

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[!--- конфигурацию](#)

[Настройка VPN Client 4.8](#)

[Настройте TACACS + сервер Использование Cisco Secure ACS](#)

[Настройте функцию нейтрализации](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Функция аутентификации прокси-сервера позволяет пользователям входить к сети или обращаться к Интернету через HTTP с их определенными профилями доступа, автоматически полученными и прикладными из TACACS + или сервер RADIUS. Профили пользователя активны только тогда, когда есть активный трафик от проверенных пользователей.

Эта конфигурация разработана, чтобы перевести web-браузер в рабочее состояние на 10.1.1.1 и нацелить его на 10.17.17.17. Поскольку Клиент VPN настроен для прохождения через оконечной точки туннеля 10.31.1.111 для получения до 10.17.17.x сеть, Туннель IPSec создан, и ПК вытаскивает IP-адрес из RTP-POOL пула (так как mode-configuration выполнен). Аутентификацию тогда запрашивает Маршрутизатор Cisco 3640. После того, как пользователь вводит имя пользователя и пароль (сохраненный на TACACS + сервер в 10.14.14.3), список доступа, переданный от сервера, добавлен к списку доступа 118.

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются эти требования:

- Cisco VPN Client настроен для установления Туннеля IPSec с Маршрутизатором Cisco 3640.
- TACACS + сервер настроен для аутентификации прокси-сервера. Посмотрите [Дополнительные сведения](#)