"Настройка проверки подлинности входящих соединений для Auth-Proxy (операционная система Cicso IOS, брандмауэр, без NAT)"

Содержание

Введение

Этот пример конфигурации первоначально преграждает траффик от внешних хостов к всем устройствам на внутренней сети до тех пор, пока не выполнена аутентификация не выполнена использованием прокси аутентификации. Список доступа, переданный от сервера (**разрешают tcp|ip|icmp любого любой**), добавляет post-authorization динамических записей к access-list 115, которые временно предоставляют доступ от внешнего ПК до внутренней сети.

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 12.0.7.T
- Маршрутизатор Cisco 3640

Примечание: Команда **ip auth-proxy** представлена 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.

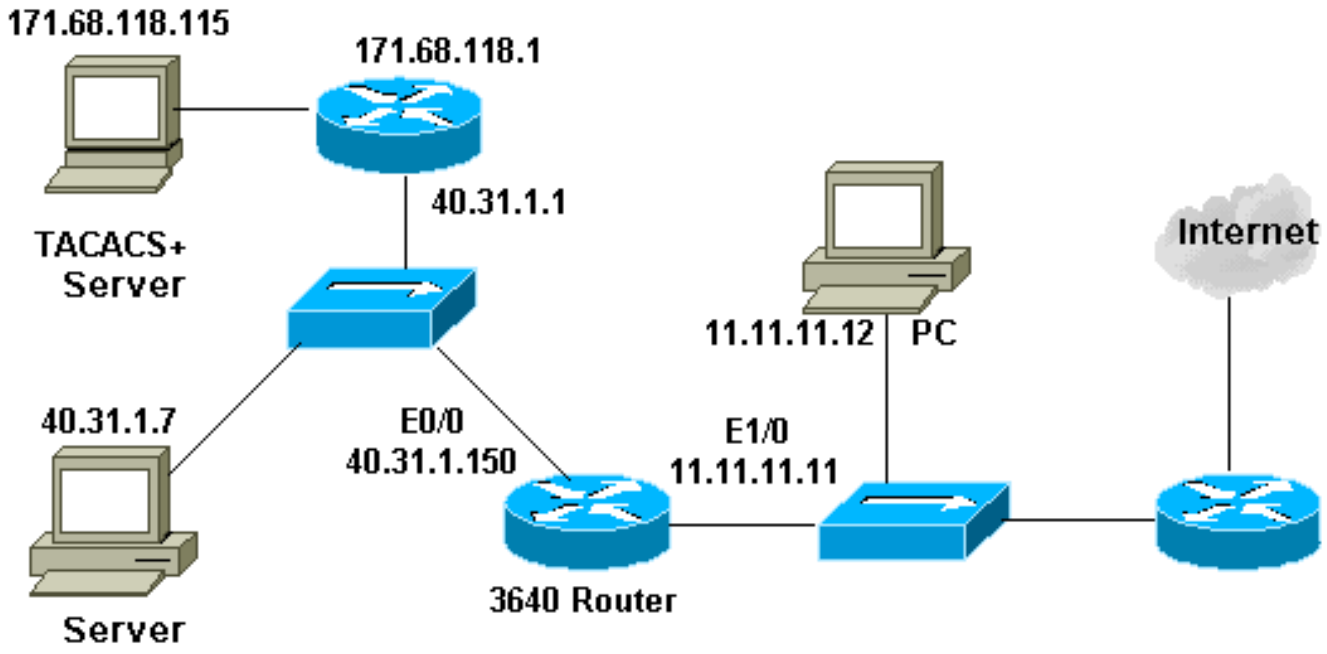
Настройка

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:



!--- конфигурацию

В данном документе используется следующая конфигурация:

Маршрутизатор 3640
Current configuration: ! version 12.0

```
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 group
RTP none aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP enable
secret 5 $1$H9zZ$z9bu5HMy4NTtjsvIhltGT0 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 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 cns event-service server ! process-max-
time 200 ! interface FastEthernet0/0 ip address
40.31.1.150 255.255.255.0 ip access-group 101 in no ip
directed-broadcast ip inspect myfw in no mop enabled !
interface FastEthernet1/0 ip address 11.11.11.11
255.255.255.0 ip access-group 115 in no ip directed-
broadcast ip auth-proxy list_a ! 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 40.31.1.1 ip http server ip http
authentication aaa ! access-list 101 permit icmp
40.31.1.0 0.0.0.255 any access-list 101 permit tcp
40.31.1.0 0.0.0.255 any access-list 101 permit udp
40.31.1.0 0.0.0.255 any access-list 101 permit icmp
171.68.118.0 0.0.0.255 any access-list 101 permit tcp
171.68.118.0 0.0.0.255 any access-list 101 permit udp
171.68.118.0 0.0.0.255 any access-list 115 permit tcp
host 11.11.11.12 host 11.11.11.11 eq www access-list 115
deny tcp any any access-list 115 deny udp any any
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 echo
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
echo-reply access-list 115 permit icmp any 40.31.1.0
0.0.0.255 packet-too-big access-list 115 permit icmp any
40.31.1.0 0.0.0.255 time-exceeded access-list 115 permit
icmp any 40.31.1.0 0.0.0.255 traceroute access-list 115
permit icmp any 40.31.1.0 0.0.0.255 unreachable access-
list 115 permit icmp any 40.31.1.0 0.0.0.255
administratively-prohibited 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 radius-server key cisco !
line con 0 transport input none line aux 0 line vty 0 4
password ww ! ! end
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Для этих команд, 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