HTTPS Inspection with Cisco Umbrella

Ben Muller
PA-NJ SE
12/3/2018

Symptoms

- Web sites and applications inspected by Cisco Umbrella might not work properly when HTTPS Inspection is enabled on Check Point Security Gateway.
- Symptoms vary between web sites and applications, and include:
    - Pages fail to load
    - issues with logging in
    - some or all functionality does not work as expected
    - invalid certificate errors
        - Chrome:
          Your connection is not private

          This server could not prove that it is <URL_or_IP_ADDRESS>; its security certificate is not trusted by your computer's operating system.

        - Firefox:
          This Connection is Untrusted

          You have asked Firefox to connect securely to <URL_or_IP_ADDRESS>, but we can't confirm that your connection is secure.

          Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

        - Opera:
          Invalid certificate

          Opera cannot verify the identity of the server "<URL_or_IP_ADDRESS>", due to a certificate problem. The server could be trying to trick you. Would you like to continue to the server?

        - Internet Explorer
          The security certificate presented by this website was not issued by a trusted certificate authority.
          The security certificate presented by this website was issued for a different website's address.

Cause

This scenario creates a situation where HTTPS inspection is performed twice on https traffic to the internet. Daisy chaining HTTPS inspection requires all outbound CA certificates to be trusted by all devices in the connection path. (Ref. sk114628). The Cisco Root Certificate Authority should trusted by both the clients and the Check Point Security Gateway. The Check Point Security Gateway CA should also be trusted by the clients.

Solution

Obtain the root CA from the Cisco Umbrella getting started guide https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information

To import the Cisco CA:

- Navigate to the HTTPS Inspection section in SmartDashboard and select Trusted CAs. Click on the Actions button and select import outbound certificate to import and add the Cisco CA to the list of trusted CAs

To make the PC trust the gateway CA certificate:

- Export the CA certificate from the SmartDashboard (on the HTTPS Inspection window of the Security Gateway, or on the HTTPS Inspection > Gateways pane).
- Install the certificates on the user's PC:
    - Manually put the certificate files in the user's PC. Click the file and follow the wizard instructions to add the certificate to the trusted root certificates repository on client machines.
    - Use GPO or group policy to distribute the certificates to a large group of users. See the documentation for more details.