IOS VPN (Маршрутизатор): Добавление нового VPN-туннеля L2L или удаленного доступа VPN к существующему VPN L2L

Содержание

Введение

В этом документе указаны шаги, необходимые для добавления нового VPN-туннеля L2L или VPN-сети удаленного доступа в конфигурацию VPN L2L, которая уже существует в маршрутизаторе IOS.

Предварительные условия

Требования

Гарантируйте корректную настройку VPN-туннеля IPSec L2L, который в настоящее время в рабочем состоянии перед попыткой этой конфигурации.

Используемые компоненты

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

- Два маршрутизатора IOS, которые выполняют версии программного обеспечения 12.4 и 12.2
- Одно устройство адаптивной защиты Cisco (ASA), который работает под управлением ПО версии 8.0

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.

Схема сети

В настоящем документе используется следующая схема сети:

Эти выходные данные являются текущими рабочими конфигурациями HQ (КОНЦЕНТРАТОР) маршрутизатор и ASA Филиала компании 1 (BO1). В этой конфигурации существует туннель L2L IPSec, настроенный между HQ и BO1 ASA.

Текущий HQ (КОНЦЕНТРАТОР) конфигурация маршрутизатора

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
```

```
 set transform-set newset
 match address VPN_BO1
!
!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Конфигурация BO1 ASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
```

```
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
```

```
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

Общие сведения

В настоящее время существует существующий туннель L2L, установленный между офисом HQ и офисом BO1. Ваша компания недавно открыла новый филиал компании (BO2). Этот новый офис требует подключения к локальным ресурсам, которые расположены в офисе HQ. Кроме того, существует дополнительное требование, чтобы позволить сотрудникам возможность работать из дома и надежно обратиться к ресурсам, которые расположены на внутренней сети удаленно. В данном примере новый VPN-туннель настроен, а также сервер VPN для удаленного доступа, который расположен в офис HQ.

Добавьте дополнительный туннель L2L к конфигурации

Это - схема сети для этой конфигурации:

Пошаговые инструкции

Этот раздел предоставляет требуемые процедуры, которые должны быть выполнены на маршрутизаторе HQ КОНЦЕНТРАТОРА.

Выполните следующие действия:

1. Создайте этот новый список доступа, который будет использоваться криптокартой, для определения представляющего интерес трафика:`HQ_HUB(config)#`**`ip access-list extended VPN_BO2`**
   `HQ_HUB(config-ext-nacl)#`**`permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`exit`**
   % Warning: Для связи для имения место другая сторона туннеля должна иметь противоположность этой записи списка контроля доступа (ACL) для той индивидуальной сети.
2. Добавьте эти записи ни в какое выражение NAT для освобождения преобразовывания посредством NAT между этими сетями:`HQ_HUB(config)#`**`ip access-list extended NAT_Exempt`**
   `HQ_HUB(config-ext-nacl)#`**`deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`permit ip 10.10.10.0 0.0.0.255 any`**

Добавьте, что эти ACL к существующему маршруту сопоставляют nonat:
```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```
% Warning: Для связи для имения место другая сторона туннеля должна иметь противоположность этой записи ACL для той индивидуальной сети.

3. Задайте адрес партнера (peer) в 1-ой фазе настройки как показано:`HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2`
   Примечание: Предварительный общий ключ должен совпасть точно с обеих сторон туннеля.
4. Создайте конфигурацию криптокарты для нового VPN-туннеля. Используйте тот же набор преобразований, который использовался в первой конфигурации VPN, поскольку все параметры настройки фазы 2 являются тем же.
```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
 HQ_HUB(config-crypto-map)#set peer 192.168.12.2
 HQ_HUB(config-crypto-map)#set transform-set newset
 HQ_HUB(config-crypto-map)#match address VPN_BO2
```
5. Теперь, когда вы настроили новый туннель, необходимо передать представляющий интерес трафик через туннель для внедрения его. Для выполнения этого выполните **расширенную команду ping** для прозванивания хоста на внутренней сети удаленного туннеля.В данном примере пропингована рабочая станция с другой стороны туннеля с адресом 10.20.20.16. Это переводит туннель в рабочее состояние между HQ и BO2. Теперь, существует два туннеля, связанные с офисом HQ. Если у вас нет доступа к системе позади туннеля, обратитесь к Решениям для Устранения проблем IPSEC VPN Наиболее распространенного соединения L2L и Удаленного доступа найти альтернативное решение с помощью `management-access`.

Пример конфигурации

HUB_HQ - Добавленный новая конфигурация VPN-туннеля L2L

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
```

```
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
```

```
line vty 0 4
!
!
end
HQ_HUB#
```

Конфигурация BO2 L2L VPN-туннеля

```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
```

```
 no ip address
 shutdown
!
ip nat inside source route-map nonat interface Ethernet1
overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

Добавьте VPN для удаленного доступа к конфигурации

Это - схема сети для этой конфигурации:

В данном примере звонила функция**, раздельное туннелирование** используется. Эта функция позволяет Клиенту IPSEC удаленного доступа условно прямым пакетам по Туннелю IPSec в зашифрованной форме, или к сетевому интерфейсу в форме открытого текста. С включенным разделенным туннелированием пакеты, не направляющиеся в назначения с другой стороны Туннеля IPSec, не должны быть зашифрованы, переданы через туннель, дешифровали, и затем маршрутизировали к конечному назначению. Это понятие применяет политику разделенного туннелирования к указанной сети. По умолчанию должен туннелировать весь трафик. Для установки политики разделенного туннелирования задайте ACL, где может быть упомянут трафик, предназначенный для Интернета.

Пошаговые инструкции

Этот раздел предоставляет требуемые процедуры, чтобы добавить возможность удаленного доступа и позволить удаленным пользователям обращаться ко всем узлам.

Выполните следующие действия:

1. Создайте пул IP-адреса, который будет использоваться для клиентов, которые соединяются через VPN-туннель. Кроме того, создайте рядового пользователя для доступа к VPN, как только завершена конфигурация.`HQ_HUB(config)#`**`ip local pool ippool 10.10.120.10 10.10.120.50`**
   `HQ_HUB(config)#`**`username vpnuser password 0 vpnuser123`**
2. Освободите определенный трафик от того, чтобы быть преобразованным посредством NAT.`HQ_HUB(config)#`**`ip access-list extended NAT_Exempt`**

```
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit
```

Добавьте, что эти ACL к существующему маршруту сопоставляют nonat:

```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

Заметьте, что туземная связь между VPN-туннелями освобождена в данном примере.

3. Позвольте связь между существующими туннелями L2L и пользователями VPN для удаленного доступа.

```
HQ_HUB(config)#ip access-list extended VPN_BO1
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

Это позволяет пользователям удаленного доступа способность связаться с сетями позади указанных туннелей.**% Warning:** Для связи для имения место другая сторона туннеля должна иметь противоположность этой записи ACL для той индивидуальной сети.

4. **Настройте раздельное туннелирование**Для включения разделенного туннелирования для VPN-подключений удостоверьтесь, что вы настраиваете ACL на маршрутизаторе. В данном примере **команда access-list split_tunnel** привязана к группе для целей раздельного туннелирования, и туннель сформирован к 10.10.10.0 / 24 и 10.20.20.0/24 и 172.16.1.0/24 сети. Трафики дешифровали к устройствам не в разделении туннеля ACL (например, Интернет).

```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

5. Настройте локальную проверку подлинности, авторизацию и сведения о конфигурации клиента, такие как wins, dns. acl представляющего интерес трафика и пул IP, для клиентов VPN.

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```

6. Настройте динамическую схему и cryto сведения о сопоставлении, требуемые к созданию VPN-туннеля.

```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
```

```
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

Пример конфигурации

Пример конфигурации 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
```

```
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
```

```
!
end
HQ_HUB#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **ping** — Эта команда позволяет вам инициировать VPN-туннель L2L как показано.

Устранение неполадок

См. эти документы для получения информации можно использовать для устранения проблем конфигурации:

- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Устранение проблем IPSec — общие сведения и использование команд debug

Совет: Когда вы очищаете сопоставления безопасности, и это не решает вопрос IPSec VPN, затем удаляет и повторно применяет соответствующую криптокарту для решения большого разнообразия проблем.

% Warning: При удалении криптокарты из интерфейса это переводит в нерабочее состояние любые Туннели IPSec, привязанные к той криптокарте. Выполните эти действия с осторожностью и рассмотрите политику управления изменениями своей организации перед переходом.

Пример

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Дополнительные сведения

- Введение в шифрование IPSec
- Страница технической поддержки протоколов согласования IPSec и IKE
- Настройка динамических участников LAN-LAN и клиентов VPN маршрутизатора IPsec
- Cisco Systems – техническая поддержка и документация