SSL Certificates Explained

https://campus.barracuda.com/doc/46203473/

This article applies to using SSL certificates when you enable SSL Inspection on the Barracuda Web Security Gateway.

What is SSL?

SSL is an acronym for Secure Sockets Layer. It is a security protocol that offers authentication, privacy, and security to internet communications. SSL *certificates* are used to secure data transfers, credit card transactions, logins and other personal information. The primary reason SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can access it. Installing an SSL Certificate on a web server triggers the padlock and the HTTPS protocol that allows the creation of a secure connection from a web server to a browser.

Barracuda Web Security Gateway Certificates

When the Barracuda Web Security Gateway intercepts an SSL session, it creates two SSL tunnels: one between the client (or *end user*) and Barracuda Web Security Gateway, and another between the Barracuda Web Security Gateway and the remote server. Since the Barracuda Web Security Gateway is the endpoint for the client SSL session, it needs to present an SSL certificate to the client which the client will accept AND that the Barracuda Web Security Gateway can use to decode the traffic so that it can inspect the data. In order to accomplish this, the Barracuda Web Security Gateway acts as a Certificate Authority (CA) and creates a signed server certificate for that domain.

For example, if the client is trying to connect to **https://www.example.com**, the Barracuda Web Security Gateway presents the client with a certificate that states the Barracuda Web Security Gateway has issued the certificate to **www.example.com**. If the client browser does not trust the Barracuda Web Security Gateway to be an issuer of certificates, or if the Barracuda Web Security Gateways certificate doesn't have the right attributes that denote it as an issuer, the browser will show an error to the end user indicating an SSL handshake issue. Some browsers, such as Chrome, are very security-conscious, and will return an error to the user if any part of this transaction is not performed exactly right and will sever the HTTPS connection. The FireFox browser, conversely, provides the ability to let the user override this behavior and manually accept the certificate.

For more information on using SSL certificates with the Barracuda Web Security Gateway, see also:

- How to Create and Install a Self-Signed Certificate for SSL Inspection

- How to Use the Barracuda Default Certificate for SSL Inspection
- Barracuda Web Security Gateway Update for SSL Inspection Certificate Handling
- Using SSL Inspection With the Barracuda Web Security Gateway

Third party CAs and subordinate certificates

Third party 'Trusted' certificates are issued by designated providers, or Certificate Authorities, who must adhere to local laws on encryption methods. Note that a public root CA such as Verisign will not provide you with a subordinate certificate; they will only provide you with a server certificate, which *cannot* be used to issue other certificates. The reason for this is that you could use a subordinate CA certificate to issue SSL certificates for any site you wanted to, and since Verisign gave you the certificate, they would be stating that they trusted you to issue SSL certificates to anyone you wanted to. Verisign and other public root CAs will not do this, in order to avoid the possibility of you issuing SSL certificates to "bad" websites with Verisign (or other public root CA) seen as trusting those sites, even though they have no knowledge of the sites.

Another scenario is that you could use that certificate to intercept SSL traffic for any user anywhere, since almost every web browser in the world trusts Verisign, for example, and you could intercept all users' traffic and have unauthorized access to all of their previously encrypted data.

Since you cannot purchase a subordinate certificate from Verisign or third party root CA, you can use a local CA program to act as a Root Certificate Authority, and use that to generate a subordinate certificate, such as with Microsoft PKI server. As long as your clients trust that local root, you could install any subordinate certificate generated by that root and use it for SSL interception on the Barracuda Web Security Gateway. If your clients do not trust that root CA, they will get errors when browsing which indicate that the SSL certificate is signed by an "untrusted issuer."

Self-signed certificates

A self-signed certificate on the Barracuda Web Security Gateway can also be used for SSL interception without the need to retrieve a certificate from a root CA, but would need to be installed in each end user browser as a Trusted Root Certification Authority.