Настройка туннеля IPSec между концентратором Cisco VPN 3000 Concentrator и брандмауэром Checkpoint NG

Содержание

Введение

Этот документ демонстрирует, как настроить Туннель IPSec с предварительными общими ключами для передачи между двумя частными сетями. В данном примере связывающиеся сети 192.168.10.x частная сеть в Cisco VPN 3000 Concentrator и 10.32. x. x частная сеть в Межсетевом экране Следующего поколения (NG) Контрольной точки.

Предварительные условия

Требования

- Трафик из Концентратора VPN и в Контрольной точке NG к Интернету — представленный здесь 172.18.124.x сети — должен течь до начала этой конфигурации.
- Пользователи должны быть знакомы с Согласованием IPsec. Этот процесс может быть разделен на пять этапов, включая две фазы Протокола IKE.Туннель IPSec инициирован

содержательным трафиком. Трафик считается содержательным при передаче между двумя одноранговыми узлами IPsec.На втором этапе обмена ключами (IKE) для равноправных пользователей протокола IPSec выполняется согласование установленной политики сопоставлений безопасности (SA) IKE. Как только узлы аутентифицируются, безопасный туннель создан с Протоколом ISAKMP.В 2-ой фазе протокола IKE Узлы IPsec используют защищенный туннель с аутентификацией для согласовывания преобразования контекстов безопасности IPsec. Согласование общей политики определяет то, как будет установлен туннель IPSec.Туннель IPSec создан, и данные передаются между узлами IPSec на основании параметров IPSec, настроенных в наборах преобразования IPSec.Разъединение туннеля IPSec выполняется при удалении сопоставлений безопасности (IPSec SA) или по истечении срока их действия.

Используемые компоненты

При разработке и тестировании этой конфигурации использовались следующие версии программного и аппаратного обеспечения:

- Концентратор серии VPN 3000 3.5.2
- Межсетевой экран контрольной точки NG

Условные обозначения

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

Схема сети

В настоящем документе используется следующая схема сети:

Примечание: Схема IP-адресации, используемая в этой конфигурации, не юридически маршрутизируема в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Конфигурации

Настройка концентратора VPN 3000

Для настройки VPN-концентратора 3000 выполните следующие действия:

1. Перейдите **к Configuration> System> Tunneling Protocols> IPsec LAN-to-LAN** для настройки сеанса между локальными сетями. Установите параметры для аутентификации и алгоритмы IKE, предварительный общий ключ, IP - адрес адресуемой точки и параметры подключения по локальной и удаленной сетям. **Щелкните "Применить".**В этой конфигурации аутентификация была установлена как ESP-MD5-HMAC, и шифрование было установлено как 3DES.
2. Перейдите **к Configuration> System> Tunneling Protocols> IPsec> Предложения ike** и установите необходимые параметры.Выберите Предложение ike IKE-3DES-MD5 и проверьте параметры, выбранные для предложения. Нажмите **Apply** для настройки сеанса между локальными сетями.Это параметры для этой конфигурации:

3. Перейдите к> **Security Configuration> Policy Management> Traffic Management Ассоциации**, выберите IPSec SA, созданный для сеанса, и проверьте параметры КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC, выбранные для сеанса между локальными сетями.В этой конфигурации название сеанса между локальными сетями было "Контрольной точкой", таким образом, КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC был создан автоматически как "L2L: Контрольная точка".Это параметры для этого SA:

Настройте контрольную точку NG

Сетевые объекты и правила определены на Контрольной точке NG для составления политики, которая принадлежит конфигурации VPN, которая будет установлена. Эта политика тогда установлена с Редактором политики Контрольной точки NG для завершения стороны Контрольной точки NG конфигурации.

1. Создайте эти два сетевых объекта для сети Checkpoint NG и сети VPN Concentrator, которая зашифрует представляющий интерес трафик.для создания объектов выберите **Manage> Network Objects**, затем выберите **New> Network**. Введите соответствующую информацию о сети, затем нажмите OK.Эти примеры показывают установленные из сетевых объектов, названных CP_inside (внутренняя сеть Контрольной точки NG) и CONC_INSIDE (внутренняя сеть Концентратора VPN).
2. Перейдите **Manage> Network Objects** и **New> Workstation** выбора для создания объектов рабочей станции для устройств VPN, Контрольной точки NG и Концентратора VPN.**Примечание:** Можно использовать объект рабочей станции Контрольной точки NG, созданный во время настройки NG начальной настройки Checkpoint. Выберите опции, чтобы установить рабочую станцию как шлюз и взаимодействующее устройство VPN, затем нажать **OK**.Эти примеры показывают установленные из объектов, названных ciscocp (Контрольная точка NG) и CISCO_CONC (VPN 3000 Concentrator):
3. Перейдите **Manage> Network Objects> Edit** для открытия Окна Workstation Properties для рабочей станции Контрольной точки NG (ciscocp в данном примере). Выберите **Topology** от выборов на левой части окна, затем выберите сеть, которая будет зашифрована. Нажмите **Edit** для установки интерфейсных свойств.В данном примере CP_inside является внутренней сетью Контрольной точки NG.
4. На Интерфейсном Окне свойств выберите опцию, чтобы определять рабочую станцию как внутреннюю, затем задать соответствующий IP-адрес. **Нажмите кнопку OK.**Показанные выборы топологии определяют рабочую станцию как внутреннюю и задают IP-адреса позади интерфейса CP_inside:
5. От Окна Workstation Properties выберите внешний интерфейс на Контрольной точке NG, которая выводит к Интернету, затем нажмите **Edit** для установки интерфейсных свойств. Выберите опцию, чтобы определять топологию как внешнюю, затем нажать **OK**.
6. От Окна Workstation Properties на Контрольной точке NG выберите **VPN** от выборов на левой части окна, затем выберите параметры IKE для шифрования и алгоритмы аутентификации. Нажмите **Edit** для настройки Свойств ike.
7. Заставьте Свойства ike совпадать со свойствами на Концентраторе VPN.В данном примере выберите параметр шифрования для **3DES** и опцию хеширования для **MD5**.
8. Выберите параметр проверки подлинности для **Предварительных общих ключей**, затем нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ быть совместимым с предварительным общим ключом на Концентраторе VPN. Нажмите **Edit**

для ввода ключа как показано, затем нажмите **Set**, **OK**.

9. Из окна Свойств ike нажмите **Advanced...** и измените эти настройки:Отмените выбор опции для **Поддержки агрессивного режима**.Выберите опцию для **обмена ключами Поддержки для подсетей**.Когда вы будете закончены, **нажмите OK**, **OK**.
10. Перейдите **Manage> Network Objects> Edit** для открытия Окна Workstation Properties для Концентратора VPN. Выберите **Topology** от выборов на левой части окна для ручного определения домена VPN.В данном примере CONC_INSIDE (внутренняя сеть Концентратора VPN) определен как домен VPN.
11. Выберите **VPN** от выборов на левой части окна, затем выберите **IKE** как схему шифрования. Нажмите **Edit** для настройки Свойств ike.
12. Заставьте Свойства ike отражать текущую конфигурацию на Концентраторе VPN.В данном примере, набор параметр шифрования для **3DES** и опция хеширования для **MD5**.
13. Выберите параметр проверки подлинности для **Предварительных общих ключей**, затем нажмите **Edit Secrets** для установки предварительного общего ключа. Нажмите **Edit** для ввода ключа как показано, затем нажмите **Set**, **OK**.
14. Из окна Свойств ike нажмите **Advanced...** и измените эти настройки:Выберите Группу Диффи-Хеллмана, соответствующую Свойствам ike.Отмените выбор опции для **Поддержки агрессивного режима**.Выберите опцию для **обмена ключами Поддержки для подсетей**.Когда вы будете закончены, **нажмите OK**, **OK**.
15. Выберите **Rules> Add Rules> Top** для настройки правил шифрования для политики. В Окне редактора политики вставьте правило с источником как CP_inside (внутренняя сеть Контрольной точки NG) и назначение как CONC_INSIDE (внутренняя сеть Концентратора VPN). Значения набора для **Сервиса = Любой**, **Действие = Шифрует**, и **Дорожка = Журнал**. Когда вы добавили Зашифровать раздел Действия правила, щелкаете правой кнопкой мыши **Действие** и выбираете **Edit Properties**.
16. Выберите **IKE** и нажмите **Edit**.
17. На окне IKE Properties изменитесь, свойства для согласия с Концентратором VPN преобразовывают.Установите опцию Transform в **Шифрование + Целостность данных (ESP)**.Установите алгоритм шифрования в **3DES**.Установите целостность данных в **MD5**.Заставьте Позволенный Шлюз одноранговой сети совпадать с Концентратором VPN (CISCO_CONC).**По завершении нажмите кнопку OK.**
18. После того, как Контрольная точка NG настроена, сохраните политику и выберите **Policy> Install** для включения его.Замечания о ходе работы показов окна установки как политика скомпилированы.Когда окно установки указывает, что установка политики завершена, нажмите **Close** для завершения процедуры.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Проверьте передачу по сети

Для тестирования связи между этими двумя частными сетями можно инициировать эхо-запрос от одной из частных сетей к другой частной сети. В этой конфигурации эхо-запрос передавался со стороны Контрольной точки NG (10.32.50.51) к сети VPN Concentrator (192.168.10.2).

Обзорный статус туннеля на контрольной точке NG

Для просмотра статуса туннеля перейдите к Редактору политики и выберите **Window> System Status**.

Обзорный статус туннеля на концентраторе VPN

Для проверки статуса туннеля на Концентраторе VPN перейдите **к Administration> Administer Sessions**.

Под Сеансами между локальными сетями выберите имя соединения для Контрольной точки, чтобы посмотреть детали на созданных SA, и количество пакетов передало/получило.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Примечание: Трафиком не должен быть PATed через Туннель IPSec с помощью открытого IP - адреса Концентратора VPN (внешний интерфейс). В противном случае, туннельные сбои. Так, IP-адрес, используемый для того, чтобы Похлопать, должен быть адресом кроме адреса, настроенного на внешнем интерфейсе.

Суммирование сетей

Когда множественный смежный, внутренние сети настроены в домене шифрования на Контрольной точке, устройство может автоматически суммировать сети относительно представляющего интерес трафика. 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, чтобы быть включенными в туннель, эти сети могут быть суммированы к 10.0.0.0 / 23.

Отладка для NG контрольной точки

Для просмотра журналов выберите **Window> Log Viewer**.

Отладка концентратора виртуальной частной сети (VPN)

Для включения отладок на Концентраторе VPN перейдите **к Configuration> System> Events> Classes**. Позвольте AUTH, AUTHDBG, IKE, IKEDBG, IPSEC и IPSECDBG для степеней серьезности ошибки регистрировать как 1 - 13. Для просмотра отладок выберите **Monitoring> Filterable Event Log**.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
```

```
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
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

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
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
```

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3 26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp 27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84 29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send IOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157] Starting

group lookup for peer 172.18.124.157 54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10 AUTH_Open() returns 9 55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9 56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174) 57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648) 58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0) 59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1 60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(51a6b48, 0, 0) 61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018 62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0) 63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0) 64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 30000 65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0) 66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156) 67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48) 68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 xmit_cnt = 1 69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB_Xmt(51a6b48) 70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB_Match(51a6b48, 3eb7ab0) 71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0) 72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298) 73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48) 74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10 AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.157 78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 **90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED** 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None 92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157 Keep-alives configured on but peer does not support keep-alives (type = None) 93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group [172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr **114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157] IKE Remote Peer configured for SA: L2L: Checkpoint** 115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157] processing IPSEC SA **116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA**

Proposal # 1, Transform # 1 acceptable 117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI! 118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300 122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg! 123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPI 305440147 124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593 125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode 126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash 127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec 128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload 129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID **130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0** 134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash 135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) ... total length : 152 137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48 139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157 Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! **143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959** 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msghdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA 158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255 159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success 160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147 Processing KEY_UPDATE msg! 165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148 Update inbound SA addresses 166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149 key_msghdr2secassoc(): Enter 167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter configured 168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter 169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success 170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY_ADD msg for SA: SPI = 0x0df37959 171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY_UPDATE, spi 0x1234a593 **172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED (msgid=54796f76)**

Дополнительные сведения

- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Series Client
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems