Configurar o ASA para redes internas duplas

Índice

Introdução

Este documento descreve como configurar uma ferramenta de segurança adaptável de Cisco (ASA) essa versão de software 9.x das corridas para o uso de duas redes internas.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em Cisco ASA que executa a versão de software 9.x.

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.

Informações de Apoio

Quando você adiciona uma segunda rede interna atrás de um Firewall ASA, considere esta informação importante:

- O ASA não apoia o endereçamento secundário.
- Um roteador deve ser usado atrás do ASA a fim conseguir o roteamento entre a rede atual e a rede recentemente adicionada.
- O gateway padrão para todos os anfitriões deve apontar ao roteador interno.
- Você deve adicionar uma rota padrão no roteador interno esses pontos ao ASA.
- Você deve cancelar o esconderijo do Address Resolution Protocol (ARP) no roteador interno.

Configurar

Use a informação que é descrita nesta seção a fim configurar o ASA.

Diagrama de Rede

Está aqui a topologia que é usada para os exemplos durante todo este documento:

> **Note**: Os esquemas de endereçamento de IP que são usados nesta configuração não são legalmente roteável no Internet. São os endereços do RFC 1918 que são usados em um ambiente de laboratório.

Configuração ASA 9.x

Se você tem a saída do **comando write terminal de** seu dispositivo Cisco, você pode usar a ferramenta Output Interpreter (clientes registrados somente) a fim indicar problemas potenciais e reparos.

Está aqui a configuração para o ASA que executa a versão de software 9.x:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
```

```
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Permita o acesso dos host internos às redes externas com PANCADINHA

Se você pretende mandar os host internos compartilhar de um único endereço público para a tradução, tradução de endereço de porta (PAT) do uso. Uma das configurações as mais simples da PANCADINHA envolve a tradução de todos os host internos de modo que pareçam ser o IP da interface externa. Esta é a configuração típica da PANCADINHA que está usada quando o número de endereços IP roteável que estão disponíveis do ISP é limitado somente a alguns, ou apenas um.

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

1. Navegue à **configuração >** ao **Firewall >** às **regras NAT**, o clique **adiciona**, e escolhe o **objeto de rede** a fim configurar uma regra dinâmica NAT:

2. Configurar a rede/host/escala para que a PANCADINHA dinâmica é exigida. Neste exemplo, todos sub-redes do interior foram selecionados. Este processo deve ser repetido para as sub-redes específicas que você deseja traduzir desse modo:

3. Clique o **NAT**, verifique a caixa de verificação **automática da regra de tradução de endereço adicionar**, entre em **dinâmico,** e ajuste a opção **traduzida do ADDR** de modo que reflita a interface externa. Se você clica o botão da elipse, ajuda-lhe a escolher um objeto PRE-configurado, tal como a interface externa:

4. O clique **avançou** a fim selecionar uma fonte e uma interface de destino:

5. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se** a fim aplicar as mudanças. Uma vez que completo, o Security Device Manager adaptável (ASDM) mostra a regra NAT:

Configuração do Roteador B

Está aqui a configuração para roteador B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
```

```
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Verificar

Alcance um site através do HTTP com um navegador da Web a fim verificar que sua configuração trabalha corretamente.

Este exemplo usa um local que seja hospedado no endereço IP 198.51.100.100. Se a conexão é bem sucedida, as saídas que são fornecidas nas seções que seguem podem ser consideradas no ASA CLI.

Conexão

Inscreva o **comando address da conexão da mostra** a fim verificar a conexão:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
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. O tráfego que combina uma conexão que preexista é permitido com o Firewall sem ser obstruída por um Access Control List da 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.

> **Note**: Refira o documento Cisco das bandeiras da conexão de TCP ASA (acúmulo e teardown da conexão) para obter mais informações sobre das bandeiras da conexão.

Troubleshooting

Use a informação que é descrita nesta seção a fim pesquisar defeitos problemas de configuração.

Syslogs

Inscreva o **comando show log** a fim ver os Syslog:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 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:192.168.1.5/58799 (203.0.113.2/58799)
```

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 informacional*.

Neste exemplo, há dois Syslog gerados. O primeiro é um mensagem de registro para indicar que o Firewall construiu uma tradução; especificamente, uma tradução dinâmica TCP (PANCADINHA). Indica o endereço IP de origem e a porta, assim como o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta traduzidos, porque 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 gerencie um log para indicar que a conexão esteve construída. Em lugar de, registra uma razão para que a conexão seja negada ou uma indicação com respeito ao fator que inibiu a conexão da criação.

Projétis luminosos do pacote

Incorpore este comando a fim permitir a funcionalidade do projétil luminoso do pacote:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

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

A funcionalidade do projétil luminoso do pacote no ASA permite que você especifique um pacote *simulado* e ver todas as várias etapas, verificações, e funções que o Firewall termina quando processa o tráfego. Com esta ferramenta, é útil identificar um exemplo do tráfego que você acredita *deve* ser reservado passar com o Firewall, e se usa que 5-tupple a fim simular o tráfego. No exemplo anterior, o projétil luminoso do pacote é usado a fim simular uma tentativa de conexão que encontre estes critérios:

- O pacote simulado chega na interface interna.
- O protocolo que é usado é TCP.

- O endereço IP cliente simulado é 192.168.1.5.
- O cliente envia o tráfego que é originado da porta 1234.
- O tráfego é destinado a um server no endereço IP 198.51.100.100.
- O tráfego é destinado à porta 80.

Observe que não havia nenhuma menção da interface externa no comando. Isto é devido ao projeto do projétil luminoso do pacote. A ferramenta di-lo como os processos do Firewall que a tentativa do tipo de conexão, que inclui como a distribuiria, e fora de que relação.

> **Tip**: Para obter mais informações sobre da funcionalidade do projétil luminoso do pacote, refira os pacotes de seguimento com seção do projétil luminoso do pacote do *manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6*.

Captação

Incorpore estes comandos a fim aplicar uma captação:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

O Firewall ASA pode capturar o tráfego que incorpora ou deixa suas relações. Esta funcionalidade da captação é fantástica porque pode definitivamente provar em se o tráfego chega, ou sae de, um Firewall. O exemplo anterior mostra a configuração de duas captações nomeadas **capin** e **capout nas** interfaces internas e externas, respectivamente. **Os comandos capture** usam a palavra-chave do **fósforo**, que permite que você especifique o tráfego que você quer capturar.

Para o exemplo da captação do *capin*, indica-se que você quer combinar o tráfego que é considerado na interface interna (ingresso ou saída) esse *host 198.51.100.100 de 192.168.1.5 do*

host tcp dos fósforos. Ou seja você quer capturar todo o tráfego TCP que for enviado do host *192.168.1.5* para hospedar *198.51.100.100*, ou vice versa. O uso da palavra-chave do **fósforo** permite que o Firewall capture esse tráfego bidirecional. **O comando capture** que é definido para a interface externa não provê o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente interno porque o Firewall conduz a PANCADINHA nesse endereço IP cliente. Em consequência, você não pode combinar com esse endereço IP cliente. Em lugar de, este exemplo usa **alguns** a fim indicar que todos os endereços IP de Um ou Mais Servidores Cisco ICM NT possíveis combinariam essa circunstância.

Depois que você configura as captações, você pode então tentar estabelecer outra vez uma conexão e para continuar ver as captações com a **mostra capture o** comando do ***<capture_name>***. Neste exemplo, você pode ver que o cliente pode conectar ao server, como evidente pelo aperto de mão da 3-maneira TCP que é considerado nas captações.

Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Firewall da próxima geração do 5500-X Series de Cisco ASA
- Solicitações para comentários (RFC)
- Guia de configuração de CLI da série de Cisco ASA, 9.0 do Â do âÂ configurando a estática e as rotas padrão
- Cisco Systems do do Â do âÂ do Suporte técnico & da documentação