Настройка концентратора VPN 3000 для связи с клиентом VPN с использованием сертификатов

Содержание

Введение

Этот документ включает пошаговые инструкции о том, как настроить концентраторы Cisco VPN серии 3000 с Клиентами VPN с использованием сертификатов.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии программного обеспечения 4.0.4A Cisco VPN 3000 Concentrator.

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

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

Сертификаты концентраторов VPN 3000 для клиентов VPN

Выполните эти шаги для настройки сертификатов VPN 3000 Concentrator для Клиентов VPN.

1. Набор правил IKE должен быть настроен для использования сертификатов на Менеджере Серии концентраторов Cisco VPN 3000. Для настройки Набора правил IKE выберите **Configuration> System> Tunneling Protocols> IPsec> IKE Proposals** и переместите **CiscoVPNClient-3DES-MD5-RSA** в Активные предложения.
2. Необходимо также настроить политику IPsec для использования сертификатов. Выберите**> Security Configuration> Policy Management> Traffic Management Ассоциации**, выделите **ESP-3DES-MD5** и затем нажмите **Modify для настройки политики IPsec** для настройки политики IPsec.
3. На окне Modify, под Цифровыми сертификатами, удостоверяются, что выбрали ваш установленный сертификат идентификации. В соответствии с Предложением ike, выберите **CiscoVPNClient-3DES-MD5-RSA** и нажмите **Apply**.
4. Для настройки Группы IPSec выберите **Configuration> User Management> Groups> Add**, добавьте группу, названную **IPSECCERT** (имя группы IPSECCERT совпадает с Подразделением (OU) в сертификате идентификации), и выберите пароль.Этот пароль не используется нигде при использовании сертификатов. В данном примере "cisco123" является паролем.
5. На той же странице нажмите Вкладку Общие и удостоверьтесь, что вы выбираете **IPsec** как Протокол туннелирования.
6. Нажмите вкладку IPsec и удостоверьтесь, что ваш настроенный IPsec Security Association (SA) выбран под контекстом безопасности IPSec, и нажмите **Apply**.
7. Для настройки Группы IPSec на VPN 3000 Concentrator выберите **Configuration> User Management> Users> Add**, задайте Имя пользователя, Пароль и Имя группы, и затем **нажмите Add**.В примере используются эти поля:Имя пользователя = cert_userПароль = cisco123Проверьте = cisco123Группа = IPSECCERT
8. Для включания отладку на VPN 3000 Concentrator, выбирают **Configuration> System> Events> Classes** и добавляют эти классы:CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10
9. Выберите **Monitoring> Filterable Event Log** для просмотра отладок.**Примечание:** Если вы решаете изменить IP-адреса, можно сделать регистрацию новых IP-адресов и установить выполненный сертификат позже с теми новыми адресами.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

См. Устранение проблем Проблем с подключением на VPN 3000 Concentrator для дополнительных сведений об устранении проблем.

Дополнительные сведения

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Client
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация