Threat Management Service

In This Section

This section describes how to configure the Threat Management Service applications.

Topics include:

TMS Service Introduction

The ISA-TMS supports routed redirect mode on IOM3, which means that traffic based on destination IP address (under attack) is filtered (scrubbed) by a variety of DDoS filtering rules provided by 3rd party code from Arbor Networks.

When a DDoS attack is detected by the Arbor Networks CP (based on cflowd counters) a notification is send to the 7750 SR CPM. This is the trigger for the 7750 SR CPM to attract the traffic under attack via the advertisement of a route with prefix the destination IP address under attack and with next-hop the scrubber. This process is called off-ramping.

At that point all destination traffic to the IP address under attack is forwarded to the 7750 SR where:

- DDoS traffic is dropped in the ISA-TMS
- Clean (non DDoS) traffic is returned back into the network. This process is called on-ramping.

Configuration Guidelines and Example

TMS Image Location

The TMS images should be stored in the same location as the other images (cpm.tim, iom.tim, etc). This is to where the BOF points.

The name of the file is peakflow-tms.tim

Configuration Example For TMS Interfaces on the SR OS

```
configure service vprn 1
         tms-interface "mda-1-1" create
             address 20.folk.43/32
             description "tms-1-1"
             port 1/1
             password "password=arbor zone-secret=admin"
         exit
     exit

     configure router
        interface "itfToArborCP"
            address 10.12.0.1/24
            port 3/2/4
        exit
     exit

     configure router policy-options
            policy-statement "exporttmsgrt"
                entry 1
                    from
                        protocol vpn-leak
                    exit
                    action accept
                    exit
                exit
                entry 2
                    from
                        protocol tms
                    exit
                    action accept
                    exit
                exit
            exit
     exit
```

Follow the usage guidelines listed below:

- Use **mda-type isa-tms**
- The tms-interface address 20.12.0.43/32 should be configured on the ArborSP via "Administration> Peakflow Appliances"
- The port is the card/mda ID
- The tms-interface address 20.12.0.43/32 results in a static-route in the Base instance

```
*A:Dut-C# show router route-table 20.12.0.43/32

===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Prefix[Flags]                            Type    Proto    Age         Pref
      Next Hop[Interface Name]                                   Metric
-------------------------------------------------------------------------------
20.12.0.43/32                                 Remote  Static   00h08m49s   5
       vprn1:mda-1-1                                                1
-------------------------------------------------------------------------------
```

- The tms-interface zone-secret=admin should match with the zone-secret used on the ArborSP
- The tms-interface password=arbor should be used as password during SSH/Telnet to TMS
- The tms-interface ipv6. This is a prerequisite for adding IPv6 TMS routes and scrubbing IPv6 traffic
- The connectivity SR/ArborSP goes via port 3/2/4 interface itfToArborCP (10.12.0.1) to an interface (10.12.0.2) of the ArborSP. On the ArborSP, to reach the TMS, a static route like this is needed: 20.12.0.0/24 with next-hop 10.12.0.1 On the SR, to reach the ArborSP a static-route like this is needed (with 138.203.71.202 the management IP address of the ArborSP (eth0): static-route 138.203.71.202/32 next-hop 10.12.0.2
- Use the same NTP server on both SR/ArborSP and enable the NTP server (because the CPM is the NTP server for isa-tms)
- A policy (in this example “exporttmsgrt”) is needed to leak TMS routes to BGP
- If you want to Telnet/ping to TMS, first enable the following services:
  - → ssh 127.1.mda.slot -l admin router management
  - → ip access add ping all 0.0.0.0/0
  - → ip access add telnet all 0.0.0.0/0
  - → ip access commit
  - → services telnet start
  - → config write
- On the ArborSP

Use a TMS cluster which holds the relevant isa-tms’ Administration> Mitigation> TMS-ISA Clusters

Put the TMS cluster in a TMS group Administration> Mitigation> TMS Groups

Use the TMS Group in the mitigation rule (Mitigation> Threat Management>Add> TMS Appliances)

Dynamic Control of IP Filter Entries

The following requirement will enhance the performance and scale of DDoS protection via a tight integration between the Arbor TMS DDoS scrubbing application and the 7750 highly scalable IP filters.

The Arbor TMS application uses a wide variety of methods for identifying specific flows that are part of a network or application Denial of Service attack. These techniques include network and application behavior analysis as well as specific packet-based content detection.

Once a specific flow has been identified as part of the attack, one of the common methods of mitigation includes host-based (source-IP), IP blacklisting. Instead of continuing to analyze every packet of that flow up to Layer 7 analysis, based on the initial detection TMS will use IP host-based blacklisting to temporarily block traffic from that source toward the destination under attack.

This feature adds the ability to have the TMS application within the 7750 signal the 7750 through the ALU API controlling highly scalable IP filters for hardware-based, source-IP blacklisting in order to significantly enhance the scale and performance of the blacklisting function.

Note: R6.0p4 or later of Arbor TMS is required to support this feature on the 7750.

This feature exemplifies how Arbor Networks and ALU continue to improve the overall DDoS detection and mitigation function.