Настройка протокола IPSec между двумя системами IOS с использованием шифрования AES

Содержание

Введение

В документе содержится пример конфигурации IPSec-туннеля IOS-to-IOS с использованием шифрования стандарта AES.

Предварительные условия

Требования

Поддержка шифрования AES была представлена в Cisco IOS® 12.2 (13) T.

Используемые компоненты

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

- Программное обеспечение Cisco IOS версии 12.3(10)
- Маршрутизаторы Cisco 1721

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

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Конфигурации

В данном документе используется следующая конфигурация.

- Маршрутизатор 1721-A
- Маршрутизатор 1721-B

Маршрутизатор 1721-A

```
R-1721-A#show run Building configuration... Current
configuration : 1706 bytes ! ! Last configuration change
at 00:46:32 UTC Fri Sep 10 2004 ! NVRAM config last
updated at 00:45:48 UTC Fri Sep 10 2004 ! version 12.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname R-1721-A ! boot-start-marker boot-
end-marker ! ! memory-size iomem 15 mmi polling-interval
60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180
no aaa new-model ip subnet-zero ip cef ! ! ! ip audit po
max-events 100 no ip domain lookup no ftp-server write-
enable ! ! ! ! !--- Define Internet Key Exchange (IKE)
policy. crypto isakmp policy 10 !--- Specify the 256-bit
AES as the !--- encryption algorithm within an IKE
policy. encr aes 256 !--- Specify that pre-shared key
authentication is used. authentication pre-share !---
Specify the shared secret. crypto isakmp key cisco123
address 10.48.66.146 ! ! !--- Define the IPSec transform
set. crypto ipsec transform-set aesset esp-aes 256 esp-
sha-hmac ! !--- Define crypto map entry name "aesmap"
that will use !--- IKE to establish the security
associations (SA). crypto map aesmap 10 ipsec-isakmp !--
- Specify remote IPSec peer. set peer 10.48.66.146 !---
Specify which transform sets !--- are allowed for this
crypto map entry. set transform-set aesset !--- Name the
access list that determines which traffic !--- should be
protected by IPSec. match address acl_vpn ! ! !
interface ATM0 no ip address shutdown no atm ilmi-
keepalive dsl equipment-type CPE dsl operating-mode
GSHDSL symmetric annex A dsl linerate AUTO ! interface
Ethernet0 ip address 192.168.100.1 255.255.255.0 ip nat
inside half-duplex ! interface FastEthernet0 ip address
10.48.66.147 255.255.254.0 ip nat outside speed auto !--
- Apply crypto map to the interface. crypto map aesmap !
ip nat inside source list acl_nat interface
```

```
FastEthernet0 overload ip classless ip route 0.0.0.0
0.0.0.0 10.48.66.1 ip route 192.168.200.0 255.255.255.0
FastEthernet0 no ip http server no ip http secure-server
! ip access-list extended acl_nat !--- Exclude protected
traffic from being NAT'ed. deny ip 192.168.100.0
0.0.0.255 192.168.200.0 0.0.0.255 permit ip
192.168.100.0 0.0.0.255 any !--- Access list that
defines traffic protected by IPSec. ip access-list
extended acl_vpn permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255 ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end R-1721-A#
```

Маршрутизатор 1721-B

```
R-1721-B#show run Building configuration... Current
configuration : 1492 bytes ! ! Last configuration change
at 14:11:41 UTC Wed Sep 8 2004 ! version 12.3 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
R-1721-B ! boot-start-marker boot-end-marker ! ! memory-
size iomem 15 mmi polling-interval 60 no mmi auto-
configure no mmi pvc mmi snmp-timeout 180 no aaa new-
model ip subnet-zero ip cef ! ! ! ip audit po max-events
100 no ip domain lookup no ftp-server write-enable ! ! !
! ! !--- Define IKE policy. crypto isakmp policy 10 !---
Specify the 256-bit AES as the !--- encryption algorithm
within an IKE policy. encr aes 256 !--- Specify that
pre-shared key authentication is used. authentication
pre-share !--- Specify the shared secret. crypto isakmp
key cisco123 address 10.48.66.147 ! ! !--- Define the
IPSec transform set. crypto ipsec transform-set aesset
esp-aes 256 esp-sha-hmac ! !--- Define crypto map entry
name "aesmap" that uses !--- IKE to establish the SA.
crypto map aesmap 10 ipsec-isakmp !--- Specify remote
IPSec peer. set peer 10.48.66.147 !--- Specify which
transform sets !--- are allowed for this crypto map
entry. set transform-set aesset !--- Name the access
list that determines which traffic !--- should be
protected by IPSec. match address acl_vpn ! ! !
interface Ethernet0 ip address 192.168.200.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet0 ip address 10.48.66.146 255.255.254.0 ip
nat outside speed auto !--- Apply crypto map to the
interface. crypto map aesmap ! ip nat inside source list
acl_nat interface FastEthernet0 overload ip classless ip
route 0.0.0.0 0.0.0.0 10.48.66.1 ip route 192.168.100.0
255.255.255.0 FastEthernet0 no ip http server no ip http
secure-server ! ip access-list extended acl_nat !---
Exclude protected traffic from being NAT'ed. deny ip
192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 permit
ip 192.168.200.0 0.0.0.255 any !--- Access list that
defines traffic protected by IPSec. ip access-list
extended acl_vpn permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255 ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 ! end R-1721-B#
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных

данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- show crypto isakmp sa - отображает состояние для ISAKMP (Internet Security Association and Key Management Protocol) SA.
- show crypto ipsec sa – выводит статистику по активным туннелям.
- show crypto engine connections active – выводит количество шифровок или дешифровок на контекст безопасности.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

- debug crypto ipsec– показывает события IPSec.
- debug crypto isakmp – отображает сообщения о событиях IKE.
- debug crypto engine– выводит информацию о криптографическом модуле.

Дополнительные сведения об устранении проблем IPSec см. в документе Основные сведения об устранении проблем в IP-безопасности и об использовании команд отладки.

Дополнительные сведения

- Cisco IOS Software Releases 12.2T – расширенный стандарт шифрования (AES)
- Настройка параметров сетевой безопасности IPSec Network Security
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems