Пример конфигурации L2TP через подключение IPsec между ПС Windows 2000/XP и PIX/ASA 7.2 с использованием общих ключей доступа

Содержание

Введение

Этот документ описывает, как настроить протокол туннелирования на уровне 2 (L2TP) через IP-безопасность (IPsec) от удаленного Microsoft Windows 2000/2003 и клиентов XP к офису корпорации Устройства безопасности PIX с помощью предварительных общих ключей с сервером RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года для проверки подлинности пользователя. Дополнительные сведения об IAS см. в документе Microsoft - контрольный список: Настройка IAS для телефонного соединения и VPN-допуска .

Основной целью настройки протокола L2TP совместно с IPsec в сценарии удаленного доступа является возможность удаленного пользователя получить VPN-доступ через общую IP-сеть без использования шлюза или выделенной линии. Это позволяет получить удаленный доступ практически из любого места при наличии обычной телефонной сети. Помимо этого, единственным требуемым клиентом для VPN-доступа является использование Windows 2000 совместно с системой Microsoft удаленного доступа к сети (DUN). Дополнительное клиентское программное обеспечение, такое как Cisco VPN Client, не требуется.

Этот документ также описывает использование Адаптивного менеджера устройств безопасности (ASDM) для настройки системы безопасности серии PIX 500 для протокола L2TP через IPsec.

Примечание: Протокол туннелирования уровня 2 (L2TP) через IPSec поддерживается на Выпуске ПО межсетевого экрана Cisco Secure PIX 6.x и позже.

Для настройки L2TP через IPsec между PIX 6.x и Windows 2000 см. Конфигурация L2TP через IPsec между межсетевым экраном PIX и Windows 2000 PC с помощью сертификатов.

Для настройки L2TP через IPsec от удаленного Microsoft Windows 2000, и клиенты XP к корпоративному узлу с помощью зашифрованного метода, обратитесь к L2TP Настройки по IPsec от Windows 2000 или Клиента XP к концентратору Cisco VPN серии 3000 Использование Предварительных общих ключей.

Предварительные условия

Требования

Перед созданием безопасного туннеля необходимо установить IP-соединение между узлами.

Проверьте, чтобы UDP-порт 1701 не был заблокирован по всей длине маршрута соединения.

Используйте только ту туннельную группу и политику группы, которые заданы по умолчанию системой Cisco PIX/ASA. Группы и групповая политика, установленные пользователем, не функционируют.

Примечание: Если или Cisco VPN Client 3.x или Cisco VPN 3000 Client 2.5 установлены, устройство безопасности не устанавливает L2TP/ТУННЕЛЬ IPSEC с Windows 2000. **Отключите систему обслуживания Cisco VPN для Cisco VPN Client 3.x или систему обслуживания ANetIKE для Cisco VPN 3000 Client 2.5, используя панель Services в Windows 2000. Для этого выберите Start > Programs > Administrative Tools > Services, запустите IPsec Policy Agent Service, используя панель Services, и перезагрузите компьютер.**

Используемые компоненты

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

- Система безопасности PIX 515E с программным обеспечением версии 7.2(1) или более

поздних
- Адаптивный менеджер устройств безопасности версии 5.2(1) или более поздних
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional с SP2
- Windows 2003 Server с IAS

Примечание: При обновлении PIX 6.3 к версии 7.x удостоверьтесь, что вы установили SP2 в Windows XP (Клиент L2TP).

Примечание: Информация в документе также допустима для Устройства обеспечения безопасности ASA.

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.

Родственные продукты

Эта конфигурация также может быть использована с системой безопасности Cisco ASA 5500 версии 7.2(1) или более поздней.

Условные обозначения

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

Общие сведения

Для настройки L2TP через IPsec выполните следующие действия.

1. Настройте режим перемещения IPsec для запуска IPsec с помощью L2TP.Клиент Windows 2000 L2TP/IPsec использует режим перемещения IPsec. Зашифрована только полезная нагрузка IP, в то время как оригинальные IP-заголовки остаются без изменения. Среди преимуществ такого режима можно отметить добавление небольшого числа байтов в каждый из пакетов и возможность устройств сети с открытым доступом видеть конечный источник и назначение пакета. Следовательно, чтобы подключить клиентов Windows 2000 L2TP/IPsec к системе безопасности необходимо настроить режим перемещения IPsec для изменения (см. этап 2 в настройке ASDM). С помощью этой функции (перемещения) можно активировать специальные процедуры (например, QoS) в промежуточной сети, основанной на данных IP-заголовков. Несмотря на это, заголовок уровня 4 зашифрован, что ограничивает обзор пакета. К сожалению, при передаче IP-заголовка открытым текстом, режим перемещения позволяет атакующему выполнить некоторый анализ трафика.
2. Настройте L2TP в соответствии с параметрами группы виртуальной частной коммутируемой сети (VPDN).

Настройка L2TP с IPsec поддерживает сертификаты, которые используют общие ключи или методы подписи RSA, а также использование динамических (в отличие от статических)

криптографических карт. Предварительно задаваемые общие ключи доступа используются при аутентификации для установки протокола L2TP через туннель IPsec.

Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация клиента Windows L2TP/IPsec
- Конфигурация сервера L2TP PIX
- Конфигурация L2TP с помощью ASDM
- Конфигурация Microsoft Windows 2003 Server с IAS

Конфигурация клиента Windows L2TP/IPsec

Выполните эти шаги для настройки L2TP через IPsec на Windows 2000. Поскольку Windows XP пропускает шаги 1 и 2 и запускается с шага 3:

1. Добавьте это значение регистра к своей машине Windows 2000:`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. Добавьте это значение регистрации к следующему ключу:`Value Name: ProhibitIpSec Data Type: REG_DWORD Value: 1`**Примечание:** В некоторых случаях (Windows XP Sp2), добавление этого ключа **(Значение: 1)**, кажется, ломает соединение, поскольку оно заставляет коробку XP выполнить согласование о L2TP только, а не L2TP с IP - безопасным соединением. Добавление политики IPsec в сочетании с данным ключом регистрации является обязательным условием. `error 800 (: 1)` для установки соединения.**Примечание:** Необходимо перезапустить Windows 2000/2003 или машину XP для изменений для вступления в силу. По умолчанию клиент Windows выполнит ряд попыток использовать IPsec со Службой сертификации (CA). Конфигурация данного ключа регистрации предотвращает возникновение таких ситуаций. Теперь можно настроить политику IPsec на устройстве, работающем под управлением Windows, для соответствия необходимым параметрам на PIX/ASA. Дополнительную информацию касательно поэтапной конфигурации политики IPsec см. Настройка соединения

L2TP/IPSec с помощью предустановленного ключа аутентификации (Q240262).Дополнительную информацию см. в документе Настройка общего ключа для использования в сетевых подключениях с протоколом туннелирования второго уровня на устройствах Windows XP (Q281555)\ .

3. Создайте сетевое подключение.
4. **В меню "Network and Dial-up Connections" нажмите правой кнопкой мыши на подключение и выберите Properties.Перейдите на вкладку "Security" и нажмите Advanced.** Выберите необходимые протоколы (см. рис.).
5. **Примечание:** Это действие применимо только к Windows XP.**Нажмите IPSec Settings, проверьте наличие параметра Use pre-shared key for authentication и введите ключ для установки общего предустановленного ключа.**В этом примере test используется в качестве предустановленного общего ключа доступа.

Конфигурация сервера L2TP PIX

PIX 7.2

```
pixfirewall#show run PIX Version 7.2(1) ! hostname
pixfirewall domain-name default.domain.invalid enable
password 8Ry2YjIyt7RRXU24 encrypted names ! !---
Configures the outside and inside interfaces. interface
Ethernet0 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 ! interface Ethernet1 nameif
inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0 nat
(inside) 0 access-list nonat pager lines 24 logging
console debugging mtu outside 1500 mtu inside 1500 !---
Creates a pool of addresses from which IP addresses are
assigned !--- dynamically to the remote VPN Clients. ip
local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0 no failover asdm image flash:/asdm-521.bin
no asdm history enable arp timeout 14400 !--- The global
and nat command enable !--- the Port Address Translation
(PAT) using an outside interface IP !--- address for all
outgoing traffic. global (outside) 1 interface nat
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
0:05:00 absolute !--- Create the AAA server group "vpn"
and specify its protocol as RADIUS. !--- Specify the IAS
server as a member of the "vpn" group and provide its !-
-- location and key. aaa-server vpn protocol radius aaa-
server vpn host 10.4.4.2 key radiuskey !--- Identifies
the group policy as internal. group-policy
DefaultRAGroup internal !--- Instructs the security
appliance to send DNS and !--- WINS server IP addresses
to the client. group-policy DefaultRAGroup attributes
wins-server value 10.4.4.99 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec default-domain value cisco.com !--- Configure
usernames and passwords on the device !--- in addition
to using AAA. !--- If the user is an L2TP client that
```

```
uses Microsoft CHAP version 1 or !--- version 2, and the
security appliance is configured !--- to authenticate
against the local !--- database, you must include the
mschap keyword. !--- For example, username <username>
password <password> mschap. username test password
DLaUiAX3l78qgoB5c7iVNw== nt-encrypted vpn-tunnel-
protocol l2tp-ipsec http server enable http 0.0.0.0
0.0.0.0 inside no snmp-server location no snmp-server
contact snmp-server enable traps snmp authentication
linkup linkdown coldstart !--- Identifies the IPsec
encryption and hash algorithms !--- to be used by the
transform set. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac !--- Since the
Windows 2000 L2TP/IPsec client uses IPsec transport
mode, !--- set the mode to transport. !--- The default
is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport !--- Specifies the
transform sets to use in a dynamic crypto map entry.
crypto dynamic-map outside_dyn_map 20 set transform-set
TRANS_ESP_3DES_MD5 !--- Requires a given crypto map
entry to refer to a pre-existing !--- dynamic crypto
map. crypto map outside_map 20 ipsec-isakmp dynamic
outside_dyn_map !--- Applies a previously defined crypto
map set to an outside interface. crypto map outside_map
interface outside crypto isakmp enable outside crypto
isakmp nat-traversal 20 !--- Specifies the IKE Phase I
policy parameters. crypto isakmp policy 10
authentication pre-share encryption 3des hash md5 group
2 lifetime 86400 !--- Creates a tunnel group with the
tunnel-group command, and specifies the local !---
address pool name used to allocate the IP address to the
client. !--- Associate the AAA server group (VPN) with
the tunnel group. tunnel-group DefaultRAGroup general-
attributes address-pool clientVPNpool authentication-
server-group vpn !--- Link the name of the group policy
to the default tunnel !--- group from tunnel group
general-attributes mode. default-group-policy
DefaultRAGroup !--- Use the tunnel-group ipsec-
attributes command !--- in order to enter the ipsec-
attribute configuration mode. !--- Set the pre-shared
key. !--- This key should be the same as the key
configured on the Windows machine. tunnel-group
DefaultRAGroup ipsec-attributes pre-shared-key * !---
Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode. tunnel-group DefaultRAGroup ppp-
attributes no authentication chap authentication ms-
chap-v2 telnet timeout 5 ssh timeout 5 console timeout 0
! 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 prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd : end
```

Конфигурация L2TP с помощью ASDM

Для настройки системы безопасности на принятие протокола L2TP через подключения IPsec

выполните следующие действия:

1. Добавьте набор преобразований IPsec и укажите IPsec для использования транспортного режима вместо туннельного. **Для этого выберите Configuration > VPN > IPSec > Transform Sets и нажмите Add.** Отобразится окно "Transform Sets".
2. Чтобы добавить набор преобразований, выполните следующие действия:Введите имя набора преобразований.Выберите способы ESP шифрования и ESP аутентификации.**Выберите режим, например Transport.Нажмите кнопку OK.**
3. Чтобы настроить способ назначения адреса, выполните следующие действия. Ниже приведен пример использования пулов IP-адресов.**Выберите Configuration > VPN > IP Address Management > IP Pools.Нажмите Add.** Появится окно Add IP Pool.Введите имя нового пула IP-адреса.Введите начальный и конечный IP-адреса.**Введите маску подсети и нажмите OK.**
4. **Выберите Configuration > VPN > General > Group Policy, чтобы настроить L2TP через IPsec в качестве действительного протокола туннелирования VPN для политики группы.** Отобразится окно "Group Policy" политика группы.
5. **Выберите политику группы (DiffGrpPolicy) и нажмите Edit.**Отображается диалоговое окно "Edit Group Policy". **Проверьте L2TP over IPSec, чтобы включить протокол для политики группы, затем нажмите OK.**
6. Чтобы назначить пул IP-адресов для туннельной группы, выполните следующие действия:**Выберите Configuration > VPN > General > Tunnel Group.**При появлении окна "Tunnel Group" выберите в таблице туннельную группу (DefaultRAGroup).**Нажмите Edit.**
7. В случае отображения окна "Edit Tunnel Group" выполните следующие действия:От вкладки "General" перейдите к вкладке "Client Address Assignment".В области "Address Pools" выберите адресный пул, чтобы назначить туннельную группу.**Нажмите Add.** В окне "Assigned Pools" отобразится адресный пул.
8. **Чтобы установить предустановленный ключ, перейдите к вкладке "IPSec", введите Pre-shared Key и нажмите OK.**
9. L2TP через IPsec использует протоколы аутентификации PPP. На вкладке "PPP" туннельной группы укажите протоколы, разрешенные для соединений PPP. **Для аутентификации выберите протокол MS-CHAP-V1.**
10. Укажите способ аутентификации пользователей, которые пытаются установить соединения L2TP через IPsec.Можно настроить систему безопасности для использования сервера аутентификации или собственной локальной базы данных. Для этого перейдите к вкладке "Authentication" туннельной группы. По умолчанию система безопасности использует собственную локальную базу данных. В раскрывающемся списке "Authentication Server Group" отображено "LOCAL". Чтобы использовать сервер аутентификации, выберите его в списке.**Примечание:** Устройство безопасности только поддерживает PAP проверок подлинности PPP и версии 1 и 2 Microsoft CHAP на локальной базе данных. EAP и CHAP выполняются с помощью прокси-серверов аутентификации. Следовательно, если удаленный пользователь относится к туннельной группе, настроенной на EAP или CHAP, а система безопасности настроена на использование локальной базы данных, подключение не будет установлено.**Примечание:** Выберите **Configuration> VPN> General> Tunnel Group** для возвращения к конфигурации туннельной группы так, чтобы можно было связать групповую политику с туннельной группой и включить Туннельную группу, Переключающуюся (дополнительный). **При появлении окна "Tunnel Group" выберите туннельную группу и нажмите Edit.Примечание:** Коммутация

Туннельной группы позволяет устройству безопасности привязать других пользователей, которые устанавливают L2TP по IP - безопасным соединениям с другими туннельными группами. Так как у каждой туннельной группы имеется свой AAA-сервер и пулы IP-адресов, пользователи могут выполнять аутентификацию с использованием свойственных их туннельной группе способов. С помощью данной функции, вместо отправки отдельного имени пользователя, пользователь отправляет имя пользователя и имя группы в формате username@group_name, где "@" является настраиваемым разделителем, а имя группы – именем туннельной группы, настраиваемым в системе безопасности.**Примечание:** Коммутация Туннельной группы включена обработкой Strip Group, которая позволяет устройству безопасности выбрать туннельную группу для подключений пользователя путем получения имени группы из имени пользователя, представленного Клиентом VPN. Далее система безопасности отправляет ту часть имени пользователя, которая содержит данные пользователя, необходимые для авторизации и аутентификации. В противном случае (если функция отключена), система безопасности отправляет имя пользователя полностью, включая именованную область. **Чтобы включить Tunnel Group Switching, проверьте Strip the realm from username before passing it on to the AAA server (Отделить именованную область от имени пользователя перед передачей AAA-серверу) и проверьте Strip the group from username before passing it on to the AAA server (Отделить группу от имени пользователя перед передачей AAA-серверу). Затем нажмите кнопку OK.**

11. Чтобы создать пользователя в локальной базе данных, выполните следующие действия:**Выберите Configuration >Properties > Device Administration > User Accounts.Нажмите Add.Если пользователь является клиентом L2TP, использующим Microsoft CHAP версии 1 или 2, а система безопасности настроена на аутентификацию согласно локальной базе данных, необходимо проверить User Authenticated using MSCHAP, чтобы включить MSCHAP.Нажмите кнопку OK.**
12. **Выберите Configuration > VPN > IKE > Policies и нажмите Add, чтобы создать политику IKE для этапа I. Нажмите OK, чтобы продолжить.**
13. (Дополнительно) При попытке различных клиентов L2TP, помимо устройства NAT, установить соединения L2TP через IPsec с системой безопасности, необходимо включить просмотр NAT, чтобы пакеты ESP передавались через одно или более устройств NAT. Для этого выполните следующие действия:**Выберите Configuration > VPN > IKE > Global Parameters.Убедитесь, что на интерфейсе включено ISAKMP.Проверьте Enable IPSec over NAT-T.Нажмите кнопку OK.**

Конфигурация Microsoft Windows 2003 Server с IAS

Чтобы настроить Microsoft Windows 2003 server с IAS, выполните следующие действия.

Примечание: Эти шаги предполагают, что IAS уже установлен на локальном компьютере. В противном случае добавьте это через **Панель управления> Добавления/удаления программы**.

1. **Выберите Administrative Tools > Internet Authentication Service и нажмите правой кнопкой мыши RADIUS Client, чтобы добавить нового клиента RADIUS. После ввода данных нажмите OK.**В данном примере показан клиент, именем которого является "Pix", а IP-адресом – 10.4.4.1. **Для Клиента-Поставщика установлено RADIUS Standard,**

единый секретный ключ – radiuskey.
2. Выберите Remote Access Policies, нажмите Connections to Other Access Servers правой кнопкой мыши и выберите Properties.
3. Убедитесь, что выбран параметр для Grant Remote Access Permissions.
4. Нажмите кнопку Edit Profile и установите флажки в следующих настройках:На вкладке "Authentication" установите Unencrypted authentication (PAP, SPAP).Убедитесь, что на вкладке Encryption выбран параметр No Encryption.Закончив все действия, нажмите кнопку OK.
5. Выберите Administrative Tools > Computer Management > System Tools > Local Users and Groups, правой кнопкой мыши нажмите Users и выберите New Users, чтобы добавить пользователя к учетной записи локального компьютера.
6. Добавьте пользователя с Паролем Cisco password1 и проверьте эти данные профиля:Убедитесь, что на вкладке General выбран параметр Password Never Expired вместо параметра User Must Change Password.На Вкладке наборный (телефонный) доступ выберите опцию для, Предоставляют доступ (или оставьте настройку по умолчанию доступа Контроля через Политику Удаленного доступа).Закончив все действия, нажмите кнопку OK.

Расширенная проверка подлинности для L2TP по IPSec с помощью Active Directory

Используйте эту конфигурацию на ASA, чтобы позволить аутентификации для соединения L2tp иметь место из Active Directory:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)# authentication pap
```

Кроме того, на клиенте L2tp перейдите к (Пользовательским) Параметрам настройки Дополнительной безопасности и выберите только опцию для Незашифрованного пароля (PAP).

Проверка

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

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- show crypto ipsec sa – отображает все текущие IKE ассоциации безопасности (SAs) узла.

```
pixfirewall#show crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1 access-list 105 permit ip host 172.16.1.1 host 192.168.0.2 local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0) remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701) current_peer: 192.168.0.2, username: test dynamic allocated peer ip: 10.4.5.15 #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23 #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0 #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: C16F05B8 inbound esp sas: spi:
```

```
0xEC06344D (3959829581) transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, }
slot: 0, conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec):
3335 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xC16F05B8
(3245278648) transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, } slot: 0,
conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV
size: 8 bytes replay detection support: Y
```

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE узла.**`pixfirewall#`**`show crypto isakmp sa`** `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: 192.168.0.2 Type : user Role : responder Rekey : no State : MM_ACTIVE`
- **show vpn-sessiondb – содержит фильтры протокола, используемые для просмотра подробной информации о соединениях L2TP через IPsec. Полной командой, вводимой в глобальном режиме конфигурации, является show vpn-sessoindb detailed remote filter protocol l2tpOverIpsec.**В следующем примере приведены данные отдельного соединения L2TP через IPsec:`pixfirewall#`**`show vpn-sessiondb detail remote filter protocol L2TPOverIPSec`**
```
Session Type: Remote Detailed Username : test Index : 1 Assigned IP : 10.4.5.15 Public IP :
192.168.0.2 Protocol : L2TPOverIPSec Encryption : 3DES Hashing : MD5 Bytes Tx : 1336 Bytes
Rx : 14605 Client Type : Client Ver : Group Policy : DefaultRAGroup Tunnel Group :
DefaultRAGroup Login Time : 18:06:08 UTC Fri Jan 1 1993 Duration : 0h:04m:25s Filter Name :
NAC Result : N/A Posture Token: IKE Sessions: 1 IPSec Sessions: 1 L2TPOverIPSec Sessions: 1
IKE: Session ID : 1 UDP Src Port : 500 UDP Dst Port : 500 IKE Neg Mode : Main Auth Mode :
preSharedKeys Encryption : 3DES Hashing : MD5 Rekey Int (T): 28800 Seconds Rekey Left(T):
28536 Seconds D/H Group : 2 IPSec: Session ID : 2 Local Addr :
172.16.1.1/255.255.255.255/17/1701 Remote Addr : 192.168.0.2/255.255.255.255/17/1701
Encryption : 3DES Hashing : MD5 Encapsulation: Transport Rekey Int (T): 3600 Seconds Rekey
Left(T): 3333 Seconds Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Bytes Tx : 1336
Bytes Rx : 14922 Pkts Tx : 25 Pkts Rx : 156 L2TPOverIPSec: Session ID : 3 Username : test
Assigned IP : 10.4.5.15 Encryption : none Auth Mode : msCHAPV1 Idle Time Out: 30 Minutes
Idle TO Left : 30 Minutes Bytes Tx : 378 Bytes Rx : 13431 Pkts Tx : 16 Pkts Rx : 146
```

Устранение неполадок

В данном разделе представлена информация по устранению неполадок конфигурации. Также показан пример выходных данных команды debug.

Команды для устранения неполадок

Определенные команды поддерживаются Интерпретатором выходных данных (только для зарегистрированных пользователей), что позволяет анализировать выходные данные команд show.

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

- **debug crypto ipsec 7 – отображает связь IPsec этапа 2.**
- **debug crypto isakmp 7 — отображает процесс установления связи по протоколу ISAKMP на этапе 1.**

Пример результата отладки

Сетевой экран PIX

PIX#**debug crypto isakmp 7** pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V ID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform # 2 acceptable Matches global IKE entry # 2 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID + extended capabilities payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa yload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo ad Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V endor ID payload (version: 1.0.0, capabilities: 20000001) Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing keys for Responder... Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ ously allocated memory for authorization-dn-attributes Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting dpd vid payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80 *!--- Phase 1 completed succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPL ETED** Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection: None Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do es not support keep-alives (type = None) Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P1 rekey timer: 21600 seconds. Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 164 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo te Proxy Host data in ID Payload: Address 192.168.0.2, Protocol 17, Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca l Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17, Port 1701 *!--- PIX identifies the L2TP/IPsec session.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPSec se ssion detected.** Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe er configured for crypto map: outside_dyn_map Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2,

IPSec S A Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti ng SPI! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine: SPI = 0xce9f6e19 *!--- Constructs Quick mode in Phase 2.* Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, **oakley constucting quick mode** Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting blank hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting proxy ID Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi tting Proxy Id: Remote host: 192.168.0.2 Protocol 17 Port 1701 Local host: 172.16.1.1 Protocol 17 Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting qm hash payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b 84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N ONE (0) total length : 144 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego tiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher : received KEY_UPDATE, spi 0xce9f6e19 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P2 rekey timer: 3059 seconds. *!--- Phase 2 completes succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7** pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09 Rule ID: 0x028D78D8 IPSEC: Deleted inbound permit rule, SPI 0x71933D09 Rule ID: 0x02831838 IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09 Rule ID: 0x029134D8 IPSEC: Deleted inbound VPN context, SPI 0x71933D09 VPN handle: 0x0048B284 IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA Rule ID: 0x028DAC90 IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA Rule ID: 0x02912AF8 IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA VPN handle: 0x0048468C IPSEC: New embryonic SA created @ 0x01BFCF80, SCB: 0x01C262D0, Direction: inbound SPI : 0x45C3306F Session ID: 0x0000000C VPIF num : 0x00000001 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0x0283A3A8, SCB: 0x028D1B38, Direction: outbound SPI : 0x370E8DD1 Session ID: 0x0000000C VPIF num : 0x00000001 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x370E8DD1 IPSEC: Creating outbound VPN context, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: New outbound encrypt rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 Dst mask: 255.255.255.255 Src ports Upper: 1701 Lower: 1701 Op : equal Dst ports Upper: 1701 Lower: 1701 Op : equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: New outbound permit rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x370E8DD1 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: Completed host IBSA update, SPI 0x45C3306F IPSEC: Creating inbound VPN context, SPI 0x45C3306F Flags: 0x00000206 SA : 0x01BFCF80 SPI : 0x45C3306F MTU : 0 bytes VCID : 0x00000000 Peer : 0x0048C164 SCB : 0x01C262D0 Channel: 0x01693F08 IPSEC: Completed inbound VPN context, SPI 0x45C3306F VPN handle: 0x0049107C IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0049107C SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: Completed outbound inner rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 1701 Lower: 1701 Op : equal Dst ports Upper: 1701 Lower: 1701 Op : equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F Rule ID: 0x02831838 IPSEC: New inbound decrypt rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op :

```
ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x45C3306F
Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F Rule ID: 0x028DAC90 IPSEC:
New inbound permit rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst
addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports
Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x45C3306F Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F Rule ID: 0x02912E50
```

Устранение неполадок с помощью ASDM

Используйте ASDM для включения функции регистрации данных в журнале и просмотра журналов.

1. **Выберите Configuration > Properties > Logging > Logging Setup, затем выберите Enable Logging и нажмите Apply, чтобы включить функцию регистрации данных в журнале.**
2. **Выберите Monitoring > Logging > Log Buffer > On Logging Level, затем выберите Logging Buffer и нажмите View для просмотра журналов.**

Проблема: Частые разъединения

Простаивающий / Превышение времени ожидания сеанса

Если время простоя установлено в 30 минут (по умолчанию), это означает, что это отбрасывает туннель после того, как "no traffic" (нет трафика) проходит через него в течение 30 минут. Клиент VPN разъединен после 30 минут независимо от значения времени простоя и встречается с сообщением об ошибках `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Настройте время простоя и превышение времени ожидания сеанса как ни один, чтобы заставить туннель всегда быть подключенным и так, чтобы никогда не был отброшен туннель.

Введите **команду vpn-idle-timeout** в режим конфигурации групповой политики или в режим конфигурации имени пользователя для настройки пользовательского периода ожидания:

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-
timeout none
```

Настройте максимальное количество времени для VPN-подключений с **командой vpn-session-timeout** в режиме конфигурации групповой политики или в режиме конфигурации имени пользователя:

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-
session-timeout none
```

Устранение неполадок Windows Vista

Совместный пользователь

L2TP/IPsec Windows Vista представил некоторые архитектурные изменения, которые мешали нескольким совместным пользователям связываться с PIX/ASA головного узла. Это поведение не происходит на Windows 2K/XP. Cisco внедрила обходной путь для этого изменения с Выпуска 7.2 (3) и больше.

ПК Vista, который не в состоянии соединиться

Если компьютер Windows Vista не в состоянии подключить сервер L2TP, затем проверить

настройку ONLY mschap-v2 под атрибутами ppp на DefaultRAGroup.

Дополнительные сведения

- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Cisco PIX 500 Series Security Appliances
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Поддержка продуктов программного обеспечения Cisco PIX Firewall
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Страница поддержки RADIUS
- Страница технической поддержки протоколов согласования IPSec и IKE
- Запросы комментариев (RFC)
- Layer Two Tunnel Protocol (L2TP)
- Cisco Systems – техническая поддержка и документация