Best Practice - Protect Against TCP SYN Flooding Attacks with TCP Accept Policies

https://campus.barracuda.com/doc/48202755/

In order to establish a TCP connection, the TCP three-way handshake must be completed. You can use different accept policies to change how incoming and outgoing TCP connections are handled on a per rule basis. Depending on the purpose of the firewall rule, choose one of the two TCP accept policies:

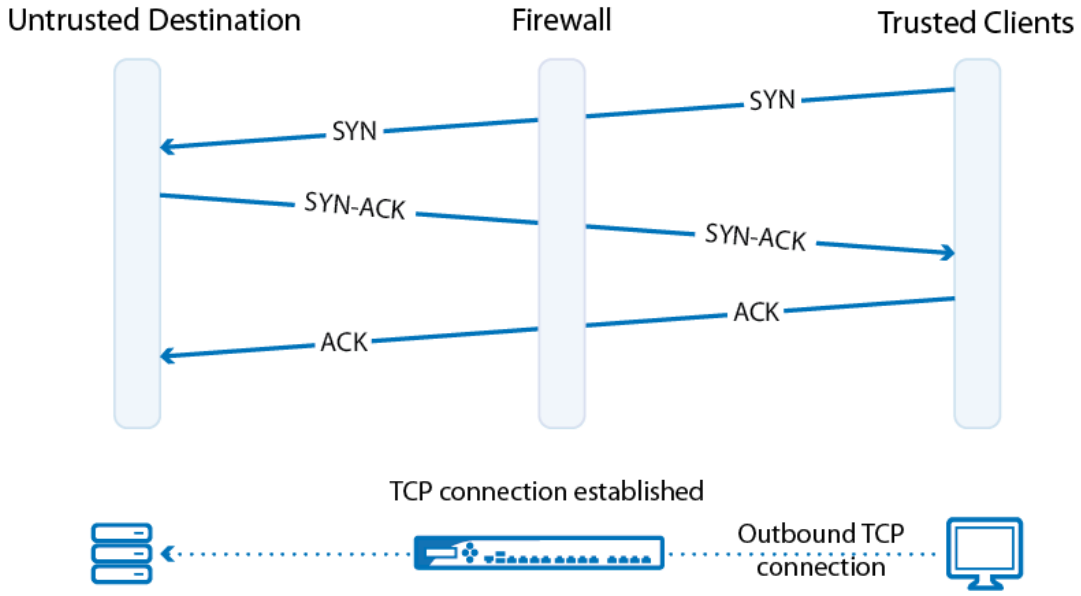
- **Outbound Accept Policy** – Use the outbound accept policy when trusted clients access untrusted networks. TCP session requests (SYN packets) are immediately forwarded to the target address if the session is allowed by the rule set. The TCP handshake occurs between the source and destination.
- **Inbound Accept Policy** – Use the inbound accept policy to protect servers against untrusted networks. TCP session requests (SYN packets) are NOT immediately forwarded to the target address even if the session is allowed by the rule set. The firewall rather establishes a complete TCP handshake with the requesting source first, assuring that the requestor is authentic (no IP spoofing) and really intends to establish a TCP session. Only after a complete TCP handshake is established, the handshake with the target is catched up and traffic will be forwarded to the target address.

To guard against DoS/DDoS attacks, configure the maximum number of new sessions and the allowed total number of sessions from a single source (**Max. Number of Sessions/Max. Number of Sessions per Source**) to protect against resource exhaustion of the Barracuda NextGen Firewall F-Series. These settings are also configured on a per-rule basis.

TCP SYN Flooding Attacks and Countermeasures

This example shows how the outbound and inbound accept policies handle TCP connections and which policy to use:

Outgoing TCP Connection with Outbound Accept Policy Enabled



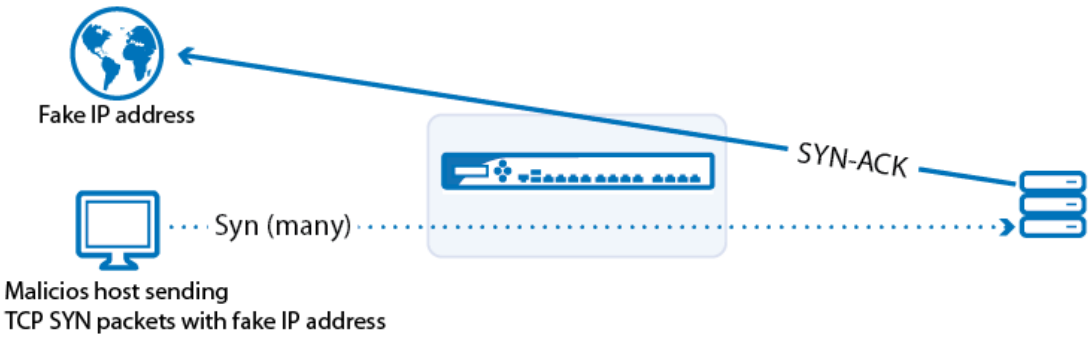
The main characteristic of the outbound policy is that the client only receives an ACK when the requested server is really up. This is important for many applications, such as a browser when it tries to connect to a server with many IP addresses for the same hostname (DNS round robin). The browser tries to connect to the first IP address it receives from the DNS server, and, if it is not successful, it tries the next one and so on. Hence, it is fatal if the firewall sends an ACK to the client if the server cannot be reached because then the browser never gets the chance to try the other IP addresses.

If you use this outbound TCP accept policy in a firewall rule forwarding traffic to an internal server, you open yourself up to a simple attack:

- **Step 1** – The unfriendly host fakes its IP address and gives itself an address, which is already in use in another network. Replies are sent to the remote network.
- **Step 2** – It then sends as many SYN packets as possible to the protected server.
- **Step 3** – The firewall simply lets the SYN packets pass through, using up its own and the protected server's resources. The SYN-ACKs are sent to the fake IP address which does not answer, keeping the connection in a pending state until it times out.
- **Step 4** – After a certain number of unanswered SYN-ACKs, the firewall recognizes the unfriendly activity and no longer accepts SYNs from the (faked) source IP address.

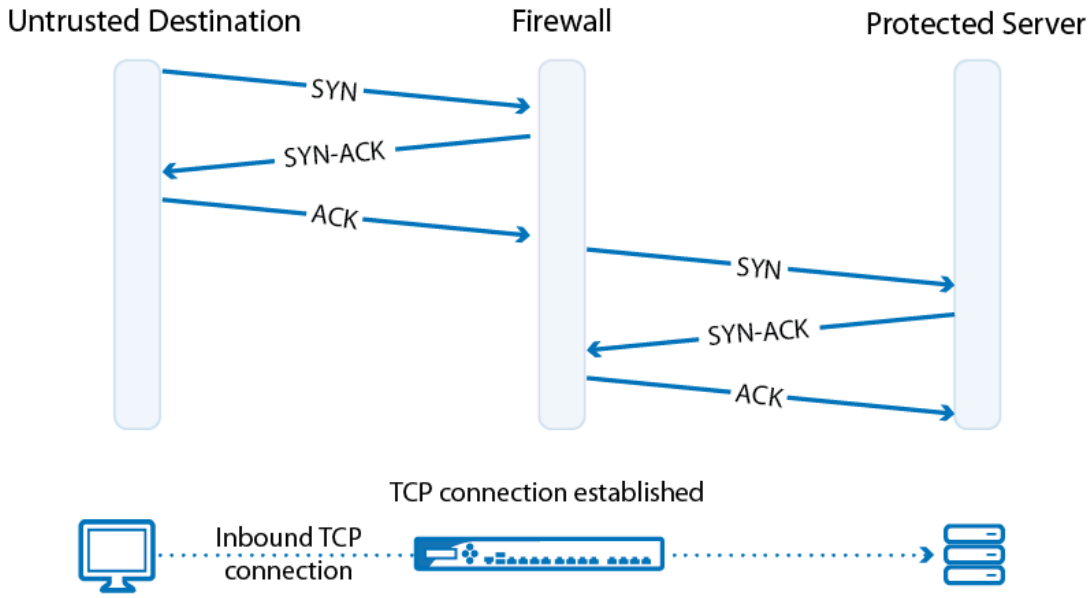
If the unfriendly host can change its IP address quickly enough, it can do this very often without a chance for the firewall to differentiate between the attack and ordinary requests.

A simple SYN flooding attack with faked IP addresses on a firewall with the outbound accept policy:

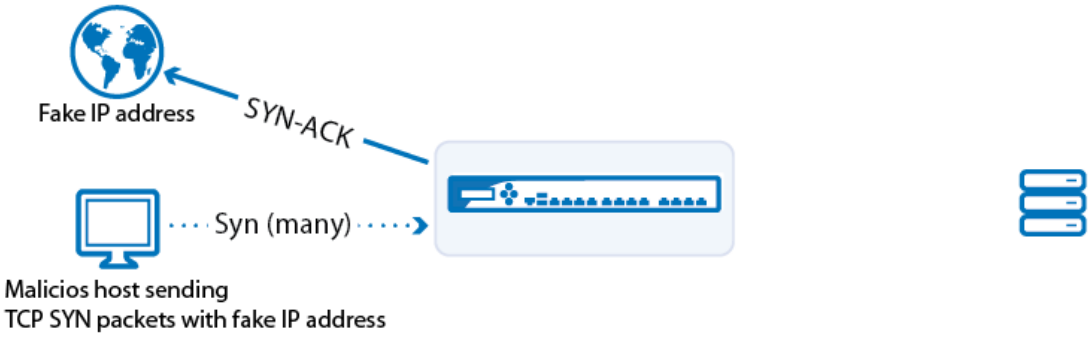


The outbound policy tells the firewall to complete the connection with the server first (verifying it is up) and then complete the connection to the client. In this case, the server eventually exhausts its resources by creating TCP connections for the fake requests. The solution to the problem is to set the **Accept Policy** of the rule to **Inbound**. This means the firewall first returns a SYN-ACK to the clients source IP address, thus verifying its real wish for a connection. Only if the connection is completed by an ACK packet, does the firewall finish building up the TCP connection to the protected server. If the source IP address is fake, the ACK packet never arrives and the firewall does not initiate the TCP connection to the protected server.

Incoming TCP Connection with Inbound Accept Policy Enabled



The same TCP SYN flooding attack on a server using the inbound accept policy:



The server does not even notice that a TCP SYN flooding attack has been launched and can continue to use its resources for valid requests, while the firewall deals with the TCP SYN flood attack. The firewall does not have to use a lot of resources because a SYN request matching a rule with inbound policy is neither logged nor appears in real time status nor in the access cache until it is categorized as a valid TCP connection. To further protect the server, you can assign limits to the total amount of sessions and the maximum number of sessions coming from one source. Set the maximum number of sessions lower than the **Max Session Slots** (**Box > Infrastructure Services > General Firewall Configuration**). If one of the limits are exceeded, further connection attempts are ignored.

Configure the TCP Accept Policies and Thresholds

To configure the settings, proceed with the following steps:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a new firewall rule or edit an existing rule.
4. In the **Edit Rule** window, select **Advanced** from the left menu.
5. You can configure the handling of **Accept Policies** within the following sections:
   - **TCP Policy** section:
     - **Syn Flood Protection (Forward)** – Select the TCP accept policy depending on what the rule is used for. For example, if the rule is used to forward traffic to a web server, select **Inbound**.
     - **Syn Flood Protection (Reverse)** – Used if the firewall rule is bi-directional. Select the TCP accept policy for the reverse connection.
   - **Resource Protection** section:

     Use the following parameters only if you encounter frequent DoS/DDoS attacks. If you set the threshold too low, it will result in blocked connections.

     - **Max. Number of Sessions** – The maximum number of accepted concurrent connections for this rule on a global basis.
     - **Max. Number of Sessions per Source** – The maximum number of accepted

concurrent connections for this rule on a per source address basis (default: = unlimited).

6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Events triggered by SYN Flood Attacks

If eventing is activated, the following events can be triggered by a TCP SYN flooding attack:

- **FW IP Spoofing Attempt Detected [4014]** or **FW Potential IP Spoofing Attempt [4015]**
- **FW Rule Connection Limit Exceeded [4016]** – Is triggered when the **Max Number Of Sessions** has been reached.
- **FW Rule Connection per Source Limit Exceeded [4018]** – Is triggered when the **Max Number of Sessions per Source** has been reached.

Figures

1. tcp_accept_outbound.png
2. tcp_accept_outbound_attack.png
3. tcp_accept_inbound.png
4. tcp_accept_inbound_attack.png