Cisco Secure DDoS Edge Protection Solution

This chapter includes configurations to implement Cisco Secure DDoS Edge Protection for different types of traffic.

Entities in the DDoS Edge Protection Solution

The Cisco Secure DDoS Edge Protection software solution stops DDoS attacks at the ingress side of the network edge.

The DDoS Edge Protection solution helps you detect DDoS attacks and take mitigation actions on the router. To enable detection services at the network edge, you need to configure the following entities:

- DDoS Edge Protection Controller: This entity manages and monitors the Detector docker application, mitigates attacks, and oversees a distributed network of edge detectors. It analyzes detection trends across the network, orchestrates cross-network visibility and mitigation, and provides complete system management for the entire service.
- DDoS Edge Protection Detector: This entity is a real-time DDoS detection microservice container application that runs as a docker-application on a router with the DDoS controller. The DDOS controller can run on a cloud, server, or customer premises and is connected to this application.

Protect GTP Traffic from DDoS Attacks

Table 1: Feature History Table

Feature Name	Release Information	Description
Protect GTP Traffic from DDoS Attacks	Release 7.10.1	Cisco Secure Distributed Denial-of-Service (DDoS) edge protection solution protects the service provider's edge network from DDoS attacks and helps mitigate them. This solution deploys a centralized controller that manages a distributed network of edge detectors that analyze and mitigate threats across networks. In this release, the controller and detector monitor GPRS Tunneling Protocol (GTP) traffic.

The NCS 540 platform supports traffic detection on the GPRS Tunneling Protocol User Plane (GTP-U). You can select on which interface the traffic must be monitored. When the protection software solution is implemented, the GTP traffic flow is filtered, and a DDoS attack is detected.

When the DDoS attack is detected, the DDoS Edge Protection Controller pushes the mitigation action to the NCS 540 router through the detector.

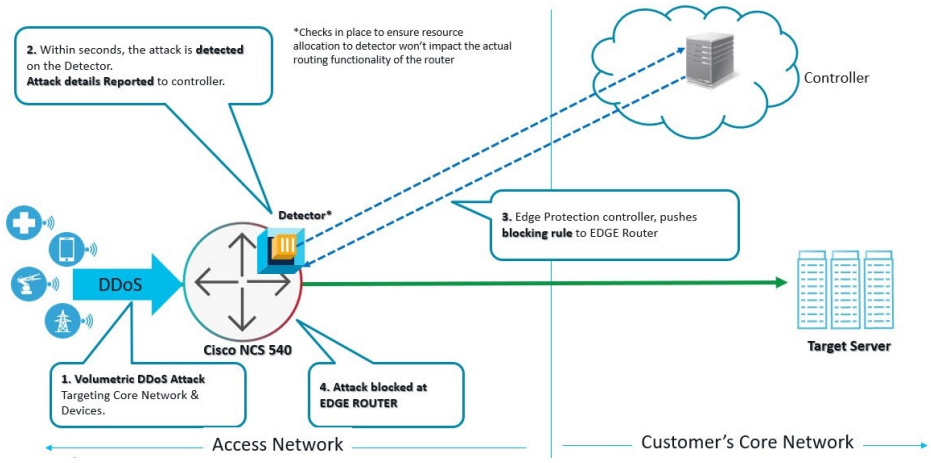
This whole process is performed through an Access Control List (ACL) configuration. A unique GTP flow is identified with a unique Tunnel Endpoint Identifier (TEID) present in the GTP header. The GTP header follows the UDP header. The identified flow that is associated with a TEID can be mitigated with the help of an ACE using the UDF option (User-defined filter) configuration in the ACL.

Note

- Only GTP-U traffic is monitored. The detection is not supported for the GTP-C traffic.
- If the GTP header is incorrect, then the sampled record is discarded.

For more information on the supported platforms, see Supported Platforms.

The following sample topology diagram shows that the NCS 540 series router runs the DDoS Edge Protection detector. The DDoS Edge Protection controller is running as an external server that manages the DDoS Edge Protection detector.



Prerequisites for Installing DDoS Edge Protection

- Configure the management interface to reach the DDoS controller IP Address.
- Manually configure the base ACL, UDF, NetFlow, and SSH configurations.

  For more information, see Install and Configure DDoS Edge Protection for GTP Traffic, on page 4.
- Use the following configuration to mitigate the DDoS attack as UDF is a qualifier for ACL:

  ```
  hw-module profile tcam format access-list ipv4 src-addr dst-addr
  src-port dst-port proto frag-bit enable-capture udf1 udf-gtp location
  <location>
  ```
- Reload the router (as a hw-module profile configuration is performed).

Restrictions of DDoS Edge Protection Solution

- Only the IPv4 GTP tunnel is supported. The inner traffic can be both IPv4 or IPv6.
- The default VRF configuration is only supported on the management port and the non-default VRF is not supported. Ensure that you configure the management port only on a default VRF so that there is communication between the docker and the controller.

Supported NCS 540 Platforms

From Cisco IOS XR 7.7.1, record type GTP is supported on the NCS 540 platform. For example:

```
flow monitor-map DetectPro_Monitor_IPV4
  record ipv4 gtp
```

You can perform DDoS Edge Protection on the following NCS 540 platforms:

Table 2: Supported NCS 540 Platforms

IOS XR Release	Platform
7.7.1	N540-ACC-SYS
	N540X-ACC-SYS
	N540-24Z8Q2C-SYS
7.10.1	N540-24Q8L2DD-SYS
	N540X-16Z4G8Q2C-D/A
	N540X-16Z8Q2C-D
	N540-28Z4C-SYS-D/A
	N540X-12Z16G-SYS-D/A
	N540X-12Z20G-SYS-D/A

Unsupported NCS 540 Platforms

The following NCS platforms are not supported:

- N540X-4Z14G2Q-D/A
- N540X-8Z16G-SYS-D/A
- N540X-6Z18G-SYS-D/A
- N540-6Z18G-SYS-D/A
- N540-6Z14G-SYS-D
- N540-FH-AGG-SYS
- N540-FH-CSR-SYS

Install and Configure DDoS Edge Protection for GTP Traffic

You can install the DDoS Edge Protection application through the DDoS edge protection controller. Perform the following:

1. Install and download the DDoS Edge Protection Controller Software package from the Software Download page. You can access the user interface, when the controller installation is complete.

   Log in to the controller services instance to monitor, manage, and control the device.

2. Perform the following base configurations such as ACL, UDF, hw-module, NetFlow configuration, and SSH manually on the NCS 540 router:

   Configure UDF

```
router(config)#udf udf-gtp header outer l4 offset 12 length 4
```

The user-defined field, allows you to define a custom key by specifying the location and size of the field to match.

For example, this command helps in matching the TEID value in the GTP header which is a 4-byte value at the 12th offset from the outer L4 header (UDP L4 header).

Configure the hardware module or TCAM

```
router(config)#hw-module profile tcam format access-list ipv4 src-addr dst-addr src-port
 dst-port proto frag-bit enable-capture udf1 udf-gtp location <location>
```

Reload the router (as hw-module profile and UDF configuration is performed).

Configure Loopback

```
RP/0/RP0/CPU0:ios(config)#interface Loopback100
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 10.1.1.1 255.255.255.255
RP/0/RP0/CPU0:ios(config)#interface Loopback101
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 10.10.10.2 255.255.255.255
RP/0/RP0/CPU0:ios(config-if)#
```

Configure ACL

```
RP/0/RP0/CPU0:ios(config)#ipv4 access-list gtp
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 2000 permit udp any any eq 2152 capture
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 2010 permit ipv4 any any
```

Note Ensure that you configure the ACL name as *gtp*. This option is applicable only for Cisco IOS XR 7.7.1 or later.

For more information on implementing access lists and prefix lists, see Understanding Access Lists.

If there is any DDoS attack, the controller performs the mitigation action using the ACL rule automatically. The controller pushes the ACL deny rules to block the traffic coming with the DDoS attacker TEID values.

Note The GTP TEID value of 0x1 varies based on the GTP Tunnel ID.

The following is a sample configuration to deny the ACE rule that denies DDoS attacker traffic with TEID value of 0x1:

```
10 deny ipv4 any any udf udf-gtp 0x1 0xffffffff
```

The controller pushes the configuration to the router.

Configure SSH

```
router(config)#ssh server v2
router(config)#ssh server netconf
router(config)#netconf agent tty
router(config)#netconf-yang agent ssh
router(config)#netconf agent tty
!
router(config)#ssh timeout 120
router(config)#ssh server rate-limit 600
router(config)#ssh server session-limit 110
router(config)#ssh server v2
```

```
router(config)#ssh server vrf default
router(config)#ssh server netconf vrf default
```

To configure TPA (until 7.8.1), perform the following steps:

```
RP/0/RP0/CPU0:ios(config)#tpa
RP/0/RP0/CPU0:ios(config-tpa)#vrf default
RP/0/RP0/CPU0:ios(config-tpa-vrf)#east-west Loopback101
RP/0/RP0/CPU0:ios(config-tpa-vrf)#address-family ipv4
RP/0/RP0/CPU0:ios(config-tpa-vrf-afi)#default-route mgmt
RP/0/RP0/CPU0:ios(config-tpa-vrf-afi)#update-source dataports Loopback100
RP/0/RP0/CPU0:ios(config-tpa-vrf-afi)#
```

To configure TPA from 7.9.1 or later on NCS 540, perform the following steps:

```
RP/0/RP0/CPU0:ios(config)#linux networking
RP/0/RP0/CPU0:ios(config-lnx-net)#vrf default
RP/0/RP0/CPU0:ios(config-lnx-vrf)#east-west Loopback101
RP/0/RP0/CPU0:ios(config-lnx-vrf)#address-family ipv4
RP/0/RP0/CPU0:ios(config-lnx-af)#default-route software-forwarding
RP/0/RP0/CPU0:ios(config-lnx-af)#source-hint default-route interface MgmtEth0/RP0/CPU0/0
RP/0/RP0/CPU0:ios(config-lnx-af)#
```

3. Reload the router (as the hw-module profile configuration is performed).
4. On the NCS 540 router, check the device connection to the DDoS controller using the **ping** command.

```
RP/0/RP0/CPU0:Router#ping 10.105.237.54
Thu Jun  1 07:16:43.654 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.105.237.54 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
RP/0/RP0/CPU0:Router#bash
Thu Jun  1 07:16:53.024 UTC
[Router:~]$ping 10.105.237.54
PING 10.105.237.54 (10.105.237.54) 56(84) bytes of data.
64 bytes from 10.105.237.54: icmp_seq=1 ttl=63 time=1.73 ms
64 bytes from 10.105.237.54: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 10.105.237.54: icmp_seq=3 ttl=63 time=1.27 ms
64 bytes from 10.105.237.54: icmp_seq=4 ttl=63 time=1.75 ms
^C
--- 10.105.237.54 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.270/1.510/1.751/0.230 ms
[Router:~]$
```

5. Add device details on the controller panel and ensure that all the three indicators (Deployment, Container, and Configuration) are green.

   For more information on installing the DDoS controller, see the DDoS Edge Protection Installation guide.

For more information on the DDoS Edge Protection, see Cisco Secure DDoS Edge Protection Data Sheet.

Verify DDoS Edge Protection Application Configuration for GTP Traffic

You can also verify if the DDoS controller pushes the CLI to the device using the following **show running-config** commands on the device:

```
RP/0/RP0/CPU0:Router#show running-config appmgr
Thu Jun  1 07:33:36.741 UTC
appmgr
 application esentryd
```

```
  activate type docker source esentryd-cisco-20230431633 docker-run-opts "-p 10000:10000/tcp
 -p 5005:5005/udp --env-file /harddisk:/ENV_6478443711ac6830700d1aeb --net=host"
 !
!

RP/0/RP0/CPU0:Router#show running-config flow monitor-map DetectPro_Monitor_IPV4
Thu Jun  1 07:34:34.236 UTC
flow monitor-map DetectPro_Monitor_IPV4
 record ipv4 gtp
 option filtered
 exporter DetectPro_GPB
 cache entries 1000000
 cache timeout active 1
 cache timeout inactive 1
 cache timeout rate-limit 100000
!

RP/0/RP0/CPU0:Router#show running-config flow exporter-map DetectPro_GPB
Thu Jun  1 07:35:10.417 UTC
flow exporter-map DetectPro_GPB
 version protobuf
 !
 transport udp 5005
 source TenGigE0/0/0/16
 destination 10.1.1.2
!

RP/0/RP0/CPU0:Router#show running-config interface tenGigE 0/0/0/16
Thu Jun  1 07:35:25.778 UTC
interface TenGigE0/0/0/16
 shutdown
 flow ipv4 monitor DetectPro_Monitor_IPV4 sampler DetectPro_SMPL ingress
 ipv4 access-group gtp ingress
!

RP/0/RP0/CPU0:Router#show appmgr application-table
Thu Jun  1 07:36:21.692 UTC
Name     Type   Config State Status
-------- ------ ------------ ------------------------------------------------
esentryd Docker  Activated   Up 8 minutes
RP/0/RP0/CPU0:Router#
```

Protect IP Traffic from DDoS Attacks

Table 3: Feature History Table

Feature Name	Release Information	Description
Protect IP Traffic from DDoS Attacks	Release 7.11.1	Cisco Secure Distributed Denial-of-Service (DDoS) Edge Protection solution protects the IP traffic in a service provider's edge network from DDoS attacks.You can mitigate any DDoS attacks at the ingress points and minimize the impact of such attacks on your network and applications running on it. This solution deploys a centralized controller that manages a distributed network of edge detectors that analyze and mitigate threats across networks.and helps mitigate them.

The DDoS edge protection supports DDoS detection of both IPv4 and IPv6 traffic. You can choose the interface on which the traffic should be monitored. When the protection software solution is implemented, it filters the IPv4 or IPv6 traffic flow and detects DDoS attacks.

Once a DDoS attack is detected, the DDoS Edge Protection Controller pushes the mitigation action to the router through the detector.

Supported Hardware

Cisco Secure DDoS edge protection is supported on the following hardware:

- N540-ACC-SYS (16GB)
- N540X-ACC-SYS (16GB)
- N540-24Z8Q2C-SYS (32GB)
- N540X-16Z4G8Q2C-D
- N540X-16Z4G8Q2C-A
- N540X-16Z8Q2C-D
- N540-28Z4C-SYS-D
- N540-28Z4C-SYS-A
- N540X-12Z16G-SYS-D
- N540X-12Z16G-SYS-A
- N540-12Z20G-SYS-D
- N540-12Z20G-SYS-A

Guidelines for installing DDoS edge protection

To ensure the DDoS edge protection capabilities are effective, these guidelines must be followed:

- Configure the management interface to reach the DDoS controller IP address.
- Manually configure the base ACL, UDF, NetFlow, and SSH configurations.

  For more information, see Install and Configure DDoS Edge Protection for IP Traffic, on page 9.
- Reload the router as a hw-module profile configuration is being performed.

Restrictions of DDoS edge protection

To ensure DDoS edge protection is configured and managed effectively, the following restrictions must be observed:

- Only default VRF configuration is supported and is limited to the management port. To ensure smooth communication between the Docker and the controller, make sure to set up the management port exclusively in the default VRF.

Install and Configure DDoS Edge Protection for IP Traffic

You can install the DDoS Edge Protection application through the DDoS edge protection controller. Perform the following:

1. Install and download the DDoS Edge Protection Controller Software package from the Software Download page. You can access the user interface, when the controller installation is complete.

   Log in to the controller services instance to monitor, manage, and control the device.
2. Perform the following base configurations such as ACL, UDF, hw-module, NetFlow configuration, and SSH manually on the router:

   Configure UDF

```
RP/0/RP0/CPU0:ios(config)#udf udf-ident header outer l3 offset 4 length 2
RP/0/RP0/CPU0:ios(config)#udf udf-chksum header outer l4 offset 16 length 2
RP/0/RP0/CPU0:ios(config)#udf udf-seqnum header outer l4 offset 4 length 4
```

   The user-defined field, allows you to define a custom key by specifying the location and size of the field to match.

   Configure the hardware module or TCAM

```
RP/0/RP0/CPU0:ios(config)#hw-module profile tcam format access-list ipv4 src-addr dst-addr
 src-port dst-port proto tcp-flags packet-length frag-bit precedence enable-capture
ttl-match udf1 udf-chksum udf2 udf-seqnum udf3 udf-ident
RP/0/RP0/CPU0:ios(config)#hw-module profile tcam format access-list ipv6 src-port dst-addr
 dst-port next-hdr tcp-flags payload-length ttl-match
```

   Reload the router (as hw-module profile and UDF configuration is performed).

   Configure Loopback

```
RP/0/RP0/CPU0:ios(config)#interface Loopback100
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 15.1.1.2 255.255.255.255
```

```
RP/0/RP0/CPU0:ios(config)#interface Loopback101
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 17.1.1.2 255.255.255.255
RP/0/RP0/CPU0:ios(config-if)#
```

Configure Netflow

```
//Configuring Monitor Map
RP/0/RP0/CPU0:ios(config)#flow monitor-map DetectPro_Monitor_IPV6
RP/0/RP0/CPU0:ios(config)# record ipv6 extended
RP/0/RP0/CPU0:ios(config)#exporter DetectPro_GPB
RP/0/RP0/CPU0:ios(config)# cache entries 1000000
RP/0/RP0/CPU0:ios(config)#cache entries active 1
RP/0/RP0/CPU0:ios(config)#cache entries inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout rate-limit 1000000
!
RP/0/RP0/CPU0:ios(config)#flow monitor-map DetectPro_Monitor_IPV4
RP/0/RP0/CPU0:ios(config)# record ipv4 extended
RP/0/RP0/CPU0:ios(config)#exporter DetectPro_GPB
RP/0/RP0/CPU0:ios(config)# cache entries 1000000
RP/0/RP0/CPU0:ios(config)#cache entries active 1
RP/0/RP0/CPU0:ios(config)#cache entries inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout rate-limit 1000000
!
//Configuring Exporter Map
RP/0/RP0/CPU0:ios(config)#flow exporter-map DetectPro_GPB
RP/0/RP0/CPU0:ios(config)#version protobuf
RP/0/RP0/CPU0:ios(config)#transport udp 5005
RP/0/RP0/CPU0:ios(config)#source TenGigE0/0/0/16
RP/0/RP0/CPU0:ios(config)#destination 15.1.1.2
!
//Configuring Sampler Map
RP/0/RP0/CPU0:ios(config)#sampler-map DetectPro_NFv9
RP/0/RP0/CPU0:ios(config)#random 1 out-of 100
!
```

Configure ACL

```
RP/0/RP0/CPU0:ios(config)#ipv4 access-list myACL
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 1301 permit ipv4 any any
!
RP/0/RP0/CPU0:ios(config)#ipv4 access-list myACL
RP/0/RP0/CPU0:ios(config-ipv6-acl)# 1301 permit ipv6 any any
!
```

For more information on implementing access lists and prefix lists, see Understanding Access-List.

If there is any DDoS attack, the controller performs the mitigation action using the ACL rule automatically.

The following is a sample configuration to deny DDoS attacker traffic using user defined ACE rule:

```
1 deny udp any eq 19 host 45.0.0.1 eq 0 packet-length eq 128 ttl eq 64
2 deny tcp any host 45.0.0.1 eq www match-all -established -fin -psh +syn -urg
packet-length eq 60 ttl eq 64
1301 permit ipv4 any any
```

The controller pushes the configuration to the router.

Configure SSH

```
RP/0/RP0/CPU0:ios(config)#ssh server v2
RP/0/RP0/CPU0:ios(config)#ssh server netconf
RP/0/RP0/CPU0:ios(config)#netconf agent tty
RP/0/RP0/CPU0:ios(config)#netconf-yang agent ssh
!
```

```
RP/0/RP0/CPU0:ios(config)#ssh timeout 120
RP/0/RP0/CPU0:ios(config)#ssh server rate-limit 600
RP/0/RP0/CPU0:ios(config)#ssh server session-limit 110
RP/0/RP0/CPU0:ios(config)#ssh server vrf default
RP/0/RP0/CPU0:ios(config)#ssh server netconf vrf default
```

To configure TPA, perform the following steps:

```
RP/0/RP0/CPU0:ios(config)#linux networking
RP/0/RP0/CPU0:ios(config-lnx-net)#vrf default
RP/0/RP0/CPU0:ios(config-lnx-vrf)#east-west Loopback101
RP/0/RP0/CPU0:ios(config-lnx-vrf)#address-family ipv4
RP/0/RP0/CPU0:ios(config-lnx-af)#default-route software-forwarding
RP/0/RP0/CPU0:ios(config-lnx-af)#source-hint default-route interface Loopback100
```

Note TPA configuration is required for the following platforms:

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

3. Reload the router (as the hw-module profile configuration is performed).
4. Check the device connection to the DDoS controller using the **ping** command.

```
RP/0/RP0/CPU0:ios#ping 10.105.237.54
Thu Jun  1 07:16:43.654 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.105.237.54 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
RP/0/RP0/CPU0:Router#bash
Thu Jun  1 07:16:53.024 UTC
[Router:~]$ping 10.105.237.54
PING 10.105.237.54 (10.105.237.54) 56(84) bytes of data.
64 bytes from 10.105.237.54: icmp_seq=1 ttl=63 time=1.73 ms
64 bytes from 10.105.237.54: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 10.105.237.54: icmp_seq=3 ttl=63 time=1.27 ms
64 bytes from 10.105.237.54: icmp_seq=4 ttl=63 time=1.75 ms
^C
--- 10.105.237.54 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.270/1.510/1.751/0.230 ms
[Router:~]$
```

5. Add device details on the controller panel and ensure that all the three indicators (Deployment, Container, and Configuration) are green.

   For more information on installing the DDoS controller, see the DDoS Edge Protection Installation guide.

For more information on the DDoS Edge Protection, see Cisco Secure DDoS Edge Protection Data Sheet.

Verify DDoS Edge Protection Application Configuration for IP Traffic

You can also verify if the DDoS controller pushes the CLI to the device using the following **show running-config** commands on the device:

```
RP/0/RP0/CPU0:Router#show running-config appmgrThu Dec 21 11:03:31.287 UTC
appmgr
application esentryd
activate type docker source esentryd-cisco-2310011873
docker-run-opts --env-file /misc/app_host/appmgr/config/esentryd/ENV_6581715a4b9d15b8a9803513
 --network host
!
!
```

```
RP/0/RP0/CPU0:Router#show flow monitor DetectPro_Monitor_IPV4 cache location 0/0/CPU0
Thu Nov 16 06:13:38.066 UTC
Cache summary for Flow Monitor DetectPro_Monitor_IPV4:
Cache size:                         1000000
Current entries:                          0
Flows added:                     2243884200
Flows not added:                          0
Ager Polls:                      2243884200
  - Active timeout                        0
  - Inactive timeout                      0
  - Immediate                             0
  - TCP FIN flag                          0
  - Emergency aged                        0
  - Counter wrap aged                     0
  - Total                        2243884200
Periodic export:
  - Counter wrap                          0
  - TCP FIN flag                          0
Flows exported                   2243884200


Matching entries:                         0
!
```

```
RP/0/RP0/CPU0:Router#show flow monitor DetectPro_Monitor_IPV6 cache location 0/0/CPU0
Thu Nov 16 06:13:43.734 UTC
Cache summary for Flow Monitor DetectPro_Monitor_IPV6:
Cache size:                         1000000
Current entries:                          0
Flows added:                          59971
Flows not added:                          0
Ager Polls:                           94437
  - Active timeout                    59971
  - Inactive timeout                      0
  - Immediate                             0
  - TCP FIN flag                          0
  - Emergency aged                        0
  - Counter wrap aged                     0
  - Total                             59971
Periodic export:
  - Counter wrap                          0
  - TCP FIN flag                          0
Flows exported                        59971


Matching entries:                         0
```

```
RP/0/RP0/CPU0:Router#show  flow exporter DetectPro_GPB location 0/0/CPU0
Thu Nov 16 06:13:58.059 UTC
Flow Exporter: DetectPro_GPB
Export Protocol: protobuf
Flow Exporter memory usage: 5265344
Used by flow monitors: DetectPro_Monitor_IPV4
                       DetectPro_Monitor_IPV6

Status: Disabled
```

```
Transport:   UDP
Destination: 15.1.1.2        (5005) VRF default
Source:      0.0.0.0         (54482)
Flows exported:                                    0 (0 bytes)
Flows dropped:                                     0 (0 bytes)

Templates exported:                                0 (0 bytes)
Templates dropped:                                 0 (0 bytes)

Option data exported:                              0 (0 bytes)
Option data dropped:                               0 (0 bytes)

Option templates exported:                         0 (0 bytes)
Option templates dropped:                          0 (0 bytes)

Packets exported:                           20355756 (27716506821 bytes)
Packets dropped:                                   0 (0 bytes)

Total export over last interval of:
  1 hour:                                         12 pkts
                                                1879 bytes
                                                  12 flows
  1 minute:                                        0 pkts
                                                   0 bytes
                                                   0 flows
  1 second:                                        0 pkts
                                                   0 bytes
                                                   0 flows
```

```
RP/0/RP0/CPU0:Router#show appmgr application-table
Thu Nov 16 06:13:58.059 UTC
Name     Type   Config State Status
-------- ------ ------------ ------------------------------------------------
esentryd Docker  Activated   Up 8 minutes
```

```
//Netflow and ACL
RP/0/RP0/CPU0:Router#show running-configuration interface tenGigE 0/0/0/19
Thu Dec 21 11:11:57.200 UTC
interface TenGigE0/0/0/19
flow ipv4 monitor DetectPro_Monitor_IPV4 sampler DetectPro_SMPL ingress
flow ipv6 monitor DetectPro_Monitor_IPV6 sampler DetectPro_SMPL ingress
ipv4 access-group myACL ingress
ipv6 access-group myACL ingress
```

Cisco secure DDoS edge protection

Distributed denial of service (DDoS) edge protection stops DDoS attacks at the network entry point.

Table 4: Feature History Table

Feature Name	Release Information	Description
Cisco secure DDoS edge protection	Release 25.2.1	You can now enable the router to detect DDoS attacks targeting MPLS traffic using DDoS edge protection. The router analyzes MPLS flows to identify malicious traffic patterns, ensuring the availability and performance of services traversing MPLS networks.

The Cisco secure DDoS edge protection software actively halts DDoS attacks at the network entry point, enabling immediate response to threats. Positioned at the network edge, it identifies DDoS threats directly on the router. This strategy minimizes network and application impact without affecting core bandwidth by avoiding backhaul of malicious traffic.

Starting from Cisco IOS XR Release 25.2.1, MPLS traffic is analyzed using the extracted information from the IPv4 and IPv6 payload to detect accurate DDoS attacks.

Supported Hardware

Cisco Secure DDoS edge protection is supported on the following hardware:

- N540-ACC-SYS (16GB)
- N540X-ACC-SYS (16GB)
- N540-24Z8Q2C-SYS (32GB)
- N540X-16Z4G8Q2C-D
- N540X-16Z4G8Q2C-A
- N540X-16Z8Q2C-D
- N540-28Z4C-SYS-D
- N540-28Z4C-SYS-A
- N540X-12Z16G-SYS-D
- N540X-12Z16G-SYS-A
- N540-12Z20G-SYS-D
- N540-12Z20G-SYS-A

Guidelines of DDoS edge protection

To ensure the DDoS edge protection capabilities are effective, these guidelines must be followed:

- Configure the management interface to reach the DDoS controller IP address.
- Manually configure the base ACL, UDF, NetFlow, and SSH configurations.

For more information, see Install and Configure DDoS Edge Protection for IP Traffic, on page 9.

- Reload the router as a hw-module profile configuration is being performed.

Restrictions of DDoS edge protection

To ensure DDoS edge protection is configured and managed effectively, these restrictions must be observed:

- Only default VRF configuration is supported and is limited to the management port. To ensure smooth communication between the Docker and the controller, make sure to set up the management port exclusively in the default VRF.
- The version protobuf of **`flow exporter-map`** is only supported for **`Monitor Map`** configured with **`record mpls ipv4-ipv6-fields`**.

Install and configure DDoS edge protection for MPLS traffic

Follow these steps to install and configure DDoS edge protection controller.

Procedure

Step 1 Install and download the DDoS edge protection controller software package from the Software Download page. You can access the user interface, when the controller installation is complete.

Step 2 Log in to the controller services instance to monitor, manage, and control the device.

Step 3 Perform the following base configurations such as ACL, UDF, hw-module, NetFlow configuration, and SSH manually on the router:

Configure UDF

```
RP/0/RP0/CPU0:ios(config)#udf udf-ident header outer l3 offset 4 length 2
RP/0/RP0/CPU0:ios(config)#udf udf-chksum header outer l4 offset 16 length 2
RP/0/RP0/CPU0:ios(config)#udf udf-seqnum header outer l4 offset 4 length 4
```

The user-defined field, allows you to define a custom key by specifying the location and size of the field to match.

Configure the hardware module or TCAM

```
RP/0/RP0/CPU0:ios(config)#hw-module profile tcam format access-list ipv4 src-addr dst-addr src-port
 dst-port proto tcp-flags packet-length frag-bit precedence enable-capture ttl-match udf1 udf-chksum
 udf2 udf-seqnum udf3 udf-ident
RP/0/RP0/CPU0:ios(config)#hw-module profile tcam format access-list ipv6 src-port dst-addr dst-port
 next-hdr tcp-flags payload-length ttl-match
```

Reload the router (as hw-module profile and UDF configuration is performed).

Configure Loopback on the router

```
RP/0/RP0/CPU0:ios(config)#interface Loopback100
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 15.1.1.2 255.255.255.255
RP/0/RP0/CPU0:ios(config)#interface Loopback101
RP/0/RP0/CPU0:ios(config-if)# ipv4 address 17.1.1.2 255.255.255.255
RP/0/RP0/CPU0:ios(config-if)#
```

Configure Netflow on the router

```
//Configuring Monitor Map
RP/0/RP0/CPU0:ios(config)#flow monitor-map DetectPro_Monitor_IPV6
RP/0/RP0/CPU0:ios(config)# record ipv6 extended
RP/0/RP0/CPU0:ios(config)#exporter DetectPro_GPB
RP/0/RP0/CPU0:ios(config)# cache entries 1000000
RP/0/RP0/CPU0:ios(config)#cache entries active 1
RP/0/RP0/CPU0:ios(config)#cache entries inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout rate-limit 1000000
!
RP/0/RP0/CPU0:ios(config)#flow monitor-map DetectPro_Monitor_IPV4
RP/0/RP0/CPU0:ios(config)# record ipv4 extended
RP/0/RP0/CPU0:ios(config)#exporter DetectPro_GPB
RP/0/RP0/CPU0:ios(config)# cache entries 1000000
RP/0/RP0/CPU0:ios(config)#cache entries active 1
RP/0/RP0/CPU0:ios(config)#cache entries inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout inactive 1
RP/0/RP0/CPU0:ios(config)#cache timeout rate-limit 1000000
!
//Configuring Exporter Map
RP/0/RP0/CPU0:ios(config)#flow exporter-map DetectPro_GPB
RP/0/RP0/CPU0:ios(config)#version protobuf
RP/0/RP0/CPU0:ios(config)#transport udp 5005
RP/0/RP0/CPU0:ios(config)#source TenGigE0/0/0/16
RP/0/RP0/CPU0:ios(config)#destination 15.1.1.2
!
//Configuring Sampler Map
RP/0/RP0/CPU0:ios(config)#sampler-map DetectPro_NFv9
RP/0/RP0/CPU0:ios(config)#random 1 out-of 100
!
```

Configure ACL on the router

```
RP/0/RP0/CPU0:ios(config)#ipv4 access-list myACL
RP/0/RP0/CPU0:ios(config-ipv4-acl)# 1301 permit ipv4 any any
!
RP/0/RP0/CPU0:ios(config)#ipv4 access-list myACL
RP/0/RP0/CPU0:ios(config-ipv6-acl)# 1301 permit ipv6 any any
!
```

For more information on implementing access lists and prefix lists, see Understanding Access-List.

If there is any DDoS attack, the controller performs the mitigation action using the ACL rule automatically.

The following is a sample configuration to deny DDoS attacker traffic using user defined ACE rule:

```
1 deny udp any eq 19 host 45.0.0.1 eq 0 packet-length eq 128 ttl eq 64
2 deny tcp any host 45.0.0.1 eq www match-all -established -fin -psh +syn -urg packet-length eq 60
ttl eq 64
1301 permit ipv4 any any
```

The controller pushes the configuration to the router.

Configure SSH

```
RP/0/RP0/CPU0:ios(config)#ssh server v2
RP/0/RP0/CPU0:ios(config)#ssh server netconf
RP/0/RP0/CPU0:ios(config)#netconf agent tty
RP/0/RP0/CPU0:ios(config)#netconf-yang agent ssh
!
RP/0/RP0/CPU0:ios(config)#ssh timeout 120
RP/0/RP0/CPU0:ios(config)#ssh server rate-limit 600
RP/0/RP0/CPU0:ios(config)#ssh server session-limit 110
```

```
RP/0/RP0/CPU0:ios(config)#ssh server vrf default
RP/0/RP0/CPU0:ios(config)#ssh server netconf vrf default
```

To configure TPA, perform the following steps:

```
RP/0/RP0/CPU0:ios(config)#linux networking
RP/0/RP0/CPU0:ios(config-lnx-net)#vrf default
RP/0/RP0/CPU0:ios(config-lnx-vrf)#east-west Loopback101
RP/0/RP0/CPU0:ios(config-lnx-vrf)#address-family ipv4
RP/0/RP0/CPU0:ios(config-lnx-af)#default-route software-forwarding
RP/0/RP0/CPU0:ios(config-lnx-af)#source-hint default-route interface Loopback100
```

Step 4 Reload the router (as the hw-module profile configuration is performed).

Step 5 Execute the **ping** command on the router and check the router connection to the DDoS controller

```
RP/0/RP0/CPU0:ios#ping 10.105.237.54
Thu Jun  1 07:16:43.654 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.105.237.54 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
RP/0/RP0/CPU0:Router#bash
Thu Jun  1 07:16:53.024 UTC
[Router:~]$ping 10.105.237.54
PING 10.105.237.54 (10.105.237.54) 56(84) bytes of data.
64 bytes from 10.105.237.54: icmp_seq=1 ttl=63 time=1.73 ms
64 bytes from 10.105.237.54: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 10.105.237.54: icmp_seq=3 ttl=63 time=1.27 ms
64 bytes from 10.105.237.54: icmp_seq=4 ttl=63 time=1.75 ms
^C
--- 10.105.237.54 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.270/1.510/1.751/0.230 ms
[Router:~]$
```

Step 6 Add device details on the controller panel and ensure that all the three indicators (Deployment, Container, and Configuration) are green.

For more information on installing the DDoS controller, see the DDoS edge protection installation guide.

For more information on the DDoS edge protection, see Cisco secure DDoS edge protection data sheet.

Verify DDoS edge protection configuration for MPLS traffic

Follow these steps to verify if the DDoS edge protection configuration is applied and active on the controller.

Procedure

Step 1 Execute the **show running-config appmgr** command on the router to verify the appmgr configuration.

```
RP/0/RP0/CPU0:Router#show running-config appmgr
appmgr
application esentryd
activate type docker source esentryd-cisco-2310011873
docker-run-opts --env-file /misc/app_host/appmgr/config/esentryd/ENV_6581715a4b9d15b8a9803513 --network
 host
```

```
!
!
```

Step 2 Execute the **show running-config** command on the router to check the monitor map that is automatically created.

```
Router#show flow monitor mon_mpls_ipv4_ipv6 cache format record location 0/RP0/CPU0
Cache summary for Flow Monitor mon_mpls_ipv4_ipv6:
Cache size:                         1000000
Current entries:                          0
Flows added:                            963
Flows not added:                          0
Ager Polls:                              83
  - Active timeout                      963
  - Inactive timeout                      0
  - Immediate                             0
  - TCP FIN flag                          0
  - Emergency aged                        0
  - Counter wrap aged                     0
  - Total                               963
Periodic export:
  - Counter wrap                          0
  - TCP FIN flag                          0
Flows exported                          963
!
```

Step 3 Execute the **show flow exporter** command on the router to check the exporter map that is automatically created.

```
Router#show  flow exporter
exporter  exporter-map
Router#show  flow exporter exp_mpls_ipv4_ipv6 location 0/RP0/CPU0
Flow Exporter: exp_mpls_ipv4_ipv6
Export Protocol: protobuf
Flow Exporter memory usage: 5265480
Used by flow monitors: mon_mpls_ipv4_ipv6

Status: Normal
Transport:   UDP
Destination: 15.1.1.2        (5005) VRF default
Source:      17.1.1.1        (54341)
Flows exported:                                  963(159519 bytes)
Flows dropped:                                     0 (0 bytes)

Templates exported:                                0 (0 bytes)
Templates dropped:                                 0 (0 bytes)

Option data exported:                              0 (0 bytes)
Option data dropped:                               0 (0 bytes)

Option templates exported:                         0 (0 bytes)
Option templates dropped:                          0 (0 bytes)

Packets exported:                                122 (159519 bytes)
Packets dropped:                                   0 (0 bytes)

Total export over last interval of:
  1 hour:                                         92 pkts
                                                119950 bytes
                                                   727 flows
  1 minute:                                       122 pkts
                                                159519 bytes
                                                   963 flows
  1 second:                                         0 pkts
                                                    0 bytes
                                                    0 flows
```

Step 4 Execute the **show appmgr application-table** command on the router to check the status of docker application.

```
RP/0/RP0/CPU0:Router#show appmgr application-table
Thu Nov 16 06:13:58.059 UTC
Name     Type   Config State Status
-------- ------ ------------ ------------------------------------------------
esentryd Docker  Activated   Up 8 minutes
```