ASA 8. 3 и позже: почта (SMTP) доступ сервера на примере конфигурации DMZ

Содержание

Введение

Этот пример конфигурации демонстрирует, как установить Устройство обеспечения безопасности ASA для доступа к серверу Протокола SMTP, расположенному в сети Demilitarized Zone (DMZ).

См. ASA 8.3 и Позже: Почта (SMTP) Доступ сервера на Примере конфигурации Внутренней сети для получения дополнительной информации о том, как установить Устройство обеспечения безопасности ASA для доступа к ПОЧТЕ/СЕРВЕРУ SMTP, расположилась на Внутренней сети.

См. ASA 8.3 и Позже: Почта (SMTP) Доступ сервера на Примере конфигурации Внешней сети для получения дополнительной информации о том, как установить Устройство обеспечения безопасности ASA для доступа к ПОЧТЕ/СЕРВЕРУ SMTP, расположилась на Внешней сети.

Дополнительные сведения о порядке настройки многоконтекстной конфигурации в устройствах защиты см. в документе PIX/ASA версий 7.x и выше: Почта (SMTP) Доступ сервера на Примере Конфигурации DMZ для одинаковой конфигурации на устройстве адаптивной защиты Cisco (ASA) с версиями 8.2 и ранее.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство адаптивной защиты Cisco (ASA), который выполняет версию 8.3 и позже.
- Маршрутизатор Cisco 1841 с выпуском 12.4 (20) T программного обеспечения Cisco IOS

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

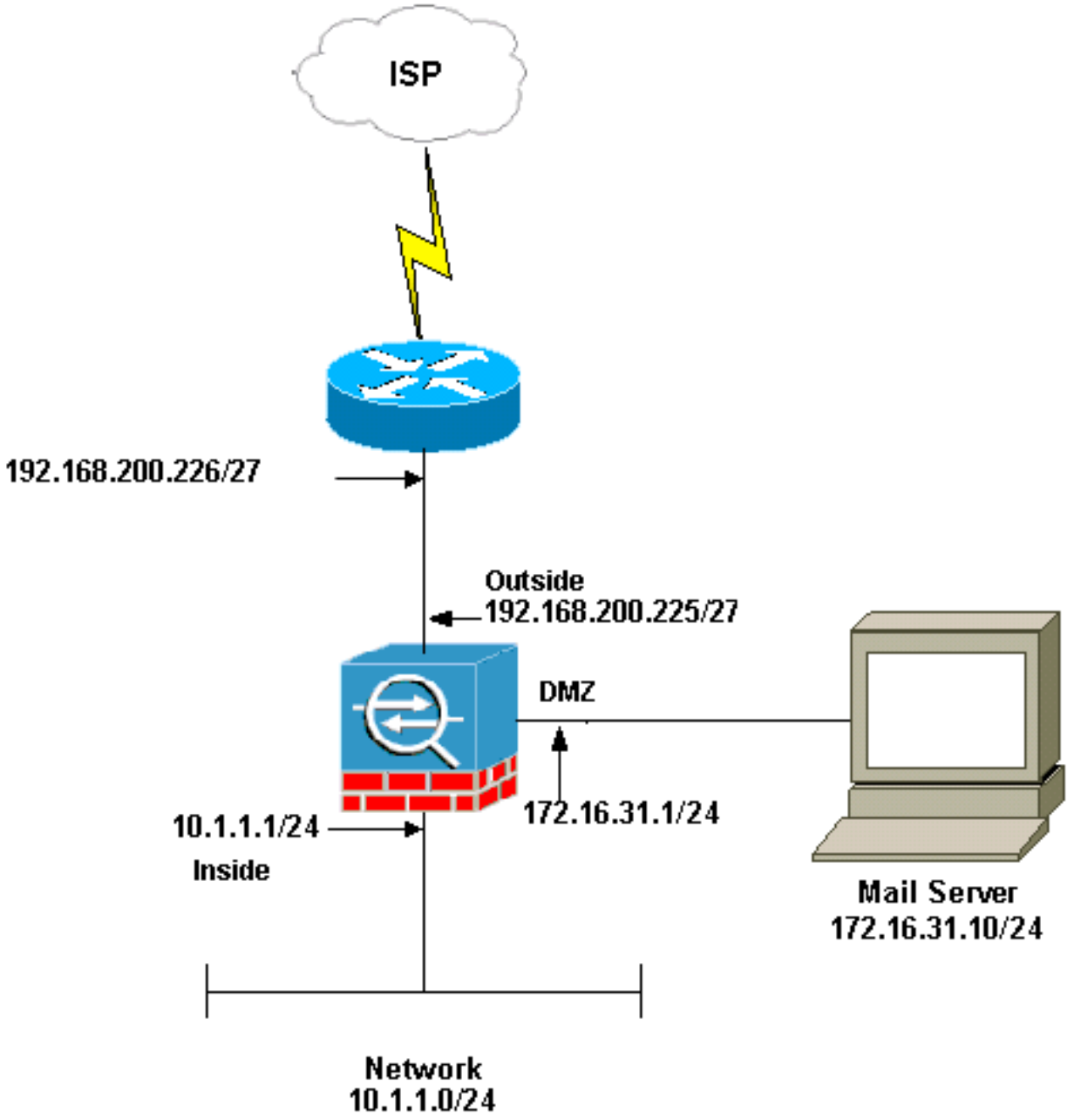
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Сетевая установка, используемая в данном примере, имеет ASA с внутренней сетью (10.1.1.0/24) и внешняя сеть (192.168.200.0/27). Почтовый сервер с IP-адресом 172.16.31.10 расположен в сети Demilitarized Zone (DMZ). Для Mailserver, к которому обратится внутренняя часть, пользователи настраивают идентичность NAT. Настройте список доступа, который является **dmz_int** в данном примере, чтобы позволить исходящие соединения SMTP от Mailserver до хостов во внутренней сети и связать его с интерфейсом DMZ.

Так же для внешних пользователей для доступа к Mailserver настраивают статическое NAT и также список доступа, который является **outside_int** в данном примере, чтобы разрешить внешним пользователям обращаться к Mailserver и связывать этот список доступа с внешним интерфейсом.

Конфигурация ASA

В данном документе используется следующая конфигурация:

Конфигурация 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]
```

Конфигурация ESMTP TLS

Примечание: При использовании шифрование Transport Layer Security (TLS) для переписки по электронной почте тогда функция проверки ESMTP (включил по умолчанию) в отбрасываниях ASA пакеты. Чтобы разрешить передачу электронных сообщения при включенном TLS, отключите функцию проверки ESMTP, как показано ниже. См. идентификатор ошибки Cisco CSCtn08326 (только зарегистрированные клиенты) для получения дополнительной информации.

```
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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- debug icmp trace — Показывает, достигают ли запросы протокола управляющих сообщений интернета (ICMP) от хостов ASA. Необходимо добавить **команду access-list** для разрешения ICMP в конфигурации для выполнения этой отладки.**Примечание:** Для использования этой отладки удостоверьтесь, что вы позволяете ICMP в `access-list outside_int` как показано в выходных данных ниже:`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 — Используемый в режиме глобальной конфигурации, чтобы позволить устройству адаптивной безопасности передать сообщения системного журнала к буферу журнала. Содержание буфера журнала ASA может быть замечено с командой show logging.

См. Настраивают Системный журнал с помощью ASDM для получения дополнительной информации о том, как установить регистрацию.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация