How To – Configure BGP on Cyberoam using the CLI Console

Applicable Version: 10.00 onwards

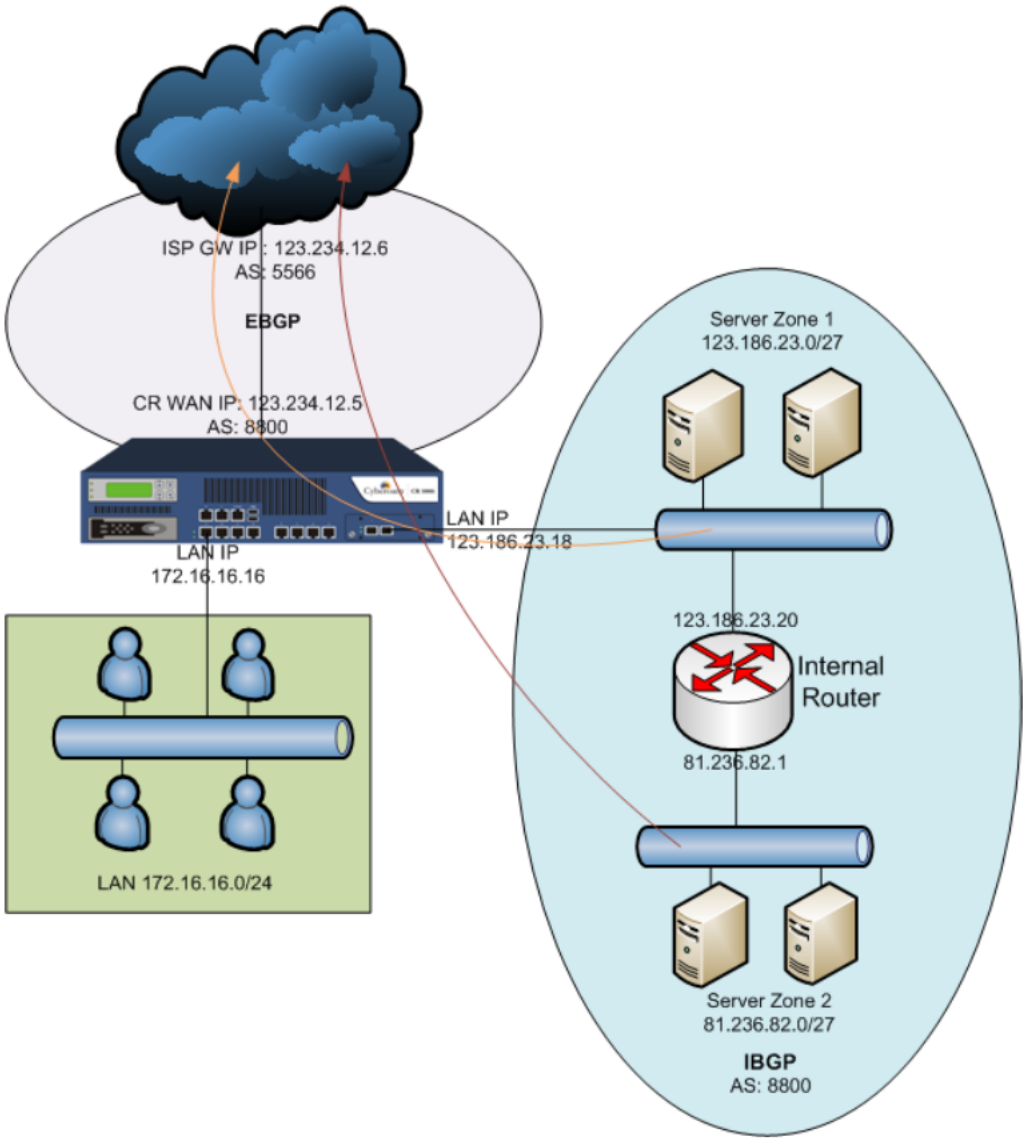
Overview

Border Gateway Protocol (BGP) is the protocol which makes core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems (AS), which is a collection of networks controlled by a common or single administrator. BGP allows the Internet to be a truly decentralized system.

Cyberoam can be configured to communicate with neighbouring ASs using BGP. This article describes how you can configure BGP in Cyberoam.

To configure BGP using the Web Admin Console, refer article Configure BGP in Cyberoam using Web Admin Console.

Scenario



As shown in the diagram, the entire network forms an AS 8800. Configure Cyberoam to act as a BGP peer or neighbour to AS 5566 and, hence, publish servers in Zone1 (123.186.23.0/27) and Zone 2 (81.236.82.0/27) over the Internet.

Prerequisites

Prior to configuration, obtain the following details from your ISP:

- BGP AS Number
- Update Source IP
- Number of Hops

Configuration

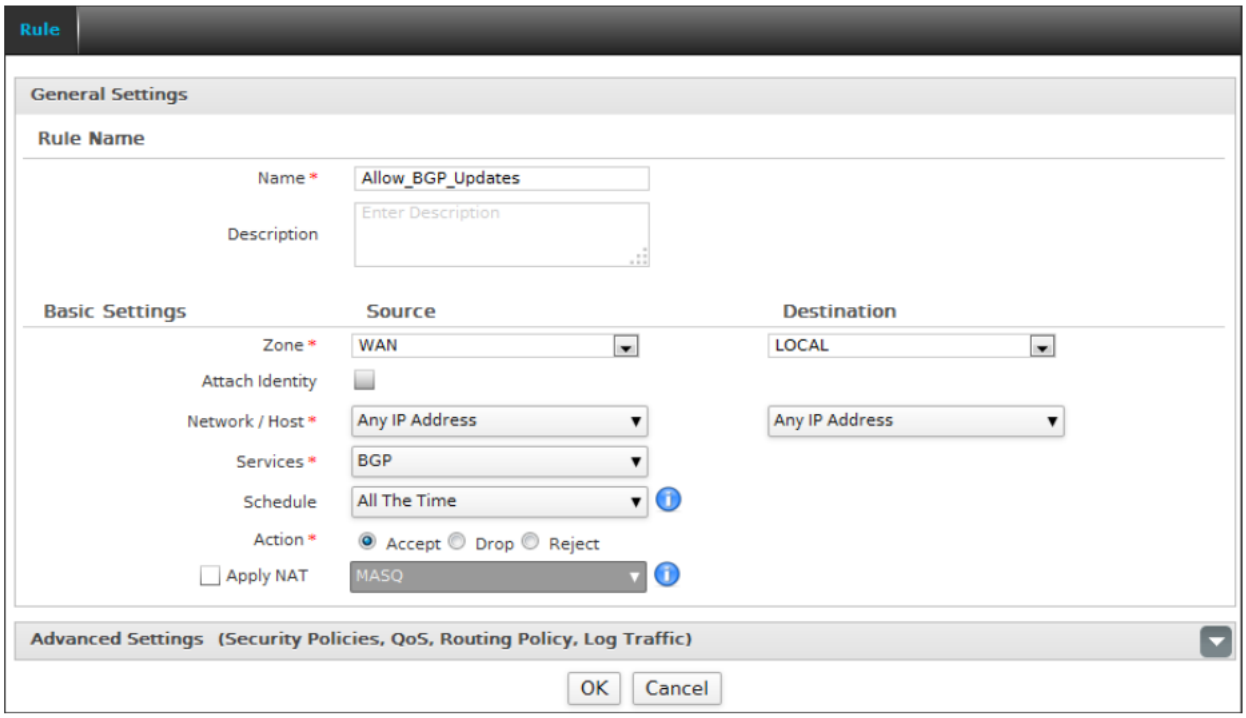
To publish servers over the Internet using BGP, configure Cyberoam as an External BGP peer with the ISP router and an Internal BGP peer with the internal router.

Configuring Cyberoam as EBGP Peer

To Configure Cyberoam as an EBGP peer, follow the steps given below.

Step 1: Create Firewall Rule to Allow Cyberoam to Receive BGP Updates

Go to **Firewall > Rule > Rule** create a new rule which allows BGP traffic from WAN to LOCAL Zones, as shown below.



Step 2: Configure Cyberoam as EBGP Peer

1. Login to Cyberoam CLI Console.
2. From the Main Menu, choose **Option 3 – Route Configuration**.
3. From the Router Management Menu, choose **Option 1 – Configure Unicast Routing**.
4. From the Unicast Routing Configuration Menu, choose **Option 3 – Configure BGP**.
5. In the BGP command prompt, fire the following commands at the console prompt:

- **Enable BGP configuration:**

  bgp> enable

  bgp# conf t

- **Declare Router-ID to identify neighbours:**

  bgp(config)# router bgp 8800

  bgp(config-router)#bgp router-id 123.234.12.5

- **Set peer parameters**

  bgp(config-router)#neighbor 123.234.12.6 remote-as 5566

  bgp(config-router)#neighbor 123.234.12.6 update-source 123.234.12.5

  Here, Update – Source command is used so that the Neighbour receives update from only the IP 123.234.12.5.

- **Publish Server Zones to the ISP**

  bgp(config-router)#network 123.186.23.0 mask 225.255.255.224

  bgp(config-router)#network 123.234.12.4/30

- **Apply Peer Authentication (Optional)**

  bgp(config-router)#neighbor 123.234.12.6 password 12345

  Where, ''12345'' is the plain text password.

  Note:
  Similar authentication/password must be configured at the peer device.

- **Save all configuration**

  bgp(config-router)#write

  The above steps configure Cyberoam as an EBGP peer to the ISP router. To check whether the EBGP peer has been successfully created, execute the following command:

  bgp(config-router)#do show ip bgp summary

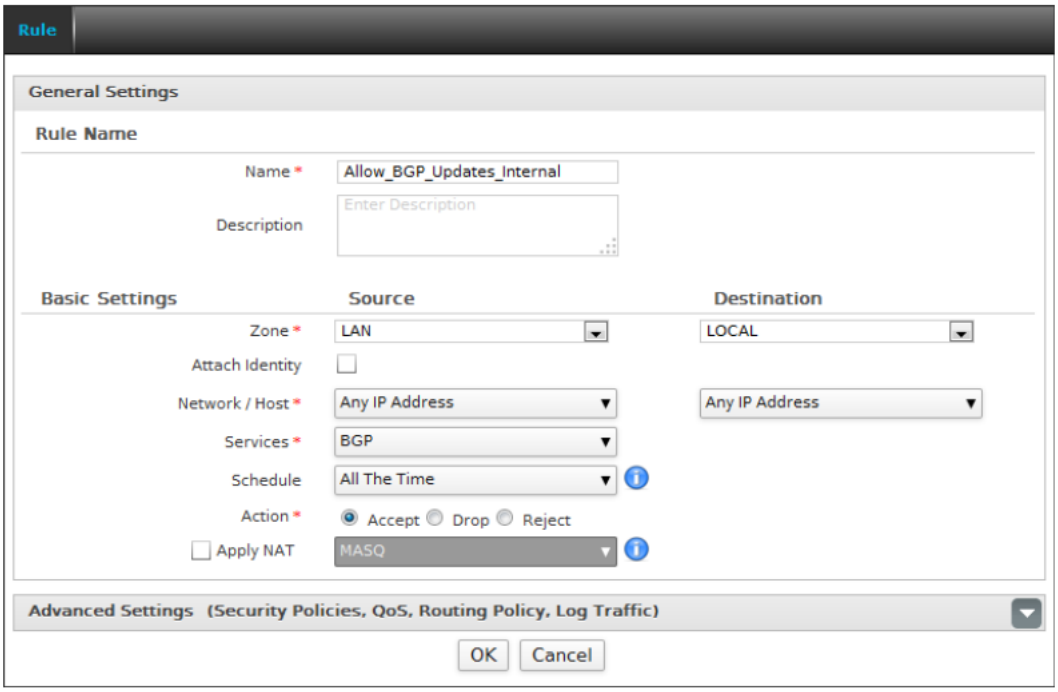
```
bgp# show ip bgp summary
BGP router identifier 172.16.16.16, local AS number 8800
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
123.234.12.6    4  5566     415     484        0    0    0 05:47:03        1
```

Configuring Cyberoam as IBGP Peer

To Configure Cyberoam as an IBGP peer, follow the steps given below.

Step 1: Create Firewall Rule to Allow BGP Updates on LAN Interface

Go to **Firewall > Rule > Rule** create a new rule which allows BGP traffic from LAN to LOCAL Zones.



Step 2: Configure Cyberoam as IBGP Peer

1. Login to Cyberoam CLI Console.
2. From the Main Menu, choose **Option 3 – Route Configuration**.
3. From the Router Management Menu, choose **Option 1 – Configure Unicast Routing**.
4. From the Unicast Routing Configuration Menu, choose **Option 3 – Configure BGP**.
5. In the BGP command prompt, fire the following commands.

- **Enable BGP configuration**

```
bgp> enable

bgp# conf t
```

- **Set peer parameters**

```
bgp(config)# router bgp 8800

bgp(config-router)#neighbor 123.186.23.20 remote-as 8800

bgp(config-router)#neighbor 123.186.23.20 update-source 123.186.23.18
```

- **Apply Peer Authentication (Optional)**

  bgp(config-router)#neighbor 123.186.23.20 password 12345

  Where, ''12345'' is the plain text password.

  Note:
  Similar authentication/password must be configured at the peer device.

The above steps configure Cyberoam as an IBGP peer to the Internal router.

To check whether the IBGP peer has been successfully created, execute the following command:

bgp(config-router)#do show ip bgp summary

```
bgp(config-router)# do sh ip bgp summary
BGP router identifier 123.234.12.5, local AS number 8800
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
123.186.23.20   4  8800      14      15        0    0    0 00:11:49        2
123.234.12.6    4  5566     147     152        0    0    0 02:25:59        1

Total number of neighbors 2
```

Step 3: Configure Internal Router to form Cyberoam's IBGP Peer

Here, we have shown the configuration of a Cisco router. Login to the router's CLI and fire the following commands

- **Enable BGP configuration**
  bgp> enable

  bgp# conf t

- **Declare Router-ID to identify neighbours**
  bgp(config)# router bgp 8800

  bgp(config-router)#bgp router-id 123.186.23.20

- **Declare server networks**

  R2(config-router)#net 81.236.82.0 mask 255.255.255.224

  R2(config-router)#net 123.186.23.0 mask 255.255.255.224

- **Set peer parameters**

  R2(config-router)#neighbor 123.186.23.18 remote-as 8800

```
R2(config-router)#neighbor 123.186.23.18 update-source 123.186.23.20
```

- **Apply Peer Authentication (Optional)**

```
bgp(config-router)#neighbor 123.186.23.18 password 12345
```

Where, ''12345'' is the plain text password.

- **Save all configuration**

```
bgp(config-router)#write
```

The above steps configure Cyberoam and the Internal Router as IBGP peers.

Document Version: 1.2 – 10 March, 2015