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

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de Rede
Configuração do ASA 8.4
Configuração do roteador
Configuração do ASA 8.4 e posterior
Verificar
Conexão
Syslog
Conversões de NAT (Xlate)
Troubleshoot
Packet Tracer
Captura
Informações Relacionadas

Introduction

Este documento descreve como instalar o Cisco Adaptive Security Appliance (ASA) com a versão 8.4(1) para uso em uma única rede interna.

Consulte o PIX/ASA: Exemplo de conexão de uma única rede interna com a configuração da Internet para a mesma configuração no ASA com versões 8.2 e anteriores.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no ASA com a versão 8.4(1).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

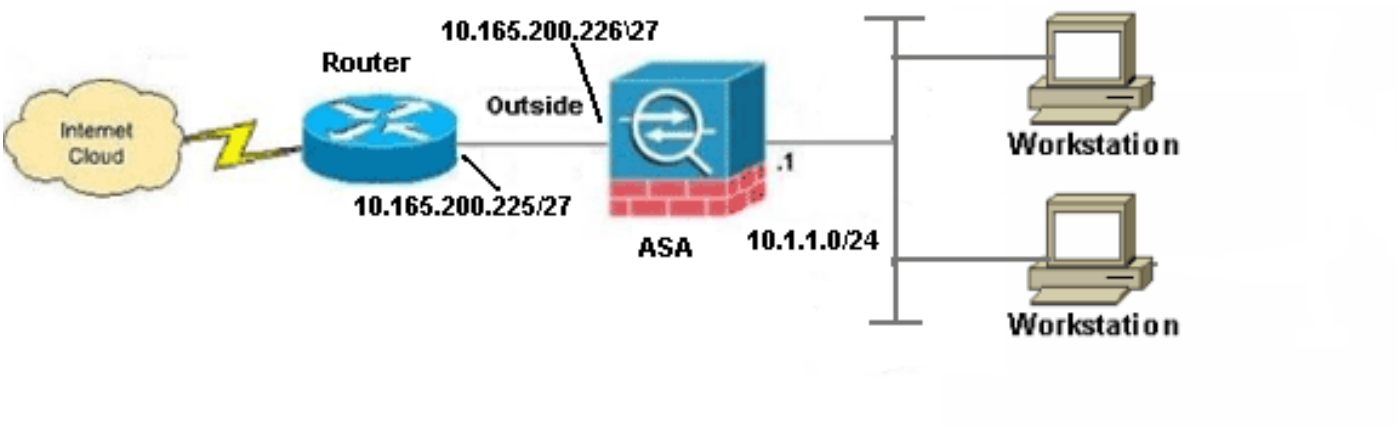
Configurar

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

> **Note**: 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:



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

Configuração do ASA 8.4

Este documento utiliza as seguintes configurações:

- Configuração do roteador
- Configuração do ASA 8.4 e posterior

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
```

Configuração do ASA 8.4 e posterior

```
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
```

Note: Para obter mais informações sobre a configuração de Network Address Translation (NAT) e Port Address Translation (PAT) no ASA versão 8.4, consulte Informações sobre o NAT.

Para obter mais informações sobre a configuração de listas de acesso no ASA versão 8.4, consulte Informações sobre listas de acesso.

Verificar

Tente acessar um site via HTTP com um navegador da Web. Este exemplo usa um site hospedado em 198.51.100.100. Se a conexão for bem-sucedida, essa saída poderá ser vista na CLI do ASA:

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 Web é permitido pelo firewall porque corresponde a uma ***conexão*** na tabela de conexão de firewall. O tráfego que corresponde

a uma conexão pré-existente é permitido através do firewall sem ser bloqueado por uma ACL de interface.

Na saída anterior, o cliente na interface interna estabeleceu uma conexão com o host 198.51.100.100 fora da interface externa. Essa conexão é feita com o protocolo TCP e está ociosa por seis segundos. Os sinalizadores de conexão indicam o estado atual dessa conexão. Mais informações sobre sinalizadores de conexão podem ser encontradas nos sinalizadores de conexão do ASA TCP.

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 gera syslogs durante a operação normal. Os syslogs variam na verbosidade com base na configuração de registro. A saída mostra dois syslogs que são vistos no nível seis, ou no nível **'informativo'**.

Neste exemplo, há dois syslogs gerados. A primeira é uma mensagem de registro que indica que o firewall criou uma **tradução**, especificamente uma PAT (dynamic TCP translation, tradução TCP dinâmica). Indica o endereço IP e a porta origem e o endereço IP e a porta convertidos à medida que o tráfego passa de dentro para fora.

O segundo syslog indica que o firewall criou uma **conexão** em sua tabela de conexão para esse tráfego específico entre o cliente e o servidor. Se o firewall tiver sido configurado para bloquear esta tentativa de conexão, ou se algum outro fator tiver inibido a criação dessa conexão (restrições de recursos ou um possível erro de configuração), o firewall não gerará um log que indique que a conexão foi criada. Em vez disso, registraria um motivo para a conexão ser negada ou uma indicação sobre qual fator inibiu a criação da conexão.

Conversões de 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 dessa configuração, o PAT é configurado para converter os endereços IP do host interno em endereços roteáveis na Internet. Para confirmar se essas traduções foram criadas, você pode verificar a tabela xlate (tradução). O comando **show xlate,** quando combinado com a palavra-chave **local** e o endereço IP do host interno, mostra todas as entradas presentes na tabela de tradução para esse host. A saída anterior mostra que há uma conversão atualmente criada para esse host entre as interfaces interna e externa. O IP e a porta do host interno são convertidos para o endereço 10.165.200.226 por nossa configuração. Os flags listados, r i , indicam que a tradução é **dinâmica** e um **mapa**. Mais informações sobre diferentes configurações

de NAT podem ser encontradas aqui: Informações sobre NAT.

Troubleshoot

O ASA oferece várias ferramentas para solucionar problemas de conectividade. Se o problema persistir após você verificar a configuração e verificar a saída listada anteriormente, essas ferramentas e técnicas podem ajudar a determinar a causa da falha de conectividade.

Packet Tracer

```
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 **packet tracer** no ASA permite especificar um pacote *simulado* e ver todas as várias etapas, verificações e funções pelas quais o firewall passa ao processar o tráfego. Com essa ferramenta, é útil identificar um exemplo de tráfego que você acredita que *deve* ter permissão para passar pelo firewall e usar esse 5 tuplas para simular o tráfego. No exemplo anterior, o packet tracer é usado para simular uma tentativa de conexão que atenda a estes critérios:

- O pacote simulado chega no **interior**.
- O protocolo usado é **TCP**.
- O endereço IP simulado do cliente é **10.1.1.154**.
- O cliente envia tráfego originado da porta **1234**.
- O tráfego é destinado a um servidor 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. Isso é feito pelo design do packet tracer. A ferramenta informa como o firewall processa esse tipo de tentativa de conexão, o que inclui como ele o rotearia e de qual interface. Mais informações sobre o packet tracer podem ser encontradas em pacotes de rastreamento com o Packet Tracer.

Captura

```
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 entra ou sai de suas interfaces. Essa funcionalidade de captura é fantástica porque pode provar definitivamente se o tráfego chega ou sai de um firewall. O exemplo anterior mostrou a configuração de duas capturas chamadas **capin** e **capout** nas interfaces interna e externa, respectivamente. Os comandos de captura usaram a palavra-chave **match**, que permite que você seja específico sobre o tráfego que deseja capturar.

Para a **capina** de captura**,** você indicou que queria corresponder o tráfego visto na interface interna (entrada ou saída) que corresponde ao **host tcp 10.1.1.154 198.51.100.100**. Em outras palavras, você deseja capturar qualquer tráfego TCP enviado do **host 10.1.1.154** para o **host 198.51.100.100** ou **vice-versa**. O uso da palavra-chave **match** permite que o firewall capture esse tráfego bidirecionalmente. O comando capture definido para a interface externa não faz referência ao endereço IP do cliente interno porque o firewall conduz PAT nesse endereço IP do cliente. Como resultado, você não pode **corresponder** a esse endereço IP do cliente. Em vez disso, este exemplo usa **qualquer** ordem para indicar que todos os possíveis endereços IP corresponderiam a essa condição.

Depois de configurar as capturas, você tentaria estabelecer uma conexão novamente e prosseguiria para exibir as capturas com o comando **show capture *<capture_name>***. Neste exemplo, você pode ver que o cliente conseguiu se conectar ao servidor como evidente pelo handshake triplo do TCP visto nas capturas.

Informações Relacionadas

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