Cisco Secure DDoS Edge Protection

Table 1: Feature History Table

Feature Name	Release Information	Description
Cisco Secure DDoS Edge Protection	Release 7.10.1	Cisco Secure DDoS Edge Protection solution provides protection from Denial-of-Service (DDoS) attacks and helps to mitigate them. DDoS Edge Protection solution helps you to: • Reduce the total cost of ownership for the DDoS solution by reducing the overall scrubbing capacity requirement which in turn reduces the overall power consumption, cooling, and other maintenance costs. • Improve customer satisfaction and helps in achieving SLAs due to the reduced attack detection and response time.

Cisco Secure DDoS Edge Protection is a software solution that stops DDoS attacks at the ingress side of the service provider network edge on the NCS 540 platform.

With the help of the DDoS Edge Protection solution, you can detect the DDoS attacks and perform mitigation actions on the router. For the detection services at the edge network, you must configure the following entities:

- DDoS Edge Protection Controller—Manages and monitors the Detector docker application and mitigates the attacks. The controller manages a distributed network of edge detectors, analyzes the detection trends across the network, and orchestrates the cross-network visibility and mitigation. The controller also delivers a complete system management lifecycle for the entire service.
- DDoS Edge Protection Detector—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.

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.

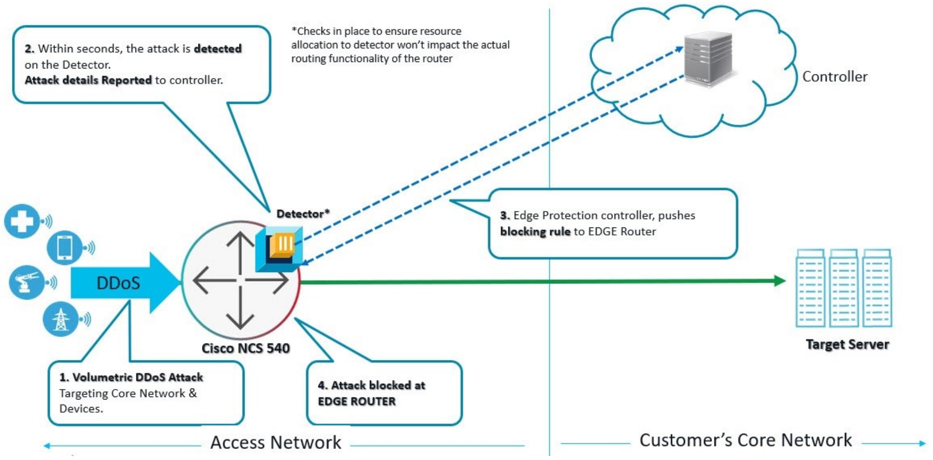
This whole process is performed through an Access Control List (ACL) configuration. A unique GTP flow is identified with a unique Tunnel Endpoint Identifier (TEID) present in the GTP header. The GTP header follows the UDP header. The identified flow that is associated with a TEID can be mitigated with 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 NCS 540 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.


2. Within seconds, the attack is detected on the Detector.
Attack details Reported to controller.
*Checks in place to ensure resource allocation to detector won't impact the actual routing functionality of the router
Controller
Detector*
3. Edge Protection controller, pushes blocking rule to EDGE Router
DDoS
Cisco NCS 540
Target Server
1. Volumetric DDoS Attack Targeting Core Network & Devices.
4. Attack blocked at EDGE ROUTER
Access Network
Customer's Core Network

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, 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
- N540H-FH-AGG-SYS
- N540-FH-CSR-SYS

Install and Configure DDoS Edge Protection

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

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#
```