Содержание

Введение

Этот документ описывает тип сертификата, который должен использоваться для расшифровки HTTPS на Cisco Web Security Appliance (WSA).

Обзор сертификата

WSA имеет способность использовать текущий сертификат и секретный ключ для использования с расшифровкой HTTPS. Однако мог бы быть беспорядок о типе сертификата, который должен использоваться, с тех пор не все x.509 сертификаты работают.

Существует два главных типа сертификатов: **Серверные сертификаты** и **Корневые сертификаты**. Все x.509 сертификаты содержат поле Basic Constraints, которое определяет тип сертификата:

- **Подвергните Объект Type=End** - Серверный сертификат
- **Подчиненный Type=CA** - Корневой сертификат

> **Примечание:** Необходимо использовать Корневой сертификат, также называемый сертификатом Подписания Центра сертификации (CA), для расшифровки HTTPS на WSA.

Корневые сертификаты

Корневой сертификат в частности создан для подписания серверных сертификатов. Можно создать и управлять собственным CA и подписать собственные серверные сертификаты.

> **Примечание:** Так как Корневой сертификат только подписывает другие сертификаты, он не может использоваться на Web-сервере для выполнения шифрования HTTPS и расшифровки.

WSA должен использовать Корневой сертификат для активной генерации серверных

сертификатов для расшифровки HTTPS. Существует две опции, доступные для использования Корневого сертификата:

- Генерируйте корневой сертификат на WSA. WSA создает свой собственный Корневой сертификат и секретный ключ, и это использует эту пару ключей для подписания Серверных сертификатов.

- Можно загрузить текущий Корневой сертификат и его секретный ключ в WSA. Поле Common Name (CN) в Корневом сертификате определяет объект (как правило, название корпорации), который доверяет любым Серверным сертификатам, которые содержат его подпись.

  Примечание: Прежде чем Серверному сертификату можно доверять, это должно быть подписанный Корневым сертификатом, который имеет подарок с открытым ключом в web-браузере.

Серверные сертификаты

Серверный сертификат в частности создан, чтобы использоваться в шифровании HTTPS и расшифровке и для проверки подлинности определенного сервера. Серверные сертификаты подписаны CA с использованием Корневого сертификата CA. Общим примером CA является VeriSign или Thawte.

> **Примечание:** Серверный сертификат не может использоваться для подписания других сертификатов; поэтому, если Серверный сертификат установлен на WSA, расшифровка HTTPS не работает.

Поле CN в Серверном сертификате задает хост, для которого сертификат предназначен, чтобы использоваться. Например, **https://www.verisign.com** использует Серверный сертификат с CN **www.verisign.com**.

Дополнительные сведения

- Web Security Appliance (WSA) Certificate usage (Расшифровка HTTPS, вход в систему GUI, Учетное Шифрование)
- Шаги для включения HTTPS проксируют на опции WSA & Certificate Signing Request (CSR)
- Шаги для включения HTTPS проксируют на (WSA) и Загружающий Корневую/Промежуточную опцию сертификата
- Cisco Systems – техническая поддержка и документация