Full (Deep) SSL Inspection - Avoid certificate errors

209 Les Carr Thu, Jul 26, 2018 Fortigate UTM 5898

Preventing certificate warnings

Posted on July 26th

SHARE THIS POST:

In this recipe, you will prevent users from receiving a security certificate warning when your FortiGate applies full SSL inspection to incoming traffic.

When full SSL inspection is used, your FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in “man-in-the-middle” attacks, which is why a user’s device may show a security certificate warning.

For more information about SSL inspection, see Why you should use SSL inspection.

Often, when a user receives a security certificate warning, they simply select **Continue**without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

There are two methods for doing this, depending on whether you are using your FortiGate’s default certificate or using a self-signed certificate.

Find this recipe for other FortiOS versions

~~5.2~~ | 5.4 | ~~5.6~~

Using the default certificate

All FortiGates have a default certificate that is used for full SSL

inspection. This certificate is also used in the default **deep-inspection** profile. To prevent your users from seeing certificate warnings, you can install this certificate on your users' devices.

If you have the right environment, you can distribute the certificate and have it installed automatically.

1. Generating a unique certificate

Online URL: https://kb2.ic.uk/article.php?id=209