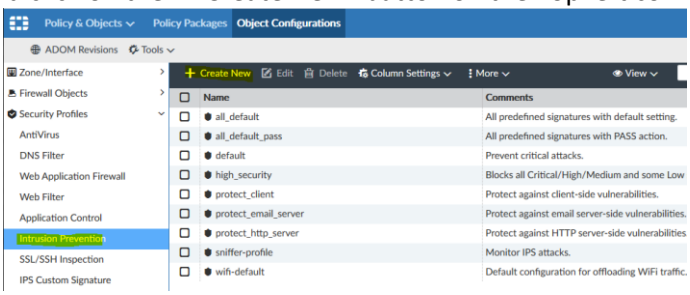
The following steps outline how to use the FortiManager to configure FortiGates to use IPS to address the certificate removal vulnerability as outlined in PSIRT FG-IR-19-144.

The steps and screenshots used in this article are based upon FortiManager 6.2.1. Similar configuration options are available on earlier versions of FortiManager.

If you have 6.2.0, it is recommended to upgraded to 6.2.1 prior processing the steps in this article given a limitation unique to 6.2.0.

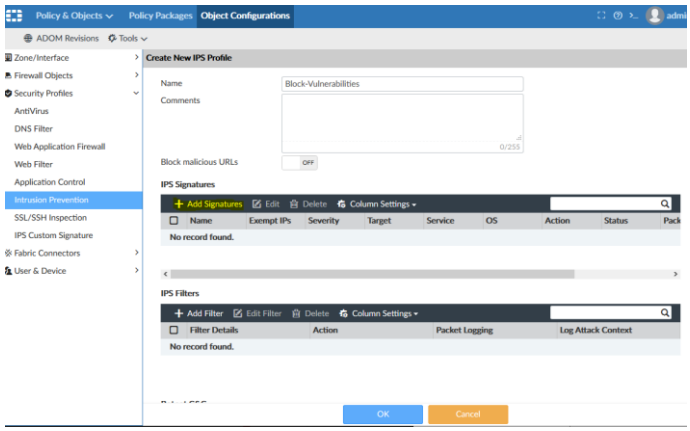
Step 1) Configure IPS Sensor

- In “Policy & Objects” > “Object Configuration”, navigate to “Security Profiles”>” Intrusion Prevention” and click on the “+ Create New” button on the Top left corner of the page:



Note: As an alternative to creating a new profile, it also possible to modify an existing profile.

- Enter Name, for example “Block-Vulnerabilities”
- Under IPS Signatures, click on the “Add Signatures” button.

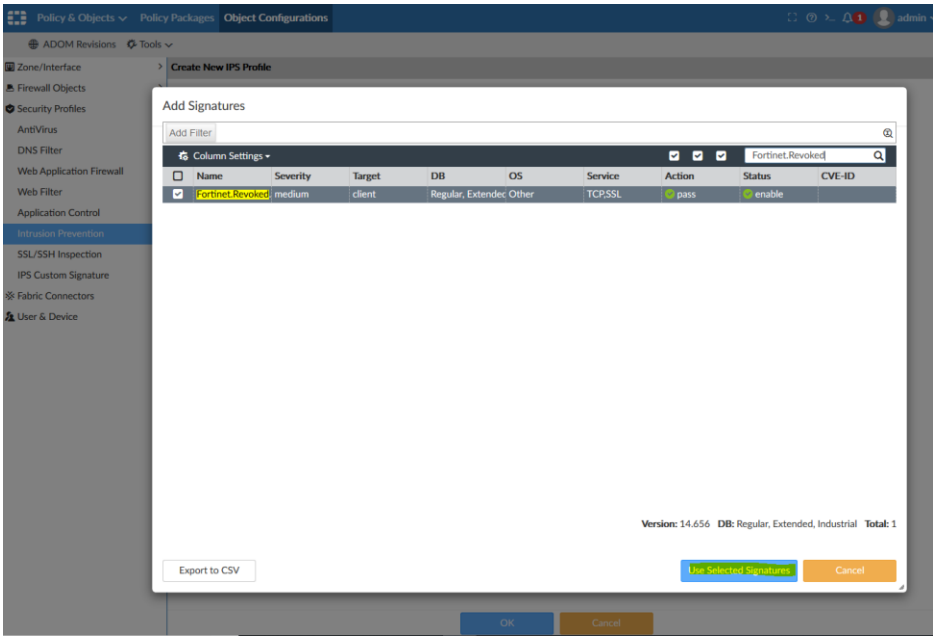


- In the Next Window, select signature "Fortinet.Revoked.SSL.Certificates"

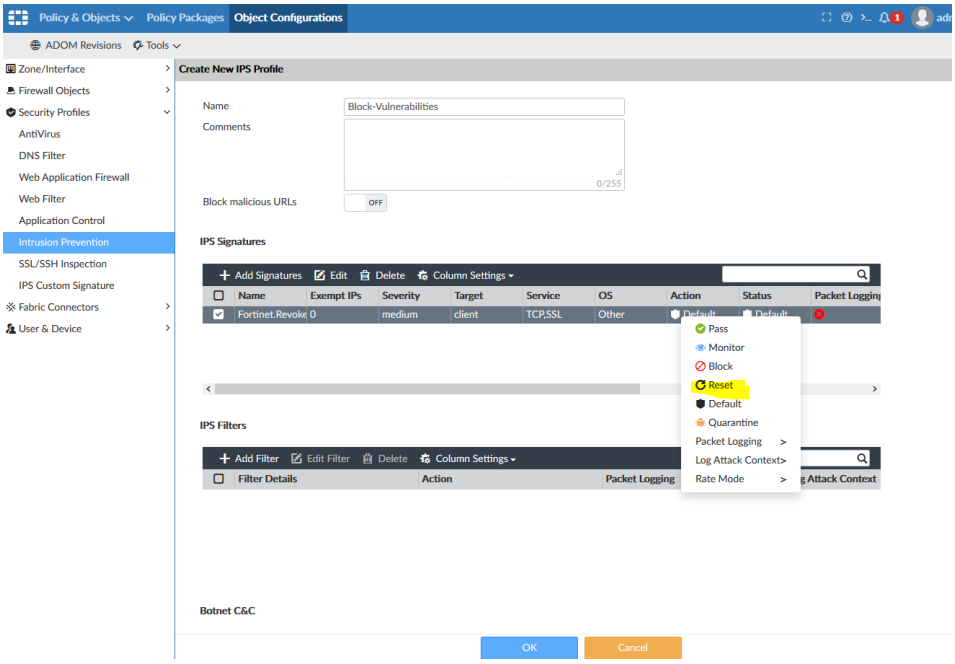
The IPS signature "Fortinet.Revoked.SSL.Certificates" is included in IPS definition version 14.00656. If "Fortinet.Revoked.SSL.Certificates" is not available, please contact Fortinet technical support.

Note: next two steps are not applicable for FMG v6.2.0GA. For workaround CLI script could be used. (FMG v6.2.1 is NOT affected)

- Select the signature and Click on “Use Selected Signatures”

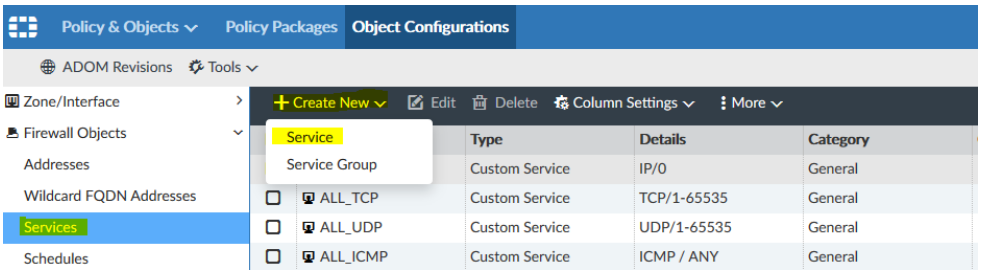


- The selected signature is now displayed under “IPS Signatures” section.
- Right click the signature and select action “Reset”, the action should change to Reset.
- Click “OK” to save the IPS sensor.

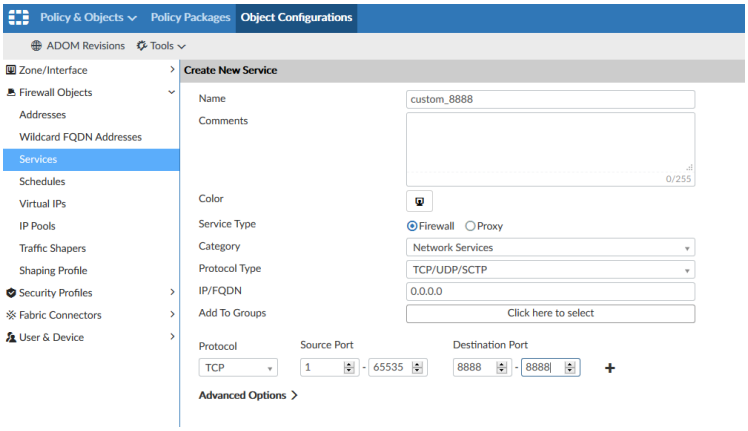


Step 2) Configure custom service

- In “Policy & Objects” > “Object Configuration”, navigate to “Firewall Objects”>” Services”, click on the “+ Create New” button and select “Service” in dropdown list:

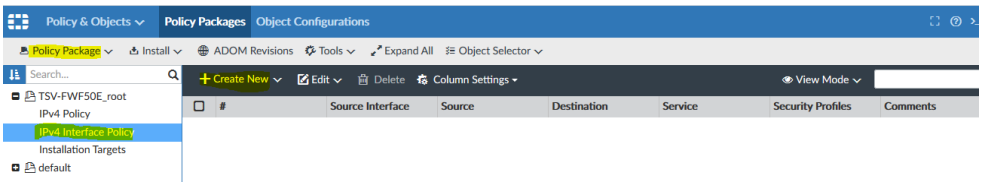


- Enter Name, for example “custom_8888”, TCP for protocol and 8888 under Destination port

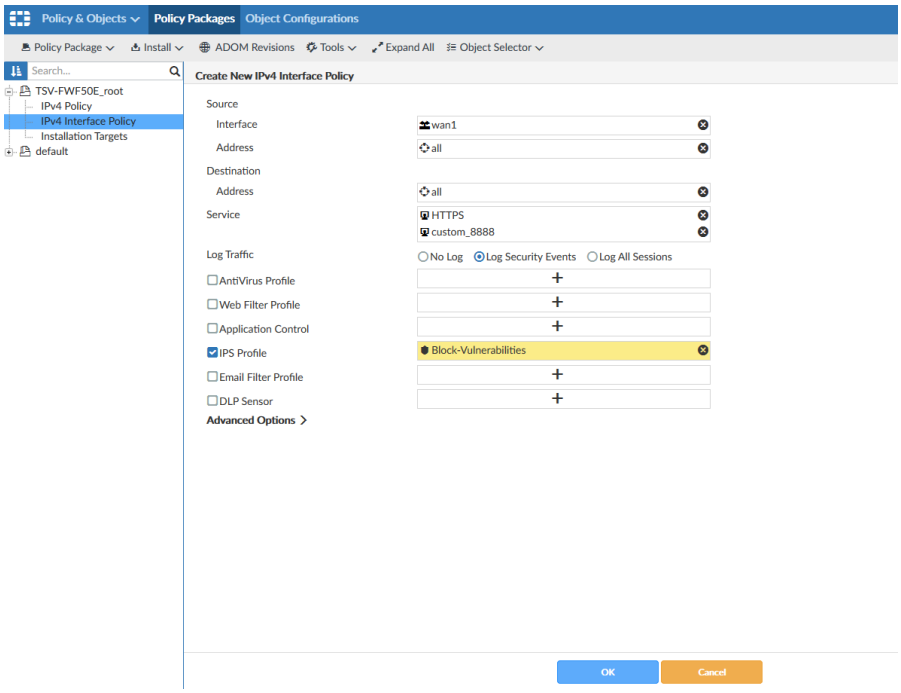


Step 3) Configure Interface policy *(for scenario when the FortiGate is directly connected to Internet)*

- In “Policy & Objects” > “Policy Packages”, navigate to the policy package serving your FortiGates(s) and under “IPv4 Interface Policy” and click on the “+ Create New” button



- Select the interface connected to the Internet under “Interface”
- Under “Service” select “HTTPS” and the custom service defined in previous step “custom_8888”
- Enable “IPS Profile” and select the IPS Sensor created/edited in step #1 (e.g., “Block-Vulnerability”)



Note: In case the FortiGate has multiple interfaces connected to Internet, configure the interface policy for all such Internet-facing interfaces.

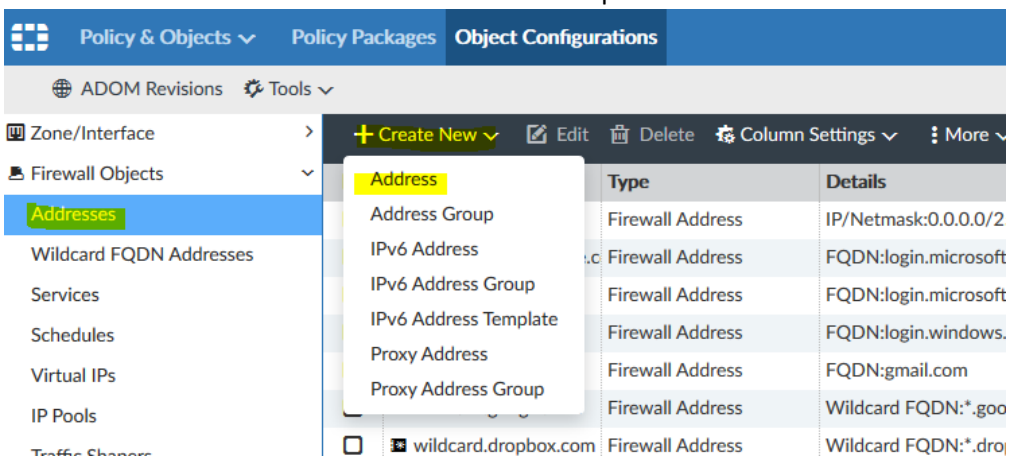
The next step is for the scenario where FortiGate is a perimeter gateway with multiple Fortinet products in protected network.

The next two steps could be skipped if such scenario is not applicable to the environment.

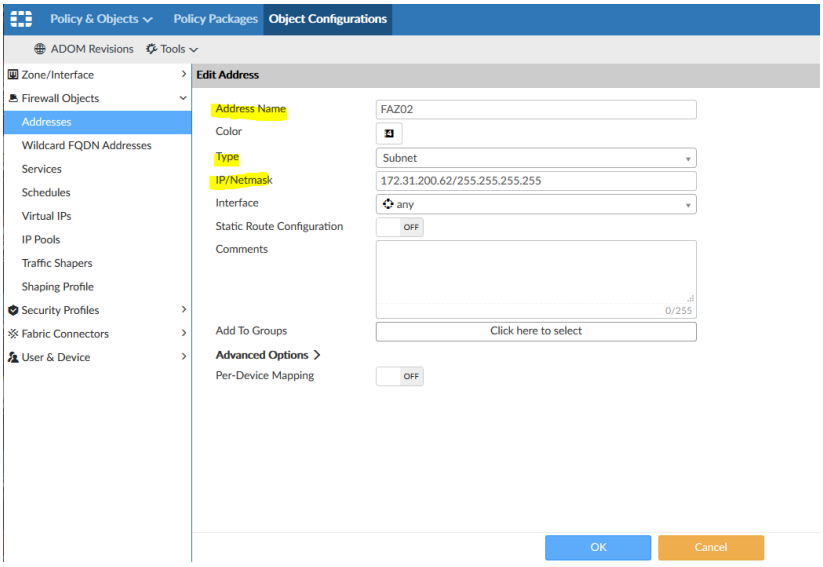
Step 4) Configure address objects for all Fortinet devices in customer network

Note: If the address objects are already configured, skip to the next step.

- In "Policy & Objects" > "Object Configuration", navigate to "Firewall Objects">" Addresses", click on the "+ Create New" button and select "Address" in dropdown list:



- In the next screen, Enter Address name, for example "FAZ02"
- Select type "Subnet".
- Subnet / IP Range > Enter the IP address of the device.
- Click "OK" to save the Address object.

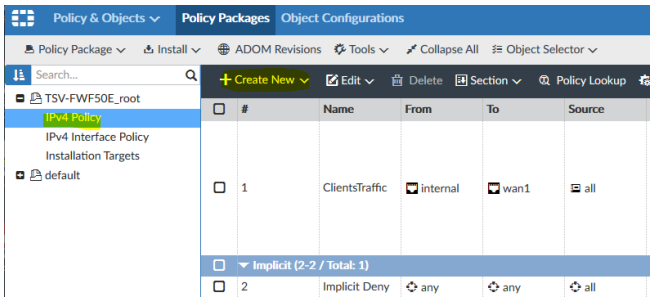


- Repeat for all Fortinet devices in protected network

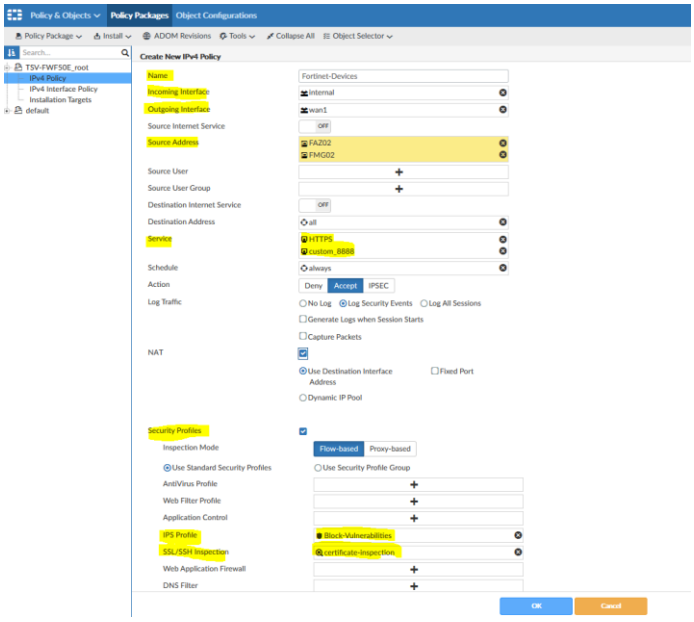
Step 5) Create firewall policy with IPS sensor

(for scenario FortiGate as a perimeter gateway with multiple Fortinet products in protected network)

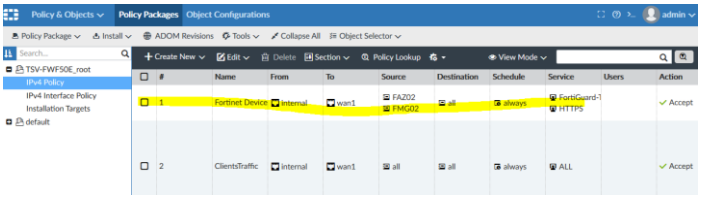
- In “Policy & Objects” > “Policy Packages”, navigate to the policy package serving your FGT(s) and under “IPv4 Policy” and click on the “+ Create New” button



- In the new policy page, Configure the following;
  Name > policy name, for example "Fortinet-Devices"
  Incoming Interface : Interface connected to Fortinet Devices
  Outgoing Interface : Interface connected to Internet
  Source : add addresses of Fortinet devices created in previous step.
  Destination :Destination Address “all”
  Service : select “HTTPS” and the custom service defined earlier “custom_8888”
  SSL/SSH Inspection : certificate-inspection

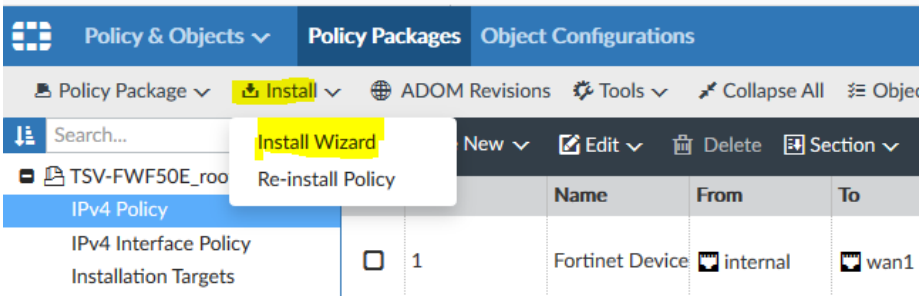


- If it is needed move new policy to be on the top of others

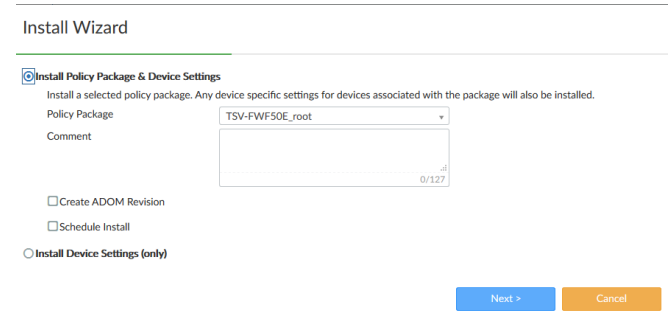


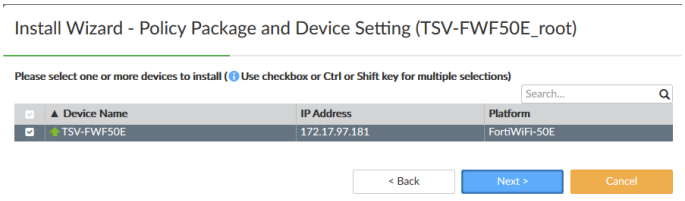
Step 6) Deploy configuration changes to FortiGate

- In “Policy & Objects” > “Policy Packages”, click on “Install” and on “Install Wizard” in dropdown list

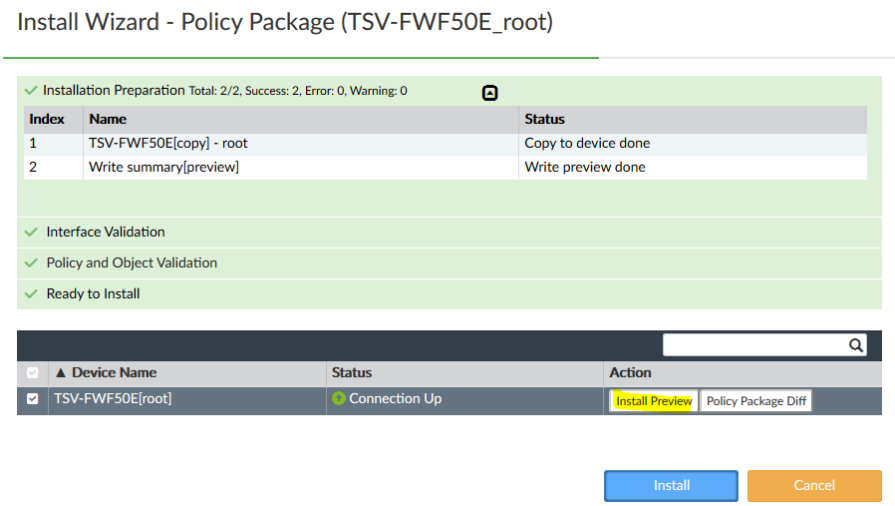


- In next steps, chose the policy package and devices where the configuration needs to be installed



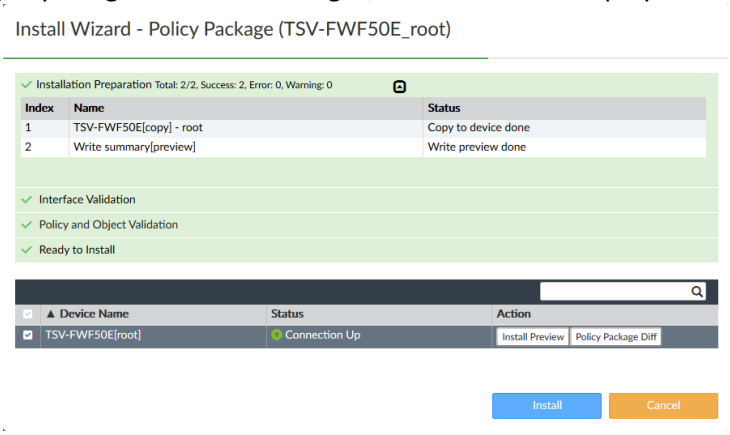


- In Installation Preparation window click on Install Preview and review the changes



- Review the changes. If it is needed it could be downloaded into a text file. Click close to close the window.

- After reviewing, if you agree with the changes, click "Install" to deploy them.



- OK status confirms that the changes been deployed successfully.