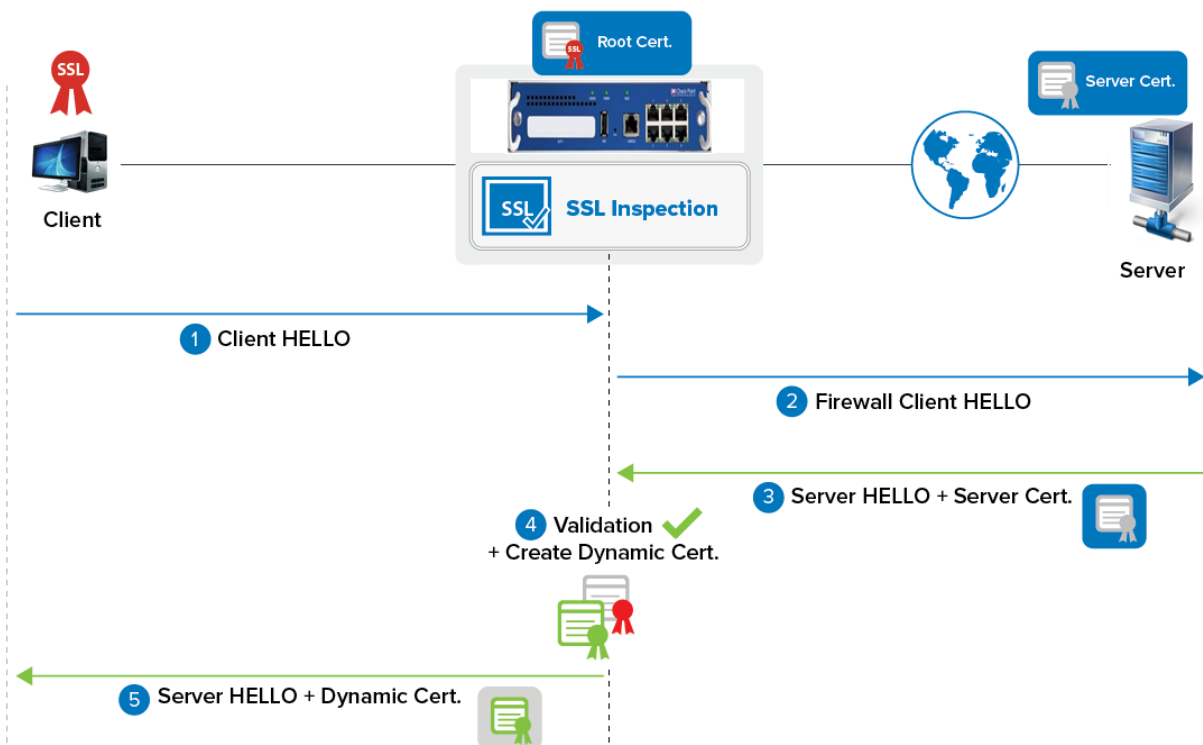


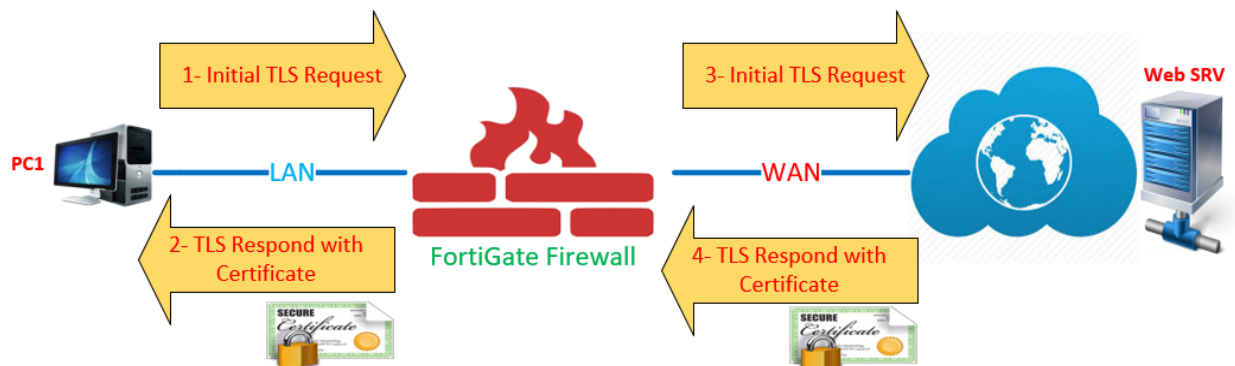
SSL Inspection:

- o Encrypted traffic, such as HTTPS, TLS and SSL connections, cannot be inspected.
- o Many connections are encrypted, such as connections to banks and other financial.
- o Many Web Sites use encryption (SSL and TLS) to protect privacy or sensitive data.
- o However, the users can also hide undesirable traffic within encrypted connections.
- o By implementing the SSL decryption, you can decrypt connections and inspect them.
- o Ensure they do not contain threats or other undesirable traffic & then re-encrypt them.
- o Use the SSL Forward Proxy decryption policy to decrypt and inspect SSL and TLS traffic.
- o SSL Forward Proxy Decryption Policy inspect SSL traffic from internal users to the web.
- o It prevents malware concealed as SSL encrypted traffic from being introduced to network.
- o SSL Forward Proxy decryption, Firewall resides between internal client and outside server.
- o Firewall uses Forward Trust certificates to establish itself as trusted third party to session.
- o Firewalls provide capability to decrypt and inspect traffic for visibility, control and security.
- o Decryption of outbound SSL traffic is implemented and takes form of SSL Forward Proxy.
- o SSL Decryption Policy, which features Firewall as an intermediate communication node.
- o SSL Decryption Policy decryption deployment commonly referred to as Man in the Middle.
- o It replaces original certificate from a final destination with resigned by a different key.
- o Checkpoint Firewall can act as proxy between a client and an HTTPS website or Internet.
- o SG Firewall decrypt inbound/outbound SSL traffic in order to apply inspection policies.
- o To configure Outbound SSL Decryption, generate self-signed certificate from SG Firewall.
- o SG device is configured to decrypt SSL traffic going to external sites as a forward proxy.

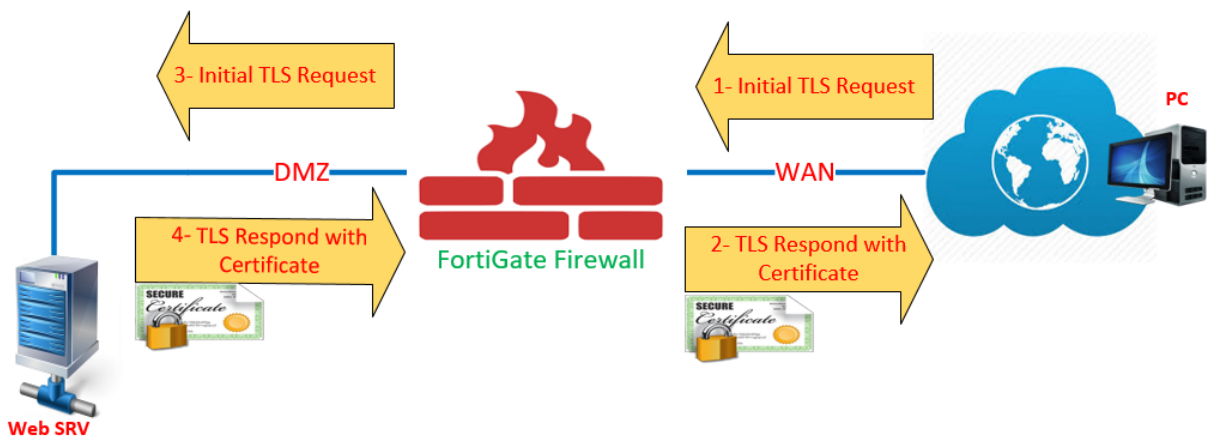


How it Operates:

The principle is very easy. If Bob tries to create SSL tunnel, Fortigate Firewall sees the https traffic and intercept it. Then instead of relaying that connection to destination, Fortigate Firewall sends its own certificate and Bobs browser accept it, because it is configured to do so. Then Fortigate Firewall creates its own SSL tunnel towards the destination. Hence working like proxy. After that the checkpoint can see what is inside that tunnel and recognize if employee is violating policy. However, you should be damn sure you are not inspecting for example banking transactions. This can be accomplished by using URL filtering as then Fortigate Firewall will know all the financial institution around.

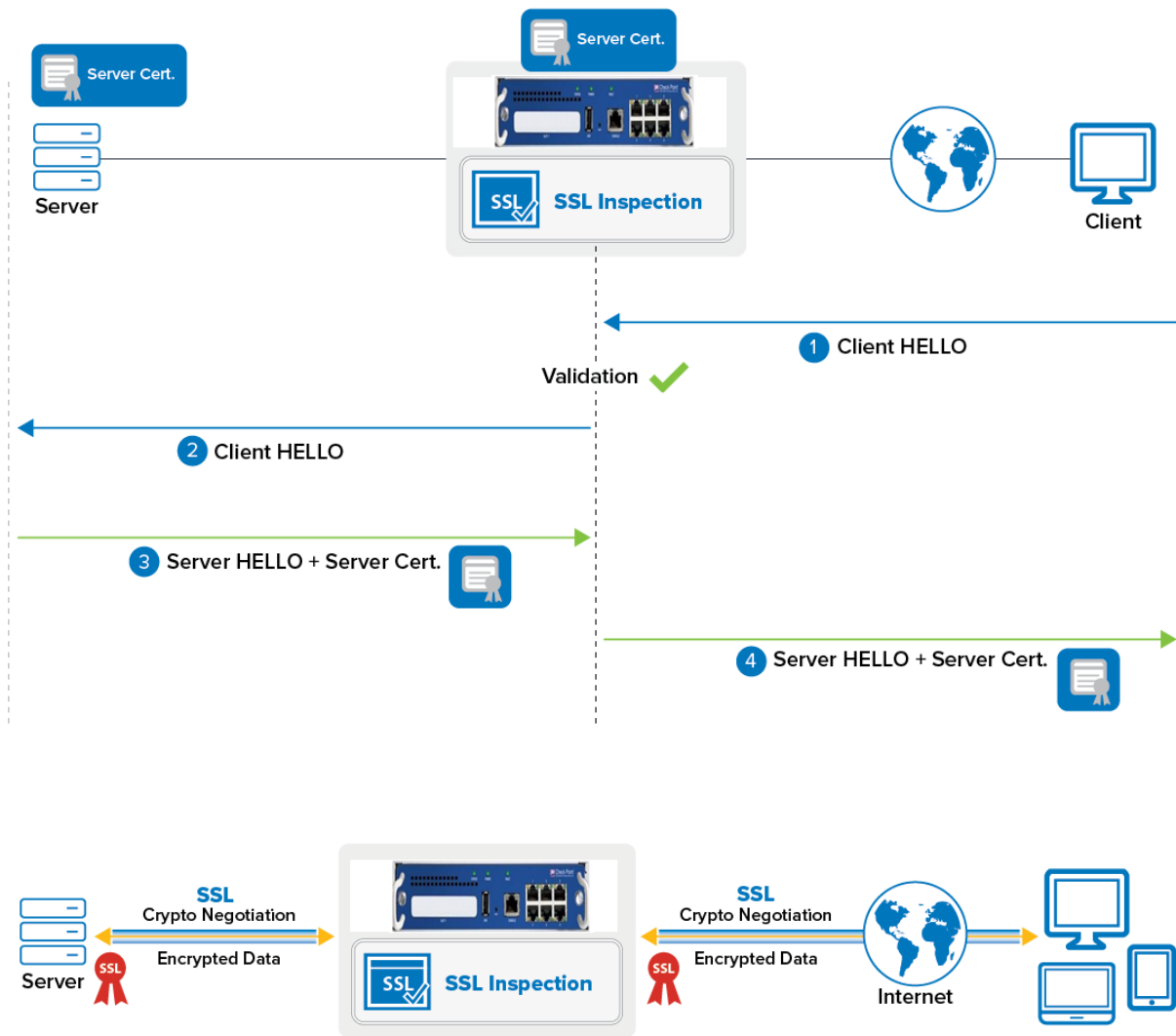


This concept can be also used for clients accessing encrypted resources in DMZ for example. And the Fortigate Firewall works here like proxy having the certificate of the server. It's like LB SSL offloading. Fortigate Firewall then answer for this request and encrypted tunnel is created between Fortigate Firewall and client, so Fortigate Firewall can inspect the traffic.



Inbound HTTPS Inspection:

Inbound HTTPS Inspection protects internal servers for example, data centers and web servers from malicious attacks coming from the Internet. Inbound connections are HTTPS connections that start from an external client and connect to an internal server in the DMZ or the network. The Fortigate Firewall compares the HTTPS request to the HTTPS Inspection Rule Base. If the request does not match a rule, the packet is not decrypted. If the request matches an inspection rule, the Fortigate Firewall uses the certificate for the internal server to create a new HTTPS connection with the external client. The Fortigate Firewall creates a new HTTPS connection with the internal server. Since the Fortigate Firewall has a secure connection with the external client, it can decrypt the HTTPS traffic.



Outbound HTTPS Inspection:

Outbound HTTPS Inspection protects internal users and perimeter servers from malicious attacks coming from the Internet on connections originated from inside the organization. Outbound connections are HTTPS connections that start from an internal client and connect to the Internet. The Fortigate Firewall compares the HTTPS request to the HTTPS Inspection Rule Base. If the request does not match a rule, the packet is not decrypted. If the request matches an inspection rule, the Fortigate Firewall makes sure that the certificate from the server (in the Internet) is valid. The Fortigate Firewall creates a new certificate, and presents it to the client, when client creates an HTTPS connection to the gateway. There are two HTTPS connections, one to the internal client and one to the server. It can then decrypt and inspect the packets according to the Fortigate Firewall and other Rule Bases.

