Настройка проверки подлинности исходящих соединений (брандмауэр Cisco IOS и NAT)

Содержание

Введение

Этот пример конфигурации первоначально блокирует трафик от основного устройства (в 10.31.1.47) на внутренней сети ко всем устройствам в Интернете, пока вы не выполняете проверку подлинности обозревателя с использованием аутентификации прокси-сервера. Список доступа, переданный от сервера (**разрешают tcp|ip|icmp любого любой**), добавляет post-authorization динамических записей к списку доступа 116, которые временно предоставляют доступ от того устройства до Интернета.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 12.2.23 программного обеспечения Cisco IOS
- Маршрутизатор Cisco 3640

Примечание: Команда "ip auth-proxy" была реализована в Cisco IOS Software Release 12.0.5.T. Эта конфигурация была протестирована с Cisco IOS Software Release 12.0.7. T.

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.

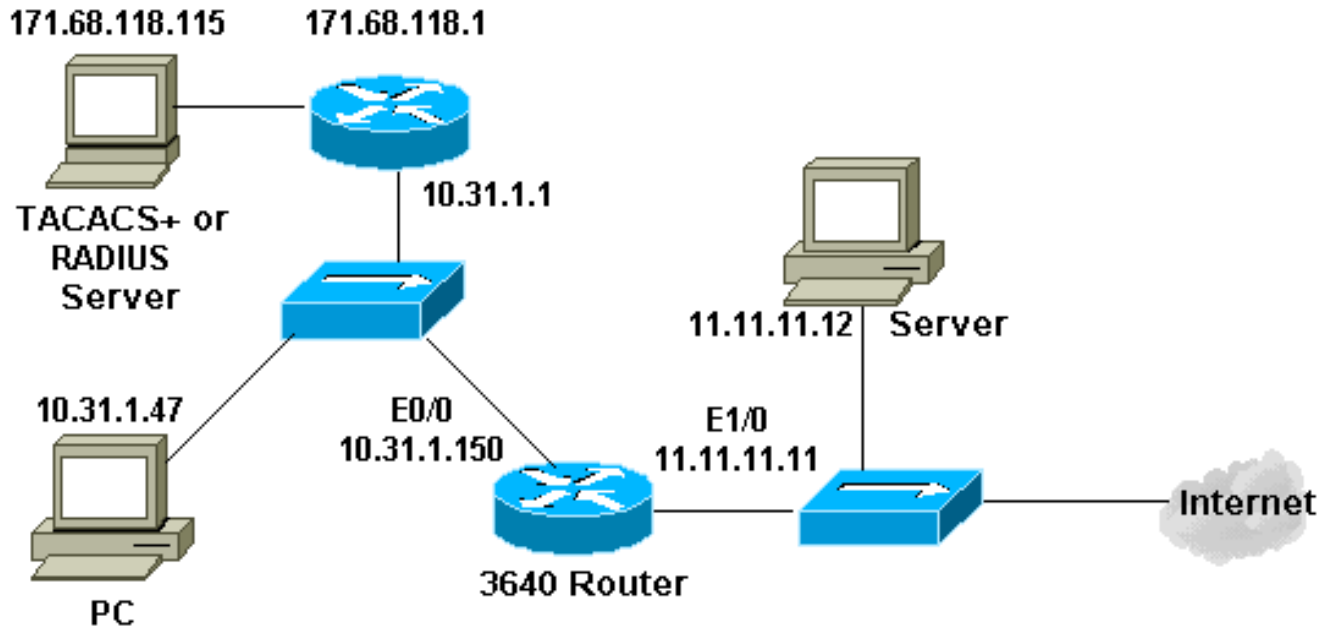
Настройка

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 3640
Current configuration: ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption

```
!
hostname security-3640
!
aaa new-model aaa group server tacacs+ RTP server
171.68.118.115 ! aaa authentication login default local
group RTP none aaa authorization exec default group RTP
none aaa authorization auth-proxy default group RTP
enable secret 5 $1$vCfr$rkuU6HLmpbNgLTg/JNM6e1 enable
password ww ! username john password 0 doe ! 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 ! process-max-time 200 ! interface
Ethernet0/0 ip address 10.31.1.150 255.255.255.0 ip
access-group 116 in ip nat inside ip inspect myfw in ip
auth-proxy list_a no ip route-cache no ip mroute-cache !
interface Ethernet1/0 ip address 11.11.11.11
255.255.255.0 ip access-group 101 in ip nat outside ! ip
nat pool outsidepool 11.11.11.20 11.11.11.30 netmask
255.255.255.0 ip nat inside source list 1 pool
outsidepool ip classless ip route 0.0.0.0 0.0.0.0
11.11.11.1 ip route 171.68.118.0 255.255.255.0 10.31.1.1
ip http server ip http authentication aaa ! access-list
1 permit 10.31.1.0 0.0.0.255 access-list 101 deny ip
10.31.1.0 0.0.0.255 any access-list 101 deny ip
127.0.0.0 0.255.255.255 any access-list 101 permit icmp
any 11.11.11.0 0.0.0.255 unreachable access-list 101
permit icmp any 11.11.11.0 0.0.0.255 echo-reply access-
list 101 permit icmp any 11.11.11.0 0.0.0.255 packet-
too-big access-list 101 permit icmp any 11.11.11.0
0.0.0.255 time-exceeded access-list 101 permit icmp any
11.11.11.0 0.0.0.255 traceroute access-list 101 permit
icmp any 11.11.11.0 0.0.0.255 administratively-
prohibited access-list 101 permit icmp any 11.11.11.0
0.0.0.255 echo access-list 116 permit tcp host
10.31.1.47 host 10.31.1.150 eq www access-list 116 deny
tcp host 10.31.1.47 any access-list 116 deny udp host
10.31.1.47 any access-list 116 deny icmp host 10.31.1.47
any access-list 116 permit tcp 10.31.1.0 0.0.0.255 any
access-list 116 permit udp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 171.68.118.0 0.0.0.255 any
access-list 116 permit tcp 171.68.118.0 0.0.0.255 any
access-list 116 permit udp 171.68.118.0 0.0.0.255 any
dialer-list 1 protocol ip permit dialer-list 1 protocol
ipx permit ! tacacs-server host 171.68.118.115 tacacs-
server key cisco radius-server host 171.68.118.115 auth-
port 1645 acct-port 1646 radius-server key cisco ! line
con 0 transport input none line aux 0 line vty 0 4 exec-
timeout 0 0 password ww ! end
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Для **команд отладки**, наряду с другими сведениями об устранении проблем, обращаются к Устранению проблем Аутентификации прокси-сервера.

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

Дополнительные сведения

- Страница поддержки межсетевого экрана IOS
- Страница поддержки TACACS/TACACS+
- TACACS+ в документации по IOS
- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация