Пример конфигурации проверки подлинности входящих соединений на Auth-Proxy (операционная система Cisco IOS брандмауэр, маршрутизатор/коммутатор и NAT)

Содержание

Введение

Этот пример конфигурации первоначально блокирует трафик с внешних хостов на все устройства на внутренней сети, пока проверка подлинности обозревателя не выполнена с помощью аутентификации прокси-сервера. После авторизации список доступа, переданный от сервера (**разрешают tcp|ip|icmp любого любой**), добавляет динамические записи к списку доступа 116, которые временно предоставляют доступ от внешнего ПК до внутренней сети.

Примечание: Конфигурация AAA, используемая в этом документе, также применима к Коммутаторам Catalyst, которые выполняют программное обеспечение Cisco IOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco IOS Software Release 12.2. 23
- Маршрутизатор Cisco 3640

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.

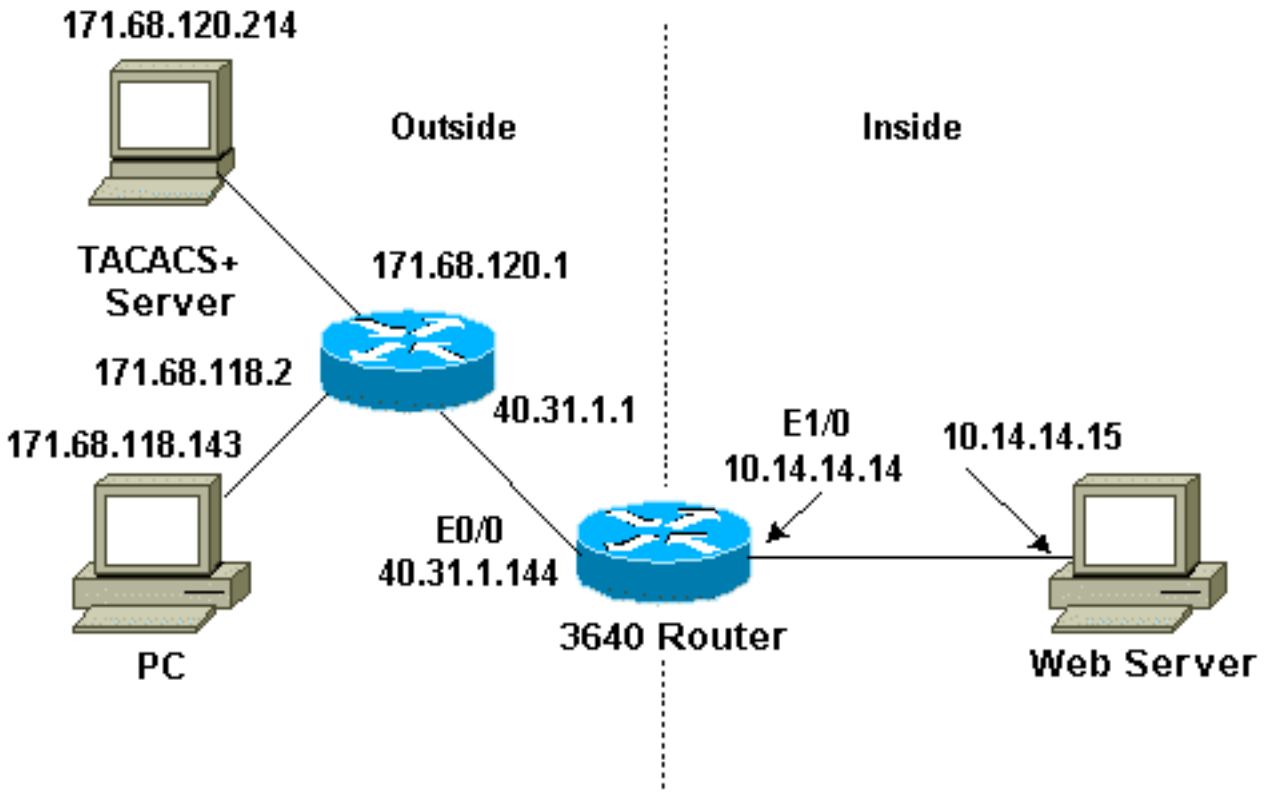
Настройка

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:



Конфигурации

В данном документе используется следующая конфигурация:

- Маршрутизатор Cisco 3640

Маршрутизатор Cisco 3640

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sec-3640
!
aaa new-model aaa group server tacacs+ RTP server
171.68.120.214 ! aaa authentication login default group
RTP none aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP enable
secret 5 $1$pqRI$3TDNFT9FdYT8Sd/q3S0VU1 enable password
ww ! ip subnet-zero ! ip inspect name myfw cuseeme
timeout 3600 ip inspect name myfw ftp timeout 3600 ip
inspect name myfw http timeout 3600 ip inspect name myfw
rcmd timeout 3600 ip inspect name myfw realaudio timeout
3600 ip inspect name myfw smtp timeout 3600 ip inspect
name myfw sqlnet timeout 3600 ip inspect name myfw
streamworks timeout 3600 ip inspect name myfw tftp
timeout 30 ip inspect name myfw udp timeout 15 ip
inspect name myfw tcp timeout 3600 ip inspect name myfw
vdolive ip auth-proxy auth-proxy-banner ip auth-proxy
auth-cache-time 10 ip auth-proxy name list_a http ip
audit notify log ip audit po max-events 100 ! interface
Ethernet0/0 ip address 40.31.1.144 255.255.255.0 ip
access-group 116 in ip nat outside ip auth-proxy list_a
no ip route-cache no ip mroute-cache speed auto half-
duplex no mop enabled ! interface Ethernet1/0 ip address
10.14.14.14 255.255.255.0 ip nat inside ip inspect myfw
in speed auto half-duplex ! !--- Interfaces deleted. !
nat pool outsidepool 40.31.1.50 40.31.1.60 netmask
255.255.255.0 ip nat inside source list 1 pool
outsidepool ip nat inside source static 10.14.14.15
40.31.1.77 ip classless ip route 0.0.0.0 0.0.0.0
40.31.1.1 ip route 171.68.118.0 255.255.255.0 40.31.1.1
ip route 171.68.120.0 255.255.255.0 40.31.1.1 no ip http
server ! access-list 116 permit tcp host 171.68.118.143
host 40.31.1.144 eq www access-list 116 deny tcp host
171.68.118.143 any access-list 116 deny udp host
171.68.118.143 any access-list 116 deny icmp host
171.68.118.143 any access-list 116 permit icmp any any
access-list 116 permit tcp any any access-list 116
permit udp any any dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit ! tacacs-server host
171.68.120.214 tacacs-server key cisco ! line con 0
transport input none line aux 0 line vty 0 4 password ww
! end
```

Проверка

Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

См. Устранение проблем Аутентификации прокси-сервера для команды и сведений об устранении проблем.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- (межсетевой экран Cisco IOS)
- Поддержка технологии безопасности и VPN
- Cisco Systems – техническая поддержка и документация