ASA/PIX: Пример конфигурации устройства ASA, разрешающей раздельное туннелирование для VPN-клиентов

Содержание

Введение

В этом документе приведены пошаговые инструкции, как разрешить клиентам VPN доступ в Интернет в то время, как их трафик туннелируется в модуль Cisco Adaptive Security Appliance (ASA) 5500. Эта конфигурация обеспечивает клиентам VPN безопасный доступ к корпоративным ресурсам по протоколу IPsec и небезопасный доступ в Интернет.

Примечание: Полное туннелирование считают самой безопасной конфигурацией, потому что это не включает одновременный доступ к устройству и к Интернету и к корпоративному ЛВСу. Компромисс между полным туннелированием и разделенным туннелированием позволяет доступ к локальной сети Клиентов VPN только. Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Пример конфигурации, разрешающей клиентам VPN доступ к локальной сети.

Предварительные условия

Требования

Этот документ предполагает, что рабочая конфигурация VPN для удаленного доступа уже существует на ASA. Если такой конфигурации еще нет, см. статью Пример настройки PIX/ASA 7.x в качестве удаленного сервера VPN с помощью ASDM.

Используемые компоненты

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

- Версия программного обеспечения 7.x Устройства безопасности серии 5500 Cisco ASA и позже
- Версия 4.0.5 Клиента VPN Cisco Systems

Примечание: Этот документ также содержит PIX 6.x конфигурация интерфейса командой строки, которая совместима для клиента Cisco VPN 3. x.

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

Клиент VPN расположен в обычной сети SOHO и подключается через Интернет к главному офису.

Родственные продукты

Эта конфигурация может также использоваться с Версией программного обеспечения 7 устройства защиты Cisco PIX серии 500. x.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В базовом сценарии "клиент VPN – ASA" весь трафик от клиента VPN шифруется и отправляется на устройство ASA независимо от конечного пункта назначения трафика. В зависимости от конфигурации и поддерживаемого количества пользователей, такая настройка может потреблять значительную пропускную способность. Раздельное туннелирование может уменьшить эту проблему, так как оно позволяет пользователям отправлять по туннелю только трафик, предназначенный для корпоративной сети. Весь прочий трафик, например обмен мгновенными сообщениями, электронная почта и просмотр

веб-страниц отправляется в Интернет через локальную сеть клиента VPN.

Настройка раздельного туннелирования в ASA

Настройте ASA 7.x с менеджером устройств адаптивной безопасности (ASDM) (ASDM) 5. x

Выполните эти шаги для настройки туннельной группы для разрешения разделенного туннелирования для пользователей в группе.

1. **Выберите Конфигурация > VPN > Общие > Групповая политика, а затем — групповую политику, которая требуется для разрешения доступа к локальной сети.** Затем нажмите **Edit**.
2. Перейдите на вкладку "Client Configuration".
3. **Снимите флажок Inherit для политики раздельных туннелей (Split Tunnel Policy) и выберите Tunnel Network List Below.**
4. **Снимите флажок Наследование для списка сетей с разделенными туннелями, затем нажмите кнопку Контроль, чтобы запустить диспетчер ACL.**
5. **В данном диспетчере выберите Добавить > Добавить список ACL..., чтобы создать новый список контроля доступа.**
6. **Укажите имя ACL и нажмите кнопку OK.**
7. **После создания списка ACL выберите Добавить > Добавить ACE..., чтобы добавить элемент контроля доступа (ACE).**
8. Задайте запись ACE, соответствующую локальной сети, расположенной за модулем ASA. В этом случае сеть является 10.0.1.0/24.Выберите **Permit**.Выберите IP-адрес **10.0.1.0**Выберите маску подсети **255.255.255.0**.*Введите описание (необязательно).***Нажмите кнопку OK.**
9. **Нажмите кнопку OK, чтобы завершить работу с приложением ACL Manager.**
10. Убедитесь, что только что созданный ACL выбран для списка сетей с разделенными туннелями.
11. **Нажмите кнопку OK, чтобы вернуться к настройке групповой политики.**
12. **Нажмите кнопку Apply и затем (если потребуется) Send, чтобы отправить эти команды в модуль ASA.**

Настройте ASA 8.x с менеджером устройств адаптивной безопасности (ASDM) (ASDM) 6. x

Выполните эти шаги для настройки туннельной группы для разрешения разделенного туннелирования для пользователей в группе.

1. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** и выберите Group Policy, в котором вы хотите включить доступ к локальной сети. Затем нажмите **Edit**.
2. Нажмите **Split Tunneling**.
3. **Снимите флажок Inherit для политики раздельных туннелей (Split Tunnel Policy) и выберите Tunnel Network List Below.**
4. **Снимите флажок Наследование для списка сетей с разделенными туннелями, затем**

нажмите кнопку Контроль, чтобы запустить диспетчер ACL.

5. **В данном диспетчере выберите Добавить > Добавить список ACL..., чтобы создать новый список контроля доступа.**
6. **Укажите имя ACL и нажмите кнопку OK.**
7. **После создания списка ACL выберите Добавить > Добавить ACE..., чтобы добавить элемент контроля доступа (ACE).**
8. Задайте запись ACE, соответствующую локальной сети, расположенной за модулем ASA. В этом случае сеть является 10.0.1.0/24.Нажмите кнопку с зависимой фиксацией **Permit**.Выберите сетевой адрес с маской **10.0.1.0/24**.Введите описание (необязательно).**Нажмите кнопку OK.**
9. **Нажмите кнопку OK, чтобы завершить работу с приложением ACL Manager.**
10. Убедитесь, что только что созданный ACL выбран для списка сетей с разделенными туннелями.
11. **Нажмите кнопку OK, чтобы вернуться к настройке групповой политики.**
12. **Нажмите кнопку Apply и затем (если потребуется) Send, чтобы отправить эти команды в модуль ASA.**

Настройте ASA 7.x и позже через CLI

Вместо того, чтобы использовать ASDM, можно выполнить эти шаги в CLI ASA для разрешения разделенного туннелирования на ASA:

Примечание: Конфигурация Разделенного туннелирования CLI является тем же и для ASA 7.x и для 8. x.

1. Переход в режим конфигурирования.`ciscoasa>`**`enable`** `Password: ********` `ciscoasa#`**`configure terminal`** `ciscoasa(config)#`
2. Создайте список доступа, определяющий сеть за модулем ASA.`ciscoasa(config)#`**`access-list Split_Tunnel_List remark The corporate network behind the ASA.`** `ciscoasa(config)#`**`access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0`**
3. Перейдите в режим конфигурирования групповой политики, которую необходимо изменить.`ciscoasa(config)#`**`group-policy hillvalleyvpn attributes`** `ciscoasa(config-group-policy)#`
4. Укажите политику раздельных туннелей. **В этом случае политика указывается как tunnelspecified.**`ciscoasa(config-group-policy)#`**`split-tunnel-policy tunnelspecified`**
5. Укажите список доступа к разделенным туннелям. **В этом случае список указывается как Split_Tunnel_List.**`ciscoasa(config-group-policy)#`**`split-tunnel-network-list value Split_Tunnel_List`**
6. Введите следующую команду:`ciscoasa(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
7. Привяжите групповую политику к туннельной группе`ciscoasa(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
8. Выйдите из обоих режимов конфигурирования.`ciscoasa(config-group-policy)#`**`exit`** `ciscoasa(config)#`**`exit`** `ciscoasa#`
9. **Сохраните конфигурацию в энергонезависимой памяти (NVRAM) и нажмите клавишу ВВОД, когда будет предложено указать имя файла источника.**`ciscoasa#`**`copy running-config startup-config`** `Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a 3847 bytes copied in 3.470 secs (1282 bytes/sec) ciscoasa#`

Настройте PIX 6.x через CLI

Выполните следующие действия:

1. Создайте список доступа, который определяет сеть позади PIX.
   PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
2. Создайте *vpn3000* группы vpn и задайте ACL разделения туннеля к нему как показано:`PIX(config)#`**vpngroup vpn3000 split-tunnel Split_Tunnel_List** **Примечание:** См. межсетевой экран Cisco Secure PIX 6.x и Cisco VPN Client 3.5 для Windows с Microsoft Windows 2000 и 2003 Проверками подлинности RADIUS IAS для получения дополнительной информации о конфигурации VPN для удаленного доступа для PIX 6.x.

Проверка

Выполните описанные в следующих разделах действия, чтобы проверить конфигурацию.

- Подключение с помощью клиента VPN
- Просмотр журнала VPN-клиента
- Проверка доступа к локальной сети с помощью эхо-запроса

Подключение с помощью клиента VPN

Чтобы проверить конфигурацию, подключите VPN-клиент к концентратору VPN.

1. **Выберите из списка запись своего подключения и нажмите Connect.**
2. Введите учетные данные.
3. **Выберите Status > Statistics..., чтобы открыть окно "Tunnel Details" (Сведения о туннелях), в котором отображаются подробные данные о туннеле и потоках трафика.**
4. Перейдите на вкладку "Route Details", чтобы увидеть маршруты к ASA, защищенные клиентом VPN.В этом примере клиент VPN защищает доступ к сети 10.0.1.0/24, а весь остальной трафик не шифруется и не отправляется по туннелю.

Просмотр журнала VPN-клиента

При исследовании Журнала клиента VPN можно определить, установлен ли параметр, который задает разделенное туннелирование. Чтобы просмотреть журнал, перейдите на вкладку "Log" (Журнал) в VPN-клиенте. **Нажмите Log Settings, чтобы настроить элементы, регистрируемые в журнале. В этом примере для IKE задано значение 3 - High, а для других элементов журнала – значение 1 - Low.**

```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:20:09.532  07/27/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.

!--- Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20
14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
```

```
Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160 22 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208
07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 26 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version
7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN
is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 30 14:20:14.238 07/27/06
Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src
port = 0 dest port=0 !--- Output is supressed.
```

Проверка доступа к локальной сети с помощью эхо-запроса

Дополнительный способ протестировать это, Клиент VPN настроен для разделенного туннелирования, в то время как туннелировано к ASA, состоит в том, чтобы использовать **команду ping** в командной строке Windows. Адрес локальной сети VPN-клиента — 192.168.0.0/24, в данной сети также присутствует другой хост с IP-адресом 192.168.0.3.

```
C:\>ping 192.168.0.3 Pinging 192.168.0.3 with 32 bytes of data: Reply from 192.168.0.3: bytes=32
time<1ms TTL=255 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Reply from 192.168.0.3:
bytes=32 time<1ms TTL=255 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Ping statistics for
192.168.0.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times
in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Устранение неполадок

Ограничение с количеством записей в ACL разделения туннеля

Существует ограничение с количеством записей в ACL, используемом для разделения туннеля. Рекомендуется не использовать больше чем 50-60 первоклассных записей для удовлетворительной функциональности. Рекомендуется реализовать опцию выделения подсети для покрытия диапазона IP-адресов.

Дополнительные сведения

- PIX/ASA 7.x как Удаленный VPN-сервер с помощью Примера конфигурации ASDM
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco Systems – техническая поддержка и документация