Centralized Data Policy Configuration Examples

This article provides some straightforward examples of configuring centralized data policy to influence traffic flow across the Viptela domain and to configure a vEdge router to be an Internet exit point.

General Centralized Data Policy Example

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a vSmart controller and that after you commit the configuration, the policy itself is pushed to the affected vEdge routers.

Here we configure a simple data policy on the vSmart controller vm9:

```text
vm9# show running-config policy
policy
data-policy test-data-policy
    vpn-list test-vpn-list
        sequence 10
        match
            destination-ip 172.16.0.0/24
        action drop
        count test-counter
    !
    default-action drop
!
lists
    vpn-list test-vpn-list
        vpn 1
    !
    site-list test-site-list
        site-id 500
    !
!
```

Then we apply this policy to the site list named test-site-list, which includes site 500:

```text
vm9# show running-config apply-policy
apply-policy
    site-list test-site-list
    data-policy test-data-policy
!
```

Immediately after we activate the configuration on the vSmart controller, it pushes the policy configuration to the vEdge routers in site 500. One of these routers is vm5, where we see that the policy has been received:

```text
vm5# show omp data-policy
policy-from-vsmart
data-policy test-data-policy
    vpn-list test-vpn-list
        sequence 10
        match
            destination-ip 172.16.0.0/24
        action drop
        count test-counter
    !
    default-action drop
!
lists
    vpn-list test-vpn-list
        vpn 1
    !
```
Control Access

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 1.1.1.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 2.2.2.2. This policy also specifies the next hop for the TCP traffic sent by 1.1.1.1, setting it to be TLOC 10.10.10.10, color gold. All other traffic is accepted as a result of the `default-action` statement.

```
policy
    lists
        site-list north
        site-id 100
        vpn-list vpn-north
        vpn 100
    !
data-policy tcp-only
    vpn-list vpn-north
    sequence 10
    match
        source-ip 1.1.1.1/32
        destination-ip 2.2.2.2/32
        protocol tcp
    action accept
    set tloc 10.10.10.10 color gold
    !
default-action accept
    !
apply-policy
    site north data-policy tcp-only
```

Restrict Traffic

This example illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 1.1.0.0/16. However, the policy accepts all other data traffic, including non-SMTP traffic from 1.1.0.0/16.

```
policy
    lists
        data-prefix-list north-ones
        ip-prefix 1.1.0.0/16
        port 25
        vpn-list all-vpns
        vpn 1
        vpn 2
        site-list north
        site-id 100
    !
data-policy no-mail
    vpn-list all-vpns
    sequence 10
    match
        source-data-prefix-list north-ones
    action drop
    !
default-action accept
    !
apply-policy
    site north data-policy no-mail
```
Allow Traffic to Exit from a vEdge Router to the Internet

The following example allows data traffic destined for two prefixes on the Internet to exit directly from the local vEdge router to the Internet destination. Configure this policy on the vSmart controller.

```plaintext
policy
  lists
    vpn-list vpn-1
      !
    site-list nat-sites
      site-id 100,200
      !
data-policy accept-nat
  vpn-list vpn-1
  sequence 100
    match
      source-ip 10.20.24.0/24
      destination-ip 10.0.12.12/32
    !
    action accept
    count nat
    nat use-vpn 0
      !
    sequence 101
    match
      source-ip 10.20.24.0/24
      destination-ip 10.1.15.13/32
    !
    action accept
    count nat_inet
    nat use-vpn 0
      !
    default-action accept
      !
apply-policy
  site-list nat-sites data-policy accept-nat
```

Using the destination port instead of a destination IP prefix allows greater flexibility for traffic exiting to the Internet. Here, traffic can go to all HTTP and HTTPS sites (ports 80 and 443, respectively). Configure this policy on a vSmart controller.

```plaintext
data-policy accept-nat
  vpn-list vpn-1
  sequence 100
    match
      source-ip 10.20.24.0/24
      destination-port 80
    !
    action accept
    count nat
    nat use-vpn 0
      !
    sequence 101
    match
      source-ip 10.20.24.0/24
      destination-port 443
    !
    action accept
    count nat_inet
    nat use-vpn 0
      !
    default-action accept
      !
```
Additional Information

Centralized Data Policy
Configuring Centralized Data Policy