vbond-as-stun-server

**vpn 0 interface tunnel-interface vbond-as-stun-server**—Enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT (on vEdge routers only). When you configure this command, vEdge routers can exchange their public IP addresses and port numbers over private TLOCs.

With this configuration, the vEdge router uses the vBond orchestrator as a STUN server, so the router can determine its public IP address and public port number. (With this configuration, the router cannot learn the type of NAT that it is behind.) No overlay network control traffic is sent and no keys are exchanged over tunnel interface configured to the the vBond orchestrator as a STUN server. However, BFD does come up on the tunnel, and data traffic can be sent on it.

Because no control traffic is sent over a tunnel interface that is configured to use the vBond orchestrator as a STUN server, you must configure at least one other tunnel interface on the vEdge router so that it can exchange control traffic with the vSmart controller and the vManage NMS.

**vManage Feature Template**

For vEdge routers only:

Configuration ► Templates ► VPN Interface Cellular (for vEdge cellular wireless routers only)
Configuration ► Templates ► VPN Interface Ethernet
Configuration ► Templates ► VPN Interface PPP

---

**Command Hierarchy**

```
vpn 0
    Interface interface-name
        tunnel-interface
            vbond-as-stun-server
```

---

**Options**

None

---

**Operational Commands**

show running-config

---

**Example**

Configure two tunnel interfaces, one to use for the exchange of control traffic (ge0/2) and the other to allow the device to discover its public IP address and port number from the vBond orchestrator (ge0/1). Note that the **no allow-service**
**stun** command, which is configured by default on tunnel interfaces, pertains to allowing or disallowing the vEdge router to generate requests to a generic STUN server so that the device can determine whether it is behind a NAT and, if so, what kind of NAT it is and what the device's public IP address and public port number are.

```
vEdge(config-interface-ge0/1)# show full-configuration
vpn 0
 interface ge0/1
   ip address 10.0.26.11/24
   tunnel-interface
     encapsulation ipsec
     vbond-as-stun-server
     no allow-service bgp
     allow-service dhcp
     allow-service dns
     allow-service icmp
     no allow-service sshd
     no allow-service netconf
     no allow-service ntp
     no allow-service ospf
     no allow-service stun
     !
   !

vEdge(config-interface-ge0/1)# exit
vEdge(config-vpn-0)# exit
vEdge(config-tunnel-interface)# show full-configuration
vpn 0
 interface ge0/2
   tunnel-interface
     encapsulation ipsec
     color lte
     no allow-service bgp
     allow-service dhcp
     allow-service dns
     allow-service icmp
     no allow-service sshd
     no allow-service netconf
     no allow-service ntp
     no allow-service ospf
     no allow-service stun
     !
   !
```

---

**Release Information**

Command introduced in Viptela Software Release 16.3.

---

**Additional Information**

See the [Configuring Network Interfaces](https://sdwan-docs.cisco.com/Product_Documentation/Command_Reference/Configuration_Commands/vbond-as-stun-server) article for your software release.

[allow-service](https://sdwan-docs.cisco.com/Product_Documentation/Command_Reference/Configuration_Commands/vbond-as-stun-server)