O ASA 8.4(x) conecta uma única rede interna ao exemplo de configuração do Internet

Índice

Introdução

Este documento descreve como estabelecer a ferramenta de segurança adaptável de Cisco (ASA) com versão 8.4(1) para o uso em uma única rede interna.

Refira o PIX/ASA: Conectando única a rede interna com o exemplo de configuração do Internet para a mesma configuração no ASA com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no ASA com versão 8.4(1).

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 você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

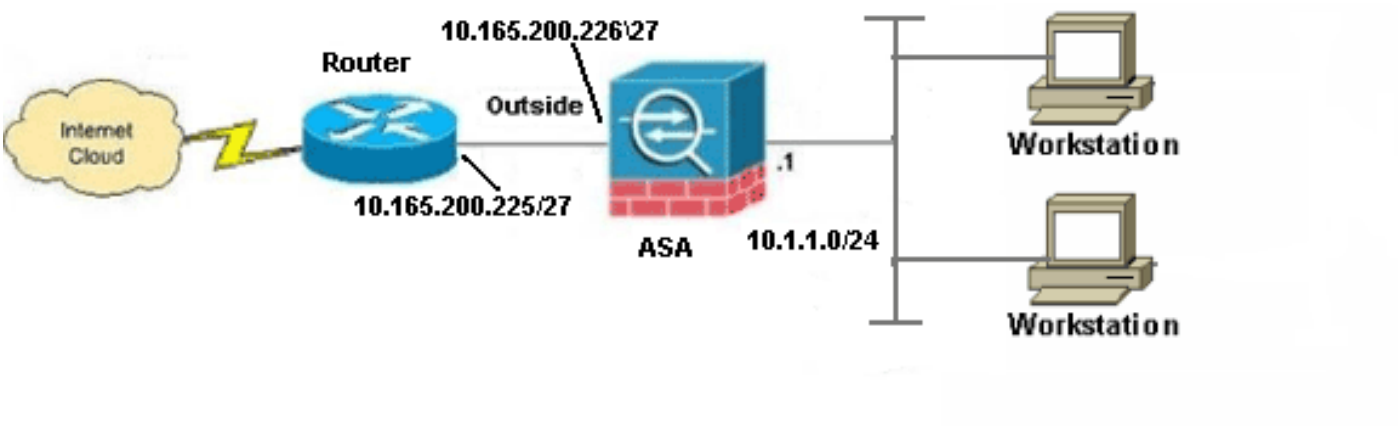
Configurar

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

> Nota: Para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



> Nota: 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 8.4

Este documento utiliza as seguintes configurações:

- Configuração do roteador
- ASA 8.4 e configuração mais atrasada

Configuração do roteador

```
Building configuration...
```

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
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
```

ASA 8.4 e configuração mais atrasada

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224
```

```
!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
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
```

> Nota: Para obter mais informações sobre da configuração do Network Address Translation (NAT) e da tradução de endereço de porta (PAT) 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 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 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, 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. 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 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

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 **"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 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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 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 aqui: Informação sobre o NAT.

Troubleshooting

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.

Pacote-projétil luminoso

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 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 **10.1.1.154**.
- 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 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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 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**,** você indicou que você quis combinar o tráfego visto na interface interna (ingresso ou saída) esse **host 198.51.100.100 de 10.1.1.154 do host tcp dos** fósforos. Ou seja você quer capturar todo o tráfego TCP que for enviado do **host 10.1.1.154 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 o estabelecimento uma conexão outra vez, 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.

Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems