How to Configure BGP with Route Based VPN Using Unnumbered VTI on IPSO

27 March 2012
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=12295
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/27/2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Configure BGP with Route Based VPN Using Unnumbered VTI on IPSO ).
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
</tr>
<tr>
<td>How to Configure BGP with Route Based VPN Using Unnumbered VTI on IPSO</td>
</tr>
<tr>
<td>Objective</td>
</tr>
<tr>
<td>Supported Versions</td>
</tr>
<tr>
<td>Supported OS</td>
</tr>
<tr>
<td>Supported Appliances</td>
</tr>
<tr>
<td>Related Documentation and Assumed Knowledge</td>
</tr>
<tr>
<td>BGP with Route Based VPN Using Unnumbered VTI on IPSO</td>
</tr>
<tr>
<td>Configuring BGP with Route Based VPN Using Unnumbered VTI</td>
</tr>
<tr>
<td>Step 1: Configuring BGP</td>
</tr>
<tr>
<td>Step 2: Configuring a Local Encryption Domain</td>
</tr>
<tr>
<td>Step 3: Configuring Remote Security Gateway Object and Encryption Domain</td>
</tr>
<tr>
<td>Step 4: Configure a VPN Community</td>
</tr>
<tr>
<td>Step 5: Configuring Appropriate Access Rules</td>
</tr>
<tr>
<td>Step 6: Configuring the VPN Tunnel Interface (VTI)</td>
</tr>
<tr>
<td>Step 7: Configuring &quot;Inbound Route Filters&quot; and &quot;Redistributing Routes to BGP&quot;</td>
</tr>
<tr>
<td>Inbound Route Filter</td>
</tr>
<tr>
<td>Route Redistribution</td>
</tr>
<tr>
<td>Step 8: Configuring a Static route</td>
</tr>
<tr>
<td>Step 9: Verifying The configuration</td>
</tr>
<tr>
<td>Verification #1 fw monitor capturing traffic on interface tun0c0 (ifid=4)</td>
</tr>
<tr>
<td>Verification #2 From Clish</td>
</tr>
<tr>
<td>Verification #3 Seen in the Log Viewer (seen BGP traffic via tun0c0 interface)</td>
</tr>
</tbody>
</table>
How to Configure BGP with Route Based VPN Using Unnumbered VTI on IPSO

Objective

This document is a step-by-step guide to setting up BGP with Route Based VPN using unnumbered VTI on IPSO.

Supported Versions

This document covers all IPSO versions.

Supported OS

- All IPSO versions
- All Check Point versions

Supported Appliances

All IP series Appliances

Related Documentation and Assumed Knowledge

Network voyager Reference Guides (http://supportcenter.checkpoint.com)

BGP with Route Based VPN Using Unnumbered VTI on IPSO

Virtual Tunnel Interfaces (VTI) can be used with Check Point route-based VPNs. A VTI is a virtual interface to the encryption domain of the peer Gateway. Each VTI is associated with a single tunnel to a peer VPN Security Gateway. As with domain-based VPNs, the tunnel and its properties is defined by a VPN community linking the two gateways. The peer gateway is also configured with a corresponding VTI. The native IP routing mechanism on each gateway can then direct traffic into the tunnel just as it would for any other type of interface, and the traffic will be encrypted.
IPSO supports only unnumbered interfaces as VTIs. Local and remote IP addresses are not configured. Instead, the interface is associated with a proxy interface from which it inherits an IP address. Traffic that is initiated by the gateway and routed through the VTI has the proxy interface IP address as the source IP address.

If you want the source IP address to be an IP address not used on the system, you can create a loopback interface with the desired IP address and use it as the proxy interface.

## Configuring BGP with Route Based VPN Using Unnumbered VTI

### In This Section

- **Step 1: Configuring BGP**
- **Step 2: Configuring a Local Encryption Domain**
- **Step 3: Configuring Remote Security Gateway Object and Encryption Domain**
- **Step 4: Configure a VPN Community**
- **Step 5: Configuring Appropriate Access Rules**
- **Step 6: Configuring the VPN Tunnel Interface (VTI)**
- **Step 7: Configuring "Inbound Route Filters" and "Redistributing Routes to BGP"**
- **Step 8: Configuring a Static route**
- **Step 9: Verifying The configuration**

### Step 1: Configuring BGP

1. Configure EBGP. EBGP is the protocol used to transport information to other BGP enabled systems in different Autonomous Systems (AS). Verify that BGP peer status is showing "Established" on both routers without any VPN.


### BGP Configuration

- **Router ID:** [default: 172.25.252.10]
- **Autonomous System (AS) Number:** 300

### Configured Peer Groups

<table>
<thead>
<tr>
<th>Peer Group</th>
<th>Description</th>
<th>Local Address</th>
<th>Peer Address</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS200 External Group</td>
<td><a href="#">AS200 External Group</a></td>
<td>172.25.252.10</td>
<td><a href="#">AS200 External Group</a></td>
<td>Delete</td>
</tr>
</tbody>
</table>
2. Enable External BGP (EBGP) multi hop support if the BGP peers are across multiple hops. Connections between BGP enabled systems in different Autonomous Systems (ASs) are called EBGP connections. BGP enforces the rule that peer routers for EBGP connections need to be on a directly attached network. If the peer routers are multiple hops away from each other or if multiple links are between them, you can override this restriction by enabling the EBGP multihop feature.

3. To verify BGP peer status, run "show bgp peers" in clish:

```
IP290[admin]# clish -c "show bgp peers"
Flags: R - Peer restarted, W - Waiting for End-Of-RIB from Peer

PeerID        AS     Routes  ActRts  State             InUpds  OutUpds  Uptime
172.26.252.10  300    0       0      Established       0       0        00:04:50

IP290[admin]#
```

```
1280-10[admin]# clish -c "show bgp peers"
Flags: R - Peer restarted, W - Waiting for End-Of-RIB from Peer

PeerID        AS     Routes  ActRts  State             InUpds  OutUpds  Uptime
172.26.201.250 200    0       0      Established       0       0        00:05:59

1280-10[admin]#
```
Step 2: Configuring a Local Encryption Domain

Go to SmartDashboard and edit the local Security Gateway object.

1. Navigate to the topology section, and select 'Manually Defined' under the VPN Domain section.
2. Click "New" and create a 'Simple Group'.
3. Leave the group blank. The encryption domain of VTI based end points are left blank, as all traffic will be routed based on static routes added pointing to the VTIs. However, if you plan to create VPNs to Security Gateways of version lower than NGX, managed by this same Security Management (SmartCenter), you must define a proper encryption domain.

Step 3: Configuring Remote Security Gateway Object and Encryption Domain

1. Create the remote peer Security Gateway.
2. Under the topology section, again select 'Manually Defined' under the VPN Domain section.
3. Click "New" and create a 'Simple Group'.

![Step 2: Configuring a Local Encryption Domain](image-url)
4. Leave the group blank.
Step 4: Configure a VPN Community

Create a new Star/Meshed VPN Community and add the VPN peers to it. Make sure that the VPN Phase 1 and Phase 2 properties, and preshared secrets and other VPN properties are correct.

Step 5: Configuring Appropriate Access Rules

1. Create appropriate VPN access rules in the Security rule base.
2. Do not include the newly created VPN community under the VPN section of the security rule.
3. Install the security policy.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate_Netw</td>
<td>Corporate_Netw</td>
<td>Any</td>
<td>Any</td>
<td>accept</td>
<td>Log</td>
</tr>
</tbody>
</table>

Step 6: Configuring the VPN Tunnel Interface (VTI)

Note: The VTI may be added via Network voyager OR via the command line using the vpn shell.

To add the VTI via Network voyager:
1. Login to Network voyager and navigate to 'Config> Checkpoint Firewall-1 > FWVPN Configuration'.
2. Enter the name of the remote peer Security Gateway object, configured in SmartDashboard and select the interface which will proxy the connection. Click "Apply".
3. If you have done the above steps in order, you should now have a VTI created and showing a status of 'OK'.
4. Click "Save" to save your configuration.
5. Take a note of the interface name. You will need this in the next step.

**FWVPN Tunnel Configuration**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Active</th>
<th>Logical Name</th>
<th>Peer Gateway</th>
<th>IP Address</th>
<th>Destination</th>
<th>Encapsulation</th>
<th>Status</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>tun001</td>
<td>on</td>
<td>tun000</td>
<td>A111111</td>
<td>10.0.0.1</td>
<td></td>
<td>Unnumbered link</td>
<td>FWVPN</td>
<td>OK</td>
</tr>
</tbody>
</table>

**Step 7: Configuring "Inbound Route Filters" and "Redistributing Routes to BGP"**

Now configure "Redistributing Routes to BGP"

Route redistribution allows you to redistribute routes from one autonomous system into another autonomous system.

To configure BGP route redistribution:

1. Click Route Redistribution under Configuration > Routing in the tree view.
2. Click BGP Routes Based on AS under the Redistribute to BGP section.
3. Select XXX from the Redistribute to Peer AS drop-down list.
4. Select YYY from the From AS drop-down list; then click Apply.

This procedure enables route redistribution from AS YYY to AS XXX. By default, all routes that are excluded from being redistributed from AS YYY are redistributed to AS XXX.

Follow the same steps on each gateway at both end of the VTI tunnel.

**Inbound Route Filter:**

**Filter Inbound Routes by AS**

*Warning: Inbound Route Filtering by AS Number will not have effect for AS Groups that use Routemap for Import*

- 525 Filter BGP routes for AS 300: enable, disable

- LocalPref: [Field]
- Weight: [Field]

**Route Filters**

- All BGP routes from AS 300: Actions: accept, restrict

All routes are currently accepted unless restricted below.

- New IP prefix to import: [Field]
**Route Redistribution:**

**Redistribute routes from Interface Routes into BGP**

*Warning: Redistribution to BGP through Voyager will not have effect for AS Groups that use Reroutemaps for Export*

<table>
<thead>
<tr>
<th>Enable redistribute Interface Routes routes to AS100?</th>
<th>on</th>
<th>off</th>
</tr>
</thead>
</table>

**Routes:**

Export all interfaces into AS 300: on/off

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet</th>
<th>Metric</th>
<th>on/off</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0c0</td>
<td>10.207.141.39/24</td>
<td>on/off</td>
<td>Metric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth0c0</td>
<td>10.10.136/24</td>
<td>on/off</td>
<td>Metric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth0c0</td>
<td>10.207.106.45/24</td>
<td>on/off</td>
<td>Metric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eth0c0</td>
<td>10.10.136/24</td>
<td>on/off</td>
<td>Metric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>loop0c0</td>
<td>127.0.0.1/22</td>
<td>on/off</td>
<td>Metric</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 8: Configuring a Static route**

Configure a static route.

For example between AS200 (172.26.252.10) & AS200 (172.26.101.38)

On AS100 side, use the following static route

172.26.101.38 with 32 bit mask and select "logical name" for the "Gateway Type" - Apply.

Now for the "Gateway Type" select the "tun0c0" from the drop down menu.
Step 9: Verifying The configuration

Verification #1 fw monitor capturing traffic on interface tun0c0 (ifid=4)

lproxy[admin]# fw monitor -e 'accept ifid=4;'
monitor: getting filter (from command line)
monitor: compiling
monitorfilter:
Compiled OK.
monitor: loading
FW-1: monitor filter loaded
monitor: monitoring (control-C to stop)
tun0c0:I[91]: 10.207.101.38 -> 10.207.141.39 (TCP) len=91 id=61825 TCP: 1183 ->
179 ...PA. seq=d8465516 ack=6d7e04e7
tun0c0:o[72]: 10.207.141.39 -> 10.207.101.38 (TCP) len=72 id=44986 TCP: 179 ->
1183 ....A. seq=6d7e04e7 ack=d8465529
tun0c0:o[91]: 10.207.141.39 -> 10.207.101.38 (TCP) len=72 id=45003 TCP: 179 ->
1183 ....A. seq=6d7e04e7 ack=d8465529
tun0c0:I[72]: 10.207.101.38 -> 10.207.141.39 (TCP) len=72 id=61838 TCP: 1183 ->
179 ....A. seq=d8465529 ack=6d7e04fa
tun0c0:I[91]: 10.207.101.38 -> 10.207.141.39 (TCP) len=72 id=61868 TCP: 1183 ->
179 ....A. seq=d8465529 ack=6d7e04fa
tun0c0:o[72]: 10.207.141.39 -> 10.207.101.38 (TCP) len=72 id=45035 TCP: 179 ->
1183 ....A. seq=6d7e04fa ack=d846553c
tun0c0:o[91]: 10.207.141.39 -> 10.207.101.38 (TCP) len=72 id=45055 TCP: 179 ->
1183 ....A. seq=6d7e04fa ack=d846553c
tun0c0:I[72]: 10.207.101.38 -> 10.207.141.39 (TCP) len=72 id=61883 TCP: 1183 ->
179 ....A. seq=d846553c ack=6d7e050d
tun0c0:I[91]: 10.207.101.38 -> 10.207.141.39 (TCP) len=72 id=61906 TCP: 1183 ->
179 ....A. seq=d846553c ack=6d7e050d
tun0c0:o[72]: 10.207.141.39 -> 10.207.101.38 (TCP) len=72 id=45093 TCP: 179 ->
1183 ....A. seq=6d7e050d ack=d846554f

Verification #2 From Clish

From Router ID 10.207.141.39

NokiaIP260:106> show bgp peers
PeerID AS Routes ActRts State InUpds OutUpds Uptime
10.207.113.2 210 0 0 Established 0 2 03:12:56
10.207.101.38 300 1 1 Established 1 1 00:01:38
NokiaIP260:107>
NokiaIP260:107>

NokiaIP260:116> show route
Codes: C - Connected, S - Static, I - IGRP, R - RIP, B - BGP,
O - OSPF intraArea (IA - interArea, E - External, N - NSSA)
A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed
S 0.0.0.0/0 via 10.207.141.1, eth1c0, cost 0, age 951530
C 1.1.1.1/32 is directly connected, loop0c0
C 10.0.0.1/32 is directly connected, loop0c0
C 10.10.1/24 is directly connected, eth2c0
S 10.207.101.38/32 via , tun0c0, cost 0, age 563
B 10.207.101/24 via , tun0c0, cost -1, age 303
C 10.207.141/24 is directly connected, eth1c0
C 127.0.0.1/32 is directly connected, loop0c0
NokiaIP260:117>
From Router 10.207.101.38

NokiaIP380:103> show bgp peers

PeerID AS Routes ActRts State InUpds OutUpds Uptime
10.207.141.39 100 4 4 Established 1 1 00:01:22

NokiaIP380:104>

NokiaIP380:102> show route

Codes: C - Connected, S - Static, I - IGRP, R - RIP, B - BGP,
O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed

S 0.0.0.0/0 via 10.207.101.1, eth1c0, cost 0, age 7380
B 1.1.1.1/32 via , tun0c0, cost -1, age 410
B 10.0.0.1/32 via , tun0c0, cost -1, age 410
B 10.10.1/24 via , tun0c0, cost -1, age 410
C 10.207.101/24 is directly connected, eth1c0
S 10.207.141.39/32 via , tun0c0, cost 0, age 742
B 10.207.141/24 via , tun0c0, cost -1, age 410
C 127.0.0.1/32 is directly connected, loop0c0

NokiaIP380:103>

Verification #3 Seen in the Log Viewer (seen BGP traffic via tun0c0 interface):

On router 10.207.141.39 (Gateway "lproxy" - Interface tun0c0)

Number: 4526
Date: 17Mar2009
Time: 1:57:58
Interface: tun0c0
Origin: lproxy
Type: Log
Action: Decrypt
Service: BGP (179)
Source Port: 1183
Source: AJIP380
Destination: lproxy
Protocol: tcp
Rule: 1
Rule UID: {608AB0EA-5870-47F5-92E4-DA85D71C3661}
Current Rule Number: 1-Standard
Community: MyIntranet
Information: service_id: BGP
Encryption Scheme: IKE
Encryption Methods: ESP: AES-128 + MD5
VPN Peer Gateway: AJIP380
Subproduct: VPN
VPN Feature: VPN
Product: VPN-1 Power/UTM
SmartDefense Profile: Default_Protection
Policy Info: Policy Name: Standard
Created at: Mon Mar 16 18:07:33 2009
Installed from: lproxy
On router 10.207.101.38 (Gateway "AJIP380" - Interface tun0c0)

Number: 368
Date: 17Mar2009
Time: 2:06:59
Interface: tun0c0
Origin: AJIP380
Type: Log
Action: Decrypt
Service: BGP (179)
Source Port: 3571
Source: lproxy
Destination: AJIP380
Protocol: tcp
Rule: 1
Rule UID: {A6F36D22-829F-4724-A7BA-4A8DEF670BAF}
Current Rule Number: 1-Standard
Community: MyIntranet
Information: service_id: BGP
Encryption Scheme: IKE
Encryption Methods: ESP: AES-128 + MD5
VPN Peer Gateway: lproxy
Subproduct: VPN
VPN Feature: VPN
Product: VPN-1 Power/UTM
SmartDefense Profile: Default_Protection
Policy Info: Policy Name: Standard
Created at: Mon Mar 16 21:05:46 2009
Installed from: AJIP380