DefensePro X
Version 10.x

Training Lab Manual
Configure Out of State Protection

Table of Contents

Contents

OVERVIEW 3
SETUP OUT OF STATE PROTECTION 3
CONFIGURE OUT OF STATE PROTECTION 4
TEST THE CONFIGURATION 4

Overview

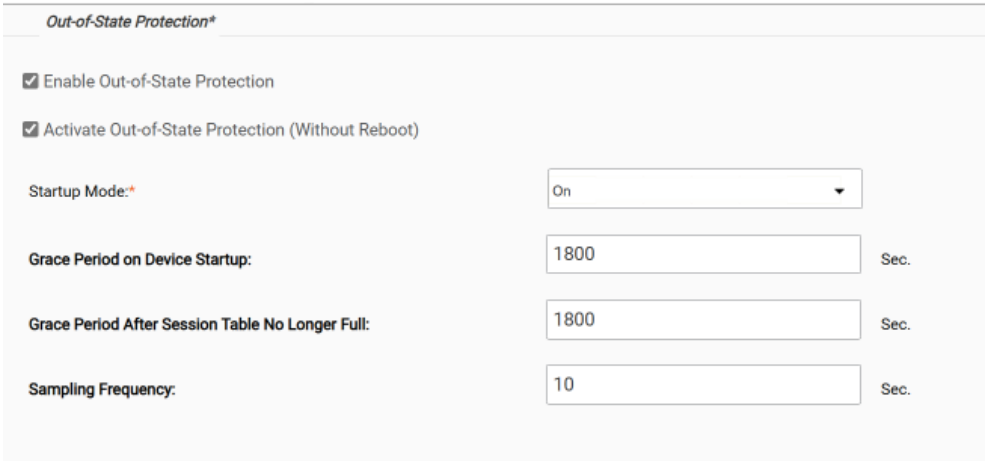
An Out of State attack is a network level denial of service attack where first packet isn't a SYN packet.

The TCP protocol, which is used for sending data over the internet, has certain characteristics that make it difficult to use Behavioral DoS (Denial of Service) mechanisms to defend against specific types of attacks sending an ACK or PSH-ACK flood.

In these situations, a different defense method called "Out of State protection" can be used. This method helps by identifying and blocking these unusual messages that don't fit the normal pattern of communication.

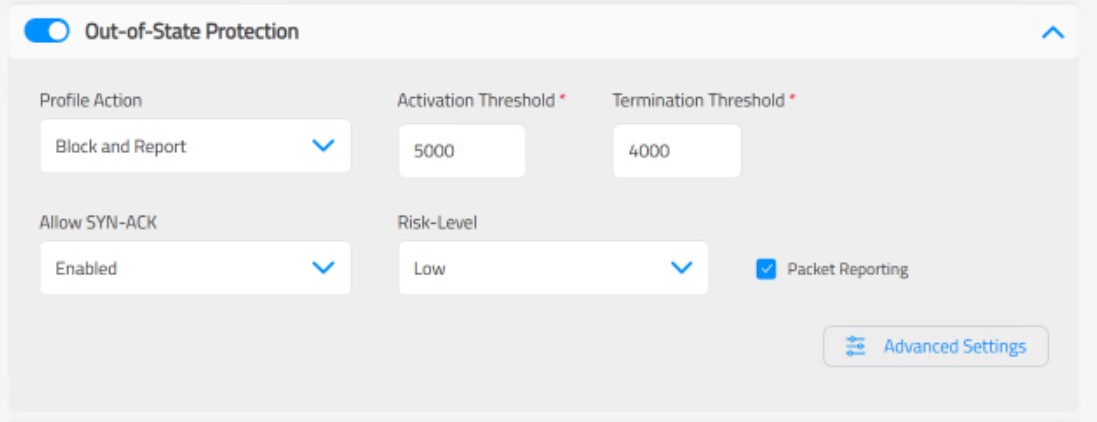
Does that make sense? If you have any questions, feel free to ask!Setup Out of State Protection

1. Select the **Configuration** perspective.
2. In **Setup** section, select **Security Settings** and then **Out-of-State Protection**.
3. By default this feature is enabled.
4. You can configure:
    a. Startup mode
    Set this one to **On** in the lab.
        i. **On** — Start Out-of-State Protection action immediately after startup (with no time to learn traffic and sessions). Sessions that started before startup get dropped. Only new, valid sessions are allowed.
        ii. **Off** — Do not start Out-of-State Protection after startup or reboot.
        iii. **Graceful** — After startup, start learning sessions (and updating the Session table) for the time specified by the Startup Timer parameter. Then, begin Out-of-State Protection actions.
    b. Grace Period on Device Startup (default 1800)
    c. Grace Period After Session Table No Longer full (default 1800)
    d. Sampling Frequency (default 10)
5. Once you change the **Startup Mode** to **On**, click on **Submit**.



Configure Out of State Protection

1. Select the **Security Operations → Security Settings** and edit the TeamXX security policy.
2. Enable **Out-ofState Protection**.
3. Click on **Advanced Settings** to review but leave the parameters default.



4. Enable as well the **BDoS Protection** again.
5. Click **Submit** button to apply the policy.

Test the Configuration

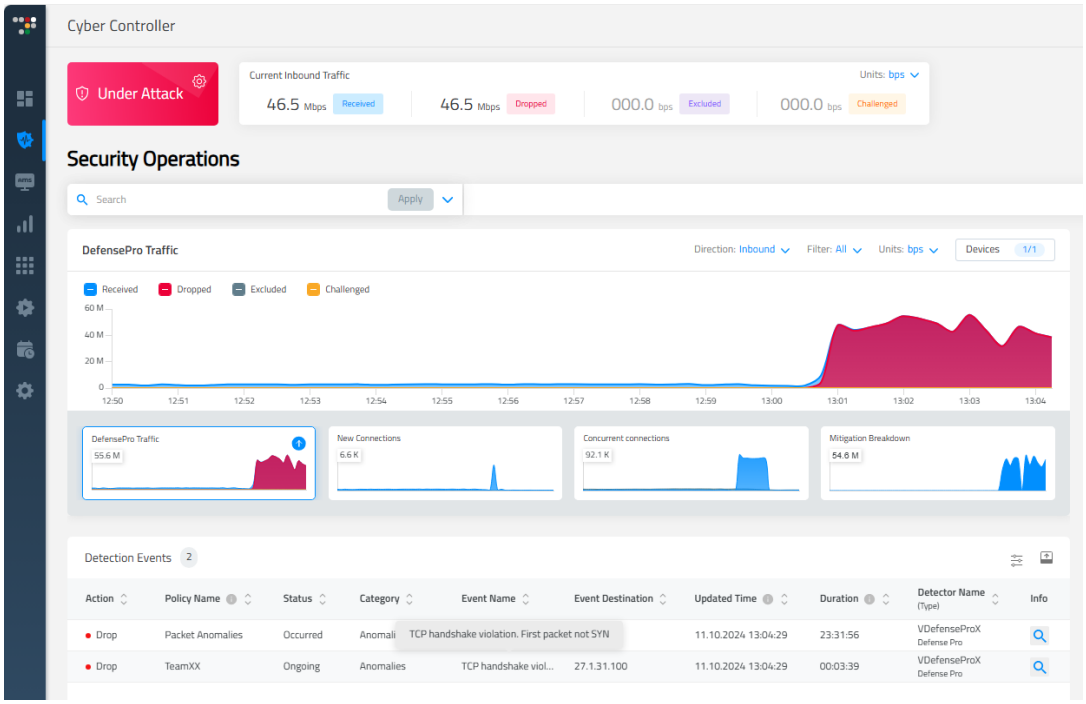
Use hping3 to send Out-of-State Attack

1. In the shell prompt type: **hping3 -p 80 -A --rand-source --flood 27.1.31.100**

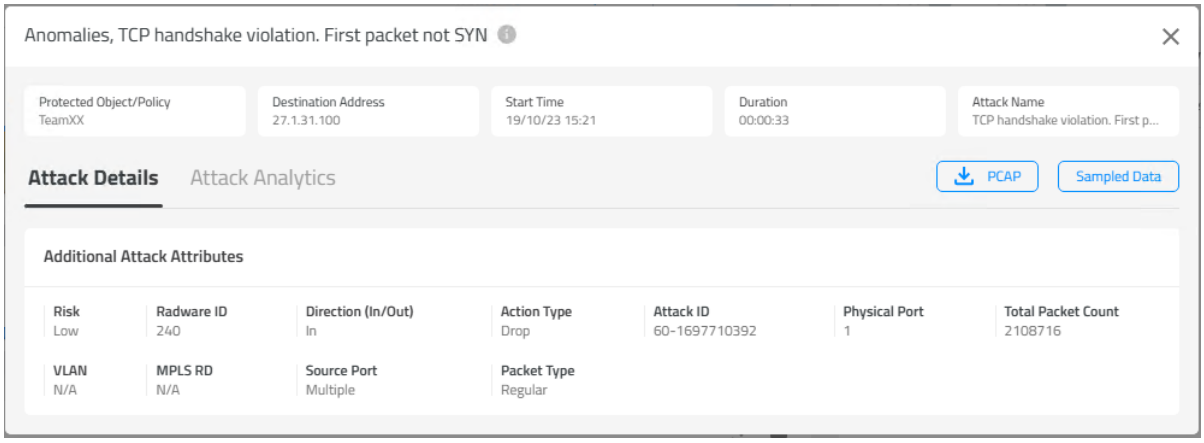
   - hping3: This is the program name. hping3 is a network tool for crafting and analyzing IP packets.
   - -p 80: This option specifies the destination port for the packet. Here, 80 targets the standard HTTP web traffic port.
   - -A: This option instructs hping3 to send a packet with an ACK flag. In TCP communication, the ACK flag is used to acknowledge the receipt of packets.
   - --rand-source: This tells hping3 to use random source IP addresses for the packets it sends.
   - --flood: Puts hping3 in flood mode, sending packets as fast as possible without waiting for replies. It's typically used for network stress testing or for executing denial of service (DoS) attacks.
   - 27.1.31.100: This is the target IP address for the packets.

   Soon after the attack is initiated from the Attack-PC, you see traps in the CLI/Syslog.

2. Use Cyber Controller to View Out-of-State Attack. Select the **Security Operations → Real-Time Monitoring** perspective.



3. View your policy under **Detection Events**. Click on the Info/maginfying glass icon to examine the **Anomalies TCP handshake violation** event.



4. At Attacker shell **stop** the attack. (CTRL-C).
5. Try a PSH-ACK flood: **hping3 -p 80 -PA --rand-source --flood 27.1.31.100**

   - -PA: This option instructs hping3 to send packets with both the SYN and ACK flags set in the TCP header.

6. Repeat the views above to examine the attack.
7. At Attacker shell **stop** the attack. (CTRL-C).
8. **Export** and save configuration file as **dpx-OOSLab-config.txt**.

For questions, contact training@Radware.com