O ASA libera 9.(x) uma conexão de três redes internas com o exemplo de configuração do Internet

Índice

Introdução

Este documento fornece a informação em como estabelecer a versão 9.1(5) adaptável da ferramenta de segurança de Cisco (ASA) para o uso com três redes internas. As rotas estáticas são usadas nos roteadores por simplicidade.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 9.1(5) adaptável da ferramenta de segurança de Cisco (ASA).

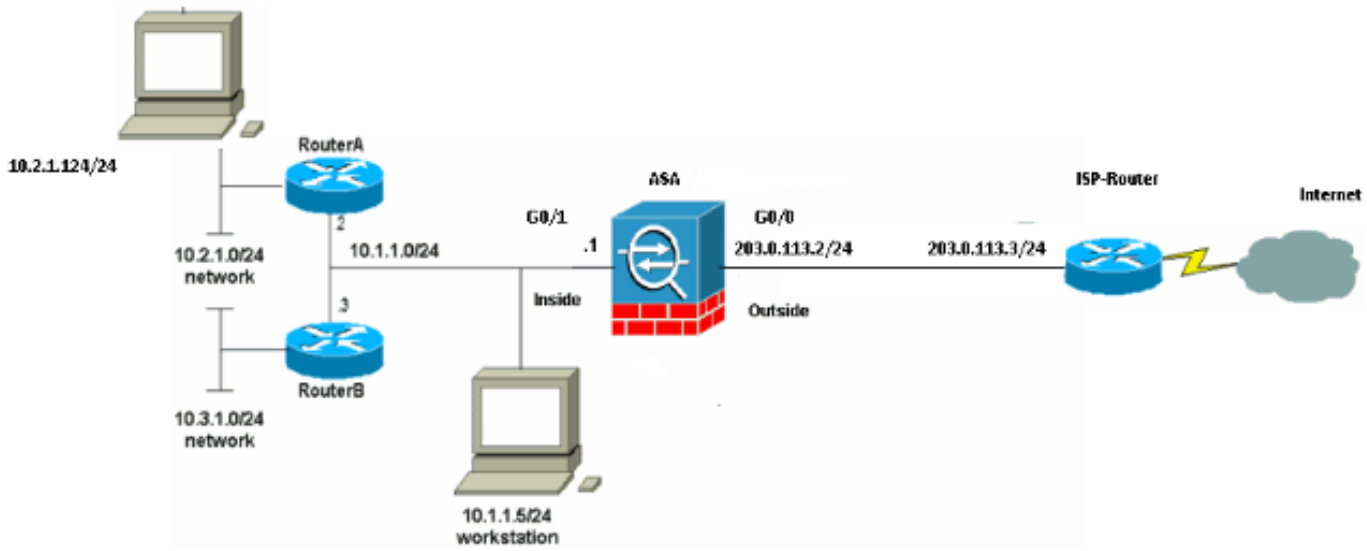
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



> **Note**: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configuração ASA 9.1

Este documento utiliza estas configurações. Se tiver a saída de um comando write terminal do dispositivo Cisco, você poderá usar o Output Interpreter (somente para clientes registrados) para exibir os possíveis problemas e soluções.

Configurações

- Configuração de Roteador A
- Configuração do Roteador B
- Revisão 9.1 ASA e configuração mais atrasada

Configuração de Roteador A

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
```

```
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
```

```
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

Configuração do Roteador B

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
```

```
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

Revisão 9.1 ASA e configuração mais atrasada

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
```

```
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Tente alcançar um 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, esta saída pode ser considerada no ASA CLI.

Conexão

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
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 e não 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 | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

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:10.2.1.124/18711 (203.0.113.2/18711)
```

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

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 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:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 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 das traduções NAT (xlate). 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 203.0.113.2 por nossa 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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O ASA fornece as ferramentas múltiplas com que para pesquisar defeitos a Conectividade. Se a edição persiste depois que você verifica a configuração e verifica a saída alistada previamente, estas ferramentas e técnicas puderam ajudar a determinar a causa de sua falha de conectividade.

Projétil luminoso do pacote

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 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 considere todas as várias etapas, verificações, e funções que o Firewall atravessa 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 usa-se 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 no **interior**.
- O protocolo usado é **TCP**.
- O endereço IP cliente simulado é **10.2.1.124**.
- O cliente envia o tráfego originado da porta **1234**.
- O tráfego é destinado a um server no IP address **198.51.100.100**.
- O tráfego é destinado à porta **80**.

Observe que não havia nenhuma menção da relação **fora no** comando. Isto é pelo 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. Mais informação sobre o projétil luminoso do pacote pode ser encontrada em uns pacotes de seguimento com projétil luminoso do pacote.

Captação

```
ASA# capture capin interface inside match tcp host 10.2.1.124 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       10.2.1.124.18711 > 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 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 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 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 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 se o tráfego chega em, ou sae de, um Firewall. O exemplo anterior mostrou a configuração de duas captações nomeadas capin e capout nas interfaces internas e externas respectivamente. Os comandos capture usaram a palavra-chave do fósforo, que permite que você seja específico sobre que tráfego você quer capturar.

Para o capin da captação, indicou-se que você quis combinar o tráfego visto na interface interna (ingresso ou saída) esse host 198.51.100.100 de 10.2.1.124 do host tcp dos fósforos. Ou seja você quer capturar todo o tráfego TCP que for enviado do host 10.2.1.124 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 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 tentaria então estabelecer outra vez uma conexão, e continua ver as captações com o comando do *<capture_name> da captação da mostra*. Neste exemplo, você pode ver que o cliente podia conectar ao server como evidente pelo aperto de mão da 3-maneira TCP visto nas captações.