EXPEDITE PROACTIVE DDoS PROTECTION DEPLOYMENT USING A10 AGALAXY SYSTEM

Configure, monitor and manage DDoS protection in asymmetric proactive mode using aGalaxy
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>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVERVIEW ............................................................</td>
</tr>
<tr>
<td>SOLUTION .............................................................</td>
</tr>
<tr>
<td>DEPLOYMENT PREREQUISITES .......................................</td>
</tr>
<tr>
<td>DEPLOYMENT MODE ..................................................</td>
</tr>
<tr>
<td>ASYMMETRIC PROACTIVE MODE .....................................</td>
</tr>
<tr>
<td>SUMMARY .............................................................</td>
</tr>
<tr>
<td>APPENDIX ..............................................................</td>
</tr>
<tr>
<td>ABOUT A10 NETWORKS ...............................................</td>
</tr>
</tbody>
</table>
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, website operators, and enterprises.

---

**Figure 1: A10 Networks ACOS architecture**

- 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 . . .
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.
**Initial Setup at Thunder TPS system (DDoS Mitigator)**

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

```plaintext
interface management
  ip address 172.20.11.2 255.255.0.0
  ip default-gateway 172.20.0.1
interface ethernet 1
  name to_ExtrRT_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.
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.

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.

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.

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.

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.
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.

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.
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.

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.
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.

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.

2. Follow the same step to create other new Zone Config Profiles, liveDemo40_Profile 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.
2. Change Operation Mode (Oper. Mode) of this Protected Zone to *Learn*, if the thresholds are not known.
A10 recommends that the zone stays in Learning mode for at least one week.

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

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

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.
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.

![Protected Zones Table](image1)

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.

![Zone Templates Table](image2)

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 u000 -p 80 -p 80 -t 100 -d 200
```

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

![Level Escalation Notification](image3)
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. Click **Mitigation Zone** next to the ongoing attack or 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 and its attack packets are dropped as a result of DDoS attack 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.
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.
2. **Submit** to apply this ZAPR enablement to `liveDemo41` protected zone and applicable Zone Config Profiles.

![User confirmation dialog]

**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.

   ```bash
   root@web_Attacker.dk:~# hping3 192.168.41.22 --rand-source -l u80 -p 80 -FA -t 100 -d 200
   192.168.41.22: Port 80 is filtered.
   root@web_Attacker.dk:~# 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.

![Galaxy portal screenshot]
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.

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.
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](image)

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.

![Device Logs](image)
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.

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.

```conf
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_ExtrRT_clients
  enable
  ip address 192.168.20.2 255.255.255.0

interface ethernet 2
  name to_InterRT_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 black-list-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 yc53t8e49gTax-CXk0ddHtp4yitlBAGyDPBCMuNXbA0c8EIy41dsA5zwQ-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 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 80 tcp
  apply-extracted-filters
  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
  port 80 tcp
  apply-extracted-filters
  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
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