Настройка проверки подлинности входящих соединений с IPsec и настройка клиента VPN с NAT и брандмауэром Cisco IOS

Содержание

Введение

В этом примере конфигурация позволяет клиенту VPN получить доступ к серверу в другой сети с помощью туннеля IPSec после успешной аутентификации пользователя.

PC с адресом 99.99.99.5 загружает веб-браузер для доступа к содержимому сервера с адресом 10.13.1.98. Так как Клиент VPN на ПК настроен для прохождения через оконечной точки туннеля 99.99.99.1 для получения до 10.13.1.x сеть, Туннель IPSec создан, и ПК вытаскивает IP-адрес из пула, названного "ourpool" (так как вы делаете mode-configuration). Маршрутизатор 3640 запрашивает аутентификацию. После того, как пользователь введет имя пользователя и пароль (хранящийся на сервере TACACS+ на 172.18.124.97), список доступа, полученный с сервера, добавится в список доступа 117.

Примечание: Команда **ip auth-proxy** была представлена в Выпуске 12.0.5 программного обеспечения Cisco IOS. T.

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 (c3640-jo3s56i-mz.121-2.3. T
- Cisco Secure VPN Client 1.0 (показанный как 2.0.7 в меню IRE client Help> About) или Cisco Secure VPN Client 1.1 (показанный как 2.1.12 в меню IRE client Help> About)

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.

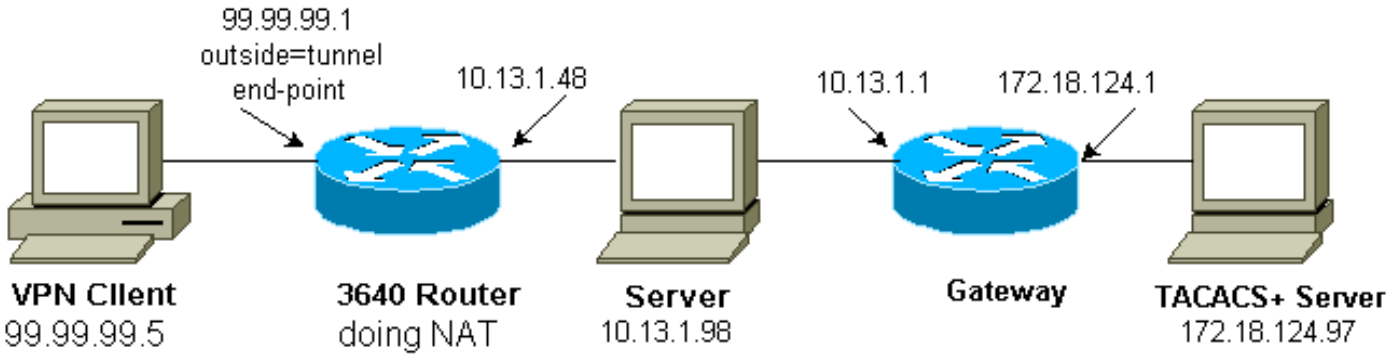
Настройка

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:

Конфигурация маршрутизатора Cisco 3640
Current configuration: ! version 12.1 service timestamps debug uptime service timestamps log uptime no service password-encryption !

```
hostname carter
!
aaa new-model aaa authentication login default group
tacacs+ none aaa authorization exec default group
tacacs+ none aaa authorization auth-proxy default group
tacacs+ enable secret 5 $1$cSvL$F6VxA7kBFAGHvhBbRlNS20
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 cns event-
service server ! crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco1234
address 0.0.0.0 0.0.0.0 crypto isakmp client
configuration address-pool local ourpool ! crypto ipsec
transform-set mypolicy esp-des esp-md5-hmac ! crypto
dynamic-map dyna 10 set transform-set mypolicy ! crypto
map test client configuration address initiate crypto
map test client configuration address respond crypto map
test 5 ipsec-isakmp dynamic dyna ! interface Loopback0
ip address 1.1.1.1 255.255.255.0 ! interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0 ip nat inside ip
inspect myfw in ip route-cache policy no ip mroute-cache
ip policy route-map nonat no mop enabled ! interface
TokenRing0/0 no ip address shutdown ring-speed 16 !
interface Ethernet2/0 ip address 99.99.99.1
255.255.255.0 ip access-group 117 in ip nat outside ip
auth-proxy list_a no ip route-cache no ip mroute-cache
no mop enabled crypto map test ! interface TokenRing2/0
no ip address shutdown ring-speed 16 ! ip local pool
ourpool 10.2.1.1 10.2.1.254 ip nat pool outsidepool
99.99.99.50 99.99.99.60 netmask 255.255.255.0 ip nat
inside source route-map rmap pool outsidepool ip
classless ip route 0.0.0.0 0.0.0.0 99.99.99.20 ip route
172.18.124.0 255.255.255.0 10.13.1.1 no ip http server !
access-list 110 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255 access-list 110 permit ip 10.13.1.0 0.0.0.255
any access-list 117 permit esp any any access-list 117
permit udp any any eq isakmp access-list 120 permit ip
10.13.1.0 0.0.0.255 10.2.1.0 0.0.0.255 dialer-list 1
protocol ip permit dialer-list 1 protocol ipx permit
route-map rmap permit 10 match ip address 110 ! route-
map nonat permit 10 match ip address 120 set ip next-hop
1.1.1.2 ! route-map nonat permit 20 ! tacacs-server host
172.18.124.97 tacacs-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

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

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

- Cisco VPN Client
- Согласование IPsec/Протоколы IKE
- Техническая поддержка межсетевого экрана Cisco IOS
- Cisco Systems – техническая поддержка и документация