Каков алгоритм для Проверки сертификата на Cisco Email Security Appliance (ESA)?

Содержание

[Введение](#)
[Каков алгоритм для Проверки сертификата на Cisco Email Security Appliance (ESA)?](#)
[Общие сведения](#)
[Определения](#)
[Размещенный проверяют алгоритм](#)
[Проверьте алгоритм](#)

Введение

При использовании TLS для отправки электронной почты через Cisco Email Security Appliance (ESA) можно принять решение выполнить Проверку сертификата с помощью любого опции 'Verify' или 'Hosted Verify'. Это - ключевая роль обеспечения доставки электронных почт по TLS, и важно знать, как выполнена эта проверка.

Каков алгоритм для Проверки сертификата на Cisco Email Security Appliance (ESA)?

Существует фактически два алгоритма, один для опции 'Verify' и другого для опции 'Hosted Verify'. Как правило, опция 'Hosted Verify' рекомендуется, поскольку это совместимо с большим разнообразием сценариев.

Общие сведения

- Эта документация основывается на AsyncOS 8.0.1 и более поздних версиях. Предыдущие версии AsyncOS могут иметь несколько другое поведение.
- Пока иначе не задано, соответствия подстановочного знака поддерживаются
- Каждый алгоритм останавливается после того, как полное совпадение и последующие проверки не оценены
- Команда CLI **tlsverify** использует, 'Проверяют Алгоритм'

Определения

- CN: Это - Общее имя, часть предмета сертификата
- SAN: Это - Подчиненное расширение Альтернативного названия к X.509. Когда используется в этом документе, мы в частности обращаемся к любым именам DNS, включенным в поле SAN.
- Почтовый домен: Это - доменная часть адреса электронной почты получателя. Например, при отправке к 'user@example.com', почтовый домен является

'example.com'
- Имена хоста MX: Это имена хоста записей MX почтового домена
- Имя хоста PTR: Это - имя хоста, возвращенное поиском PTR DNS IP-адреса, с которым соединяется ESA
- Имена хоста Маршрута SMTP: Если маршрут SMTP настроен для этого назначения, это - имя хоста, используемое в маршруте SMTP

Размещенный проверяют алгоритм

1. Если сертификат будет содержать SAN атрибуты, то *только* они будут использоваться, и CN будет проигнорирован. Если не будет никаких SAN атрибутов в сертификате, CN будет только использоваться. Это соответствует RFC 6125.
2. Сертификат проверен против почтового домена.
3. Сертификат проверен против любых имен хоста маршрута SMTP, которые могут существовать.
4. Сертификат проверен против имени (имен) хоста MX.
5. Если ни одна из предыдущих проверок не успешно выполнилась, сбои проверки.

Проверьте алгоритм

1. SAN атрибуты проверены против почтового домена.
2. CN проверен против почтового домена. **Примечание:** Соответствия подстановочного знака не поддерживаются.
3. SAN атрибуты проверены против имени хоста PTR.
4. Если ни одна из предыдущих проверок не успешно выполнилась, сбои проверки.