Cisco Secure DDoS Edge Protection

Table 1: Feature History Table

Feature Name	Release Information	Description
Cisco Secure DDoS Edge Protection	Release 24.3.1	You can now block malicious traffic at peering edge routers, stopping distributed denial-of-service (DDoS) attacks at the network entry point and ensuring constant service availability and reliability in your network. 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. 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.

Components of Cisco Secure DDoS Edge Protection

The Cisco Secure DDoS Edge Protection consists of these components:

- A highly available centralized controller that manages a collection of detectors deployed on routers. The controller can be cloud-based or on-premises. Key functions of the controller include
  - managing the container lifecycle for detectors

- configuring and editing detector profiles and security settings
- checking detector health, displaying real-time attack forensics and threat intelligence analyses
- controlling DDoS attack mitigation at the network ingress point
- providing real-time and historical event reporting, and
- operational control and incident response.

- A collection of detectors that are deployed on edge or peering routers. The detector is a resource-efficient application container for real-time DDoS detection deployed on routers and managed by the centralized controller. It analyzes IPv4 and IPv6 traffic on each ingress interface to identify DDoS attacks as they occur.

Upon detecting a DDoS attack, the centralized controller promptly begins mitigation. The mitigation includes enforcing a deny ACL to block the attack traffic while still allowing legitimate traffic to pass through.

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.

Supported Platform Variants

These line cards support Cisco Secure DDoS Edge Protection.

- A9K-16X100GE-TR
- A99-32X100GE-TR
- A9K-4HG-FLEX-TR
- A9K-4HG-FLEX-SE
- A99-4HG-FLEX-TR
- A99-4HG-FLEX-SE
- A9K-8HG-FLEX-TR
- A9K-8HG-FLEX-SE
- A9K-20HG-FLEX-TR
- A9K-20HG-FLEX-SE
- A99-32X100GE-X-TR

- A99-32X100GE-X-SE
- A99-10X400GE-X-TR, and
- A99-10X400GE-X-SE.

These fixed-port routers support Cisco Secure DDoS Edge Protection.

- ASR 9902 and
- ASR 9903.

Unsupported Platform Variants

These line cards don't support DDoS Edge Protection.

- A9K-8X100G-LB-SE
- A9K-8X100G-LB-TR
- A9K-8X100GE-SE
- A9K-8X100GE-TR
- A9K-4X100GE-SE
- A9K-4X100GE-TR
- A9K-400G-DWDM-TR
- A9K-MOD400-SE
- A9K-MOD400-TR
- A9K-MOD200-SE
- A9K-MOD200-TR
- A9K-24X10GE-1G-SE
- A9K-24X10GE-1G-TR
- A9K-48X10GE-1G-SE
- A9K-48X10GE-1G-TR
- A9-12X100GE
- A9-8X100GE-SE, and
- A9-8X100GE-TR

- Restrictions of Cisco Secure DDoS Edge Protection, on page 3
- Install and Configure DDoS Edge Protection, on page 4

Restrictions of Cisco Secure DDoS Edge Protection

- The DDoS Edge Protection supports only IPv4 and IPv6 traffic.

- The DDoS Edge Protection does not support tunnel traffic.
- The system supports only the default VRF configuration, and it applies solely to the management port. For effective communication between the Docker and the controller, you must configure the management port to operate within the default VRF exclusively. This setup guarantees that the Docker can reliably interact with the controller without any network interruptions.

Install and Configure DDoS Edge Protection

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

Before you begin

- Configure the management interface to reach the DDoS controller IP address.
- Perform the base configuration of the Access Control List (ACL), NetFlow, and Secure Shell (SSH) settings.

Step 1 Download and install 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.

Step 2 Configure a Loopback on the router.

Example:

```
Router(config)# interface Loopback100
Router(config-if)# ipv4 address 209.165.200.225 255.255.255.224
Router(config-if)# exit
Router(config)# interface Loopback101
Router(config-if)# ipv4 address 209.165.200.226 255.255.255.224
Router(config-if)#commit
```

Step 3 Configure an ACL on the router.

Example:

```
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.

Here is a sample configuration to deny DDoS attacker traffic using a user-defined ACL 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 sends the configuration updates to the router.

Step 4 Configure SSH on the router.

Example:

```
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
Router(config)#commit
```

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

Example:

```
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:~]$ping 10.105.237.54
PING 10.105.237.54 (10.105.237.54) 56(84) bytes of data.
64 bytes from 10.105.237.54: icmp_seq=1 ttl=63 time=1.73 ms
64 bytes from 10.105.237.54: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 10.105.237.54: icmp_seq=3 ttl=63 time=1.27 ms
64 bytes from 10.105.237.54: icmp_seq=4 ttl=63 time=1.75 ms
^C
--- 10.105.237.54 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.270/1.510/1.751/0.230 ms
[Router:~]$
```

Step 6 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.

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-ver)#transport udp 5005
Router(config-fem)#source TenGigE0/0/0/16
Router(config-fem)#destination 209.165.200.225
Router(config-fem)#exit
//Configuring Sampler Map
Router(config)#sampler-map DetectPro_NFv9
Router(config-sm)#random 1 out-of 100
```

For more information on installing the DDoS controller, see the Cisco Secure 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

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

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

Example:

```
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 "--env-file
/harddisk:/ENV_6478443711ac6830700d1aeb --net=host"
 !
!
```

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

Example:

```
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
```

Example:

```
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
```

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

Example:

```
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
```

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

Example:

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