1. In the Forefront TMG Management console tree, click **Firewall Policy**.
2. On the **Tasks** tab, click **Enable Intrusion Detection**.
3. On the **Common Attacks** tab, select **Enable intrusion detection**.
4. Select one or more of the following:
   * **Windows out-of-band (WinNuke)**. Select this option when Forefront TMG will generate an event if an out-of-band denial of service attack is attempted against a computer protected by Forefront TMG.
   * **Land**. Select this option when Forefront TMG will generate an event if a TCP SYN packet is sent with a spoofed source IP address and port number that matches that of the destination IP address and port number.
   * **Ping of death**. Select this option when Forefront TMG will generate an event if an IP fragment is received with more data than the maximum IP packet size.
   * **IP half scan**. Select this option when Forefront TMG will generate an event if repeated attempts to connect to a destination computer are made and no corresponding ACK packets are communicated.
   * **UDP bomb**. Select this option when Forefront TMG will generate an event if there is an attempt to send an illegal UDP packet. Although an event will be generated when the attack occurs, you must specifically enable and configure an alert to trigger an action.
   * **Port scan**. Select this option when Forefront TMG will generate an event if an attempt is made to count the services running on a computer by probing each port for a response.
5. If you selected **Port scan**, also specify the following:
   * **Detect after attacks on well-known ports**. Type the maximum number of well-known ports that can be scanned before generating an event when a port scan attack is detected. A well-known port is any port in the range from 1 through 2048.
   * **Detect after attacks on ports**. Type the maximum number of ports that can be scanned before generating an event when a port scan attack is detected.
6. If you want Forefront TMG to log all dropped packets, verify that **Log dropped packets** is selected.
7. Click **OK**.
8. In the details pane, click the **Apply** button to save and update the configuration, and then click **OK**.

Source: https://technet.microsoft.com/en-us/library/cc984458.aspx