Настройте защищенное взаимодействие между сетями Site-to-Site IPsec туннель IKEv1 между ASA и маршрутизатором Cisco IOS

Содержание

Введение

Этот документ описывает, как настроить от узла к узлу (LAN-LAN) туннель Версии 1 (IKEv1) Обмена ключами между сетями IPSec через CLI между устройством адаптивной защиты Cisco (ASA) и маршрутизатором, который выполняет программное обеспечение Cisco IOS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco IOS
- Cisco ASA
- Общие понятия IPSec

Используемые компоненты

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

- 5512-X ASA Серии Cisco , который работает под управлением ПО версии 9.4 (1)
- Маршрутизатор интегрированных служб Cisco 1941 (ISR), который выполняет версию программного обеспечения Cisco IOS 15.4 (3) M2

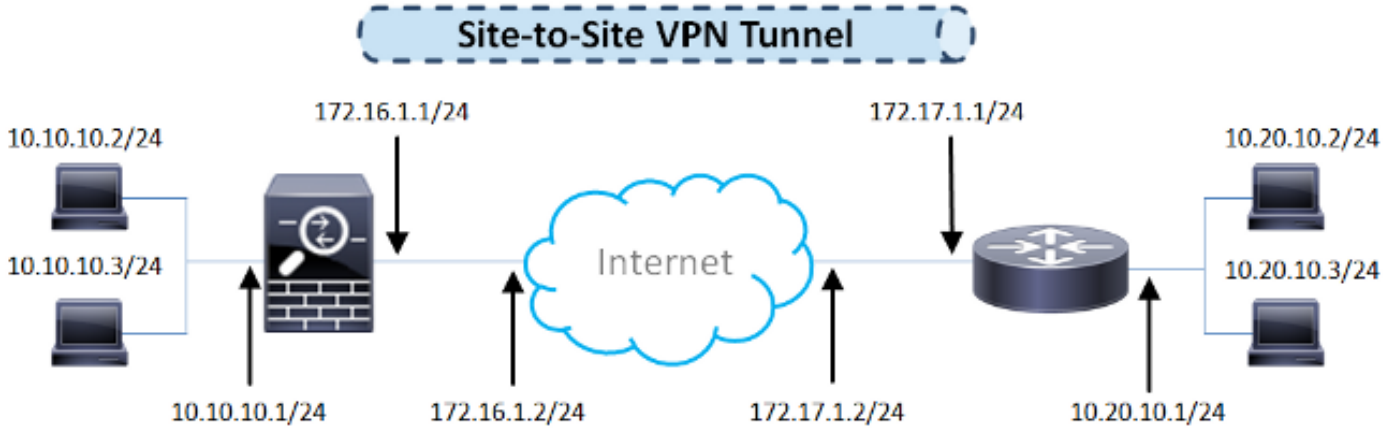
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

В этом разделе описывается завершить конфигурации интерфейса командой строки маршрутизатора IOS и ASA.

Схема сети

Сведения в этом документе используют эту сетевую установку:



Конфигурация ASA

Настройте интерфейсы ASA

Если интерфейсы ASA не настроены, гарантируют настройку, по крайней мере, IP-адресов, имен интерфейсов и уровней безопасности:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **Примечание:** Гарантируйте, что существует подключение и к внутреннему и к внешним сетям, и особенно к удаленному узлу, который будет использоваться для установления туннеля VPN типа «узел-узел». Можно использовать эхо-запрос для проверки основного подключения.

Настройте политику IKEv1 и включите IKEv1 на внешнем интерфейсе

Для настройки политики Протокола ISAKMP для соединений IKEv1 введите **крипто-ikev1** команду **<priority> политики**:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **Примечание:** Когда обе из политики от двух узлов содержит ту же аутентификацию, шифрование, хэш и значения параметра Диффи-Хеллмана, соответствие политики IKEv1 существует. Для IKEv1 политика удаленного узла должна также задать срок действия, меньше чем или равный сроку действия в политике, которую передает инициатор. Если сроки службы не идентичны, то ASA использует более короткий срок

действия.

Примечание: Если вы не задаете значение для данного параметра политики, значение по умолчанию применено.

Необходимо включить IKEv1 на интерфейсе, который завершает VPN-туннель. Как правило, это - внешняя сторона (или *общественность*) интерфейс. Для включения IKEv1 войдите**, крипто-ikev1 выполняют** команду **<interface-name>** в режиме глобальной конфигурации:

```
crypto ikev1 enable outside
```

Настройте туннельную группу (профиль прямого соединения локальных сетей)

Для туннеля между локальными сетями (LAN-to-LAN) тип профиля подключения является **ipsec-l2l**. Для настройки общего ключа IKEv1 введите режим конфигурации *атрибутов IPSec туннельной группы*:

```
crypto ikev1 enable outside
```

Настройте ACL для трафика VPN интереса

ASA использует Списки контроля доступа (ACL) для дифференциации трафика, который должен быть защищен с IP - безопасным шифрованием от трафика, который не требует защиты. Это защищает исходящие пакеты, которые совпадают с Системой управления заявки о разрешении на природопользование (ACE), и гарантирует, что входящие пакеты, которые совпадают с ACE разрешения, имеют защиту.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

Примечание: ACL для трафика VPN использует источник и IP - адреса назначения после Технологии NAT.

Примечание: ACL для трафика VPN должен быть отражен на обоих из узлов VPN.

Примечание: Если существует потребность добавить новую подсеть к защищенному трафику, просто добавьте подсеть/хост к соответствующему object-group и завершите зеркальное изменение на удаленном узле VPN.

Настройте освобождение NAT

Примечание: Конфигурация, которая описана в этом разделе, является дополнительной.

Как правило, не должно быть никакого NAT, выполненного на трафике VPN. Для освобождения того трафика необходимо создать идентичность правило NAT. Идентичность правило NAT просто преобразовывает адрес в тот же адрес.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

Настройте набор преобразований IKEv1

Набор преобразований IKEv1 является комбинацией протоколов безопасности и алгоритмов, которые определяют способ, которым ASA защищает данные. Во время согласований IPsec Security Association (SA) узлы должны определить набор преобразований или предложение, которое является тем же для обоих из узлов. ASA тогда применяет набор преобразований, с которым совпадают, или предложение для создания SA, который защищает потоки данных в списке доступа для той криптокарты.

Для настройки набора преобразований IKEv1 введите **крипто-команду ipsec ikev1 transform-set**:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Настройте Криптокарту и Примените ее к Интерфейсу

Криптокарта определяет Политику IPsec, которая будет договорной в КОНТЕКСТЕ БЕЗОПАСНОСТИ IPSEC, и включает:

- Список доступа для определения пакетов, которые IP - безопасное соединение разрешает и защищает
- Одноранговая идентификация
- Локальный адрес для Трафика IPSec
- Наборы преобразований IKEv1

Например:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Можно тогда применить криптокарту к интерфейсу:

```
crypto map outside_map interface outside
```

Окончательная конфигурация ASA

Вот окончательная конфигурация на ASA:

```
crypto map outside_map interface outside
```

Конфигурация интерфейса командой строки маршрутизатора IOS

Настройте интерфейсы

Если интерфейсы маршрутизатора IOS еще не настроены, то, по крайней мере, LAN и Интерфейсы WAN должны быть настроены. Например:

```
crypto map outside_map interface outside
```

Гарантируйте, что существует подключение и к внутреннему и к внешним сетям, и особенно к удаленному узлу, который будет использоваться для установления туннеля VPN типа «узел-узел». Можно использовать эхо-запрос для проверки основного подключения.

Настройте ISAKMP (IKEv1) политика

Для настройки Политики ISAKMP для соединений IKEv1 введите команду **<priority> crypto isakmp policy** в режим глобальной конфигурации . Например:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **Примечание:** Можно настроить множественные Наборы правил IKE на каждом узле, который участвует в IPSec. Когда Ike согласование начинается, он пытается найти общую политику, которая настроена на обоих из узлов, и он запускается с политики наивысшего приоритета, которая задана на удаленном узле.

Настройте Crypto ISAKMP Key

Для настройки *предварительно разрешенного* ключа проверки подлинности введите **команду crypto isakmp key** в режим глобальной конфигурации:

```
crypto isakmp key cisco123 address 172.16.1.1
```

Настройте ACL для трафика VPN интереса

Используйте расширенное или Именованный список доступа для определения трафика, который должен быть защищен шифрованием. Например:

```
crypto isakmp key cisco123 address 172.16.1.1
```

> **Примечание:** ACL для трафика VPN использует источник и IP - адреса назначения после NAT.

> **Примечание:** ACL для трафика VPN должен быть отражен на обоих из узлов VPN.

Настройте освобождение NAT

> **Примечание:** Конфигурация, которая описана в этом разделе, является дополнительной.

Как правило, не должно быть никакого NAT, выполненного на трафике VPN. Если перегрузка NAT используется, то route-map должен использоваться для освобождения трафика VPN интереса из трансляции. Заметьте, что в access-list, который используется в route-map, должен быть запрещен трафик VPN интереса.

```
crypto isakmp key cisco123 address 172.16.1.1
```

Настройте набор преобразований

Для определения Команды IPsec transform set (приемлемая комбинация протоколов безопасности и алгоритмов), введите **команду crypto ipsec transform-set** в режим глобальной конфигурации. Например:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

Настройте Криптокарту и Примените ее к Интерфейсу

Чтобы создать или модифицировать элемент криптокарты и ввести режим конфигурации криптокарты, введите команду глобальной кофигурации **криптокарты**. Для элемента криптокарты, чтобы быть завершенными, существуют некоторые аспекты, которые должны быть определены как минимум:

- Узлы IPsec, к которым может быть передан защищенный трафик, должны быть определены. Это узлы, с которыми может быть установлен SA. Для определения Узла IPsec в элементе криптокарты введите **команду set peer**.
- Наборы преобразований, которые приемлемы для использования с защищенным трафиком, должны быть определены. Для определения наборов преобразований, которые могут использоваться с элементом криптокарты, ввести **команду set transform-set**.
- Трафик, который должен быть защищен, должен быть определен. Для определения расширенного списка доступа для элемента криптокарты введите команду **адреса соответствия**.

Например:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

Заключительный шаг должен применить ранее определенный набор криптокарты к интерфейсу. Для применения этого введите команду настройки интерфейса **криптокарты**:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Окончательная конфигурация IOS

Вот заключительная конфигурация интерфейса командой строки маршрутизатора IOS:

```
interface GigabitEthernet0/0
```

```
crypto map outside_map
```

Проверка

Перед проверкой, подключен ли туннель и что он передает трафик, необходимо гарантировать, что трафик интереса передается или к ASA или к маршрутизатору IOS.

> **Примечание:** На ASA программное средство пакетного трассировщика, которое совпадает с трафиком интереса, может использоваться для инициирования Туннеля IPSec (такого как **ввод пакетного трассировщика в tcp 10.10.10.10 12345 10.20.10.10 80 подробных**, например).

Проверка фазы 1

Чтобы проверить, подключена ли Фаза 1 IKEv1 на ASA, введите **команду show crypto isakmp sa**. Ожидаемые выходные данные должны видеть состояние **MM_ACTIVE**:

```
ciscoasa# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 172.17.1.1
   Type    : L2L            Role    : responder
   Rekey   : no             State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Чтобы проверить, подключена ли Фаза 1 IKEv1 на IOS, введите **команду show crypto isakmp sa**. Ожидаемые выходные данные должны видеть **Активное состояние**:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Проверка фазы 2

Чтобы проверить, подключена ли Фаза 2 IKEv1 на ASA, введите **команду show crypto ipsec sa**. Ожидаемые выходные данные должны видеть обоих Индекс Параметра безопасности входящего и исходящего трафика (SPI). Если трафик проходит через туннель, необходимо видеть инкремент счетчиков encaps/decaps.

> **Примечание:** Для каждой записи ACL существует отдельный входящий/исходящий созданный SA, который мог бы привести к длинным выходным данным **команды show**

crypto ipsec sa (зависящий от количества первоклассных записей в крипто-ACL).

Например:

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

     access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


     #pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 8A9FE619
     current inbound spi : D8639BD0

   inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
   outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Чтобы проверить, подключена ли Фаза 2 IKEv1 на IOS, введите **команду show crypto ipsec sa**. Ожидаемые выходные данные должны видеть и входящий и исходящий SPI. Если трафик проходит через туннель, необходимо видеть инкремент счетчиков encaps/decaps.

Например:

```
Router#show crypto ipsec sa peer 172.16.1.1
```

```
interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Проверка фазы 1 и 2

В этом разделе описываются команды, которые можно использовать на ASA или IOS для проверки подробных данных для обеих Фаз 1 и 2.

Введите **команду show vpn-sessiondb** в ASA для проверки:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed
```

```
Connection  : 172.17.1.1
Index       : 2                     IP Addr     : 172.17.1.1
Protocol    : IKEv1 IPsec
Encryption  : IKEv1: (1)AES128 IPsec: (1)AES128
Hashing     : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx    : 100500                Bytes Rx    : 101400
Login Time  : 18:06:02 UTC Wed Jul 22 2015
Duration    : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
 Tunnel ID   : 2.1
 UDP Src Port : 500                  UDP Dst Port : 500
 IKE Neg Mode : Main                 Auth Mode    : preSharedKeys
 Encryption  : AES128                Hashing     : SHA1
 Rekey Int (T): 86400 Seconds        Rekey Left(T): 86093 Seconds
 D/H Group   : 2
 Filter Name :

IPsec:
 Tunnel ID   : 2.2
 Local Addr  : 10.10.10.0/255.255.255.0/0/0
 Remote Addr : 10.20.10.0/255.255.255.0/0/0
 Encryption  : AES128                Hashing     : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds         Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes      Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes           Idle TO Left : 26 Minutes
 Bytes Tx    : 100500                Bytes Rx    : 101400
 Pkts Tx     : 1005                  Pkts Rx     : 1014

NAC:
 Reval Int (T): 0 Seconds            Reval Left(T): 0 Seconds
 SQ Int (T)  : 0 Seconds             EoU Age(T)  : 309 Seconds
 Hold Left (T): 0 Seconds            Posture Token:
 Redirect URL :

ciscoasa#
```

Введите **команду show crypto session** в IOS для проверки:

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound: #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

Устранение неполадок

Этот раздел предоставляет сведения, который можно использовать для устранения проблем конфигурации.

> **Примечание:** См. раздел Важные сведения о командах отладки и Устранение проблем системы безопасности IP - Понимание и Использование Документов Cisco команд отладки перед использованием **команд отладки**.

Программное средство средства проверки IPSec LAN-to-LAN

Чтобы автоматически проверить, допустима ли конфигурация IPSec LAN-to-LAN между ASA и IOS, можно использовать программное средство Средства проверки IPSec LAN-to-LAN. Программное средство разработано так, чтобы оно приняло **технологию показа** или **команду show running-config** или от ASA или от маршрутизатора IOS. Это исследует конфигурацию и пытается обнаружить, базировалась ли криптокарта, Туннель IPSec между локальными сетями настроен. Если настроено, это выполняет многоточечную проверку конфигурации и выделяет любые ошибки конфигурации и параметры настройки для туннеля, о котором выполнили бы согласование.

Отладки ASA

Для устранения проблем согласования туннеля IPSec IKEv1 на межсетевом экране ASA можно использовать эти **команды отладки**:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

> **Примечание:** Если количество VPN-туннелей на ASA является значительным, **узел debug crypto condition, B.C.D** команда должна использоваться перед включением отладок для ограничения выходных данных отладки для включения только указанного узла.

Отладки маршрутизатора IOS

Для устранения проблем согласования туннеля IPSec IKEv1 на маршрутизаторе IOS можно использовать эти команды отладки:

```
debug crypto ipsec
debug crypto isakmp
```

> **Примечание:** Если количество VPN-туннелей на IOS является значительным, **одноранговый ipv4 debug crypto condition, B.C.D** должен используется перед включением отладок для ограничения выходных данных отладки для включения только указанного узла.

Совет: См. IPSEC VPN Наиболее распространенного соединения L2L и Удаленного доступа, Устраняющий неполадки Документа Cisco Решений для получения дополнительной информации о том, как устранить неполадки сквозного VPN-соединение.

Ссылки

- Важные сведения о командах отладки
- Устранение проблем IPSec — общие сведения и использование команд debug
- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Средство проверки IPSec LAN-to-LAN
- Cisco Systems – техническая поддержка и документация