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

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Настройка
Схема сети
Конфигурации
Конфигурация ESMTP TLS
Проверка
Устранение неполадок
Дополнительные сведения

Введение

Этот пример конфигурации предоставляет сведения о том, как установить Устройство адаптивной защиты (ASA) для доступа к почтовому серверу, расположенному на внешней 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 Примере конфигурации Внутренней сети для устанавливания Устройства обеспечения безопасности ASA для доступа к ПОЧТЕ/СЕРВЕРУ SMTP расположилась на Внутренней сети.

См. PIX/ASA 7.x и позже: Почта (SMTP) Доступ сервера на Примере конфигурации Внешней сети 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.

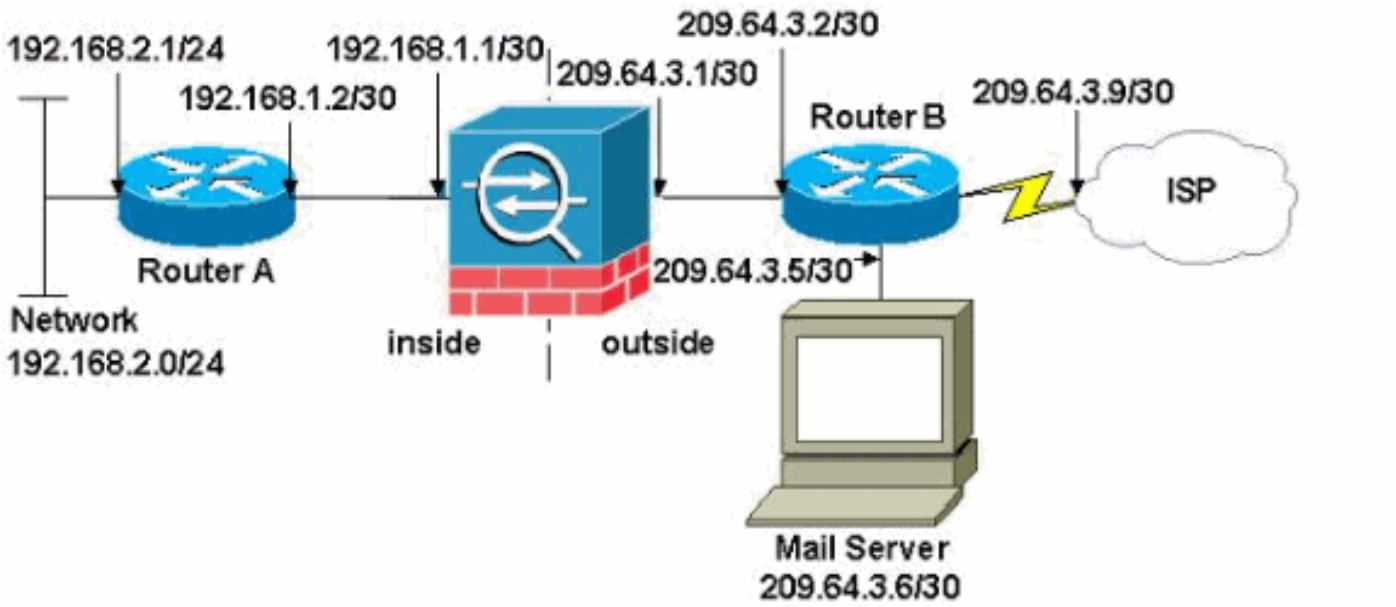
Настройка

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 (192.168.1.0/30) и внешняя сеть (209.64.3.0/30). Почтовый сервер с IP-адресом 209.64.3.6 расположен во внешней сети. Настройте Выражение NAT так, чтобы любой трафик от 192.168.2.x сеть, которая проходит от внутреннего интерфейса (Ethernet0) к внешнему интерфейсу (Ethernet 1), преобразовал в адрес в диапазоне от 209.64.3.129 до 209.64.3.253. Последний доступный адрес (209.64.3.254) зарезервирован для Преобразования адресов портов (PAT).

Конфигурации

Эти конфигурации используются в данном документе:

- ASA
- Маршрутизатор A
- 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 ! !--- Configure the
inside interface. ? interface Ethernet3 nameif inside
security-level 100 ip address 192.168.1.1
255.255.255.252 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 209.64.3.1 255.255.255.252 ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa831-k8.bin ftp mode passive pager lines 24 mtu
inside 1500 mtu outside 1500 no failover no asdm history
enable arp timeout 14400 !--- This command states that
any traffic !--- from the 192.168.2.x network that
passes from the inside interface (Ethernet0) !--- to the
outside interface (Ethernet 1) translates into an
address !--- in the range of 209.64.3.129 through
209.64.3.253 and contains a subnet !--- mask of
255.255.255.128. object network obj-
209.64.3.129_209.64.3.253 range 209.64.3.129-
209.64.3.253 !--- This command reserves the last
available address (209.64.3.254) for !--- for Port
Address Translation (PAT). In the previous statement, !-
-- each address inside that requests a connection uses
one !--- of the addresses specified. If all of these
addresses are in use, !--- this statement provides a
failsafe to allow additional inside stations !--- to
establish connections. object network obj-209.64.3.254
host 209.64.3.254 !--- This command indicates that all
addresses in the 192.168.2.x range !--- that pass from
the inside (Ethernet0) to a corresponding global !---
designation are done with NAT. !--- As outbound traffic
is permitted by default on the ASA, no !--- static
commands are needed. object-group network nat-pat-group
network-object object obj-209.64.3.129_209.64.3.253
network-object object obj-209.64.3.254 object network
obj-192.168.2.0 subnet 192.168.2.0 255.255.255.0 nat
(inside,outside) dynamic nat-pat-group !--- Creates a
```

```
static route for the 192.168.2.x network with
192.168.1.2. !--- The ASA forwards packets with these
addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1 !--- Sets
the default route for the ASA Firewall at 209.64.3.2.
route outside 0.0.0.0 0.0.0.0 209.64.3.2 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
since "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 rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp ! service-
policy global_policy global
Cryptochecksum:8a63de5ae2643c541a397c2de7901041 : end
```

Маршрутизатор A

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1 ! ! line con 0 transport input none line aux
0 autoselect during-login line vty 0 4 exec-timeout 5 0
password ww login ! end
```

Маршрутизатор B

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
```

```
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the ASA-facing Ethernet
interface. ip address 209.64.3.2 255.255.255.252 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the server-facing Ethernet interface. ip
address 209.64.3.5 255.255.255.252 no ip directed-
broadcast ! interface Serial0 !--- Assigns an IP address
to the Internet-facing interface. ip address 209.64.3.9
255.255.255.252 no ip directed-broadcast no ip mroute-
cache ! interface Serial1 no ip address no ip directed-
broadcast ! ip classless !--- All non-local packets are
to be sent out serial 0. In this case, !--- the IP
address on the other end of the serial interface is not
known, !--- or you can specify it here. ip route 0.0.0.0
0.0.0.0 serial 0 ! !--- This statement is required to
direct traffic destined to the !--- 209.64.3.128 network
(the ASA global pool) to the ASA to be translated !---
back to the inside addresses. ip route 209.64.3.128
255.255.255.128 209.64.3.1 ! ! line con 0 transport
input none line aux 0 autoselect during-login line vty 0
4 exec-timeout 5 0 password ww login ! end
```

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

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