Configurar o ASA para acesso ao servidor de e-mail SMTP em redes DMZ, internas e externas

Contents

Introduction

Este documento descreve como configurar um Cisco Adaptive Security Appliance (ASA) para acesso a um servidor SMTP (Simple Mail Transfer Protocol) localizado na zona desmilitarizada (DMZ), na rede interna ou na rede externa.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA com software versão 9.1 ou posterior
- Cisco 2800C Series Router com Cisco IOS® Software Release 15.1(4)M6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

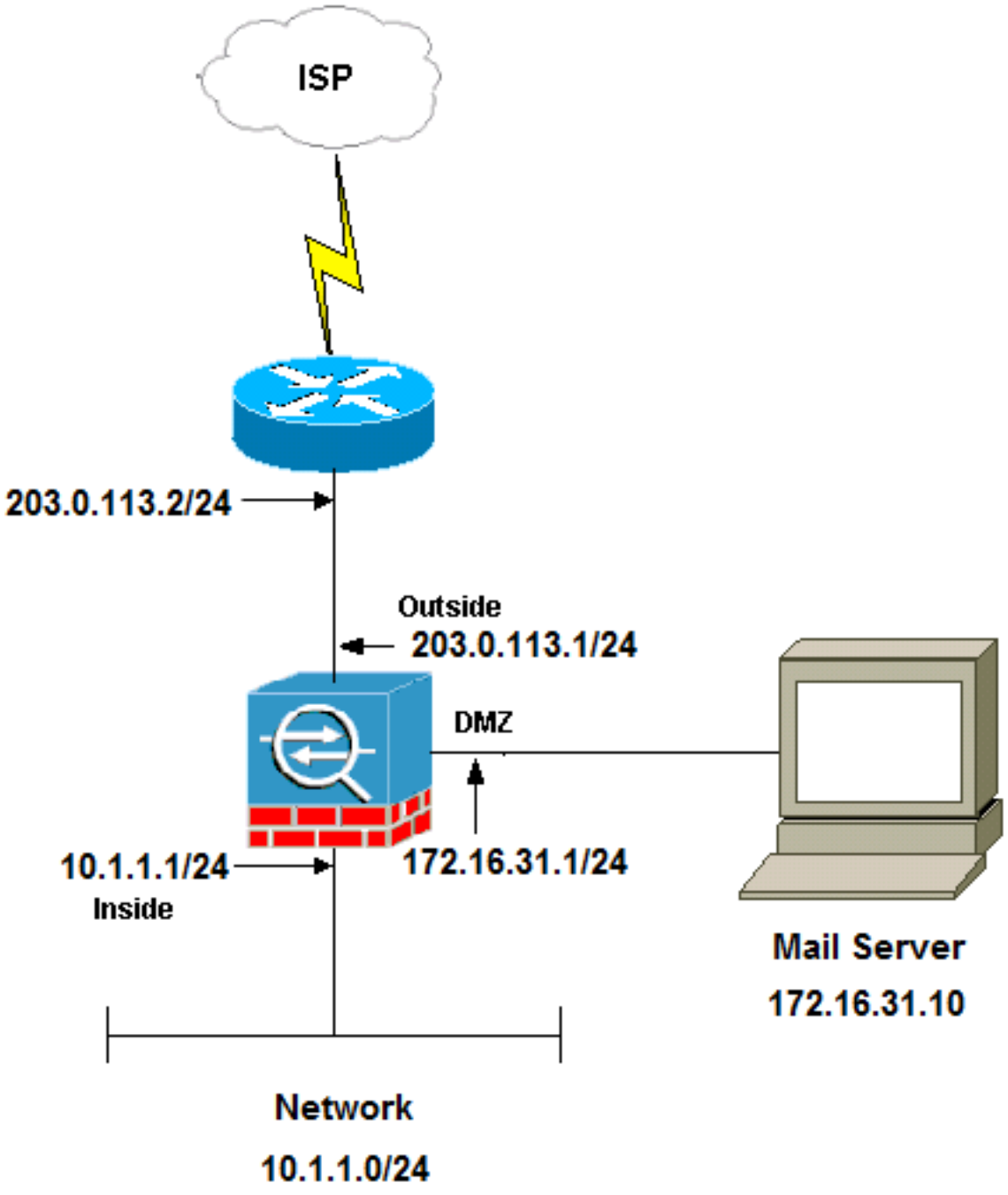
Esta seção descreve como configurar o ASA para acessar o servidor de e-mail na rede DMZ, na rede interna ou na rede externa.

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

Servidor de e-mail na rede DMZ

Diagrama de Rede

A configuração descrita nesta seção usa esta configuração de rede:



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

A configuração de rede usada neste exemplo tem o ASA com uma rede interna em **10.1.1.0/24** e uma rede externa em **203.0.113.0/24**. O servidor de e-mail com endereço IP **172.16.31.10** está

localizado na rede DMZ. Para que o servidor de e-mail seja acessado pela rede interna, você deve configurar a identidade Network Address Translation (NAT).

Para que os usuários externos acessem o servidor de e-mail, você deve configurar um NAT estático e uma lista de acesso, que é **outside_int** neste exemplo, para permitir que os usuários externos acessem o servidor de e-mail e vinculem a lista de acesso à interface externa.

Configuração do ASA

Esta é a configuração do ASA para este exemplo:

```
show run
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names

!--- Configure the dmz interface.

interface GigabitEthernet0/0
nameif dmz
security-level 50
ip address 172.16.31.1 255.255.255.0
!

!--- Configure the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0

!--- Configure inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa912-k8.bin
ftp mode passive

!--- This access list allows hosts to access
!--- IP address 172.16.31.10 for the SMTP port from outside.

access-list outside_int extended permit tcp any4 host 172.16.31.10 eq smtp
```

```
object network obj1-10.1.1.0
 subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- This network static does not use address translation.
!--- Inside hosts appear on the DMZ with their own addresses.

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
nat (inside,dmz) static obj-10.1.1.0

!--- This Auto-NAT uses address translation.
!--- Hosts that access the mail server from the outside
!--- use the 203.0.113.10 address.

object network obj-172.16.31.10
host 172.16.31.10
nat (dmz,outside) static 203.0.113.10

access-group outside_int in interface outside

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
timeout floating-conn 0:00:00
!
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

!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.

policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!

!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.
```

```
service-policy global_policy global
```

Configuração de TLS ESMTP

Se você usar a criptografia TLS (Transport Layer Security) para comunicação por e-mail, o recurso de inspeção ESMTP (Extended Simple Mail Transfer Protocol) (ativado por padrão) no ASA descartará os pacotes. Para permitir os e-mails com TLS ativado, desative o recurso de inspeção ESMTP como mostrado no próximo exemplo.

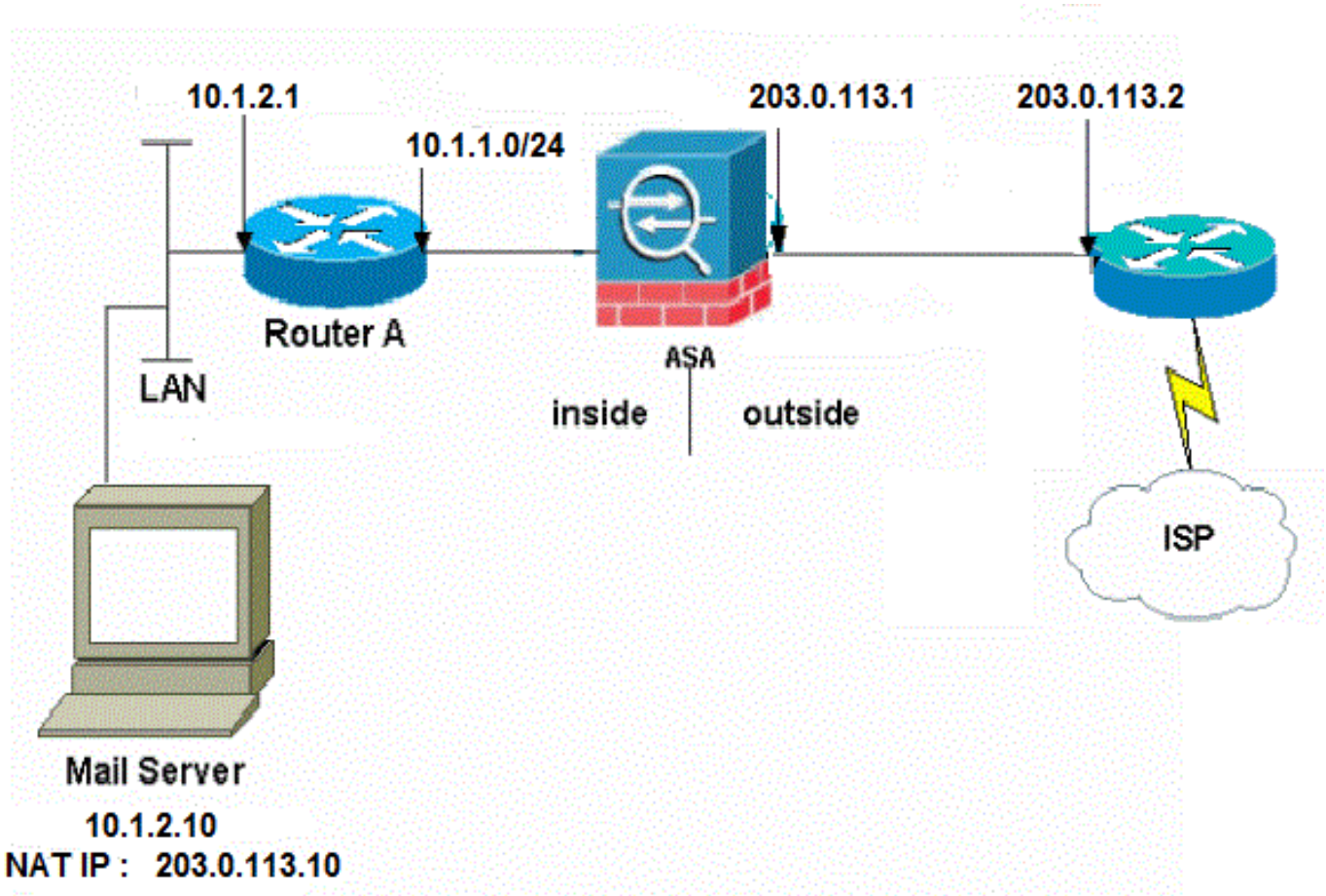
> **Note**: Consulte o bug da Cisco ID CSCtn08326 (somente clientes registrados) para obter mais informações.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

Servidor de e-mail na rede interna

Diagrama de Rede

A configuração descrita nesta seção usa esta configuração de rede:



A configuração de rede usada neste exemplo tem o ASA com uma rede interna em **10.1.1.0/24** e uma rede externa em **203.0.113.0/24**. O servidor de e-mail com o endereço IP **10.1.2.10** está localizado na rede interna.

Configuração do ASA

Esta é a configuração do ASA para este exemplo:

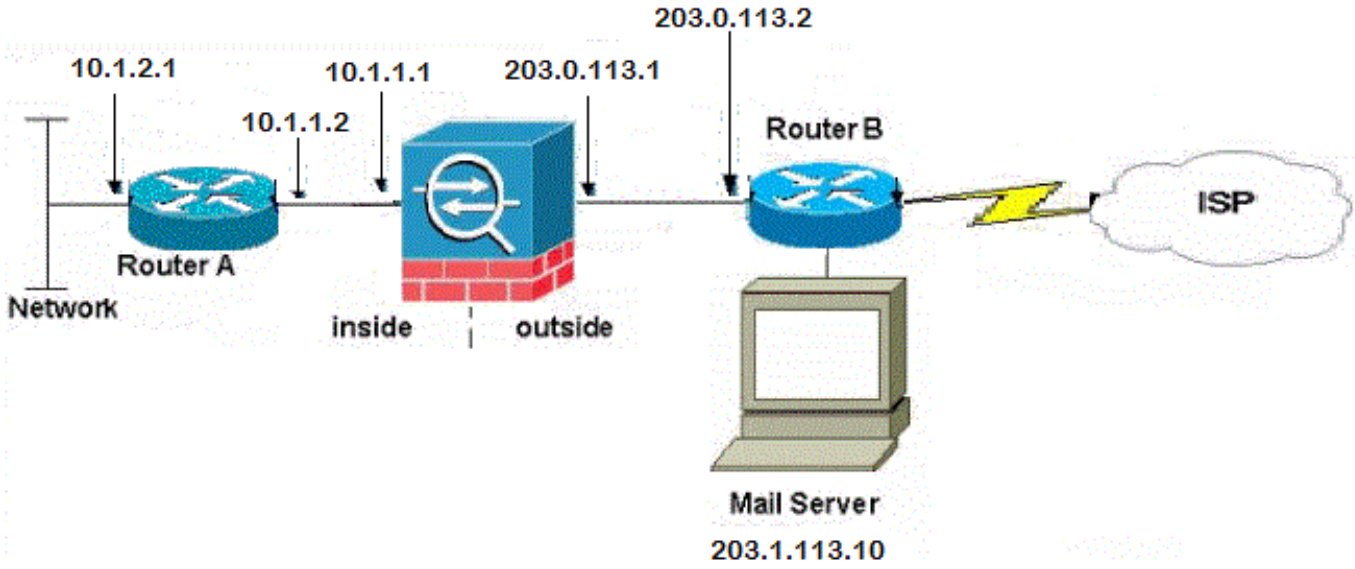
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- Define the IP address for the inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!--- Define the IP address for the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

!--- Create an access list that permits Simple
!--- Mail Transfer Protocol (SMTP) traffic from anywhere
!--- to the host at 203.0.113.10 (our server). The name of this list is
!--- smtp. Add additional lines to this access list as required.
!--- Note: There is one and only one access list allowed per
!--- interface per direction, for example, inbound on the outside interface.
!--- Because of limitation, any additional lines that need placement in
!--- the access list need to be specified here. If the server
!--- in question is not SMTP, replace the occurrences of SMTP with
!--- www, DNS, POP3, or whatever else is required.

access-list smtp extended permit tcp any host 10.1.2.10 eq smtp

--Omitted--

!--- Specify that any traffic that originates inside from the
!--- 10.1.2.x network NATs (PAT) to 203.0.113.9 if
!--- such traffic passes through the outside interface.

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic 203.0.113.9

!--- Define a static translation between 10.1.2.10 on the inside and
!--- 203.0.113.10 on the outside. These are the addresses to be used by
!--- the server located inside the ASA.
```

```
object network obj-10.1.2.10
host 10.1.2.10
nat (inside,outside) static 203.0.113.10

!--- Apply the access list named smtp inbound on the outside interface.

access-group smtp in interface outside

!--- Instruct the ASA to hand any traffic destined for 10.1.2.0
!--- to the router at 10.1.1.2.

route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

!--- Set the default route to 203.0.113.2.
!--- The ASA assumes that this address is a router address.

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1
```

Servidor de e-mail na rede externa

Diagrama de Rede

A configuração descrita nesta seção usa esta configuração de rede:



Configuração do ASA

Esta é a configuração do ASA para este exemplo:

```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!--- Define the IP address for the inside interface.
```

```
interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!--- Define the IP address for the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

!--- This command indicates that all addresses in the 10.1.2.x range
!--- that pass from the inside (GigabitEthernet0/2) to a corresponding global
!--- destination are done with dynamic PAT.
!--- As outbound traffic is permitted by default on the ASA, no
!--- static commands are needed.

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- Creates a static route for the 10.1.2.x network.
!--- The ASA forwards packets with these addresses to the router
!--- at 10.1.1.2
route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

!--- Sets the default route for the ASA Firewall at 203.0.113.2

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

--Omitted--

: end
```

Verificar

Use as informações fornecidas nesta seção para verificar se a configuração funciona corretamente.

Servidor de e-mail na rede DMZ

Ping de TCP

O ping TCP testa uma conexão sobre TCP (o padrão é Internet Control Message Protocol (ICMP)). Um ping TCP envia pacotes SYN e considera o ping bem-sucedido se o dispositivo destino enviar um pacote SYN-ACK. Você pode executar no máximo dois pings TCP simultâneos por vez.

Aqui está um exemplo:

```
ciscoasa(config)# ping tcp
```

```
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Conexão

O ASA é um Firewall stateful e o tráfego de retorno do servidor de e-mail é permitido pelo Firewall porque corresponde a uma conexão na tabela de conexão do Firewall. O tráfego que corresponde a uma conexão atual é permitido pelo Firewall sem ser bloqueado por uma ACL (Access Control List, lista de controle de acesso) de interface.

No próximo exemplo, o cliente na interface externa estabelece uma conexão com o host 203.0.113.10 da interface DMZ. Essa conexão é feita com o protocolo TCP e está ociosa por dois segundos. Os sinalizadores de conexão indicam o estado atual desta conexão:

```
ciscoasa(config)# show conn  address  172.16.31.10
1 in use, 2 most used
TCP outside  203.0.113.2:16678 dmz  172.16.31.10:25, idle 0:00:02, bytes 921, flags UIO
```

Registro

O Firewall ASA gera syslogs durante a operação normal. Os syslogs variam na verbosidade com base na configuração de registro. Esta saída mostra dois syslogs que aparecem no nível seis (o nível *informativo*) e no nível sete (o nível *de depuração*):

```
ciscoasa(config)# show logging  | i 172.16.31.10

%ASA-7-609001: Built local-host dmz:172.16.31.10

%ASA-6-302013: Built inbound TCP connection 11 for outside:203.0.113.2/16678
(203.0.113.2/16678) to dmz:172.16.31.10/25 (203.0.113.10/25)
```

O segundo syslog neste exemplo 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 ligação, ou se algum outro fator tiver inibido a criação desta ligação (restrições de recursos ou um possível erro de configuração), o Firewall não gerará um registro que indique que a ligação foi criada. Em vez disso, registraria um motivo para a conexão ser negada ou uma indicação sobre o fator que inibiu a criação da conexão.

Por exemplo, se a ACL externa não estiver configurada para permitir 172.16.31.10 na porta 25, você verá esse log quando o tráfego for negado:

%ASA-4-106100: access-list outside_int negado tcp outside/203.0.113.2(3756) -> dmz/172.16.31.10(25) hit-cnt 5 intervalo de 300 segundos

Isso ocorreria quando uma ACL está ausente ou configurada incorretamente como mostrado aqui:

```
access-list outside_int extended permit tcp any4 host 172.16.31.10 eq http

access-list outside_int extended deny ip any4 any4
```

Conversões de NAT (Xlate)

Para confirmar se as 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 que estão presentes na tabela de tradução para esse host. A próxima saída mostra que há uma conversão atualmente criada para esse host entre a DMZ e as interfaces externas. O endereço IP do servidor DMZ é convertido para o endereço 203.0.113.10 de acordo com a configuração anterior. Os sinalizadores listados (**s** neste exemplo) indicam que a conversão é *estática*.

```
ciscoasa(config)# show nat detail
Manual NAT Policies (Section 1)
1 (dmz) to (outside) source static obj-172.16.31.10 obj-203.0.113.10
   translate_hits = 7, untranslate_hits = 6
   Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static obj-172.16.31.10 203.0.113.10
   translate_hits = 1, untranslate_hits = 5
   Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:172.16.31.10 to outside:203.0.113.10
   flags s idle 0:10:48 timeout 0:00:00
NAT from inside:10.1.1.0/24 to dmz:10.1.1.0/24
   flags sI idle 79:56:17 timeout 0:00:00
NAT from dmz:172.16.31.10 to outside:203.0.113.10
   flags sT idle 0:01:02 timeout 0:00:00
NAT from outside:0.0.0.0/0 to dmz:0.0.0.0/0
   flags sIT idle 0:01:02 timeout 0:00:00
```

Servidor de e-mail na rede interna

Ping de TCP

Aqui está um exemplo de saída de ping TCP:

```
ciscoasa(config)# PING TCP
```

```
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Conexão

Aqui está um exemplo de verificação de conexão:

```
ciscoasa(config)# show conn  address  10.1.2.10
1 in use, 2 most used
TCP outside  203.0.113.2:5672 inside  10.1.2.10:25, idle 0:00:05, bytes 871, flags UIO
```

Registro

Aqui está um exemplo de syslog:

```
%ASA-6-302013: Built inbound TCP connection 553 for outside:203.0.113.2/19198
(203.0.113.2/19198) to inside:10.1.2.10/25 (203.0.113.10/25)
```

Conversões de NAT (Xlate)

Aqui estão alguns exemplos de saídas de comandos **show nat detail** e **show xlate**:

```
ciscoasa(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-10.1.2.10 203.0.113.10
   translate_hits = 0, untranslate_hits = 15
   Source - Origin: 10.1.2.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate

NAT from inside:10.1.2.10 to outside:203.0.113.10
   flags s idle 0:00:03 timeout 0:00:00
```

Servidor de e-mail na rede externa

Ping de TCP

Aqui está um exemplo de saída de ping TCP:

```
ciscoasa# PING TCP
Interface: inside
Target IP address: 203.1.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 10.1.2.10
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.1.113.10 port 25
from 10.1.2.10 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Conexão

Aqui está um exemplo de verificação de conexão:

```
ciscoasa# show conn address 203.1.113.10
1 in use, 2 most used
TCP inside 10.1.2.10:13539 outside 203.1.113.10:25, idle 0:00:02, bytes 898, flags UIO
```

Registro

Aqui está um exemplo de syslog:

```
ciscoasa# show logging | i 203.1.113.10

%ASA-6-302013: Built outbound TCP connection 590 for outside:203.1.113.10/25
(203.1.113.10/25) to inside:10.1.2.10/1234 (203.0.113.1/1234)
```

Conversões de NAT (Xlate)

Aqui está um exemplo de saída do comando **show xlate**:

```
ciscoasa# show xlate | i 10.1.2.10

TCP PAT from inside:10.1.2.10/1234 to outside:203.0.113.1/1234 flags ri idle
0:00:04 timeout 0:00:30
```

Troubleshoot

O ASA oferece várias ferramentas para solucionar problemas de conectividade. Se o problema persistir depois que você verificar a configuração e verificar as saídas descritas na seção anterior, essas ferramentas e técnicas podem ajudá-lo a determinar a causa da falha de conectividade.

Servidor de e-mail na rede DMZ

Packet Tracer

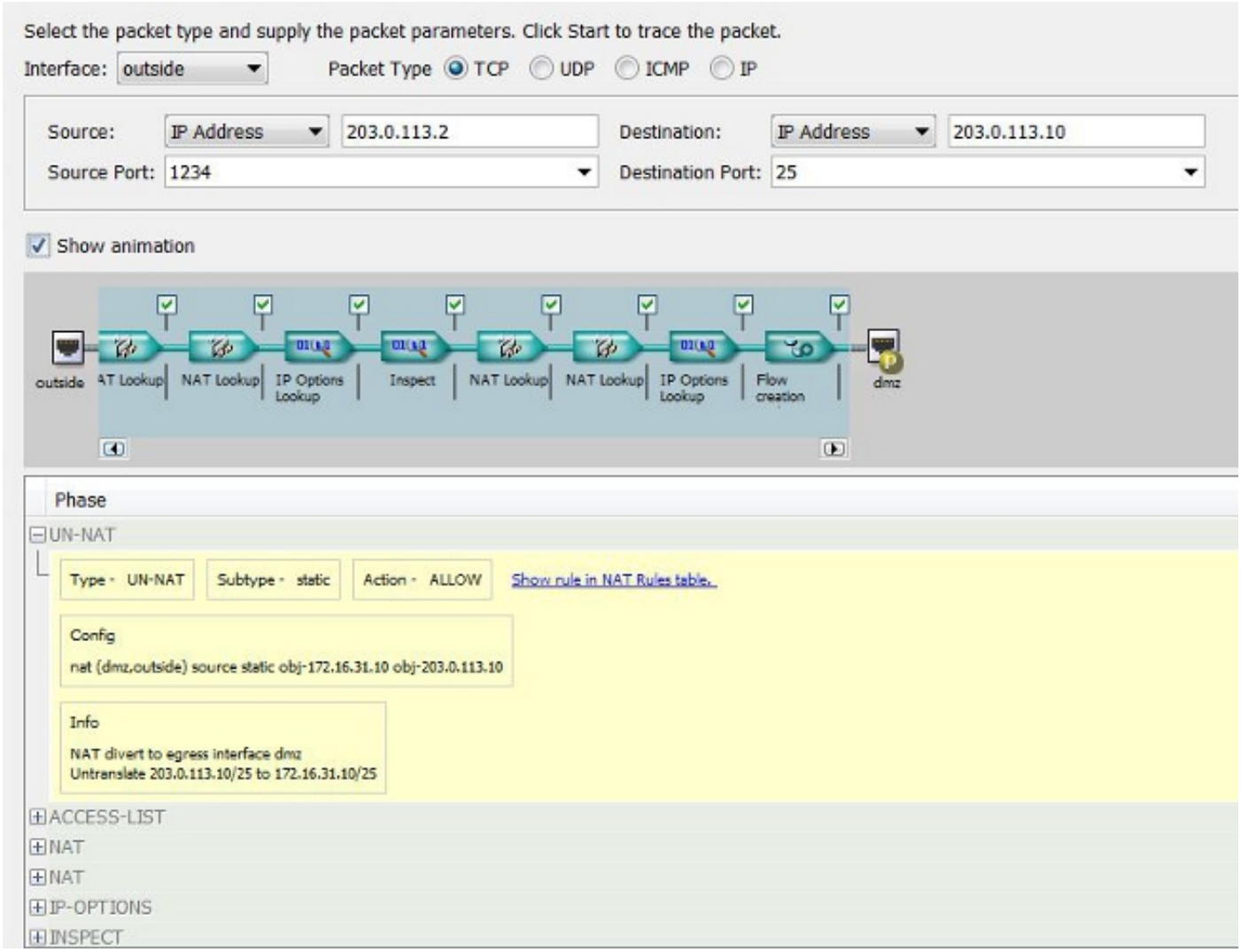
A funcionalidade packet tracer no ASA permite especificar um pacote *simulado* e visualizar todas as várias etapas, verificações e funções pelas quais o Firewall passa ao processar o tráfego. Com essa ferramenta, é útil identificar um exemplo de tráfego que você acredita que *deve* ter permissão para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

- O pacote simulado chega ao **exterior**.
- O protocolo usado é o **TCP**.
- O endereço IP do cliente simulado é **203.0.113.2**.
- O cliente envia tráfego originado da porta **1234**.
- O tráfego é destinado a um servidor no endereço IP **203.0.113.10**.
- O tráfego é destinado à porta **25**.

Aqui está um exemplo de saída do packet tracer:

```
packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.31.10 obj-203.0.113.10
Additional Information:
NAT divert to egress interface dmz
Untranslate 203.0.113.10/25 to 172.16.31.10/25

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

Aqui está um exemplo do Cisco Adaptive Security Device Manager (ASDM):



Observe que não há nenhuma menção da interface *DMZ* nas saídas anteriores. 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.

> **Tip**: Para obter informações adicionais sobre o recurso packet tracer, consulte a seção Tracing Packets with Packet Tracer do *Cisco ASA 5500 Series Configuration Guide usando CLI, 8.4 e 8.6*.

Captura do pacote

O firewall ASA pode capturar o tráfego que entra ou sai de suas interfaces. Essa funcionalidade de captura é muito útil porque pode provar definitivamente se o tráfego chega ou sai de um Firewall. O próximo exemplo mostra a configuração de duas capturas chamadas **capd** e **capout** nas interfaces DMZ e externa, respectivamente. Os comandos capture usam uma palavra-chave match, que permite que você seja específico sobre o tráfego que deseja capturar.

Para a **captura capd** neste exemplo, é indicado que você deseja corresponder ao tráfego visto na interface DMZ (entrada ou saída) que corresponde ao host TCP 172.16.31.10/host 203.0.113.2. Em outras palavras, você deseja capturar qualquer tráfego TCP enviado do host 172.16.31.10 para o host 203.0.113.2, ou vice-versa. O uso da palavra-chave match permite que o Firewall capture esse tráfego bidirecionalmente. O comando capture que é definido para a interface externa não faz referência ao endereço IP do servidor de email interno porque o Firewall conduz

um NAT nesse endereço IP do servidor de email. Como resultado, você não pode corresponder ao endereço IP desse servidor. Em vez disso, o próximo exemplo usa a palavra **any** para indicar que todos os possíveis endereços IP corresponderiam a essa condição.

Depois de configurar as capturas, você deve tentar estabelecer uma conexão novamente e continuar a visualizar as capturas com o comando **show capture_name>**. Neste exemplo, você pode ver que o host externo conseguiu se conectar ao servidor de e-mail, como evidente pelo handshake triplo do TCP visto nas capturas:

```
ASA#  capture capd interface dmz match tcp host 172.16.31.10 any
ASA#  capture capout interface outside match tcp any host 203.0.113.10

ASA#   show capture capd

3 packets captured

  1: 11:31:23.432655       203.0.113.2.65281 > 172.16.31.10.25: S 780523448:
  780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       172.16.31.10.25 > 203.0.113.2.65281: S 2123396067:
  2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       203.0.113.2.65281 > 172.16.31.10.25. ack 2123396068
  win 32768

ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.65281 > 203.0.113.10.25: S 1633080465:
  1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       203.0.113.10.25 > 203.0.113.2.65281: S 95714629:
  95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914        203.0.113.2.65281 > 203.0.113.10.25: . ack 95714630
  win 32768
```

Servidor de e-mail na rede interna

Packet Tracer

Aqui está um exemplo de saída do packet tracer:

```
CLI : packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.1.2.10
 nat (inside,outside) static 203.0.113.10
Additional Information:
NAT divert to egress interface inside
Untranslate 203.0.113.10/25 to 10.1.2.10/25

Phase: 3
```

```
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group smtp in interface outside
access-list smtp extended permit tcp any4 host 10.1.2.10 eq smtp
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x77dd2c50, priority=13, domain=permit, deny=false
       hits=1, user_data=0x735dc880, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
       src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
       dst ip/id=10.1.2.10, mask=255.255.255.255, port=25, tag=0, dscp=0x0
       input_ifc=outside, output_ifc=any
```

Servidor de e-mail na rede externa

Packet Tracer

Aqui está um exemplo de saída do packet tracer:

```
CLI :  packet-tracer input inside tcp 10.1.2.10 1234 203.1.113.10 25 detailed

--Omitted--

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 203.1.113.0 255.255.255.0 outside

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.1.2.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.1.2.10/1234 to 203.0.113.1/1234
Forward Flow based lookup yields rule:
in id=0x778b14a8, priority=6, domain=nat, deny=false
hits=11, user_data=0x778b0f48, cs_id=0x0, flags=0x0, protocol=0
src ip/id=10.1.2.0, mask=255.255.255.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=inside, output_ifc=outside
```

Informações Relacionadas

- Mensagens de syslog do Cisco ASA Series
- Exemplo de captura de pacote ASA com CLI e configuração ASDM
- Guia de configuração da CLI do Cisco ASA Series, 9.0 - Configurando NAT de objeto de rede
- Suporte técnico e documentação - Cisco Systems