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

Содержание

Введение

Этот пример конфигурации показывает способ установки устройства защиты ASA для доступа к почтовому серверу (SMTP), расположенному во внутренней сети.

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

См. ASA 8.3 и Позже: Почта (SMTP) Доступ сервера на Конфигурации Внешней сети Exampleto установила Устройство обеспечения безопасности ASA для доступа к ПОЧТЕ/СЕРВЕРУ SMTP, расположенной на Внешней сети.

См. PIX/ASA 7.x и позже: Почта (SMTP) Доступ сервера на Примере конфигурации Внутренней сети для получения дополнительной информации 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.

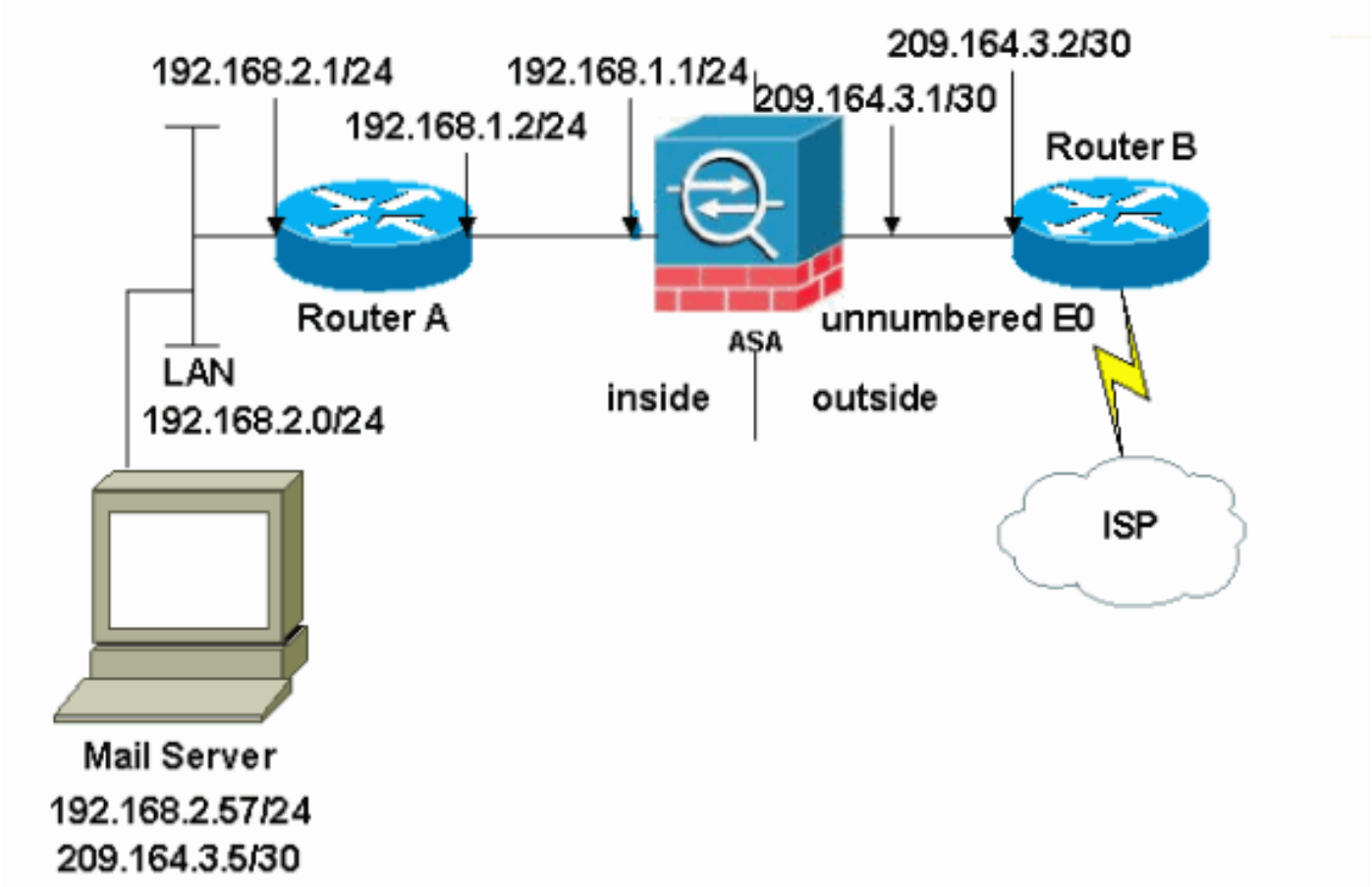
Настройка

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 (192.168.1.0/24) и внешняя сеть (209.164.3.0/30). Почтовый сервер с IP-адресом 209.64.3.5 расположен во внутренней сети.

Конфигурации

Эти конфигурации используются в данном документе:

- ASA
- Маршрутизатор B

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 no security-level no ip address !
interface Ethernet1 shutdown no nameif no security-level
no ip address ! interface Ethernet2 shutdown no nameif
no security-level no ip address ! !--- Define the IP
address for the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 192.168.1.1
255.255.255.0 ! !--- Define the IP address for the
outside interface. interface Ethernet4 nameif outside
security-level 0 ip address 209.164.3.1 255.255.255.252
! interface Ethernet5 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
```

```
ftp mode passive !--- Create an access list that permits
Simple !--- Mail Transfer Protocol (SMTP) traffic from
anywhere !--- to the host at 209.164.3.5 (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 209.164.3.5 eq smtp
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover no asdm history enable arp timeout 14400 !---
Specify that any traffic that originates inside from the
!--- 192.168.2.x network NATs (PAT) to 209.164.3.129 if
!--- such traffic passes through the outside interface.
object network obj-192.168.2.0 subnet 192.168.2.0
255.255.255.0 nat (inside,outside) dynamic 209.164.3.129
!--- Define a static translation between 192.168.2.57 on
the inside and !--- 209.164.3.5 on the outside. These
are the addresses to be used by !--- the server located
inside the ASA. object network obj-192.168.2.57 host
192.168.2.57 nat (inside,outside) static 209.164.3.5 !--
- 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 192.168.x.x !--- to the router at
192.168.1.2. route inside 192.168.0.0 255.255.0.0
192.168.1.2 1 !--- Set the default route to 209.164.3.2.
!--- The ASA assumes that this address is a router
address. route outside 0.0.0.0 0.0.0.0 209.164.3.2 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 snmp-server enable traps snmp authentication
linkup linkdown coldstart telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! !--- SMTP/ESMTP is
inspected as "inspect esmtp" is included in the map.
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 !
!--- SMTP/ESMTP is inspected as "inspect esmtp" is
included in the map. service-policy global_policy global
Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

Маршрутизатор B

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname 2522-R5
 !
 enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
 !
```

```
 ip subnet-zero
 !
 !
 !
 !
 !
 interface Ethernet0

!--- Sets the IP address of the Ethernet interface to
209.164.3.2. ip address 209.164.3.2 255.255.255.252 !
interface Serial0 !--- Instructs the serial interface to
use !--- the address of the Ethernet interface when the
need arises. ip unnumbered ethernet 0 ! interface
Serial1 no ip address no ip directed-broadcast ! ip
classless !--- Instructs the router to send all traffic
!--- destined for 209.164.3.x to 209.164.3.1. ip route
209.164.3.0 255.255.255.0 209.164.3.1 !--- Instructs the
router to send !--- all other remote traffic out serial
0. ip route 0.0.0.0 0.0.0.0 serial 0 ! ! line con 0
transport input none line aux 0 autoselect during-login
line vty 0 4 exec-timeout 5 0 password ww login ! end
```

Примечание: Конфигурация маршрутизатора A не добавлена. Только необходимо дать IP-адреса на интерфейсах и установить шлюз по умолчанию в 192.168.1.1, который является внутренним интерфейсом ASA.

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
```

Примечание: В версии ASA 8.0.3 и позже, **команда allow-tls** доступна для разрешения электронной почты TLS с осмотрите esmtp, включенным как показано:

```
policy-map type inspect esmtp tls-esmtp
parameters
allow-tls
inspect esmtp tls-esmtp
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Logging buffered 7 команд направляет сообщения к консоли ASA. Если подключение к

почтовому серверу является проблемой, исследуйте консольные сообщения отладки для определения местоположения IP-адресов посылающих и принимающих станций для определения проблемы.

Дополнительные сведения

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