Содержание

Вопрос:

Как выдвинуть самоподписанный корневой сертификат с Групповой политикой или GPO?

Примечание: Эта статья Базы Знаний ссылается на программное обеспечение, которое не поддерживается Cisco. Информация предоставлена как любезность для вашего удобства. Для дальнейшей поддержки свяжитесь с поставщиком программного обеспечения.

С версией 5.5.x AsyncOS и выше, Cisco Web Security Appliance предоставляет способность дешифровать Трафик HTTPS путем включения прокси HTTPS в соответствии с> Security GUI Сервисы> прокси HTTPS. С включенной расшифровкой HTTPS клиенты должны были бы доверять сертификату, загруженному или генерируемому под разделом прокси HTTPS во избежание наблюдения ошибок сертификата на клиентских компьютерах.

Самоподписанным или генерируемым сертификатам на WSA по сути не доверяли бы клиентские компьютеры и если не доверяемый, то клиенты должны будут вручную принять предупреждение сертификата. Если мы не хотим, чтобы все пользователи прошли шаги принятия недоверяемого подписанного сертификата от Cisco WSA вручную, то мы можем выдвинуть сертификат к клиентским компьютерам через Групповую политику (GPO).

См. ниже статей, которые предоставляют подробную информацию о том, как выполнить это:

Соединение: http://www.unixwiz.net/techtips/deploy-webcert-gp.html

Соединение: http://technet.microsoft.com/en-us/library/cc738131 (v=ws.10) .aspx

Соединение: http://technet.microsoft.com/en-us/library/cc770315 (v=ws.10) .aspx