PIX/ASA 7.x: доступ к почтовому серверу на примере конфигурации DMZ

Содержание

Введение

Этот пример конфигурации показывает, как настроить брандмауэр PIX для доступа к почтовому серверу, расположенному в сети с демилитаризованной зоной DMZ.

Примечание: См. дополнительные сведения об установке Microsoft Exchange в Документации Cisco для брандмауэра Cisco Secure PIX. Выберите версию программного обеспечения и прочитайте соответствующую главу по настройке Microsoft Exchange в руководстве по конфигурации.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

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

- Брандмауэр PIX 535
- Программное обеспечение брандмауэра PIX, выпуск 7.1(1)
- Маршрутизатор Cisco 2600
- Программное обеспечение Cisco IOS®, версия 12.3.14T

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа

использовались только данные, полученные от устройств с конфигурацией по умолчанию. В рабочей сети необходимо изучить потенциальное воздействие всех команд.

Условные обозначения

См. дополнительные сведения об условных обозначениях в данном документе в статье Условные обозначения для технических терминов Sisco.

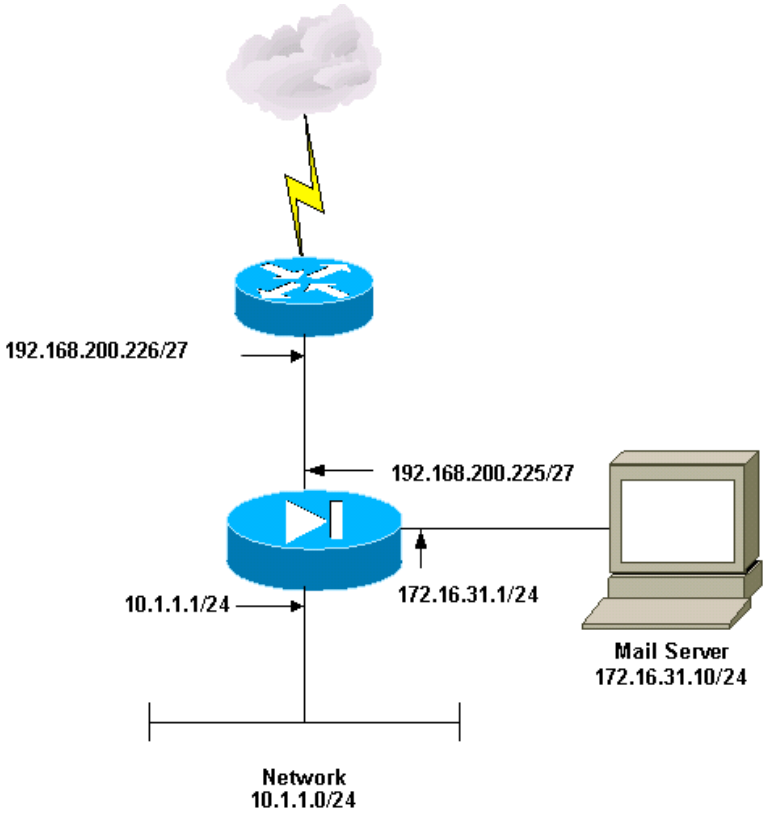
Настройка

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

Примечание: См. дополнительные сведения о командах, используемых в данном документе, в Средстве поиска команды (только для зарегистрированных пользователей).

Схема сети

В данном документе используется следующая настройка сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, запрещено распространять в Интернете. Это адреса RFC 1918 , которые использовались в лабораторной среде.

Конфигурация PIX

В данном документе используется следующая конфигурация:

Конфигурация PIX
`PIX Version 7.1(1)` `!`

```
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
shutdown
nameif BB
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
!
interface Ethernet3
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet4
nameif outside
security-level 0
ip address  192.168.200.225 255.255.255.224
!
interface Ethernet5
nameif dmz
security-level 10
ip address 172.16.31.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system flash:/pix711.bin
ftp mode passive


!--- Этот список доступа разрешает доступ узлов
!--- к IP-адресу 192.168.200.227 порта
!--- протокола простой передачи электронной почты (SMTP).


access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp


!--- Разрешает исходящие соединения SMTP.
!--- Этот список доступа разрешает узлу с IP-адресом 172.16.31.10,
!--- где расположен порт SMTP, получать доступ к любому другому узлу.


access-list dmz_int extended permit tcp host 172.16.31.10 any eq smtp

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400
global (outside) 1  192.168.200.228-192.168.200.253 netmask 255.255.255.224
global (outside) 1  192.168.200.254
nat (inside) 1 10.1.1.0 255.255.255.0


!--- В этой статичной сети не используется преобразование адресов.
!--- Внутри нее узлы отображаются в DMZ со своими собственными адресами.


static (inside,dmz) 10.1.1.0 10.1.1.0 netmask 255.255.255.0


!--- В этой статичной сети используется преобразование адресов.
!--- Узлы, находящиеся вне сети, при получении доступа к почтовому серверу
!--- используют адрес 192.168.200.227.


static (dmz,outside)  192.168.200.227 172.16.31.10 netmask 255.255.255.255
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
!
!

!--- Команда inspect esmtp (включенная в карту) позволяет серверу
!--- SMTP/ESMTP проверять приложение.


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
!

!--- Команда inspect esmtp (включенная в карту) позволяет серверу
!--- SMTP/ESMTP проверять приложение.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]
```

Конфигурация ESMTP TLS

Примечание: При использовании шифрования TLS для получения и передачи электронной почты, функция проверки ESMTP (подключаемая по умолчанию) в PIX теряет пакеты. Чтобы разрешить передачу электронных сообщения при включенном TLS, отключите функцию проверки ESMTP, как показано ниже.

```
pix(config)#policy-map global_policy
pix(config-pmap)#class inspection_default
pix(config-pmap-c)#no inspect esmtp
pix(config-pmap-c)#exit
pix(config-pmap)#exit
```

Проверка

Для этой конфигурации отсутствует процедура проверки.

Устранение неполадок

Этот раздел содержит сведения об устранении неполадок конфигурации.

Команды устранения неполадок

Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает определенные команды **show**. Используйте OIT для просмотра аналитических данных по выходным данным команды **show**.

Примечание: См. раздел "Важные сведения о командах отладки" до применения команд **отладки**.

- **debug icmp trace** — Показывает, получает ли PIX запросы протокола управляющих сообщений от узлов. Для выполнения этой отладки выполните команду **access-list**, чтобы разрешить ICMP в конфигурации.

  Примечание: Для использования этой отладки убедитесь, что в `access-list outside_int` разрешен ICMP, как показано 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 buffer debugging** — Отображает установленные соединения и отказы в подключении к узлам, которые используют PIX. Эти сведения хранятся в буфере журнала PIX, а данные можно просмотреть с использованием команды **show log**.

См. дополнительные сведения о настройке записей в журнал в разделе Настройка системного журнала PIX.

Дополнительные сведения

- **Программное обеспечение брандмауэра Cisco PIX**
- **Справочное руководство для брандмауэра PIX Cisco Secure**
- **Примечания по продуктам безопасности (включая PIX) для специалистов**
- **Документы RFC**
- **Техническая поддержка и документация – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/97294/pix7x-mailserver.shtml