DDoS Protection on the Security Gateway

Best Practices

24 August 2014

Check Point Software Technologies Ltd.
We Secure the Internet.

Protected
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=35013)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 August 2014</td>
<td>Penalty box is supported from R75.45 (&quot;Penalty Box&quot; on page 11).</td>
</tr>
<tr>
<td>6 August 2014</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on DDoS Protection on the Security Gateway Best Practices).
Contents

Important Information............................................................................................................. 3
Introduction.............................................................................................................................. 5
Before an Attack - Best Practices.......................................................................................... 6
  Recommended Gateway Settings ......................................................................................... 6
  Traffic Monitoring and Bandwidth Provisioning ................................................................. 7
When Under Attack................................................................................................................ 8
  Mitigation Strategy............................................................................................................... 8
  Volumetric Attacks and Gateway Protections ...................................................................... 8
  Slow Attacks and Gateway Protections .............................................................................. 9
Key DDoS Protections on the Gateway .................................................................................. 10
  SYN Attack Protection ...................................................................................................... 10
  Rate Limiting for DoS Mitigation ....................................................................................... 11
  Penalty Box ........................................................................................................................ 11
Other DDoS Gateway Protections ......................................................................................... 12
  Gateway Settings for Web Attacks ..................................................................................... 12
  Network Quota ................................................................................................................... 12
  Geo Protections .................................................................................................................. 12
  Global State Table Values ................................................................................................. 12
Summary of Gateway DDoS Protections and Identification ................................................... 13
Check Point Incident Response Services ............................................................................. 14
Introduction

With the upsurge in Distributed Denial of Services (DDoS) activity and the continued increase in the size and intensity of the incidents, Check Point recommends that customers consider a comprehensive DDoS solution that includes a combination of:

- Dedicated DDoS protection technologies, including the Check Point DDoS Protector appliance.
- DoS Enhancements in the Check Point Gateway.
- Check Point Incident Response Service.

Use this document:

- To learn how to harden your Check Point Security Gateways for a DDoS attack in networks that are not protected by the Check Point DDoS Protector appliance.
- As first-aid resource when under a DDoS attack.
Before an Attack - Best Practices

To be able to handle a DDoS attack, you need to prepare a DDoS strategy ahead of time. We recommend that you:

- Optimize the Security Gateway to mitigate attacks.
- Make preparations upstream from your Security Gateway. For example, overprovision your Internet pipe.

Recommended Gateway Settings

Here are some recommended Best Practices to harden Security Gateways and prepare for a DDoS attack.

   Supported from R76

2. **Aggressive Aging settings** — These settings manage the connections table capacity and memory consumption of the firewall. They allow the Security Gateway to handle large amounts of unexpected traffic, especially during a Denial of Service attack. Aggressive Aging starts to operate when the gateway still has available memory and the connections table is not entirely full. This reduces the chance of connectivity problems during low-resource conditions.
   These are global setting. A few things should be considered, such as long term connections.
   Configure these settings in the IPS tab > Protections > By Protocol > IPS Software Blade > Network Security > Denial of Service:
   - TCP start timeout – 3 seconds
   - TCP session timeout – 300 seconds – Watch for idle connections
   - TCP end timeout – 1 second
   - UDP virtual session timeout – 5 seconds
   - ICMP virtual session timeout– 3 seconds
   Supported from R76.

3. **Multi-Queue** — A SYN Flood usually arrives at one external-facing network interface card only. The Multi-Queue feature improves the Security Gateway performance during SYN Flood attacks by configuring more than one traffic queue for each network interface card, and using more CPU dispatcher cores for traffic acceleration. Run it on machines with 2 or more cores. The supported interface card drivers are igb and ixgbe.
   Support is built-in to the Security Gateway from R76 and higher. For older versions, a Hotfix is available to add the Multi-Queue feature.

4. **DNS services on the Gateway** — Consider using a global DNS service to resolve DNS requests, so that a DNS-based attack does not reach the Security Gateways.
Before an Attack - Best Practices

Traffic Monitoring and Bandwidth Provisioning

Prepare for DDoS attacks in these ways:

Bandwidth Provisioning

- **ISP Bandwidth to the Gateway:** Generously over-provision the network bandwidth of the Internet pipe to your Security Gateways. If the pipe becomes saturated during a DoS volumetric attack, connectivity issues may make it difficult to configure changes on the gateway to fix the problem. It is good practice to use an independent management network, with a dedicated management interface on the gateway, so that management operations are not degraded by an attack.

- **Gateway Interface bonding:** Configure Link Aggregation with Load Sharing (Active/Active) to increase the available bandwidth on Gateway interfaces and ClusterXL Gateway cluster interfaces. For configuration instructions, see the *Gaia Administration Guide* for your version. Supported from R75.40 on Gaia.

Traffic Monitoring and Profiling

- **Set a TCP Traffic Baseline** - Identify how many SYN’s per second are normal, and note that behavior as a baseline. This will allow you to more effectively defend against SYN attacks using the IPS SYN Attack protection. There are a number of ways to do this, including monitoring PPS and TCPDUMP.

- **Monitor traffic bandwidth utilization** of your public services, for example HTTP/HTTPS and DNS. Run a client in the Internet and monitor its responsiveness.

- **Monitor CPU utilization** of your public Web servers, and Security Gateways.

- **Do traffic profiling.** If traffic is normally mostly HTTP/HTTPS and is suddenly 80% UDP port 70, you have a problem.

DDoS Support

- Set up a support arrangement with the Check Point Incident Response Team ("Check Point Incident Response Services" on page 14).

- Set up a support arrangement with a Scrubbing Center for DDoS protection.
When Under Attack

When under attack, take action to understand the type of attack. Some of the performance and monitoring tools that you can use are listed in the schematic diagram at the end of this guide.

Make sure that you can contact the Security Gateway to remedy the situation. If the Internet pipe to the Security Gateway is saturated, and you cannot connect to the Security Gateway, you must solve the problem upstream. Contact your ISP or Scrubbing Center to help you solve the problem.

If the line to the Security Gateway is not saturated, find out if the attack is a:

- Volumetric attack (a flood).
- Slow attack, for example, one that targets a slow internal database.

For a volumetric attack, find out if the traffic is:

- TCP (for example HTTP/HTTPS)
- Non-TCP, such as UDP (for example DNS)

Try to find out if the attack source addresses are spoofed or real.

Mitigation Strategy

Your defense strategy for protections on the Gateway should be to block the attack low in the OSI model layer, in this order:

1. System
2. SecureXL/Performance Pack
3. Firewall

Block remaining issues at higher levels. Performance may be degraded if you block attacks at these higher levels:

1. IPS
2. Application Protections

The protections and DDoS identification methods for each layer are summarized in the schematic diagram at the end of this guide. The next section shows you what to do first.

Volumetric Attacks and Gateway Protections

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Example Attack</th>
<th>Recommended Protection(s)</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Spoofed</td>
<td>The attacker sends a flood of SYNs to the server(s). Normally from spoofed, random sources. This can drain firewall resources (by filling the state tables, for example) as well as server resources.</td>
<td>SYN Attack Protection (on page 10) in Cookie mode</td>
<td>Excellent</td>
</tr>
<tr>
<td>TCP Not spoofed</td>
<td>The attacker controls the source IP addresses, maybe 1000s of them, using a botnet. SYNdefender is not effective because the attacker can complete the 3-way handshake. Also, we do not know the source addresses, so we cannot block them individually.</td>
<td>Rate Limiting for DoS Mitigation (on page 11) Penalty Box (on page 11) with IPS</td>
<td>Good</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Example Attack</td>
<td>Recommended Protection(s)</td>
<td>Effectiveness</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Non-TCP Spoofed without DNS servers behind the Gateway</td>
<td>A DNS flood of packets from many IP addresses.</td>
<td>Rate Limiting for DoS Mitigation (on page 11) of DNS</td>
<td>Excellent</td>
</tr>
<tr>
<td>Non-TCP Spoofed with DNS servers behind the Gateway</td>
<td>A DNS flood of packets from many IP addresses.</td>
<td>Rate Limiting for DoS Mitigation (on page 11): Either: Define a white list of allowed DNS hosts. Or: Any IP address is allowed a small number of DNS packets per minute.</td>
<td>Partial. If the attacker uses a large number of random sources, a large number of packets is allowed</td>
</tr>
<tr>
<td>Non –TCP Not spoofed</td>
<td>An attack from one source or a small set of distinct sources, with very high rate. Some or all of the sources are not spoofed.</td>
<td>Rate Limiting for DoS Mitigation (on page 11) Either define a rule to block the sources, Or put a rate limit on the sources (for example, no one IP address can send more than 100 packets per second.</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

### Slow Attacks and Gateway Protections

A typical slow attack happens in a Web application environment. The client talks to web server, that passes requests for dynamic content services to the application server. The application server may need services from a database. Database queries (using SQL for example), are relatively slow.

**Example Slow Attack**

The attacker sends traffic that involves many database queries. This causes a DoS on the database, with relatively little network traffic.

**Recommended Protection**

1. Identify the characteristics of the attack. For example, the URL, or some other property of the HTTP header.
2. Write a signature to block the attack. For example, use the IPS protection **HTTP Header Rejection**.
3. Turn on the Penalty Box (on page 11). If there are more than a set number of violations per second, the violation is blocked for a configurable number of minutes. This prevents the attack.
Key DDoS Protections on the Gateway

When your network resources are under attack, these are the most effective DDoS Protections to enable on the Security Gateway:

- SYN Attack Protection in SYN Cookie Mode (Supported from R65)
- Rate Limiting for DoS Mitigation (Supported from R76)
- Penalty Box (Supported from R76)
- IP Fragments (Supported from R60, enhanced in R77.20)

There are IPS protections for application-specific DoS attacks:

- DNS
  - DNS ANY Request
  - Inbound DNS Requests
  - DNS Maximum Request Length
- HTTP
  - Header Rejection
  - Web Servers HTTP POST Denial of Service
  - Web Servers HTTP Flooding Denial of Service
  - Web Servers Slow HTTP Denial of Service
  - HTTP Format Sizes

If the attacks are directed towards SMTP, there are more protections to enable, depending on the situation. See the protection descriptions for details.

SYN Attack Protection

In SYN Cookie mode, connections are not registered in the connection table until the connection proves itself legitimate. This makes the regular use of SYN Protections less performance intensive.

Configure these settings in the IPS tab > Protections > By Protocol > IPS Software Blade > Network Security > TCP > SYN Attack

- Timeout for SYN Attack Identification – 5-10 seconds
- Protect external interface Only
- Switch to SYN Active Defense upon detection of at least – 50 SYN packets per timeout
- SYN Cookie Mode (Supported from R65)

To optimize this protection, see:

- sk74480 (http://supportcontent.checkpoint.com/solutions?id=sk74480)
- sk86721 (http://supportcontent.checkpoint.com/solutions?id=sk86721)
Rate Limiting for DoS Mitigation

A policy limits traffic from specific sources and services. For example, you can configure a limit that allows any IP address a maximum of 5 concurrent connections. Even if the attacker controls a botnet with thousands of nodes, the gateway is able to handle all the connections.

The policy is configured using a command line. A policy rule has these parts:

- **Match**: By one or many sources, destination, or country.
- **Limit**: This can be enforced by bandwidth and packet rate, number of concurrent connections, and connection rate.
- **Action**: Drop, notify, or bypass.


Supported from R76.

**Example of Rate Limiting HTTP Connections:**

This rule limits connections on TCP port 80 to the server at 192.168.3.4. The limit is 20 new connections per second, per client, and the rule times out after 1 hour (3600 seconds):

```
fw samp add -a d -l r -t 3600 quota service 6/80 destination cidr:192.168.3.4/32 new-conn-rate 20 track source flush true
```

If a majority of the DoS traffic is coming from a specific region, add the source option to the rule. For example, this rule applies only to hosts from Botland, with country code QQ (an imaginary country):

```
fw samp add -a d -l r -t 3600 quota service 6/80 source cc:QQ destination cidr:192.168.3.4/32 new-conn-rate 20 track source flush true
```

**Example of a rule with ASN:**

This rule drops all packets (-a d) with the source IP address in the IPv4 address block (cidr:192.0.2.0/24), from the autonomous system number 64500 (asn:AS64500):

```
fw samp -a d quota source asn:AS64500,cidr:192.0.2.0/24 service any pkt-rate 0 flush true
```

Penalty Box

The Penalty Box makes sure that packets that arrive from suspected sources are dropped early, and improves performance under heavy load, such as caused by a DDoS attack.

If traffic through the gateway commits more than a configured number of violations per second, the source IP address enters a penalty box for a period of time (the default is 3 minutes). During that time, traffic from that IP address is slowed or blocked.

There are two kinds of violations:

- Firewall rule violation – The connection is matched to a Drop rule, and blocked.
- IPS violation – Traffic is matched to a signature of any IPS protection, and blocked.

For configuration details, see sk74520 ([http://supportcontent.checkpoint.com/solutions?id=sk74520](http://supportcontent.checkpoint.com/solutions?id=sk74520)).

Supported from R75.45. Some options are only available in higher versions. See sk74520.
Other DDoS Gateway Protections

Gateway Settings for Web Attacks

If you determine that the attack involves authentic web traffic, change the settings of the TCP services HTTP and HTTPS.

1. In the TCP Service Properties window, click Advanced.
2. In the Advanced TCP Service Properties window:
   - Session Timeout, Other: 300 sec (5 min)
   - Aggressive Aging Timeout, Other: 15-30 seconds

Supported from R65

Network Quota

Configure the maximum number of network connections allowed from the same source, for a specified number of seconds.

1. Do a full analysis of the environment. Find the normal rate of connections per second from hosts to the specific application or host.
2. In SmartDashboard, open the IPS tab.
3. Click Protections > By Protocol > IPS Software Blade > Network Security > IP and ICMP.
4. Double-click Network Quota.
5. In the Protection Details window > Network Exceptions, add the specific host or application as the Source.
6. In the Protection Details window > General, click Edit.
7. Set the connections per second, according to your environment.
8. Click Advanced and set the number of seconds during which connections from one source will be dropped.

Supported from R65. For R76 and higher use Rate Limiting for DoS Mitigation (on page 11) instead.

Geo Protections

In some cases, overall business survivability takes precedence over the continued operations of a specific country. Before activating Geo Protections, consider blocking specific countries regions during the initial first wave of an attack. This traffic can be isolated for a period of time while a more refined method of protection is established.

Configure these settings in the IPS tab > Geo Protection.

Supported from R70.20. For R76 and higher use Rate Limiting for DoS Mitigation (on page 11), which is a more efficient geographic solution.

Global State Table Values

Lowering the TCP and UDP timeout values globally can help keep the state tables from filling up during an attack.

Lowering these values could have an impact on applications, especially for users who are very far away from the data centers. It is therefore important to monitor the environment while changing these settings.

Configure these settings in the Global Properties > Stateful Inspection.

- TCP start timeout: Lower to 2-5 seconds, and monitor the effect.
- UDP session timeout: Lower to 2-5 seconds for traffic like DNS, and monitor the effect.

Supported in all versions.
**Summary of Gateway DDoS Protections and Identification**

This diagram shows the Gateway protections, and some of the performance and monitoring tools that you can use to identify attacks.

The protections and identification methods are shown per layer. Your defense strategy should be to block the attack in the lowest layer possible. In general, higher layer protections consume more CPU resources.

<table>
<thead>
<tr>
<th>Low CPU</th>
<th>High CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating/Kernel</strong></td>
<td><strong>System Level Layer</strong></td>
</tr>
</tbody>
</table>
| 64bit OS Recommended Core XL MultiQueue | **Performance Analysis** -sk33781**  
Operating System Interface RX/TX Tuning |
| **SecureXL – Performance Pack Layer** | **SecureXL Monitoring** |
| SecureXL Controls  
Penalty Box – R75.4+ sk74520  
Enhanced Durability Feature – sk33239  
DoS Mitigation in SIM – R76  
Fragmented/Options Drop – sk74520.sim erdos (-o/-f)  
Accelerated Drop Rules – sk67861 | SecureXL Monitoring  
Penalty Box - “sim erdos -z”  
Enhanced Durability Feature -cat /proc/ppk/hlqos  
Drop Templates – fwacct stats -d  
Accelerated Drop Rules - “sim dropcfg -l”  
Determine Accelerated vs non-Accelerated Flow |
| **Firewall Layer** | **Firewall Monitoring** |
| Firewall Controls  
Protections: SYN Attack, Fragment Packet, Network Quota, Non-TCP Flooding  
Settings: Global State Table, Aggressive Aging, Services State Timer SAM Rules | Firewall Monitoring  
Blade Logs Monitoring Blade Concurrent Connection/New Connection Count/PPS |
| **IPS Layer** | **IPS Monitoring** |
| IPS Controls  
Geo Protections – block specific countries or regions  
Snort IPS Rules – R75.4OVS/R76  
Microsoft TCP IP Selective Acknowledgement  
TCP Window Size Enforcement Sequence Verifier TLS Renegotiation Attacks | IPS Monitoring  
IPS CPU Consumption – sk43733 |
| **Application Layer Protections** | **Application Monitoring** |
| Application Controls  
General HTTP Worm Catcher – block specific URL  
DNS ANY Request Malformed Packet  
General DNS Settings HTTP Header Rejection Security Servers | Application Monitoring  
IPS CPU Consumption – sk43733 “top” |
Check Point Incident Response Services

The Check Point Incident Response Service helps customers prepare for and respond to any security breach with 24/7 dedicated experts help to speed recovery and return to business as usual.

The Incident Response Service operates 24x7 around the world. Access to the service is available through an annual retainer contract. Deliverables of the service include: real-time remediation assistance, rule-base and protection activation recommendations, traffic and attack analysis, custom protection development, recommendations for configuration changes for third-party systems and service providers as well as incident reports and post event data collection and analysis.

For customers with established incident response programs, the Check Point service becomes an extension of internal incident response teams. Providing advanced product expertise and with direct access to developers and threat specialists, the Check Point experts augment internal capabilities, either onsite or remotely, as required.

Check Point’s ThreatCloud is the first collaborative network to fight cybercrime. It incorporates over 250M addresses analyzed for Bot discovery, over 4.5 million malware signatures and more than 300,000 malware-infested websites. Incident Response customers gain additional value from ThreatCloud though the uploading of their log data into the ThreatCloud infrastructure. With the expansion of the ThreatCloud initiative, Check Point engineers have real-time access to general attack trends and customer specific event data. Incidents can then be analyzed to pinpoint attack methodologies and source information. They can also compare against an ever-expanding database of threat intelligence.

When a security incident occurs, call the Check Point Incident Response Hotline: +1-866-923-0907

A conference call line is immediately opened to assess and triage the event. Your system and network resources are analyzed and a baseline pattern is established. Logs and malware are analyzed and recommendations and remediation are documented in your Incident Report and Incident Response Portal.