Versa Networks Elastic Services Cluster

This document summarizes the Versa Networks Elastic Services Cluster, which scales the service and IO (input/output) planes.

Summary

Two or more Versa Operating System™ (VOS™) nodes can form an Elastic Services Cluster that can scale both the service plane and the IO (input/output) plane. Multiple nodes can perform stateful services such as SD-WAN termination, TLS Decryption, AV, IPS, CASB, and DLP at any location, hub, or spoke. It supports high throughput with bare metal and virtual nodes. The cluster does not have any dependency on how traffic enters the Versa Elastic Services Cluster. It can handle packets even if packets of the same flow are received on different cluster nodes. The Versa Elastics Services Cluster can automatically add more service-plane and IO-plane capacity as required.

Details

Many customers from financial, insurance, defense, banking, and other segments do all their security services in-house for compliance reasons. Most security services require break-and-inspect (decryption and inspection of traffic). Because customers in this segment have very sensitive information, they prefer to do all break-and-inspect within very limited, highly guarded premises. As a result, traffic from several thousand branch sites is brought to one or two hub locations. Because of the large volume of traffic that is received at these hub sites, several VOS nodes are deployed that play the role of SD-WAN edge devices as well as security devices that may include TLS Termination, NextGen Firewall, Unified Threat Management, Anti-Virus, Intrusion Prevention, Cloud Access Security Broker (CASB), as well as Data Loss Prevention (DLP).

Two or more VOS nodes can form an Elastic Services Cluster that can scale both the service plane and the IO (input/output) plane. Multiple nodes can perform stateful services such as SD-WAN termination, TLS Decryption, AV, IPS, CASB, and DLP at any location, hub, or spoke. Various nodes can also have different underlay connectivity.

The Versa Elastic Services Cluster (ECS) can scale almost linearly. Cluster nodes can be bare metal or virtual. Thus, the cluster can also sustain very high throughput in Cloud Service Provider deployments.

The Versa ECS removes any requirements regarding traffic ingress from the LAN and WAN sides. It is more resilient when an internal router fragments and sprays (ECMPs) to different downstream stateful devices.

Figure 1 shows a typical hub location that has deployed multiple VOS nodes. A VOS node can be configured to do one or more roles:

1. IO (Input/Output) Node: In this case, the VOS instance plays the role of SD-WAN Edge node, which communicates with other SD-WAN nodes on the WAN side and internal routers on the LAN side. These nodes are also responsible for load-balancing the traffic to the service nodes.
2. Service Node: In this case, the VOS instance plays the role of Service node. These nodes are mainly involved in CPU-intensive services. These VOS instances can be configured to TLS Termination, NextGen Firewall, Unified Threat Management, Anti-Virus, Intrusion Prevention, Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP).
3. Hybrid: In this case, the VOS instance serves as both an IO node and a Service Node.

In Figure 1, traffic from multiple spoke SD-WAN sites (VOS5, VOS6, VOS7) is brought to a hub site that has multiple hybrid VOS instances. Subnets belonging to the internal Layer 3 LAN are announced equally by all four VOS instances at the hub site. A remote spoke site load-balances/ECMPs packets belonging to different flows or the same flow to one or more VOS instances at the hub site. Packets for the same flow could also arrive at the hub site at different VOS instances (VOS1, VOS2, VOS3, VOS4). There is no dependency on how packets arrive at these hub VOS instances from the LAN or WAN sides. Besides SD-WAN functions, each VOS node at the hub sites also does TLS termination of the inner packet, NGFW, Anti-Virus, Intrusion Prevention, CASB, DLP, and other security functions.

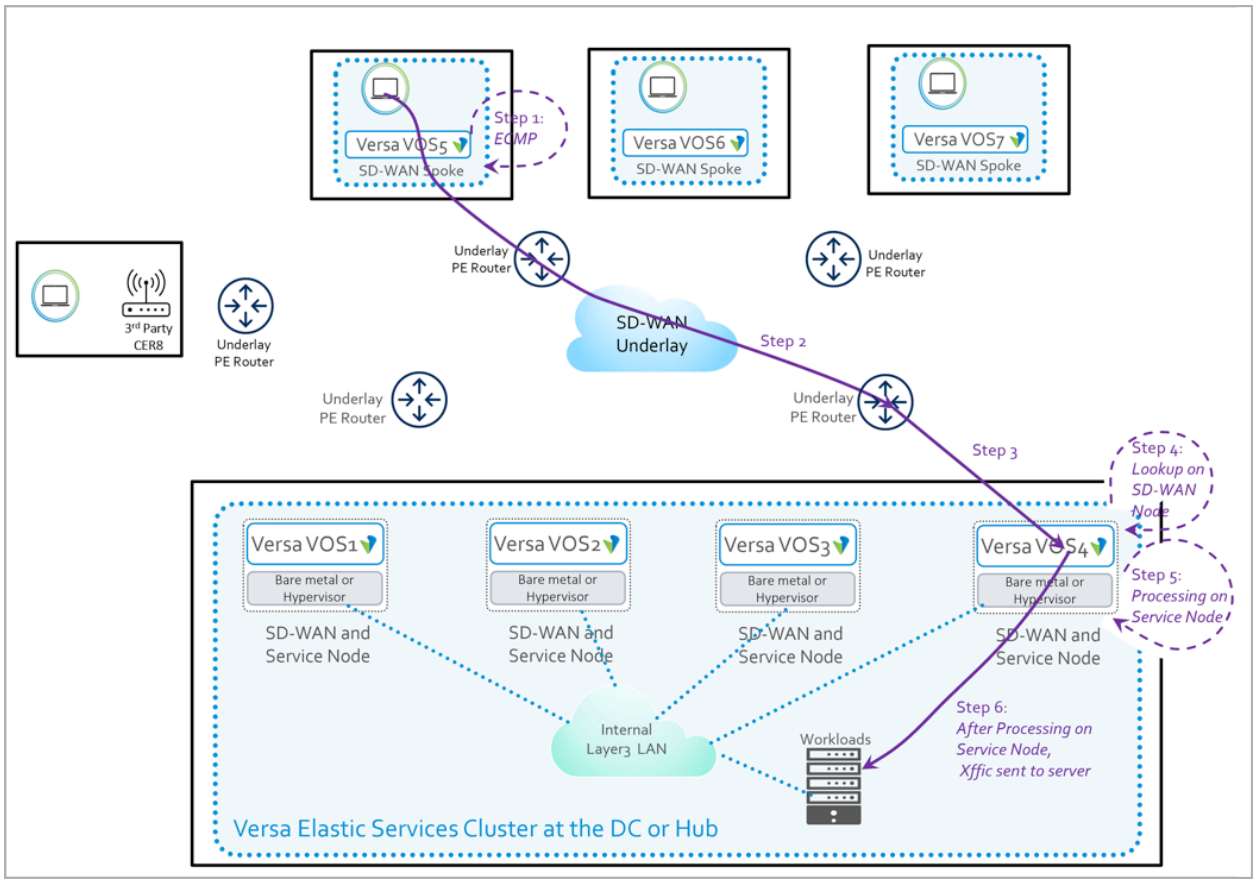

Figure 1.

In Figure 1, traffic relating to flow (e.g., Flow50) is received by VOS4 at the hub site. At a later time, the SLA offered by the underlay path between spoke-site VOS5 and right-most hub-site (VOS4) could change. As a result, the Spoke-VOS1 might forward traffic relating to Flow50 to the left-most hub node (VOS1), as shown in Figure 2. Because any security device, such as VOS4, must inspect both sides of the same flow, VOS1 forwards packets relating to Flow50 to VOS4, which performs security processing for that flow.

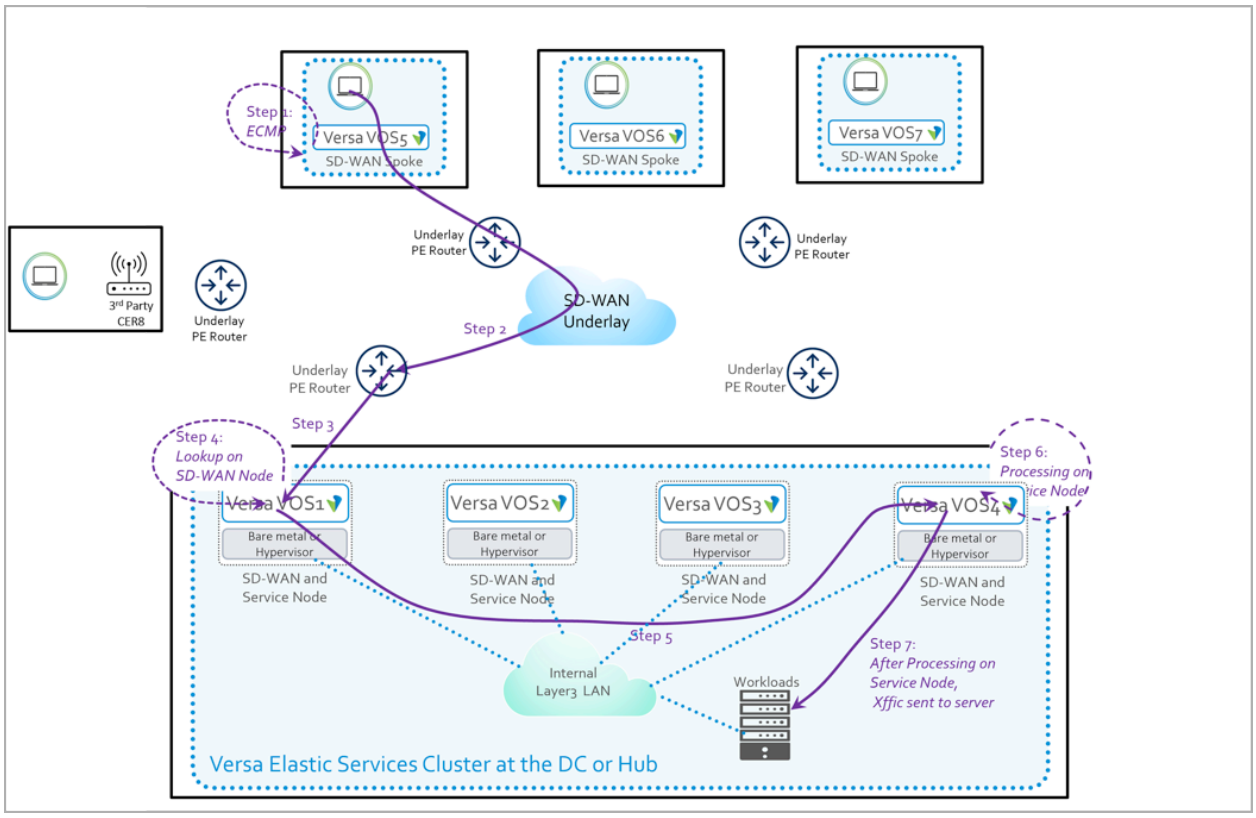

Figure 2.

All the VOS instances (VOS1 through VOS4) at the hub site could also announce their local routes to the underlay Provider Edge (PE) router so that non-SD-WAN nodes can also access various resources at the hub site. When traffic is received from a third-party customer edge router (CER8) at an underlay PE router serving the hub site, the PE router ECMPs the traffic to one of the four VOS nodes at the hub site from which it has received traffic. Traffic for a specific flow (Flow51) is received on VOS3, which also performs security processing for it. This is shown in Figure 3. If there are underlay changes in the Provider network between CER8 and the hub site, the next packet for Flow51 could arrive at a different VOS instance (VOS2) at the hub site. This is shown in Figure 4. VOS2 would forward packets for Flow51 to VOS3 since VOS3 is doing security-service processing for Flow51.

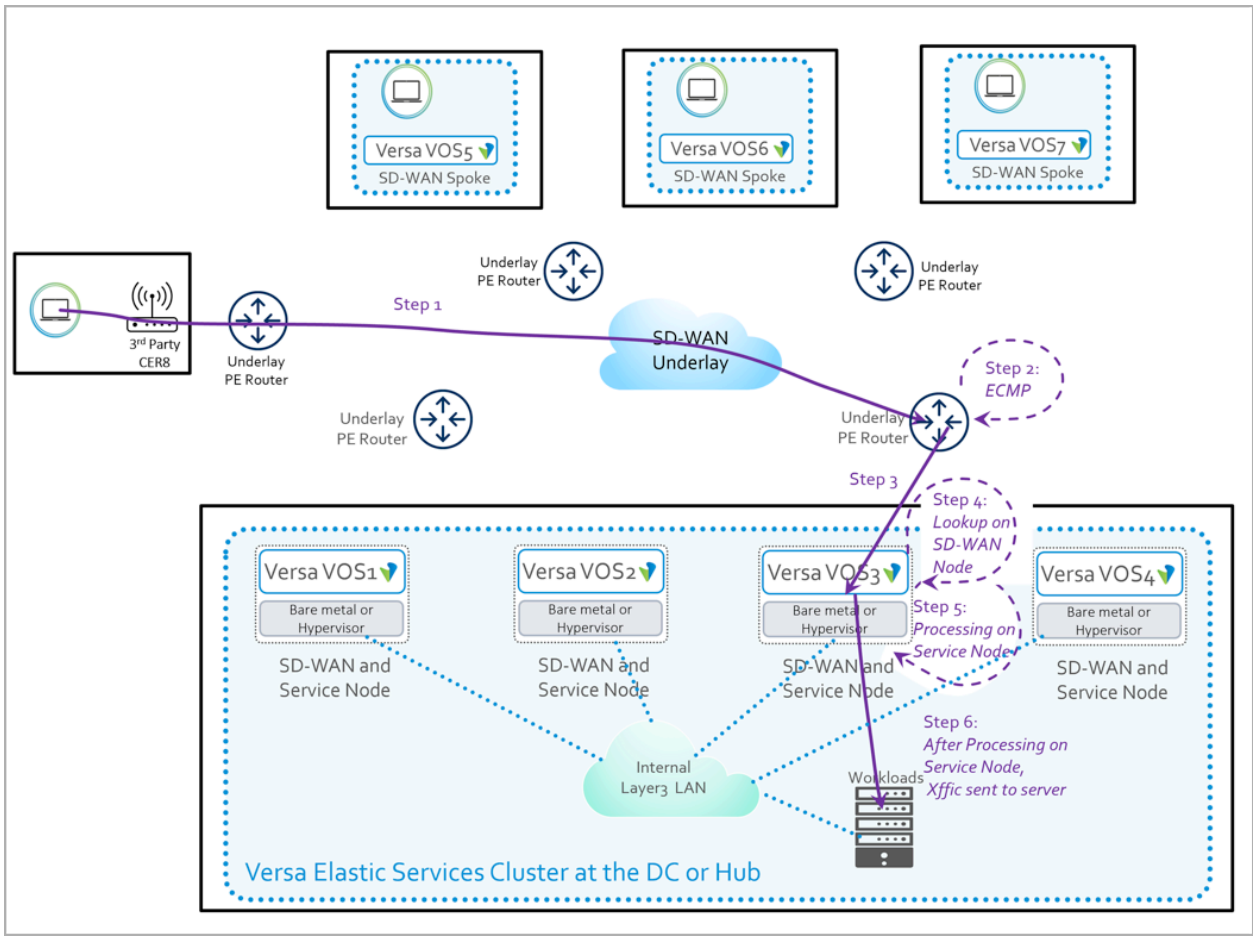

Figure 3.

Updated: Thu, 24 Oct 2024 10:54:18 GMT

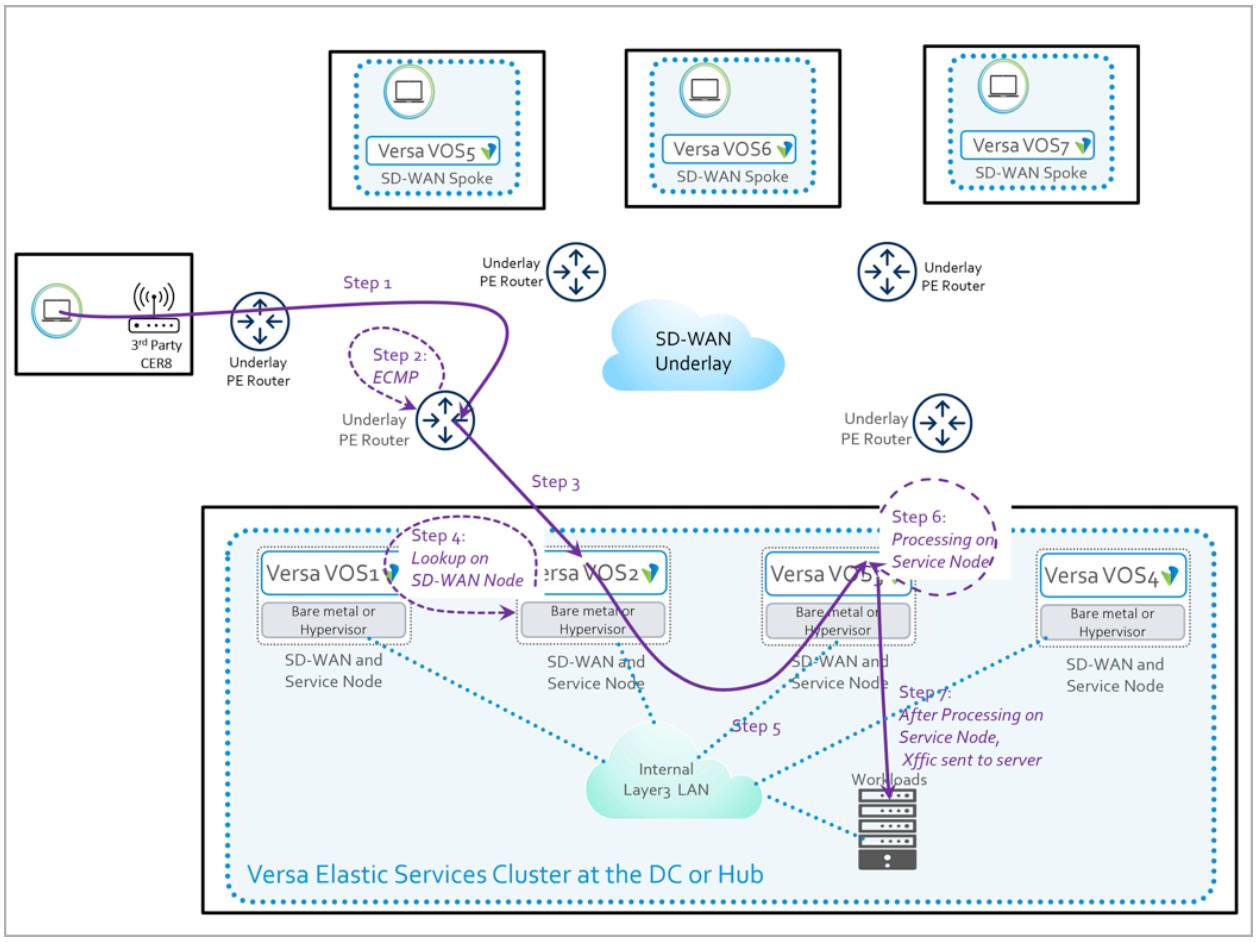

Figure 4.

The Versa Elastic Service Cluster automatically load-balances between various cluster nodes as required. The Versa Elastic Service Cluster nodes can be bare metal nodes, virtual nodes, or a combination. It can automatically add more service processing capacity or I/O capacity, as shown in Figure 5.

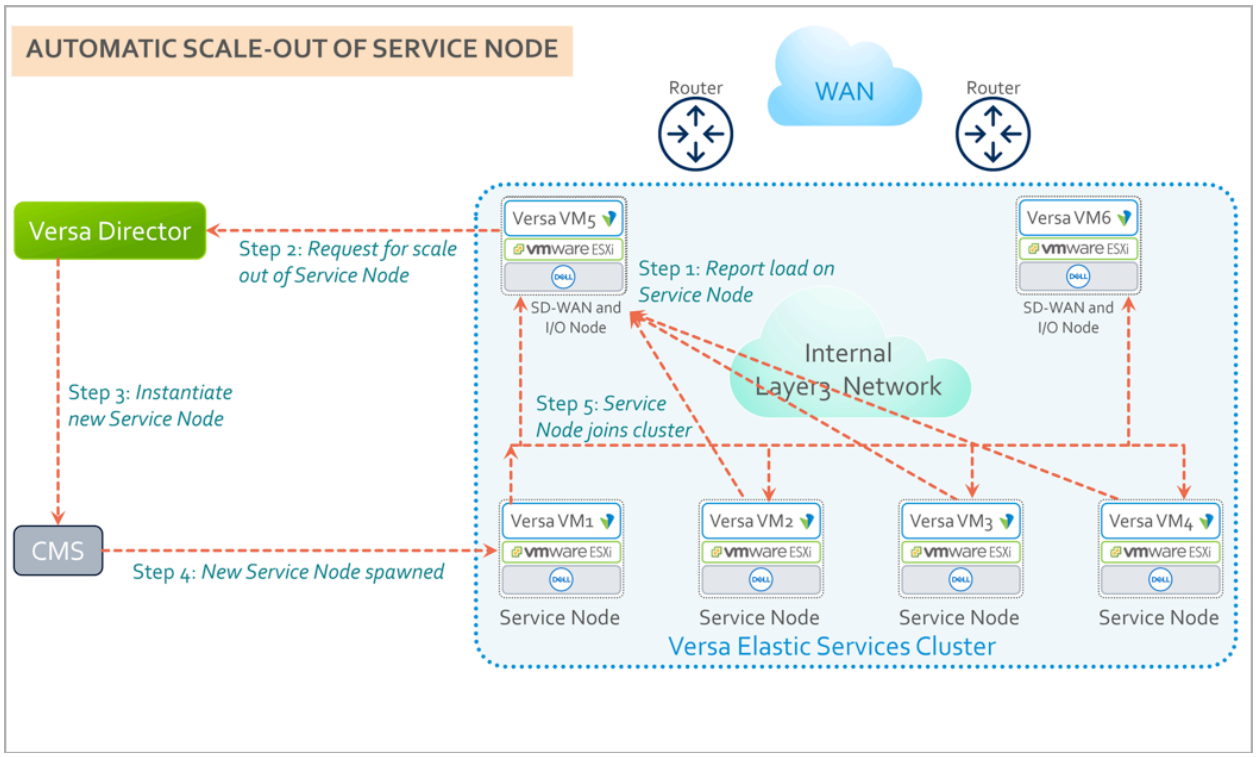

Figure 5.