# Ренегоциация LAN-to-LAN конфигураций между концентраторами Cisco VPN, Cisco IOS и устройствами PIX

## Содержание



## Введение

Этот документ сообщает о результатах лабораторного испытания IP-безопасности (IPSec), пересмотр туннеля между локальными сетями (LAN-to-LAN) между другими Продуктами Cisco VPN в различных сценариях, таких как перезагрузка устройства VPN, повторно вводит, и завершение работы вручную Сопоставлений безопасности IPSec (SA).

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

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

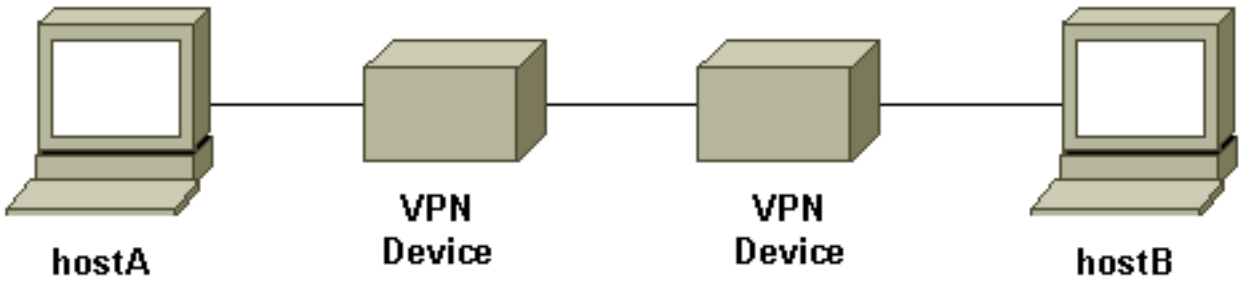
- Релиз 12.1 программного обеспечения Cisco IOS (5) T8
- Релиз программного обеспечения PIX Cisco 6.0 (1)
- Версия программного обеспечения 3.0 (3) A Cisco VPN 3000 Concentrator
- Версия программного обеспечения концентратора 5.2 (21) Cisco VPN 5000

IP - трафик, используемый в этом тесте, является двунаправленными пакетами Протокола ICMP между хостой и hostB.

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

Это - принципиальная схема испытательного стенда.




Устройства VPN представляют маршрутизатор Cisco IOS, межсетевой экран Cisco Secure PIX, Cisco VPN 3000 Concentrator или Концентратор Cisco VPN 5000.

### Условные обозначения

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

## Сценарии проверки

Были протестированы три общих сценария. Ниже приводится краткое определение сценариев проверки:

- **Завершение работы вручную КОНТЕКСТОВ БЕЗОПАСНОСТИ IPSEC** — Входы пользователя в систему на устройствах VPN и вручную очищает КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC с помощью интерфейса командной строки (CLI) или графического пользовательского интерфейса (GUI).
- **Повторно введите** — Обычная Фаза IPSec I и этап 2 повторно вводит, когда истекает определенный срок действия. В этом тесте два устройства завершения VPN имеют ту же фазу I и настроенный срок действия этапа 2.
- **Перезагрузка устройства VPN** — Любой конец оконечных точек соединения VPN-туннеля был перезагружен для моделирования перерыва в обслуживании.

**Примечание:** Для туннелей между локальными сетями (LAN-to-LAN), где Концентратор VPN 5000 используется, концентратор настроен с помощью туннельного респондента и Основного режима.

## Результаты тестирования

| Настройка | Вручную завершение КОНТЕКСТОВ | Повторно ввести | Перезагрузка устройства VPN |
|---|---|---|---|

| | БЕЗОПАСНОСТИ IPSEC | | |
|---|---|---|---|
| IOS к PIX | • Туннель, восстановленный после фазы I или SA этапа 2, очищен с обеих сторон<br>• Тестовый поток данных работает | • Тестовый поток данных все еще работает после того, как фаза I или этап 2 повторно вводят | • С сообщением поддержки активности IKE, включенным на обоих устройствах, восстановлен туннель<br>• Тестовый traffic1 работает после того, как туннель восстановился |
| IOS к VPN 3000 | • Туннель, восстановленный после фазы I или SA этапа 2, очищен с обеих сторон<br>• Тестовый поток данных работает | • Тестовый поток данных все еще работает после того, как фаза I или этап 2 повторно вводят | • С сообщением поддержки активности IKE, включенным на обоих устройствах, восстановлен туннель<br>• Тестовый traffic1 работает после того, как туннель восстановился |
| IOS к VPN 5000 | • На IOS: Тестовый поток данных все еще работает | • Тестовый поток данных все | • Туннель не в состоянии восстанавливаться |

| | | | |
|---|---|---|---|
| | после того, как SA этапа 2 очищенКогда SA фазы I очищен, VPN-туннель выключаетсяТестовый поток данных прекращает работать<br>• На VPN 5000: Туннель не в состоянии восстанавливаться после ручной очистки SAДолжен очистить и фазу I и SA этапа 2 на IOS для восстановления туннеля | еще работает после этапа 2 повторно вводят<br>• Фаза, которую я повторно ввожу, перевела туннель в нерабочее состояние<br>• Тестовый поток данных прекращает работать<br>• Должен вручную очистить SA для возвращения туннеля | после перезагрузки любое устройство VPN (с двунаправленным тестовым трафиком)<br>• Тестовый поток данных прекращает работать<br>• Должен вручную очистить SA на устройстве, которое не было перезагружено для возвращения туннеля |
| PIX к VPN 3000 | • Туннель, восстановленный после фазы I или SA этапа 2, | • Тестовый поток данных все | • Тестовый traffic1 работает после того, как |

| | | | |
|---|---|---|---|
| | очищен с обеих сторон<br>• Тестовый поток данных работает | еще работает после того, как фаза I или этап 2 повторно вводят | туннель восстановился<br>• С Dead Peer Detection (DPD) [2] (включил по умолчанию), восстановленный туннель |
| PIX к VPN 5000 | • На PIX: Тестовый поток данных все еще работает после того, как SA этапа 2 очищенКогда SA фазы I очищен, VPN-туннель выключилсяТестовый поток данных прекращает работать<br>• На VPN 5000: Туннель не в состоянии восстанавливаться, после вручную очищает SAДолжен очистить и фазу I и SA этапа 2 на PIX для восстановления туннеля | • Тестовый поток данных все еще работает после этапа 2 повторно вводят<br>• Фаза, которую я повторно ввожу, перевела туннель в нерабочее состояние<br>• Тестовый поток данных прекра | • Туннель не в состоянии восстанавливаться после перезагрузки любое устройство VPN (с двунаправленным тестовым трафиком)<br>• Тестовый поток данных прекращает работать<br>• Должен вручную очистить SA на устройстве, которое не было перезагружено для возвращения туннеля |

| | | | |
|---|---|---|---|
| | | щает работать<br>• Должен вручную очистить SA для возвращения туннеля | |
| VPN 3000 к VPN 5000 | • На VPN 3000: Туннель восстановлен после вручную ясный сеансТрафик все еще работает<br>• На VPN 5000: Туннель не в состоянии восстанавливаться после вручную ясный туннельТестовый поток данных прекращает работатьДолжен очистить SA на VPN 3000 для восстановления туннеля | • Тестовый поток данных все еще работает, или после фаза I или после этап 2 повторно вводят | • Туннель не в состоянии восстанавливаться после перезагрузки любого устройства VPN (с двунаправленным тестовым трафиком)<br>• Тестовый поток данных прекращает работать<br>• Должен вручную очистить SA на устройстве, которое не было перезагружено для возвращения туннеля |

[1], Как описано выше, используемый тестовый поток данных является двунаправленными пакетами ICMP между хостой и hostB. В тесте перезагрузки устройства VPN

однонаправленный трафик также протестирован для моделирования наихудшего случая (где трафик только от хоста позади устройства VPN, которое не перезагружено к устройству VPN, которое перезагружено). Как может замеченный по таблице, с сообщением поддержки активности IKE или с протоколом DPD, VPN-туннель может быть восстановлен с наихудшего случая.

[2] DPD являются частью Протокола Unity. В настоящее время эта функция только доступна на Cisco VPN 3000 Concentrator с версией программного обеспечения 3.0 и выше и на Межсетевом экране PIX с версией программного обеспечения 6.0 (1) и выше.

## Дополнительные сведения

- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки концентратора Cisco VPN 5000
- Страница поддержки PIX
- Страница поддержки IPSec
- Cisco Systems – техническая поддержка и документация