Implementing Cisco ASR 9000 vDDoS Mitigation

This module provides information about how to implement Cisco ASR 9000 vDDoS mitigation to protect network infrastructures and resources from distributed denial-of-service (DDoS) attacks.

- Cisco ASR 9000 vDDoS Mitigation Overview, on page 1
- Information about Implementing Cisco ASR 9000 vDDoS Mitigation, on page 2

Cisco ASR 9000 vDDoS Mitigation Overview

Distributed denial-of-service (DDoS) attacks target network infrastructures or computer services resources. The primary goal of DDoS attacks is to deny legitimate users access to a particular computer or network resources, which results in service degradation, loss of reputation, and irretrievable data loss. DDoS Mitigation is the process of detecting increasingly complex and deceptive assaults and mitigating the effects of the attack to ensure business continuity and resource availability.

The Arbor Peakflow solution protects customer networks by mitigating undesirable traffic caused by DDoS attacks. It comprises a number of functions as well as a set of hardware devices that implement those functions. Peakflow SP means the control components such as monitoring the network, detecting attacks, and coordinating an attack response. Peakflow SP runs on SP appliances or in virtual machines. Peakflow Threat Management System (TMS) or Peakflow SP TMS is the data plane component to remove DDoS attacks.

Using Netflow and BGP, Arbour Peakflow solution monitors the network ingress points to build a base line for network behavior and traffic patterns. It will then perform ongoing monitoring to detect anomalies and flag them as potential attacks. These potential attacks are presented to network operations via a GUI, email, or SNMP which allows a range of actions to be taken, including initiating a response or marking an event as a false alarm. If there is an attack, the Arbor Peakflow solution redirects all traffic for the destination through the TMS which can remove unwanted traffic and clean the traffic as effectively as possible without blocking valid connections. The new path to the TMS where the traffic from the original path is diverted is called off-ramp traffic path. The path from the TMS egress interface to the original destination of the traffic where the clean traffic is sent is called on-ramp traffic path.

Cisco has partnered with Arbor Networks to deliver DDoS attack mitigation capabilities on Cisco ASR 9000 Series routers by integrating the Threat Management System (TMS) DDoS mitigation functionality to the Cisco ASR 9000 router. The TMS will be implemented on the ASR 9000 VSM (Virtualized Services Module) hosted in the ASR 9000 chassis.

Information about Implementing Cisco ASR 9000 vDDoS Mitigation

There are different ways to implement DDoS mitigation. In the centralized model, a dedicated part of the network will be the scrubbing center (TMS) to clean the traffic and the traffic to the victim will be diverted to the scrubbing center. In the distributed approach, scrubbers are installed at the edge of the network. In the mixed approach, scrubbers will be present at the edge and the scrubbing center will handle the additional traffic. You should choose the mitigation strategy suitable for your network.

The mechanisms to create an effective diversion and re-injection path include BGP Flowspec, injecting a more specific route by diverting traffic to the victim in to the TMS, tunneling traffic to the TMS and from the TMS, putting the malicious and clean traffic in different VRFs or VPNs, and using ACL Based Forwarding (ABF) to steer traffic. These tools can be used in different combinations like tunnel diversion & VRF re-injection, diversion using a /32 prefix and VPN re-injection, and /32 diversion and GRE tunnel re-injection to implement a range of routing designs.

Prerequisites for Implementing Cisco ASR 9000 vDDoS Mitigation

These prerequisites are required to implement DDoS Mitigation support on the Cisco ASR 9000 Series Router.

- You need Cisco IOS XR software release 5.3.0 or later installed on the Cisco ASR 9000 Series Router.
- ASR 9000 Series Route Switch Processor 440 (RSP 440) or above is required.
- You need to insert the VSM card in the Cisco ASR 9000 Series Router.
- TFTP should be enabled on the CIsco ASR 9000 Series Router.
- You need to uninstall any pre-existing virtual service on the VSM card.
- You need to pair the ASR 9000 vDDoS solution with Arbor Peakflow SP.

Restrictions for Implementing Cisco ASR 9000 vDDoS Mitigation

The following restriction apply for implementing Cisco ASR 9000 vDDoS mitigation.

- Only one vDDoS instance is supported per VSM card.

Configuring Cisco ASR 9000 vDDoS Mitigation

This section provides information about the configuration tasks required for implementing ASR 9000 vDDoS mitigation. This section only provides information about Cisco ASR9000 specific configuration. For Arbor Peakflow SP configuration, see *Arbor Networks SP and Threat Management System (TMS) User Guide* .

Installing Cisco ASR 9000 vDDoS Software

Arbor Networks TMS and ArbOS are packaged together with configuration files in an Open Virtualization Archive (.ova) file. Installation of ASR 9000 vDDoS software on the VSM card consists of the following steps:

1. Copy the OVA file that contains Arbor TMS and Arbor OS to the ASR 9000 router using TFTP or FTP. Use the correct path and filename for your build. When you are prompted for the remote host, type the IP address of the remote host. For destination file name, press enter.

```
RP/0/RSP0/CPU0:router# copy tftp:/Peakflow-TMS-8.0.0-EKU0.ova disk0:
```

2. Enable the virtual service.

```
RP/0/RSP0/CPU0:router# virtual-service enable
RP/0/RSP0/CPU0:router# commit
```

3. Install the TMS VSM software.

```
RP/0/RSP0/CPU0:router# virtual-service install name tms3 package
/disk0:/Peakflow-TMS-8.0.0-EKU0.ova node 0/1/CPU0
```

   The installation may take 10-12 minutes to complete.

4. Check the progress of the installation process by using the **show virtual-service list** command.

```
RP/0/RSP0/CPU0:router# show virtual-service list
```

   If installation is in process, this command shows the status as installing. When installation is complete, you can rerun this show command to verify that the virtual service is listed as installed.

Configuring Interfaces for TMS Mitigation

Once you install the VSM module, twelve virtual Network Interface Card (vNIC) interfaces are available between the VSM module and the router. You can use some of these vNIC interfaces for TMS mitigation and others for management of the TMS virtual instance. The mitigation interfaces are bundled into a single logical interface. The logical interface can be divided into subinterfaces for diversion and re-injection of traffic.

1. Map vNIC interfaces on the router to TMS interfaces on the VSM card.

```
RP/0/RSP0/CPU0:router(config)# virtual-service tms3
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/0
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/1
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/2
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/3
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/4
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/5
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/6
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/7
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/8
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/9
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/10
RP/0/RSP0/CPU0:router(config-virt-service)# vnic interface tenGigE 0/1/1/11
RP/0/RSP0/CPU0:router(config-virt-service)# commit
RP/0/RSP0/CPU0:router(config-virt-service)# activate
RP/0/RSP0/CPU0:router(config-virt-service)# commit
```

2. Check the progress of the activation process by using the **show virtual-service list** command.

```
RP/0/RSP0/CPU0:router# show virtual-service list
```

   Once the VM is activated, the status changes to activated.

3. Create ethernet bundle interface for mitigation interfaces 0-3 and 7-10.

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether  2
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.1.2.3 255.0.0.0
RP/0/RSP0/CPU0:router(config-if)# bundle load-balancing hash src-ip
RP/0/RSP0/CPU0:router(config-if)# exit
```

4. Add member interfaces to the ethernet bundle.

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/0
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/1
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/2
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/3
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit


RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/7
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/8
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/9
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit

RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/10
RP/0/RSP0/CPU0:router(config-if)# bundle-id 2 mode on
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit
```

5. Configure TMS management interfaces 5 and 6.

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/5
RP/0/RSP0/CPU0:router(config-if)# ip address 10.2.1.10 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/6
RP/0/RSP0/CPU0:router(config-if)# ip address 10.2.1.5 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# load interval 30
RP/0/RSP0/CPU0:router(config-if)# commit
```

6. Set up unused interfaces 4 and 11.

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/4
RP/0/RSP0/CPU0:router(config-if)# shut down
RP/0/RSP0/CPU0:router(config-if)# commit
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/1/1/11
RP/0/RSP0/CPU0:router(config-if)# shut down
RP/0/RSP0/CPU0:router(config-if)# commit
```

7. Configure subinterfaces for diversion and re-injection.

```
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 2.100
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 100
RP/0/RSP0/CPU0:router(config-subif)# ipv4 address 10.1.2.100 255.255.255.240
RP/0/RSP0/CPU0:router(config-subif)#  bundle load-balancing hash src-ip
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 2.101
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 101
RP/0/RSP0/CPU0:router(config-subif)# vrf onramp
RP/0/RSP0/CPU0:router(config-subif)# ipv4 address 10.1.2.130 255.255.255.240
```

Uninstalling the TMS Virtual Service

Before installing the TMS software on VSM card, you need to remove any existing TMS virtual service on the VSM card. Perform the followings steps to remove any instances of the TMS virtual service.

1. Enable the virtual services on the VSM card.

   ```
   RP/0/RSP0/CPU0:router(config)# virtual-service enable
   RP/0/RSP0/CPU0:router(config)# commit
   ```

2. Use the **show virtual-service list** command to see the list of virtual services available on the VSM card.

   ```
   RP/0/RSP0/CPU0:router# show virtual-service list
   ```

3. If the TMS virtual instance is listed, de-activate the TMS virtual instance.

   ```
   RP/0/RSP0/CPU0:router(config)# no virtual-service tms3
   RP/0/RSP0/CPU0:router(config)# commit
   ```

4. Uninstall the TMS virtual instance.

   ```
   RP/0/RSP0/CPU0:router# virtual-service uninstall name tms3 node 0/1/CPU0
   ```