A10 Thunder TPS Hybrid DDoS Protection Deployment with Verisign OpenHybrid

Thunder TPS Signals DDoS Attack Information to Verisign’s OpenHybrid, Creating a Powerful, Hybrid, DDoS Protection Solution
Table of Contents

Overview..........................................................................................................................................................3
Deployment Prerequisites ..................................................................................................................................3
   On-Premise DDoS Protection .........................................................................................................................3
   Cloud-Based DDoS Protection ......................................................................................................................3
Hybrid DDoS Protection Solution Overview ..................................................................................................3
   Working Concept .........................................................................................................................................3
   Thunder TPS Deployment Model ..................................................................................................................3
   Solution Topology ......................................................................................................................................4
Example Hybrid DDoS Protection Solution Topology .....................................................................................5
Setting Up Verisign Cloud-Based DDoS Protection ..........................................................................................5
Configuring Thunder TPS for DDoS Alert Signaling .......................................................................................7
   General Configuration .................................................................................................................................7
   Sample CLI Configuration ...........................................................................................................................7
   A Script for Signaling ................................................................................................................................9
Protected Objects and Violation Actions ........................................................................................................11
   Configure DDoS Zone Object .......................................................................................................................11
   CLI Configuration ......................................................................................................................................14
   Traffic Profile Auto Learning ......................................................................................................................14
   Add Mitigation Rules and Violation Actions for Signaling .......................................................................16
   CLI Configuration ......................................................................................................................................19
Proof of Concept for Hybrid DDoS Protection Solution ..................................................................................19
   Log and Report on Thunder TPS ..................................................................................................................19
   Verisign Portal View ................................................................................................................................20
Summary ......................................................................................................................................................21
Appendix ......................................................................................................................................................21
   Thunder TPS Configuration .........................................................................................................................21
   DDoS Script for Verisign Solution ................................................................................................................24
About A10 Networks .....................................................................................................................................25

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.
Overview
This guide explains how to build a hybrid DDoS protection solution using A10 Networks® Thunder TPS™ line of Threat Protection Systems integrated with a cloud-based Distributed Denial of Service (DDoS) protection service. A10 Thunder TPS, powered by A10 Networks Advanced Core Operating System (ACOS®), is a scalable high-performance DDoS protection device. It protects against multi-vector DDoS attacks and provides various DDoS detection and mitigation options that can be customized. This guide leverages a script execution, which extends the integration capability of A10's DDoS protection solution.

The Verisign DDoS Protection Service, powered by the OpenHybrid architecture, is an intelligent, cloud-based DDoS protection service. OpenHybrid is an open Application Programming Interface (API) architecture and provides interoperability and flexibility, allowing on-premise security devices to signal threat information to Verisign.

The hybrid DDoS protection solution in this guide consists of A10 Thunder TPS as an on-premise DDoS protection device, and Verisign DDoS Protection Service as a cloud-based DDoS protection service. A10 Thunder TPS functions as a DDoS detector and sends signals to Verisign’s cloud service by executing a script as a violation action. This solution allows the customer a means of moving quickly to a DDoS cloud protection solution when a DDoS attack becomes too large for the customer’s infrastructure to handle.

Deployment Prerequisites
To deploy the A10-Verisign hybrid DDoS protection solution, the following are required:

On-Premise DDoS Protection
- A10 Networks Thunder 3030S TPS, 4435(S) TPS, 6435(S) TPS or 6635(S) TPS
  - ACOS TPS release 3.2 or higher
  - Internet access from Thunder TPS (data port) for signaling
- A border (upstream) router

Cloud-Based DDoS Protection
- A subscription for Verisign DDoS Protection Service
- A user account for Verisign’s portal

Hybrid DDoS Protection Solution Overview

Working Concept
This hybrid DDoS protection solution combines an on-premise DDoS protection device with a cloud-based DDoS protection service. Thunder TPS is deployed as the on-premise DDoS protection device, which provides full-time DDoS detection and mitigation against any DDoS attack traffic, including so-called multi-vector attacks, which combine network layer (L3/L4) attacks and sophisticated application layer (L7) attacks.

This is already a powerful DDoS protection solution; however, there may be one additional concern, namely those times when your uplinks are simply overwhelmed by a large volumetric DDoS attack. The answer is to have cloud-based DDoS protection such as the Verisign Cloud DDoS Protection Service as a joint solution for such incidents.

When Thunder TPS detects patterns that may overwhelm the uplink, it signals attack and victim information to Verisign as one of the configurable actions. Upon receiving the signal from Thunder TPS, a Verisign support ticket is issued instantly, and the support team will contact with and assist the customer right away.

Thunder TPS Deployment Model
With this solution, Thunder TPS functions as a volumetric DDoS attack detector on top of a full-time multi-vector DDoS protection device. Therefore, Thunder TPS is deployed with an in-path deployment model such as Symmetric or Asymmetric Proactive mode so that it can inspect all incoming traffic. It can also be deployed in TAP mode.
As Thunder TPS supports L2 (transparent) mode or L3 (routing) mode, it can fit any type of network topology. You can locate it right in front of a border router in L2 mode, or between a border router and firewall(s) in L3 mode, just like a normal router.

**Solution Topology**

Figure 1 shows a sample hybrid DDoS protection solution topology with Thunder TPS and Verisign.

![Solution Topology Diagram](image)

**Figure 1: Hybrid DDoS protection solution topology**

Below is a process flow for this hybrid solution.

1. Thunder TPS monitors all incoming traffic using DDoS protection rules. With in-path deployment, all of the traffic is monitored by Thunder TPS and forwarded to the final destination unless an anomaly is detected. In the case of a TAP mode deployment, all traffic is analyzed and then dropped at the Thunder TPS.

2. Once Thunder TPS detects any anomalous traffic based on behavior analysis or any predefined countermeasures, it takes DDoS protection actions. For example, it will:
   a. Escalate the suspicious traffic to the next protection level
   b. Enforce some countermeasures (if configured)
   c. Signal DDoS attack information to Verisign by executing a script
   d. Log and store the DDoS event, and more

3. Upon receiving the signal from Thunder TPS, Verisign OpenHybrid automatically creates a DDoS attack event under the alerts page and issues a ticket number. Then, Verisign support contacts the customer and assists to protect against volumetric DDoS attacks.

4. Once agreed upon by both parties, Verisign will initiate traffic redirection using a BGP or DNS technique, in order to scrub traffic.

5. Verisign scrubs the suspect traffic, and then only clean traffic is forwarded to the original destination using a generic routing encapsulation (GRE) tunnel (or regular path, if available).
Example Hybrid DDoS Protection Solution Topology

Figure 2 shows a topology diagram of the hybrid DDoS protection solution presented in this deployment guide.

Setting Up Verisign Cloud-Based DDoS Protection

1. Log in on the Verisign DDoS Protection Service Portal.

2. Make sure that account setup and on-premise devices are properly registered/set up by Verisign.
   a. Go to Account Setting > Account Services and check the account services information.
b. Go to **Account Setting > Monitoring** and confirm the number of devices registered as OpenHybrid Sources. These sources correspond to the "source_id" within the integration script.

3. Obtain an API key for signaling.
   In order to take advantage of the OpenHybrid architecture, a REST API is used to signal DDoS attack events. An API key is required for a secure communication between Verisign OpenHybrid and the source (on-premise) devices. The API key is located on the **My Profile** page of the portal.
Configuring Thunder TPS for DDoS Alert Signaling

General Configuration

In this example, Thunder TPS is deployed in asymmetric proactive model using routing (L3) mode. All incoming traffic passes through the Thunder TPS device for full-time on-premise DDoS protection.

The following needs to be configured properly based on your environment:

- Host name
- A DNS server to resolve the Verisign portal site
- Interface/network/VLAN configuration
  - All the interfaces are marked as “ddos outside” (by default).
  - For TAP mode, create appropriate VLAN(s) and add the interface as “ddos tap”.
  - Secure Internet access using data port for communication with Verisign.
- Routing configuration (static or dynamic routing protocol)
  - It’s in asymmetric proactive mode and all ports are marked as “ddos outside” by default, so make sure that return/response traffic will not pass the Thunder TPS device. Otherwise, all return traffic will be monitored/checked and might be interrupted unnecessarily.
- General DDoS setting
  - Log enabled
  - Protection enabled

  **Note:** Please enable DDoS protection after you configure the DDoS protected object (or “Allow all” rule). Otherwise, traffic will be dropped.

  - (Optional) “Allow all” rule for any destination

  **Note:** This is recommended when you deploy Thunder TPS for the first time until you configure DDoS protected objects. This can be removed once you configure DDoS protected objects.

Sample CLI Configuration

```bash
! system anomaly log
system attack log
system ddos-attack log
!
ip dns primary 8.8.8.8
!```
hostname TH3030S-TPS
!
interface management
  ip address 10.100.9.155 255.255.255.0
  ip default-gateway 10.100.9.1
!
interface ethernet 1
  name To_RT-A
  ddos outside
    enable
    ip address 192.168.0.155 255.255.255.0
!
interface ethernet 2
  name To_RT-B
  ddos outside
    enable
    ip address 192.168.1.155 255.255.255.0
!
interface ethernet 3
  name Internet_access
    enable
    ip address 10.100.10.155 255.255.255.0
!
!
ip route 0.0.0.0 /0 10.100.10.1
ip route 192.168.9.0 /24 192.168.1.114
ip route 203.0.113.0 /24 192.168.0.119
!
ddos protection enable
!
!
Note: For TAP mode deployment, use the following sample interface configuration instead of interface ethernet 1 and 2 above.

!
vlan 200
  tagged ethernet 4
!
vlan 202
  tagged ethernet 4
!
!

ddos tap
ethernet 4
!
A Script for Signaling

Table 1 shows parameters used for signaling (API communication) between Thunder TPS and Verisign. Some parameters use variables passed by Thunder TPS based on the event and others are static values.

Table 1: Parameters for Signaling

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API_Key</td>
<td>Unique API key used for authentication to the Verisign OpenHybrid API. This can be found in the Verisign portal as stated in the <a href="#">previous section</a>.</td>
</tr>
<tr>
<td>source_id</td>
<td>Unique ID of Thunder TPS (or any signaling source). This corresponds to the source ID under the “Monitoring” tab in the Verisign portal.</td>
</tr>
<tr>
<td>alert_type</td>
<td>Alert classification. In this solution, Thunder TPS alert type (e.g., the indicator that triggered the escalation) and threshold value are used. The corresponding TPS DDoS variables are defined as “$DDOS_ALERT_TYPE” and “$DDOS_THRESHOLD”.</td>
</tr>
<tr>
<td>misc_info</td>
<td>String value (max. 1,000 characters) for miscellaneous information. In this solution, it uses the Thunder TPS DDoS event type that is defined as variable “$DDOS_EVENT”.</td>
</tr>
<tr>
<td>destination</td>
<td>DDoS attack target information. In this solution, zone description is used for this. The variable is “$DDOS_DESCRIPTION”.</td>
</tr>
<tr>
<td>destination_port_list</td>
<td>Targeted port information where attack is detected. On Thunder TPS, this is the port defined in the DDoS DST zone object where the violation occurred. The variable is “$DDOS_DST_PORT”.</td>
</tr>
<tr>
<td>destination_protocol_list</td>
<td>Targeted protocol information where attack is detected. On Thunder TPS, this is the protocol defined in the DDoS DST zone object where the violation occurred. The variable is “$DDOS_PROTOCOL”.</td>
</tr>
<tr>
<td>Status</td>
<td>Status information. Static value “ACTIVE”.</td>
</tr>
<tr>
<td>severity</td>
<td>Severity information. Static value “HIGH”.</td>
</tr>
</tbody>
</table>

*Note:* For more details of Verisign OpenHybrid, see the [specification](#).

1. Download the shell script file (file name verisign.sh) from the [A10 Support Page](#).
2. Open the script file and edit the variables as needed:
   a. Replace “API_Key” with the one you obtained at the Verisign portal.
   b. Update “source_id” with appropriate signal source ID.
3. Import the script (verisign.sh) to Thunder TPS.
   
   [CLI] #import ddos script verisign.sh use-mgmt-port scp://root@scp-server-ip/folder/verisign.sh
   
   [GUI] Navigate to DDoS Protection > Templates > General > DDoS Script and click “Import” ➜ Add “verisign.sh” as File Name and specify the protocol and location of your server. Click “Apply” ➜.

![Figure 7: Import a script file](#)
Here is the full `verisign.sh` script for the Thunder TPS hybrid DDoS protection solution using Verisign OpenHybrid.

```bash
#!/bin/sh
# Copyright 2015, A10 Networks.
# Thunder TPS DDoS script for Verisign DDoS Cloud Service
# Version 1.0 - 12.01.2015
#
### 1. REPLACE “API_Key” VALUE WITH YOURS PROVIDED BY VERISIGN ###
### 2. UPDATE ‘source_id’ WITH PROPER SIGNAL SOURCE DEVICE ID ###
###          NOTE: MAKE SURE TO USE UNIX EOL FORMAT ###
#
API_Key="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
curl -k -i -X POST https://<Verisign OpenHybrid URL> -H "Authorization: AMP $API_Key" -d \
"{    'source_id' : 'A10Source2',    'alert_type' : '$DDOS_ALERT_TYPE $DDOS_THRESHOLD',    'misc_info' : '$DDOS_EVENT',    'destination_port_list' : [$DDOS_DST_PORT],    'destination_protocol_list' : [$DDOS_PROTOCOL],    'status' : 'ACTIVE',    'severity' : 'HIGH',    'destination' : '$DDOS_DESCRIPTION' 
}
```

Note: If you're using a Windows device to edit/create the script, please make sure that you use **UNIX EOL Format**. Otherwise, the script execution may fail due to “command not found”. Some editors such as Notepad++ can change the EOL format.

Figure 8: UNIX EOL Format on Notepad++
Protected Objects and Violation Actions

This section provides the DDoS protection configuration of Thunder TPS. With the "protected zone" object, Thunder TPS provides an advanced on-premise DDoS protection and simultaneously, a signaling solution. On-premise DDoS protection includes, but is not limited to: traffic pattern monitoring using an auto learned traffic profile or static thresholds; 5 levels of DDoS mitigation rule sets with automatic DDoS level escalation; a variety of other actions. For more details about DDoS protection features using "protected zone object", refer to the DDoS Mitigation Guide.

In this example, Thunder TPS is deployed in asymmetric proactive mode to protect a web server, and it uses auto traffic profile learning for monitoring and detection. As for DDoS mitigation, there is no countermeasure set on level 0. If traffic exceeds any of the indicator thresholds, the traffic will immediately be escalated to level 1 and a basic countermeasure (i.e., SYN packet authentication) is applied to protect destination/victims. While all incoming traffic is evaluated, only successfully authenticated traffic is forwarded to the destination. Mitigation level 2 is also configured for more aggressive countermeasures along with Verisign signaling as a violation action. If the traffic keeps coming in on level 2 and exceeds the indicators’ threshold (for example, pkt-rate), Thunder TPS sends a signal to Verisign by executing the above script. It’s highly recommended that you configure Verisign signaling violation action on the highest mitigation level you have.

Configure DDoS Zone Object

This section guides you through the creation of a DDoS DST zone protected object step-by-step. It’s set as idle mode and will be activated in a later section.

1. Navigate to DDoS Protection > Protected Objects > Zones.
2. Click “Create”.
3. In the Basic box, add the following values:
   a. Zone Name: Z1V
   b. IP Address: IP addresses or subnets to be protected (192.168.9.113).

   ![Figure 9: DDoS zone object creation]

4. Move to the Global Parameters tab and add the following values:
   a. Description: "example.com-192.168.9.113"
      
      **Note:** This information is used as “Resource” information on the Verisign portal.
   b. Operational Mode: “Idle”
   c. Check “Enable Logging” and “Logging Periodic”.
   d. Apply Threshold Profile:
      i. Create by clicking “+” icon and a pop-up window shows up.
      ii. Add Zone Profile Name: “ZP-Z1V”.
      iii. Click "Apply" to close the pop-up window.
5. Move to Service Port.
   a. Click “+” icon.
   b. Add “80” as Port or Port Range and select “http” from pull-down menu.
   c. Expand Details.
   d. Check Enable Detection.
   e. Check Protection Level 0 under Configure Protection Level section.
   f. Repeat these steps if there are other ports/services being used on the same server/destination.
6. (Option) Move to **IP Protocol**.
   This is to allow ICMP traffic and TCP/UDP traffic other than the port(s) defined in the above steps, if any are being used on the destination server.
   a. Click “+” icon.
   b. Select “icmp-v4” from IP Protocol, expand **Details** and check **Enable Detection**.
   c. Click “+” icon.
   d. Add “tcp”, “udp” and else accordingly. “Enable Detection” is not available here but you can add GLID (traffic rate limit) as needed.

7. Click **Update** icon at the bottom of this page to save the configuration changes.
**CLI Configuration**

```
ddos dst zone Z1V
  ip 192.168.9.113
  description example.com-192.168.9.113
  zone-profile ZP-Z1V
  operational-mode idle
  log enable periodic
  ip-proto tcp
  ip-proto udp
  ip-proto icmp-v4
    detection-enable
  port 80 http
    detection-enable
  level 0

Traffic Profile Auto Learning**

In order to perform automatic learning of traffic patterns, follow the steps below.

1. Confirm the original status of Threshold Profile (ZP-Z1V) created in the previous section.
   a. Navigate to **DDoS Protection > Templates > Zone > Threshold Profile**.
   b. Click **Edit** icon of the **Threshold Profile**: “ZP-Z1V”.
   c. Confirm that no items/values are listed under “port 80 HTTP” and also “ICMP-v4” protocol.

![Figure 14: DDoS zone template – Threshold Profile default](image)

2. Enable auto traffic profile learning during peace time.
   a. Navigate to **DDoS Protection > Protected Objects > Zones > Z1V**.
   b. On **Global Parameters** box, change **Operational Mode** to “Learning”.
      
      **Note:** Run enough time for Thunder TPS to learn and build a good traffic pattern profile. It’s also recommended to perform this operation during peak traffic hours.
   c. Stop “Learning” mode by changing the operational mode back to “Idle”.
      
      **Note:** It’s recommended to set back to “Idle” instead of “Monitor” mode until you review and confirm the threshold values of all indicators to avoid any unexpected traffic drop.
3. Confirm learned traffic threshold profile.
   a. Navigate to DDoS Protection > Templates > Zone > Threshold Profile.
   b. Click Edit icon of the Threshold Profile: “ZP-Z1V”.
   c. Confirm that indicators for both "port 80 HTTP" and "ICMP-v4" protocols are populated with threshold values (for both threshold per zone and per source).

   [Sample CLI output – Port 80 HTTP]
   TH3030S-TPS(config)#ddos zone-profile ZP-Z1V
   TH3030S-TPS(config-zone prf)#port 80 http
   TH3030S-TPS(config-zone prf-port)#show context
!Context configuration: 1044 bytes
port 80 http
  indicator pkt-rate
    src-threshold 108
    zone-threshold 198
  indicator syn-rate
    src-threshold 9
    zone-threshold 16
  indicator fin-rate
    src-threshold 9
    zone-threshold 16
  indicator rst-rate
    src-threshold 0
    zone-threshold 0
  indicator small-window-ack-rate
    src-threshold 0
    zone-threshold 0
  indicator empty-ack-rate
    src-threshold 81
    zone-threshold 148
  indicator small-payload-rate
    src-threshold 9
    zone-threshold 16
  indicator bytes-to-bytes-from-ratio
    src-threshold 0.00
    zone-threshold 0.00
  indicator syn-fin-ratio
    src-threshold 1.50
    zone-threshold 1.11
  indicator conn-miss-rate
    src-threshold 9
    zone-threshold 16
  indicator pkt-drop-rate
    src-threshold 0
    zone-threshold 0
  indicator pkt-drop-ratio
    src-threshold 0.00
    zone-threshold 0.00
  indicator concurrent-conns
    src-threshold 18
    zone-threshold 33

4. (Optional) Update values/threshold as needed.
5. Change operation mode to “Monitor” to activate the protected zone object “Z1V”.

**Add Mitigation Rules and Violation Actions for Signaling**

This section describes how to configure countermeasures and violation actions on Thunder TPS for this hybrid DDoS protection solution.

In this example, you have 3 mitigation levels configured (level 0-2). Level 0 is used as a pass-through rule and only for traffic pattern monitoring. If the traffic has violated any zone thresholds defined above, Thunder TPS escalates all of the traffic within the zone to level 1, where a countermeasure (i.e. SYN packet authentication) is applied to this traffic to validate the source/clients. With this rule, any traffic from unauthenticated sources will be dropped. If the attack traffic keeps coming in and exceeds the threshold, it’s then escalated to level
2 for further and more aggressive mitigations (i.e. SYN packet authentication, ACK packet authentication, black-list policy et. al.). Furthermore, you will have a static threshold for packet rates to detect any possibility of volumetric attacks that may overwhelm Internet uplink capacity. If traffic exceeds the threshold, Thunder TPS executes the script to signal a DDoS alert to the Verisign portal.

**Note:** It’s recommended that you have the Verisign signaling as a violation action on the highest mitigation level.

1. Configure TCP type DDoS zone-template for SYN authentication countermeasure.
   a. Navigate to **DDoS Protection > Templates > Zone > TCP**.
   b. Click **Create** icon.
   c. Add following information:
      i. **Name:** "tcp-l1"
      ii. Check **SYN Authentication**.
      iii. Select “Retransmit Check” as **Type**.
      iv. (option) Select “Blacklist-src” as **Fail Action**.
   d. Click **Apply** icon.
   e. Repeat these steps (a – d) to create TCP mitigation rule for level 2 "tcp-l2”.

![Figure 17: DDoS zone template – TCP](image)

2. Configure DDoS violation action for signaling.
   a. Navigate to **DDoS Protection > Templates > Action > Violation Action**.
   b. Click **Create** icon.
   c. Add the following information:
      i. **Name:** verisign
      ii. Select “verisign.sh” from the pull-down list on **Execute Script**.
      iii. Add “10” on **Execute Script Timeout**.
d. Click **Apply** icon.

![Image of DDoS violation action with script]

**Figure 18: DDoS violation action with script**

3. Apply the countermeasure and violation action on the mitigation levels of the DDoS DST zone object (Z1V).
   a. Navigate to **DDoS Protection > Protected Objects > Zones**.
   b. Click **Edit** icon of the “Z1V” zone.
   c. Configure Level 1 with TCP zone-template.
      i. Move to **Service Port** tab and expand **Details**.
      ii. Move to **Level 1** on **Configure Protection Level**.
      iii. Check **Protection Level 1**.
      iv. Select “tcp-l1” from pull-down list on **TCP** template box.
   d. Configure Level 2 with TCP zone-template
      i. Move to **Level 2** tab on **Configure Protection Level**.
      ii. Check **Protection Level 2**.
      iii. Select “tcp-l2” from pull-down list on **TCP** template box.
   e. Configure static threshold and violation action on level 2.
      i. On **Indicator** row, click “+” icon.
      ii. Select “Pkt-rate” from pull-down list on **Indicator**.
      iii. Add “500” as **Threshold Per Zone**.
      iv. Select “verisign” on **Violation Action**.
      v. (Optional) Add “20” as **Score** of Pkt-rate indicator.
      vi. (Optional) On **Escalation Score** section, add “21” as **Zone** Escalation Score.

   **Note**: Scoring setting/operation is optional and can be used with higher escalation levels (i.e., 3). All indicators have a score of 1 by default when traffic exceeds the threshold. In this example, if traffic exceeded pkt-rate 500 pps, the violation action (script execution) is initiated and the score becomes 20. If any other indicator threshold (auto learned) is exceeded, the score increases 1, resulting in a total score of 21. Then, all traffic in this zone will be escalated to the next level, if configured.

   f. Click **Update** icon at the bottom of this page to save the configuration changes.
**CLI Configuration**

```bash
! ddos violation-actions verisign
  execute-script verisign.sh
execute-script-timeout 10
!
ddos zone-template tcp tcp-l1
  syn-authentication retransmit-check min-delay 10
  syn-authentication fail-action blacklist-src
!
ddos zone-template tcp tcp-l2
  out-of-seq 64 action blacklist-src
  zero-win 24 action blacklist-src
  syn-authentication send-rst
  syn-authentication pass-action authenticate-src
  syn-authentication fail-action blacklist-src
  ack-authentication retransmit-check timeout 15
  ack-authentication retransmit-check min-delay 10
  ack-authentication pass-action authenticate-src
  ack-authentication fail-action reset
!
ddos dst zone Z1V
  ip 192.168.9.113
  description example.com-192.168.9.113
  zone-profile ZP-Z1V
  operational-mode monitor
  log enable periodic
  ip-proto tcp
  ip-proto udp
  ip-proto icmp-v4
    detection-enable
  port 80 http
    detection-enable
```
level 0
level 1
  zone-template tcp tcp-l1
level 2
  zone-escalation-score 21
  zone-template tcp tcp-l2
  indicator pkt-rate
  score 20
  zone-threshold 500
  zone-violation-actions verisign

Proof of Concept for Hybrid DDoS Protection Solution
This section shows the result of the hybrid DDoS protection solution, including the Verisign portal view of a DDoS attack violating the DDoS protection rules configured on Thunder TPS.

This POC was tested with a SYN flood attack while simulated normal traffic was passing through the Thunder TPS without any interruption.

Log and Report on Thunder TPS

Figure 20: Thunder TPS – DDoS detection log
The Incidents page under Dashboard shows status and events regarding defined DDoS protected objects. In this example, an incident has been created automatically when Thunder TPS detected a violation due to a SYN flood attack.

Figure 21: Thunder TPS – Dashboard Incidents
The Monitoring page shows detailed traffic information, statistics and indicators for each application port (service port) under the zone. In the Charts pane, the detected DDoS event is marked with a red square as seen in Figure 22.
Verisign Portal View

On the Verisign portal, you see one new alert on the Dashboard page that was signaled by Thunder TPS (A10source2) using the script.

![Figure 23: Verisign portal – Dashboard](image)

On the Alert page, you can see more details regarding the DDoS attack event.

![Figure 24: Verisign portal – Alert view](image)

![Figure 25: Verisign portal – Alert view details](image)
Summary
This deployment guide provides step-by-step configuration for a joint hybrid DDoS solution consisting of an on-premise DDoS protection device from A10 Networks and a cloud-based DDoS protection service from Verisign. Thunder TPS is deployed as the on-premise DDoS protection device, providing full-time DDoS detection and mitigation against any type of attack traffic, including multi-vector attacks, which include network layer (L3/L4) attacks and sophisticated application layer (L7) attacks. In addition, Thunder TPS is used as a detector for volumetric DDoS attacks that could overwhelm an organization's Internet uplink capacity. In such a case, Thunder TPS can signal DDoS attack information to the Verisign DDoS Protection Service to activate cloud-based DDoS protection. With this deployment, users can be assured of a comprehensive and agile DDoS protection solution that detects and mitigates DDoS attacks quickly and effectively.

Appendix
Here is the sample configuration of Thunder TPS used for this deployment guide.

Thunder TPS Configuration

```
! monitor buffer-usage 91750
! multi-config enable
! system anomaly log
system attack log
system ddos-attack log
! terminal idle-timeout 0
! ip dns primary 8.8.8.8
! hostname TH3030S-TPS
! interface management
   ip address 10.100.9.155 255.255.255.0
   ip default-gateway 10.100.9.1
!
interface ethernet 1
name To_RT-A
ddos outside
   enable
   ip address 192.168.0.155 255.255.255.0
!
interface ethernet 2
name To_RT-B
ddos outside
   enable
   ip address 192.168.1.155 255.255.255.0
!
interface ethernet 3
name Internet_access
   enable
   ip address 10.100.10.155 255.255.255.0
!
```
interface ethernet 4
!
interface ethernet 5
  enable
!
interface ethernet 6
  enable
!
interface ethernet 7
!
interface ethernet 8
!
interface ethernet 9
!
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
!
ip route 0.0.0.0 /0 10.100.10.1
!
ip route 192.168.9.0 /24 192.168.1.114
!
ip route 203.0.113.0 /24 192.168.0.119
!
ddos protection enable
!
ddos zone-template tcp tcp-l1
  syn-authentication retransmit-check min-delay 10
  syn-authentication fail-action blacklist-src
!
ddos zone-template tcp tcp-l2
  out-of-seq 64 action blacklist-src
  zero-win 24 action blacklist-src
  syn-authentication send-rst
  syn-authentication pass-action authenticate-src
  syn-authentication fail-action blacklist-src
  ack-authentication retransmit-check timeout 15
  ack-authentication retransmit-check min-delay 10
  ack-authentication pass-action authenticate-src
  ack-authentication fail-action reset
!
!
ddos violation-actions verisign
  execute-script verisign.sh
  execute-script-timeout 10
!
ddos zone-profile ZP-Z1V
  port 80 http
    indicator pkt-rate
src-threshold 108
zone-threshold 198
indicator syn-rate
  src-threshold 9
  zone-threshold 16
indicator fin-rate
  src-threshold 9
  zone-threshold 16
indicator rst-rate
  src-threshold 0
  zone-threshold 0
indicator small-window-ack-rate
  src-threshold 0
  zone-threshold 0
indicator empty-ack-rate
  src-threshold 81
  zone-threshold 148
indicator small-payload-rate
  src-threshold 9
  zone-threshold 16
indicator bytes-to-bytes-from-ratio
  src-threshold 0.00
  zone-threshold 0.00
indicator syn-fin-ratio
  src-threshold 1.50
  zone-threshold 1.11
indicator conn-miss-rate
  src-threshold 9
  zone-threshold 16
indicator pkt-drop-rate
  src-threshold 0
  zone-threshold 0
indicator pkt-drop-ratio
  src-threshold 0.00
  zone-threshold 0.00
indicator concurrent-conns
  src-threshold 18
  zone-threshold 33
ip-proto icmp-v4
indicator pkt-rate
  src-threshold 0
  zone-threshold 0
indicator pkt-drop-rate
  src-threshold 0
  zone-threshold 0
indicator frag-rate
  src-threshold 0
  zone-threshold 0
indicator pkt-drop-ratio
  src-threshold 0.00
  zone-threshold 0.00
indicator bytes-to-bytes-from-ratio
  src-threshold 0.00
  zone-threshold 0.00
Deployment Guide | A10 Thunder TPS Hybrid DDoS Protection Deployment with Verisign OpenHybrid

! ddos src default ipv6
! ddos dst default ip
  14-type icmp
  14-type other
  14-type tcp
    drop-on-no-port-match disable
  14-type udp
    drop-on-no-port-match disable
! ddos dst default ipv6
!
!

ddos dst zone Z1V
  ip 192.168.9.113
  description example.com-192.168.9.113
  zone-profile ZP-Z1V
  operational-mode monitor
  log enable periodic
  ip-proto tcp
  ip-proto udp
  ip-proto icmp-v4
    detection-enable
  port 80 http
    detection-enable
    level 0
    level 1
      zone-template tcp tcp-l1
    level 2
      zone-escalation-score 21
      zone-template tcp tcp-l2
      indicator pkt-rate
        score 20
        zone-threshold 500
        zone-violation-actions verisign

! end

DDoS Script for Verisign Solution
#!/bin/sh
# Copyright 2015, A10 Networks.
# Thunder TPS DDoS script for Verisign DDoS Cloud Service
# Version 1.0 - 12.01.2015
#
### 1. REPLACE “API_Key” VALUE WITH YOURS PROVIDED BY VERISIGN ###
### 2. UPDATE ‘source_id’ WITH PROPER SIGNAL SOURCE DEVICE ID   ###
###          NOTE: MAKE SURE TO USE UNIX EOL FORMAT             ###
#
API_Key="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
curl -k -i -X POST https://<Verisign OpenHybrid URL> -H "Authorization: AMP
$API_Key" -d \n  
  ‘source_id’ : ‘A10Source2’, \n  ‘alert_type’ : ‘$DDOS_ALERT_TYPE $DDOS_THRESHOLD’, \n  ‘..."
About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com