Настройка туннеля IPSec – концентратор Cisco VPN 3000 к межсетевому экрану Checkpoint 4.1

Содержание

Введение

Этот документ демонстрирует, как сформировать туннель IPSec с предварительными ключами для соединения 2-х частных сетей:

- Внутренняя частная сеть концентратора Cisco VPN 3000 (192.168.1.x).
- Внутренняя частная сеть межсетевого экрана Checkpoint 4.1 (10.32.50.x).

Предполагается, что поток трафика из внутренней сети концентратора VPN и внутренней сети межсетевого экрана Checkpoint 4.1 в Интернет (представленный здесь сетями 172.18.124.X) существует до начала настройки этой конфигурации.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Концентратор VPN 3000
- Выпуск ПО 2.5.2.F на концентраторе VPN 3000
- Межсетевой экран Checkpoint 4.1

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.

Схема сети

В настоящем документе используется следующая схема сети:

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка концентратора VPN 3000

Для настройки концентратора VPN 3000 выполните следующие шаги.

1. **Выберите Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Modify (Конфигурация > Система > Протоколы туннелирования > IPSec > Предложения IKE > Изменить) для создания предложения обмена ключами в Интернете (IKE) под названием des-sha с хэшированием по алгоритму защищенного хэша (SHA), шифрованием по стандарту DES и 1-й группой Диффи-Хелмана. В поле Lifetime (Срок действия) оставьте значение по умолчанию – 86400 секунд.Примечание:** Допустимый диапазон для Срока действия IKE Концентратора VPN составляет 60-2147483647 секунд.
2. **Выберите Configuration > System > Tunneling Protocols > IPSec > IKE Proposals (Конфигурация > Система > Протоколы туннелирования > IPSec > Предложения IKE). Для активации предложения IKE выберите des-sha и нажмите кнопку Activate (Активировать).**
3. **Выберите Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add (Конфигурация > Система > Протоколы туннелирования > IPSec LAN–LAN > Добавить).**Задайте туннель IPsec to_checkpoint с адресом Checkpoint в качестве второй стороны (Peer). В поле Preshared Key (Предварительно согласованный ключ) введите действующий ключ. В поле Authentication (Аутентификация) выберите ESP/SHA/HMAC-160. В поле Encryption (Шифрование) выберите DES-56. Введите предложение IKE (в этом примере – des-sha), а также локальные и удаленные сети.
4. **Выберите Configuration > Policy Management > Traffic Management > Security Associations > Modify (Конфигурация > Управление политиками > Управление трафиком > Ассоциации безопасности > Изменить). Убедитесь в том, что параметр Perfect Forward Secrecy (Защита от разглашения использованных ключей) установлен в значение Disabled (Отключено), а параметр IPsec Time Lifetime (Срок действия**

временного интервала IPSec) установлен в значение по умолчанию –28800 секунд.**Примечание:** Допустимый диапазон для Срока действия IPSec Концентратора VPN составляет 60-2147483647 секунд.
5. Сохраните конфигурацию.

Настройка межсетевого экрана Checkpoint 4.1

Для настройки межсетевого экрана Checkpoint 4.1 выполните следующие шаги.

1. **Поскольку у производителей различаются установленные по умолчанию сроки действия для IKE и IPSec, щелкните Properties > Encryption (Свойства > Шифрование), чтобы согласовать сроки действия на Checkpoint со значениями по умолчанию на концентраторе VPN.**Срок действия IKE по умолчанию для концентратора VPN – 86400 секунд (1440 минут).Срок действия IPsec по умолчанию для концентратора VPN – 28800 секунд.
2. **Для настройки объекта внутренней (cpinside) сети за устройством Checkpoint выберите Manage > Network objects > New (или Edit) > Network (Управление > Объекты сетей > Создать (Изменить) > Сеть).** Настройка должна согласоваться со значением Remote Network (Удаленная сеть) на концентраторе VPN.
3. **Для редактирования объекта шлюза, который является параметром Peer (Удаленная сторона) для концентратора VPN (устройство Checkpoint RTPCPVPN), выберите Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить).В поле Location (Местоположение) выберите Internal (Внутри). В поле Type (Тип) выберите Gateway (Шлюз). В разделе Modules Installed (Установленные модули) отметьте VPN-1 & FireWall-1 и Management Station (Станция управления).**
4. **Для настройки объекта внешней (inside_cisco) сети за концентратором VPN выберите Manage > Network objects > New (или Edit) > Network (Управление > Объекты сетей > Создать (Изменить) > Сеть).** Настройка должна согласоваться с настройкой «локальной» сети на концентраторе VPN.
5. **Чтобы добавить объект для внешнего шлюза концентратора VPN (cisco_endpoint) выберите Manage > Network objects > New > Workstation (Управление > Сетевые объекты > Создать > Рабочая станция).** Это открытый (Public) интерфейс концентратора VPN.**В разделе Location (Местоположение) выберите External (Снаружи). В поле Type (Тип) выберите Gateway (Шлюз).Примечание:** Не выбирать флажок "VPN-1/FireWall-1".
6. **Для изменения параметров на вкладке VPN оконечного устройства шлюза Checkpoint (именуемого RTPCPVPN) выберите Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить).** На вкладке Domain (Домен) выберите Other (Другой) и затем адрес внутри сети Checkpoint (cpinside) в раскрывающемся списке. **В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit (Редактировать).**
7. **Измените свойства IKE для шифрования DES в соответствии с настройками DES-56 и Encryption Algorithm (Алгоритм шифрования) на концентраторе VPN.**
8. **Измените свойства IKE для хэширования SHA1 в соответствии с алгоритмом SHA/HMAC-160, применяемым на концентраторе VPN.Отмените Aggressive Mode (Агрессивный режим).Отметьте флажок Supports Subnets (Поддерживает подсети).В разделе Authentication Method (Метод аутентификации) отметьте флажок Pre-Shared

Secret (Предварительно согласованный секретный ключ). Эти данные должны соотноситься с режимом аутентификации и предварительно согласованными ключами концентратора VPN.

9. **Выберите Edit Secrets (Редактирование секретных ключей) для приведения предварительно согласованного ключа к фактическому значению параметра Preshared Key концентратора VPN.isakmp key ключ address адрес netmask маска_подсети**
10. **Для редактирования вкладки VPN cisco_endpoint Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить). В разделе Domain (Домен) выберите Other (Другой) и затем укажите внутреннее пространство сети Cisco (inside_cisco). В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit (Редактировать).**
11. **Измените свойства IKE для шифрования DES в соответствии с настройками DES-56, Encryption Algorithm на концентраторе VPN.**
12. **Измените свойства IKE для хэширования SHA1 в соответствии с алгоритмом SHA/HMAC-160, применяемым на концентраторе VPN.**Измените следующие настройки:**Отмените Aggressive Mode (Агрессивный режим).Отметьте флажок Supports Subnets (Поддерживает подсети).В разделе Authentication Method (Метод аутентификации) отметьте флажок Pre-Shared Secret (Предварительно согласованный секретный ключ).** Эти данные должны соотноситься с режимом аутентификации и предварительно согласованными ключами концентратора VPN.
13. **Выберите Edit Secrets (Редактирование секретных ключей) для приведения предварительно согласованного ключа к фактическому значению параметра Preshared Key концентратора VPN.**
14. В окне Policy Editor (Редактор политик) вставьте правило, в качестве источника и назначения для которого используется inside_cisco и cpinside (двустороннее соединение). Задайте параметры: Service=Any, Action=Encrypt и Track=Long.
15. **Затем под заголовком Action (Действие) щелкните зеленый значок Encrypt (Шифровать) и выберите пункт Edit properties (Изменить свойства), чтобы настроить политики шифрования.**
16. **Выберите IKE, затем выберите Edit (Редактировать).**
17. В окне свойств IKE измените эти свойства в соответствии с преобразованиями IPSec для концентратора VPN.**В разделе Transform (Преобразование) выберите Encryption + Data Integrity (ESP) (Шифрование + контроль целостности данных [инкапсулирующая защита содержимого]). Требуется алгоритм шифрования DES, целостность данных SHA1, а разрешенным одноранговым шлюзом должен быть внешний шлюз Cisco (с именем cisco_endpoint). Нажмите кнопку OK.**
18. **После настройки контрольной точки выберите в меню Checkpoint пункты Policy > Install (Политика > Установить), чтобы изменения вступили в силу.**

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Суммирование сетей

При настройке нескольких смежных внутренних сетей в домене шифрования на устройстве Checkpoint последнее может автоматически суммировать сети с точки зрения трафика, представляющего интерес. Если концентратор VPN не настроен соответственно, то туннель с большой вероятностью функционировать не будет. Например, если внутренние сети 10.0.0.0/24 и 10.0.1.0/24 настроены на включение в туннель, они могут быть суммированы как 10.0.0.0/23.

Отладка концентратора VPN 3000

Концентратор VPN может выдавать следующие отладочные сообщения: IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. **Это настраивается в меню Configuration > System > Events > Classes (Конфигурация > Система > События > Классы).**

Сообщения отладки можно просмотреть в разделе Monitoring > Event log > Get Log (Контроль > Журнал событий > Получить журнал).

Для наблюдения за туннельным трафиком между локальными сетями выберите Monitoring > Sessions (Контроль > Сеансы).

Для очистки туннеля выберите Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout (Администрирование > Администрирование сеансов > Сеансы между локальными сетями > Действия – Выход).

Отладка межсетевого экрана Checkpoint 4.1

Примечание: Это было установкой Microsoft Windows NT. Поскольку в окне Policy Editor (Редактор политик) для отслеживания задан параметр Long (Длительно), в окне Log Viewer (Просмотр журнала) отклоненный трафик должен отображаться красным цветом. Для получения более подробных отладочных данных выполните команды:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

и в другом окне:

```
C:\WINNT\FW1\4.1\fwstart
```

Для сброса ассоциаций безопасности на устройстве Checkpoint выполните следующие команды:

```
fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t
ISAKMP_AH_table -x
```

На вопрос Are you sure? (Вы уверены?) ответьте yes (да).

Пример результата отладки

Концентратор Cisco VPN 3000

```
1 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=180 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
```

```
  Responder Cookie(8):  00 00 00 00 00 00 00 00
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       164

7 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=406 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164

9 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=407 172.18.124.157
processing SA payload

10 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=181 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       92

13 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=182 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       2
  Length        :       80

16 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=183 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

18 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=184 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 2 (2)
  Life Time     :       86400 seconds

23 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=185 172.18.124.157
Transform # 2 Decode for Proposal # 1:
  Transform #   :       2
  Transform ID  :       IKE (1)
  Length        :       36

25 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=186 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 2:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  Auth Method   :       Preshared Key (1)
  DH Group      :       Oakley Group 1 (1)
  Life Time     :       86400 seconds

30 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=408 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

35 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=409 172.18.124.157
```

```
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

38 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=410 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

41 02/13/2001 14:21:28.530 SEV=7 IKEDBG/0 RPT=411 172.18.124.157
Oakley proposal is acceptable

42 02/13/2001 14:21:28.530 SEV=9 IKEDBG/1 RPT=107 172.18.124.157
processing vid payload

43 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=412 172.18.124.157
processing IKE SA

44 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=413 172.18.124.157
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

49 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=414 172.18.124.157
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

52 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=415 172.18.124.157
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

55 02/13/2001 14:21:28.530 SEV=7 IKEDBG/28 RPT=3 172.18.124.157
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

56 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=416 172.18.124.157
constructing ISA_SA for isakmp

57 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=417 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

58 02/13/2001 14:21:28.630 SEV=8 IKEDECODE/0 RPT=187 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

64 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=418 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152
```

```
66 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=419 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

68 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=420 172.18.124.157
processing ke payload

69 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=421 172.18.124.157
processing ISA_KE

70 02/13/2001 14:21:28.630 SEV=9 IKEDBG/1 RPT=108 172.18.124.157
processing nonce payload

71 02/13/2001 14:21:28.650 SEV=9 IKEDBG/0 RPT=422 172.18.124.157
constructing ke payload

72 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=109 172.18.124.157
constructing nonce payload

73 02/13/2001 14:21:28.650 SEV=9 IKEDBG/38 RPT=7 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

75 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=110 172.18.124.157
constructing vid payload

76 02/13/2001 14:21:28.650 SEV=9 IKE/0 RPT=26 172.18.124.157
Generating keys for Responder...

77 02/13/2001 14:21:28.650 SEV=8 IKEDBG/0 RPT=423 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

78 02/13/2001 14:21:28.770 SEV=8 IKEDECODE/0 RPT=188 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

84 02/13/2001 14:21:28.770 SEV=8 IKEDBG/0 RPT=424 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

86 02/13/2001 14:21:28.770 SEV=9 IKEDBG/1 RPT=111 172.18.124.157
Processing ID

87 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=425 172.18.124.157
processing hash

88 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=426 172.18.124.157
computing hash

89 02/13/2001 14:21:28.770 SEV=9 IKEDBG/23 RPT=7 172.18.124.157
Starting group lookup for peer 172.18.124.157

90 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=427 172.18.124.157
Found Phase 1 Group (172.18.124.157)

91 02/13/2001 14:21:28.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.157
```

```
Authentication configured for Internal

92 02/13/2001 14:21:28.870 SEV=9 IKEDBG/1 RPT=112 172.18.124.157
constructing ID

93 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=428
construct hash payload

94 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=429 172.18.124.157
computing hash


95 02/13/2001 14:21:28.870 SEV=8 IKEDBG/0 RPT=430 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5)  ... total length : 64

96 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=431 172.18.124.157
Starting phase 1 rekey timer

97 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=189 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       164

104 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=432 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 160

107 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=433 172.18.124.157
processing hash

108 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=434 172.18.124.157
processing SA payload

109 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=190 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       52

112 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=191 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E3
  Length        :       40

116 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=192 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       28

118 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=193 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  HMAC Algorithm:       SHA (2)
```

```
  Encapsulation :       Tunnel (1)

121 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=113 172.18.124.157
processing nonce payload

122 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=114 172.18.124.157
Processing ID

123 02/13/2001 14:21:29.030 SEV=5 IKE/35 RPT=14 172.18.124.157
Received remote IP Proxy Subnet data in ID Payload:
 Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0

125 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=115 172.18.124.157
Processing ID

126 02/13/2001 14:21:29.030 SEV=5 IKE/34 RPT=14 172.18.124.157
Received local IP Proxy Subnet data in ID Payload:
 Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

128 02/13/2001 14:21:29.030 SEV=5 IKE/66 RPT=4 172.18.124.157
IKE Remote Peer configured for SA: L2L: to_checkpoint

129 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=435 172.18.124.157
processing IPSEC SA

130 02/13/2001 14:21:29.030 SEV=7 IKEDBG/27 RPT=1 172.18.124.157
IPSec SA Proposal # 1, Transform # 1 acceptable

131 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=436 172.18.124.157
IKE: requesting SPI!

132 02/13/2001 14:21:29.030 SEV=8 IKEDBG/6 RPT=6
IKE got SPI from key engine: SPI = 0x4d6e483f

133 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=437 172.18.124.157
oakley constucting quick mode

134 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=438 172.18.124.157
constructing blank hash

135 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=439 172.18.124.157
constructing ISA_SA for ipsec

136 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=116 172.18.124.157
constructing ipsec nonce payload

137 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=117 172.18.124.157
constructing proxy ID

138 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=440 172.18.124.157
Transmitting Proxy Id:
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0

141 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=441 172.18.124.157
constructing qm hash

142 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=442 172.18.124.157
SENDING Message (msgid=7755aa11) with payloads :
HDR + HASH (8)  ... total length : 156

144 02/13/2001 14:21:29.270 SEV=8 IKEDECODE/0 RPT=194 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
```

```
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

151 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=443 172.18.124.157
RECEIVED Message (msgid=7755aa11) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 52

153 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=444 172.18.124.157
processing hash

154 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=445 172.18.124.157
loading all IPSEC SAs

155 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=118 172.18.124.157
Generating Quick Mode Key!

156 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=119 172.18.124.157
Generating Quick Mode Key!

157 02/13/2001 14:21:29.270 SEV=7 IKEDBG/0 RPT=446 172.18.124.157
Loading subnet:
  Dst: 192.168.1.0  mask: 255.255.255.0
  Src: 10.32.50.0  mask: 255.255.255.0

159 02/13/2001 14:21:29.270 SEV=4 IKE/49 RPT=6 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3

161 02/13/2001 14:21:29.270 SEV=8 IKEDBG/7 RPT=6
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe3

162 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=447
pitcher: rcv KEY_UPDATE, spi 0x4d6e483f

163 02/13/2001 14:21:29.670 SEV=8 IKEDECODE/0 RPT=195 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

170 02/13/2001 14:21:29.670 SEV=6 IKE/0 RPT=27 172.18.124.157
Duplicate Phase 2 packet detected!

171 02/13/2001 14:21:29.760 SEV=8 IKEDECODE/0 RPT=196 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
  Responder Cookie(8):  24 18 40 A1 3B E4 95 26
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       7755aa11
  Length        :       60

178 02/13/2001 14:21:29.760 SEV=6 IKE/0 RPT=28 172.18.124.157
Duplicate Phase 2 packet detected!
```

```
179 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=448
pitcher: recv KEY_SA_ACTIVE spi 0x4d6e483f

180 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=449
KEY_SA_ACTIVE old rekey centry found with new spi 0x4d6e483f

181 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=5 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

182 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=450 172.18.124.157
IKE SA MM:f2ea8e68 rcv'd Terminate: state MM_ACTIVE_REKEY
flags 0x000000e6, refcnt 1, tuncnt 0

184 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=451 172.18.124.157
IKE SA MM:f2ea8e68 terminating:
flags 0x000000a6, refcnt 0, tuncnt 0

185 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=452
sending delete message

186 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=453 172.18.124.157
constructing blank hash

187 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=454
constructing delete payload

188 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=455 172.18.124.157
constructing qm hash

189 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=456 172.18.124.157
SENDING Message (msgid=87b7c1a4) with payloads :
HDR + HASH (8)  ... total length : 80

191 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=457 172.18.124.157
IKE SA MM:241840a1 rcv'd Terminate: state MM_REKEY_DONE
flags 0x00000082, refcnt 1, tuncnt 1

193 02/13/2001 14:21:29.880 SEV=6 IKE/0 RPT=29 172.18.124.157
Removing peer from peer table failed, no match!

194 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=458
sending delete message

195 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=459 172.18.124.157
constructing blank hash

196 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=460
constructing ipsec delete payload

197 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=461 172.18.124.157
constructing qm hash

198 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=462 172.18.124.157
SENDING Message (msgid=63f2abb8) with payloads :
HDR + HASH (8)  ... total length : 68

200 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=6 172.18.124.157
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

201 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=463 172.18.124.157
IKE SA MM:241840a1 terminating:
flags 0x00000082, refcnt 0, tuncnt 0

202 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=464
```

```
sending delete message

203 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=465 172.18.124.157
constructing blank hash

204 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=466
constructing delete payload

205 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=467 172.18.124.157
constructing qm hash

206 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=468 172.18.124.157
SENDING Message (msgid=d6a00071) with payloads :
HDR + HASH (8)  ... total length : 80

208 02/13/2001 14:21:29.880 SEV=4 AUTH/22 RPT=13
User 172.18.124.157 disconnected

209 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=469
pitcher: received key delete msg, spi 0x2962069b

210 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=470
pitcher: received key delete msg, spi 0xda163fe2

211 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=471
pitcher: received key delete msg, spi 0x4d6e483f

212 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=472
pitcher: received key delete msg, spi 0xda163fe3

213 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=473
pitcher: received a key acquire message!

214 02/13/2001 14:21:29.890 SEV=4 IKE/41 RPT=6 172.18.124.157
IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157
local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0,
SA (L2L: to_checkpoint)

217 02/13/2001 14:21:29.890 SEV=9 IKEDBG/0 RPT=474 172.18.124.157
constructing ISA_SA for isakmp

218 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=475 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1)  ... total length : 84

219 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=197 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       SA (1)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       84

225 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=476 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

227 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=477 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

229 02/13/2001 14:21:30.430 SEV=9 IKEDBG/0 RPT=478 172.18.124.157
```

```
processing SA payload

230 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=198 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       56

233 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=199 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ISAKMP (1)
  #of Transforms:       1
  Length        :       44

236 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=200 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       IKE (1)
  Length        :       36

238 02/13/2001 14:21:30.440 SEV=8 IKEDECODE/0 RPT=201 172.18.124.157
Phase 1 SA Attribute Decode for Transform # 1:
  Encryption Alg:       DES-CBC (1)
  Hash Alg      :       SHA (2)
  DH Group      :       Oakley Group 1 (1)
  Auth Method   :       Preshared Key (1)
  Life Time     :       86400 seconds

243 02/13/2001 14:21:30.440 SEV=7 IKEDBG/0 RPT=479 172.18.124.157
Oakley proposal is acceptable

244 02/13/2001 14:21:30.440 SEV=9 IKEDBG/0 RPT=480 172.18.124.157
constructing ke payload

245 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=120 172.18.124.157
constructing nonce payload

246 02/13/2001 14:21:30.440 SEV=9 IKEDBG/38 RPT=8 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
es: 20000001)

248 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=121 172.18.124.157
constructing vid payload

249 02/13/2001 14:21:30.440 SEV=8 IKEDBG/0 RPT=481 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4)  ... total length : 192

250 02/13/2001 14:21:30.540 SEV=8 IKEDECODE/0 RPT=202 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       KE (4)
  Exchange Type :       Oakley Main Mode
  Flags         :       0
  Message ID    :       0
  Length        :       152

256 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=482 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

258 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=483 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

260 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=484 172.18.124.157
processing ke payload

261 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=485 172.18.124.157
processing ISA_KE

262 02/13/2001 14:21:30.540 SEV=9 IKEDBG/1 RPT=122 172.18.124.157
processing nonce payload

263 02/13/2001 14:21:30.560 SEV=9 IKE/0 RPT=30 172.18.124.157
Generating keys for Initiator...

264 02/13/2001 14:21:30.570 SEV=9 IKEDBG/1 RPT=123 172.18.124.157
constructing ID

265 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=486
construct hash payload

266 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=487 172.18.124.157
computing hash

267 02/13/2001 14:21:30.570 SEV=8 IKEDBG/0 RPT=488 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5)  ... total length : 64

268 02/13/2001 14:21:30.740 SEV=8 IKEDECODE/0 RPT=203 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68

274 02/13/2001 14:21:30.740 SEV=8 IKEDBG/0 RPT=489 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

276 02/13/2001 14:21:30.740 SEV=9 IKEDBG/1 RPT=124 172.18.124.157
Processing ID

277 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=490 172.18.124.157
processing hash

278 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=491 172.18.124.157
computing hash

279 02/13/2001 14:21:30.740 SEV=9 IKEDBG/23 RPT=8 172.18.124.157
Starting group lookup for peer 172.18.124.157

280 02/13/2001 14:21:30.830 SEV=8 IKEDECODE/0 RPT=204 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       ID (5)
  Exchange Type :       Oakley Main Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       0
  Length        :       68
```

```
286 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=31 172.18.124.157
Duplicate Phase 1 packet detected!

287 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=32
MM received unexpected event EV_RESEND_MSG in state MM_I_DONE

288 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=492 172.18.124.157
Found Phase 1 Group (172.18.124.157)

289 02/13/2001 14:21:30.840 SEV=7 IKEDBG/14 RPT=8 172.18.124.157
Authentication configured for Internal

290 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=493 172.18.124.157
Oakley begin quick mode

291 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=494 172.18.124.157
Starting phase 1 rekey timer

292 02/13/2001 14:21:30.840 SEV=4 AUTH/21 RPT=15
User 172.18.124.157 connected

293 02/13/2001 14:21:30.840 SEV=8 IKEDBG/6 RPT=7
IKE got SPI from key engine: SPI = 0x08201539

294 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=495 172.18.124.157
oakley constucting quick mode

295 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=496 172.18.124.157
constructing blank hash

296 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=497 172.18.124.157
constructing ISA_SA for ipsec

297 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=125 172.18.124.157
constructing ipsec nonce payload

298 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=126 172.18.124.157
constructing proxy ID

299 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=498 172.18.124.157
Transmitting Proxy Id:
  Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0

302 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=499 172.18.124.157
constructing qm hash

303 02/13/2001 14:21:30.840 SEV=8 IKEDBG/0 RPT=500 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 184

305 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=205 172.18.124.157
ISAKMP HEADER :         ( Version 1.0 )
  Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
  Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
  Next Payload  :       HASH (8)
  Exchange Type :       Oakley Quick Mode
  Flags         :       1   (ENCRYPT )
  Message ID    :       23bc1709
  Length        :       164

312 02/13/2001 14:21:31.000 SEV=8 IKEDBG/0 RPT=501 172.18.124.157
RECEIVED Message (msgid=23bc1709) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
```

```
th : 156

315 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=502 172.18.124.157
processing hash

316 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=503 172.18.124.157
processing SA payload

317 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=206 172.18.124.157
SA Payload Decode :
  DOI           :       IPSEC (1)
  Situation     :       Identity Only (1)
  Length        :       48

320 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=207 172.18.124.157
Proposal Decode:
  Proposal #    :       1
  Protocol ID   :       ESP (3)
  #of Transforms:       1
  Spi           :       DA 16 3F E4
  Length        :       36

324 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=208 172.18.124.157
Transform # 1 Decode for Proposal # 1:
  Transform #   :       1
  Transform ID  :       DES-CBC (2)
  Length        :       24

326 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=209 172.18.124.157
Phase 2 SA Attribute Decode for Transform # 1:
  Life Time     :       28800 seconds
  Encapsulation :       Tunnel (1)
  HMAC Algorithm:       SHA (2)

329 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=127 172.18.124.157
processing nonce payload

330 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=128 172.18.124.157
Processing ID

331 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=129 172.18.124.157
Processing ID

332 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=504 172.18.124.157
loading all IPSEC SAs

333 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=130 172.18.124.157
Generating Quick Mode Key!

334 02/13/2001 14:21:31.010 SEV=9 IKEDBG/1 RPT=131 172.18.124.157
Generating Quick Mode Key!

335 02/13/2001 14:21:31.010 SEV=7 IKEDBG/0 RPT=505 172.18.124.157
Loading subnet:
  Dst: 10.32.50.0  mask: 255.255.255.0
  Src: 192.168.1.0  mask: 255.255.255.0

337 02/13/2001 14:21:31.010 SEV=4 IKE/49 RPT=7 172.18.124.157
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4

339 02/13/2001 14:21:31.010 SEV=9 IKEDBG/0 RPT=506 172.18.124.157
oakley constructing final quick mode
```

```
340 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=507 172.18.124.157
SENDING Message (msgid=23bc1709) with payloads :
HDR + HASH (8)  ... total length : 76

342 02/13/2001 14:21:31.010 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0xda163fe4

343 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=508
pitcher: rcv KEY_UPDATE, spi 0x8201539

344 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=509
pitcher: recv KEY_SA_ACTIVE spi 0x8201539

345 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=510
KEY_SA_ACTIVE no old rekey centry found with new spi 0x8201539, mess_id 0x0
```

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация