Deployment Guide

DDoS Protection for Web and DNS Servers

TABLE OF CONTENTS

1 INTRODUCTION

Denial of Service (DoS) and Distributed DoS (DDoS) attacks are a prevalent and ever-increasing threat. The organizations at risk have spread from “obvious” targets, such as government agencies and the largest organizations, to mid-size financial institutions and charitable foundations. High-profile DDoS attacks have increased dramatically over the last few years, leaving every Internet-based business or web site at potential risk.

The A10 Thunder and AX Series Application Delivery Controllers (ADCs) add another security layer for load balanced servers and applications. Adding to an in-depth defense strategy, key protections are architected into A10 device hardware and software.

A10 provides high-performance detection and prevention against DDoS and protocol attacks that can cripple servers and take down applications. Since the A10 Thunder and AX Series ADCs are placed between the routers and data center resources, these ADCs are ideally positioned to detect and stop attacks directed at any data center server or application. Using specialized ASICs, A10 can continue to inspect, stop, and redirect all application traffic at network speeds.

2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide explains various kinds of DoS/DDoS attack types and also A10 solutions for each DDoS type. DDoS protection is built into the A10 Thunder and AX Series ADC platforms, which are designed to handle high-volume DDoS attacks, allowing legitimate application traffic to be serviced without interruption.

In this guide, the main focus is to protect web servers and DNS servers from DDoS attacks by using some of the many DDoS protection techniques A10 offers.

3 WHAT IS DDOS?

DDoS is a type of DoS attack where multiple systems infected with a Trojan or malware are used to target a particular system, causing a denial of service. If a hacker (attacker) mounts an attack from a single host, this is classified as a DoS attack. In contrast, in a DDoS attack, many systems are used simultaneously to launch attacks against a remote system.

There are many techniques to launch DDoS attacks. As an example of a DDoS attack, an attacker begins by exploiting a vulnerability in one computer system and making that system the DDoS master (handler). It is from the master system that the intruder identifies and communicates with other systems that can be compromised (the “botnet”). The attacker loads cracking tools onto multiple compromised systems. With a single command, the hacker then instructs remote machines to launch flood attacks against a specified target, usually one or more web servers. The target system becomes busy dealing with the flood of incoming messages and/or connections sent by the botnets. This essentially forces the target system to shut down or its service to become unavailable, thereby denying service to legitimate users.

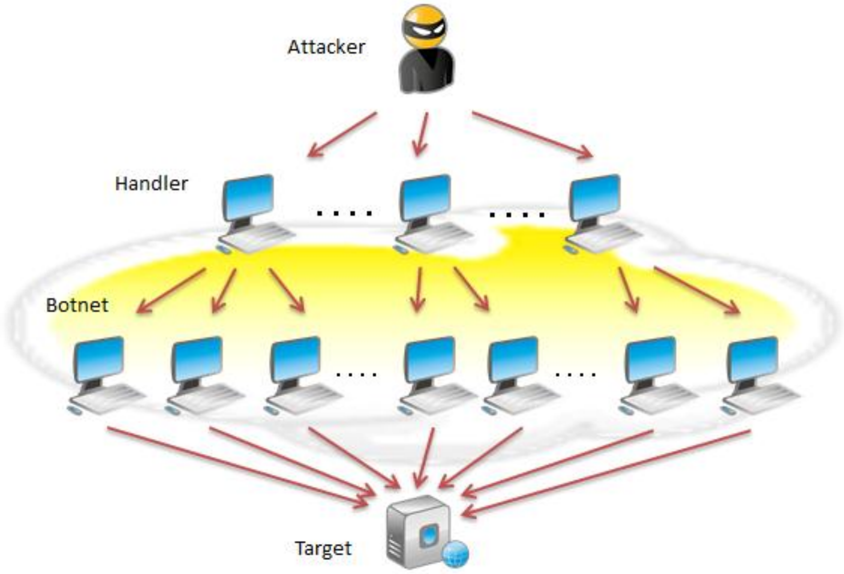


Figure 1: DDoS attack using a botnet

Today, DDoS consists of a series of attack types that can be broadly divided into the following categories:

- Resource Starvation Attacks – This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second. Examples include SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more.

- Bandwidth Consumption Attacks – The goal is to saturate the network bandwidth of the target site. Examples include ICMP floods, UDP floods and other spoofed-packet floods (Smurf and Fraggle attacks).

- Application Layer Attacks – The goal is to crash the target web server. Examples include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or OpenBSD vulnerabilities, and more. The magnitude is measured in requests per second.

- DNS DDoS Attack – This type of attack is used for either attacking the target DNS server(s) or using DNS servers to amplify the attack traffic volume going to the target. Examples include DNS flood, Spoofing-based DNS DoS attack, and DNS amplification attack. Additional, basic attacks types include DNS flood, Recursive DNS attack, Garbage DNS attack, and Reflective DNS attack.

A10 offers a range of mitigation technologies to deal with such DDoS attacks and other similar attacks, thereby ensuring service availability for legitimate users. This allows whole classes of attacks to be mitigated, not just the current attack of the day.

4 TYPES OF DDOS ATTACKS AND HOW TO MITIGATE THEM

This section describes in detail the types of DDoS attacks mitigated by A10's solutions, and how they are defeated. This deployment guide assumes that the DDoS target system (victim) is essentially a web server and DNS server.

Since there are so many kinds of DDoS attacks, they are divided into four types based on attack method and target type:

- Network Attacks - Flood Attacks
- Network Attacks - Malformed Packets Attacks
- Application / HTTP Attacks
- DNS Server Attacks

4.1 NETWORK ATTACKS—FLOOD ATTACKS

This section describes a common type of network attack, the “flood” attack.

4.1.1 SYN FLOOD ATTACK

The SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the “3-way handshake”). This is an old attack but still the favorite (about 25 percent of all DDoS attacks in 2012).

The attacker/botnet sends multiple TCP SYN requests to the target. Often, these packets are sent with randomly-generated spoofed source IP addresses. The target system responds to each SYN request by sending a SYN-ACK to establish a valid connection, and then continues to wait for acknowledgement for each of the requests, yet such confirmation never arrives. Thus, the connection table of the server fills up and as it does, all new connections are dropped and legitimate users are effectively cut off from accessing the server.

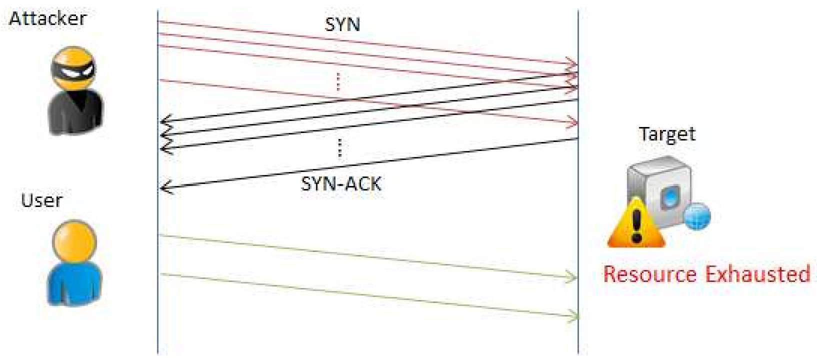


Figure 2: SYN Attack

Mitigation: SYN Cookies

A10 provides enhanced protection against TCP SYN flood attacks, with the SYN Cookie feature. The SYN cookie feature enables the A10 device to continue to serve legitimate clients during a TCP SYN flood attack, without allowing illegitimate traffic to consume system resources. The A10 device supports SYN Cookies for Layer 4-7 SLB traffic and for Layer 2/3 traffic passing through the A10 device.

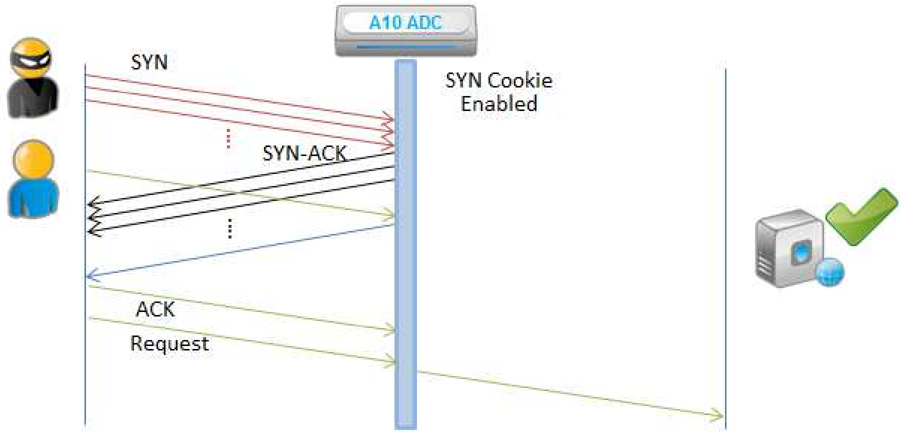


Figure 3: SYN Attack Protection - SYN Cookies

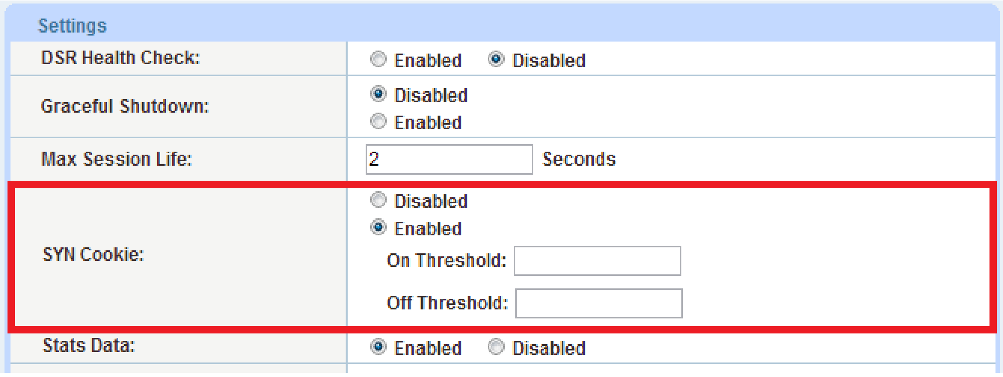
On select A10 ADC models, you can enable hardware-based SYN Cookies, which are a faster and easier-to-configure alternative to the software-based SYN Cookies available on all A10 ADC devices. Hardware-based SYN Cookie support can be configured with on/off thresholds for dynamic activation and deactivation. The benefit of this feature is that when there is no TCP SYN attack, TCP options are preserved.

The following section shows how to configure hardware-based SYN Cookies for Layer 4-7 SLB traffic.

Configuration for Hardware-based SYN Cookies for Layer 4-7 SLB traffic [GUI]

1. Navigate to **Config Mode** > **SLB** > **Service** > **Global** > **Settings**.
   Note*: Prior to ACOS 2.7.1, SYN Cookies can be configured at* ***Config Mode > Service > SLB > Global > Settings****.*

2. Select **Enabled** next to SYN Cookie. (Setting the **On Threshold** and **Off Threshold** values is optional.)



Settings

DSR Health Check:	○ Enabled ● Disabled
Graceful Shutdown:	● Disabled ○ Enabled
Max Session Life:	2 Seconds
SYN Cookie:	○ Disabled ● Enabled On Threshold: Off Threshold:
Stats Data:	● Enabled ○ Disabled

Figure 4: SYN Cookie

3. Click **OK** and then click **Save** to store your configuration changes.

Configuration [CLI]

Use the following command at the global configuration level of the Command Line Interface (CLI):

```
ACOS(config)#syn-cookie
```

The following command enables dynamic SYN cookies, to activate only when the number of concurrent half-open TCP connections exceeds 50,000 (system-wide basis). SYN cookies are then disabled again after the number falls below 30,000 (system-wide basis).

```
ACOS(config)#syn-cookie on-threshold 50000 off-threshold 30000
```

***Note**: For software-based or Layer 2/3 SYN Cookie configuration information, see the System Configuration and Administration Guide.*

4.1.2 ICMP FLOOD ATTACK

An ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers often will attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

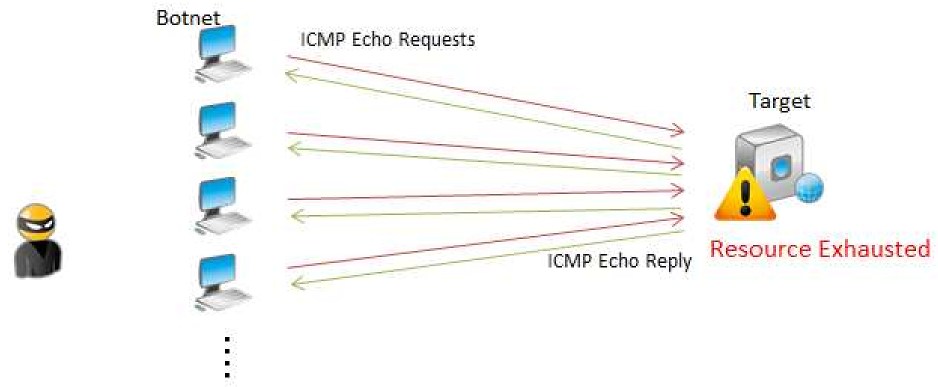


Figure 5: ICMP Flood Attack

Mitigation: ICMP Rate Limiting

A10 provides an ICMP Rate Limiting feature that monitors the rate of ICMP traffic and drops ICMP packets when the configured thresholds (the "normal rate") are exceeded.

You can configure ICMP rate limiting filters globally, on individual Ethernet interfaces, and in virtual server templates. If you configure ICMP rate limiting filters at more than one of these levels, all filters are applicable.

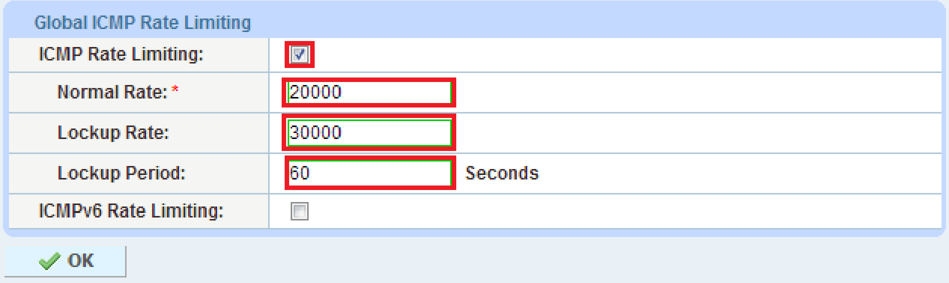
Configuration [GUI]

1. Navigate to **Config Mode > Security > Network > ICMP Rate Limiting**.
   ***Note**: Prior to ACOS 2.7.1, ICMP Rate Limiting can be configured at **Config Mode > Network > ICMP Rate Limiting**.*

2. Select the **ICMP Rate Limiting** checkbox to activate the configuration field

3. Enter **Normal Rate** (mandatory*);* 20,000 packets per second (PPS*)* in this example.

4. Enter **Lockup Rate** and **Lockup Period** (both optional*);* 30,000 PPS and 60 seconds in this example.



Global ICMP Rate Limiting

ICMP Rate Limiting:	☑
Normal Rate: *	20000
Lockup Rate:	30000
Lockup Period:	60 Seconds
ICMPv6 Rate Limiting:	□

Figure 6: ICMP Rate Limiting

5. Click **OK** and then click **Save** to store your configuration changes.

Note*: Please set appropriate thresholds (Normal Rate, Lockup Rate) based on your environment and network activity.*

Configuration [CLI]

Use the following command at the global configuration level of CLI:

```
ACOS(config)#icmp-rate-limit 20000 lockup 30000 60
```

4.1.3 UDP FLOOD ATTACK

This DDoS attack leverages the User Datagram Protocol (UDP), a sessionless networking protocol. This type of attack floods random ports on the target system with numerous UDP packets, causing the target to repeatedly check for the application listening at that port, and (when no application is found), to reply with an ICMP Destination Unreachable packet. This process can exhaust host resources, and can ultimately lead to inaccessibility.

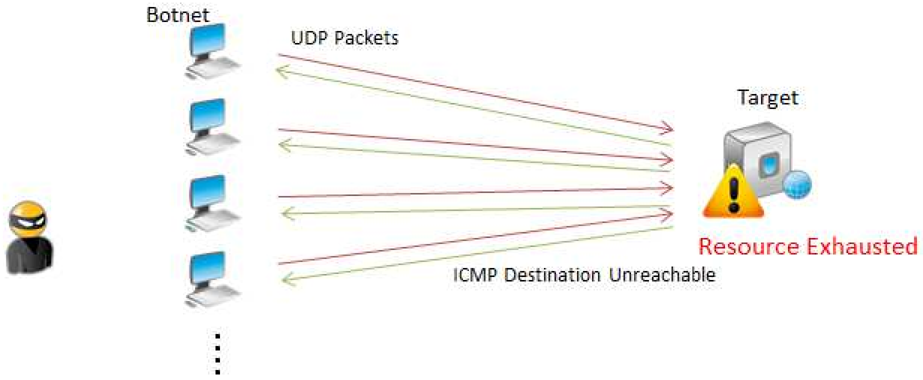


Figure 7: UDP Flood Attack

Mitigation: Source IP Based Connection-rate Limiting

A10 provides Source-IP based connection-rate limiting to mitigate UDP floods and similar attacks. Source-IP based connection-rate limiting protects the system from excessive connection requests from individual clients.

Note: *This feature applies only to SLB virtual ports.*

Note: *The current release does not support configuration or monitoring of Source-IP based connection-rate limiting using the GUI.*

Configuration [CLI]

Use the following command at the global configuration level of the CLI. In this example, the system allows up to 2,000 UDP connection requests per 100-millisecond (ms) interval. This limit applies to all virtual ports combined. If a client sends more than 2,000 requests within 100 ms, the client is locked out for 30 seconds and logged.

```
ACOS(config)#slb conn-rate-limit src-ip udp 2000 per 100 shared exceeded log
lockout 30
```

4.1.4 SMURF ATTACK

The Smurf attack is a DoS attack in which large numbers of ICMP packets with the intended victim's spoofed source IP address are sent to a broadcast IP address. This causes all hosts on the network to reply to the ICMP request, resulting in significant traffic to the victims. This is an amplification type of attack.

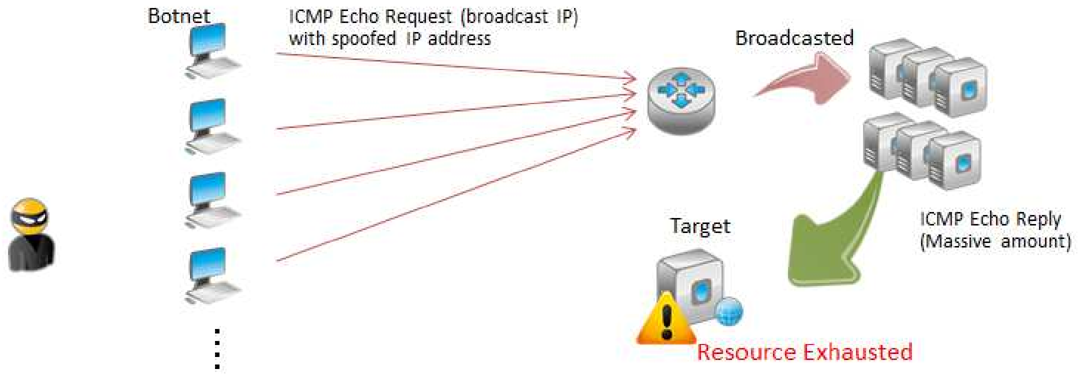

Botnet
ICMP Echo Request (broadcast IP) with spoofed IP address
Broadcasted
Target
ICMP Echo Reply (Massive amount)
Resource Exhausted

Figure 8: Smurf Attack

Mitigation: ICMP Rate Limiting

A10 ADCs do not forward (and flood) such directed broadcasts to the local network by default. This default behavior prevents a Smurf attack from occurring in case the destination IP address is behind the A10 ADC device.

If the victim is a back-end server of the A10 ADC device, ICMP rate limiting prevents Smurf attacks. For more details and configuration, please refer to the section ICMP Flood.

4.2 NETWORK ATTACKS—MALFORMED PACKETS

4.2.1 IP OPTION EXPLOIT

IP packets with certain sequences of intentionally malformed IP options can trigger an unaligned access problem in the victim's kernel, causing a DoS situation.

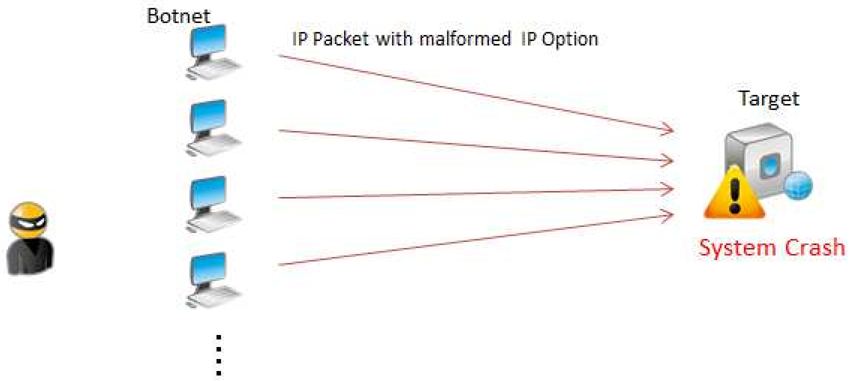


Figure 9: IP Option Exploit

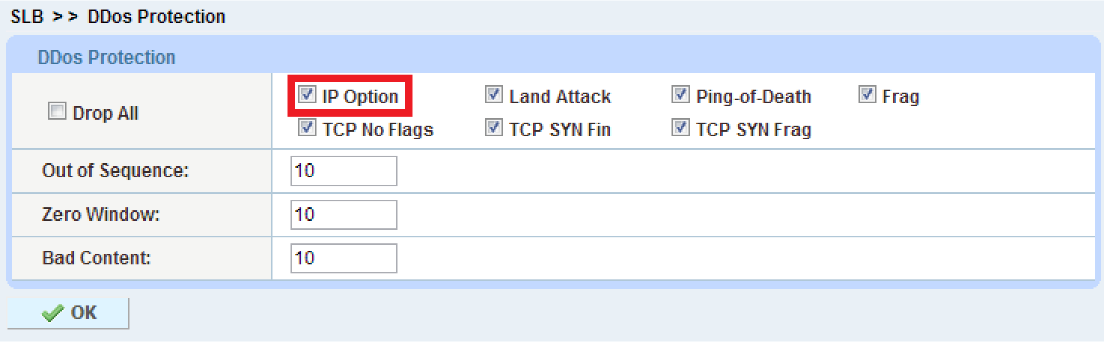
Mitigation: DDoS Protection "IP Option"

A10 provides the DDoS Protection "IP Option" filter, which drops all packets that contain any IP options.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection****.*
2. Select **IP Option**.

3. Click **OK** and then click **Save** to store your configuration changes.



SLB > > DDos Protection

DDos Protection

□ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 10: DDoS Protection - IP Option

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop ip-option
```

4.2.2 LAND ATTACK

A Land Attack consists of spoofed TCP packets with the SYN flag set, and with the same source and destination IP address/port as that of the target machine. This causes the victim to reply to itself continuously.

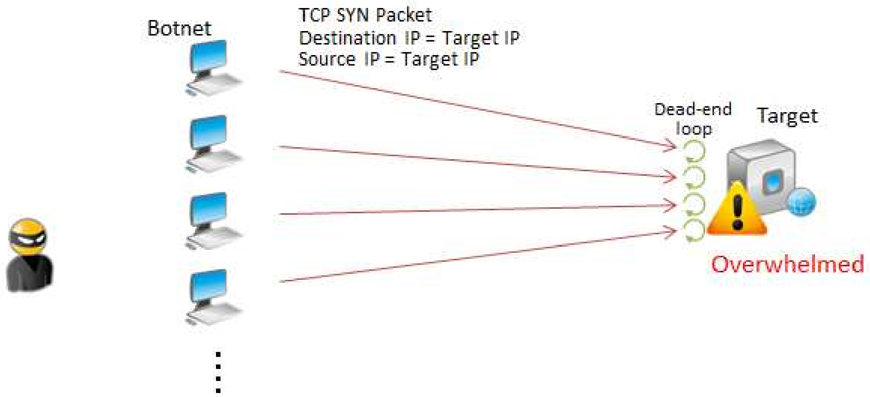


Figure 11: Land Attack

Mitigation: DDoS Protection "Land Attack"

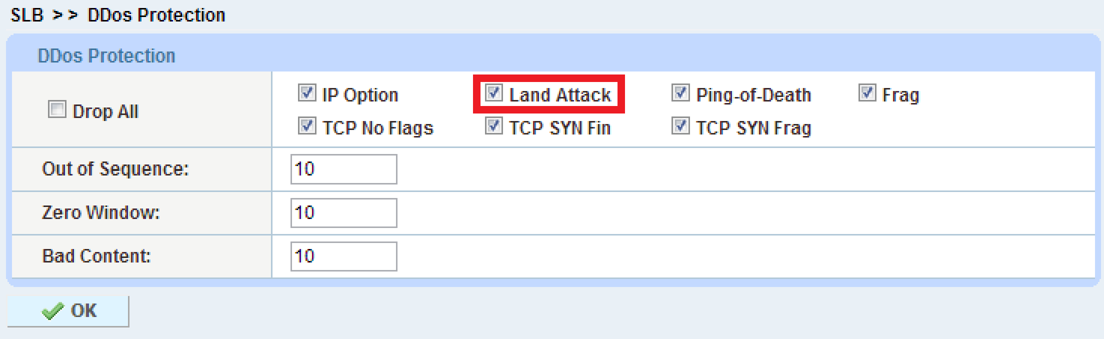
A10 provides the DDoS Protection "Land Attack" filter, which drops spoofed SYN packets containing the same IP address as the source and destination.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection****.*

2. Select **Land Attack**.

3. Click **OK** and then click **Save** to store your configuration changes.



SLB > > DDos Protection

DDos Protection

□ Drop All	☑ IP Option ☑ TCP No Flags	☑ Land Attack ☑ TCP SYN Fin	☑ Ping-of-Death ☑ TCP SYN Frag	☑ Frag
Out of Sequence:	10			
Zero Window:	10			
Bad Content:	10			

Figure 12: DDoS Protection - Land Attack

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop land-attack
```

4.2.3 PING OF DEATH

A Ping of Death attack involves the attacker sending multiple malformed pings to the target system. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size; for example, 1,500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet.

In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing DoS for legitimate packets.

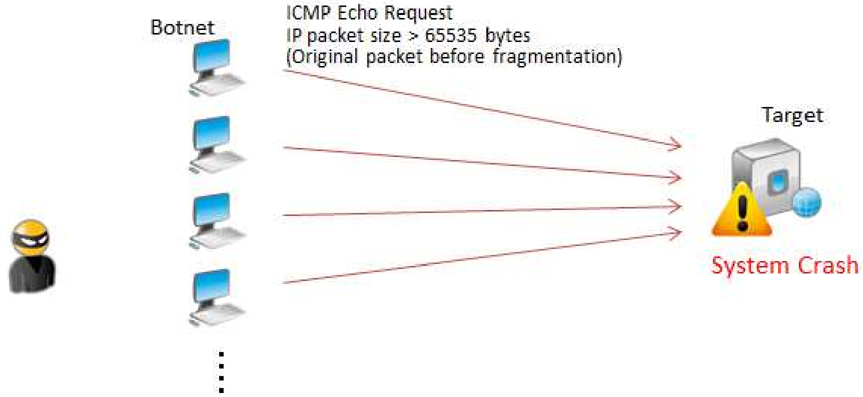

Botnet
ICMP Echo Request
IP packet size > 65535 bytes
(Original packet before fragmentation)
Target
System Crash

Figure 13: Ping of Death Attack

Mitigation: DDoS Protection "Ping-of-Death"

A10 provides the DDoS Protection "Ping-of-Death" filter, which drops all jumbo IP packets longer than the maximum valid IP packet size (65,535 bytes). These inhospitably lengthy packets are themselves the “ping of death” packets.

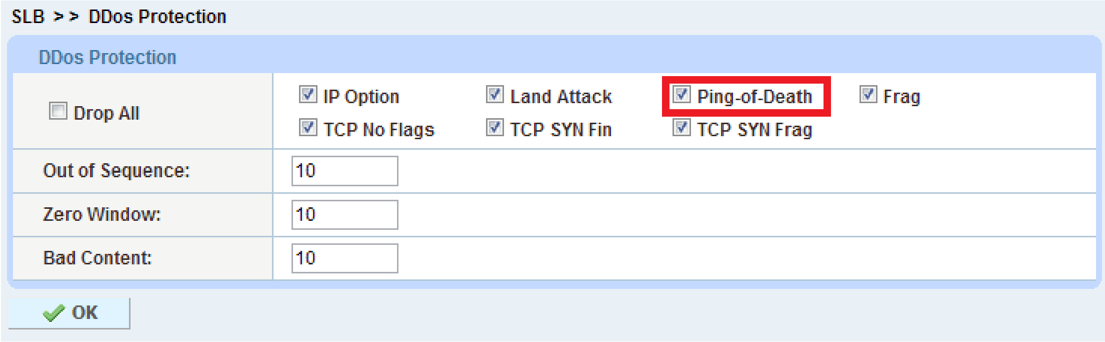
Note*: On FTA / FPGA models, the Ping-of-Death option drops IP packets longer than 65,535 bytes. On other models, the option drops all IP packets longer than 32,000 bytes.*

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection****.*

2. Select **Ping-of-Death**.

3. Click **OK** and then click **Save** to store your configuration changes.



SLB > > DDos Protection

DDos Protection

☐ Drop All

☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag

☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag

Out of Sequence: 10

Zero Window: 10

Bad Content: 10

Figure 14: DDoS Protection - Ping-of-Death

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop ping-of-death
```

4.2.4 IP FRAGMENTATION ATTACK

IP fragmentation exploits the IP fragmentation process by breaking up a single IP datagram into two or more IP datagrams of smaller size for attack activity (DDoS). There are many kinds of IP fragmentation exploits such as IP fragment overlap, IP fragmentation buffer full, IP fragment overrun, IP fragment overwrite, IP fragment too many datagrams, IP fragment incomplete datagram, and IP fragment too small.

IP fragment overlap is the basis for the Teardrop DoS attack.

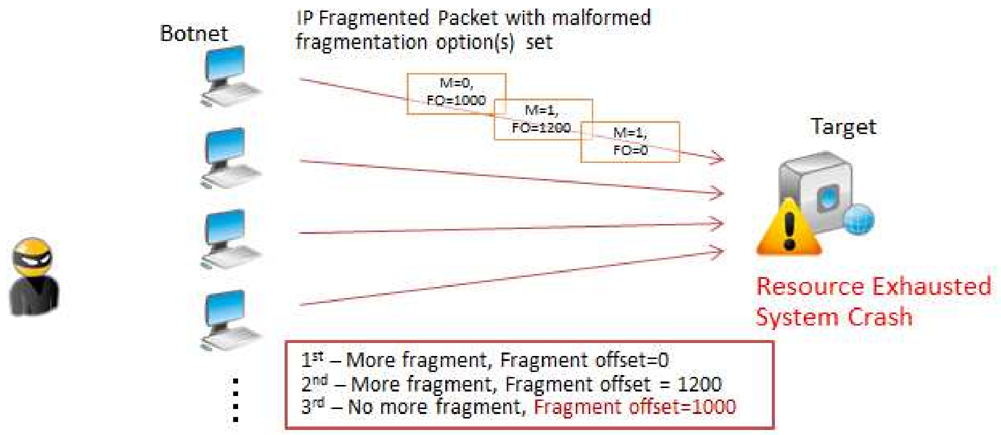

Botnet
IP Fragmented Packet with malformed fragmentation option(s) set
M=0, FO=1000
M=1, FO=1200
M=1, FO=0
Target
Resource Exhausted
System Crash
1st – More fragment, Fragment offset=0
2nd – More fragment, Fragment offset = 1200
3rd – No more fragment, Fragment offset=1000

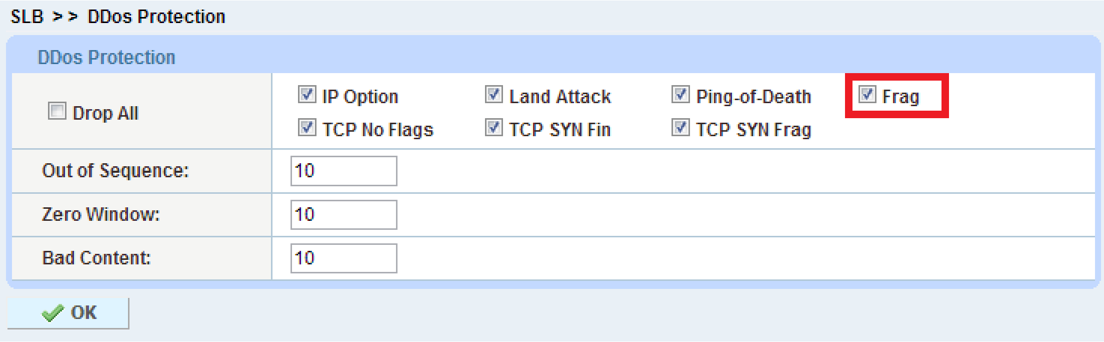
Figure 15: IP Fragmentation Attack

Mitigation: DDoS Protection "Frag"

A10 provides the DDoS Protection "Frag" filter, to drop all IP fragments, which can be used to attack hosts running IP stacks that have known vulnerabilities in their fragment reassembly code.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note: *Prior to ACOS 2.7.1, DDoS Protection is located on **Config Mode > Service > SLB > Global > DDoS Protection**.*
2. Select **Frag**.
3. Click **OK** and then click **Save** to store your configuration changes.



SLB > > DDos Protection

DDos Protection

☐ Drop All	☑ IP Option ☑ TCP No Flags	☑ Land Attack ☑ TCP SYN Fin	☑ Ping-of-Death ☑ TCP SYN Frag	☑ Frag
Out of Sequence:	10			
Zero Window:	10			
Bad Content:	10			

Figure 16: DDoS Protection – Frag

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop frag
```

4.2.5 TCP NO FLAG EXPLOIT

The TCP No-flag exploit consists of pure data packets with no TCP flags set (TCP Null). An attacker uses a TCP NULL scan to determine whether ports are open or closed on the target machine.

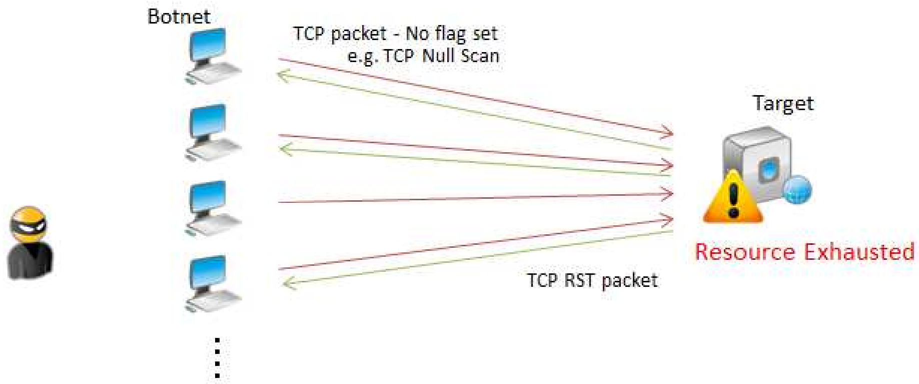


Figure 17: TCP No Flag Attack

Mitigation: DDoS Protection "TCP No Frag"

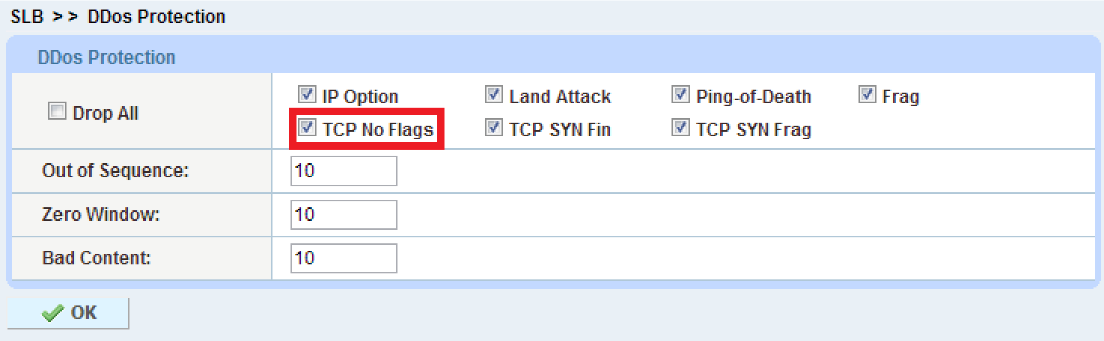
A10 provides the DDoS Protection "TCP No Flags" filter, which drops all TCP packets that do not have any TCP flags set.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection***.

2. Select **TCP No Flags**.

3. Click **OK** and then click **Save** to store your configuration changes.


SLB > > DDos Protection

DDos Protection

☐ Drop All

☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag

☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag

Out of Sequence: 10

Zero Window: 10

Bad Content: 10

Figure 18: DDoS Protection - TCP No Flags

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop tcp-no-flag
```

4.2.6 TCP SYN+FIN EXPLOIT

In his type of attack, the attacker sends a TCP segment with both the SYN and the FIN bits set. This tricks the target machine into almost simultaneously entering both SYN_RCVD and CLOSE_WAIT states. The target machine then is stuck in CLOSE_WAIT state until expiration of the keepalive timer.

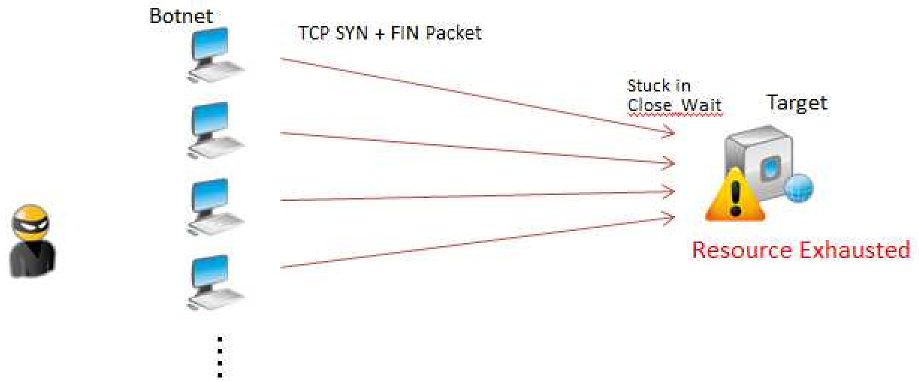


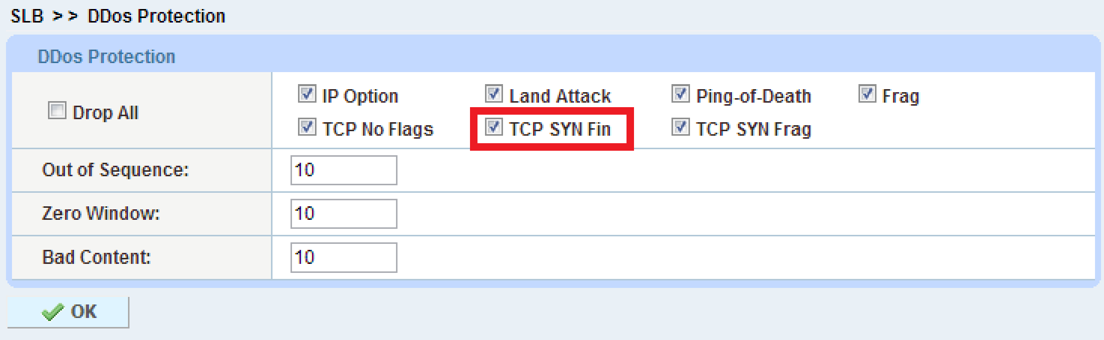
Figure 19: TCP SYN+Fin Attack

Mitigation: DDoS Protection "TCP SYN Fin"

A10 provides DDoS Protection "TCP SYN Fin" filter, to drop all TCP packets in which both the SYN and FIN flags are set.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection***.
2. Select **TCP SYN Fin**.
3. Click **OK** and then click **Save** to store your configuration changes.


SLB >> DDos Protection

DDos Protection

□ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 20: DDoS Protection - TCP SYN Fin

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop tcp-syn-fin
```

4.2.7 TCP SYN FRAGMENT ATTACK

The TCP SYN fragment attack attempts to exhaust a system’s limited resources by sending bogus TCP segments (SYN packet fragments). The target system catches the fragments, waiting for the remaining packets to arrive for reassembly. The SYN queue is filled to maximum capacity and will stall in a SYN-RECEIVED state, preventing legitimate connections.

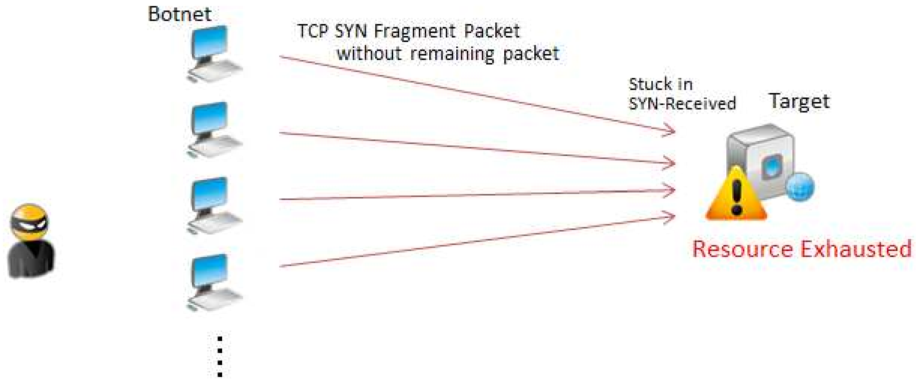


Figure 21: TCP SYN Fragment Attack

Mitigation: DDoS Protection "TCP SYN Frag"

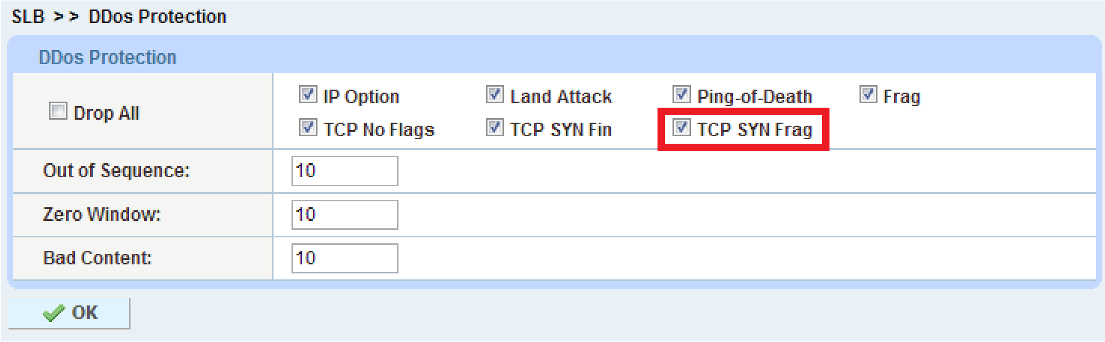
A10 provides the DDoS Protection "TCP SYN Frag" filter, to drop incomplete (fragmented) TCP SYN packets, which can be used to launch TCP SYN flood attacks.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note: *Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection***.

2. Select **TCP SYN Frag**.

3. Click **OK** and then click **Save** to store your configuration changes.



SLB >> DDos Protection

DDos Protection

□ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 22: DDoS Protection - TCP SYN Frag

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop tcp-syn-frag
```

4.2.8 OUT OF SEQUENCE ATTACK

TCP provides a connection-oriented, reliable, sequence-preserving data stream service, to guarantee that the application receives data in the correct order. When a TCP stream (consisting of TCP segments) are received out of sequence, they are buffered by the destination system until they can be re-ordered and re-assembled.

An attacker may conduct a low-bandwidth DoS attack against a target machine providing services based on TCP (such as HTTP, SMTP, or FTP). By sending many out of sequence TCP segments, the attacker can cause the target machine to consume all available memory buffers, likely leading to a system crash.

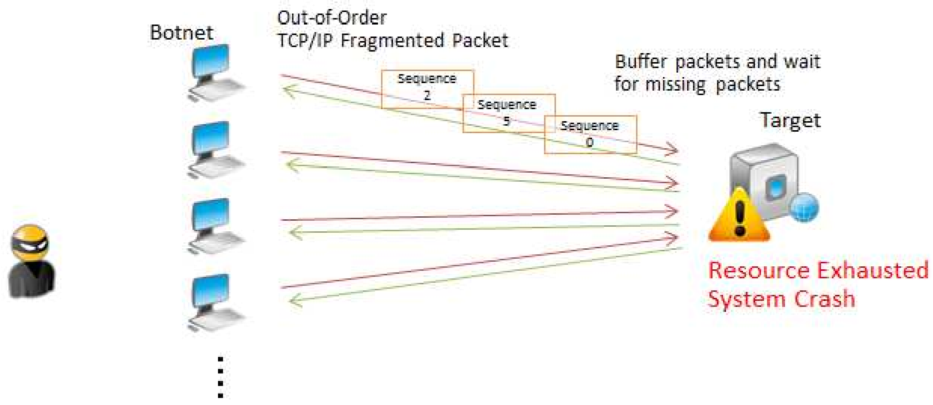


Figure 23: Out of Sequence Attack

Mitigation: IP Anomaly Filter "Out of Sequence" with System-wide PBSLB

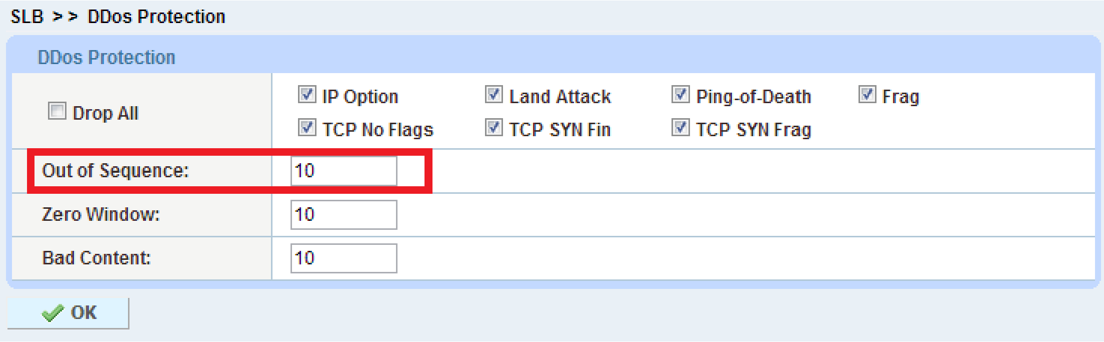
A10 provides the DDoS Protection "Out of Sequence" feature. This feature works along with system-wide Policy-Based SLB, and checks for out-of-sequence packets in new HTTP or HTTPS connection requests from clients.

Note: *This feature is valid only when the proxy type on the virtual server/port is configured as HTTP, HTTPS or SSL-Proxy but not TCP.*

Configuration for Out of Sequence filtering [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection****.*

2. Enter the threshold (in this example, 10) in the **Out of Sequence** field.



SLB > > DDos Protection

DDos Protection

☐ Drop All

☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag

☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag

Out of Sequence: 10

Zero Window: 10

Bad Content: 10

Figure 24: DDoS Protection - Out of Sequence

3. Click **OK** and then click **Save** to store your configuration changes.

Configuration for Out of Sequence filtering [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop out-of-sequence 10
```

(This example shows 10. The range is 1-127.)

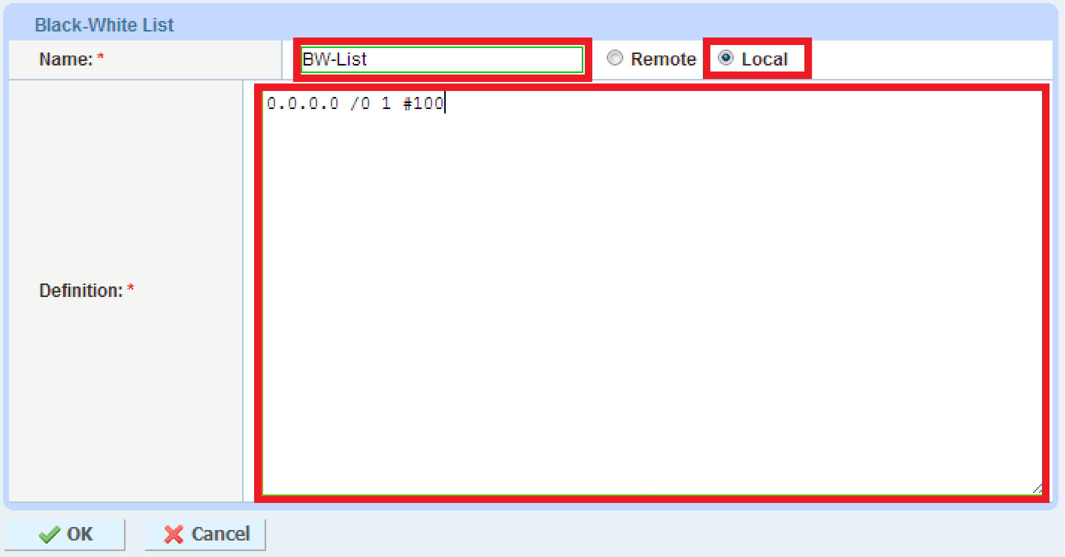
Configuration for System-Wide PBSLB [GUI / CLI]

Policy-based SLB provides additional DDoS protection options. A Black/White List is used as part of configuration. The Black/White List identifies clients and specifies traffic limits for them. You can import the list from a TFTP server (GUI & CLI) or configure it locally (GUI only). After importing or configuring the Back/White List, the CLI is required to complete the configuration.

1. Navigate to **Config Mode** > **SLB** > **Black-White List**.
   Note: *Prior to ACOS 2.7.1, PBSLB is located on* ***Config Mode > Service > PBSLB***.

2. Click **Add**.

3. Enter the **Black-White List** name (in this example, “BW-List”) and import the list from a TFTP server (GUI & CLI) or configure it locally (GUI only). In this example, the list is configured locally in the text entry field and uses a dynamic entry (0.0.0.0/0) with a limit of 100 concurrent sessions for each client.



Name: BW-List

```
0.0.0.0 /0 1 #100
```

Figure 25: PBSLB Black/White List

4. Click **OK**.

5. Continue to the next section. The CLI is required to complete this configuration.

[CLI] Black/White Lists also are configurable in the CLI by importing the file:

1. Import the Black/White List, if not already on the system.

   - Use a command such as the one in this example to download the file periodically:

     ```
     ACOS(config)#bw-list BW-List tftp://10.100.2.240/BW-List.txt
     ```

   - Use a command such as this one instead, if you want to import the file one time:

     ```
     ACOS(config)#import bw-list BW-List3 tftp://10.100.2.224/BW-List.txt
     ```

2. To apply the Black/White List and apply to system-wide PBSLB, use the following commands at the global configuration level of the CLI:

   ```
   ACOS(config)#system pbslb bw-list BW-List
   ACOS(config)#system pbslb over-limit lockup 5 logging 10
   ```

In the CLI example above, the Black/White List is applied to system-wide PBSLB with a lockup time of 5 minutes and logging interval of 10 minutes.

***Note**: The sample BW-List contains group ID 1; however, you don't need to configure the group ID in a PBSLB configuration since a wildcard address is used in the list. To use a specific host or subnet address in the list, please configure the action (reset or drop) for each group ID accordingly.*

4.2.9 TCP ZERO WINDOW ATTACK

The Zero Window attack exploits TCP vulnerabilities, specifically those related to window scaling.

The way the attack works is that an attacker creates a connection with a target system, then sets the window size to zero (or a very small value). This causes the target system to send zero-window probes but no data. By creating large numbers of such connections, the attacker can consume the target system resource (TCP memory pool) and prevent legitimate new connections from opening.

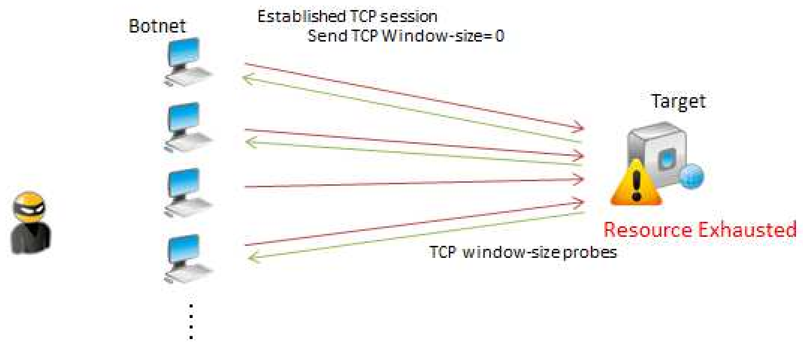


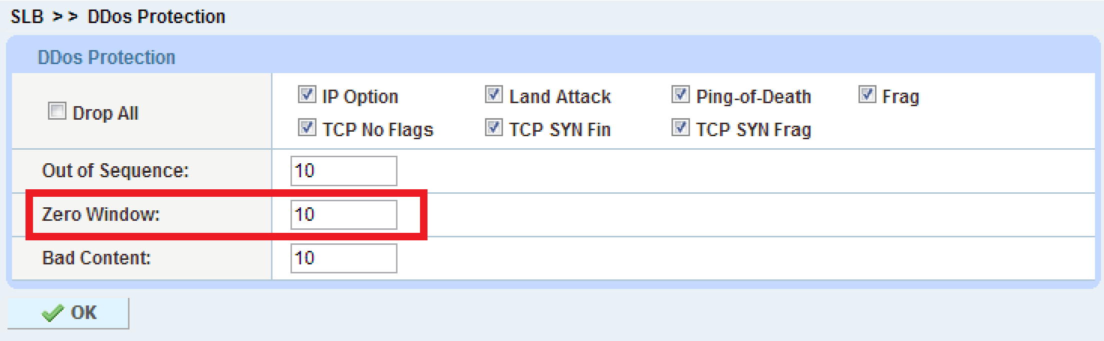
Figure 26: TCP Zero Window Attack

Mitigation: IP Anomaly Filter "Zero Window" and system-wide PBSLB
A10 provides the DDoS Protection "Zero Window" filter, which works along with system-wide PBSLB. This filter checks for a zero-length TCP window in new HTTP or HTTPS connection requests from clients.

Configuration [GUI]

1. Navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.
   ***Note**: Prior to ACOS 2.7.1, DDoS Protection is located on **Config Mode > Service > SLB > Global > DDoS Protection**.*

2. Enter the **Threshold** (in this example,10) in the **Zero Window** field and click **OK**.



SLB >> DDos Protection

DDos Protection

☐ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 27: DDoS Protection - Zero Window

3. Click **OK** then click **Save** to store your configuration changes.

4. For system-wide PBSLB configuration, see Out of Sequence Attack.

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop zero-window 10
```

(This example shows 10. The range is 1-127.)

4.2.10 TEARDROP ATTACK

The Teardrop attack exploits an overlapping IP fragment bug in some common operating systems. Fragmented packets are sent in a jumbled and confused order to the target system. When the receiving system attempts to reassemble them, it does not know how to handle the request and ultimately crashes.

Mitigation: DDoS Protection "Frag"

A10 device provides the DDoS Protection "Frag" filter to mitigate this kind of attack. Please see IP Fragmentation Attack.

4.3 APPLICATION / HTTP ATTACKS

4.3.1 INVALID PAYLOAD PACKETS (HTTP/SSL)

Some DDoS methods/tools such as Sockstress attack the target system by sending invalid payloads (bad content) after successfully establishing a connection. By sending massive amounts of such packets, the attacker consumes the target's system resources, resulting in an unavailable system for legitimate users.

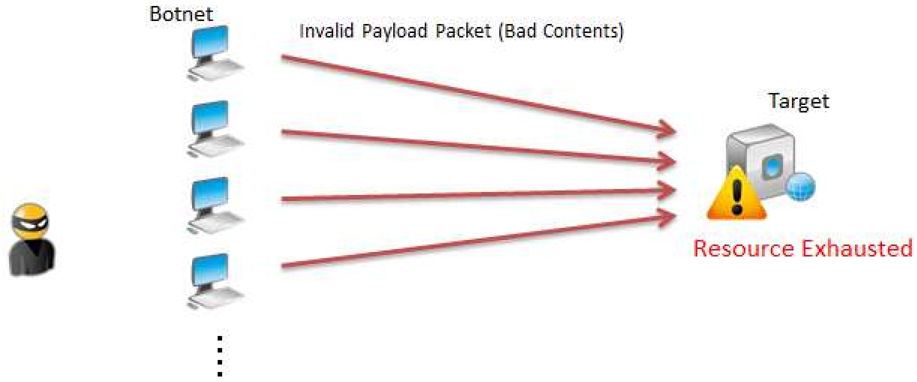


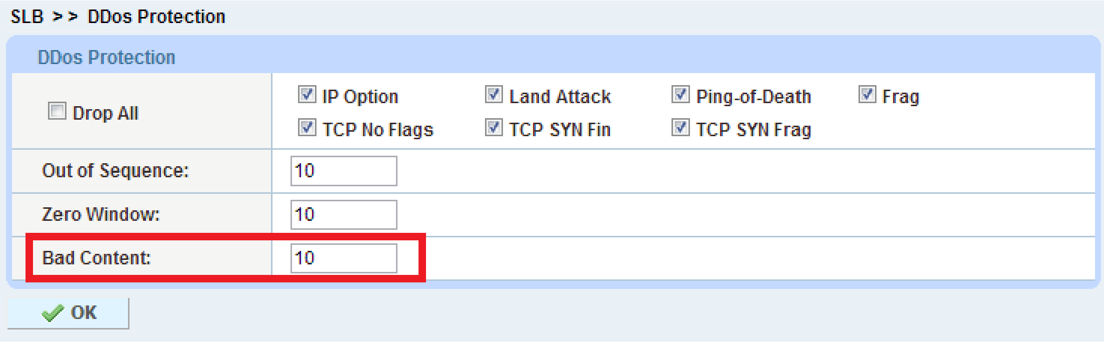
Figure 28: Invalid Payload Packet (Bad Contents)

Mitigation: IP Anomaly Filter "Bad Content" with system-wide PBSLB
A10 provides the DDoS Protection "Bad Content" filter, which works along with system-wide PBSLB to check for invalid HTTP or SSL payloads in new HTTP or HTTPS connection requests from clients.

Configuration [GUI]

1. Navigate to **Config Mode > Security > Network > DDoS Protection**.
   Note*: Prior to ACOS 2.7.1, DDoS Protection is located on* ***Config Mode > Service > SLB > Global > DDoS Protection****.*

2. Enter threshold (in this sample, 10) in the **Bad Content** and click **OK**.



SLB >> DDos Protection

DDos Protection

□ Drop All	☑ IP Option ☑ Land Attack ☑ Ping-of-Death ☑ Frag ☑ TCP No Flags ☑ TCP SYN Fin ☑ TCP SYN Frag
Out of Sequence:	10
Zero Window:	10
Bad Content:	10

Figure 29: DDoS Protection - Bad Content

3. For system-wide PBSLB configuration, see Out of Sequence Attack.

Configuration [CLI]

Use the following command at the global configuration level of the CLI:

```
ACOS(config)#ip anomaly-drop bad-content 10
```

This example shows 10. The range is 1-127.

4.3.2 HTTP GET FLOOD

An HTTP GET Flood is a Layer 7 application layer DDoS attack method in which attackers send a huge flood of HTTP GET packets, requesting large amounts of data/objects from the target server. Since the 3-way TCP handshake has been completed, those requests look like a legitimate connection. However, due to the amount of requests coming from botnets, the target system is overwhelmed. As a result, the server cannot respond to legitimate requests from users.

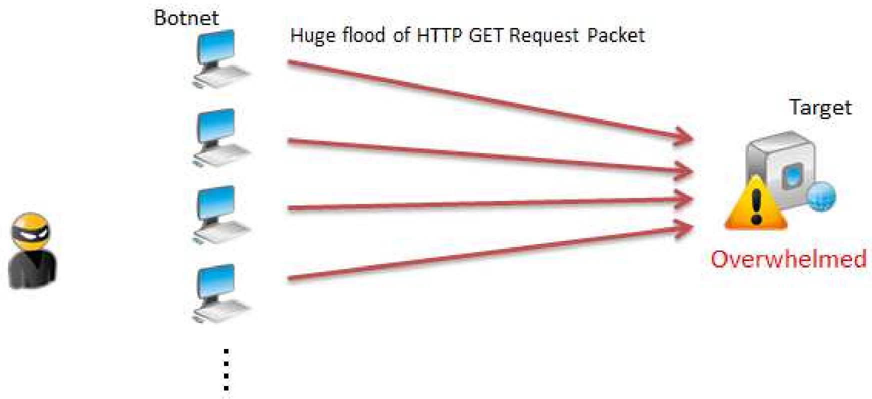


Figure 30: HTTP GET Flood Attack

Mitigation: IP Limiting (Policy Template)

A10 provides the IP Limiting feature to rate limit Layer 7 requests based on concurrent requests and request rate. The feature also supports Layer 4 connection-rate limiting options and can be combined with Layer 7 request-rate limiting.

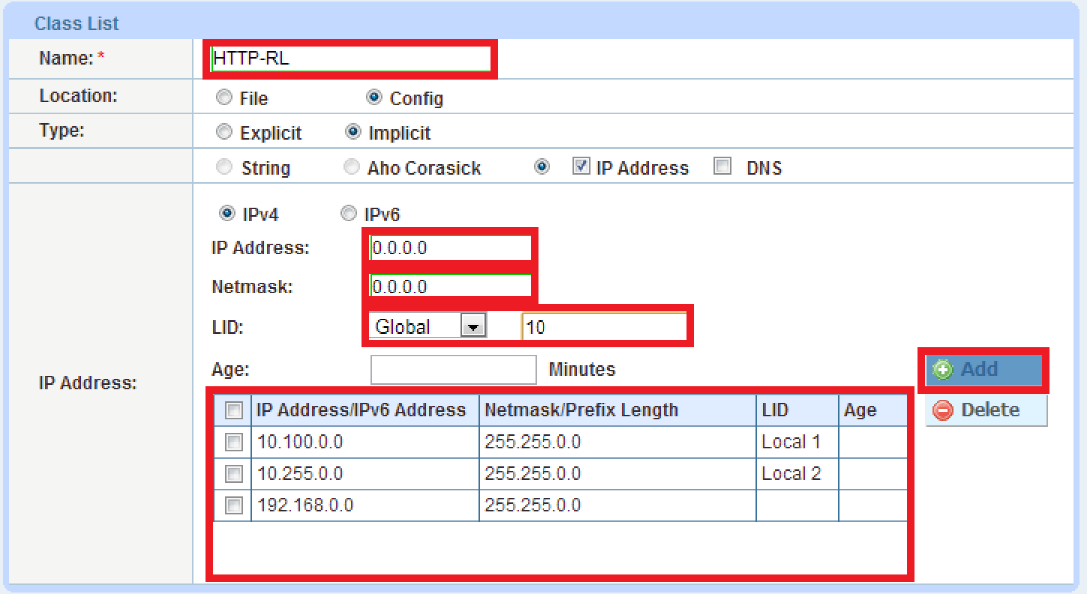
Configuration [GUI]

1. Navigate to **Config Mode** > **SLB** > **Service** > **Class List**.
   Note: Prior to ACOS 2.7.1, PBSLB is located on ***Config Mode > Service > SLB > Class List***.

2. Click **Add**.

3. Enter a **Name** (in this example, “HTTP-RL”) and enter the IP addresses along with the Limit ID (LID). In this example, the class list is as follows:

```
10.100.0.0 /16 local id 1 ; LID 1 applies to any client in this subnet
10.255.0.0 /16 local id 2 ; LID 2 applies to any client in this subnet
192.168.0.0 /16 ; No LID is applied to client in this subnet (Exception List)
0.0.0.0 /0 global id 10 ; GLID 10 is applied to all other client
```



Class List

Name: *	HTTP-RL
Location:	○ File ● Config
Type:	○ Explicit ● Implicit
	○ String ○ Aho Corasick ● ☑ IP Address □ DNS
IP Address:	● IPv4 ○ IPv6 IP Address: 0.0.0.0 Netmask: 0.0.0.0 LID: Global 10 Age: Minutes

□	IP Address/IPv6 Address	Netmask/Prefix Length	LID	Age
□	10.100.0.0	255.255.0.0	Local 1	
□	10.255.0.0	255.255.0.0	Local 2	
□	192.168.0.0	255.255.0.0		

Figure 31: Class List

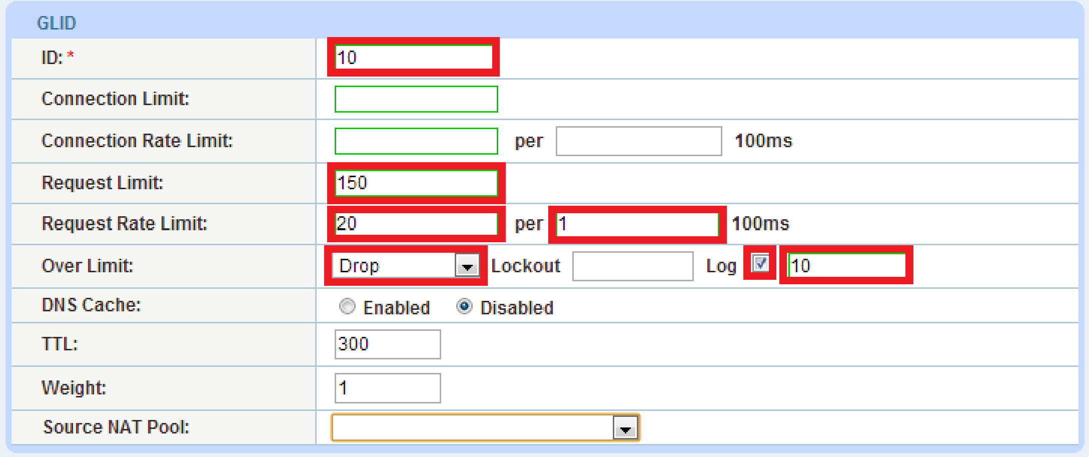
4. Click **OK**.

5. To configure Global ID (e.g. 10), Navigate to **Config Mode** > **SLB** > **Service** > **GLID**.
   Note: *Prior to ACOS 2.7.1, PBSLB is located on* ***Config Mode > Service > SLB > GLID***.

6. Click **Add**.

7. Enter **ID** (for example, 10) and enter the rate limiting settings. In this example, GLID 10 is configured as follows:

   - GLID 10 is for all other clients (including public IP addresses).
   - Layer 7 Request Rate is 150 sessions.
   - Layer 7 Request Rate Limit is 20 per 100 ms.
   - Over Limit Action is Drop and logging is enabled with a 10-minute interval.



GLID

ID: *	10
Connection Limit:	
Connection Rate Limit:	per 100ms
Request Limit:	150
Request Rate Limit:	20 per 1 100ms
Over Limit:	Drop Lockout Log ☑ 10
DNS Cache:	○ Enabled ● Disabled
TTL:	300
Weight:	1
Source NAT Pool:	

Figure 32: GLID

8. Click **OK**.

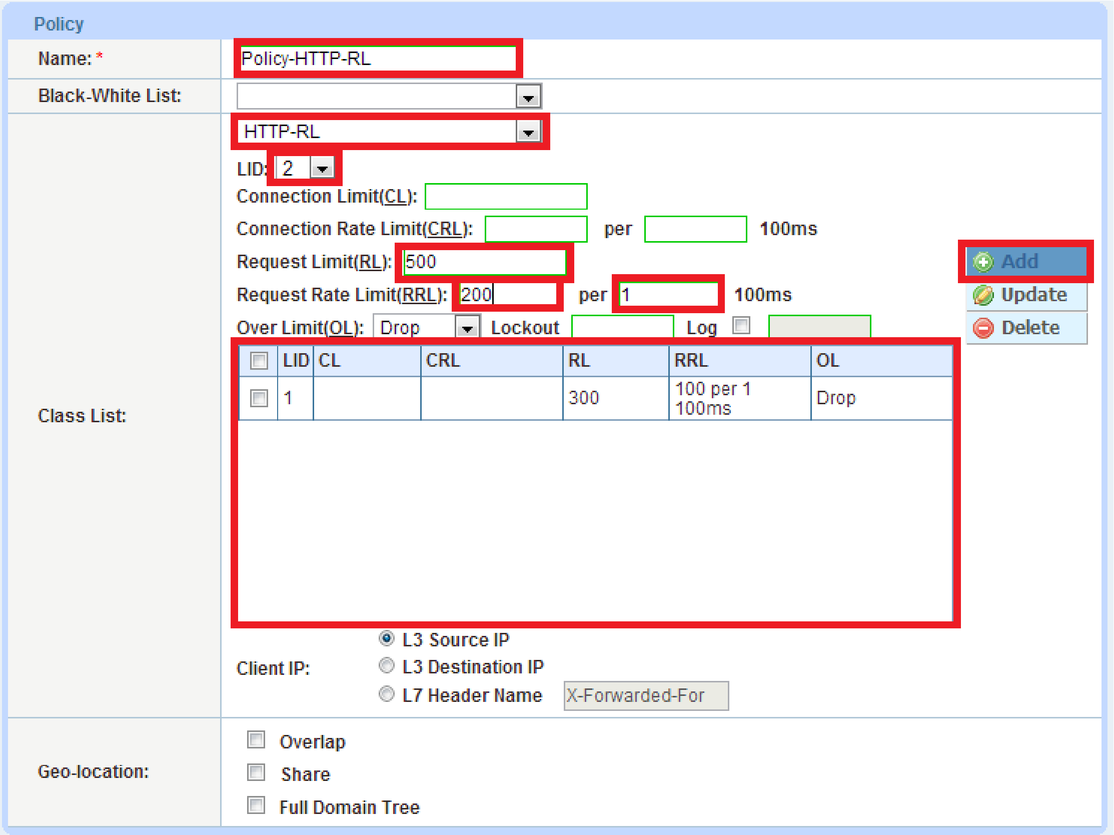
9. To configure a Policy template, navigate to **Config Mode** > **Security** > **Template** > **Policy**. ***Note****: Prior to ACOS 2.7.1, PBSLB is located on* ***Config Mode > Service > Template > Application > Policy****.*

10. Click **Add**.

11. Enter a **Name** (in this example, “Policy-HTTP-RL”) and select the class list from the drop-down menu. (The class list in this example is “HTTP-RL”.)

12. Configure each LID with an action according to the class list specified. In this example, class list “HTTP-RL” has 2 LIDs configured:

    - LID 1 for 10.100.0.0/16 (Regular HTTP user)
        - Request Limit: 300
        - Request Rate Limit: 100 per 100 ms
    - LID 2 for 10.255.0.0/16 (heavy HTTP user)
        - Request Limit : 500
        - Request Rate Limit: 200 per 100 ms



Policy

Name: * Policy-HTTP-RL

Black-White List:

Class List: HTTP-RL

LID: 2

Connection Limit(CL):

Connection Rate Limit(CRL): per 100ms

Request Limit(RL): 500

Request Rate Limit(RRL): 200 per 1 100ms

Over Limit(OL): Drop Lockout Log ☐

☐	LID	CL	CRL	RL	RRL	OL
☐	1			300	100 per 1 100ms	Drop

Client IP: ● L3 Source IP ○ L3 Destination IP ○ L7 Header Name X-Forwarded-For

Geo-location: ☐ Overlap ☐ Share ☐ Full Domain Tree

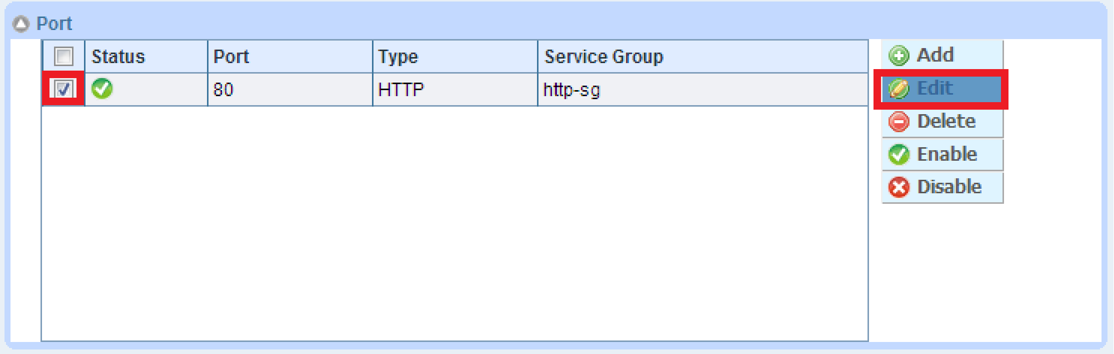
Figure 33: Policy Template

13. Click **OK**.

14. To Apply the Policy Template to Virtual Server (or Virtual Port), Navigate to **Config Mode** > **SLB** > **Service** > **Virtual Server**.
Note: *Prior to ACOS 2.7.1, PBSLB is located on **Config Mode** > **Service** > **SLB** > **Virtual Server**.*

15. Select and Edit a **Virtual Server** where you want to apply the Layer 7 rate limit.
Note: *If you didn't configure a virtual server yet, please do so by clicking **Add**.*

16. In the **Port** section, select the virtual server port where you want to apply the Layer 7 rate-limiting Policy template (for example, "Policy-HTTP-RL"). Click **Edit**.
Note: *The Layer 7 rate-limiting Policy template can be applied onto the virtual server itself by choosing the policy in the **Policy Template** column. In this example, the Policy template is applied to the virtual server port.*

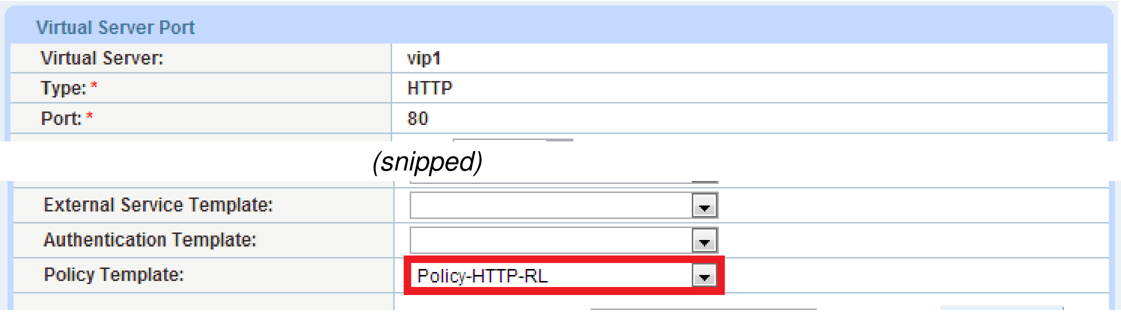


Port

□	Status	Port	Type	Service Group
☑	✓	80	HTTP	http-sg

Figure 34: Editing Virtual Server Port under Virtual Server

17. On the Virtual Server Port page, select the Policy template from the **Policy Template** drop-down list.



Virtual Server Port

Virtual Server:	vip1
Type: *	HTTP
Port: *	80

(snipped)

External Service Template:	
Authentication Template:	
Policy Template:	Policy-HTTP-RL

Figure 35: Editing Virtual Server Port under Virtual Server

18. Click **OK** then **Save** to store your configuration changes.

Configuration [CLI]

Following is the CLI equivalent of the configuration shown in the GUI above example:

```
ACOS(config)#class-list HTTP-RL
ACOS(config-class list)#10.100.0.0 /16 lid 1
ACOS(config-class list)#10.255.0.0 /16 lid 2
ACOS(config-class list)#0.0.0.0 /0 glid 10
ACOS(config-class list)#192.168.0.0 /16
ACOS(config-class list)#exit

ACOS(config)#glid 10
ACOS(config-global lid)#request-limit 150
ACOS(config-global lid)#request-rate-limit 20 per 1
ACOS(config-global lid)#over-limit-action log 10
ACOS(config-class list)#exit

ACOS(config)#slb template policy Policy-HTTP-RL
ACOS(config-policy)#class-list name HTTP-RL
ACOS(config-policy)#class-list lid 1
ACOS(config-policy-policy lid)#request-limit 300
ACOS(config-policy-policy lid)#request-rate-limit 100 per 1
ACOS(config-policy-policy lid)#exit
ACOS(config-policy)#class-list lid 2
ACOS(config-policy-policy lid)#request-limit 500
ACOS(config-policy-policy lid)#request-rate-limit 200 per 1
ACOS(config-policy-policy lid)#exit
ACOS(config-policy-policy)#exit

ACOS(config)#slb virtual-server vip1
ACOS(config-slb vserver)#port 80 http
ACOS(config-slb vserver-vport)#template policy Policy-HTTP-RL
```

4.3.3 HTTP POST FLOOD

An HTTP POST flood is a type of DDoS attack in which the volume of POST requests overwhelms the target server so that the server cannot respond to them all. This can result in exceptionally high utilization of system resources and consequently crash the server.

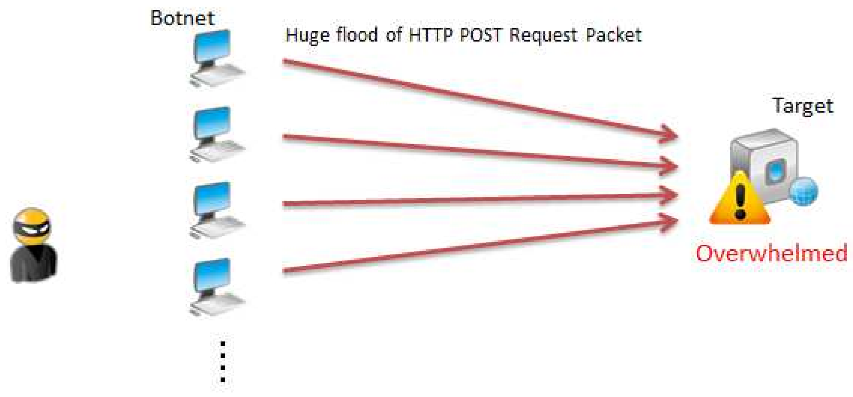


Figure 36: HTTP POST Flood Attack

Mitigation: IP Limiting (Policy Template)

IP Limiting also can be applied to mitigate HTTP POST Flood attacks. Please refer to the section HTTP GET Flood.

4.3.4 SLOWLORIS

Slowloris is especially dangerous to hosts running HTTP services (for example: Apache, dhttpd, Tomcat and GoAhead). It is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network.

Slowloris operates by holding as many connections to the target web server open as possible, for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request at a very slow rate. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

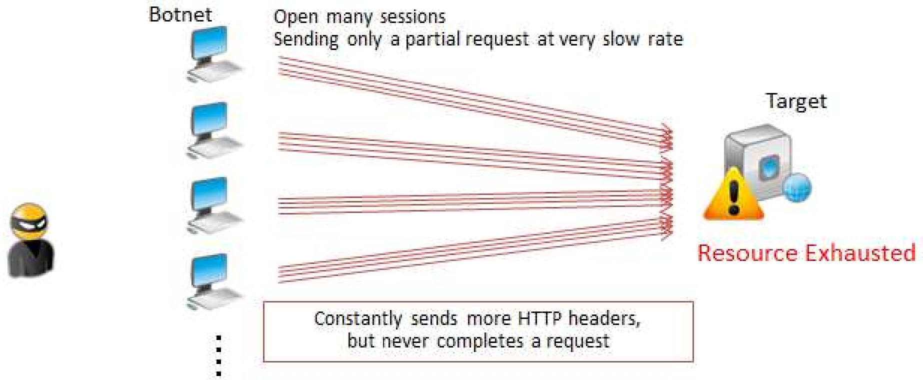

Botnet
Open many sessions
Sending only a partial request at very slow rate
Target
Resource Exhausted
Constantly sends more HTTP headers, but never completes a request

Figure 37: Slowloris Attack

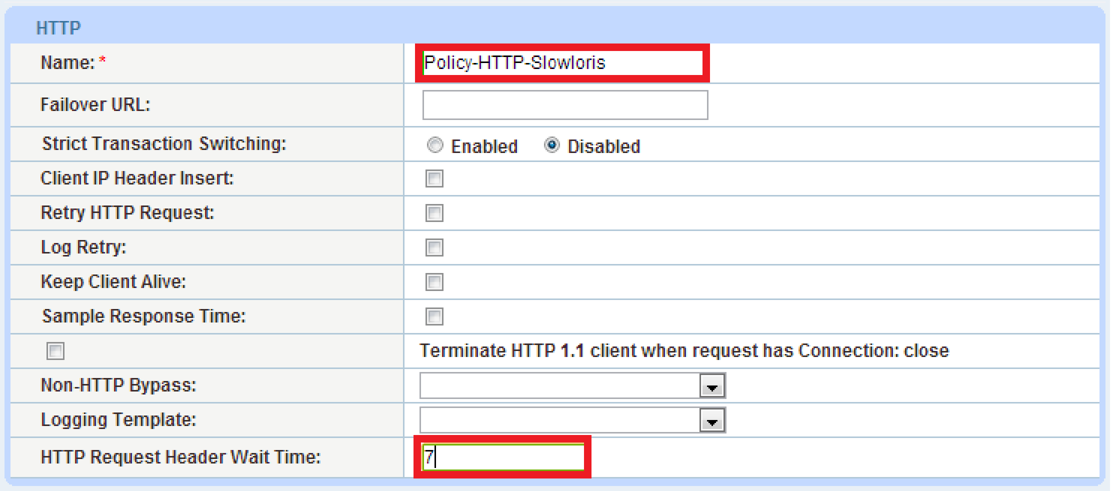
Mitigation: HTTP Template with "HTTP Request Header Time Out"

A10 provides the HTTP Request Header Time Out option in HTTP templates. This option enables an A10 ADC device to detect this type of slow-rate HTTP attack. Also, in ACOS 2.7.1-P1 and above, enhanced SLB DDoS protection command are available (currently CLI only).

Note*: The HTTP Request Header Time Out option is available in ACOS 2.7.0-P2 (CLI only) and ACOS 2.7.1-P1 and above (CLI and GUI).*

Configuration [GUI]

1. Navigate to **Config Mode** > **SLB** > **Template** > **Application** > **HTTP**.
2. Click **Add**.
3. Enter **Name** and **HTTP Request Header Wait Time** (sec). In this example, the name is “Policy-HTTP-Slowloris”. The HTTP Request Header Wait Time is 7 (default value if enabled).



HTTP

Name: *	Policy-HTTP-Slowloris
Failover URL:	
Strict Transaction Switching:	○ Enabled ● Disabled
Client IP Header Insert:	□
Retry HTTP Request:	□
Log Retry:	□
Keep Client Alive:	□
Sample Response Time:	□
□	Terminate HTTP 1.1 client when request has Connection: close
Non-HTTP Bypass:	
Logging Template:	
HTTP Request Header Wait Time:	7

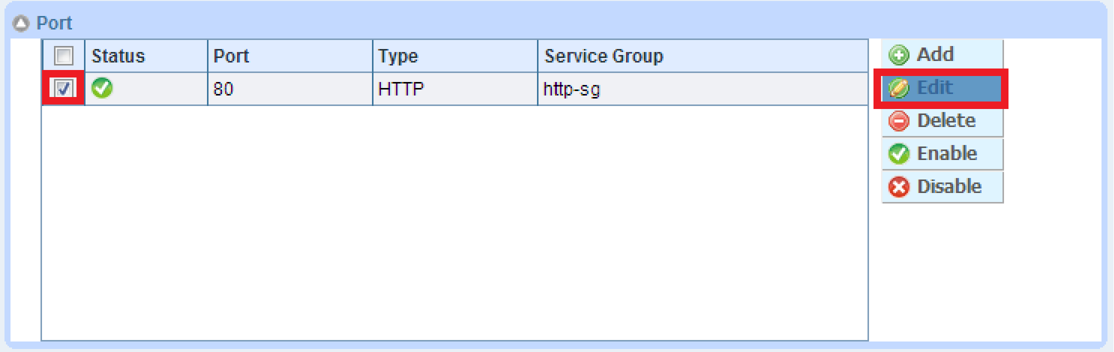
Figure 38: Configure HTTP Request Header Time in HTTP Template

4. Click **OK**.

5. Apply the HTTP template (in this example, “Policy-HTTP-Slowloris”) to the virtual server port, under the virtual server setting. To do so, navigate to Navigate to **Config Mode** > **SLB** > **Service** > **Virtual Server**.
   Note: *Prior to ACOS 2.7.1, PBSLB is located at* ***Config Mode > Service > SLB > Virtual Server***.

6. Select and edit a virtual server where you want to apply the HTTP policy
   Note: *If you didn’t configure a virtual server yet, please do so by clicking* ***Add***.

7. In the **Port** section, select a virtual server port where you want to apply the HTTP template (in this example, “Policy-HTTP-Slowloris”). Click **Edit**.

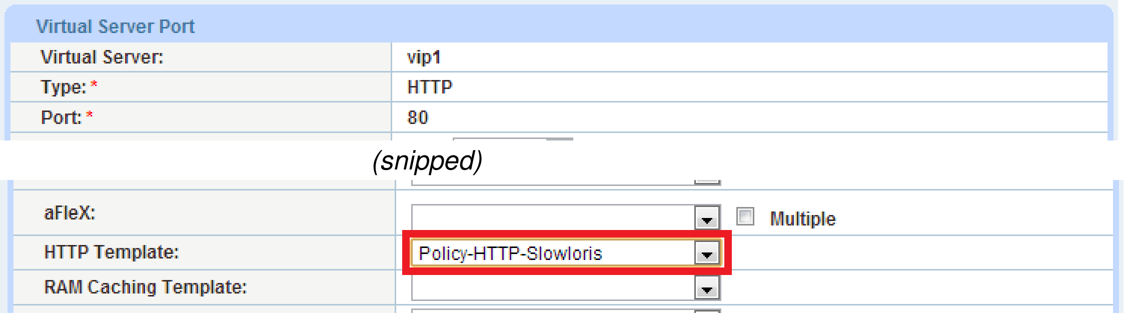


Port

□	Status	Port	Type	Service Group
☑	✓	80	HTTP	http-sg

Figure 39: Editing Virtual Server Port under Virtual Server

8. On the Virtual Server Port page, select the HTTP template (in this example, “Policy-HTTP-Slowloris”) from the **HTTP Template** drop-down list.



Virtual Server Port

Virtual Server:	vip1
Type: *	HTTP
Port: *	80

(snipped)

aFleX:	□ Multiple
HTTP Template:	Policy-HTTP-Slowloris
RAM Caching Template:	

Figure 40: Apply HTTP template on a virtual port

9. Click **OK**.

10. Go to the third step in the CLI section.

Configuration [CLI]

The CLI is required to complete the configuration. If you used the GUI procedure above, go to step 3 in this CLI procedure.

1. Use the following commands to configure the HTTP Request Wait Time:

```
ACOS(config)#slb template http Policy-HTTP-Slowloris
ACOS(config-http)#req-hdr-wait-time 7
```

2. Use following commands to apply the HTTP template to a virtual server port:

```
ACOS(config)#slb virtual-server vip1
ACOS(config-slb vserver)#port 80 http
ACOS(config-slb vserver-vport)#template http Policy-HTTP-Slowloris
```

3. (CLI only) Use following command at the global configuration level to enable enhanced SLB DDoS protection:

```
ACOS(config)#slb enable-ddos
```

4.3.5 SLOW POST ATTACK

A Slow POST attack is a common HTTP DoS attack, wherein an attacker sends HTML POSTs at slow rates under the same session. The Slow POST attack causes the web server application threads to await the end of boundless POSTs in order to process them. This causes exhaustion of web server resources and prevents service for legitimate traffic. Some DoS tools such as Tor's Hammer and R.U.D.Y DoS use this method with some new functionality to make detecting and tracking the attacker more difficult.

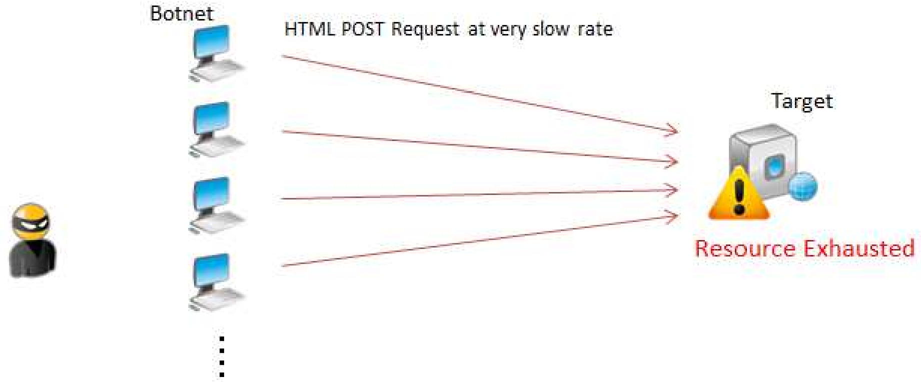


Figure 41: Slow POST Attack

Mitigation: HTTP Template "HTTP Request Header Time Out"

This attack has similar behavior to a Slowloris attack. Likewise, an A10 ADC device can mitigate this kind of attack with the HTTP Request Header Time Out feature, configured within HTTP templates. For more details and configuration, please refer to Slowloris.

In addition, A10 provides the "Force Delete Timeout" option in TCP-Proxy templates. This option forces deletion of any session that is still active after the specified number of seconds. When used in combination with the reset-fwd and reset-rev options, it can help clean up user connections with RSTs instead of allowing the connections to hang. For more details of Force Delete Timeout option, please see the *System Configuration and Administration Guide*.

4.3.6 SOCKSTRESS ATTACK

Sockstress is a program used to attack servers running common operating systems (such as Windows, Mac, Linux, BDS, and so on) on the Internet and other networks utilizing TCP. This includes any router or other Internet appliance that accepts TCP connections. An attacker tries to exploit the TCP/IP stack vulnerability by flooding a target system with an excessive number of TCP connections, by sending specially crafted packets with the TCP receive window size set to a very small value.

After the TCP connection is established (3-way handshake), the attacker sends an HTTP request and sets the window size to zero. The target system sends zero-window probes, but no data since the window size is 0. The connection keeps consuming kernel memory and, by creating large numbers of such connections, attackers can exhaust the TCP memory pool and block new connections from opening.

Sockstress attacks typically use the following strategies:

- Connection Flood Stress
- Zero Window Stress
- Small Window Stress
- Segment Hole Stress
- Req, Fin, Pause Stress

Mitigation: System-wide PBSLB (with IP Anomaly Filter) and IP Limiting

Sockstress uses several attack strategies as described above. Most attacks can be mitigated by the IP Anomaly Filtering along with system-wide PBSLB. For Connection Flood attacks, the IP Limiting feature with Layer 4 Rate Limiting will help prevent system resources on target systems from being overwhelmed.

For IP Anomaly filter and system-wide PBSLB configuration, please refer to Out of Sequence Attack, TCP Zero Window Attack and Invalid Payload Packets (HTTP/SSL).

For IP Limiting configuration, please refer to HTTP GET Flood. You can use (or add) Connection Limit and Connection Rate Limit options to enable Layer 4 rate limiting when you configure the LID action in the Policy template and/or GLID.

4.4 DNS SERVER ATTACKS

The DNS infrastructure is one of the most attractive targets for attackers, since many essential Internet-based applications including web access, e-mail, and voice services heavily rely on DNS. Moreover, DNS traffic usually is unrestricted, meaning many organizations have limited defense mechanisms in place to monitor their DNS traffic and to protect their DNS infrastructure from attacks.

4.4.1 DNS FLOOD ATTACK

DNS Flood attacks are used to attack a target DNS server directly by sending high amounts of DNS requests to UDP port 53. The target DNS server is overwhelmed in attempting to process those DNS requests, resulting in an unavailable service and denying service to legitimate requests.

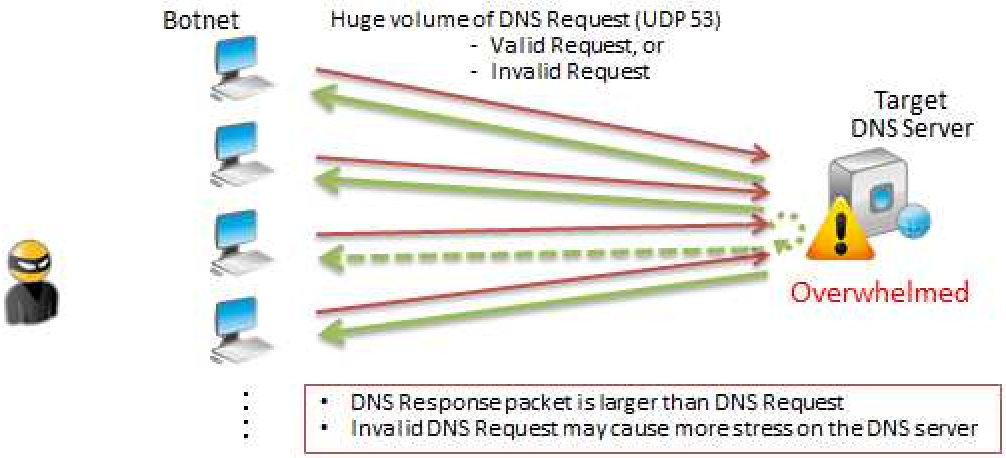

Botnet
Huge volume of DNS Request (UDP 53)
- Valid Request, or
- Invalid Request
Target
DNS Server
Overwhelmed
• DNS Response packet is larger than DNS Request
• Invalid DNS Request may cause more stress on the DNS server

Figure 42: DNS Flood Attack

Mitigation: DNS Firewall Feature

A10 provides the DNS Firewall feature to perform sanity checks on DNS client requests. In some cases of DNS Flood, DNS Requests are sent to UDP port 53 without containing a valid DNS Request header. This type of attack is known as a DNS UDP Flood attack. The A10 ADC device can discard the invalid requests.

The DNS Firewall feature also provides connection-rate limiting for "look-alike" valid DNS requests flooded by a botnet. This protection helps the target DNS server avoid overload.

Configuration [GUI]

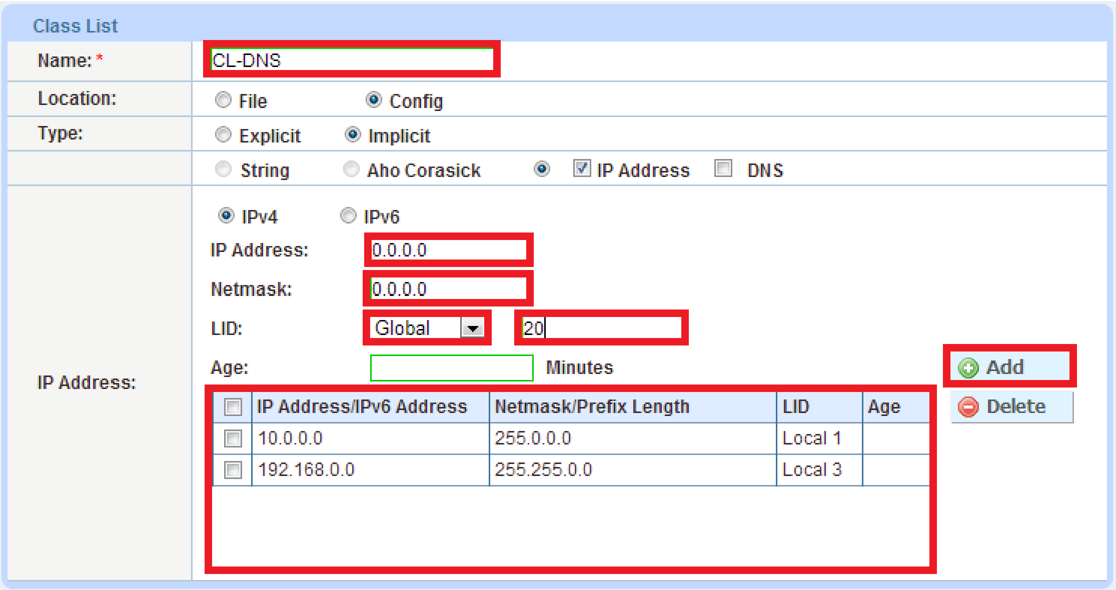
1. Navigate to **Config Mode** > **SLB** > **Service** > **Class List**.
   Note: *Prior to ACOS 2.7.1, PBSLB is located on* ***Config Mode > Service > SLB > Class List***.

2. Click **Add**.

3. Enter **Name** and **IP Address** and enter the LID entries. In this example, the class list is named “CL-DNS” and contains three IP address subnets with LIDs assigned:

```
10.0.0.0 /8       Local LID 1  ; e.g. Internal client
192.168.0.0 /16   Local LID 3  ; e.g. Guest client
0.0.0.0 /0        Global LID 20; e.g. Else (External client)
```

***Note**: Local IDs (LIDs) can provide connection-rate limiting only, whereas GLIDs can additionally provide connection limiting, request limiting, and request-rate limiting features.*



Class List

Name: * CL-DNS

Location: ○ File ● Config

Type: ○ Explicit ● Implicit

○ String ○ Aho Corasick ● ☑ IP Address □ DNS

IP Address:

● IPv4 ○ IPv6

IP Address: 0.0.0.0

Netmask: 0.0.0.0

LID: Global 20

Age: Minutes

Add

Delete

□	IP Address/IPv6 Address	Netmask/Prefix Length	LID	Age
□	10.0.0.0	255.0.0.0	Local 1	
□	192.168.0.0	255.255.0.0	Local 3	

Figure 43: Class List

4. Click **OK**.

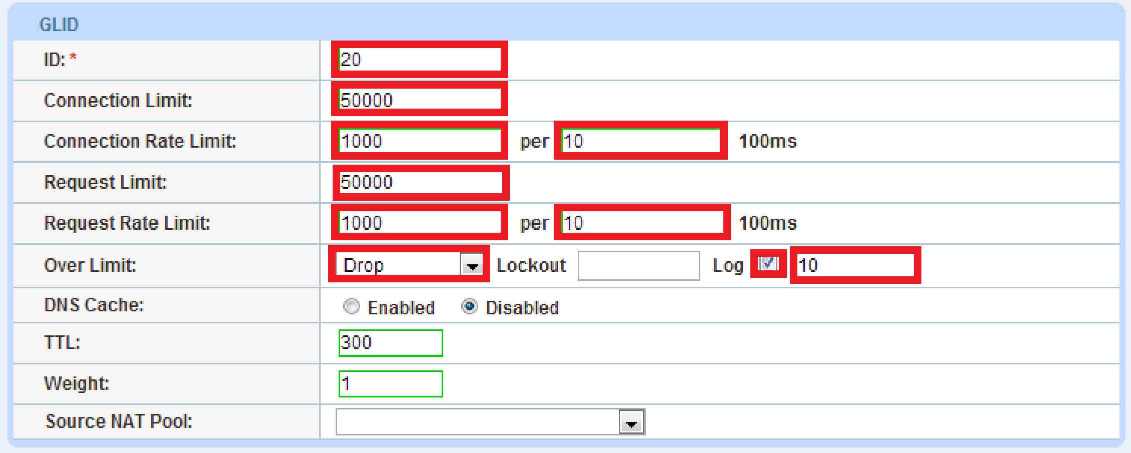
5. Navigate to **Config Mode** > **SLB** > **Service** > **GLID**.
   ***Note**: Prior to ACOS 2.7.1, PBSLB is located on **Config Mode > Service > SLB > GLID**.*

6. Click **Add**.

7. Enter the limit ID (GLID or LID) and configure rate limiting and other settings. In this example, GLID 20 is specified:

   - DNS Connection Limit : 50,000 sessions
   - DNS Request Limit : 50,000 sessions

- DNS Request Rate Limit: 1,000 requests per second (RPS)
- Over Limit Action: Drop and Logging with 10-minute interval



GLID

ID: *	20
Connection Limit:	50000
Connection Rate Limit:	1000 per 10 100ms
Request Limit:	50000
Request Rate Limit:	1000 per 10 100ms
Over Limit:	Drop Lockout Log ☑ 10
DNS Cache:	○ Enabled ● Disabled
TTL:	300
Weight:	1
Source NAT Pool:	

Figure 44: GLID setting

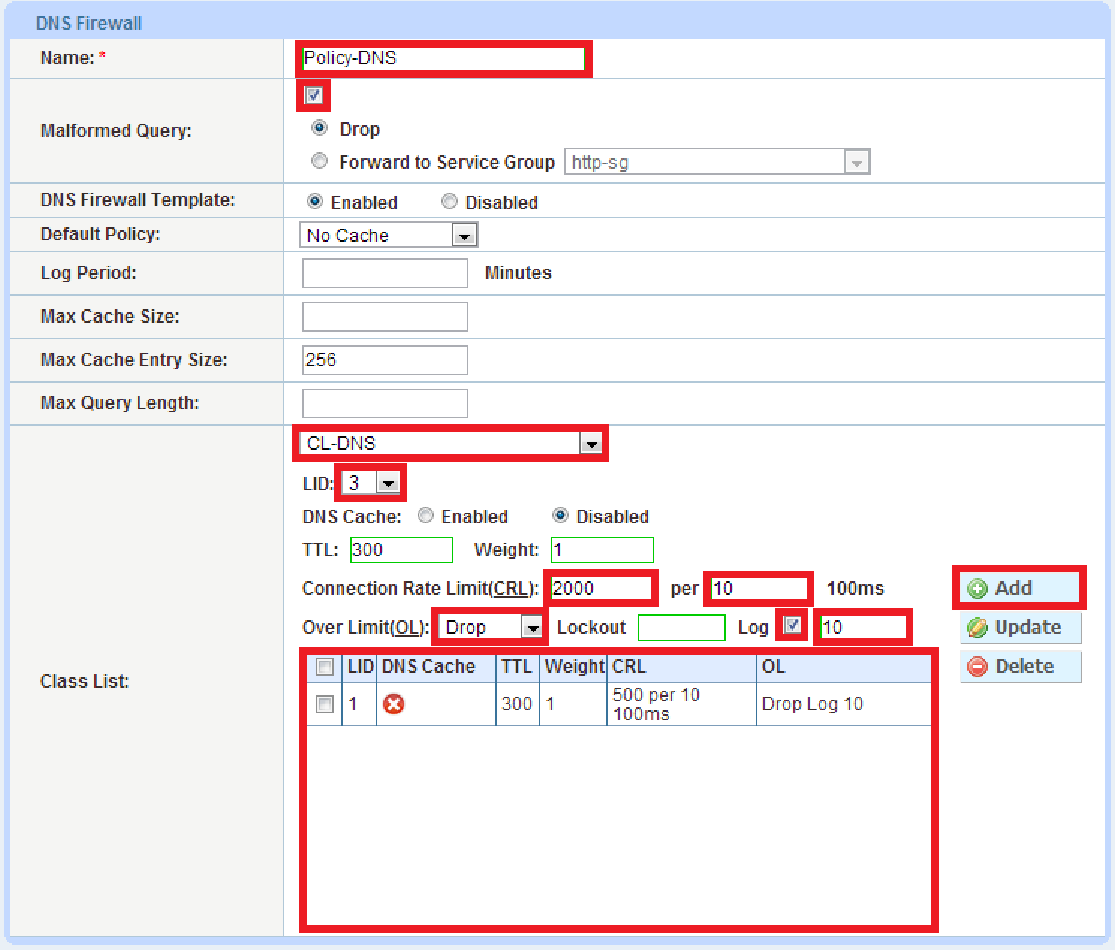
8. Navigate to **Config Mode** > **Security** > **Template** > **DNS Firewall**.
   Note*: Prior to ACOS 2.7.1, PBSLB is located on* ***Config Mode > Service > Template > Application > DNS****.*

9. Click **Add**.

10. Enter a **Name** and select **Malformed Query**, then select the class list from the **Class List** drop-down menu. In this example, the name is "Policy-DNS" and the class list is "CL-DNS".

11. Configure conditions/actions for each GLID or LID specified in the class list. In this example,

    - LID 1 - Connection Rate Limit : 500 RPS, Overlimit action : Drop with logging
    - LID 3 - Connection Rate Limit : 2,000 RPS, Overlimit action: Drop with logging



DNS Firewall

Name: *	Policy-DNS
Malformed Query:	☑ ● Drop ○ Forward to Service Group http-sg
DNS Firewall Template:	● Enabled ○ Disabled
Default Policy:	No Cache
Log Period:	Minutes
Max Cache Size:	
Max Cache Entry Size:	256
Max Query Length:	
Class List:	CL-DNS LID: 3 DNS Cache: ○ Enabled ● Disabled TTL: 300 Weight: 1 Connection Rate Limit(CRL): 2000 per 10 100ms Over Limit(OL): Drop Lockout Log ☑ 10

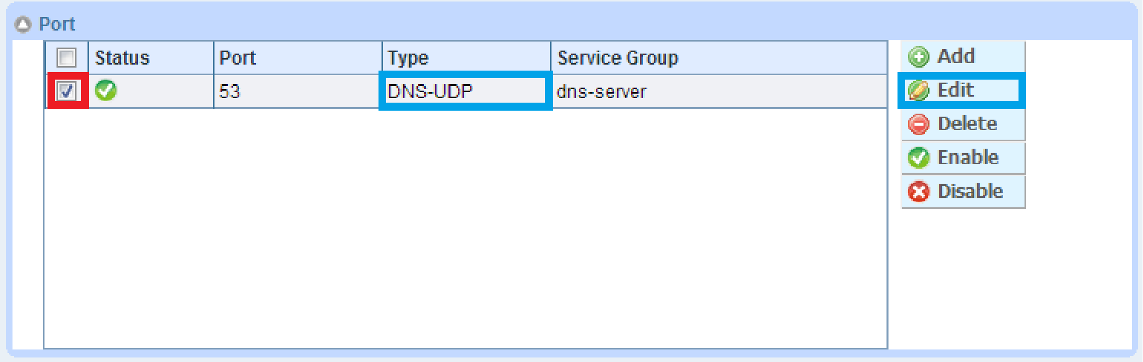
□	LID	DNS Cache	TTL	Weight	CRL	OL
□	1	☒	300	1	500 per 10 100ms	Drop Log 10

Figure 45: DNS Firewall Template

12. To Apply the DNS Firewall template to a virtual port, navigate to **Config Mode** > **SLB** > **Service** > **Virtual Server**.
    Note: *Prior to ACOS 2.7.1, PBSLB is located on **Config Mode > Service > SLB > Virtual Server**.*

13. Select and edit a virtual server where you want to apply the DNS Firewall template.
    Note: *If you didn't configure a virtual server yet, please do so by clicking **Add**.*

14. In the **Port** section, select a virtual server port where you want to apply the DNS Firewall Policy template (in this example, "Policy-DNS") then click **Edit**.
    Note: *You can take advantage of the DNS sanity check if the proxy mode (service type) selected on the virtual port is DNS-UDP (instead of UPD). This is selected from the **Type** drop-down list.*

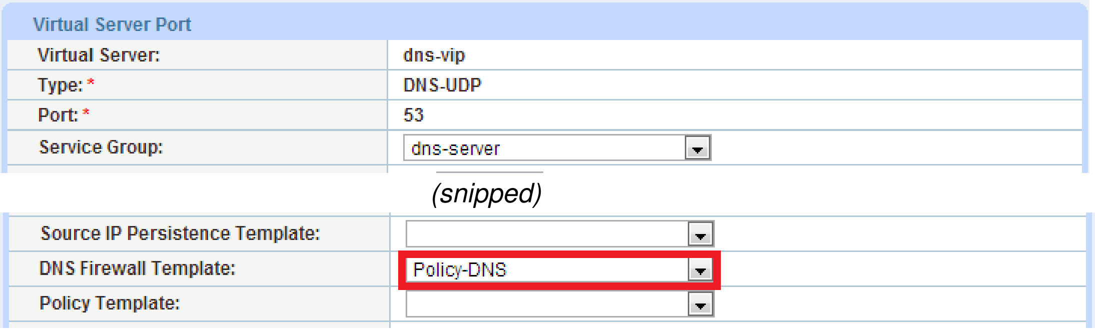


Port

□	Status	Port	Type	Service Group
☑	✓	53	DNS-UDP	dns-server

Figure 46: Editing Virtual Port (DNS-UDP type)

15. On the Virtual Server Port page, select the DNS Firewall policy (in this example, “Policy-DNS”) from the **DNS Firewall Template** drop-down list.



Virtual Server Port

Virtual Server:	dns-vip
Type: *	DNS-UDP
Port: *	53
Service Group:	dns-server

(snipped)

Source IP Persistence Template:	
DNS Firewall Template:	Policy-DNS
Policy Template:	

Figure 47: Select DNS Firewall policy template

16. Click **OK** then **Save** to store your configuration changes.

Configuration [CLI]

Following is the CLI equivalent of the GUI example above:

```
ACOS(config)#class-list CL-DNS
ACOS(config-class list)#10.0.0.0 /8 lid 1
ACOS(config-class list)#0.0.0.0 /0 lid 10
ACOS(config-class list)#192.168.0.0 /16 lid 2
ACOS(config-class list)#exit

ACOS(config)#glid 20
ACOS(config-global lid)#conn-limit 50000
ACOS(config-global lid)#conn-rate-limit 1000 per 10
ACOS(config-global lid)#request-limit 50000
ACOS(config-global lid)#request-rate-limit 1000 per 10
ACOS(config-global lid)#over-limit-action log 10
ACOS(config-global lid)#exit

ACOS(config)#slb template dns Policy-DNS
ACOS(config-dns)#malformed-query drop
ACOS(config-dns)#class-list name CL-DNS
ACOS(config-dns)#class-list lid 1
ACOS(config-dns-lid)#conn-rate-limit 500 per 10
ACOS(config-dns-lid)#over-limit-action log 10
ACOS(config-dns-lid)#class-list lid 3
ACOS(config-dns-lid)#conn-rate-limit 2000 per 10
ACOS(config-dns-lid)#over-limit-action log 10
ACOS(config-dns-lid)#exit
ACOS(config-dns)#exit

ACOS(config)#slb virtual-server dns-vip
ACOS(config-slb vserver)#port 53 dns-udp
ACOS(config-slb vserver-vport)#template dns Policy-DNS
ACOS(config-slb vserver-vport)#exit
ACOS(config-slb vserver)#exit
ACOS(config-slb)#exit

ACOS(config)#write memory
```

4.4.2 DNS AMPLIFICATION ATTACK

DNS Amplification attacks send valid UDP-based DNS requests using a spoofed IP address (such as in the case of a Smurf attack) to the intended target (victim). Due to the nature of the DNS protocol, the volume of DNS responses is much larger than that of DNS requests, so that the attacker is able to amplify the volume of the traffic destined to the target system.

The attacker can enhance the DNS Amplification attack further by:

- Intentionally sending DNS requests that expect a large volume of response (for example, "any" requests).
- Using a botnet to send even more such requests simultaneously.

The results of this attack have two potential targets (victims). One is the system that is the legitimate holder of the spoofed IP address. The other is the DNS server receiving the requests, which might be overwhelmed in attempting to process the series of requests.

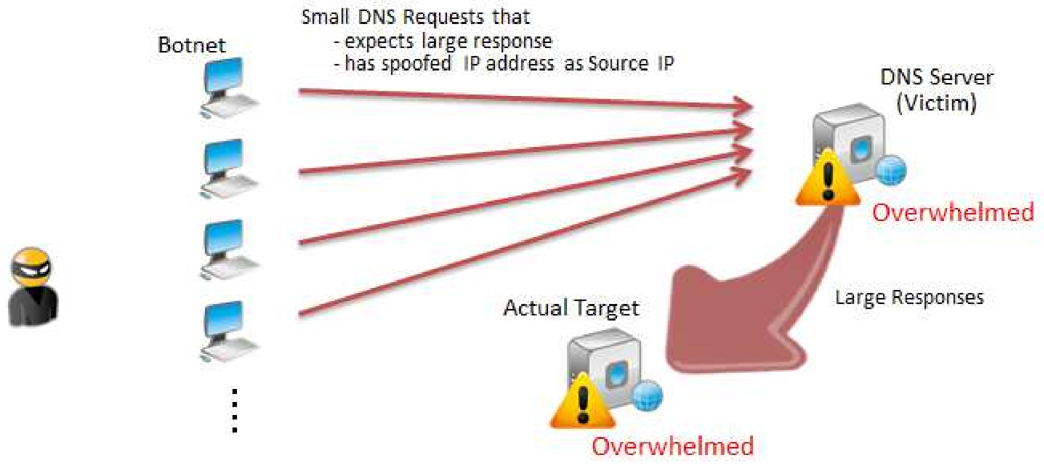


Figure 48: DNS Amplification Attack

Mitigation: Combination of DNS Firewall Template, IP Limiting and System-wide PBSLB

A10 offers mitigation technologies to deal with the DNS Amplification attack, using the DNS Firewall feature in combination with IP Limiting and system-wide PBSLB. As described in a previous section, the DNS Firewall feature includes granular DNS connection-rate limiting (and connection limiting if a GLID is used) in addition to the DNS request sanity check. You also can combine IP Limiting with system-wide PBSLB to limit maximum connections and connection rate on a per-client basis.

For more details and configuration of the DNS Firewall feature, please refer to DNS Flood Attack.

For system-wide PBSLB configuration, please refer to Out of Sequence Attack.

For more details and configuration of IP Limiting, please refer to HTTP GET Flood. You can use (or add) connection limiting and connection-rate limiting to enable Layer 4 rate limiting when you configure the LID action in the Policy template or GLID.

***Note**: In addition to the features described above, A10 provides enhanced and very flexible DNS DDoS protection (such as DNS "any" filtering and rate limiting) using aFleX. aFleX is outside the scope of this deployment guide.*

***Note**: In ACOS 2.7.1-P1 and above, an additional security feature, Web Application Firewall (WAF), is available. However, the WAF is outside the scope of this deployment guide. For information about this feature, please see the Web Application Firewall Guide.*

5 SUMMARY AND CONCLUSION

The sections above show how to mitigate DDoS attacks, specifically those that frequently target web servers and DNS servers, by deploying DDoS mitigation features of the A10 ADC device.

Recommendations

When using the A10 ADC to deal with DDoS attacks, the following key features are recommended:

- DDoS Protection should be enabled.
- Hardware-based SYN Cookies should be enabled (if supported on your model).
- IP Anomaly filters should to be turned on along with system-wide PBSLB using dynamic Black/White List entries (IP address 0.0.0.0/0).
- IP Limiting should be configured.
- DNS Firewall feature should be enabled and applied to virtual ports configured for service type UDP-DNS.

More Information

By using the A10 ADC device (A10 Thunder and AX Series Application Delivery Controllers), significant benefits are achieved for DDoS attack mitigation. For more information about A10 ADC products, please refer to the following URLs:

http://www.a10networks.com/products/axseries.php

http://www.a10networks.com/resources/solutionsheets.php

http:/www.a10networks.com/resources/casestudies.php