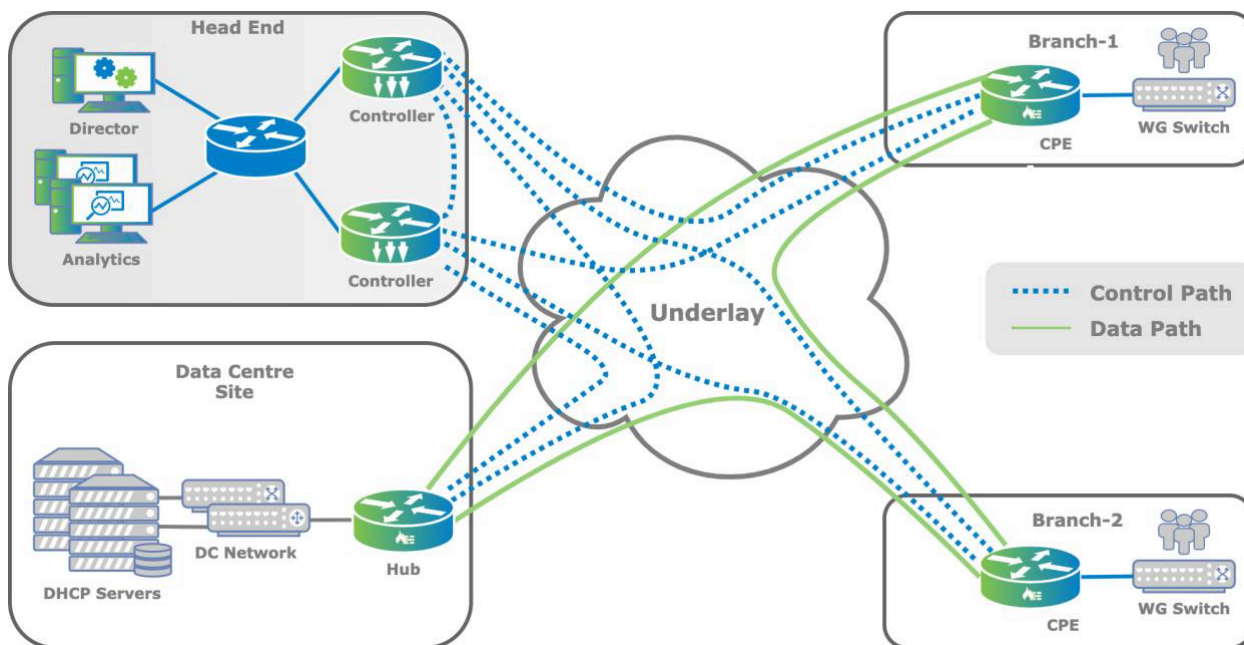


## SD-WAN Overlay Networks

 For supported software information, click [here](#).

The Versa Networks SD-WAN is based on overlay tunnels, and all traffic traveling through the tunnels is encrypted. In the SD-WAN overlay design you need to consider the IP addressing scheme for the overlay network and whether you want all data traffic to follow the encrypted overlay.

The following figure shows the topology of an SD-WAN overlay network, to illustrate the overlay and underlay networks. The network consists of a data center two single-homed remote branches that are managed by a Versa Networks headend, which consists of Director, Analytics and Controller node. All sites and the headend are connected to all the available transport networks.



Hubs and branches connect to the Controller node, which serves as an attachment point for the management plane and control plane. SD-WAN overlay topologies are built through the exchange of MP-BGP NLRI communities in combination with import and export policies, and they provide the flexibility to create multiple topologies, using Director Workflows, without any restrictions.

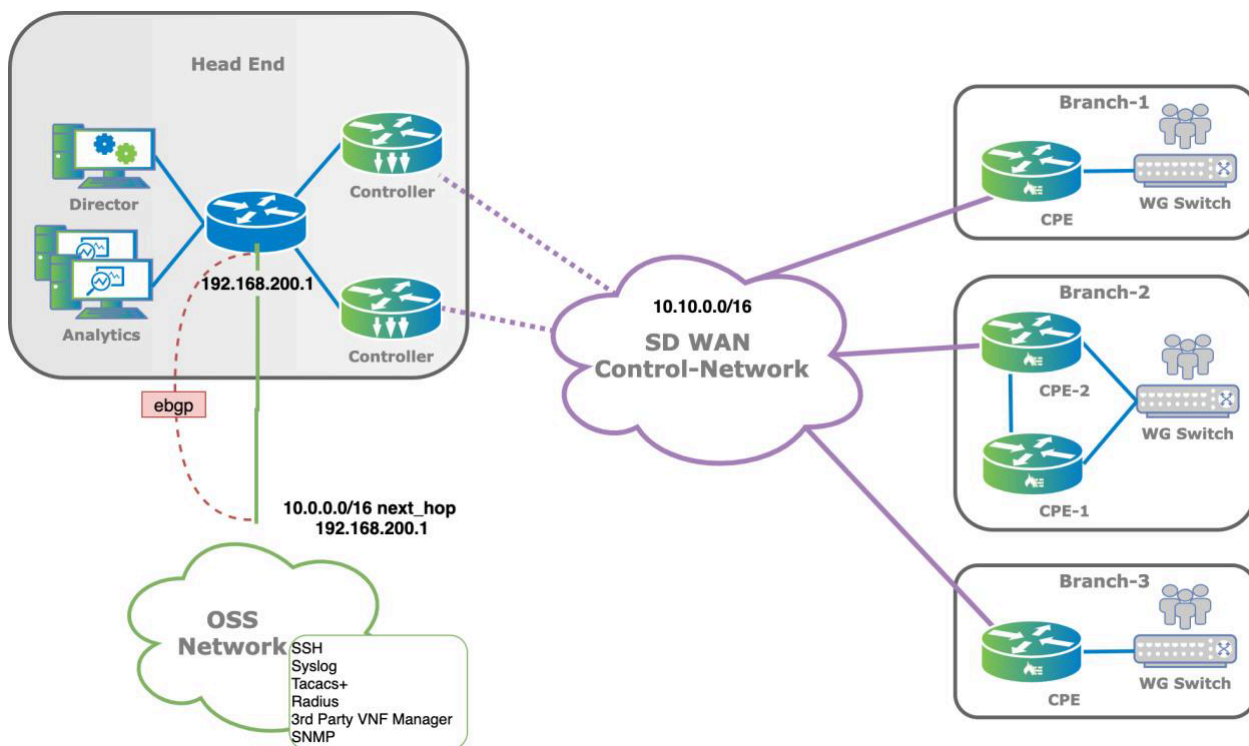
## Overlay IP Addressing

The Versa Networks SD-WAN is based on overlay tunnels, which are used to abstract the underlay networks. By default, two overlay networks are built between the branches:

- Encrypted overlay, which uses an IPsec tunnel
- Plain-text overlay, which uses a VXLAN tunnel

For more information about the tunnels used for overlay networks, see [Secure Control and Data Overlay Tunnel Solution](#).

The addresses for the SD-WAN overlay tunnels follow a specific overlay IP addressing scheme. In principle, the overlay network is routable in the SD-WAN control network, that is, between both the Controller nodes and the branches, and the control network southbound of the Director node (or northbound of the SD-WAN Controller node), as illustrated in the following figure.



However, in some deployments, you must choose what to include in the overlay IP addressing scheme when you are integration with an OSS/BSS. For example, the control network must have IP address reachability between VOS edge devices and services such as TACACS+, RADIUS, syslog collectors, and third-party VNF managers. For more information, see [Configure the Overlay Addressing Scheme](#)

The following are best practices for overlay IP addressing:

- Configure the overlay IP addressing method and pool when you initially set up the Versa Director. You cannot

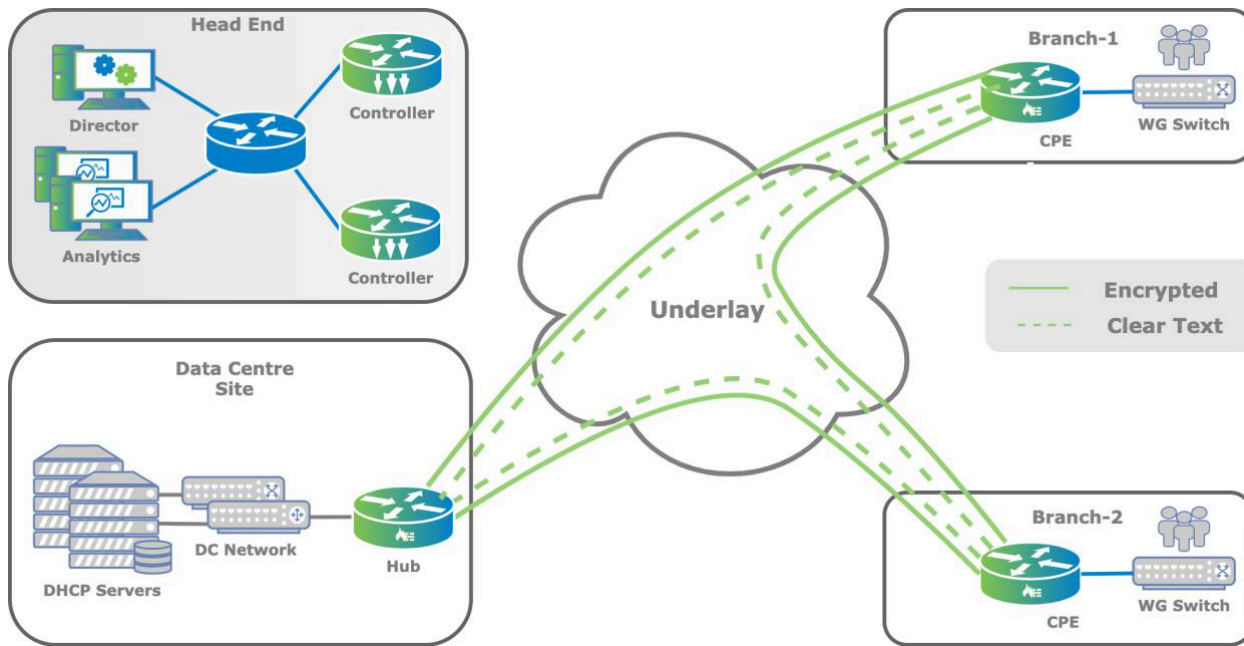
modify the method later. Ensure that you choose the correct method and that you allocate a large enough subnet to cover the expected size of the deployment.

- It is recommended that you use the “do not encode” option to optimize the use of IP addressing space.

---

## Encrypted and Clear-Text Overlay

By default, all data traffic follows the encrypted overlay, as illustrated in the following figure.



If you need to change the default tunnel used for data transport, you can do so in one of the following ways:

- Statically configuring encrypted or clear-text transmission of data per WAN interface
- Dynamically setting the transmission mode by configuring an SD-WAN policy

Note that if you configure both WAN interface static definition and SD-WAN policy, the SD-WAN policy takes precedence.

---

## Define Per-Interface Encryption Statically

You can statically define the encryption method per WAN interface if the underlay is a private or secured circuit such as an MPLS service provided as part of a service provider Layer 3 VPN service. Traditionally, network administrators have considered these private Layer 3 VPNs as secured and did not typically encrypt data over it. In a similar manner, you can consider the MPLS Layer 3 VPN as secured, and so data can be transported using the clear-text tunnel.

A benefit of clear-text transport is that it does not use IPsec overhead on the platform.



To configure static definition per WAN interface:

---

[https://docs.versa-networks.com/Solutions/SD-WAN\\_Design/05\\_SD-WAN\\_Overlay\\_Networks](https://docs.versa-networks.com/Solutions/SD-WAN_Design/05_SD-WAN_Overlay_Networks)

Updated: Thu, 24 Oct 2024 10:49:51 GMT

Copyright © 2024, Versa Networks, Inc.

1. In Appliance view, select the Configuration tab in the top menu bar.
2. Select Services  > SD-WAN > Site in the left menu bar.
3. In the Site pane, click the  Edit icon.
4. In the WAN Interfaces tab, select a WAN interface. The Edit WAN Interfaces popup window displays.



5. In the Encryption field, select the desired encryption for the interface:
  - Always—Encrypt all traffic.
  - Never—Do not encrypt traffic.
  - Optional—Encryption is optional.
6. Click OK.

For more information, see [Configure Encryption on WAN Interfaces](#).

---

## Use SD-WAN Policy To Dynamically Define Encryption

In some scenarios, you need to dynamically turn off encryption for some traffic, for example, for traffic that is already encrypted by an application (such as HTTPS or TLS/SSL secured application data) and traffic that is of no interest, from a security point of view, to the enterprise (such as recreational traffic from Facebook and YouTube). To turn off encryption for these types of traffic, you configure an SD-WAN forwarding profile, in which you set the desired encryption, and then you associate the forwarding with an SD-WAN policy that identifies the traffic to match.



To use SD-WAN policy to dynamically define encryption:

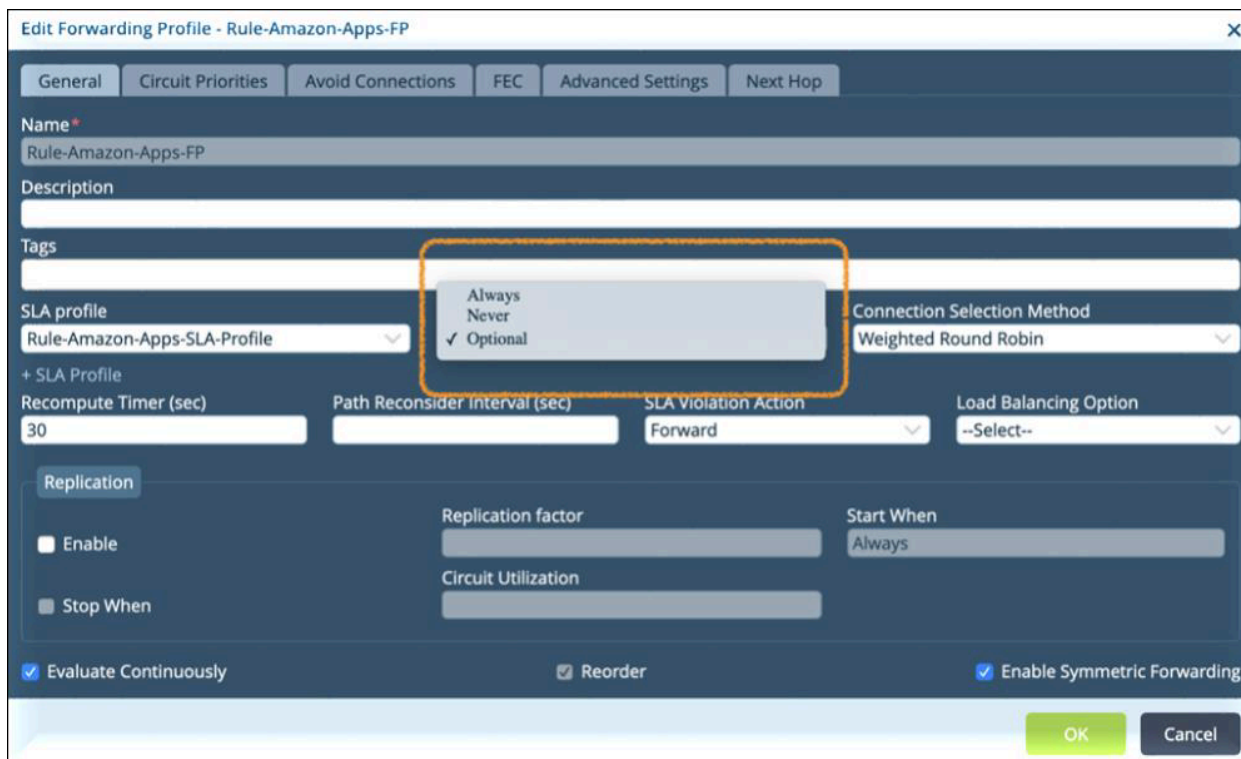
---

[https://docs.versa-networks.com/Solutions/SD-WAN\\_Design/05\\_SD-WAN\\_Overlay\\_Networks](https://docs.versa-networks.com/Solutions/SD-WAN_Design/05_SD-WAN_Overlay_Networks)

Updated: Thu, 24 Oct 2024 10:49:51 GMT

Copyright © 2024, Versa Networks, Inc.

1. In Appliance view, select the Configuration tab in the top menu bar.
2. Select Services  > SD-WAN > Forwarding Profiles in the left menu bar.
3. Click the  Add icon. The Edit Forwarding Profile popup window displays.



4. In the Encryption field, select the desired encryption.

For more information, see [Configure SD-WAN Traffic-Steering](#).

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

[Configure Encryption on WAN Interfaces](#)

[Configure SD-WAN Traffic-Steering](#)