

Configuring an IPS sensor to protect against common attacks

Go to **Security Profiles > Intrusion Protection > IPS Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.

Create a new IPS filter. Set the **Target** to **server** and set the **Action** to **Block All**.

Apply

Sensor Type Filter Based Specify Signatures

[Filter Options]

Severity

- critical
- high
- medium
- low
- info

Target

- client
- server

OS

- BSD
- Linux
- MacOS
- Other
- Solaris
- Windows

| Name | Severity | Target | OS |
|--|----------|----------------|---------|
| 2Wire.Wireless.Router.XSRF.Password.Reset | medium | server, client | Windows |
| 3Com.3CDaemon.FTP.Server.Buffer.Overflow | high | server | Windows |
| 3Com.Intelligent.Management.Center.Directory.Traversal | medium | server | Windows |
| 3Com.Intelligent.Management.Center.Information.Disclosure | medium | server | Windows |
| 3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS | medium | server | Windows |
| 4D.WebStar.FTP.Command.Buffer.Overflow | high | server | Windows |
| 4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow | medium | server | Windows |
| 7T.IGSS.ODBC.Server.Memory.Corruption | medium | server | Windows |
| 7T.Interactive.Graphical.SCADA.File.Operations.Buffer.Overflow | high | server | Windows |
| 7Technologies.IGSS.SCADA.System.Directory.Traversal | medium | server | Windows |
| 427BB.Cookie.Based.Authentication.Bypass | medium | server | All |
| 427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection | medium | server | All |
| 1024CMS.Standard.PHP.File.Inclusion | high | server | Windows |
| ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow | critical | server | Windows |

1 / 206 [Total: 2877]

Action Signature Defaults Monitor All Block All Reset Quarantine

Packet Logging

Adding the IPS sensor to a security policy

Go to **Policy > Policy > Policy**. Edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** and set it to use the new sensor.

Policy Type Firewall VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Logging Options

No Log

Adding a DoS security policy

Go to **Policy > Policy > DoS Policy**.

Create a new policy. The **Incoming Interface** is your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.

Incoming Interface

Source Address

Destination Address

Service

Anomalies

| Name | <input checked="" type="checkbox"/> Status | <input checked="" type="checkbox"/> Logging | Action | Threshold |
|------------------|--|---|--------|-----------|
| tcp_syn_flood | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 20 |
| tcp_port_scan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 1000 |
| tcp_src_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 5000 |
| tcp_dst_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 5000 |
| udp_flood | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 2000 |
| udp_scan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 2000 |
| udp_src_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 5000 |
| udp_dst_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 5000 |
| icmp_flood | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 250 |
| icmp_sweep | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 100 |
| icmp_src_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 300 |
| icmp_dst_session | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Block | 1000 |

Results



WARNING: Causing a DoS attack is illegal, unless you own the server under attack. Before performing an attack, make sure you have the correct server IP.

Perform an DoS `tcp_sync_flood` attack to the web server IP address. IPS blocks the TCP sync session when it reaches the `tcp_syn_flood` threshold, in this case 20.

Go to **Log & Report > Security Log > Intrusion Protection** to view the results of the DoS policy.

Select an entry to view more information, including the severity of the attack and the attack name.

wnload Raw Log

| Severity | Src | Protocol | Count | Attack Name | Attack ID | Level | |
|----------|----------------|----------|-------|---------------|-----------|----------|----------------------------|
| critical | 172.20.120.123 | tcp | 4 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 3 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 2 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 1 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 5 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 9 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 2 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 7 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 3 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 4 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 2 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |
| critical | 172.20.120.123 | tcp | 11 | tcp_syn_flood | 100663396 | critical | anomaly: tcp_syn_flood, 21 |

| | | | |
|-----------------|--|-----------------|--|
| Dst | 172.20.120.24 | Virtual Domain | root |
| Protocol Number | 6 | Severity | critical |
| Service | http | Protocol | tcp |
| Identity Index | 0 | Message | anomaly: tcp_syn_flood, 21 > threshold 20, repeats 4 times |
| Dst Port | 80 | Reference | http://www.fortinet.com/ids/VID100663396 |
| roll | 65522 | Status | clear_session |
| Timestamp | Wed Apr 24 16:04:33 2013 | Sequence Number | 0 |
| Policy ID | 0 | Src Interface | wan1 |
| Src | 172.20.120.123 | Count | 4 |
| Level | alert | Sensor | DoS-policy1 |
| pcap_id | 100663396 | Src Port | 62132 |
| Log ID | 18432 | Sub Type | anomaly |
| Attack ID | 100663396 | Attack Name | tcp_syn_flood |
| Date/Time | 04-24 16:04 (Wed Apr 24 16:04:33 2013) | | |