DEPLOYMENT GUIDE

EXPEDITE PROACTIVE DDOS PROTECTION DEPLOYMENT USING A10 AGALAXY SYSTEM

Configure, monitor and manage DDoS protection in asymmetric proactive mode using aGalaxy

OVERVIEW

Organizations are increasingly dependent on the availability of their services and their ability to connect to the Internet. Downtime results in immediate revenue loss. One of the largest persistent threats to service uptime is Distributed Denial of Service Attacks (DDoS). The networking industry and business analysts are seeing a trend in increasing DDoS attacks.

These attacks are occurring more frequently and with greater intensity and increased sophistication. Legacy DDoS protection solutions suffer from the following fatal limitations that have made them ineffective at protecting against these attacks:

- Lack of flexibility
- Inability to scale

A10 Networks A10 Thunder® Threat Protection System (TPS) has been designed from the ground up to address these problems and protect services and connectivity from the next generation of threats.

A10 aGalaxy management system provides centralized management, orchestration, monitoring, alerting, reporting and detecting of DDoS attacks and defenses.

This Deployment Guide focuses on using A10 aGalaxy management system to expedite the deployment of proactive DDoS protection on Thunder TPS system.

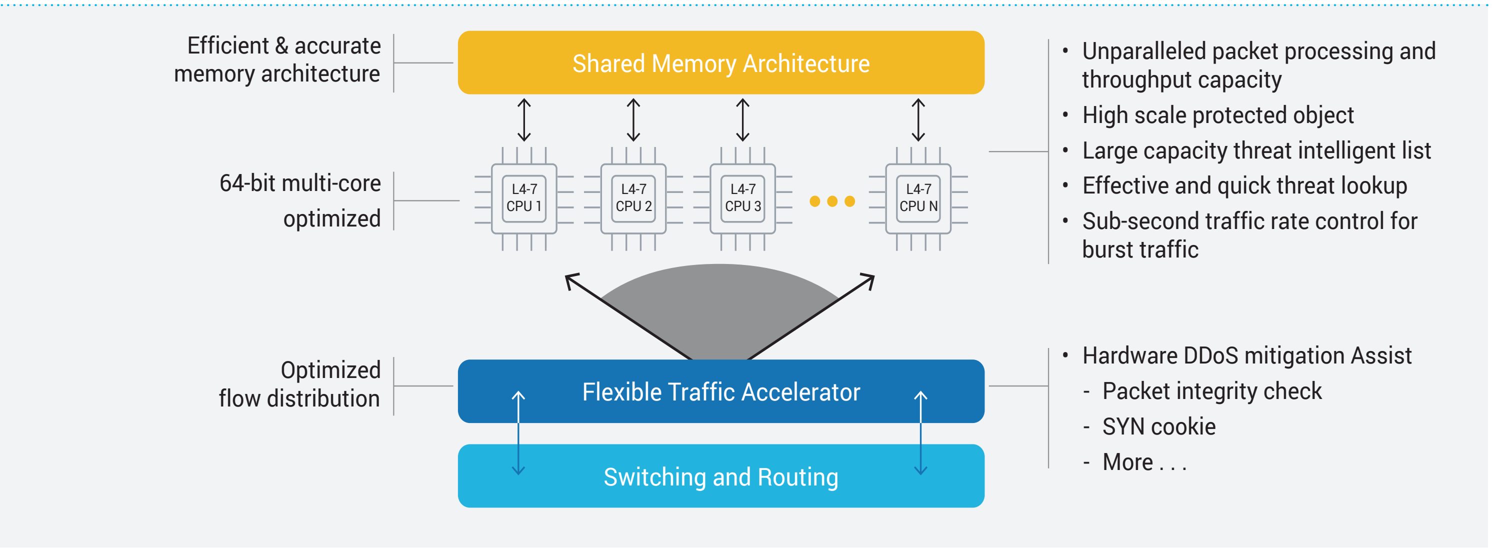
TABLE OF CONTENTS

SOLUTION

A10 Thunder TPS product line provides high-performance, network-wide protection from DDoS attacks and maintains service availability against a variety of volumetric, protocol, resource, and other sophisticated application attacks by offering flexible deployment options.

- Multi-vector application & network protection
  - Detect and mitigate application and network attacks
  - Flexible scripting and deep packet inspection (DPI) for rapid response
- High performance mitigation
  - Mitigate maximum 155 Gbps of attack throughput
  - Mitigate maximum 200 million packets per second
- Broad deployment options
  - Symmetric, Asymmetric, Out-of-Band (TAP) deployment options
    - Routed (L3), Transparent (L2) modes
    - BGP, Tunneling protocols (GRE and IP-in-IP) and else
- Open SDK / RESTful API (aXAPI) for third party integration

The Thunder TPS product line is built on the Advanced Core Operating System (ACOS®) platform, with A10's Symmetric Scalable Multi-Core Processing (SSMP) software architecture. This architecture delivers high performance and leverages a shared-memory architecture to allow the efficient tracking of network flows and accurate DDoS protection enforcement for service providers, web site operators, and enterprises.



Efficient & accurate memory architecture
Shared Memory Architecture
64-bit multi-core optimized
L4-7 CPU 1
L4-7 CPU 2
L4-7 CPU 3
L4-7 CPU N
Optimized flow distribution
Flexible Traffic Accelerator
Switching and Routing
• Unparalleled packet processing and throughput capacity
• High scale protected object
• Large capacity threat intelligent list
• Effective and quick threat lookup
• Sub-second traffic rate control for burst traffic
• Hardware DDoS mitigation Assist
- Packet integrity check
- SYN cookie
- More . . .

Figure 1: A10 Networks ACOS architecture

The A10 aGalaxy management system provides centralized management of Thunder TPS systems and policies, orchestrates detection and mitigation of DDoS attacks, and delivers a single-pane-of-glass view of the generated reports across all managed Thunder TPS appliances.

- Real-time DDOS Defense Management System
- Stops DDoS Attacks
- Simplify Management
- Automated Detection and Mitigation
- Automatic Service Discovery with Detection 2.0
- Maximize IT Agility
- Report on Attacks and Network Activity
- RESTful API (aGAPI) for third-party integration

The A10 aGalaxy management system also offers built-in default Zone Protection Profiles, Zone Templates and Operational Policies to expedite the deployment of DDoS protection, especially in service provider environments, and serve as the reference points for customizing new protection configuration based on various DDoS protection strategies. This deployment guide uses asymmetric proactive deployment mode as an example to show the configuration procedure and validation process via A10 aGalaxy system. Similar procedure and process can be applied to other DDoS protection deployment modes.

DEPLOYMENT PREREQUISITES

To expedite the deployment of proactive DDoS protection on A10 Thunder TPS system using A10 aGalaxy management system, you need the following:

- Thunder TPS 1040, 3040, 4435, 5845, 7445 or 14045, and its license
- ACOS TPS release 3.2.4-TPS-P1 or higher
- aGalaxy for TPS release 5.0.2 or higher, and its license
- Management Network connectivity between Thunder TPS and aGalaxy systems
- sFlow Control Network connectivity between Thunder TPS and aGalaxy systems
- Data Network connectivity among Thunder TPS system, clients (simulating DDoS attackers) and servers (simulating DDoS targets)

DEPLOYMENT MODE

The asymmetric deployment topology that is addressed in this deployment guide dictates the Thunder TPS system is always in the data path (Proactive) and monitoring only the client-to-server direction of traffic (Asymmetric).

This deployment guide provides comprehensive information about the topology and the mode.

ASYMMETRIC PROACTIVE MODE

OVERVIEW

In Asymmetric Proactive Mode, inbound traffic is always diverted along the “modified” path while the return traffic follows the “native” path. With this deployment mode, a DDoS detection system is optional in the network because the Thunder TPS system has an insight into all the inbound traffic. However, integration with DDoS detection system may be beneficial since it can cover other area of network in large network and/or real-time threshold tuning via SDK/API.

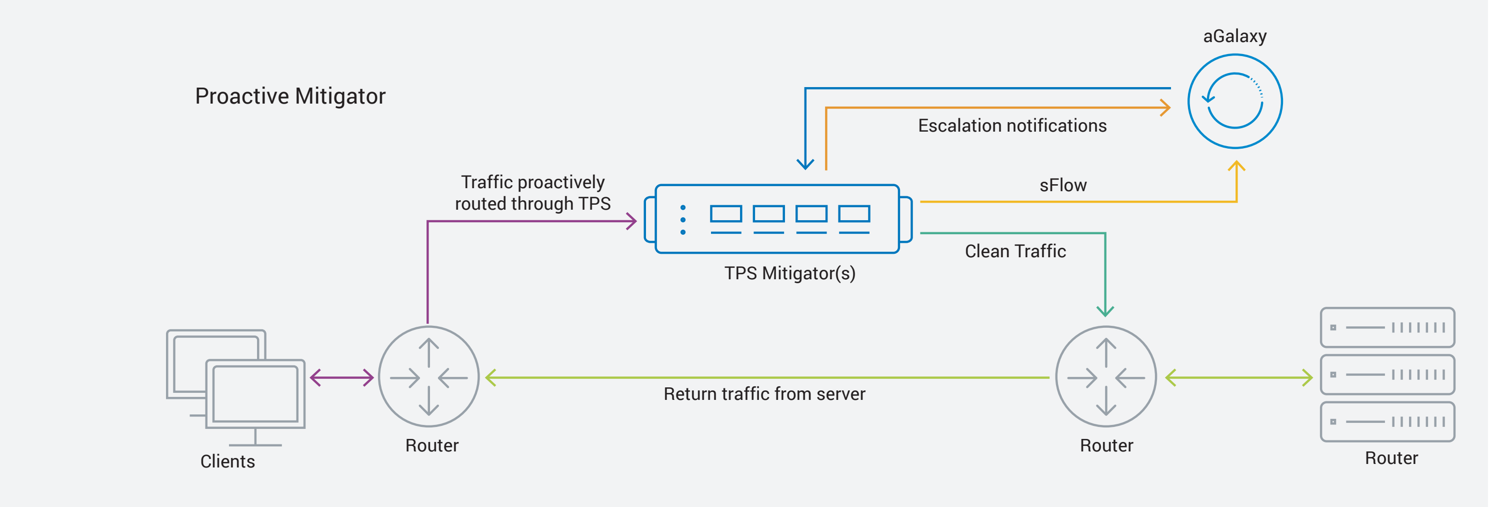


Figure 2: Asymmetric Proactive Mode

Initial Setup at Thunder TPS system (DDoS Mitigator)

- Management Network
- sFlow Control Network
- Data Network
- DDoS Protection
- DDoS Pattern Recognitio

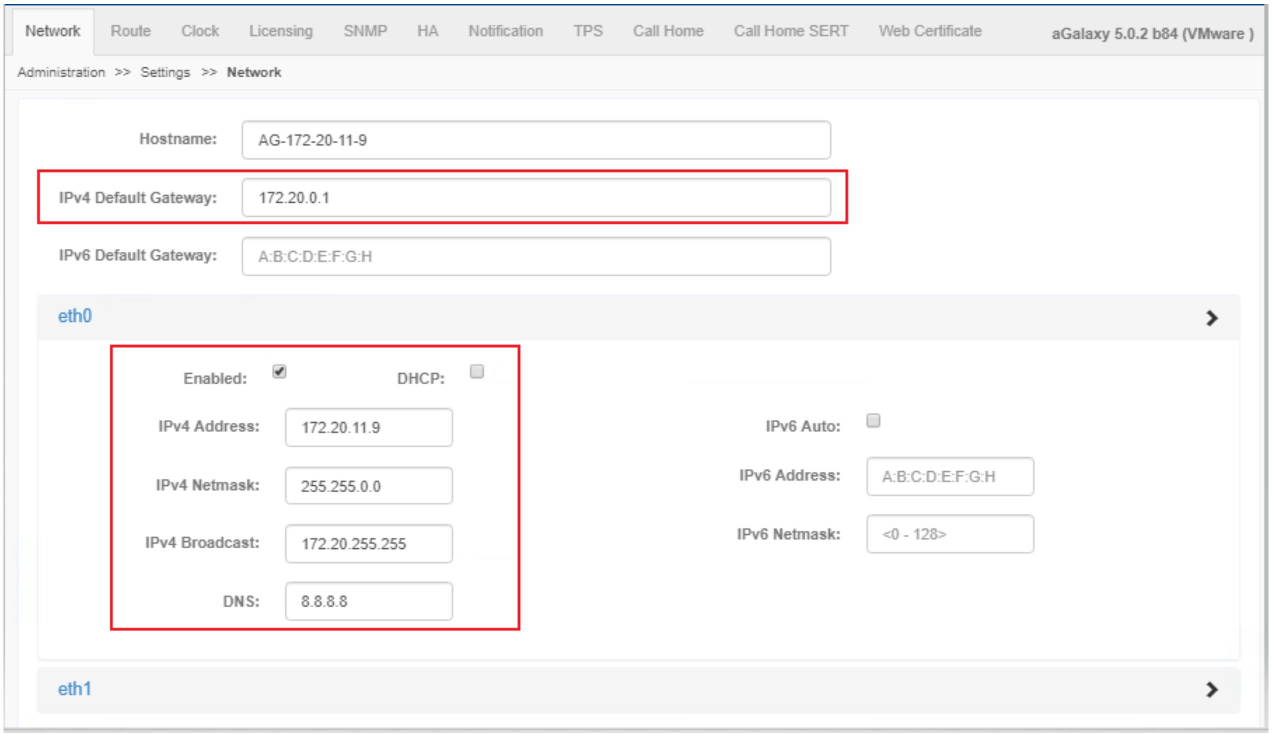
```
interface management
  ip address 172.20.11.2 255.255.0.0
  ip default-gateway 172.20.0.1
interface ethernet 1
  name to_ExtRT_clients
  ip address 192.168.20.2 255.255.255.0
interface ethernet 2
  name to_IntRT_servers
  ip address 192.168.30.2 255.255.255.0
```

```
interface ethernet 5
  name to_xFlowNW
  ip address 192.168.255.2 255.255.255.0

ddos protection enable
ddos protection rate-interval 1sec

ddos pattern-recognition dedicated-cpus 2
ddos pattern-recognition enable
```

Initial Setup at aGalaxy system (DDoS Management System)

Review and update the Network configuration via aGalaxy portal, if required, and confirm the Thunder TPS system has been added under the Device List and belongs a Device Group.

1. Login to aGalaxy and go to **Administration >> Settings >> Network** on the dropdown menu. The Network page displays Hostname, Default Gateway and eth0 and eth1 network interface configurations of aGalaxy.
   Ensure aGalaxy can reach the Thunder TPS system via both eth0 (Management Network) and eth1 (sFlow Control Network) interfaces.



Hostname: AG-172-20-11-9

IPv4 Default Gateway: 172.20.0.1

IPv6 Default Gateway: A:B:C:D:E:F:G:H

eth0

Enabled: ☑ DHCP: □

IPv4 Address: 172.20.11.9

IPv4 Netmask: 255.255.0.0

IPv4 Broadcast: 172.20.255.255

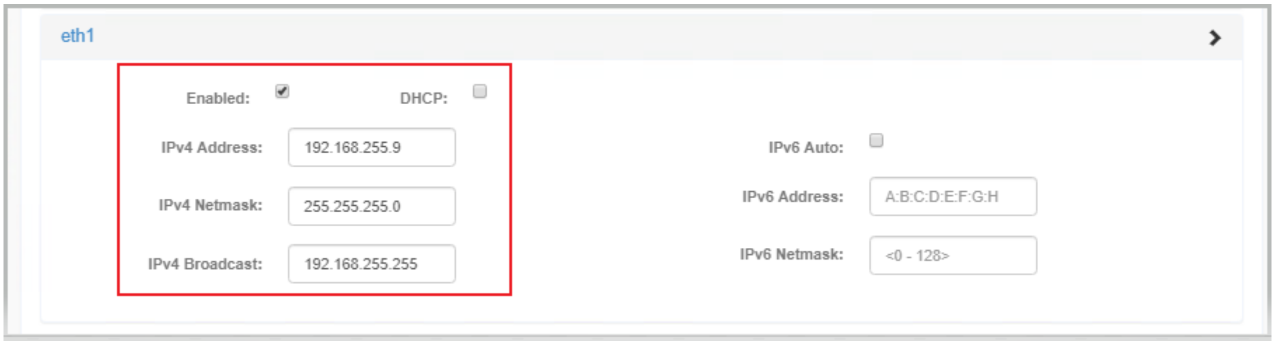
DNS: 8.8.8.8

IPv6 Auto: □

IPv6 Address: A:B:C:D:E:F:G:H

IPv6 Netmask: <0 - 128>

eth1



eth1

Enabled: ☑ DHCP: □

IPv4 Address: 192.168.255.9

IPv4 Netmask: 255.255.255.0

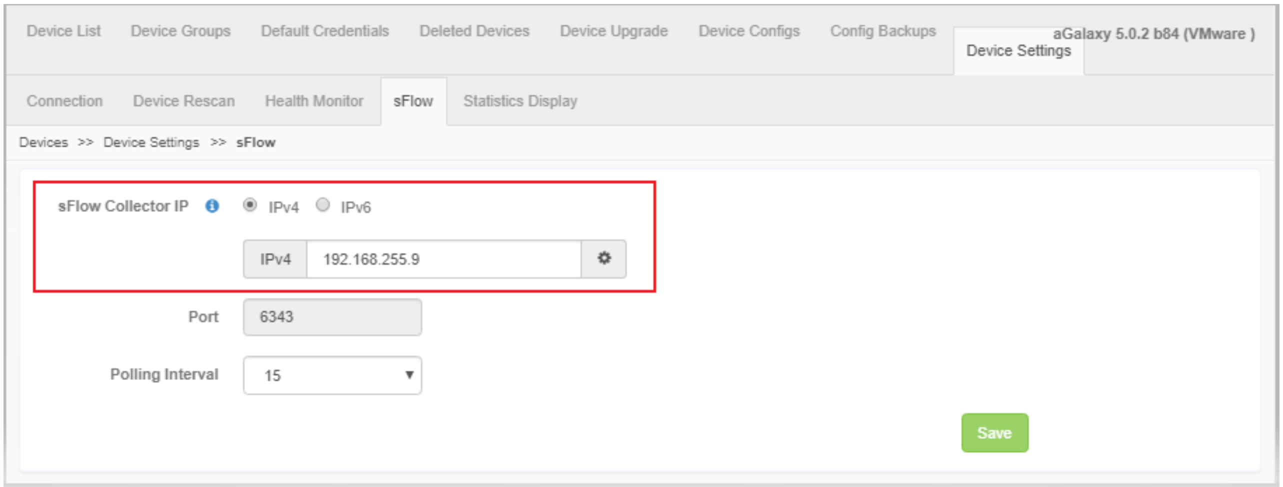
IPv4 Broadcast: 192.168.255.255

IPv6 Auto: □

IPv6 Address: A:B:C:D:E:F:G:H

IPv6 Netmask: <0 - 128>

2. Navigate to **Devices >> Device Settings >> sFlow** page, pick the IP address of eth1 as the sFlow Collector IP to receive random sampling packets and statistics in sFlow datagrams from managed devices for analysis.



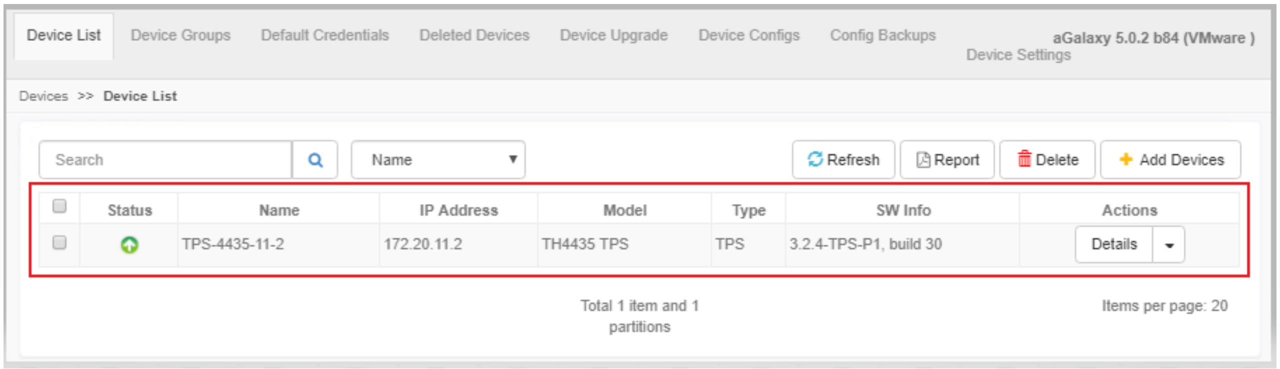
sFlow Collector IP ● IPv4 ○ IPv6

IPv4 192.168.255.9

Port 6343

Polling Interval 15

3. Go to **Devices >> Device List** on the dropdown menu. The **Device List** page displays the list of ACOS devices that are currently managed by aGalaxy. Use **Add Devices** to add the target Thunder TPS system to the list and ensure its **Status** shows as Up.

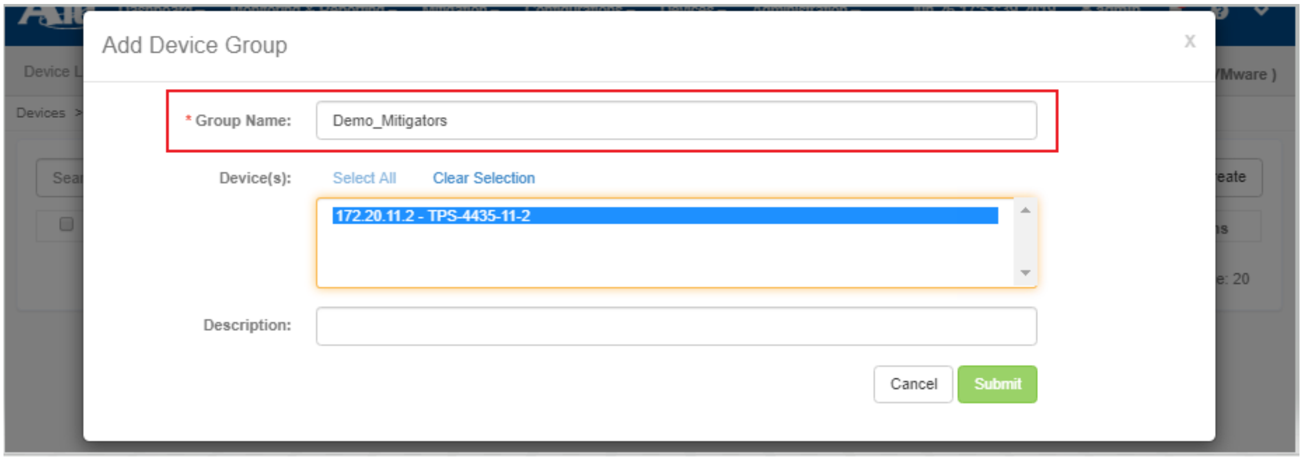


□	Status	Name	IP Address	Model	Type	SW Info	Actions
□	⬆	TPS-4435-11-2	172.20.11.2	TH4435 TPS	TPS	3.2.4-TPS-P1, build 30	Details ▾

Total 1 item and 1 partitions

Items per page: 20

4. From the **Devices >> Device Groups** page, create a device group, *Demo_Mitigators* as an example, and add the Thunder TPS system. AGalaxy identifies the device(s) that acts as mitigators through Device Groups and applies the Protected Zone configuration via a Device Group.



* Group Name: Demo_Mitigators

Device(s): 172.20.11.2 - TPS-4435-11-2

Description:

5. Follow the same steps to add more Thunder TPS systems and Device Groups to the list.

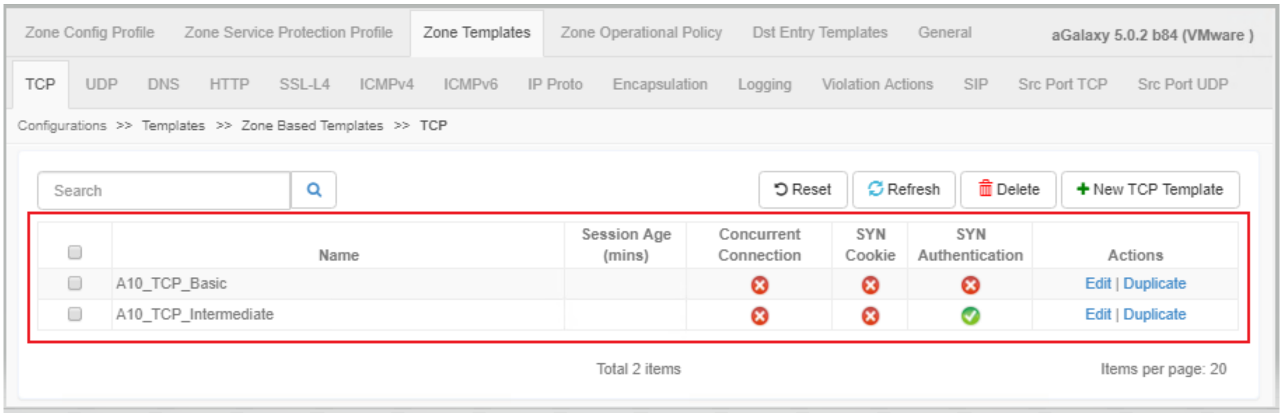
INITIAL PROTECTED ZONE CONFIGURATION AT AGALAXY SYSTEM

Using built-in default Zone Templates and Zone Operation Policy

Review the built-in default Zone Templates and Policies at aGalaxy and add other new templates to customize the mitigation options of the protocol if applicable.

1. Go to **Configurations >> Templates >> Zone Templates** on the dropdown menu. These TCP and UDP etc. Zone Templates pages displays the list of built-in *A10_TCP and A10_UDP* templates. Click **Edit** next to each zone template to review its pre-defined configuration of mitigation and countermeasure options.

__NOTE__: These default zone templates do not allow any modification; use __Duplicate__ to customize a similar one.

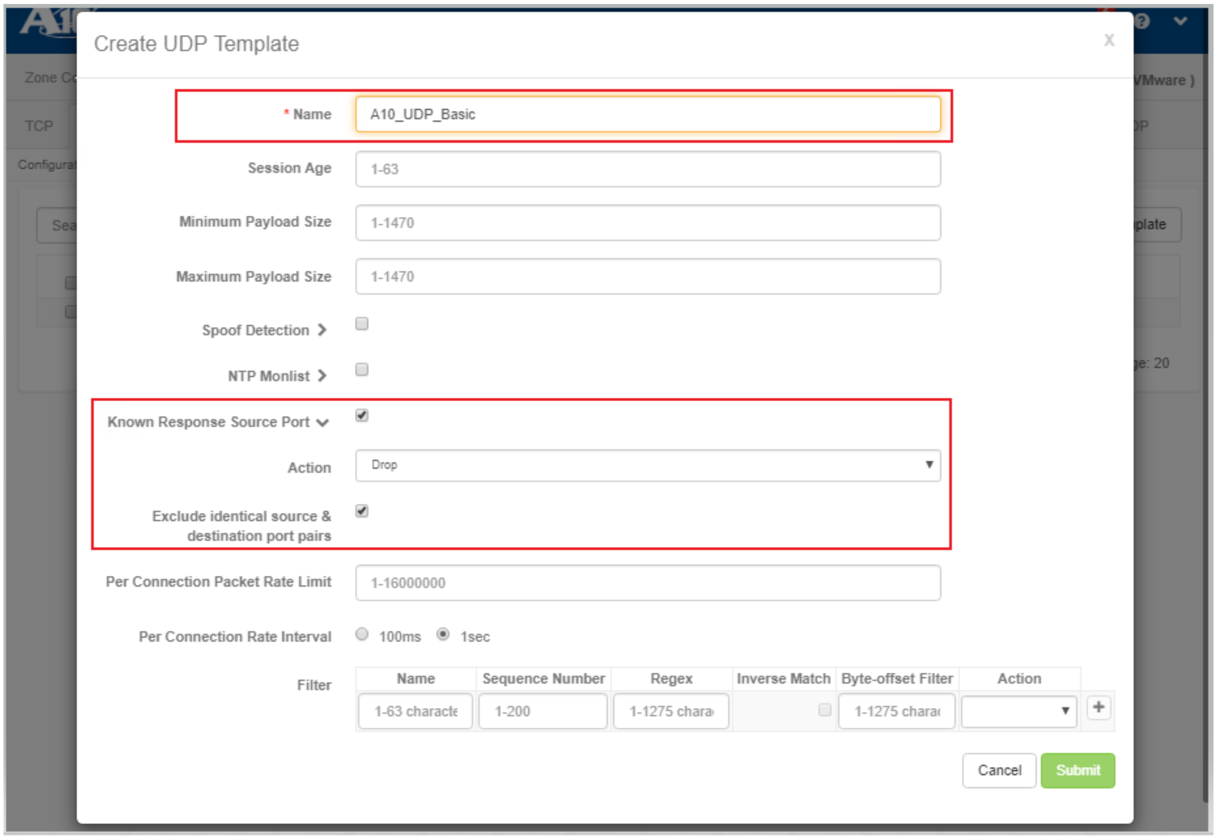


□	Name	Session Age (mins)	Concurrent Connection	SYN Cookie	SYN Authentication	Actions
□	A10_TCP_Basic		☒	☒	☒	Edit | Duplicate
□	A10_TCP_Intermediate		☒	☒	✓	Edit | Duplicate

Total 2 items

Items per page: 20

2. Consider using **Duplicate** or **New Template** to customize a new template, *A10_UDP_Basic* as an example; select Know Response Source Port and Exclude identical source & destination port pairs as its mitigation options.


Create UDP Template

* Name: A10_UDP_Basic

Session Age: 1-63

Minimum Payload Size: 1-1470

Maximum Payload Size: 1-1470

Spoof Detection: □

NTP Monlist: □

Known Response Source Port: ☑

Action: Drop

Exclude identical source & destination port pairs: ☑

Per Connection Packet Rate Limit: 1-16000000

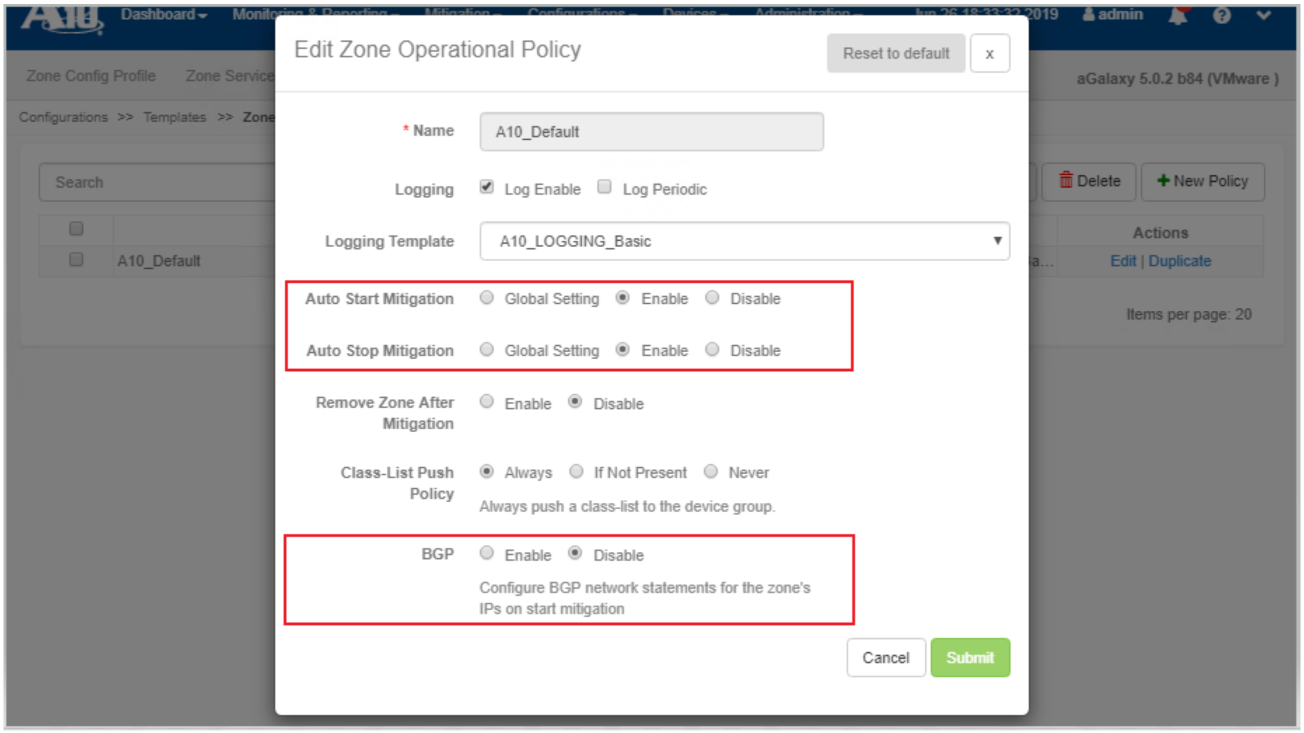
Per Connection Rate Interval: ○ 100ms ● 1sec

Filter:

Name	Sequence Number	Regex	Inverse Match	Byte-offset Filter	Action
1-63 characte	1-200	1-1275 chara	□	1-1275 charac	

3. Follow the same step to create other new Zone Templates.

4. Go to **Configurations >> Templates >> Zone Operational Policy** on the dropdown menu. Click **Edit** next to the built-in *A10_Default* policy to review its pre-defined configuration of logging, mitigation, class-list and BGP options. **Edit** or **Duplicate** at this built-in *A10_Default* policy to enable Auto Start Mitigation, Auto Stop Mitigation; and disable BGP statement for this Proactive DDoS Protection deployment.



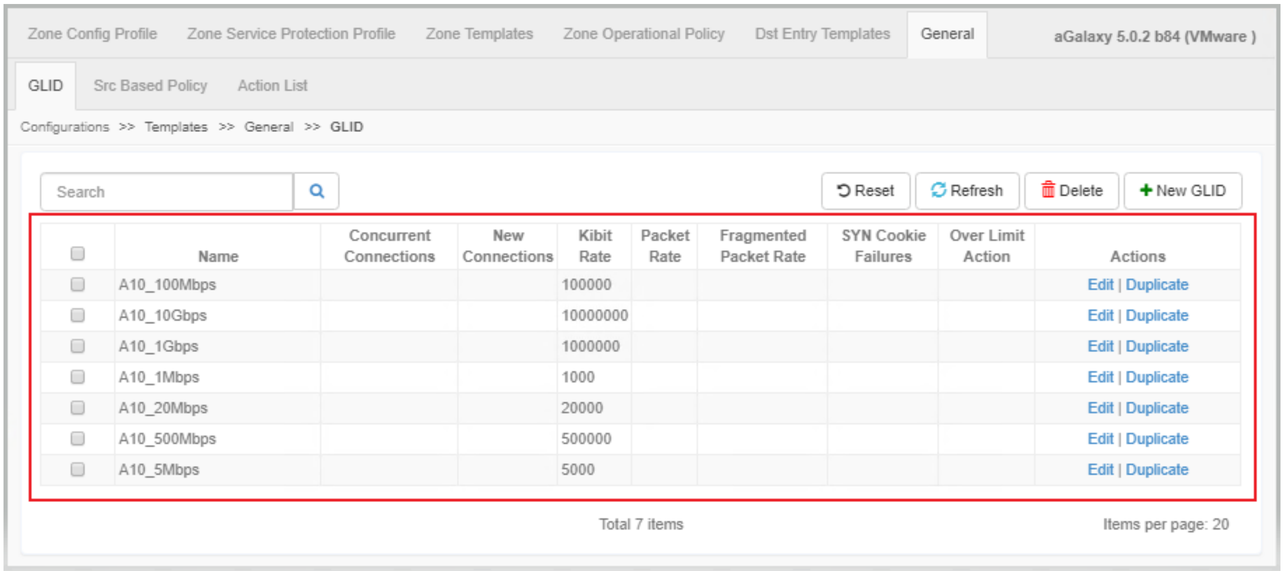
Edit Zone Operational Policy

* Name	A10_Default
Logging	☑ Log Enable □ Log Periodic
Logging Template	A10_LOGGING_Basic
Auto Start Mitigation	○ Global Setting ● Enable ○ Disable
Auto Stop Mitigation	○ Global Setting ● Enable ○ Disable
Remove Zone After Mitigation	○ Enable ● Disable
Class-List Push Policy	● Always ○ If Not Present ○ Never Always push a class-list to the device group.
BGP	○ Enable ● Disable Configure BGP network statements for the zone's IPs on start mitigation

5. Use **Duplicate** or **New Policy** to customize new Zone Operational Policy and others.

6. Go to **Configurations >> Templates >> General** on the dropdown menu. The **GLID** page displays the list of built-in GLID rate limiting rules. Click **Edit** next to each GLID to review its pre-defined rate limiting rules.

*NOTE: These default GLID rules do not allow any modification; use **Duplicate** to customize a similar one.*

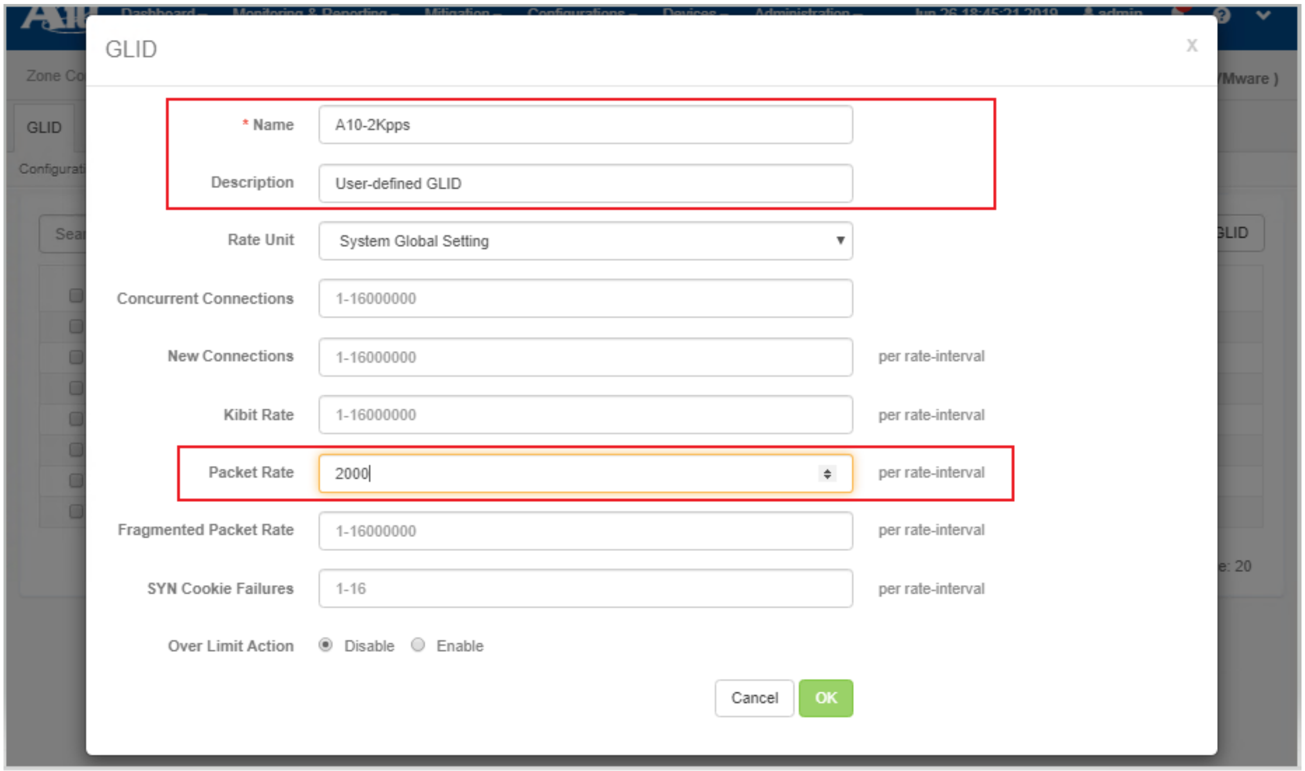


□	Name	Concurrent Connections	New Connections	Kibit Rate	Packet Rate	Fragmented Packet Rate	SYN Cookie Failures	Over Limit Action	Actions
□	A10_100Mbps			100000					Edit | Duplicate
□	A10_10Gbps			10000000					Edit | Duplicate
□	A10_1Gbps			1000000					Edit | Duplicate
□	A10_1Mbps			1000					Edit | Duplicate
□	A10_20Mbps			20000					Edit | Duplicate
□	A10_500Mbps			500000					Edit | Duplicate
□	A10_5Mbps			5000					Edit | Duplicate

Total 7 items

Items per page: 20

7. Consider using **Duplicate** or **New GLID** to customize a new GLID, *A10-2Kpps* as an example; set *2000* per rate-interval at its rate-limit packet rate.



GLID

* Name	A10-2Kpps	
Description	User-defined GLID	
Rate Unit	System Global Setting ▾	
Concurrent Connections	1-16000000	
New Connections	1-16000000	per rate-interval
Kibit Rate	1-16000000	per rate-interval
Packet Rate	2000	per rate-interval
Fragmented Packet Rate	1-16000000	per rate-interval
SYN Cookie Failures	1-16	per rate-interval
Over Limit Action	● Disable ○ Enable	

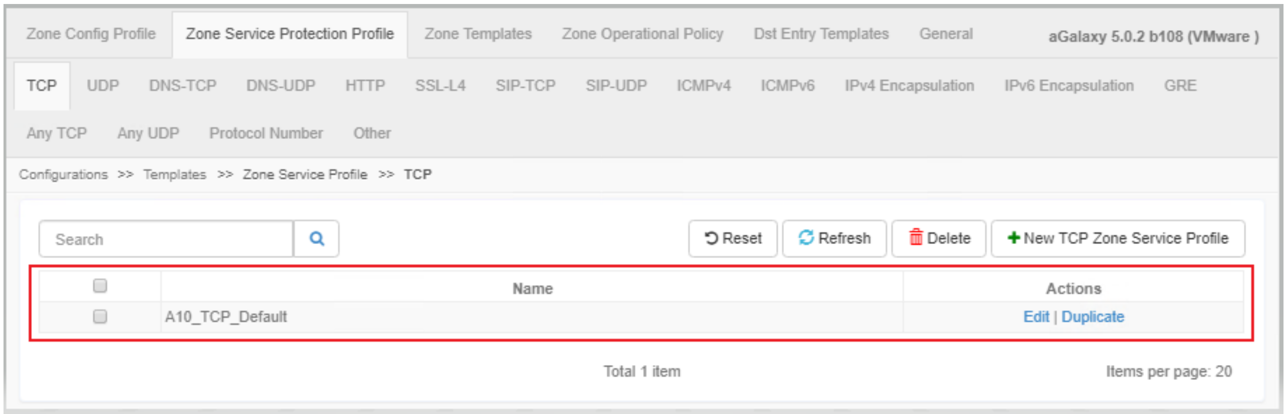
8. Follow the same step to create other new GLID rate-limit rules.

Using built-in default Zone Service Protection Profiles

Review the built-in default Zone Service Protection Profiles at aGalaxy and add other new protection profiles to customize the protection configuration of the protocol if applicable.

1. Go to **Configurations >> Templates >> Zone Service Protection Profile** on the dropdown menu. These TCP and UDP etc. Zone Service Protection Profile pages displays the list of built-in *A10_TCP* and *A10_UDP* profiles. Click **Edit** next to each zone protection profile to review its pre-defined protection configuration.

   NOTE: These default protection profiles do not allow any modification; use ***Duplicate*** to customize a similar one.
   NOTE: These default protection profiles are available from aGalaxy release 5.0.2 b104 release or higher.

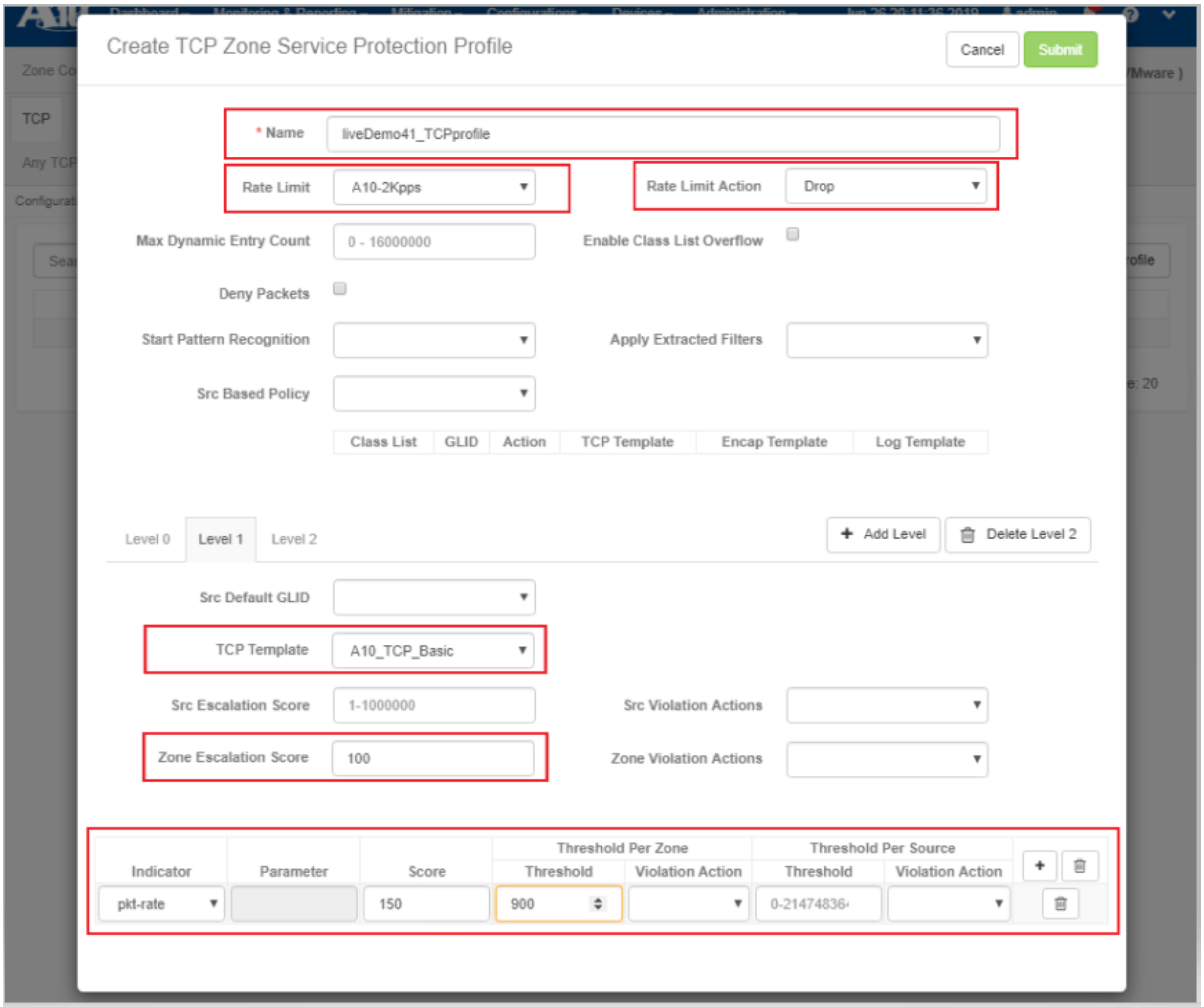


Configurations >> Templates >> Zone Service Profile >> TCP

□	Name	Actions
□	A10_TCP_Default	Edit | Duplicate

Total 1 item   Items per page: 20

2. Consider using **Duplicate** or **New Template** to customize a new zone protection profile, *liveDemo41_TCPprofile* as an example; use *A10-2Kpps* GLID (2000pps) as its packet rate limit and *Drop* as its rate limit action (violation action); at bottom Level 0, assign 100 as Zone Escalation Score and **add** *pkt-rate* indicator with *150* as its score and *900* as its Threshold Per Zone to trigger Level Escalation to Level 1 when the Thunder TPS system detects the live traffic of the protected TCP port is above 900 pps – adding score 150 which exceeds the Zone Escalation Score of 100; use **Add Level** to add *Level 1* and *Level 2* at the bottom; at Level 1, assign the same Zone Escalation Score and pkt-rate indicator as Level 0, and select *A10_TCP_Basic* template as TCP Template to apply its corresponding countermeasures when escalated; at Level 2, only select *A10_TCP_Intermediate* template as TCP Template to apply its corresponding countermeasures when escalated, but no Zone Escalation as Level 2 is the last zone escalation level of the protected TCP port.



Create TCP Zone Service Protection Profile

* Name	liveDemo41_TCPprofile		
Rate Limit	A10-2Kpps	Rate Limit Action	Drop
Max Dynamic Entry Count	0 - 16000000	Enable Class List Overflow	☐
Deny Packets	☐		
Start Pattern Recognition		Apply Extracted Filters	
Src Based Policy			

Class List	GLID	Action	TCP Template	Encap Template	Log Template

Level 0 | Level 1 | Level 2

Src Default GLID			
TCP Template	A10_TCP_Basic		
Src Escalation Score	1-1000000	Src Violation Actions	
Zone Escalation Score	100	Zone Violation Actions	

Indicator	Parameter	Score	Threshold Per Zone		Threshold Per Source	
			Threshold	Violation Action	Threshold	Violation Action
pkt-rate		150	900		0-21474836	

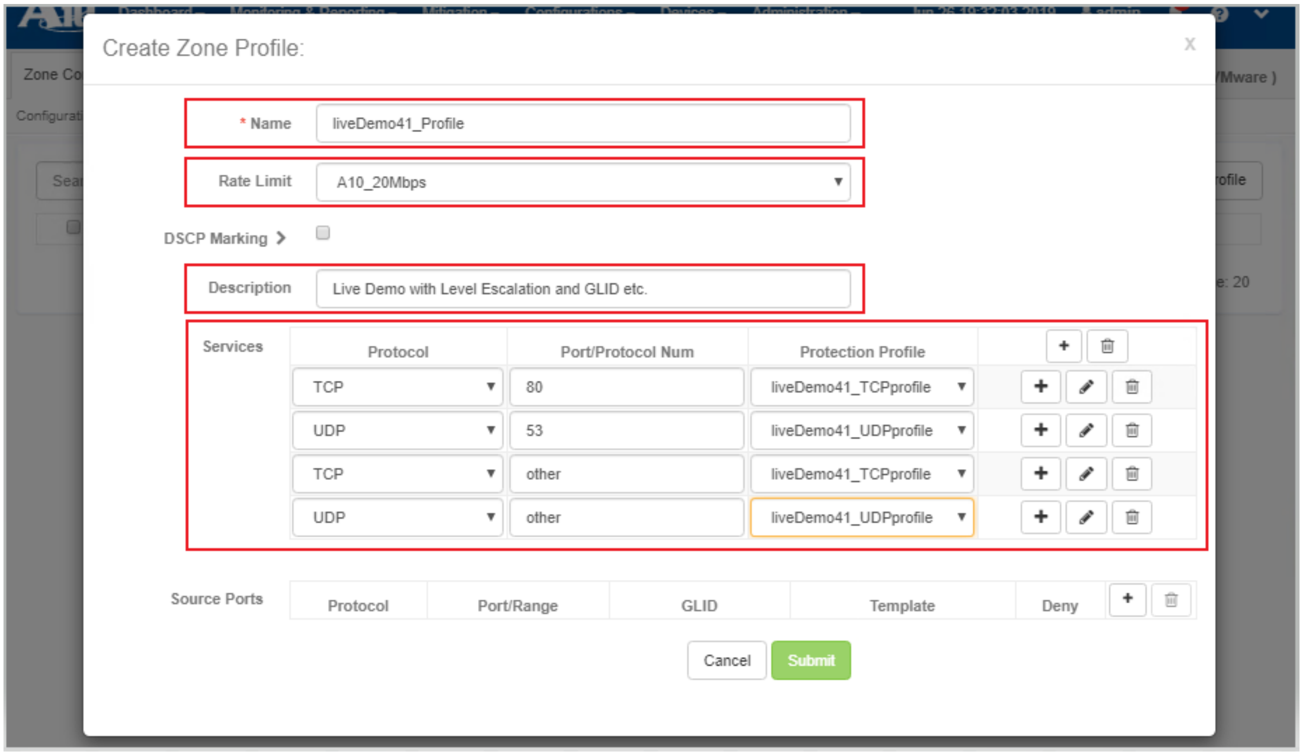
3. Follow the same step to create other new Service Protection Profile, *liveDemo41_UDPprofile* under UDP as an example.

CREATING ZONE CONFIG PROFILES FROM ZONE SERVICE PROTECTION PROFILES

New Zone Config Profiles

Create new Zone Config Profile to pre-select the service ports and corresponding DDoS protection configurations, such as TCP:80, UDP:53, TCP:other, and UDP:other, using newly created or built-in default TCP and UDP Zone Service Protection Profiles, to expedite new Protected Zone creation.

1. Go to **Configurations >> Templates >> Zone Config Profile** on the dropdown menu. Click **New Zone Profile** to create a new Zone Profile, *liveDemo41_Profile* as an example. At here, pick *A10_20Mbps GLID* (20Mbps) as its bandwidth rate limit for entire protected zone, and add *TCP:80, UDP:53, TCP:other*, and *UDP:other* as its protected services with corresponding liveDemo41_TCPprofile and liveDemo41_UDPprofile Zone Service Protection Profiles.



Create Zone Profile:

* Name: liveDemo41_Profile

Rate Limit: A10_20Mbps

DSCP Marking > □

Description: Live Demo with Level Escalation and GLID etc.

Services

Protocol	Port/Protocol Num	Protection Profile
TCP	80	liveDemo41_TCPprofile
UDP	53	liveDemo41_UDPprofile
TCP	other	liveDemo41_TCPprofile
UDP	other	liveDemo41_UDPprofile

Source Ports

Protocol	Port/Range	GLID	Template	Deny

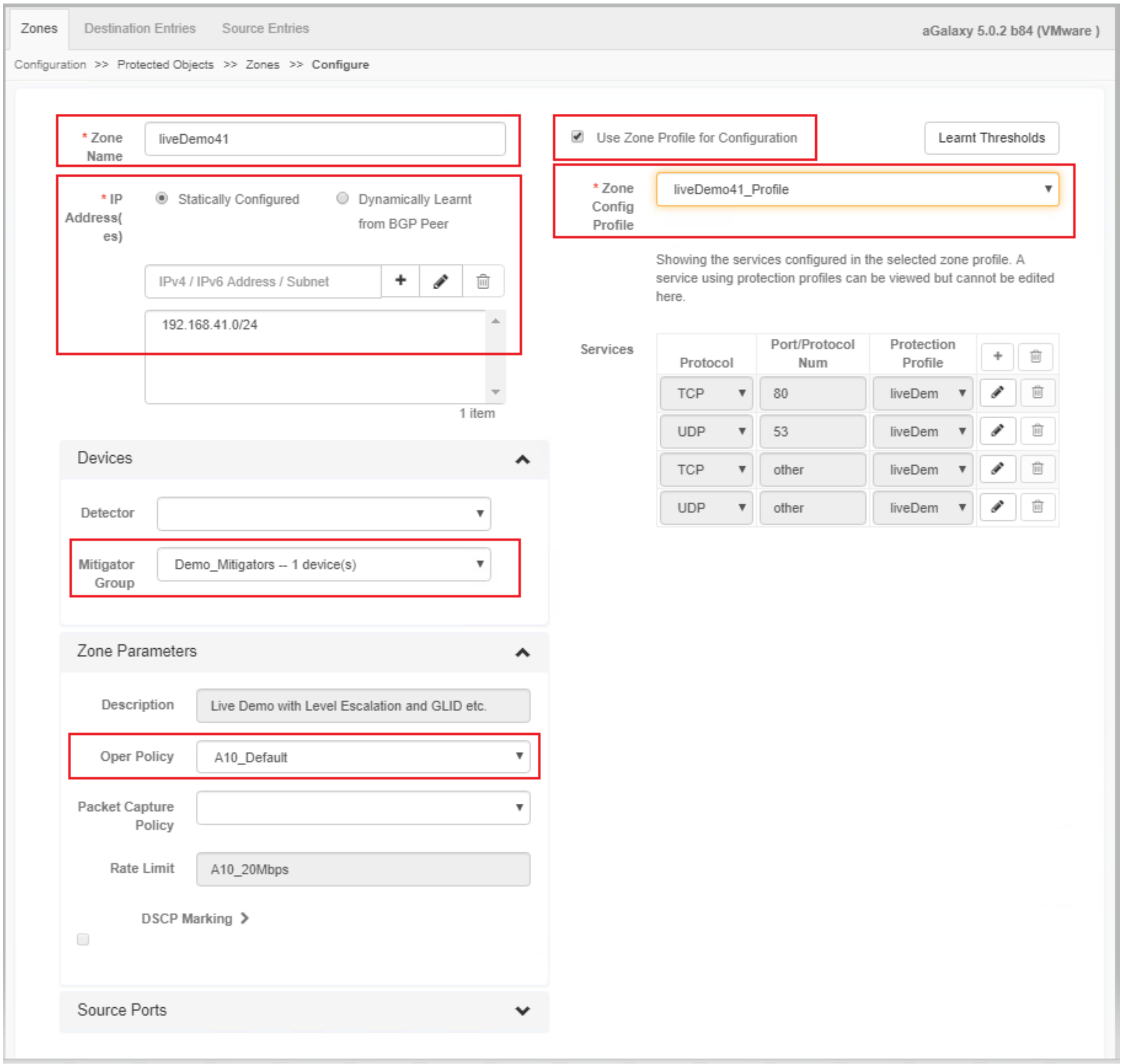
2. Follow the same step to create other new Zone Config Profiles, *liveDemo40_Proflle* as an example.

CREATING PROTECTED ZONE AND DEPLOYING DDOS PROTECTION TO THUNDER TPS SYSTEM IN MINUTES

New Protected Zone creation and deployment at aGalaxy

Create new Protected Zone from existing Zone Config Profile to protect TCP:80, UDP:53, TCP:other, and UDP:other services in 192.168.41.0/24 subnet, using newly created Zone Config Profiles, and deploy to Thunder TPS system in minutes.

1. Go to **Configurations >> Protected Objects >> Zones** on the dropdown menu. On Zones page, click **Add New** to create a new Protected Zone, *liveDemo41* as an example, and select *liveDemo41_Profile* as its Zone Config Profile which automatically populates corresponding TCP and UDP services and their Protection Profiles; assign *192.168.41.0/24* subnet as its protected IP subnet; select *Demo_Mitigators* device group (including the Thunder TPS system) as the Mitigator Group; and confirm *A10_Default* is pre-populated Zone Operational Policy.
   Click **Save** or **Save&Exit** at bottom to push the newly created *liveDemo41* Protected Zone to the Thunder TPS system.



Zones | Destination Entries | Source Entries | aGalaxy 5.0.2 b84 (VMware)

Configuration >> Protected Objects >> Zones >> **Configure**

* Zone Name: liveDemo41

☑ Use Zone Profile for Configuration

Learnt Thresholds

* IP Address(es): ● Statically Configured ○ Dynamically Learnt from BGP Peer

IPv4 / IPv6 Address / Subnet

192.168.41.0/24

1 item

* Zone Config Profile: liveDemo41_Profile

Showing the services configured in the selected zone profile. A service using protection profiles can be viewed but cannot be edited here.

Services

Protocol	Port/Protocol Num	Protection Profile
TCP	80	liveDem
UDP	53	liveDem
TCP	other	liveDem
UDP	other	liveDem

Devices

Detector:

Mitigator Group: Demo_Mitigators -- 1 device(s)

Zone Parameters

Description: Live Demo with Level Escalation and GLID etc.

Oper Policy: A10_Default

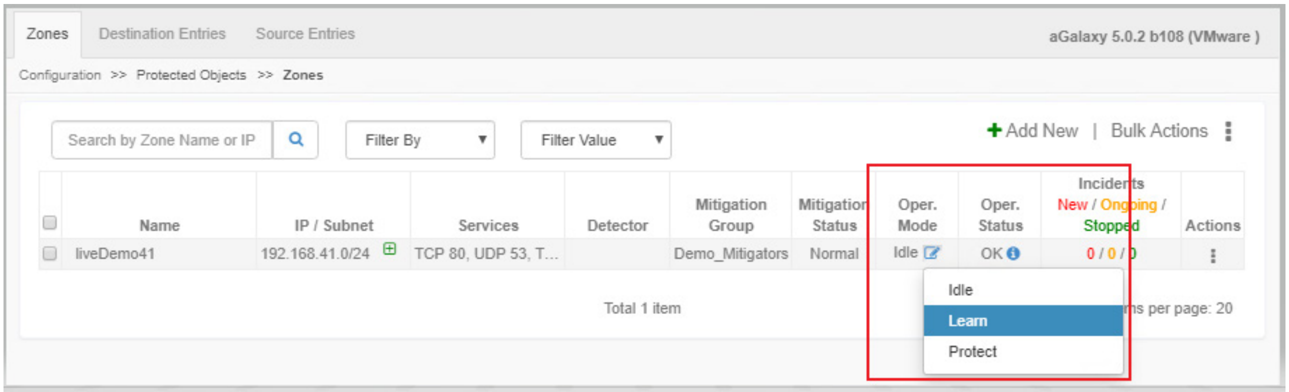
Packet Capture Policy:

Rate Limit: A10_20Mbps

DSCP Marking ☐

Source Ports

2. Change Operation Mode (Oper. Mode) of this Protected Zone to *Learn*, if the thresholds are not known.



Zones | Destination Entries | Source Entries | aGalaxy 5.0.2 b108 (VMware)

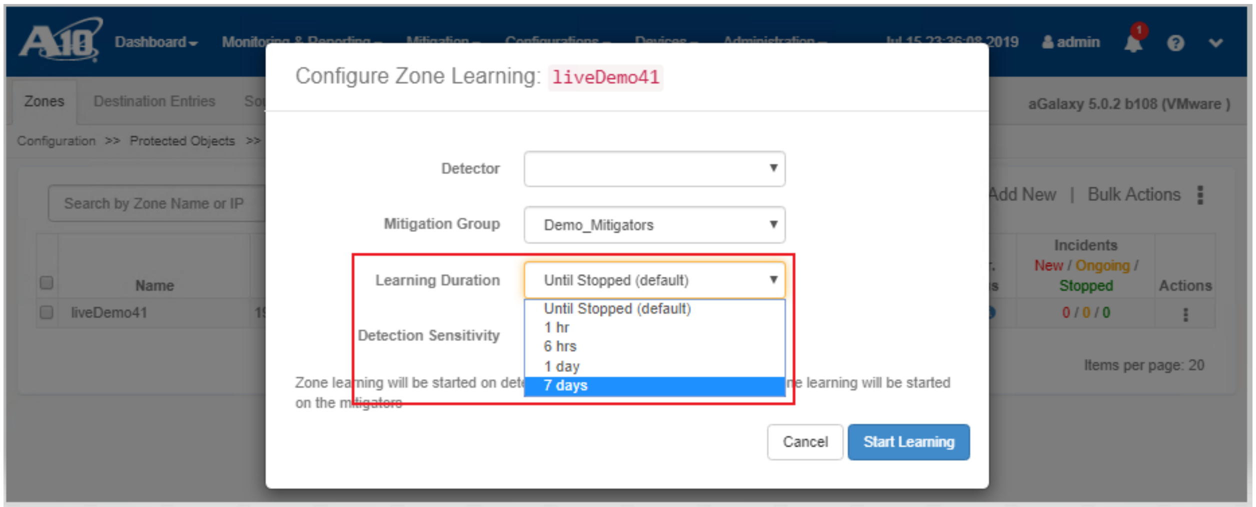
Configuration >> Protected Objects >> **Zones**

Search by Zone Name or IP | Filter By | Filter Value | + Add New | Bulk Actions

☐	Name	IP / Subnet	Services	Detector	Mitigation Group	Mitigation Status	Oper. Mode	Oper. Status	Incidents New / Ongoing / Stopped	Actions
☐	liveDemo41	192.168.41.0/24	TCP 80, UDP 53, T...		Demo_Mitigators	Normal	Idle	OK	0 / 0 / 0	⋮

Total 1 item | Items per page: 20

A10 recommends that the zone stays in Learning mode for at least one week.



Configure Zone Learning: liveDemo41

Detector:

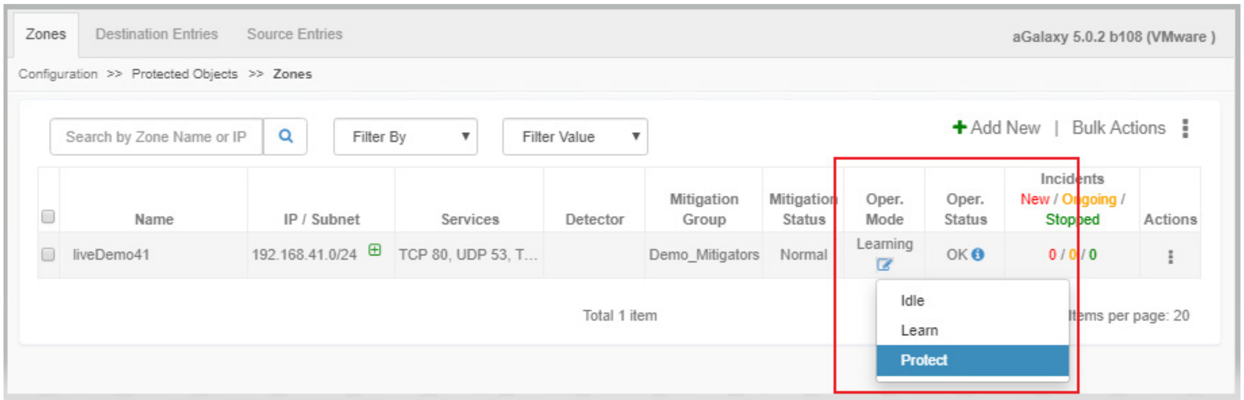
Mitigation Group: Demo_Mitigators

Learning Duration: Until Stopped (default)

Detection Sensitivity

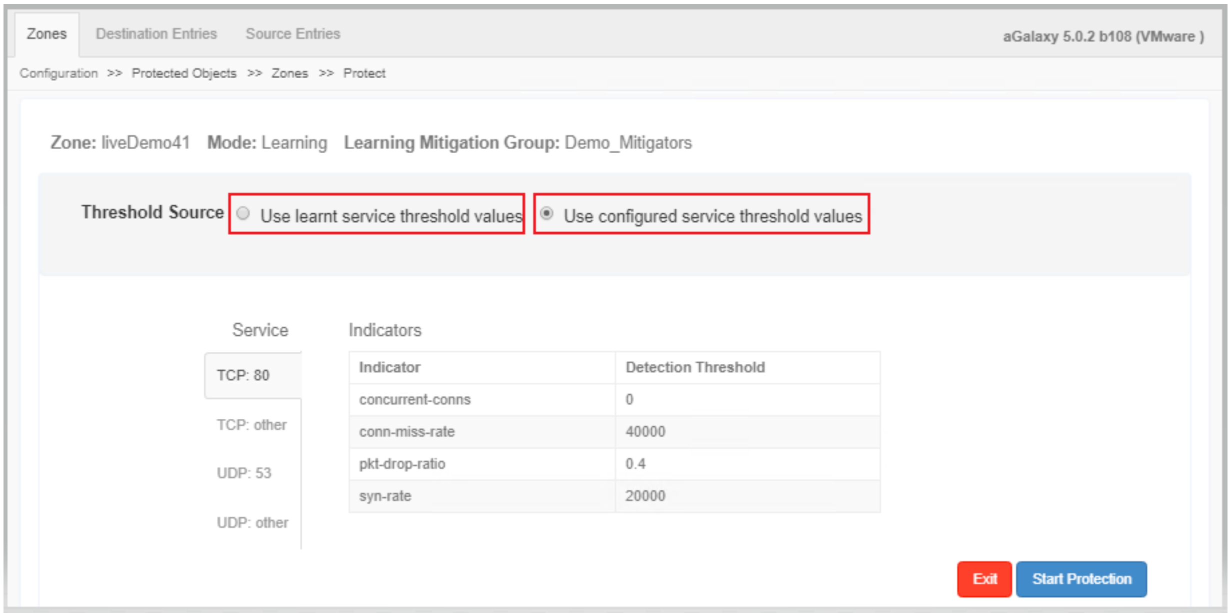
Zone learning will be started on det… …e learning will be started on the mitigators

3. Change Operation Mode (Oper. Mode) of this Protected Zone to *Protect*, after the learning period ends.



Name	IP / Subnet	Services	Detector	Mitigation Group	Mitigation Status	Oper. Mode	Oper. Status	Incidents New / Ongoing / Stopped	Actions
liveDemo41	192.168.41.0/24 ⊞	TCP 80, UDP 53, T…		Demo_Mitigators	Normal	Learning	OK	0 / 0 / 0	⋮

4. Click **Use learnt service threshold values** or **Use configured service threshold values,** then **Start Protection** to activate DDoS protection at this *liveDemo41* protected zone.



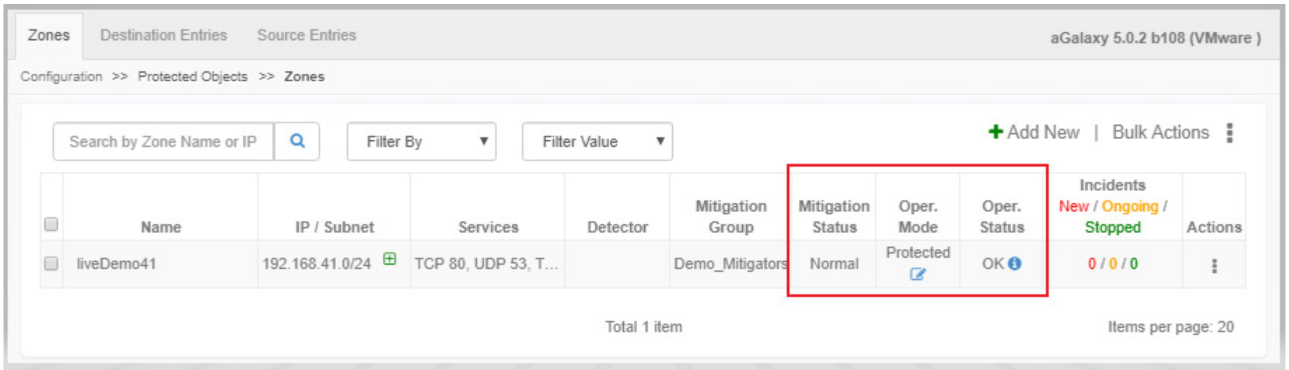
Zone: liveDemo41 **Mode:** Learning **Learning Mitigation Group:** Demo_Mitigators

Threshold Source ○ Use learnt service threshold values ● Use configured service threshold values

Indicators

Indicator	Detection Threshold
concurrent-conns	0
conn-miss-rate	40000
pkt-drop-ratio	0.4
syn-rate	20000

5. Confirm this *liveDemo41* protected zone now shows *Protected* at its **Operation Mode**, *Normal* at **Mitigation Status** and *OK* at **Operation Status**.


Zones
Destination Entries
Source Entries
aGalaxy 5.0.2 b108 (VMware)
Configuration >> Protected Objects >> Zones
Search by Zone Name or IP
Filter By
Filter Value
+ Add New | Bulk Actions

□	Name	IP / Subnet	Services	Detector	Mitigation Group	Mitigation Status	Oper. Mode	Oper. Status	Incidents New / Ongoing / Stopped	Actions
□	liveDemo41	192.168.41.0/24 ⊞	TCP 80, UDP 53, T...		Demo_Mitigators	Normal	Protected	OK	0 / 0 / 0	⋮

Total 1 item

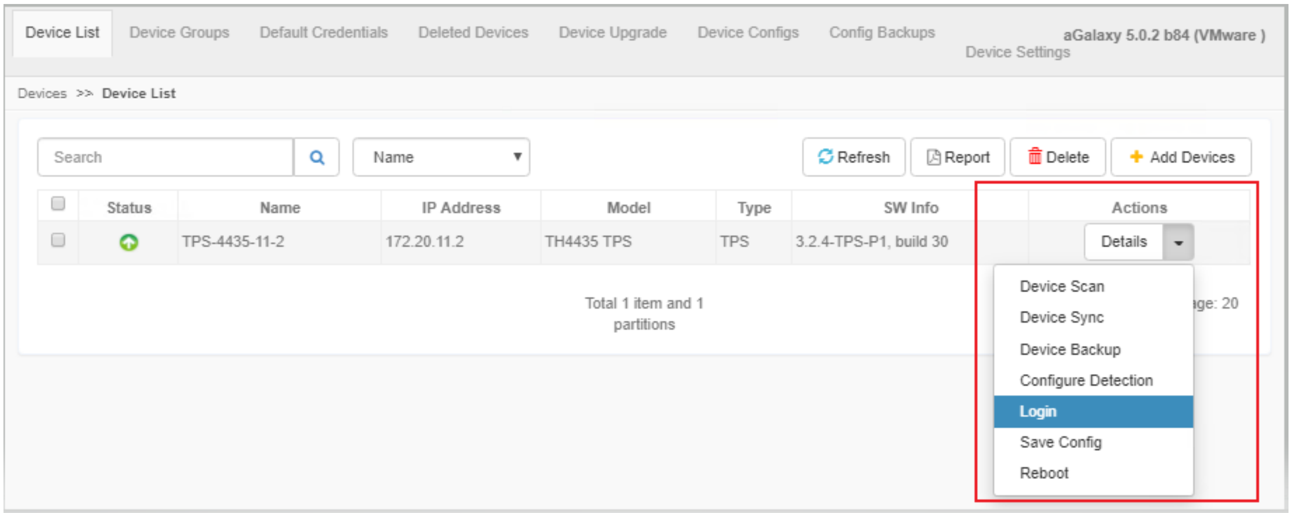
Items per page: 20

6. Follow the same New Protected Zone creation and deployment steps to expedite DDoS protection for other IP subnets or IP addresses.

REVIEWING NEWLY DEPLOYED PROTECTED ZONE ON THUNDER TPS SYSTEM

Under Device List on aGalaxy, **Login** can be used to login onto the target Thunder TPS system GUI to review the newly deployed Protected Zones and Templates, liveDemo41 and A10_TCP_Basic for example.

1. Go to **Devices >> Device List** dropdown menu on aGalaxy. Click **Login** next to the Thunder TPS system to access the Thunder TPS system GUI.

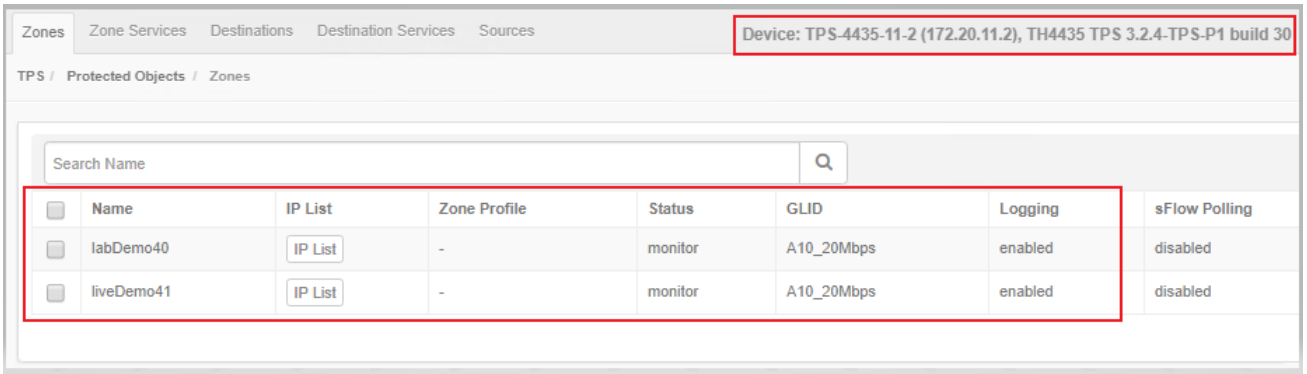


□	Status	Name	IP Address	Model	Type	SW Info		Actions
□	●	TPS-4435-11-2	172.20.11.2	TH4435 TPS	TPS	3.2.4-TPS-P1, build 30		Details ▾

Total 1 item and 1 partitions

ge: 20

2. Go to **TPS >> Protected Objects** dropdown menus on Thunder TPS system GUI. Review and confirm all newly created Protected Zones are deployed on this Thunder TPS system and in *Monitor* status.



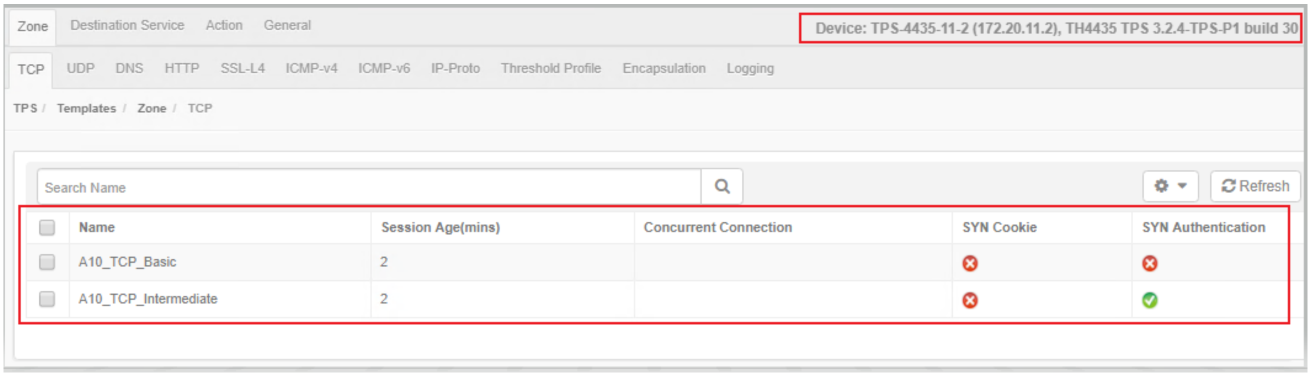
Device: TPS-4435-11-2 (172.20.11.2), TH4435 TPS 3.2.4-TPS-P1 build 30

TPS / Protected Objects / Zones

Search Name

☐	Name	IP List	Zone Profile	Status	GLID	Logging	sFlow Polling
☐	labDemo40	IP List	-	monitor	A10_20Mbps	enabled	disabled
☐	liveDemo41	IP List	-	monitor	A10_20Mbps	enabled	disabled

3. Go to **TPS >> Templates** dropdown menus on Thunder TPS system GUI. Review and confirm all built-in and customized Zone Templates are deployed on this Thunder TPS system.



Device: TPS-4435-11-2 (172.20.11.2), TH4435 TPS 3.2.4-TPS-P1 build 30

TPS / Templates / Zone / TCP

Search Name

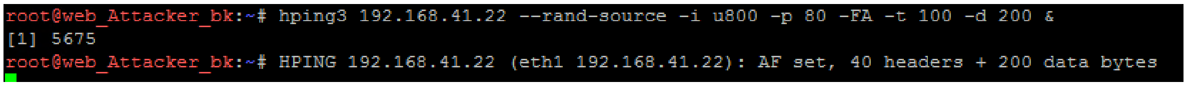
☐	Name	Session Age(mins)	Concurrent Connection	SYN Cookie	SYN Authentication
☐	A10_TCP_Basic	2		✗	✗
☐	A10_TCP_Intermediate	2		✗	✓

Logout of Thunder TPS system GUI once done.

VALIDATING THE PROACTIVE DDOS PROTECTION DEPLOYMENT

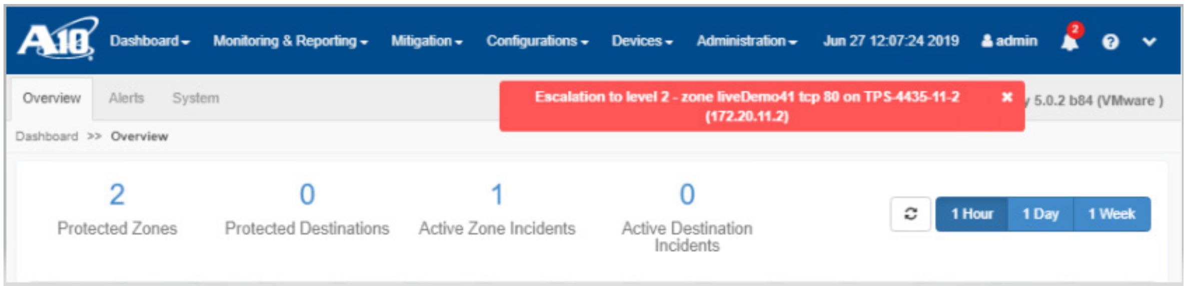
The following lab validation simulates an actual DDoS Attack. Please perform it only in an enclosed environment.

1. Inject FIN-ACK flood attack with HPIING3 from a client to the TCP:80 service on server 192.168.41.22 in the protected zone liveDemo41 as an example.



```
root@web_Attacker_bk:~# hping3 192.168.41.22 --rand-source -i u800 -p 80 -FA -t 100 -d 200 &
[1] 5675
root@web_Attacker_bk:~# HPING 192.168.41.22 (eth1 192.168.41.22): AF set, 40 headers + 200 data bytes
```

2. Confirm on aGalaxy that it has received the Level Escalation notification upon Thunder TPS detects this attack.



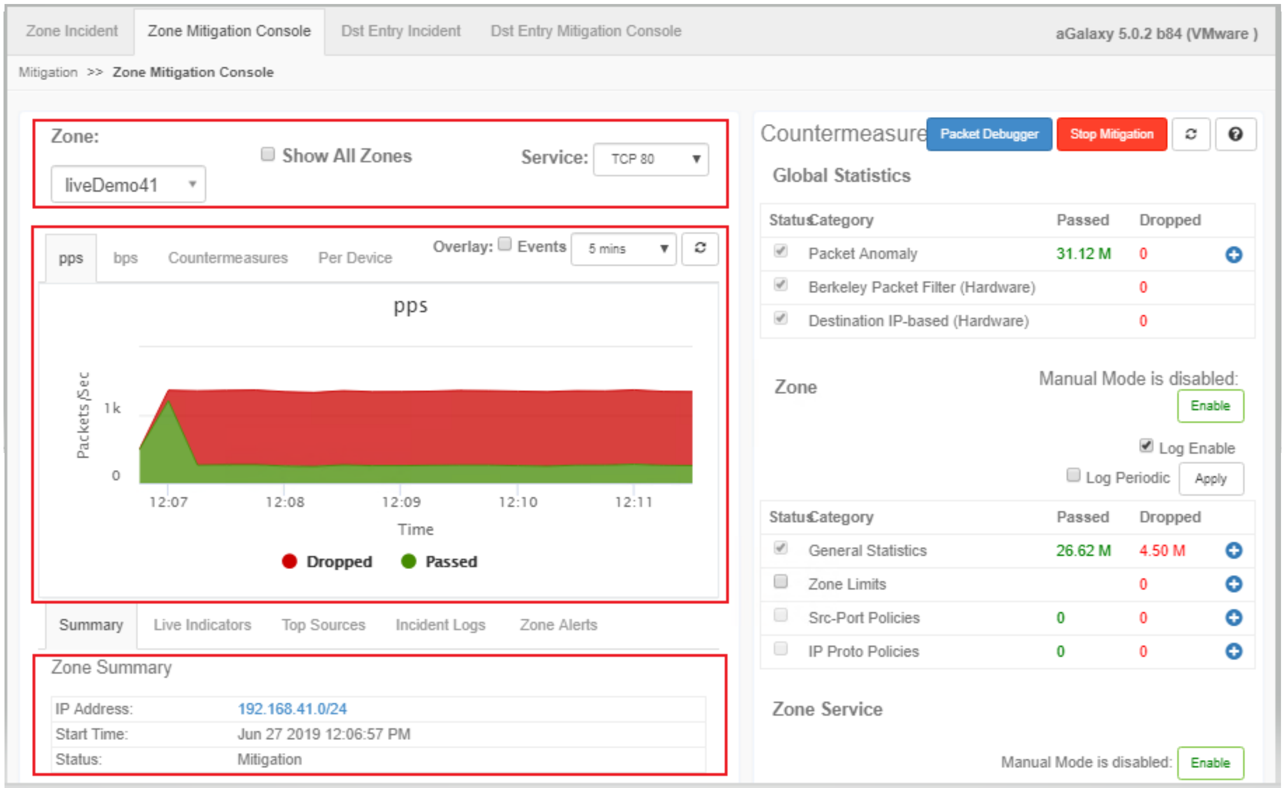
Escalation to level 2 - zone liveDemo41 tcp 80 on TPS-4435-11-2 (172.20.11.2)

Dashboard >> Overview

2	0	1	0
Protected Zones	Protected Destinations	Active Zone Incidents	Active Destination Incidents

3. Click **Active Zone Incidents** or go to **Mitigation >> Zone Incidents** on the dropdown menu. Confirm aGalaxy shows this ongoing attack and is around 1Kpps.

4.



Zone: liveDemo41

Service: TCP 80

Global Statistics

Status	Category	Passed	Dropped
☑	Packet Anomaly	31.12 M	0
☑	Berkeley Packet Filter (Hardware)		0
☑	Destination IP-based (Hardware)		0

Zone

Manual Mode is disabled:

☑ Log Enable

□ Log Periodic

Status	Category	Passed	Dropped
☑	General Statistics	26.62 M	4.50 M
□	Zone Limits		0
□	Src-Port Policies	0	0
□	IP Proto Policies	0	0

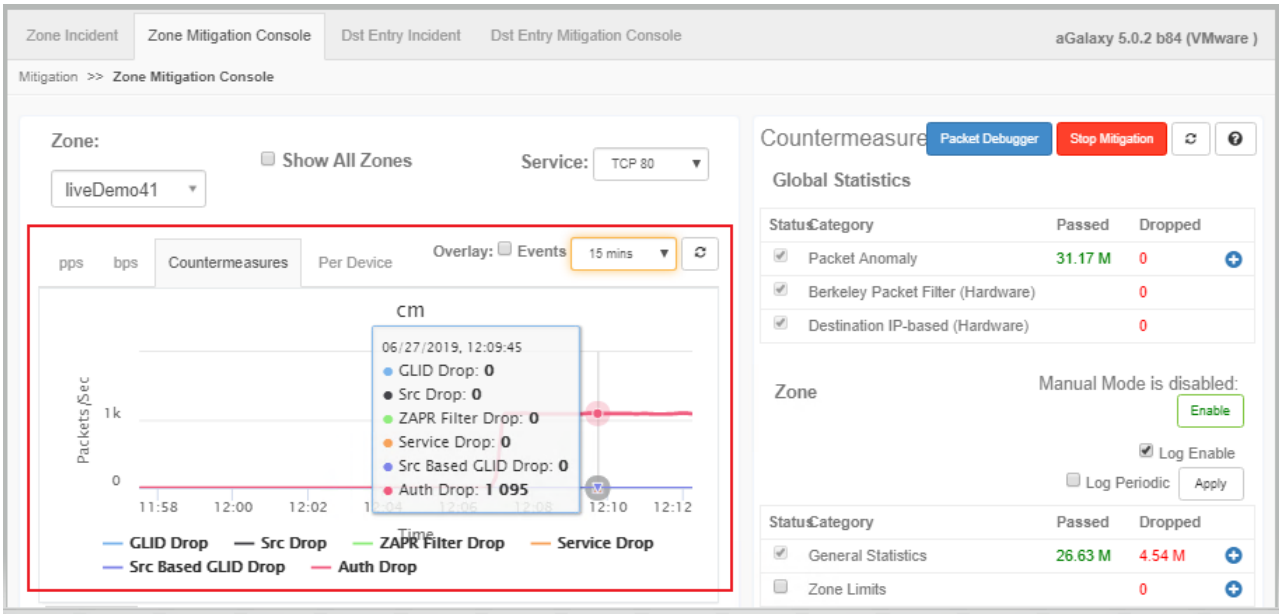
Zone Service

Manual Mode is disabled:

Zone Summary

IP Address:	192.168.41.0/24
Start Time:	Jun 27 2019 12:06:57 PM
Status:	Mitigation

5. Select **Countermeasures** tab to confirm aGalaxy shows **Auth Drop** is the primary countermeasure to thwart this DDoS attack per *A10_TCP_Intermediate* template of the *liveDemo41* protected zone configuration.



Zone: liveDemo41

Service: TCP 80

06/27/2019, 12:09:45
- GLID Drop: **0**
- Src Drop: **0**
- ZAPR Filter Drop: **0**
- Service Drop: **0**
- Src Based GLID Drop: **0**
- Auth Drop: **1 095**

Global Statistics

Status	Category	Passed	Dropped
☑	Packet Anomaly	31.17 M	0
☑	Berkeley Packet Filter (Hardware)		0
☑	Destination IP-based (Hardware)		0

Zone

Manual Mode is disabled:

☑ Log Enable

□ Log Periodic

Status	Category	Passed	Dropped
☑	General Statistics	26.63 M	4.54 M
□	Zone Limits		0

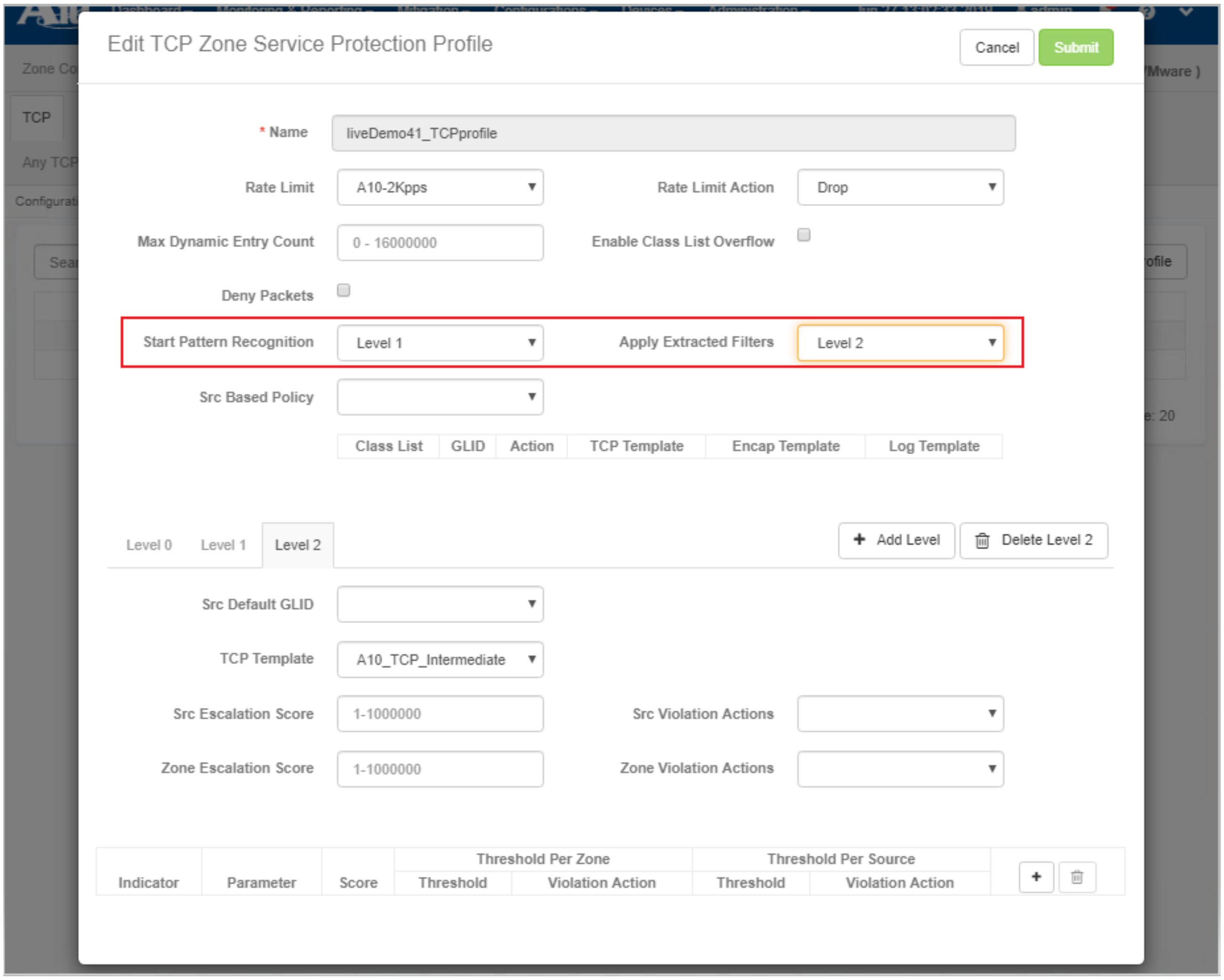
USING ZAPR AS THE COUNTERMEASURE AT LEVEL ESCALATION

ZAPR, Zero-day Attack Pattern Recognition, can help increase mitigation accuracy on volumetric-based attacks by inspecting and learning attack traffic patterns and applying pattern filters to mitigate the volumetric DDoS attacks.

ZAPR enables Thunder TPS system to identify and extract attack patterns from excessive traffic dropped by packet rate limit (GLID) and other countermeasures using machine learning techniques. ZAPR can start its pattern recognition and apply the extracted filters in according to the Level Escalation configuration of the protected TCP, UDP and DNS services ports. ZAPR can work in asymmetric proactive mode (shown below) as well as symmetric reactive mode (not shown).

Enabling ZAPR as the countermeasure

1. Go to **Configurations >> Templates >> Zone Service Protection Profile** on the dropdown menu. Update existing TCP Service Protection Profile, liveDemo41_TCPprofile, to use ZAPR as the countermeasure; set **Start Pattern Recognition** at Level 1 and **Apply Extracted Filters** at Level 2.



Edit TCP Zone Service Protection Profile

Cancel Submit

* Name: liveDemo41_TCPprofile

Rate Limit: A10-2Kpps ▾ Rate Limit Action: Drop ▾

Max Dynamic Entry Count: 0 - 16000000 Enable Class List Overflow □

Deny Packets □

Start Pattern Recognition: Level 1 ▾ Apply Extracted Filters: Level 2 ▾

Src Based Policy: ▾

Class List	GLID	Action	TCP Template	Encap Template	Log Template

Level 0 Level 1 Level 2 + Add Level 🗑 Delete Level 2

Src Default GLID: ▾

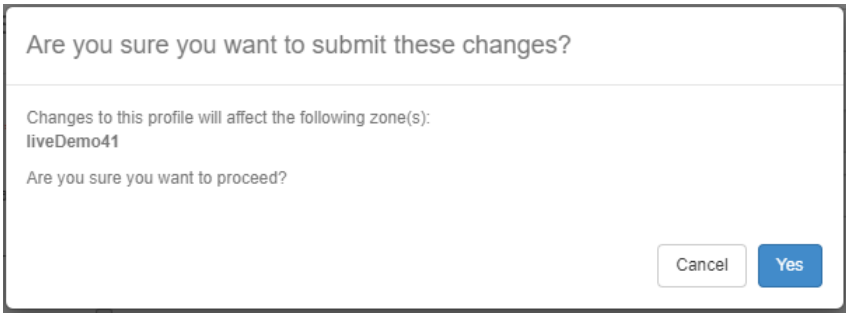
TCP Template: A10_TCP_Intermediate ▾

Src Escalation Score: 1-1000000 Src Violation Actions: ▾

Zone Escalation Score: 1-1000000 Zone Violation Actions: ▾

Indicator	Parameter	Score	Threshold Per Zone		Threshold Per Source		+ 🗑
			Threshold	Violation Action	Threshold	Violation Action	

2. **Submit** to apply this ZAPR enablement to *liveDemo41* protected zone and applicable Zone Config Profiles.



Are you sure you want to submit these changes?

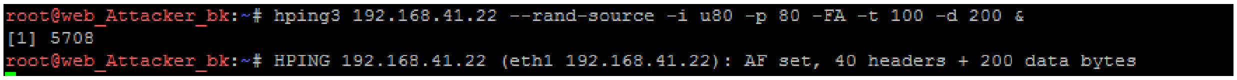
Changes to this profile will affect the following zone(s):
liveDemo41

Are you sure you want to proceed?

VALIDATING ZAPR AS THE COUNTERMEASURE

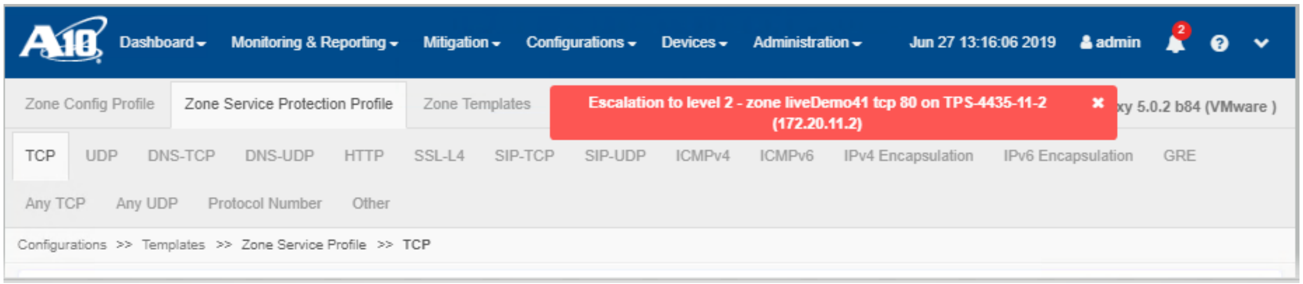
The following lab validation simulates an actual DDoS Attack. Please perform it only in an enclosed environment.

1. Inject the same FIN-ACK flood attack to TCP:80 service on server 192.168.41.22 in *liveDemo41* protected zone but with higher volume.



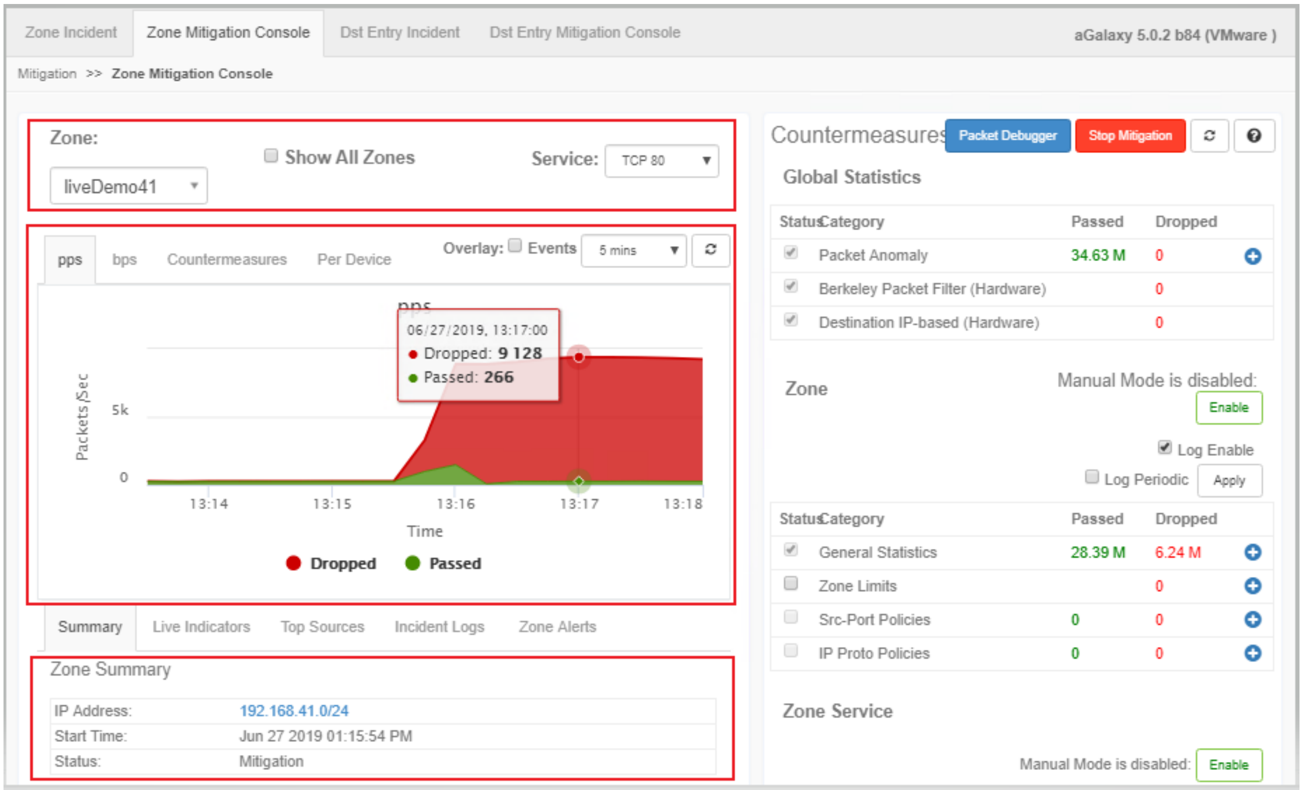
```
root@web_Attacker_bk:~# hping3 192.168.41.22 --rand-source -i u80 -p 80 -FA -t 100 -d 200 &
[1] 5708
root@web_Attacker_bk:~# HPING 192.168.41.22 (eth1 192.168.41.22): AF set, 40 headers + 200 data bytes
```

2. Confirm on aGalaxy portal that it has received the Level Escalation notification (Level 2) as Thunder TPS system detected this attack.



Escalation to level 2 - zone liveDemo41 tcp 80 on TPS-4435-11-2 (172.20.11.2)

3. Go to **Mitigation >> Zone Mitigation Console** on the dropdown menu. Confirm aGalaxy shows this ongoing attack is against TCP:80 protected service of the *liveDemo41* protected zone, but at higher 9Kpps rate, and its attack packets are dropped as a result of DDoS attack mitigation.



06/27/2019, 13:17:00
● Dropped: **9 128**
● Passed: **266**

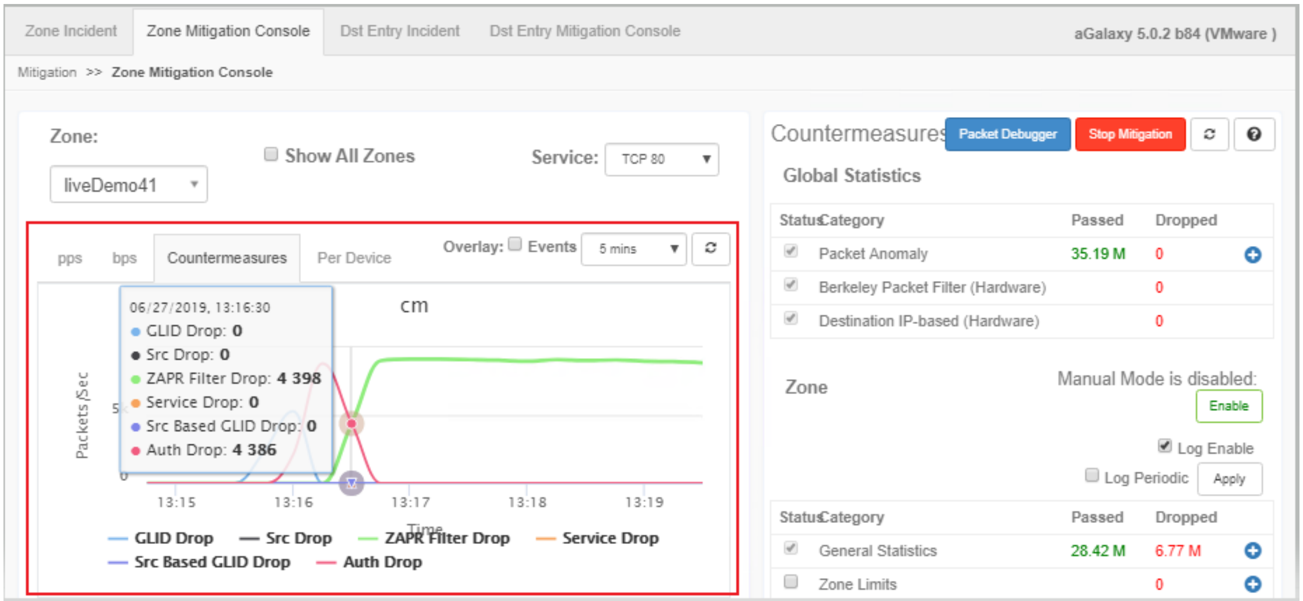
Zone Summary

IP Address:	192.168.41.0/24
Start Time:	Jun 27 2019 01:15:54 PM
Status:	Mitigation

Status	Category	Passed	Dropped
☑	Packet Anomaly	34.63 M	0
☑	Berkeley Packet Filter (Hardware)		0
☑	Destination IP-based (Hardware)		0

Status	Category	Passed	Dropped
☑	General Statistics	28.39 M	6.24 M
□	Zone Limits		0
□	Src-Port Policies	0	0
□	IP Proto Policies	0	0

4. Select **Countermeasures** tab to confirm aGalaxy shows **Auth Drop** is the first countermeasure to thwart this DDoS attack and **ZAPR Filter Drop** takes over to mitigate this DDoS attack on *liveDemo41* protected zone upon ZAPR completed its attack pattern recognition and applied the extracted filter.

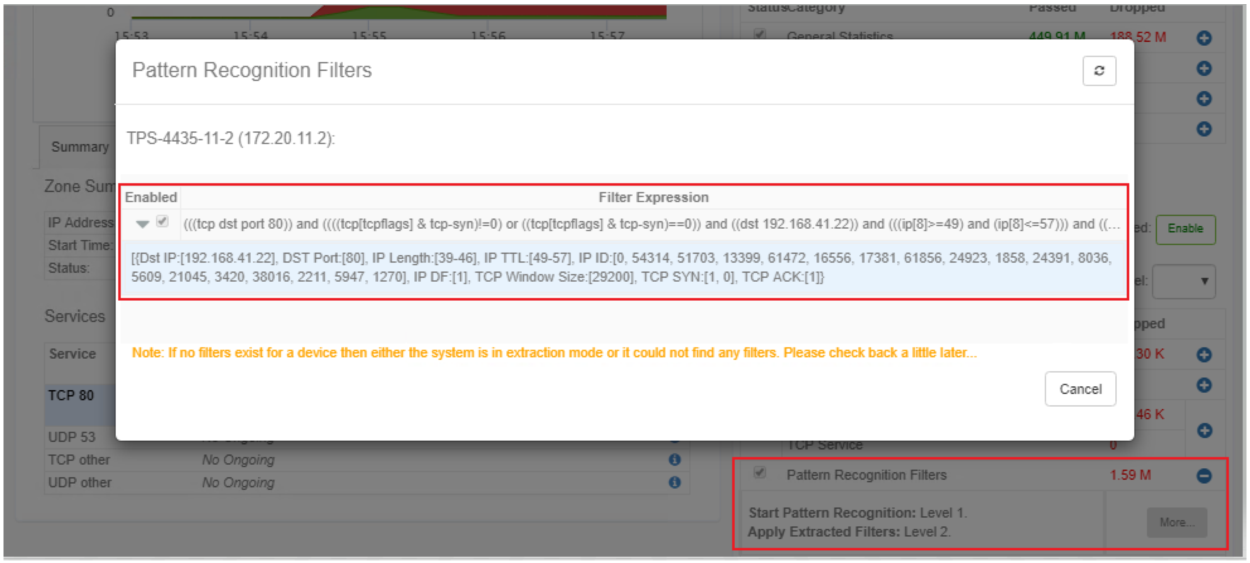


06/27/2019, 13:16:30
● GLID Drop: **0**
● Src Drop: **0**
● ZAPR Filter Drop: **4 398**
● Service Drop: **0**
● Src Based GLID Drop: **0**
● Auth Drop: **4 386**

Status	Category	Passed	Dropped
☑	Packet Anomaly	35.19 M	0
☑	Berkeley Packet Filter (Hardware)		0
☑	Destination IP-based (Hardware)		0

Status	Category	Passed	Dropped
☑	General Statistics	28.42 M	6.77 M
□	Zone Limits		0

5. Click the **More** button next to **Pattern Recognition Filters** field at bottom of **Zone Mitigation Console** to examine the extracted ZAPR filter which shows the attack is a *FIN-ACK* flood against server *192.168.41.22* and its *TCP:80* service with an IP Length range (238-242), IP TTL (*97-101*) and certain TCP Window Size (*512*).



Pattern Recognition Filters

TPS-4435-11-2 (172.20.11.2):

Enabled	Filter Expression
☑	(((tcp dst port 80)) and ((((tcp[tcpflags] & tcp-syn)!=0) or ((tcp[tcpflags] & tcp-syn)==0)) and ((dst 192.168.41.22)) and (((ip[8]>=49) and (ip[8]<=57))) and ((...

[{Dst IP:[192.168.41.22], DST Port:[80], IP Length:[39-46], IP TTL:[49-57], IP ID:[0, 54314, 51703, 13399, 61472, 16556, 17381, 61856, 24923, 1858, 24391, 8036, 5609, 21045, 3420, 38016, 2211, 5947, 1270], IP DF:[1], TCP Window Size:[29200], TCP SYN:[1, 0], TCP ACK:[1]}

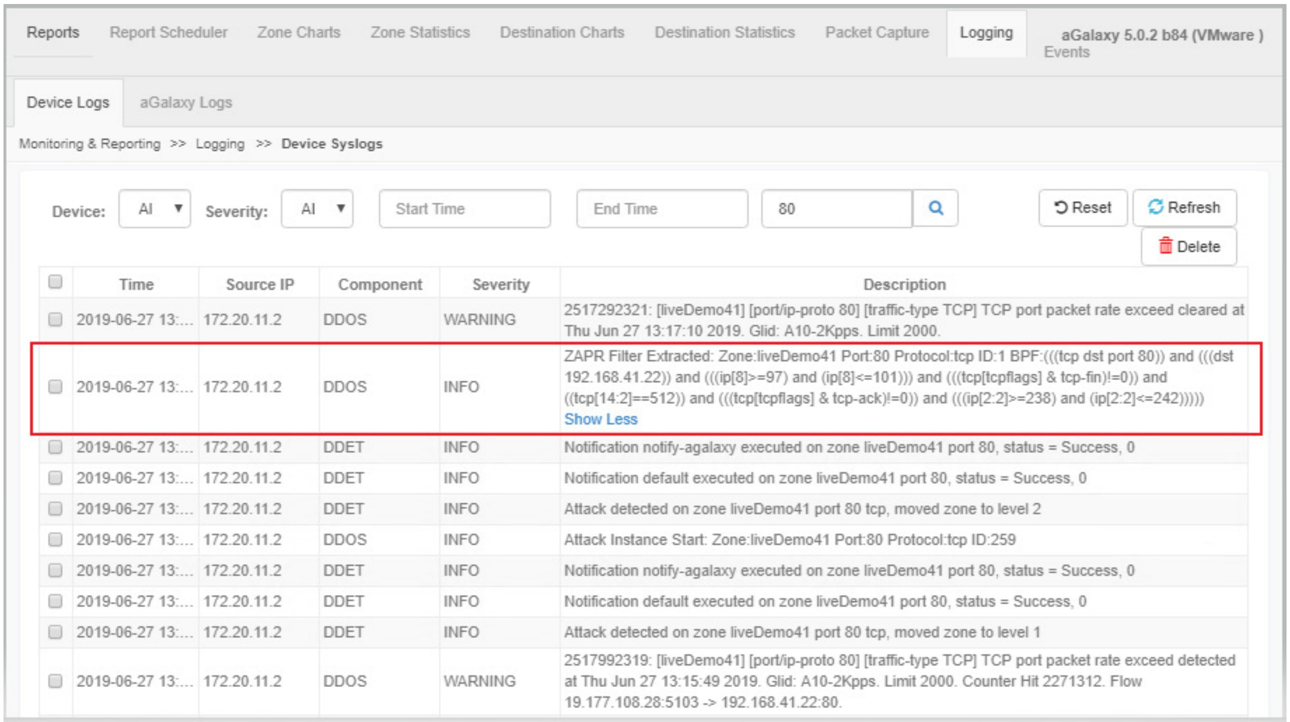
Note: If no filters exist for a device then either the system is in extraction mode or it could not find any filters. Please check back a little later...

Pattern Recognition Filters 1.59 M

Start Pattern Recognition: Level 1.
Apply Extracted Filters: Level 2.

6. Go to **Monitoring & Reporting >> Logging >> Device Logs** on the dropdown menu. ZAPR event log (ZAPR Filter Extracted syslog message) is forwarded by the Thunder TPS system and displayed on aGalaxy.

NOTE*: The TCP port packet rate exceed cleared message after ZAPR Filter Extracted message indicates the applied ZAPR filter is effective at mitigate this DDoS attack.*

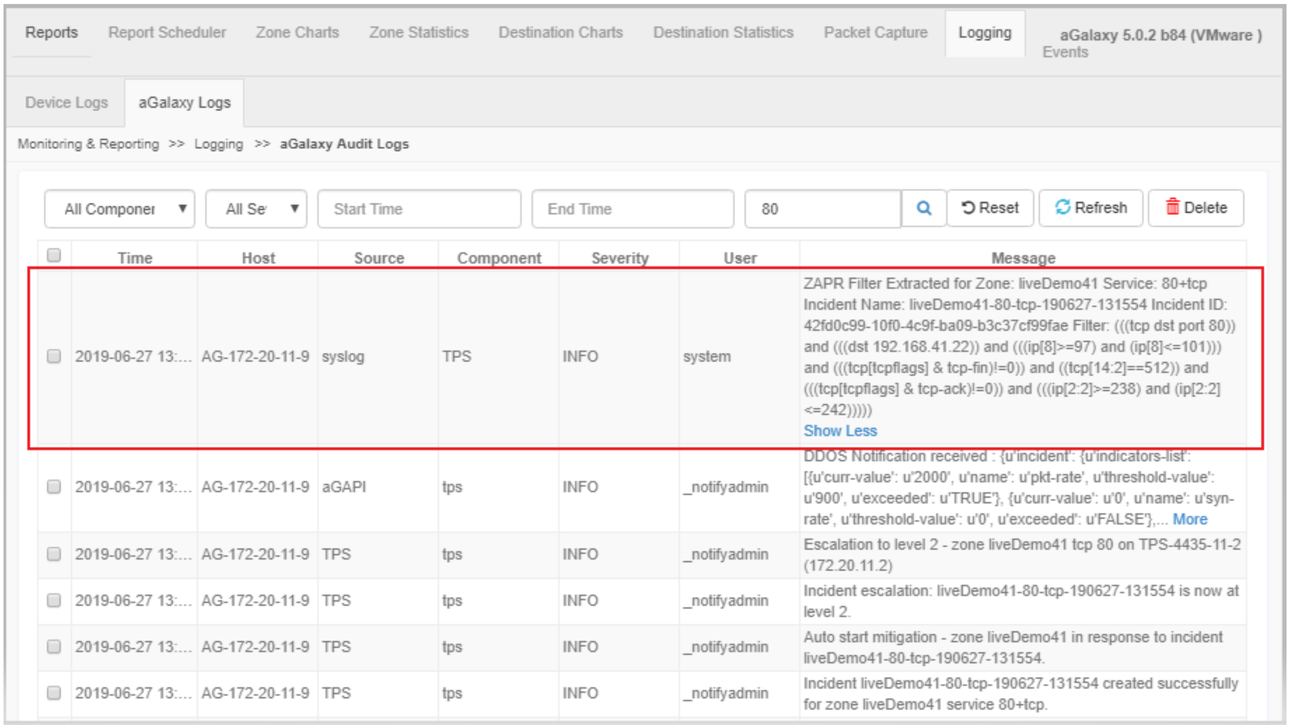


Monitoring & Reporting >> Logging >> Device Syslogs

Device: Al ▾ Severity: Al ▾ Start Time End Time 80

□	Time	Source IP	Component	Severity	Description
□	2019-06-27 13:...	172.20.11.2	DDOS	WARNING	2517292321: [liveDemo41] [port/ip-proto 80] [traffic-type TCP] TCP port packet rate exceed cleared at Thu Jun 27 13:17:10 2019. Glid: A10-2Kpps. Limit 2000.
□	2019-06-27 13:...	172.20.11.2	DDOS	INFO	ZAPR Filter Extracted: Zone:liveDemo41 Port:80 Protocol:tcp ID:1 BPF:(((tcp dst port 80)) and (((dst 192.168.41.22)) and (((ip[8]>=97) and (ip[8]<=101))) and (((tcp[tcpflags] & tcp-fin)!=0)) and ((tcp[14:2]==512)) and (((tcp[tcpflags] & tcp-ack)!=0)) and (((ip[2:2]>=238) and (ip[2:2]<=242))))) Show Less
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Notification notify-agalaxy executed on zone liveDemo41 port 80, status = Success, 0
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Notification default executed on zone liveDemo41 port 80, status = Success, 0
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Attack detected on zone liveDemo41 port 80 tcp, moved zone to level 2
□	2019-06-27 13:...	172.20.11.2	DDOS	INFO	Attack Instance Start: Zone:liveDemo41 Port:80 Protocol:tcp ID:259
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Notification notify-agalaxy executed on zone liveDemo41 port 80, status = Success, 0
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Notification default executed on zone liveDemo41 port 80, status = Success, 0
□	2019-06-27 13:...	172.20.11.2	DDET	INFO	Attack detected on zone liveDemo41 port 80 tcp, moved zone to level 1
□	2019-06-27 13:...	172.20.11.2	DDOS	WARNING	2517992319: [liveDemo41] [port/ip-proto 80] [traffic-type TCP] TCP port packet rate exceed detected at Thu Jun 27 13:15:49 2019. Glid: A10-2Kpps. Limit 2000. Counter Hit 2271312. Flow 19.177.108.28:5103 -> 192.168.41.22:80.

7. Go to **Monitoring & Reporting >> Logging >> aGalaxy Logs** on the dropdown menu. The same ZAPR event log (ZAPR Filter Extracted message) is recorded by aGalaxy and shows in aGalaxy Audit Logs.



□	Time	Host	Source	Component	Severity	User	Message
□	2019-06-27 13:...	AG-172-20-11-9	syslog	TPS	INFO	system	ZAPR Filter Extracted for Zone: liveDemo41 Service: 80+tcp Incident Name: liveDemo41-80-tcp-190627-131554 Incident ID: 42fd0c99-10f0-4c9f-ba09-b3c37cf99fae Filter: (((tcp dst port 80)) and (((dst 192.168.41.22)) and (((ip[8]>=97) and (ip[8]<=101))) and (((tcp[tcpflags] & tcp-fin)!=0)) and ((tcp[14:2]==512)) and (((tcp[tcpflags] & tcp-ack)!=0)) and (((ip[2:2]>=238) and (ip[2:2] <=242))))) Show Less
□	2019-06-27 13:...	AG-172-20-11-9	aGAPI	tps	INFO	_notifyadmin	DDOS Notification received : {u'incident': {u'indicators-list': [{u'curr-value': u'2000', u'name': u'pkt-rate', u'threshold-value': u'900', u'exceeded': u'TRUE'}, {u'curr-value': u'0', u'name': u'syn-rate', u'threshold-value': u'0', u'exceeded': u'FALSE'},... More
□	2019-06-27 13:...	AG-172-20-11-9	TPS	tps	INFO	_notifyadmin	Escalation to level 2 - zone liveDemo41 tcp 80 on TPS-4435-11-2 (172.20.11.2)
□	2019-06-27 13:...	AG-172-20-11-9	TPS	tps	INFO	_notifyadmin	Incident escalation: liveDemo41-80-tcp-190627-131554 is now at level 2.
□	2019-06-27 13:...	AG-172-20-11-9	TPS	tps	INFO	_notifyadmin	Auto start mitigation - zone liveDemo41 in response to incident liveDemo41-80-tcp-190627-131554.
□	2019-06-27 13:...	AG-172-20-11-9	TPS	tps	INFO	_notifyadmin	Incident liveDemo41-80-tcp-190627-131554 created successfully for zone liveDemo41 service 80+tcp.

This concludes the Proactive DDoS Protection deployment and validation.

SUMMARY

This guide describes how to expedite the deployment of proactive DDoS protection on A10 TPS system using A10 aGalaxy management system. This guide uses asymmetric proactive deployment mode as an example to show how these built-in default DDoS protection profiles and templates at aGalaxy system help expedite the DDoS protection deployment in minutes, as well as how to use them as the reference to customize the DDoS protection strategies also in minutes. Contact your local A10 sales team to help you design your DDoS protection strategies and deployment process.

For more information about A10 Thunder TPS Series products, see the following documents:

- A10 aGalaxy Configuration Guide
- A10 Thunder TPS DDoS Mitigation Guide
- ACOS 3.0 SDK Guide

APPENDIX

Thunder TPS system configuration highlight along with ZAPR enablement at TCP:80 service port in *liveDemo41* protected zone.

NOTE*: ZAPR configuration will be populated by aGalaxy upon Level Escalation triggered.*

```
!
! multi-ctrl-cpu 4
!
! ddos pattern-recognition dedicated-cpus 2
!
system ddos-attack log
!
hostname TPS-4435-11-2
!
interface management
  ip address 172.20.11.2 255.255.0.0
  ip default-gateway 172.20.0.1
!
interface ethernet 1
  name to_ExtRT_clients
  enable
  ip address 192.168.20.2 255.255.255.0
!
interface ethernet 2
  name to_IntRT_servers
  enable
  ip address 192.168.30.2 255.255.255.0
!
interface ethernet 5
  name to_xFlowNW
  enable
  ip address 192.168.255.2 255.255.255.0
!
glid A10-2Kpps
  description “User-defined GLID”
  pkt-rate-limit 2000
!
glid A10_20Mbps
  description “Pre-defined GLID”
  bit-rate-limit 20000
!
ddos protection enable
ddos protection rate-interval 1sec
!
ddos pattern-recognition enable
!
ddos zone-template logging A10_LOGGING_Basic
!
ddos zone-template tcp A10_TCP_Basic
  zero-win 16
!
ddos zone-template tcp A10_TCP_Intermediate
  zero-win 16
  syn-authentication send-rst
  syn-authentication pass-action authenticate-src
  syn-authentication fail-action blacklist-src
  ack-authentication retransmit-check timeout 3
  ack-authentication retransmit-check min-delay 1
  ack-authentication pass-action authenticate-src
  ack-authentication fail-action drop
!
ddos zone-template udp A10_UDP_Basic
  known-resp-src-port action drop exclude-src-resp-port
!
ddos zone-template udp A10_UDP_Intermediate
  spoof-detect timeout 5
  spoof-detect pass-action authenticate-src
  spoof-detect fail-action drop
  known-resp-src-port action drop exclude-src-resp-port
!
ddos notification-template notify-agalaxy
  api
    host-ipv4-address 172.20.11.9 use-mgmt-port
    timeout 30
    relative-uri /agapi/v1/ddos/notification/
    authentication
      relative-login-uri /agapi/auth/login/
      relative-logoff-uri /agapi/auth/logout/
      auth-username _notifyadmin
      auth-password encrypted ycS3t8e49gTax-CXkOddHtp4yitlBAGyDPBCMuNXbAOc8EIy41dsA5zwQ-jLjV2wDn
!
```

ddos notification-template-common

```
  default-template notify-agalaxy
!
ddos src default ip
!
ddos src default ipv6
!
ddos dst default ip
  l4-type icmp
  l4-type other
  l4-type tcp
    syn-auth disable
    drop-on-no-port-match disable
  l4-type udp
    drop-on-no-port-match disable
!
ddos dst default ipv6
  l4-type icmp
  l4-type other
  l4-type tcp
    syn-auth disable
    drop-on-no-port-match disable
  l4-type udp
    drop-on-no-port-match disable
!
ddos dst zone liveDemo41
  operational-mode monitor
  ip 192.168.41.0/24
  description “Live Demo with Level Escalation and GLID etc.”
  glid A10_20Mbps
  zone-template logging A10_LOGGING_Basic
  log enable
  port 53 udp
    glid A10-2Kpps action drop
    enable-top-k
    level 0
      zone-escalation-score 100
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 1
      zone-escalation-score 100
      zone-template udp A10_UDP_Basic
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 2
      zone-template udp A10_UDP_Intermediate
  port 80 tcp
    glid A10-2Kpps action drop
    enable-top-k
    pattern-recognition heuristic
    level 0
      zone-escalation-score 100
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 1
      zone-escalation-score 100
      zone-template tcp A10_TCP_Basic
      start-pattern-recognition
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 2
      zone-template tcp A10_TCP_Intermediate
      apply-extracted-filters
  port other tcp
    enable-top-k
    glid A10-2Kpps action drop
    level 0
      zone-escalation-score 100
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 1
      zone-escalation-score 100
      zone-template tcp A10_TCP_Basic
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 2
      zone-template tcp A10_TCP_Intermediate
  port other udp
    enable-top-k
    glid A10-2Kpps action drop
    level 0
      zone-escalation-score 100
      indicator pkt-rate
        score 150
        zone-threshold 900
    level 1
      zone-escalation-score 100
      zone-template udp A10_UDP_Basic
      indicator pkt-rate
        score 150
        zone-threshold 900
  level 2
   zone-template udp A10_UDP_Intermediate
!
logging syslog information
!
logging host 172.20.11.9 use-mgmt-port
!
router bgp 64512
 network 192.168.0.0/16 route-map A10-SET-
NEXT-HOP
 neighbor 192.168.20.1 remote-as 64512
!
router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.60.0 0.0.0.255 area 0
 router-id 3.3.3.3
!
route-map A10-SET-NEXT-HOP permit 1
!
sflow setting counter-polling-interval 15
sflow setting local-collection disable
!
sflow collector ip 192.168.255.9 6343
 customized-setting export
  a10-proprietary-polling
!
sflow agent address 172.20.11.2
!
sflow polling ddos enable 3_0-compatibility
sflow polling ddos enable-anomaly-stats
!
snmp-server enable service
!
snmp-server enable traps all
!
snmp-server host 172.20.11.9 version v2c
public
!
End
```

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-DG-16171-EN-01 AUG 2019