# Cisco Secure DDoS Edge Protection

***Table 1: Feature History Table***

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Secure DDoS Edge Protection | Release 7.11.1 | Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])<br><br>We have now moved distributed denial-of-service (DDoS) protection to the network edge, ensuring 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.<br><br>A centralized controller manages DDoS mitigation capabilities using information from a collection of detectors deployed on the routers. These detectors analyze IPv4 and IPv6 traffic in real-time to identify DDoS attacks. Upon detection, the controller enforces deny ACLs to block malicious traffic while allowing legitimate traffic.<br><br>This local inspection enhances visibility, speeds up response times, and optimizes the network without the need for additional hardware or attack traffic redirection. |

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 and counteracts DDoS threats directly on the router. This strategy minimizes network and application impact without affecting core bandwidth by avoiding backhaul of malicious traffic.

The DDoS Edge Protection solution helps you detect DDoS attacks and take mitigation actions on the router. To enable detection services at the core network, 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.

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/IPv6 traffic flow and detects DDoS attacks.

Once a DDoS attack is detected, the DDoS Edge Protection Controller initiates a mitigation action, specifying the necessary steps to counteract the attack. This includes enabling traffic classification (TC) as part of the mitigation measures, implementation of rate limiting and so on.

### Supported Routers

Cisco Secure DDoS Edge Protection is supported on the following hardware:

- NCS-55A1-48Q6H
- NCS-55A1-48Q6H-SE
- NCS-55A1-48Q-DTC
- NCS-57D2-18DD-S
- NCS-57C3-MOD-S
- NCS-57C3-MOD-SE-S
- NCS-55A1-36H-SE-S
- NCS-55A1-36H-DTC
- NCS-55A1-36H-GLE
- NCS-55A1-36H-S
- NCS-55A2-MOD-SE-S
- NCS-55A2-MOD-HD-S
- NCS-55A2-MOD-SYS
- NCS-55A2-MOD-HX-S
- NCS-55A2-MOD-SE-H-S
- NCS-55A1-24H
- NCS-57B1-6D24H-S
- NCS-57B1-5D24H-SE

- NCS-5501
- NCS-5501-SE
- NCS-55A1-24Q6H-S
- NCS-55A1-24Q-DTCR
- NCS-55A1-24Q-RPHY
- NCS-55A1-24Q6H-SS
- NCS-57C1-48Q6D-S
- NCS-5502-SE
- NCS-5502-U100

### Benefits of Cisco Secure DDoS Edge Protection

- Stops DDoS attacks at the network ingress
- Requires no additional hardware or facilities such as power, rack space, and cooling
- Requires no changes to the architecture
- Avoids the need to overprovision network facilities such as links and routers to account for attack traffic
- Prevents backhauling of malicious traffic
- Minimizes network outages and optimizes the end-user experience, and
- Meets low-latency application requirements.



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

# Restrictions of DDoS Edge Protection Solution

- Only IPv4 and IPv6 traffic is supported.

- 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

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:

3. Configure a user-defined field (UDF) on the router.

```
Router(config)#udf udf-ident header outer l3 offset 4 length 2
Router(config)#udf udf-chksum header outer l4 offset 16 length 2
Router(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.

4. 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 tcp-flags packet-length frag-bit precedence enable-capture ttl-match
udf1 udf-chksum udf2 udf-seqnum udf3 udf-ident
Router(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).

5. Configure a Loopback on the router.

```
Router(config)#interface Loopback100
Router(config-if)# ipv4 address 15.1.1.2 255.255.255.255
Router(config-if)# exit
Router(config)#interface Loopback101
Router(config-if)# ipv4 address 17.1.1.2 255.255.255.255
Router(config-if)#commit
```

6. Configure an ACL on the router.

```
Router(config)#ipv4 access-list myACL
Router(config-ipv4-acl)# 1301 permit ipv4 any any
Router(config-ipv4-acl)# exit
Router(config)#ipv6 access-list myACL
Router(config-ipv6-acl)# 1301 permit ipv6 any any
Router(config-ipv6-acl)#exit
Router(config)#commit
```

   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
```

Configuration updates are sent by the controller to the router.

7. Configure SSH on the router.

```
Router(config)#ssh server v2
Router(config)#ssh server netconf
Router(config)#netconf agent tty
Router(config-netconf-tty)#netconf-yang agent ssh
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
```

8. Configure TPA on the router.

```
Router(config)#tpa
Router(config-tpa)#linux networking
Router(config-tpa-vrf)#vrf default
Router(config-tpa-vrf)#east-west Loopback101
Router(config-tpa-vrf)#address-family ipv4
Router(config-tpa-vrf-afi)#default-route software-forwarding
Router(config-tpa-vrf-afi)#source-hint default-route interface Loopback100
Router(config-tpa-vrf-afi)#
```

**Note** TPA configuration is not required for NCS 5700 routers.

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

10. Execute the **ping** command on the router and check the router connection to the DDoS controller.

```
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:~]$
```

11. Enter the details of the device into the DDoS edge protection controller panel and verify that the Deployment, Container, and Configuration indicators all display green.

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

The controller automatically performs the following netflow configuration on the router:

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

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

# Verify DDoS Edge Protection Application Configuration

To ensure the DDoS controller has applied the configuration to the device, check the active configuration on the router.

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
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"
 !
!
```

2. Execute the **show flow monitor** command on the router to check the monitor map that is automatically created.

```
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
```

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

```
RP/0/RP0/CPU0:Router#show  flow exporter
exporter  exporter-map
RP/0/RP0/CPU0:tortin#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
```

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
RP/0/RP0/CPU0:Router#
```