - Misture indicações NAT e de PANCADINHA

Diagrama de Rede

Neste exemplo, o ISP fornece a gerente de rede um intervalo de endereço de 209.165.201.1 a 209.165.201.30 para que a empresa use-se. A gerente de rede decidiu usar 209.165.201.1 para a interface interna no roteador de Internet e 209.165.201.2 para a interface externa no ASA. Você é deixado então com 209.165.201.3 com 209.165.201.30 para usar-se para o conjunto NAT. Contudo, a gerente de rede sabe que, a qualquer altura, pode haver mais de 28 povos que tentam sair do ASA. A gerente de rede decidiu tomar 209.165.201.30 e fazer-lhe um endereço PAT de modo que os usuários múltiplos pudessem compartilhar de um endereço ao mesmo tempo.

Estes comandos instruem o ASA traduzir o endereço de origem a 209.165.201.3 com 209.165.201.29 para que os primeiros 27 usuários internos passem através do ASA. Depois que estes endereços são esgotados, a seguir o ASA traduz todos os endereços de origem subsequentes a 209.165.201.30 até que um dos endereços no conjunto NAT se torne livre.

> Nota: Um esquema de endereçamento de wildcard é usado na declaração NAT. Esta indicação diz o ASA para traduzir todo o endereço de fonte interna quando sai ao Internet. O endereço nesse comando pode ser mais específico, se desejado.

Versão ASA 8.3 e mais atrasado

Está aqui a configuração.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurar - Instruções NAT múltipla com indicações manuais

Diagrama de Rede

Neste exemplo, o ISP fornece outra vez a gerente de rede um intervalo de endereço de 209.165.201.1 a 209.165.201.30. A gerente de rede decide atribuir 209.165.201.1 à interface interna no roteador de Internet e 209.165.201.2 à interface externa do ASA.

Contudo, nesta encenação, um outro segmento de LAN privado é colocado fora do roteador de Internet. A gerente de rede prefere não desperdiçar endereços do conjunto global quando os anfitriões nestas duas redes falam entre si. A gerente de rede ainda precisa de traduzir o endereço de origem para todos os usuários internos (10.0.0.0/8) quando sai ao Internet.

Esta configuração não traduz aqueles endereços com um endereço de origem de 10.0.0.0/8 e um endereço de destino de 198.51.100.0/24. Traduz o endereço de origem de todo o tráfego iniciado de dentro da rede 10.0.0.0/8 e destinado para em qualquer lugar a não ser 198.51.100.0/24 em um endereço da escala 209.165.201.3 com 209.165.201.30.

Se você tem a saída de um **comando write terminal de** seu dispositivo Cisco, você pode usar a ferramenta Output Interpreter (clientes registrados somente).

Versão ASA 8.3 e mais atrasado

Está aqui a configuração.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configurar - Use a política NAT

Diagrama de Rede

Quando você usa uma lista de acessos com o **comando nat** para todo o ID do NAT a não ser 0, você permite a política NAT.

A política NAT permite que você identifique o tráfego local para a tradução de endereços pela especificação dos endereços de rementente e destinatário (ou de portas) em uma lista de acessos. O NAT regular usa /portas dos endereços de origem somente. A política NAT usa

ambas as /portas dos endereços de rementente e destinatário.

> Nota: Todos os tipos da política de suporte NAT NAT à exceção da isenção de NAT (0 listas de acesso nat). A isenção de NAT usa um Access Control List (ACL) a fim identificar os endereços locais, mas difere da política NAT porque as portas não são consideradas.

Com política NAT, você pode criar o NAT múltiplo ou as instruções estáticas que identificam o mesmo endereço local enquanto a combinação da /porta da fonte e da /porta do destino é original para cada indicação. Você pode então combinar endereços globais diferentes a cada par da /porta da fonte e da /porta do destino.

Neste exemplo, a gerente de rede tem que fornecer o acesso para o endereço IP de destino 172.30.1.11 para a porta 80 (Web) e a porta 23 (telnet), mas deve usar dois endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes como um endereço de origem. 209.165.201.3 é usado como um endereço de origem para a Web e 209.165.201.4 é usado para o telnet, e deve converter todos os endereços internos, que estão na escala 10.0.0.0/8. A gerente de rede pode fazer esta com:

Using the Manual Nat statements:

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Versão ASA 8.3 e mais atrasado

Está aqui a configuração.

Using the Manual Nat statements:

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11
```

```
object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> Nota: Para obter mais informações sobre da configuração do NAT e da PANCADINHA na versão ASA 8.4, refira a informação sobre o NAT.
>
> Para obter mais informações sobre da configuração das Listas de acesso na versão ASA 8.4, refira a informação sobre Listas de acesso.

Verificar

Tente alcançar um Web site através do HTTP com um web browser. Este exemplo usa um local que seja hospedado em 198.51.100.100. Se a conexão é bem sucedida, a saída na próxima seção pode ser considerada no ASA CLI.

Conexão

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
flags UIO
```

O ASA é um firewall stateful, e o tráfego de retorno do servidor de Web é permitido para trás com o Firewall porque combina uma ***conexão na*** tabela de conexão do Firewall. Trafique que combina uma conexão que preexista seja permitida com o Firewall sem ser obstruída por uma relação ACL.

Na saída precedente, o cliente na interface interna estabeleceu uma conexão ao host de 198.51.100.100 fora da interface externa. Esta conexão é feita com o protocolo de TCP e foi inativa por seis segundos. As bandeiras da conexão indicam o estado atual desta conexão. Mais informação sobre bandeiras da conexão pode ser encontrada em bandeiras da conexão de TCP ASA.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431
```

```
Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.0.0.2/57431 (209.165.201.3/57431)
```

O Firewall ASA gerencie Syslog durante a operação normal. Os Syslog variam na verbosidade baseada na configuração de registro. A saída mostra dois Syslog que são vistos a nível seis, ou o nível **"informativo"**.

Neste exemplo, há dois Syslog gerados. O primeiro é um mensagem de registro que indique que o Firewall construiu uma **tradução**, especificamente uma tradução dinâmica TCP (PANCADINHA). Indica o endereço IP de origem e a porta e o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta traduzidos enquanto o tráfego atravessa do interior às interfaces externas.

O segundo Syslog indica que o Firewall construiu uma **conexão em** sua tabela de conexão para este tráfego específico entre o cliente e servidor. Se o Firewall foi configurado a fim obstruir esta tentativa de conexão, ou algum outro fator inibiu a criação desta conexão (confinamentos de recurso ou um possível erro de configuração), o Firewall não geraria um log que indicasse que a conexão esteve construída. Em lugar de registraria uma razão para que a conexão seja negada ou uma indicação sobre que fator inibiu a conexão da criação.

Traduções NAT (xlate)

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Como parte desta configuração, a PANCADINHA é configurada a fim traduzir os endereços IP de Um ou Mais Servidores Cisco ICM NT do host interno aos endereços que são roteável no Internet. A fim confirmar que estas traduções estão criadas, você pode verificar a tabela do xlate (tradução). O comando show xlate**,** quando combinado com o **palavra-chave local** e o endereço IP de Um ou Mais Servidores Cisco ICM NT do host interno, mostra todas as entradas atuais na tabela de tradução para esse host. A saída precedente mostra que há uma tradução construída atualmente para este host entre as interfaces internas e externas. O IP do host interno e a porta são traduzidos ao endereço de 10.165.200.226 pela configuração.

As bandeiras alistaram, **r mim**, indicam que a tradução é **dinâmica** e um **portmap**. Mais informação sobre configurações de NAT diferentes pode ser encontrada na informação sobre o NAT.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.