Настройка проверки подлинности входящих соединений на прокси с проверкой подлинности без Cisco IOS брандмауэра и NAT

Содержание

Введение

Этот пример конфигурации первоначально блокирует трафик от основного устройства (в 11.11.11.12) на внешней сети ко всем устройствам на внутренней сети, 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 115, которые временно предоставляют доступ от основного устройства 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" 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.

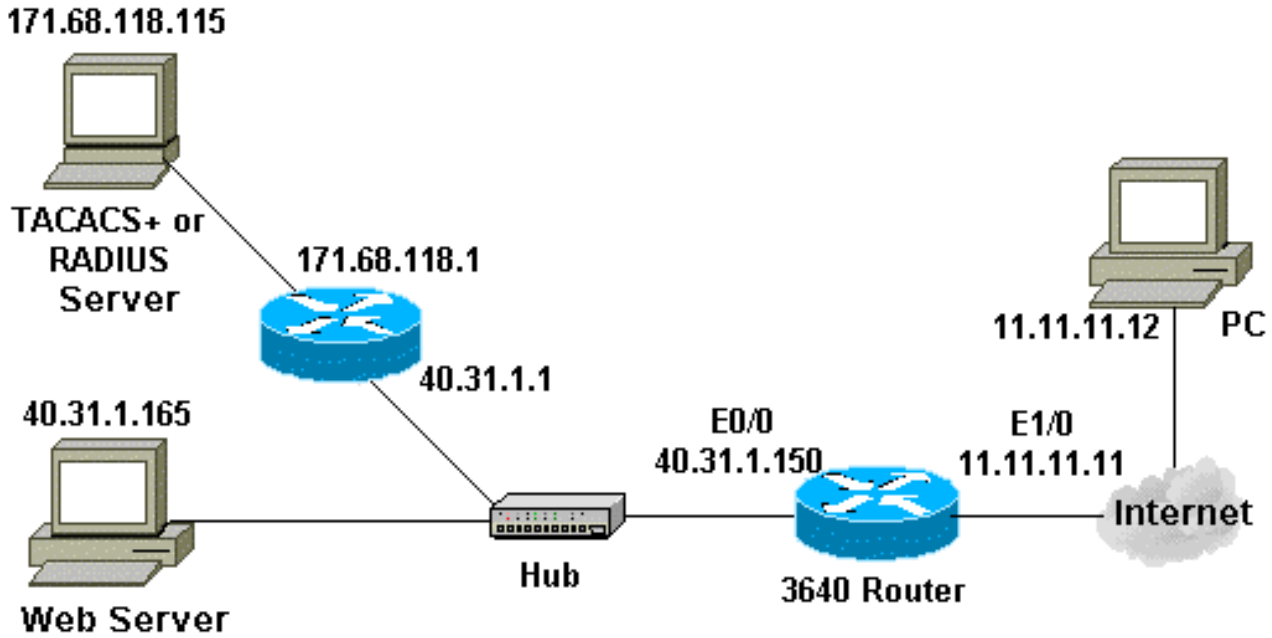
Настройка

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 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname security-3640
!
!--- Turn on authentication. aaa new-model !--- Define
the server group and servers for TACACS+ or RADIUS. aaa
group server tacacs+|radius RTP server 171.68.118.115 !
!--- Define what you need to authenticate. 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 ! !--- You want the router name to appear as
banner. ip auth-proxy auth-proxy-banner !--- You want
the access-list entries to timeout after 10 minutes. ip
auth-proxy auth-cache-time 10 !--- You define the list-
name to be associated with the interface. 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 no ip directed-broadcast no mop enabled !
interface FastEthernet1/0 ip address 11.11.11.11
255.255.255.0 !--- Apply the access-list to the
interface. ip access-group 115 in no ip directed-
broadcast !--- Apply the auth-proxy list-name. ip auth-
proxy list_a ! ip classless ip route 171.68.118.0
255.255.255.0 40.31.1.1 !--- Turn on the http server and
authentication. ip http server ip http authentication
aaa ! !--- This is our access-list for auth-proxy
testing - !--- it denies only one host, 11.11.11.12,
access - to minimize disruption !--- to the network
during testing. access-list 115 permit tcp host
11.11.11.12 host 11.11.11.11 eq www access-list 115 deny
icmp host 11.11.11.12 any access-list 115 deny tcp host
11.11.11.12 any access-list 115 deny udp host
11.11.11.12 any access-list 115 permit udp any any
access-list 115 permit tcp any any access-list 115
permit icmp any any dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit ! !--- Define the
server(s). 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

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