How to Prefer Particular Uplink for Direct Internet Access

Contents

Introduction

This document describes how to prefer a particular interface for Direct Internet Access (DIA) with the help of vSmart data policy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of SD-WAN Policy Framework.

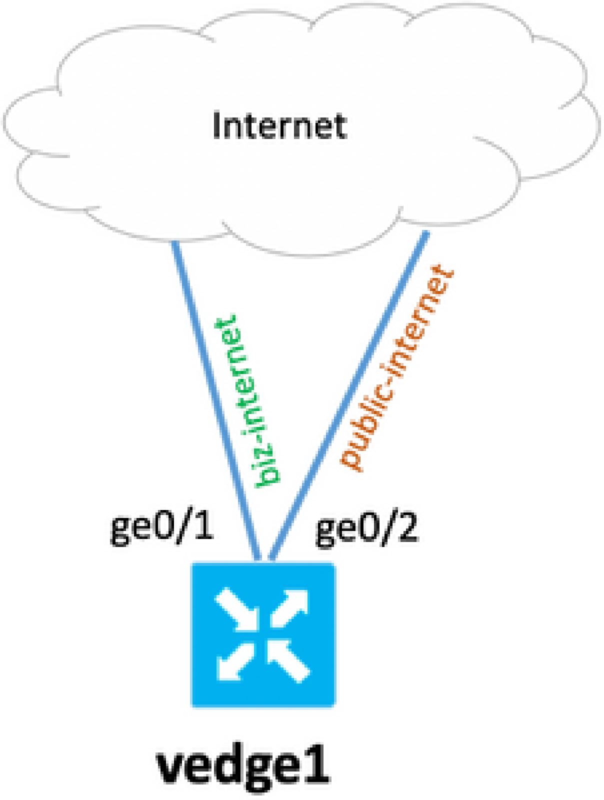
Components Used

The information in this document is based on vEdge router and vSmart controller.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

vEdge router has two uplink interfaces, with basic underlay and overlay configuration. The main aim is to prefer ge0/1 interface for all traffic to Internet host with address 203.0.113.137 from local subnet 192.0.2.0/24.

vEdge router configuration:

```
 interface ge0/1
  ip address 192.168.109.104/24
  nat
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
!
interface ge0/2
  ip address 192.168.110.104/24
  nat
  !
  tunnel-interface
   encapsulation ipsec
   color public-internet
!
 !
 ip route 0.0.0.0/0 192.168.109.10
 ip route 0.0.0.0/0 192.168.110.10
!
vpn 40
 ip route 0.0.0.0/0 vpn 0
```

vSmart controller configuration:

```
policy
 lists
  data-prefix-list SOURCE_PREFIX
   ip-prefix 192.0.2.0/24
  !
  data-prefix-list DESTINATION_PREFIX
   ip-prefix 203.0.113.137/32
  !
  site-list branch40
   site-id 40
  !
 !
policy
 data-policy FORCE_GE0_1
  vpn-list VPN_40
   sequence 100
    match
     source-data-prefix-list SOURCE_PREFIX
     destination-data-prefix-list DESTINATION_PREFIX
    !
    action accept
     nat use-vpn 0
     set
      local-tloc color biz-internet encap ipsec
     !
    !
   !
   default-action accept
  !
 !
apply-policy
 site-list branch40
  data-policy FORCE_GE0_1 from-service
 !
!
```

Verify

Use this section in order to confirm that your configuration works properly.

Before the policy was applied:

```
show policy service-path vpn 40 interface ge0/7 source-ip 192.0.2.222 dest-ip 203.0.113.137
protocol 6
Next Hop: Remote
Remote IP: 192.168.110.10, Interface ge0/2 Index: 6
```

Then activate policy on vSmart and ensure policy from vSmart is applied to vEdge:

```
vedge1# show policy from-vsmart
from-vsmart data-policy FORCE_GE0_1
 direction from-service
 vpn-list VPN_40
  sequence 100
   match
    source-data-prefix-list      SOURCE_PREFIX
    destination-data-prefix-list DESTINATION_PREFIX
   action accept
    nat use-vpn 0
    no nat fallback
    set
     local-tloc color biz-internet
     local-tloc encap ipsec
  default-action accept
from-vsmart lists vpn-list VPN_40
 vpn 40
from-vsmart lists data-prefix-list DESTINATION_PREFIX
 ip-prefix 203.0.113.137/32
from-vsmart lists data-prefix-list SOURCE_PREFIX
 ip-prefix 192.0.2.0/24
```

After the policy was applied:

```
show policy service-path vpn 40 interface ge0/7 source-ip 192.0.2.222 dest-ip 203.0.113.137
protocol 6
Next Hop: Remote
Remote IP: 192.168.109.10, Interface ge0/1 Index: 5
```

Also, you can see a connection in the NAT translation table:

```
vedge1# show ip nat filter nat-vpn 0 nat-ifname ge0/1 vpn 40 protocol tcp 192.0.2.222
203.0.113.137
ip nat filter nat-vpn 0 nat-ifname ge0/1 vpn 1 protocol tcp 192.0.2.222 203.0.113.137 61213 443
public-source-address 192.168.109.104
public-dest-address 203.0.113.137
public-source-port 61213
public-dest-port 443
filter-state established
idle-timeout 0:00:54:11
outbound-packets 12593
outbound-octets 1186104
inbound-packets 16601
inbound-octets 4576423
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.