Настройка прозрачного режима NAT для IPSec на концентраторе VPN 3000

Содержание

Введение

Преобразование сетевых адресов (NAT) было разработано для преодоления проблемы дефицита адресного пространства межсетевого протокола 4-й версии (IPV4). Сегодня домашние пользователи и небольшие офисные сети используют NAT как альтернативу приобретению зарегистрированных адресов. Корпорации реализуют NAT в отдельности или с межсетевым экраном для защиты своих внутренних ресурсов.

Конфигурация «многие к одному», наиболее часто реализуемое решение NAT, связывает несколько частных адресов с одним внешним маршрутизируемым адресом. Такая конфигурация также называется «преобразованием адресов портов» (PAT). Ассоциация реализуется на уровне портов. Решение PAT создает проблемы для трафика IPSec, в котором никаких портов не используется.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Концентратор Cisco VPN 3000

- Клиент Cisco VPN 3000, выпуски 2.1.3 и выше
- Клиент и концентратор Cisco VPN 3000, выпуски 3.6.1 и выше для NAT-T

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Протокол инкапсулирующей защиты содержимого

Протокол 50 (инкапсулирующая защита содержимого, ESP) обрабатывает пакеты IPSec с шифрованием/инкапсуляцией. Большинство устройств PAT не работает с ESP, поскольку они запрограммированы для работы только с протоколом управления передачей (TCP), протоколом пользовательских дейтаграмм (UDP) и межсетевым протоколом управляющих сообщений (ICMP). Кроме того, устройства PAT не позволяют привязывать несколько индексов параметров безопасности (SPI). Прозрачный режим NAT в клиенте Cisco VPN 3000 Client решает эту проблему, инкапсулируя ESP в UDP-дейтаграммы и отправляя их на согласованный порт. Имя атрибута, подлежащего активации на концентраторе VPN 3000, – IPSec through NAT (IPSec посредством NAT).

Новый протокол NAT-T, имеющий статус стандарта IEF (на момент подготовки настоящей статьи стандарт еще не утвержден в окончательной редакции), также инкапсулирует пакеты IPSec в UDP, но работает на порту 4500. Этот номер порта не настраивается.

Как работает прозрачный режим NAT?

Включение прозрачного режима IPSec на концентраторе VPN создает невидимые правила фильтра и применяет их к внешнему фильтру. Затем настроенный номер порта передается VPN-клиенту прозрачным образом при подключении VPN-клиента. На входящей стороне входящий трафик UDP с этого порта проходит непосредственно на обработку IPSec. Трафик расшифровывается и декапсулируется, после чего маршрутизируется обычным образом. На исходящей стороне IPSec зашифровывает и инкапсулирует трафик, а затем применяет заголовок UDP (при соответствующей настройке). Рабочие правила фильтра деактивируются и удалены из соответствующего фильтра при трех условиях: при отключении IPSec по UDP для группы, при удалении группы и при удалении последнего активного сеанса IPSec посредством ассоциаций безопасности UDP на этом порту. Отправляются сообщения поддержания, не позволяющие устройству NAT закрыть привязку портов по причине неактивности.

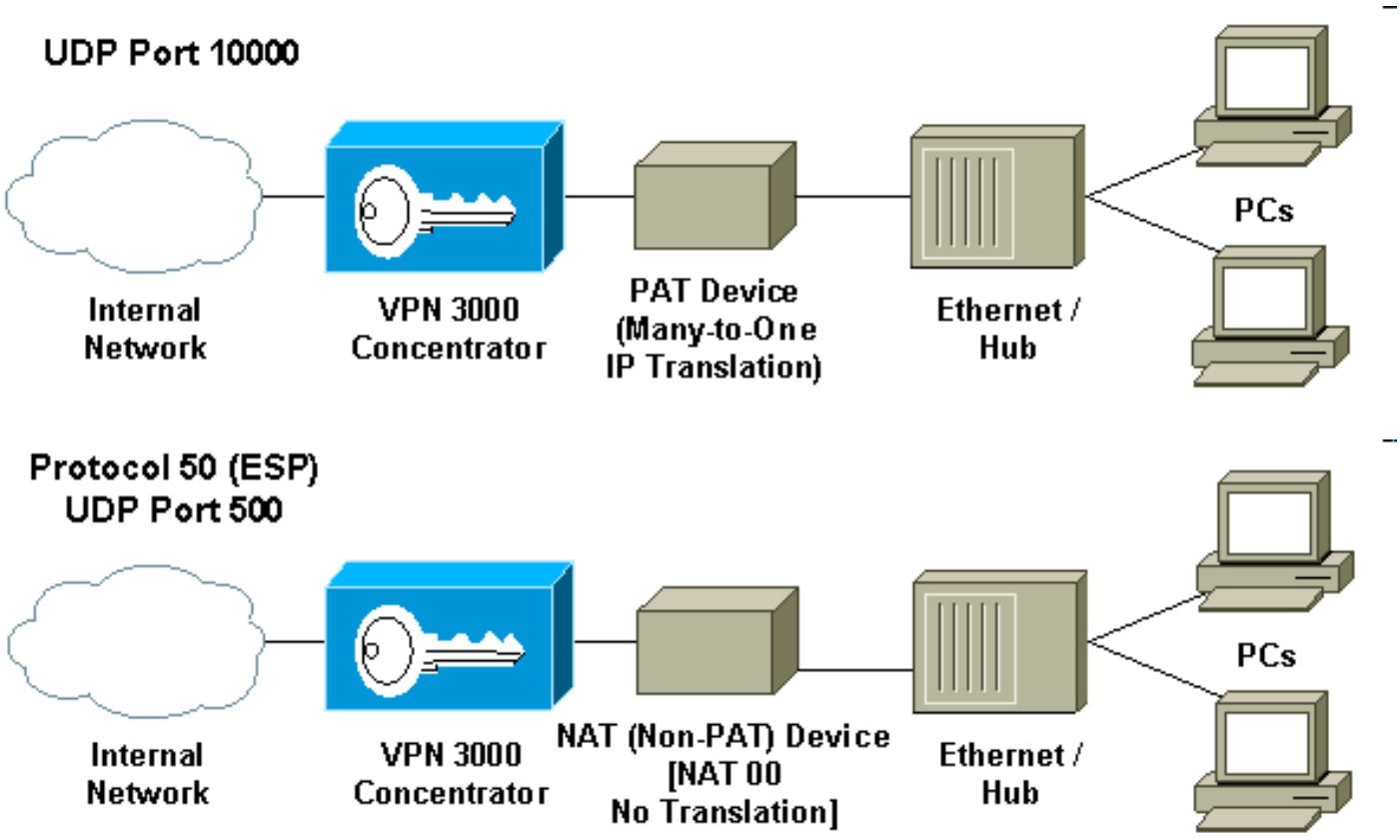
Если на концентраторе VPN включена реализация IPSec через NAT-T, то VPN-концентратор или VPN-клиент будет использовать режим инкапсуляции UDP NAT-T. NAT-T работает путем автоматического обнаружения устройств NAT между VPN-клиентом и VPN-концентратором во время согласования IKE. Для работы NAT-T необходимо следить за тем, чтобы на участке между VPN-концентратором и VPN-клиентом не был заблокирован порт UDP 4500. Кроме того, в случае использования предыдущей конфигурации IPSec/UDP, где этот порт уже задействован, необходимо перенастроить старую конфигурацию IPSec/UDP

для работы по другому порту UDP. Поскольку NAT-T является проектом стандарта IETF, он должен пойти на пользу в окружениях с устройствами нескольких поставщиков, если другие поставщики реализуют этот стандарт.

В отличие от IPSec по UDP/TCP, NAT-T работает как с подключениями VPN-клиентов, так и с подключениями LAN–LAN. Кроме того, режим NAT-T поддерживается маршрутизаторами Cisco IOS® и аппаратными межсетевыми экранами PIX.

Для работы NAT-T не нужно включать IPSec по UDP.

Настройка прозрачного режима NAT



Для настройки прозрачного режима NAT на концентраторе VPN придерживайтесь следующего порядка действий.

Примечание: В то время как IPSec по TCP / NAT-T настроен глобально, IPSec по UDP настроен на на основание группы.

1. Настройте IPSec по UDP:**На концентраторе VPN выберите Configuration > User Management > Groups (Конфигурация > Управление пользователями > Группы).Для добавления группы выберите Add (Добавить). Для изменения существующей группы выберите ее и нажмите кнопку Modify (Изменить).Выберите вкладку IPSec, отметьте IPSec through NAT (IPSec через NAT) и настройте параметр IPSec through NAT UDP Port (IPSec через UDP-порт NAT).** Порт по умолчанию для IPSec через NAT – 10000 (и источник, и адресат), но эту настройку можно изменить.
2. Настройте IPSec по NAT-T и/или IPSec по TCP:**На концентраторе VPN выберите Configuration (Конфигурация) > System (Система) > Tunneling Protocols (Протоколы туннелирования) > IPSec > NAT Transparency (Прозрачный режим NAT).Отметьте**

флажок IPSec over NAT-T and/or TCP (IPSec по NAT-T и/или TCP).

Если все разрешено, придерживайтесь следующего порядка:

1. IPSec по TCP.
2. IPSec по NAT-T.
3. IPSec по UDP.

Настройка VPN-клиента Cisco VPN Client для использования прозрачного режима NAT

Для использования IPSec по UDP или NAT-T необходимо активировать IPSec по UDP на VPN-клиенте Cisco 3.6 или более поздней версии. В случае IPSec по UDP назначение UDP-порта выполняется концентратором VPN, в то время как при NAT-T применяется фиксированный порт UDP 4500.

Для использования IPSec по TCP необходимо разрешить этот режим на VPN-клиенте и вручную настроить используемый порт.

Дополнительные сведения

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