Service Chaining

Service chaining allows data traffic to be rerouted through one or more services, such as firewall, load balancer, and intrusion detection and prevention (IDP) devices.

Services in the Network

Services such as firewall, load balancer, and intrusion detection and prevention (IDP) are often run within a virtualized environment, and they may physically be centralized in one location or in several locations for redundancy. Services may be internal, cloud based, or external subscriptions. Networks must be able to reroute traffic from any location in the network through such services.

Customers want the ability to internally spawn or externally subscribe to new services on demand—for capacity, redundancy, or simply to select best-of-breed technologies. For example, if a firewall site exceeds its capacity, a customer can spawn new firewall service at a new location. Supporting this new firewall would require the configuration of policy-based, weighted load distribution to multiple firewalls.

Following are some of the reasons to reroute a traffic flow through a service or chain of services:

- Traffic flow from a less secure region of a network must pass through a service, such as a firewall, or through a chain of services to ensure that it has not been tampered with.
- For a network that consists of multiple VPNs, each representing a function or an organization, traffic between VPNs must traverse through a service, such as a firewall, or through a chain of services. For example, in a campus, interdepartmental traffic might go through a firewall, while intradepartmental traffic might be routed directly.
- Certain traffic flows must traverse a service, such as a load balancer.

Today, the only way to reroute traffic flow is by provisioning every routing node—from the source to the service node to the systems beyond the service node—with a policy route. This is done either by having an operator manually configure each node or by using a provisioning tool that performs the configuration for each node on behalf of the operator. Either way, the process is operationally complex to provision, maintain, and troubleshoot.

Provisioning Services in the Viptela Overlay Network

In the Viptela solution, the network operator can enable and orchestrate all service chaining from a central controller, that is, from the vSmart controller. No configuration or provisioning is required at any of the vEdge routers.

The general flow of service chaining in a Viptela network is as follows:

- vEdge routers advertise the services available in their branch or campus—such as firewall, IDS, and IDP—to the vSmart controllers in their domain. Multiple vEdge routers can advertise the same services.
- vEdge routers also advertise their OMP routes and TLOCs to the vSmart controllers.
For traffic that require services, policy on the vSmart controller changes the next hop for the OMP routes to the service landing point. In this way, the traffic is first processed by the service before being routed to its final destination.

The following figure illustrates how service chaining works in the Viptela solution. The network shown has a centralized vEdge hub router that is connected to two branches, each with a vEdge router. The standard network design implements a control policy such that all traffic from branch site 1 to branch site 2 travels through the vEdge hub router. Sitting behind the hub router is a firewall device. So now, assume we want all traffic from site 1 to site 2 to first be processed by the firewall. Traffic from the vEdge router at site 1 still flows to the vEdge hub router, but instead of sending it directly to site 2, the hub router redirects the traffic to the firewall device. When the firewall completes its processing, it returns all cleared traffic to the hub, which then passes it along to the vEdge router at site 2.

Service Route SAFI

The hub and local branch vEdge routers advertise the services available in their networks to the vSmart controllers in its domain using service routes, which are sent via OMP using the service route Subsequent Address Family Identifier (SAFI) bits of the OMP NLRI. The vSmart controllers maintain the service routes in their RIB, and they do not propagate these routes to the vEdges.

Each service route SAFI has the following attributes:

- VPN ID (vpn-id)—Identifies the VPN that the service belongs to.
• Service ID (svc-id)—Identifies the service being advertised by the service node. The Viptela software has the following predefined services:
  ◦ FW, for firewall (maps to svc-id 1)
  ◦ IDS, for Intrusion Detection Systems (maps to svc-id 2)
  ◦ IDP, for Identity Providers (maps to svc-id 3)
  ◦ netsvc1, netsvc2, netsvc3, and netsvc4, which are reserved for custom services (they map to svc-id 4, 5, 6, and 7, respectively)

• Label—For traffic that must traverse a service, the vSmart replaces the label in the OMP route with the service label in order to direct the traffic to that service.

• Originator ID (originator-id)—The IP address of the service node that is advertising the service.

• TLOC—The transport location address of the vEdge that is “hosting” the service.

• Path ID (path-id)—An identifier of the OMP path.

---

Service Chaining Policy

To route traffic through a service, you provision either a control policy or a data policy on the vSmart controller. You use a control policy if the match criteria are based on a destination prefix or any of its attributes. You use a data policy if the match criteria include the source address, source port, DSCP value, or destination port of the packet or traffic flow. You can provision the policy directly via CLI, or it can be pushed from the vManage management system.

The vSmart controller maintains OMP routes, TLOC routes, and service routes in its route table. A given OMP route carries a TLOC and the label associated with it. On a vSmart controller, a policy can be applied that changes the TLOC and its associated label to be that of a service.

---

Additional Information

Configuring Centralized Control Policy
Service Chaining Configuration Examples