ASA 8.3 e mais atrasado: Acesso de servidor do correio (S TP) no exemplo da configuração DMZ

Índice

Introdução

Esta configuração de exemplo demonstra como estabelecer a ferramenta de segurança ASA para o acesso a um server do Simple Mail Transfer Protocol (SMTP) situado na rede da zona desmilitarizada (DMZ).

Refira ASA 8.3 e mais atrasado: Envie o acesso de servidor (S TP) no exemplo de configuração da rede interna para obter mais informações sobre de como estabelecer a ferramenta de segurança ASA para o acesso a um server mail/SMTP situado na rede interna.

Refira ASA 8.3 e mais atrasado: Envie o acesso de servidor (S TP) no exemplo de configuração da rede externa para obter mais informações sobre de como estabelecer a ferramenta de segurança ASA para o acesso a um server mail/SMTP situado na rede externa.

Refira PIX/ASA 7.x e acima: Envie o acesso de servidor (S TP) no exemplo da configuração DMZ para a configuração idêntica na ferramenta de segurança adaptável de Cisco (ASA) com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- A ferramenta de segurança adaptável de Cisco (ASA) essa executa a versão 8.3 e mais recente.
- Cisco 1841 Router com liberação 12.4(20)T do Cisco IOS ® Software

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.

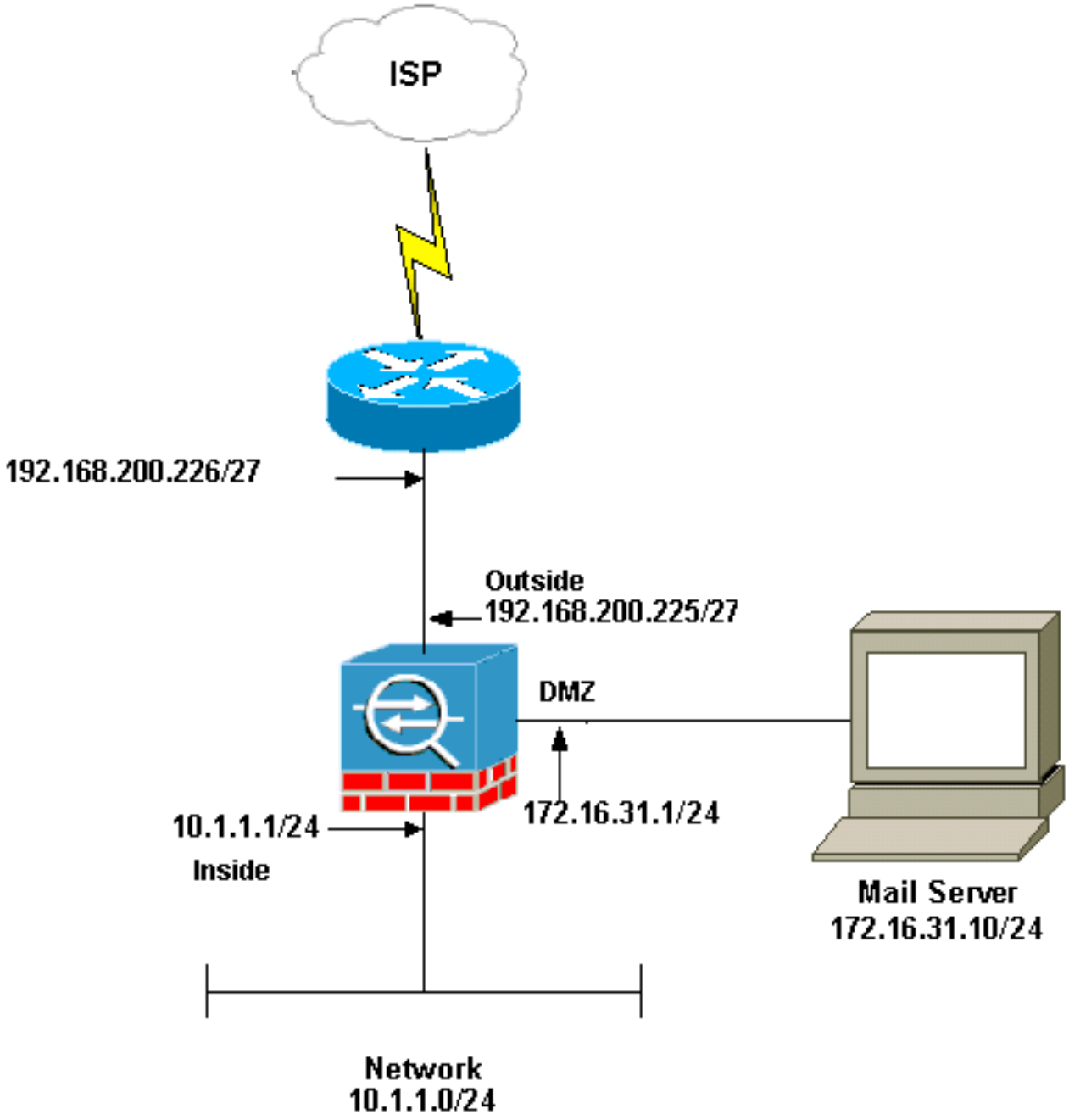
Configurar

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

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

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.

A instalação de rede usada neste exemplo tem o ASA com rede interna (10.1.1.0/24) e a rede externa (192.168.200.0/27). O mail server com endereço IP 172.16.31.10 é ficado situado na rede da zona desmilitarizada (DMZ). Para que o mail server seja alcançado pelo interior, os usuários configuram a identidade NAT. Configurar uma lista de acessos, que seja **dmz_int** neste exemplo, a fim permitir as conexões SMTP que parte do mail server aos anfitriões na rede interna e ligá-las à relação DMZ.

Similarmente para que os usuários externos alcancem o mail server configurar um NAT estático e uma lista de acessos, que seja **outside_int** neste exemplo, a fim permitir usuários externos alcançar o mail server e ligar igualmente esta lista de acessos à interface externa.

Configuração ASA

Este documento utiliza esta configuração:

Configuração ASA

```
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0
shutdown no nameif security-level 0 no ip address !
interface Ethernet1 shutdown no nameif no security-level
no ip address ! interface Ethernet2 no nameif no
security-level no ip address ! !--- Configure the inside
interface. interface Ethernet3 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! !---
Configure the outside interface. interface Ethernet4
nameif outside security-level 0 ip address
192.168.200.225 255.255.255.224 ! !--- Configure dmz
interface. interface Ethernet5 nameif dmz security-level
10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host 192.168.200.227 eq smtp !--- Allows outgoing
SMTP connections. !--- This access list allows host IP
172.16.31.10 !--- sourcing the SMTP port to access any
host. access-list dmz_int extended permit tcp host
172.16.31.10 eq smtp any pager lines 24 mtu BB 1500 mtu
inside 1500 mtu outside 1500 mtu dmz 1500 no failover no
asdm history enable arp timeout 14400 object network
obj-192.168.200.228-192.168.200.253 range
192.168.200.228-192.168.200.253 object network obj-
192.168.200.254 host 192.168.200.254 object-group
network nat-pat-group network-object object obj-
192.168.200.228-192.168.200.253 network-object object
obj-192.168.200.254 object network obj-10.1.1.0 subnet
10.1.1.0 255.255.255.0 nat (inside,outside) dynamic nat-
pat-group !--- 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 network static uses address
translation. !--- Hosts that access the mail server from
the outside !--- use the 192.168.200.227 address. object
network obj-172.16.31.10 host 172.16.31.10 nat
(dmz,outside) static 192.168.200.227 access-group
outside_int in interface outside access-group dmz_int in
interface dmz route outside 0.0.0.0 0.0.0.0
192.168.200.226 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 timeout uauth 0:05:00 absolute no snmp-server
location no snmp-server contact telnet timeout 5 ssh
timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
!--- 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
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda : end
[OK]
```

Configuração ESMTP TLS

Nota: Se você usa a criptografia do Transport Layer Security (TLS) para uma comunicação do email então a característica da inspeção de ESMTP (permitida à revelia) no ASA deixa cair os pacotes. A fim permitir os email com o TLS permitido, desabilite a característica da inspeção de ESMTP como esta saída mostra. Refira a identificação de bug Cisco CSCtn08326 (clientes registrados somente) para mais informação.

```
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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

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

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- debugar o traço ICMP — Mostra se os pedidos do Internet Control Message Protocol (ICMP) dos anfitriões alcançam o ASA. Você precisa de adicionar o **comando access-list** a fim permitir o ICMP em sua configuração a fim executar este debuga.**Nota:** A fim usar isto debugar-lo, certifique-se de permitir o ICMP no `outside_int da lista de acesso` como esta saída mostra:`access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp`
  `access-list outside_int extended permit icmp any any`
- 7 protegido de registro — Usado no modo de configuração global para permitir a ferramenta de segurança adaptável de enviar mensagens do syslog ao buffer de registro. Os índices do buffer de registro ASA podem ser considerados com o comando show logging.

Consulte para configurar o Syslog usando o ASDM para obter mais informações sobre de como estabelecer o registro.

Informações Relacionadas

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