ASA 8.3 y posterior: Ejemplo de Acceso al Servidor de Correo (SMTP) en la Configuración de DMZ

Contenido

Introducción

Esta configuración de ejemplo muestra cómo configurar el dispositivo de seguridad ASA para acceder a un servidor SMTP (protocolo simple de transferencia de correo) ubicado en la red de zona desmilitarizada (DMZ).

Consulte ASA 8.3 y posteriores: Ejemplo de Configuración de Acceso de Servidor de Correo (SMTP) en Red Interna para obtener más información sobre cómo configurar el Dispositivo de Seguridad ASA para acceder a un servidor de correo/SMTP ubicado en la red interna.

Consulte ASA 8.3 y posteriores: Ejemplo de Configuración de Acceso de Servidor de Correo (SMTP) en Red Externa para obtener más información sobre cómo configurar ASA Security Appliance para acceder a un servidor de correo/SMTP ubicado en la red Externa.

Consulte PIX/ASA 7.x y versiones posteriores: Acceso al servidor de correo (SMTP) en el ejemplo de configuración de DMZ para la configuración idéntica en Cisco Adaptive Security Appliance (ASA) con las versiones 8.2 y anteriores.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adaptive Security Appliance (ASA) que ejecuta la versión 8.3 y posteriores.
- Router Cisco 1841 con software Cisco IOS® versión 12.4(20)T

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

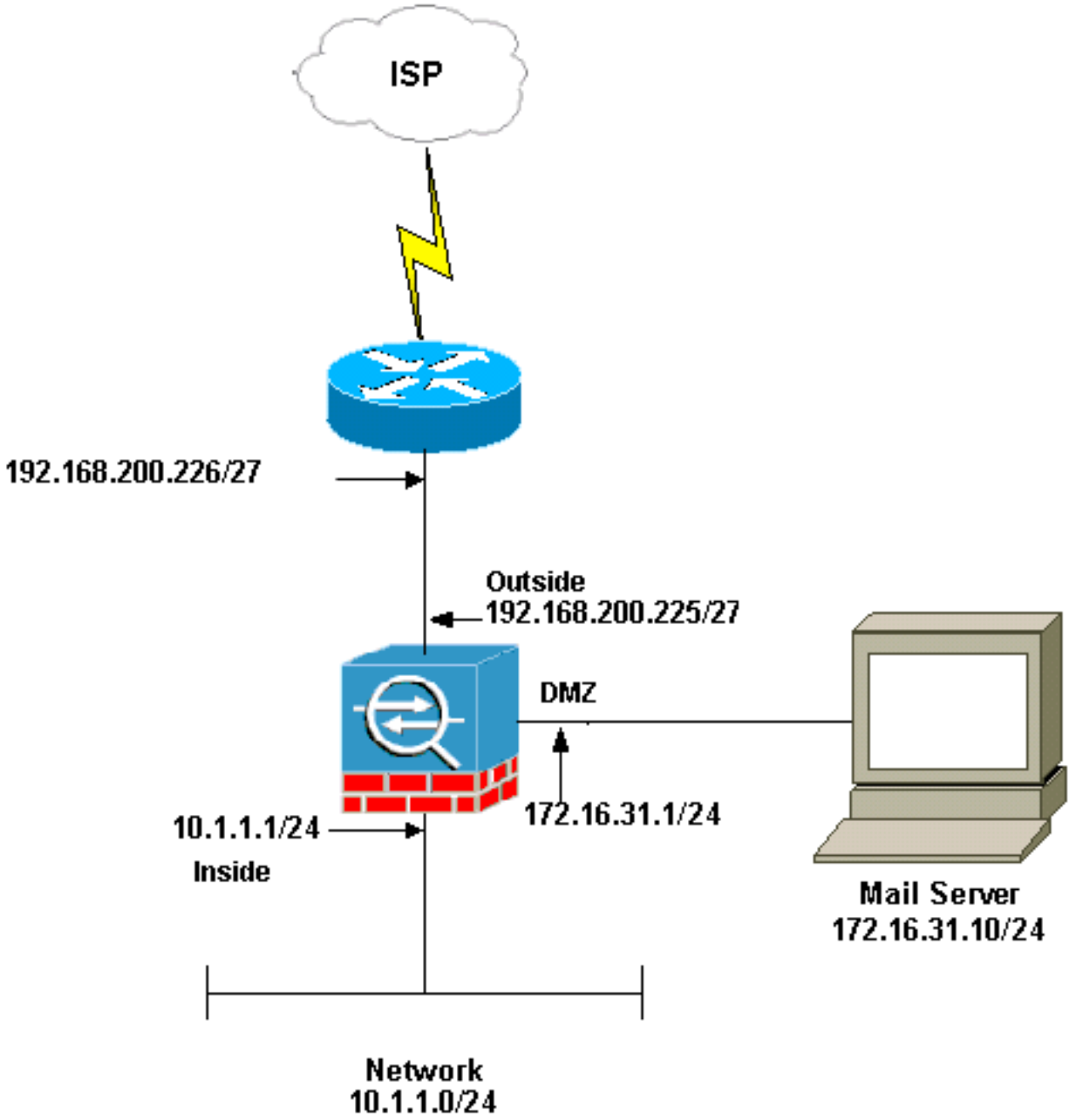
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

La configuración de red utilizada en este ejemplo tiene el ASA con la red interna (10.1.1.0/24) y la red externa (192.168.200.0/27). El servidor de correo con la dirección IP 172.16.31.10 se encuentra en la red de zona desmilitarizada (DMZ). Para que el servidor de correo sea accedido por el interior, los usuarios configuran la identidad NAT. Configure una lista de acceso, que es **dmz_int** en este ejemplo, para permitir las conexiones SMTP salientes del Mailserver a los hosts de la red interna y enlazarlo a la interfaz DMZ.

De manera similar para que los usuarios externos accedan al servidor de correo configure una NAT estática y también una lista de acceso, que es **outside_int** en este ejemplo, para permitir que los usuarios externos accedan al servidor de correo y enlacen esta lista de acceso a la interfaz exterior.

Configuración ASA

Este documento usa esta configuración:

Configuración 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]
```

Configuración de ESMTP TLS

Nota: Si utiliza el cifrado de seguridad de la capa de transporte (TLS) para la comunicación por correo electrónico, la función de inspección de ESMTP (activada de forma predeterminada) en el ASA descarta los paquetes. Para permitir los correos electrónicos con TLS habilitado, inhabilite la función de inspección ESMTP como muestra este resultado. Consulte Cisco bug ID CSCtn08326 (sólo clientes registrados) para obtener más información.

```
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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- debug icmp trace : muestra si las solicitudes del protocolo de mensajes de control de Internet (ICMP) de los hosts llegan al ASA. Debe agregar el comando **access-list** para permitir el ICMP en su configuración para ejecutar este debug.**Nota:** Para utilizar este debug, asegúrese de permitir ICMP en la `lista de acceso outside_int` como muestra este resultado:
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- logging buffered 7 —Se utiliza en el modo de configuración global para permitir que el dispositivo de seguridad adaptable envíe mensajes syslog al búfer de registro. El contenido del buffer de registro ASA se puede ver con el comando show logging.

Consulte Configuración de Syslog con ASDM para obtener más información sobre cómo configurar el registro.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems