Использование серверов RADIUS с продуктами VPN 3000

Содержание

Введение

Этот документ описывает определенные предупреждения, найденные при использовании некоторых серверов RADIUS с VPN 3000 Concentrator и Клиентами VPN.

- Сервер RADIUS Windows 2000 требует Протокола аутентификации пароля (PAP) для аутентификации Cisco VPN Client. (Клиенты IPSEC)
- Использование сервера RADIUS, который не поддерживает Протокол квитирования с аутентификацией Microsoft (MSCHAP), требует, чтобы параметры MSCHAP были отключены на VPN 3000 Concentrator. (Клиенты Протокола двухточечного туннелирования [PPTP])
- Использование шифрования с PPTP требует, чтобы return приписал Ключи MPPE MSCHAP от RADIUS. (Клиенты PPTP)
- С Windows 2003 может использоваться MS-CHAP v2, но метод аутентификации должен быть установлен как "RADIUS с Истечением".

Некоторые из этих примечаний появились в Комментариях к выпуску продукта.

Перед началом работы

Условные обозначения

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

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

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

- Концентратор Cisco VPN 3000
- Cisco VPN Client

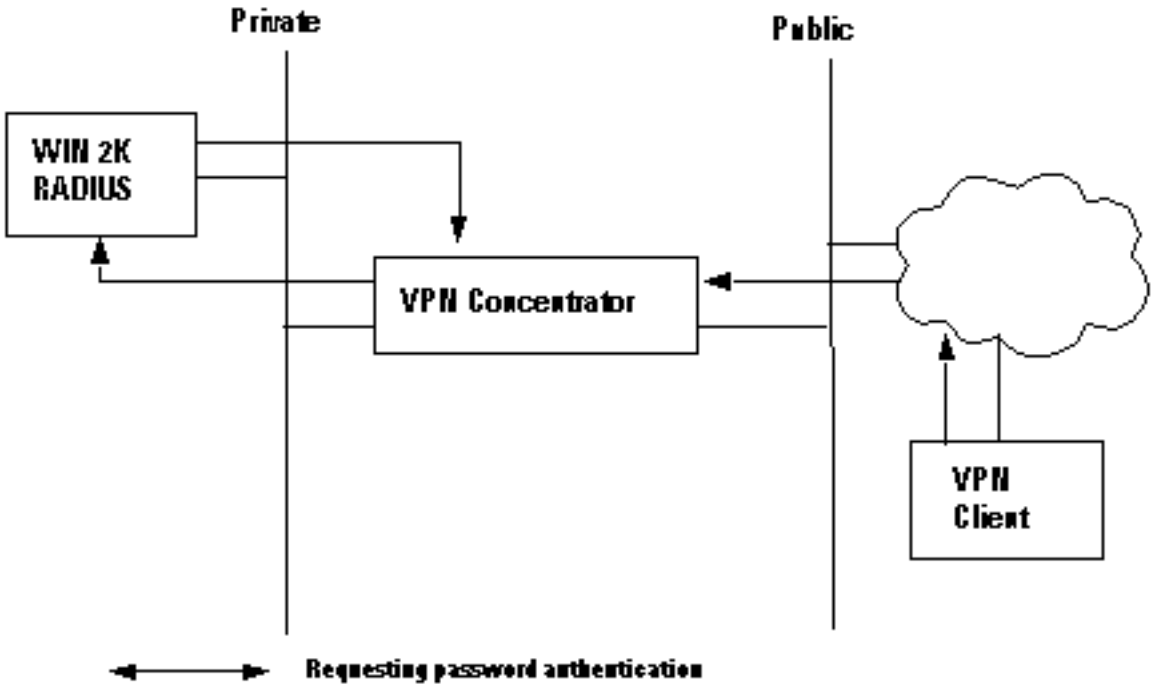
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Использование сервера RADIUS Windows 2000 для аутентификации Cisco VPN Client

Можно использовать сервер RADIUS Windows 2000 для аутентификации Пользователя VPN-клиента. В следующем сценарии (Клиент VPN запрашивает аутентификацию), VPN 3000 Concentrator получает запрос от Клиента VPN, содержащего имя пользователя и пароль пользователя клиента. Прежде, чем передать имя пользователя/пароль к серверу RADIUS Windows 2000 в частной сети для проверки, Концентратор VPN хеширует его, с помощью алгоритма HMAC/MD5.

Сервер RADIUS Windows 2000 требует PAP для аутентификации сеанса Клиента VPN. Чтобы позволить серверу RADIUS аутентифицировать Пользователя VPN-клиента, проверьте **Незашифрованную проверку подлинности (PAP, SPAP)** параметр на окне **Profile Наборного (телефонный) доступа Редактирования** (по умолчанию, этот параметр не проверен). Для установки этого параметра выберите **Remote Access Policy**, вы используете, выбираете **Properties** и выбираете **вкладку Authentication**.

Обратите внимание на то, что слово*, Незашифрованное* на названии этого параметра, вводит в заблуждение. Использование этого параметра *не* вызывает прорыв системы безопасности, потому что, когда Концентратор VPN передает пакет проверки подлинности к серверу RADIUS, это не представляет пароль ясное. Концентратор VPN получает имя пользователя/пароль и зашифрованные пакеты от Клиента VPN, и выполняет хэш HMAC/MD5 на пароле прежде, чем передать пакет проверки подлинности к серверу.



Использование сервера RADIUS, не поддерживающего MSCHAP

Некоторые серверы RADIUS не поддерживают проверка подлинности пользователя MSCHAPv2 или MSCHAPv1. При использовании сервер RADIUS, который не поддерживает MSCHAP (v1 или v2), необходимо настроить протокол аутентификации PPTP Базовой группы, чтобы использовать PAP и/или CHAP и также отключить параметры MSCHAP. Примерами серверов RADIUS, которые не поддерживают MSCHAP, является сервер RADIUS v1 61 Ливингстона или любой сервер RADIUS на основе кода Ливингстона.

Примечание: Без MSCHAP *не* будут зашифрованы пакеты к и от Клиентов PPTP.

Использование шифрования с PPTP

Для использования шифрования с PPTP сервер RADIUS должен поддержать аутентификацию MSCHAP и должен передать Ключи MPPE MSCHAP атрибута return за каждой проверкой подлинности пользователя. Примеры серверов RADIUS, которые поддерживают этот атрибут, показывают ниже.

- Cisco Secure ACS для Windows - версия 2.6 или позже
- Funk Software Steel-Belted RADIUS
- Сервер аутентификации Microsoft Internet Authentication Server на пакете параметров сервера NT 4.0
- Microsoft Commercial Internet System (MCIS 2.0)
- Сервер Microsoft Windows 2000 - Internet Authentication Server

Дополнительные сведения

- Страница поддержки RADIUS

- Страница поддержки Cisco Secure ACS для Windows
- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Series Client
- Страница поддержки IPSec
- Страница поддержки PPTP
- RFC 2637: Протокол PPTP
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems