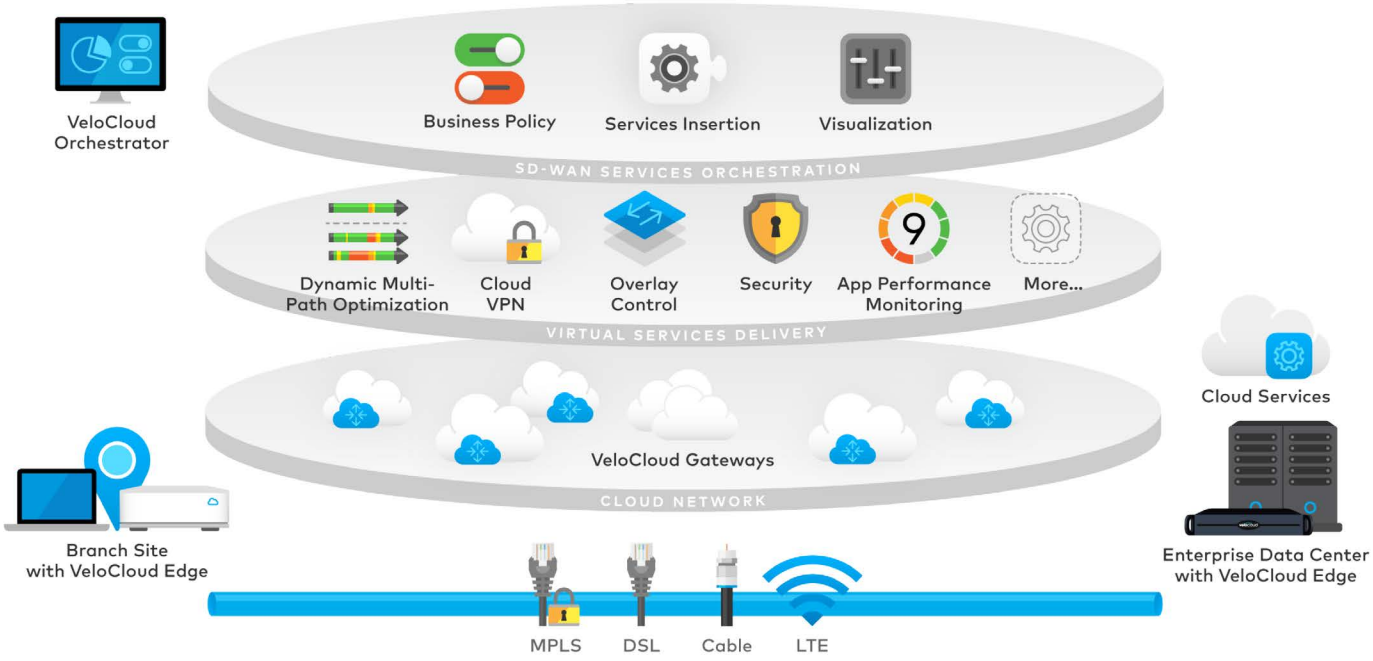
VeloCloud Secure SD-WAN

Table of contents

Introduction

The VeloCloud Cloud-Delivered SD-WAN has a robust architecture that ensures superior enterprise and cloud application performance over Internet and hybrid WAN connections, while also simplifying deployment and reducing costs. VeloCloud SD-WAN brings SDN concepts to the WAN providing an architecture that decouples the network control, management and forwarding functions, enabling network control to become directly programmable, and abstracting the underlying infrastructure for applications and network services. Business policies implemented by the logical overlay abstracts application flows to become independent of the underlying physical transport.



VeloCloud provides a transport independent secure overlay that enables the use of any combination of broadband Internet or MPLS links. The architecture is comprised of three layers:

Cloud Network

Data center backhaul penalties are eliminated with a cloud-ready network, providing an optimized direct path to public and private enterprise clouds. Secure SD-WAN overlay tunnels (Edge-to-Edge or Edge-to-Cloud) enable access to enterprise and cloud applications (e.g. SaaS/IaaS).

Virtual Services

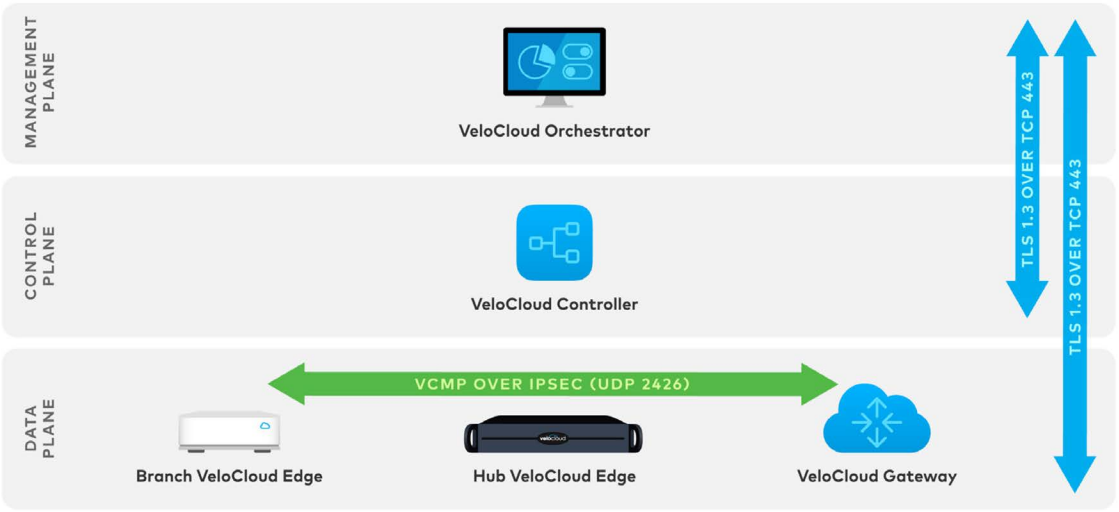
The branch office footprint is reduced with single-click, seamless insertion and chaining of virtualized services on-premise or in the cloud. Services may be provided by Velocloud including DMPO, Cloud VPN, Routing, Segmentation, NGFW, and Voice Quality monitoring, or they can be offered by third party virtual services such as Cloud Web Security.

Automation and Orchestration

Zero-touch branch network deployment is enabled by automation and business policy-based orchestration.

Secure SD-WAN Architecture

VeloCloud SD-WAN architecture ensures secure communication between the Management, Control and Data planes. The following diagram shows the methods used to secure the communication between these layers.



Securing Traffic between the Management and Data Planes

The VCE/VCG establishes a TLS 1.3 session to the VCO, mutually authenticating each other during session setup to receive policy updates and upload statistics. Once the TLS connection is established, the VCO performs a fingerprint match of the TLS client certificate sent by VCE/VCG against the one stored in the VCO database corresponding to that particular VCE/VCG. In case of a fingerprint mismatch, the VCO issues a "deactivate command" to the VCE/VCG. This authentication strategy is commonly known as "public key pinning" where the VCE/VCG contacts the VCO every 30 seconds.

Securing Traffic between the Management and Control Planes

Traffic between the VCC and VCO is secured with TLS 1.3. The VCC uses this connection to upload VCE usage statistics to the VCO. The VCC is typically deployed on-premise in enterprise data centers alongside the hub VCE.

Securing Traffic within the Data Plane and Control Planes

Traffic between the VCE's, and between the VCE and VCG/VCC, use VCMP tunnels secured with IKEv2/IPsec. The use of IKEv2 makes these tunnels inherently resistant to DoS attacks. Encrypted traffic uses a destination port of UDP 2426 which is the same as the VCMP tunnel port.

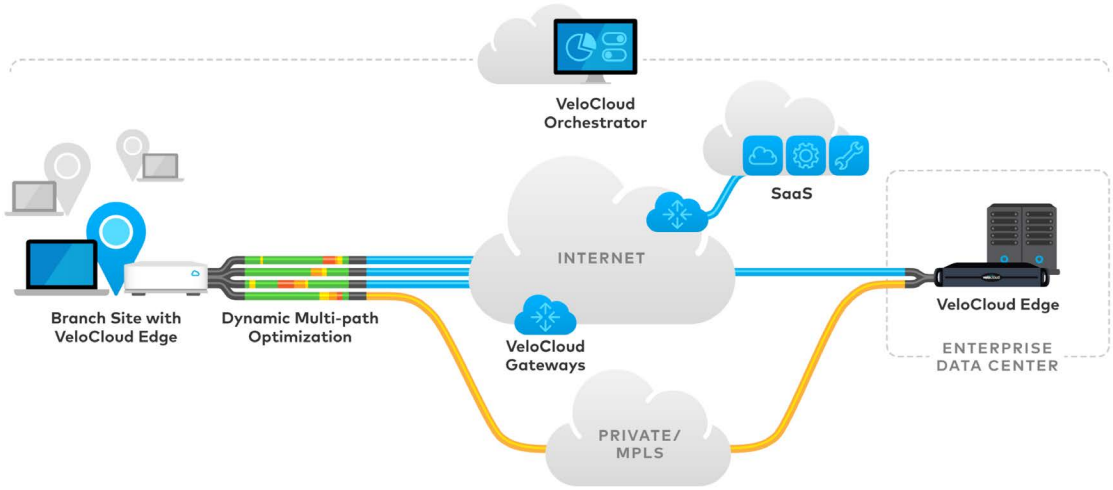
Secure SD-WAN with Deployment Flexibility

The VeloCloud SD-WAN architecture accommodates a variety of customer deployment use-cases, while also securing communication within these deployments. Two use cases commonly deployed by customers include:

Cloud-Delivered SD-WAN

A cloud SD-WAN solution delivers the promise of not only using the Internet for transport, but also leveraging the advantages of the cloud in a hybrid deployment architecture. Customers gain the benefits of the cloud-based service delivery infrastructure of the VeloCloud SD-WAN solution. In addition to providing superior application performance and the most optimal, direct access to cloud-based applications, other advantages of this architecture include:

- Ease of deployment
- Ability to monitor and control paths including peering through the Internet, a difficult achievement with an on-premise deployment



In this architecture customers use VeloCloud-hosted VCO and VCG infrastructure for management, control, and data plane functions. All management traffic between the cloud-hosted VCO, branches, and data center sites is secured with TLS 1.3. Data plane traffic between branches and data centers is secured by IKEv2/IPsec.

This architecture accommodates two types of deployments:

VCG as a Controller

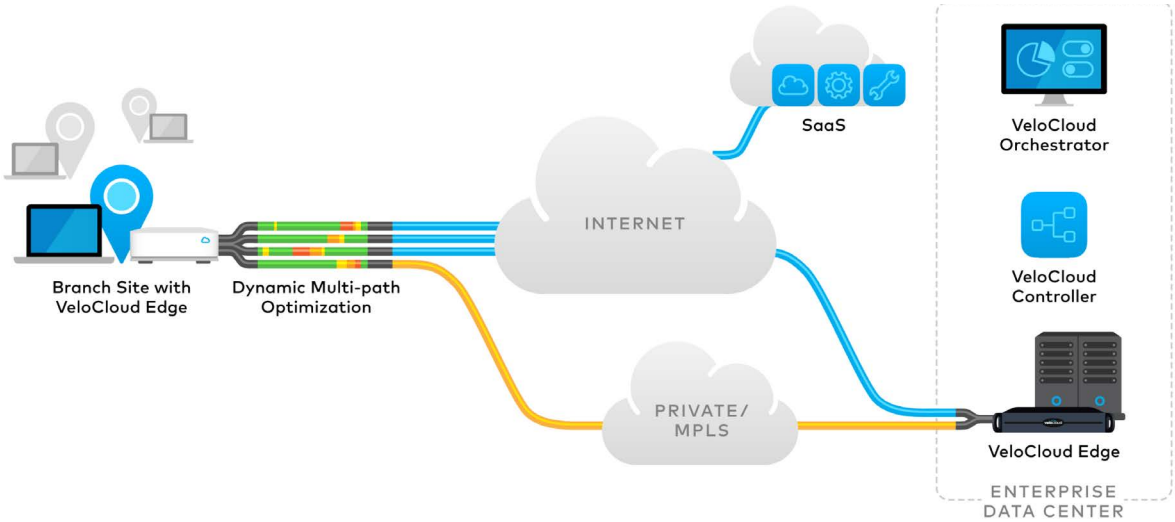
Customers use the VeloCloud-hosted VCG to perform control plane functions such as route reflector. All data plane traffic flows between the branch and data center locations. Control plane traffic between the branch and data center sites and the cloud-hosted VCG is encrypted using IKEv2/IPsec. The VCG enables support for secure dynamic branch-to-branch traffic.

VCG as Both Controller and Conduit to Cloud Services

Customers use the VeloCloud-hosted VCG as a controller as well as to connect branch sites to Cloud services such as SaaS/IaaS sites. This architecture provides optimized access to cloud-based applications and services. Traffic between the branch sites and the VCG is encrypted with IKEv2/IPsec. Traffic from the VCG to the SaaS/IaaS sites is encrypted with IKEv1/IPsec to accommodate potential third party VPN gateways that may not be able to support an IKEv2 key exchange.

On-Premise SD-WAN

Customers using this architecture deploy all the components of the VeloCloud SD-WAN solution on-premise in their network. All management, control, and data plane traffic never leaves the customer network and cloud traffic is backhauled to regional or data center hubs.



The VCO and VCC are installed in customer data center locations, both in the main and the disaster recovery data centers. High availability data centers are key in designing these networks. Using the VCO's disaster recovery feature, the configuration between the active VCO in the main data center and the standby VCO in the disaster recovery data center is securely backed up. VCE data plane traffic between the branch and data center sites is encrypted by IKEv2/IPsec tunnels, while traffic to the VCC is encrypted by IKEv2/IPsec.

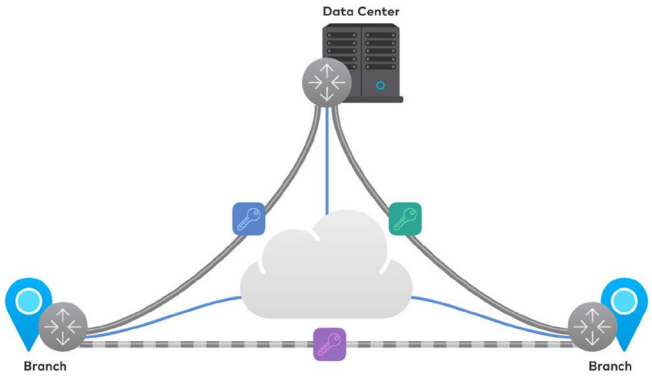
VeloCloud SD-WAN vs. Legacy VPN Solutions

Compared to some traditional VPNs, the VeloCloud SD-WAN architecture is more secure, more scalable, and easier to deploy and manage. The illustrations below compare the features or deployment options of the VeloCloud SD-WAN solution with two widely used legacy VPN solutions. Legacy VPN 1 establishes a secure overlay tunnel network between the data center and branch sites with the ability to set up dynamic branch-to-branch tunnels. Legacy VPN 2 uses a centralized key distribution mechanism to distribute the same set of IPsec keys to all sites subscribed to a particular group. The VeloCloud SD-WAN VPN architecture contains the best attributes of both legacy VPN features.

Legacy VPN 1

Secure, but Complex

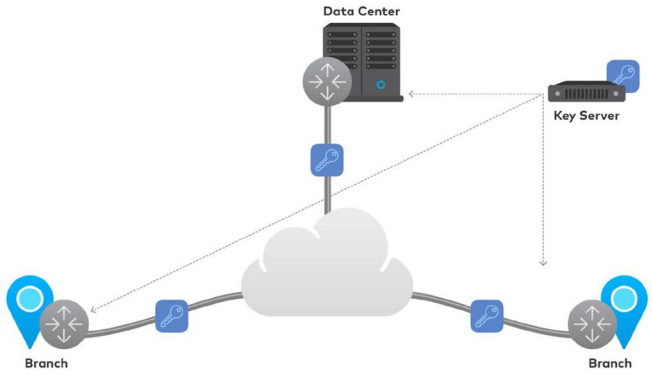
- ✔ PKI
- ✔ Unique Key per Tunnel
- ✔ Secure Onboarding
- ✘ Centralized Orchestrator
- ✘ Full Segmentation Support
- ✘ Integrated Certificate Server
- ✘ Tunnel Integrity Check



Legacy VPN 2

Simple, but Insecure

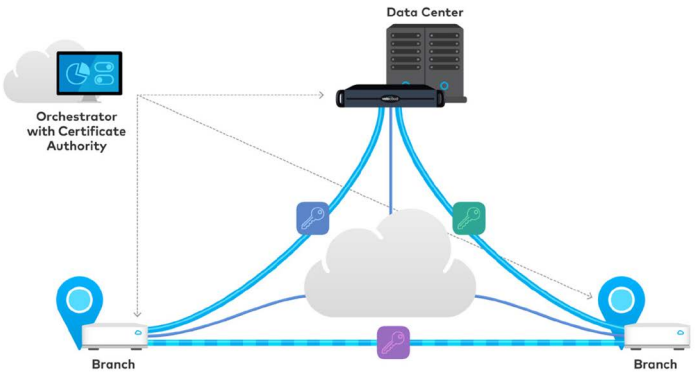
- ✘ PKI
- ✘ Unique Key per Tunnel
- ✘ Secure Onboarding
- ✔ Centralized Orchestrator
- ✘ Full Segmentation Support
- ✘ Integrated Certificate Server
- ✘ Tunnel Integrity Check



SD-WAN

Cloud-Delivered SD-WAN

- ✔ PKI
- ✔ Unique Key per Tunnel
- ✔ Secure Onboarding
- ✔ Centralized Orchestrator
- ✔ Full Segmentation Support
- ✔ Integrated Certificate Server
- ✔ Tunnel Integrity Check



Some details on the different features/deployment options discussed in the illustrations above include:

PKI
Public Key Infrastructure uses a Certificate Authority (CA) to distribute certificates used for authentication in VPN deployments. This method is more secure and scalable than the traditional pre-shared key mode of authentication.

Unique Keys per Tunnel
Using unique keys per VPN tunnel results in a more secure solution than when the same set of keys is shared by more than two sites. As the number of sites sharing the same set of keys increases, the impact of a potential attack increases proportionally. Using unique keys per tunnel limits the attack surface to the two sites connected by the tunnel.

Secure Onboarding
This feature ensures that new sites connecting to an existing VPN are authenticated and authorized before they are allowed to connect. If devices are stolen from an existing site or shipped to a wrong destination, they are not allowed to connect to the VPN.

Centralized Orchestrator
In this highly scalable deployment method, policy changes or updates are done at the central orchestrator and then easily distributed to the entire network. In a VPN solution, central distribution of policies is recommended. However, central distribution of the encryption keys by a Key Server could compromise VPN security. If the keys are stolen during an attack on the Key Server, or during a Key Server DoS attack, the entire VPN could be taken out of service.

Full Segmentation Support
Segmentation plays a key role in networks where traffic from different customers and/or business entities must be isolated from each other. Full support for segmentation includes isolation of management, control and data plane traffic.

Integrated Certificate Server
PKI is recommended for authentication because it offers a more secure and scalable solution than pre-shared key authentication. PKI requires a certificate server for certificate management and distribution. In most legacy VPNs the certificate server is an additional entity deployed in the network. An integrated certificate server eliminates the burden of deploying a separate certificate server platform just to enable PKI for VPN use.

Tunnel Integrity Check
When an existing branch or hub site in a VPN is compromised, this feature ensures that the site's certificate is immediately revoked and all tunnels to that site are deleted. A data integrity check, on the other hand, ensures that a packet is not tampered with in transit. This check is performed by IPsec in VeloCloud SD-WAN and the two legacy VPNs.

Management Plane Security

Secure Onboarding and Activation

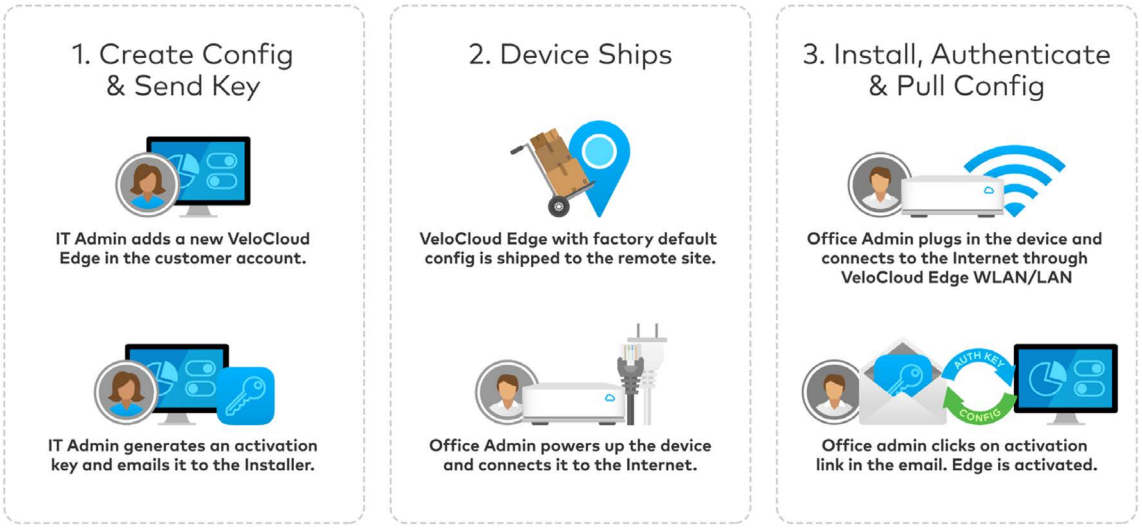
Once connected to the Internet in a zero-touch deployment, VeloCloud Edge appliances automatically authenticate, connect, and receive configuration instructions. This VCE deployment model obviates the need for IT personnel presence at the remote location, as well as the requirement for pre-staging the VCE prior to shipping. There is no security risk to losing a VCE during shipment as it contains no configuration or credentials to connect to the enterprise network. In fact, there is no site-specific configuration at all required for the deployment.

The VeloCloud SD-WAN solution supports two methods of VCE zero-touch deployment and activation: Pull Activation and Push Activation, as shown below.

	Pull Activation Office Admin Activates	Push Activation Central NOC Activates
No IT Visit Required	✓	✓
No Pre-staging Required	✓	✓
No Security Risk if Box Is Lost	✓	✓
No Site-by-site Link Profile Needed	✓	✓
No Device Tracking Needed	✓	
Requires Email to Office Admin	✓	
Requires Knowledge of Device to Site		✓

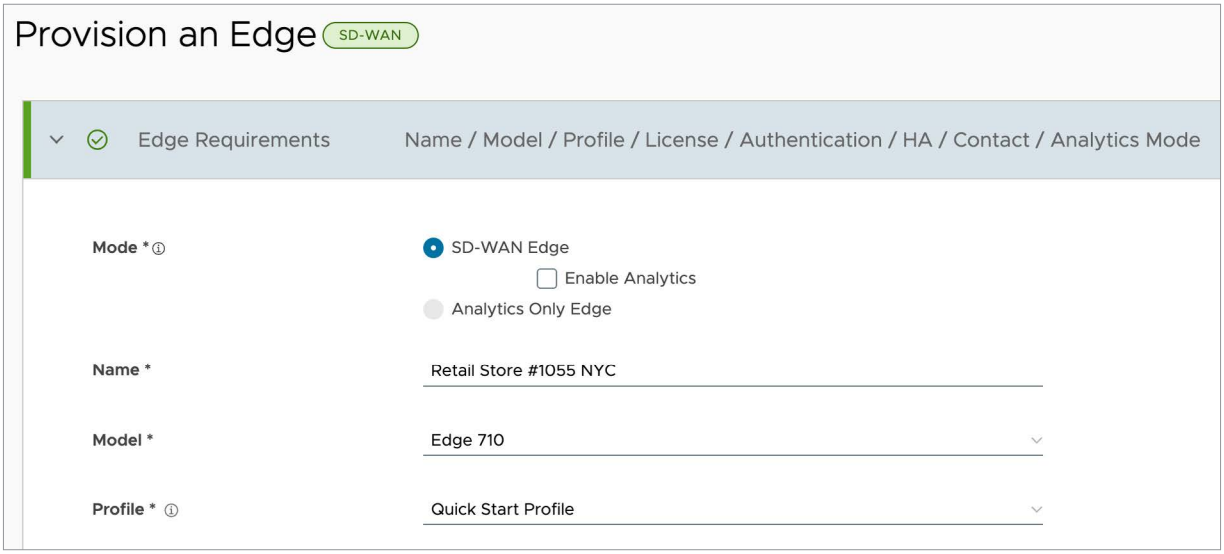
Pull Activation

For the Pull Activation method the VCE is shipped to the customer site with a factory-default configuration. Prior to activation the VCE contains no configuration or credentials to connect to the enterprise network.



The Pull activation method consists of two steps:

1. **Provisioning**
   On the VCO, the IT Admin creates a New Edge in the customer account.

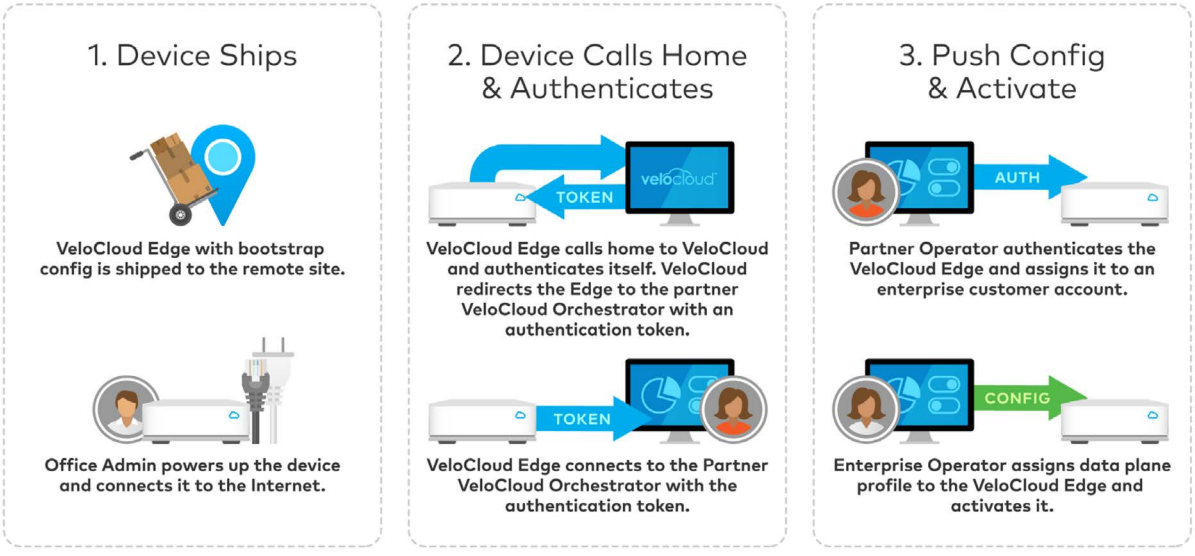


2. **Activation**
   To activate the VCE, an HMAC-based activation code is sent offline as an email to the Office Admin who will perform the activation. The Activation Key expires after 30 days. Once the VCE is powered up and connected to the Internet, the office admin connects to the Internet via the VCE LAN ports (wired or wireless), opens the activation email, and clicks on the activation code link. The VCE establishes a secure TLS 1.3 session to the VCO and the Velocloud Orchestrator assigns an authentication token to the VCE which is used for subsequent communications with the VCO to avoid anti-spoofing.

   Once activated, the VCE configuration is transmitted over a mutually authenticated TLS 1.3 VCO-to-VCE session. Each VCE has a unique ID mapped to the serial number of the VCE to prevent counterfeiting of the VCE.

Push Activation

For the Push Activation method, the VCE is activated without the requirement for an office admin to click on an activation link.



Some scenarios that require a Push activation include:

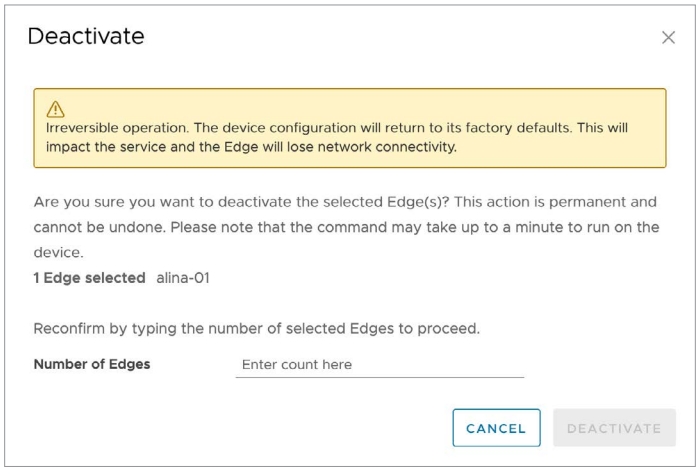
- When a Service Provider outsources the physical installation of devices at a site. In most instances just to connect cables and power the person who installs the device may neither be an employee of the end customer nor of the Service Provider.
- When the person at the remote site is unable to connect a laptop/tablet/phone to the VCE and therefore cannot use an email or clicking on an activation code/URL.

In the Push Activation method, the VCE has no configuration or credentials to connect to the enterprise network prior to activation. The VCE, once connected to the Internet, calls home to the VeloCloud VCO via a secure TLS 1.3 tunnel, and it is authenticated against the credentials it presents. These credentials and the call home URL are embedded in the VCE during manufacturing. The data is stored in a tamper-proof location inaccessible by connecting to the VCE.

Upon successful authentication, the VCE is issued a further certificate token and redirected to the partner VCO. The VCE now connects to the partner VCO with a secure TLS 1.3 tunnel and authenticates itself using the new certificate token. Once authenticated with the partner VCO, the VCE is assigned to an enterprise account where it is activated and assigned a data plane profile.

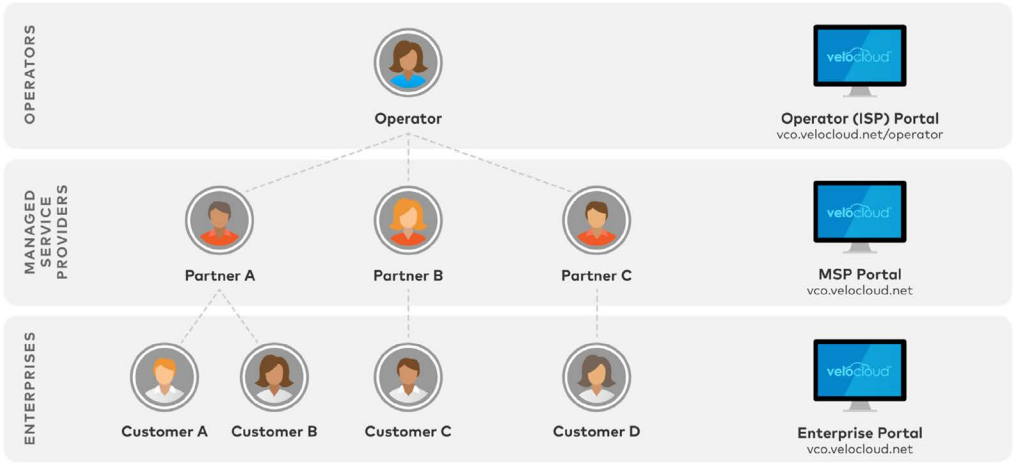
Revocation

In the event of a VCE compromise, the IT administrator can remotely deactivate a VCE from the VCE remote actions page, as shown below. This action deletes the VCE configuration and restores factory defaults.



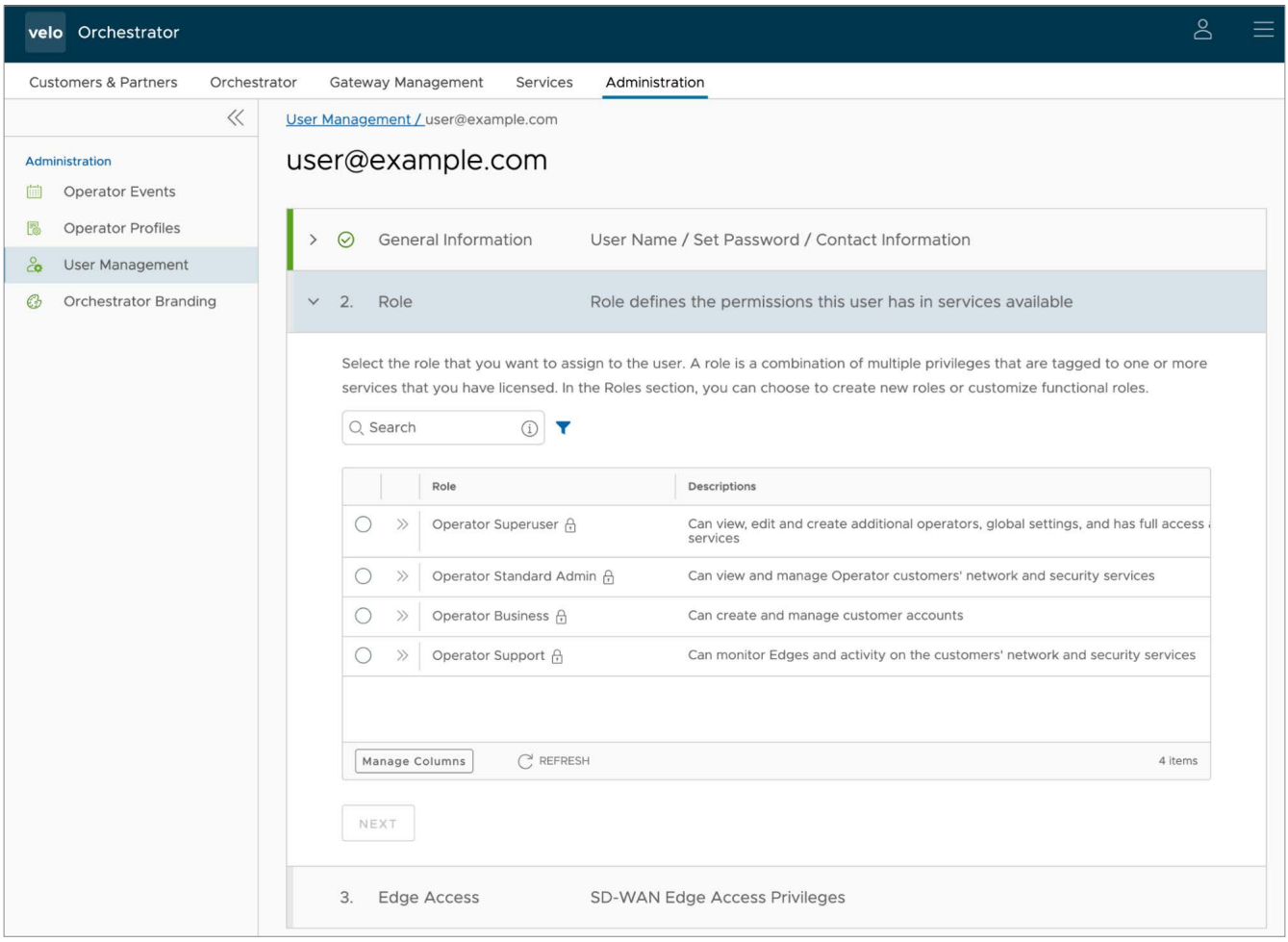
Role-Based Access Control on VCO

The VCO implements Role-Based Access Control (RBAC) to provide secure multi-tenancy to ensure that authenticated users can see and manage only the functions allowed by their assigned role. A user is categorized as one of three types defining their scope of access. Multiple roles are defined within each user type. Each role has a set of privileges that enable users of that role to perform a defined set of VCO functions.



Operator Users

This user type has visibility and management into the entire VCO including VCGs, Partners and Enterprise customers. The VCO portal for Operators provides access to all Enterprises and Partners, allows for assignment of Enterprises to Partners, and enables VCG management. Operator users are created on the VCO using the following interface:



Roles defined for Operator Users include:

SuperUser Operator

This role is assigned to a network administrator responsible for managing the overall network, the network administrator team, as well as the enterprise customers. This operator can create and modify other operator accounts on the VCO.

Standard Operator

This role is assigned to members of the network administrator team and can manage the network and the enterprise customers supported, but cannot create or modify other operator accounts on the VCO.

Business Specialist

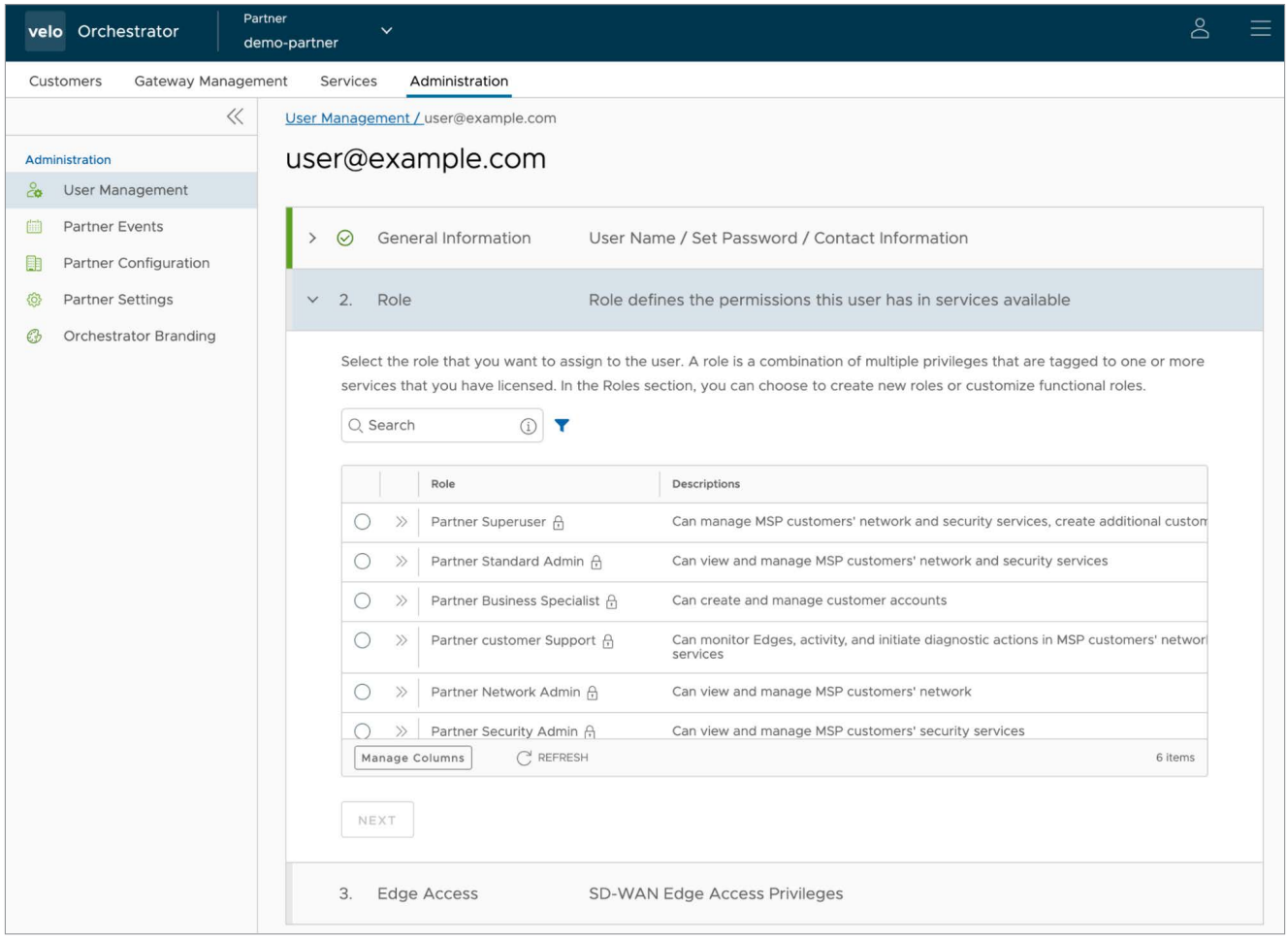
This role is assigned to a sales/business specialist responsible for a set of enterprise customers. These users can create and manage customer accounts but cannot configure or fully monitor edges.

Customer Support Operator

This role is assigned to customer support team members and can monitor and troubleshoot the Enterprise's VCE's.

Managed Service Provider (MSP) Users

This user type belongs to an MSP and manages multiple Enterprise customers. The VCO portal for MSPs provides access to their Enterprises, enables the creation of new Enterprise Accounts, and performs complete management of customer edges. MSP users are created by VCO Operators using the following interface:



Roles defined for MSP Users include:

Superuser

This role is assigned to an MSP network administrator responsible for managing the Partner network, the MSP administrator team, as well as the enterprise customers supported by the MSP. This user can create and modify customers and other MSP users on the VCO.

Standard Admin

This role is assigned to members of the MSP network administrator team. This user can view and manage the customers supported by the MSP, but cannot create or modify other MSP user accounts on the VCO.

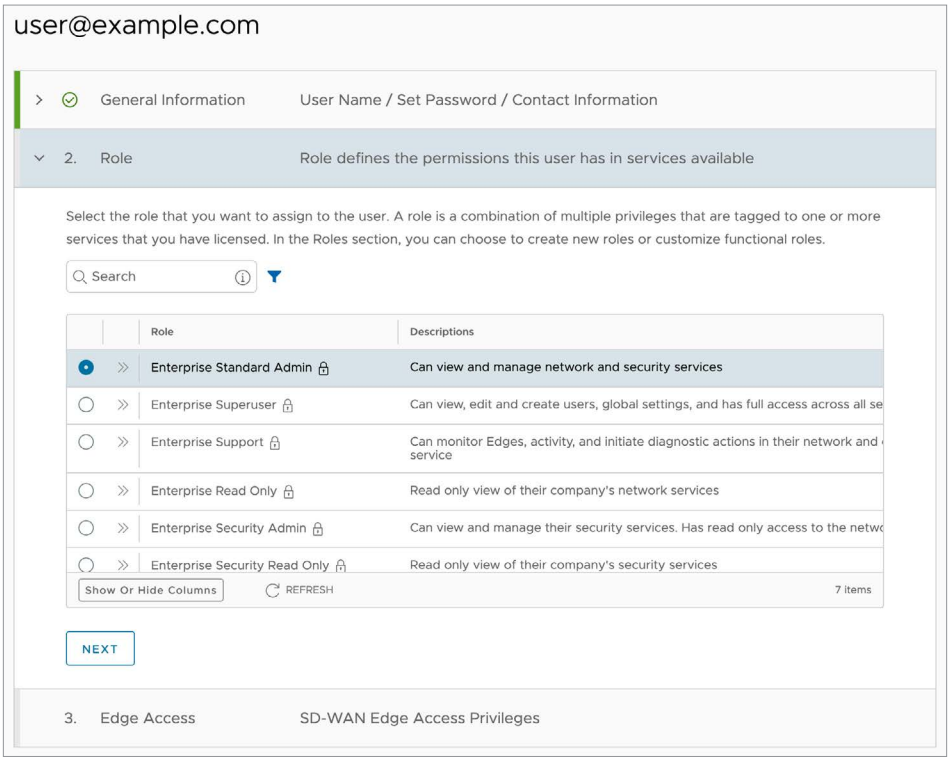
Customer Support

This role is assigned to members of the Enterprise's customer support team and can view and troubleshoot the Enterprise network.

Enterprise Users

This user type has visibility and management within a single Enterprise. The VCO portal for Enterprise users allows the creation, configuration, and monitoring of edges only within that enterprise.

Enterprise users are created by the Partners or Operators on the VCO using the interface shown below:



Roles defined for Enterprise Users include:

Superuser
This role is assigned to the Enterprise Customer's network administrator responsible for managing the Enterprise's IT operations and the rest of the administrator team. This user can create and modify additional administrator accounts on the VCO.

Standard Admin
This role is assigned to members of the Enterprise's IT network administrator team and can view and manage the Enterprise account, but cannot create or modify other administrator accounts on the VCO.

Customer Support
This role is assigned to members of the Enterprise's customer support team and can view and troubleshoot the Enterprise network.

Enterprise Read Only
This role can monitor the Enterprise network, but cannot make any configuration changes.

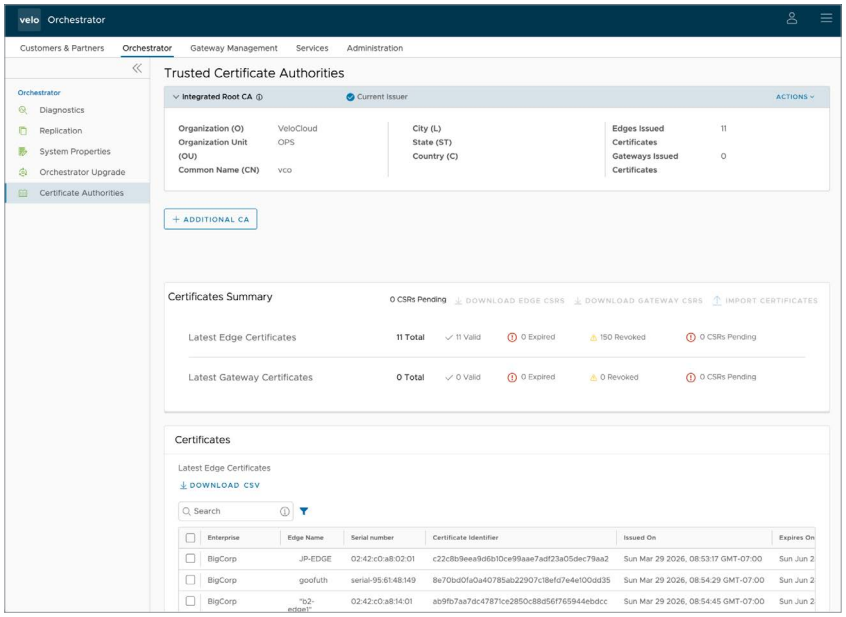
VCO Authentication

Radius
Operator users can be defined either locally on the VCO (Native mode) or via an external RADIUS server. The user role mapping can likewise be defined locally or via a RADIUS server and passed back as attributes during VCO authentication. By using RADIUS, authentication operators can leverage their existing user management infrastructure to determine authentication and access control functions on the VCO. Configuring RADIUS authentication options is available only to Operators.

Multi-Factor Authentication
The VCO supports Two Factor Authentication for Operator, MSP and Enterprise users. When enabled, user login attempts are verified with a pin sent via text message to a user's phone. The user provides the pin back to the VCO where it is validated to match a stored value for successful authentication.

Built-in Certificate Server in the VCO

The VCO uses a built-in Certificate server to manage the overall PKI lifecycle of all VCE's and VCG's.



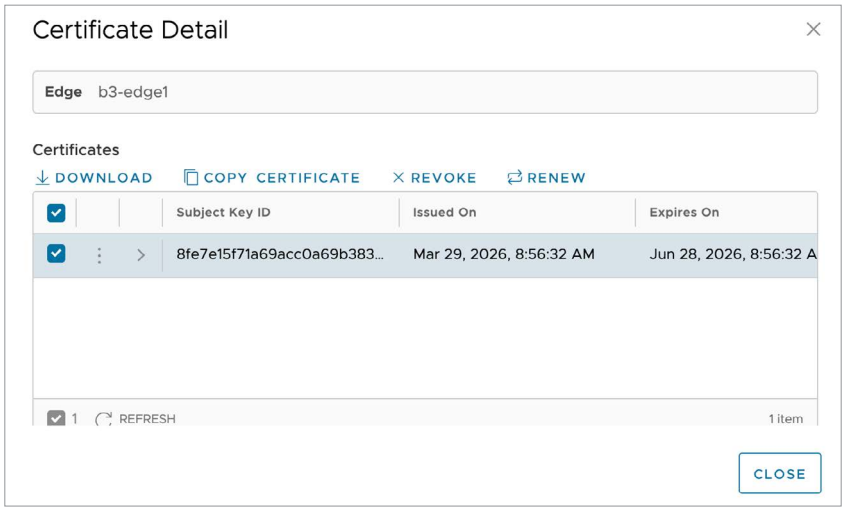
Certificates issued by the certificate server are used for the authentication of:

- Management plane TLS 1.3 tunnels between the VCO and VCE/VCG
- Control and Data plane IKEv2/IPsec tunnels between VCE's, and between VCE and VCG

Certificates are issued to VCE's when they are activated with the VCO. Device certificates and private keys are valid for 90 days, and refreshed every 65 days. The certificates are based on RSA 2048-bit private/public keys.

The VCO maintains a CRL, refreshed every 30 seconds, and the VCE's and VCG's retrieve the updated CRL from the VCO along with other periodic configuration updates.

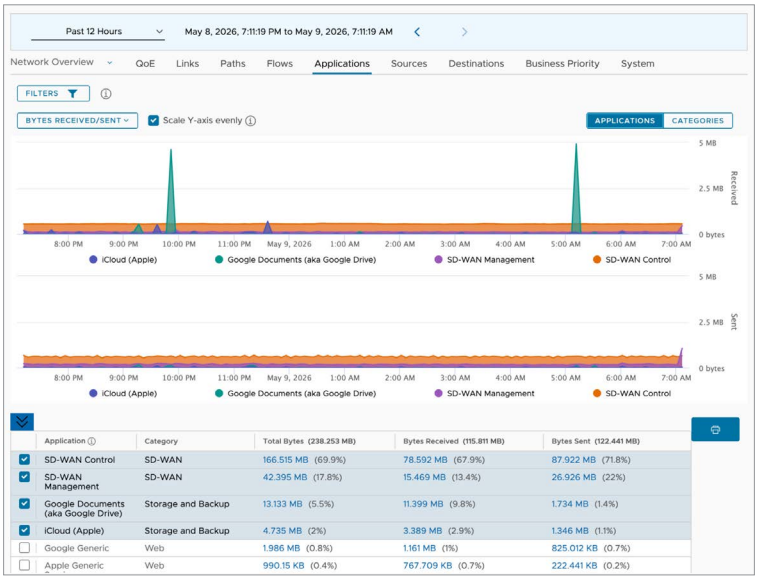
In case of a breach or device theft, the administrator can revoke the VCE/VCG certificates on the VCO and deactivate the VCE, or put a VCG out-of-service, thereby eliminating the compromised entities from the network. Certificate revocation can be performed by Superuser Operators.



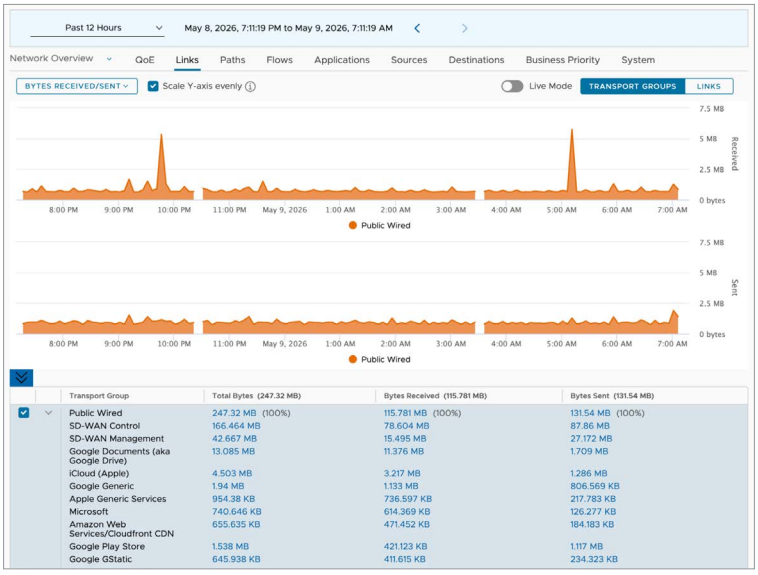
The public and private keys of the certificate server can be replaced by the administrator at any point, ensuring that unauthorized personnel cannot access the VCO with old certificates. In the event of a VCO certificate replacement, the VCE's do not have to be re-activated because the VCE certificates are pinned by the orchestrator and hence are considered safe for obtaining a new certificate from the replacement certificate server. An unauthorized user in possession of an older CA private key is unable to generate a certificate masquerading as a VCE to authenticate to the VCO because that would require generating the public-private key pair matching the VCE which it is attempting to masquerade as.

Traffic Visibility and Monitoring

The VCO provides in-depth visibility into the traffic flowing across the VeloCloud SD-WAN. VeloCloud's deep application recognition identifies more than 2500 applications and sub-applications using protocol data signatures, pattern matching, session correlation, certificate identification and an up-to-date database of well-known SaaS applications. Visibility on the VCO allows IT administrators to track trends in application use over time. Administrators can also view the source of these applications and quarantine clients who could potentially compromise the network.



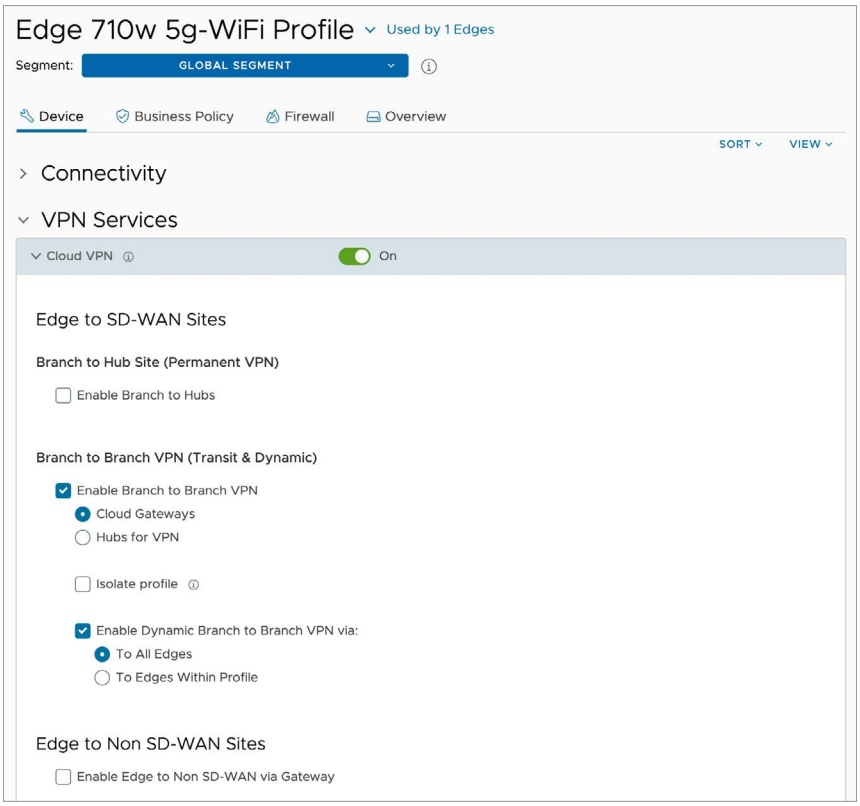
The VCO provides detailed traffic statistics for each of the transport types connected to a site. Application-to-transport mappings are useful to validate compliance requirements.



For example, many enterprises have InfoSec policies mandating that all non-business traffic (such as social networking or Internet media) must use low-cost public wired transport. It is therefore a violation of policy for any of these applications to use private wired transport. The administrator can identify the source host generating such traffic from the "Sources" tab shown above and apply a policy to block that host from sending non-compliant traffic over private wired transport.

Control and Data Plane Security

A VPN between VeloCloud sites, and/or between a VeloCloud site and a non-VeloCloud site, is configured by enabling the 'Cloud VPN' feature in the customer profile configuration as shown below.



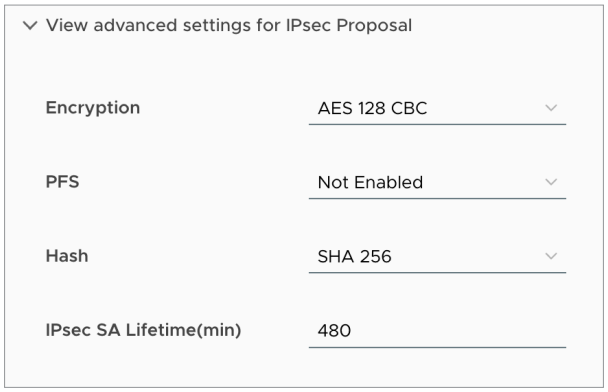
VPN between VeloCloud Sites

Traffic between VCE's, and between a VCE and VCG, is secured with a VCMP-over-IPsec tunnel. IPsec uses AES-128 or AES-256 bit keys for confidentiality, and SHA-1 or SHA-256 for data integrity protection. Encrypted traffic has a destination port of UDP 2426 which is the same as the VCMP tunnel port. VPN between VeloCloud sites can be:

Branch-to-DC-Hub Tunnels: IPsec for these tunnels is negotiated using IKEv2.

Branch-to-Branch Tunnels: These tunnels are established using one of 3 methods:

- Tunnels via the VCG: Branch-to-Branch traffic flowing through the VCG is encrypted with an enterprise-wide static AES-128 bit key. The encryption key is delivered by the VCO to the VCE during VCE activation. The traffic is encrypted and decrypted by the branch VCE's and there is no decryption at the VCG.
- Tunnels via a Hub: IPsec for these tunnels is established using IKEv2. The tunnels are established between the branch VCE and the Hub VCE. Branch-to-branch traffic is encrypted at the initiating branch, then decrypted and re-encrypted at the Hub before being decrypted again at the terminating branch site.
- Dynamic branch-to-branch tunnels: These IPsec tunnels are negotiated using IKEv2 and are directly established between the two branch VCE's.

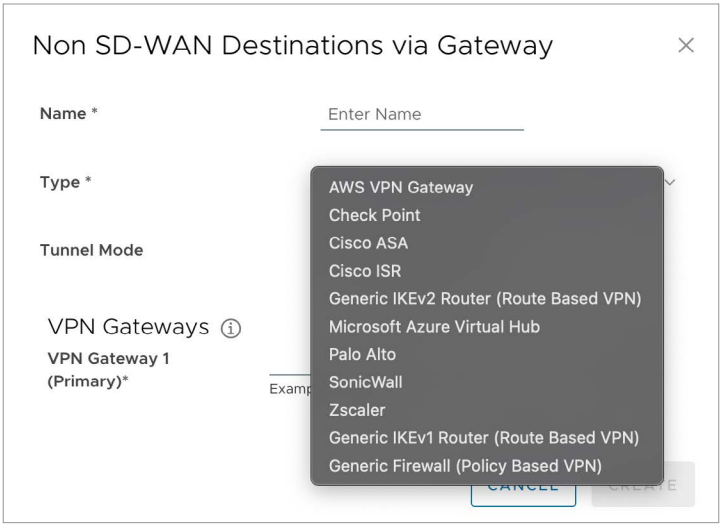


IPsec parameters are configured in the customer configuration page as shown above.

VPN Support between VeloCloud and Non-VeloCloud Sites

The VCG supports IPsec tunnels to non-VeloCloud sites such as Amazon AWS, Microsoft Azure, and other VPN concentrators. Connectivity to the non-VeloCloud site uses IKEv1 key management and pre-shared key authentication, and AES-128 or AES-256 IPSec for data encryption.

VPN traffic from a VCE to a non-VeloCloud site is decrypted at the intermediate VCG and then re-encrypted with the separate key negotiated with the non-VeloCloud site. The administrator can select from a list of specific or generic non-VeloCloud sites in the Network Services configuration page, as shown below.



Key Management and Rekey Interval

IKE lifetime is eight hours and IPSec lifetime is one hour. A rekey happens at a random interval between half of the lifetime and 20 seconds before the end of the lifetime.

Segmentation

Network isolation is a critical security feature for enterprise customers. Typical use cases include:

- Data isolation or separation by user (e.g. Guest, PCI, or Corporate), or byline of business (e.g. Engineering or HR)
- Supporting overlapping IP addresses between VLANs

Data Isolation/Separation

There are different ways to achieve network isolation, including physical isolation by separating the CDE and non-CDE devices

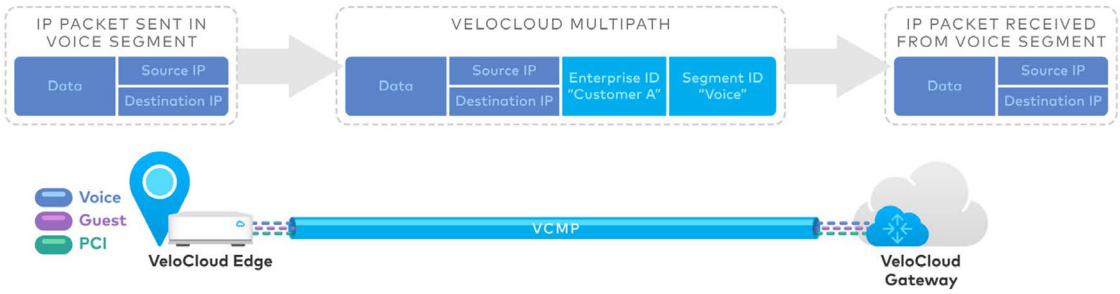
and wiring, or logical isolation by using technologies like inter-VLAN firewalls or virtual routing and forwarding (VRF). Use of inter-VLAN firewall rules to isolate the CDE network presents several drawbacks: it is complicated to create and manage the set of firewall policies, it requires a unique subnet for each VLAN on each edge, and it relies on a single global routing table which, in turn, increases the size of the routing table.

VeloCloud recommends segmentation to isolate networks—using a VRF-like concept. With segmentation, no inter-VLAN firewall rules are required because isolation is inherent, each segment can use the same subnet at each branch, and routing tables are simplified because they are per-segment.

VeloCloud segmentation comprises two layers:

- At the customer level, an Enterprise ID is inserted into the VCMP header to isolate different customers.
- Within the same customer, a Segment ID is inserted into the VCMP header to isolate different segments.

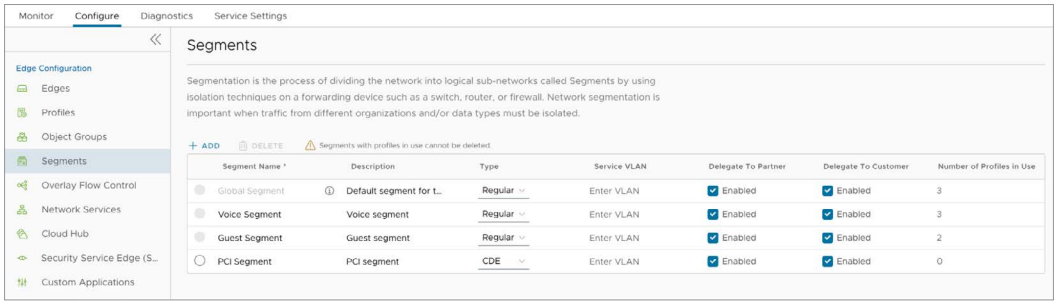
At the control plane level the combination of an Enterprise ID and a Segment ID identifies a unique segment in the SD-WAN network. Networks with different segment IDs cannot see each other's routes, thereby achieving the required isolation.



By default, all VCE interfaces—both LAN and WAN—share a default Global Segment. For customers who do not require segmentation, no additional segment is created and both the WAN and LAN share the same routing table. For customers who do require segmentation, segments must be created and assigned to the interfaces of the segments.

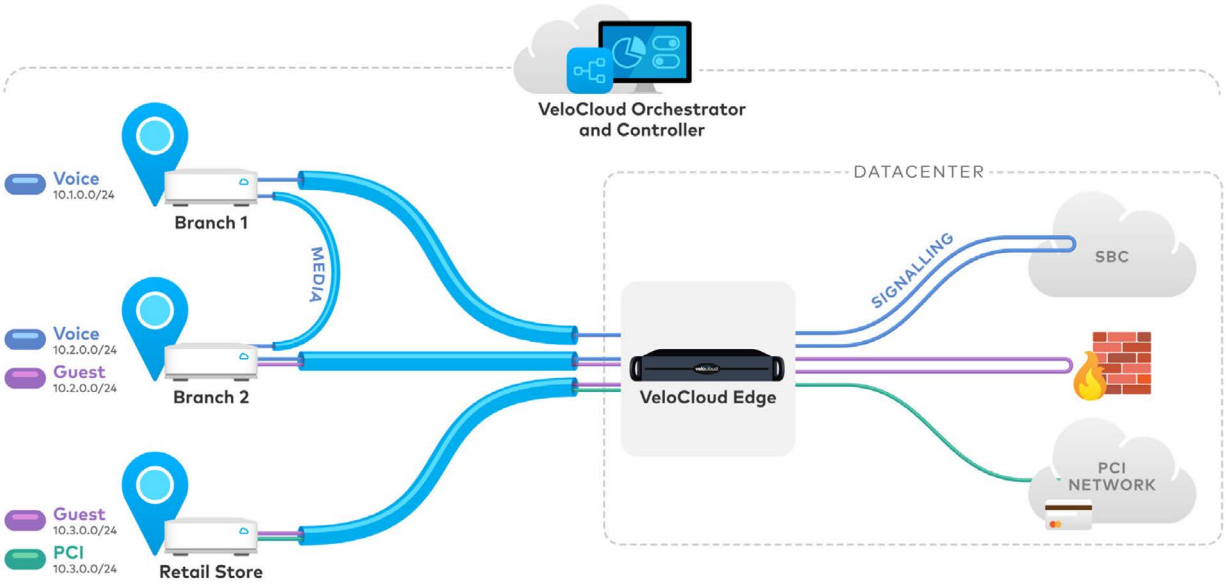
In the example retail customer network topology given below there are three services: two branches have voice service; the retail store branch has voice service; the retail store branches have Point-of-Sales (POS) endpoints that must be PCI compliant; and Guest WiFi is provided in select branches. Three segments must be provisioned: Voice, Guest and PCI. The Voice and Guest segments have no route information about the PCI network, which effectively isolates the PCI network from the rest of the customer network.

Further, with Velocloud Segment-aware topology insertion, different VPN profiles can be enabled for each segment. For example, Guest traffic can be backhauled to remote data center firewall services, Voice media can flow direct from Branch-to-Branch based on dynamic tunnels, and the PCI segment can backhaul traffic to the data center to exit out of PCI network. The UI snapshot below shows how to create the segments.



Supporting Overlapping IP Addresses between VLANs

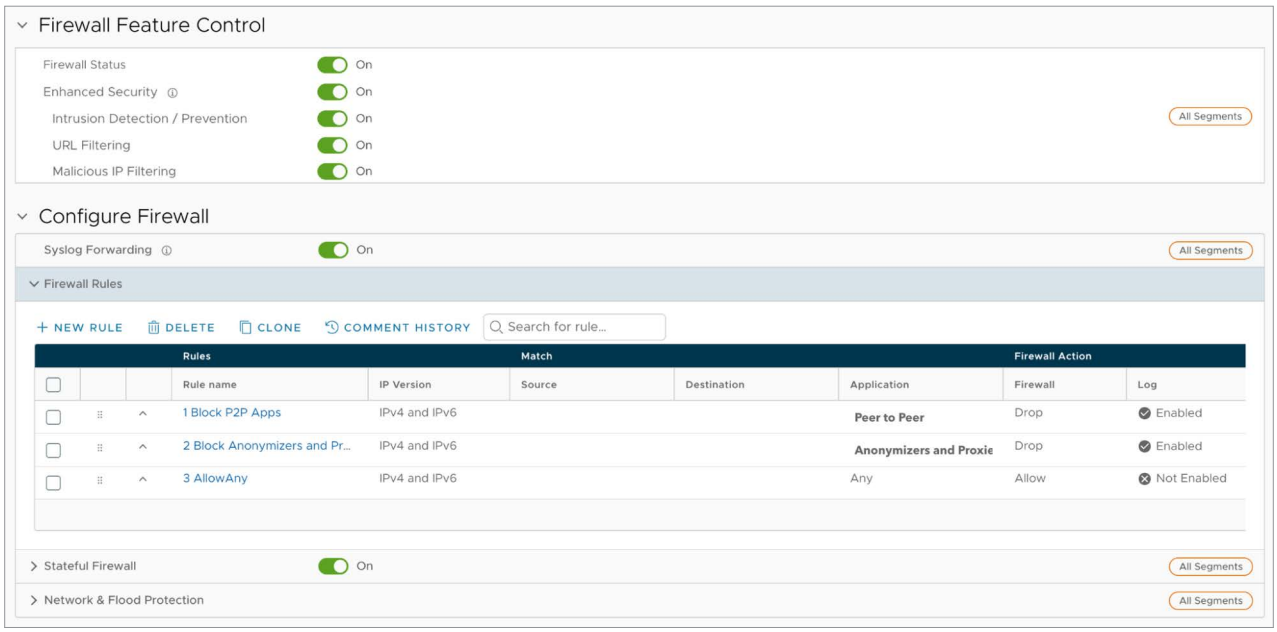
Sometimes it is desirable to use the same IP address in different VLANs at a branch. There are several use cases for this, but the two most common ones are enterprises simplifying their configurations by always being able to quickly identify which site a subnet belongs to (since it is the same in each segment), and service providers who offer "double play" or "triple play" services and assign the same subnet to each service corresponding to a different handoff on the Partner Gateway.



This use case is illustrated above with the addition of the subnet, corresponding to each segment, on the VeloCloud Branch Edge.

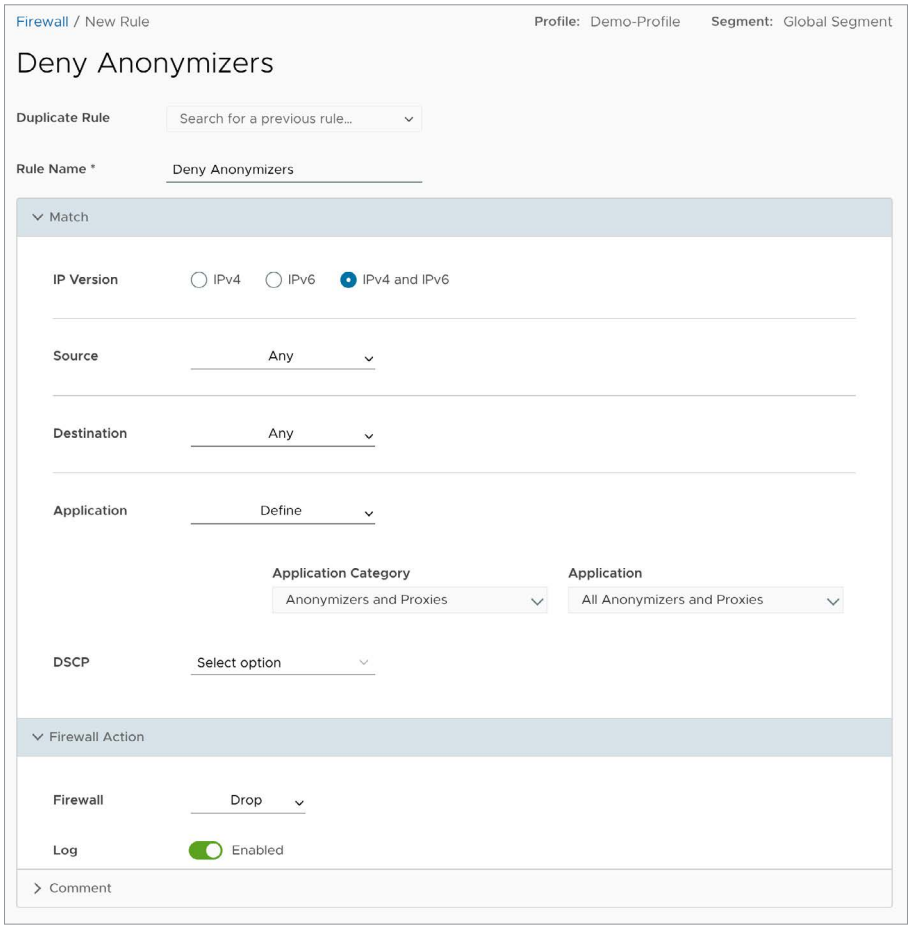
Integrated Firewall

The VCE supports stateful and context-aware policies. The firewall delivers granular control of micro-applications and protocol-hopping applications, such as Skype and other peer-to-peer applications (e.g. disabling Skype video and chat, but allowing Skype audio). The secure firewall service is user and device OS-aware with the ability to segregate voice, video, data, and compliance traffic. Policies are easily controlled for BYOD devices (for example Apple iOS, Android, Windows, MAC OS) on the corporate network.



Outbound Firewall Rules

These rules filter application traffic originating from hosts or subnets in the branch LAN destined towards Internet/WAN sites. The firewall recognizes 5000+ applications and can be configured to perform very granular filtering. Actions include allowing or denying the traffic, and any action taken can optionally be logged.



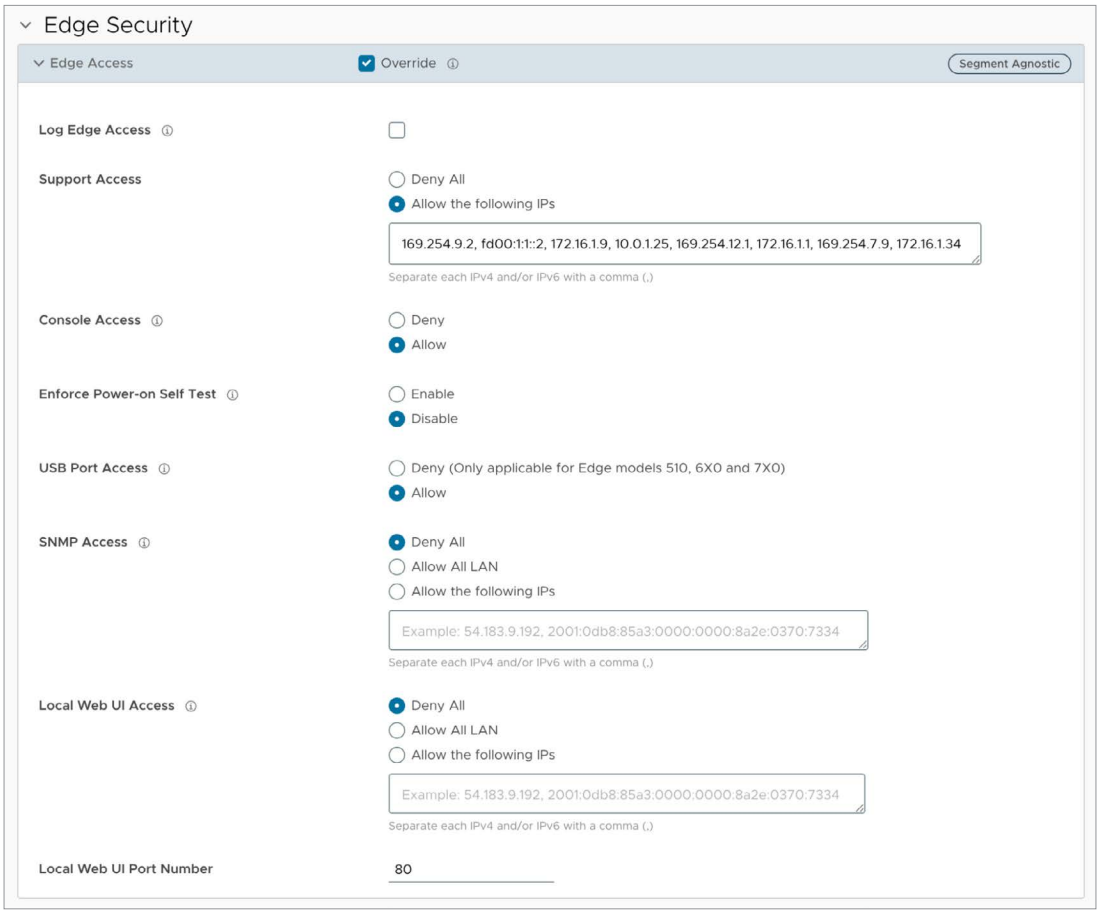
Inbound Firewall Rules

These rules filter traffic originating from Internet/WAN sites destined towards hosts in the branch LAN. Two types of Inbound firewall rules are supported:

- **Port Forwarding Rules:** These rules redirect traffic from specific WAN sites and ports, destined to a host and port within the branch LAN. Traffic can be forwarded to a different host in the branch, such as an IDS/IPS server, for inspection before reaching the intended host.
- **1:1 NAT Rules:** These rules map a public IP address to an Inside (LAN) IP address. A 1:1 NAT mapping can only be configured with IP addresses that do not belong to the VeloCloud Edge. The mapping can also translate outside IP addresses in different subnets from the WAN interface address if the ISP routes traffic for the subnet towards the VeloCloud Edge. Each mapping is between one IP address outside the firewall and one LAN IP address inside the firewall. Within each mapping, the ports forwarding to a specific inside IP address can be configured.

In addition to securing the branch, the firewall can also limit traffic destined to the VCE itself. The firewall can be configured to restrict SSH and SNMP access to the VCE, to restrict access to the VCE's local Web UI, and to change the port number from the default of 80.

It is recommended to deny all SSH access to the VCE and, at most, to allow access only to the customer support team.

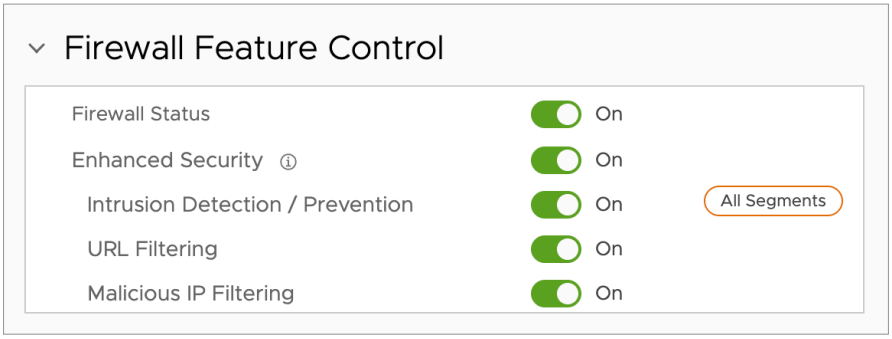


Enhanced Firewall Services

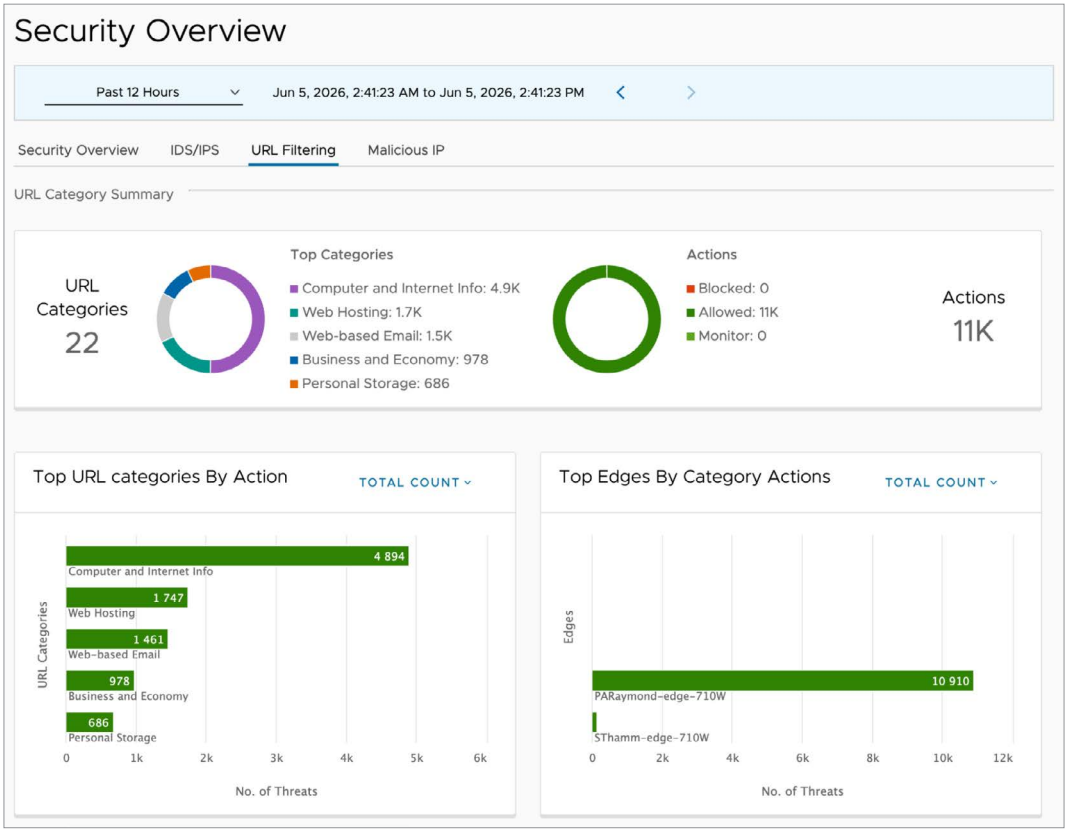
VeloCloud Enhanced Firewall Services (EFS) is an add-on security feature for VeloCloud SD-WAN Edges that brings enterprise-grade, cloud-managed security directly to branch locations. It provides advanced, native threat protection for Branch-to-Branch, Branch-to-Hub, and Direct Internet Access (DIA) traffic.

EFS expands on the integrated firewall with advanced security layers:

- Intrusion Detection and Prevention (IDS/IPS): Actively scans and drops malicious traffic matching known exploit signatures.
- URL Category and Reputation Filtering: Controls and blocks access to websites based on their content category (e.g., adult content, gambling) or security risk level.
- Malicious IP Filtering: Automatically blocks inbound and outbound traffic connecting to known malicious or suspicious IP addresses.

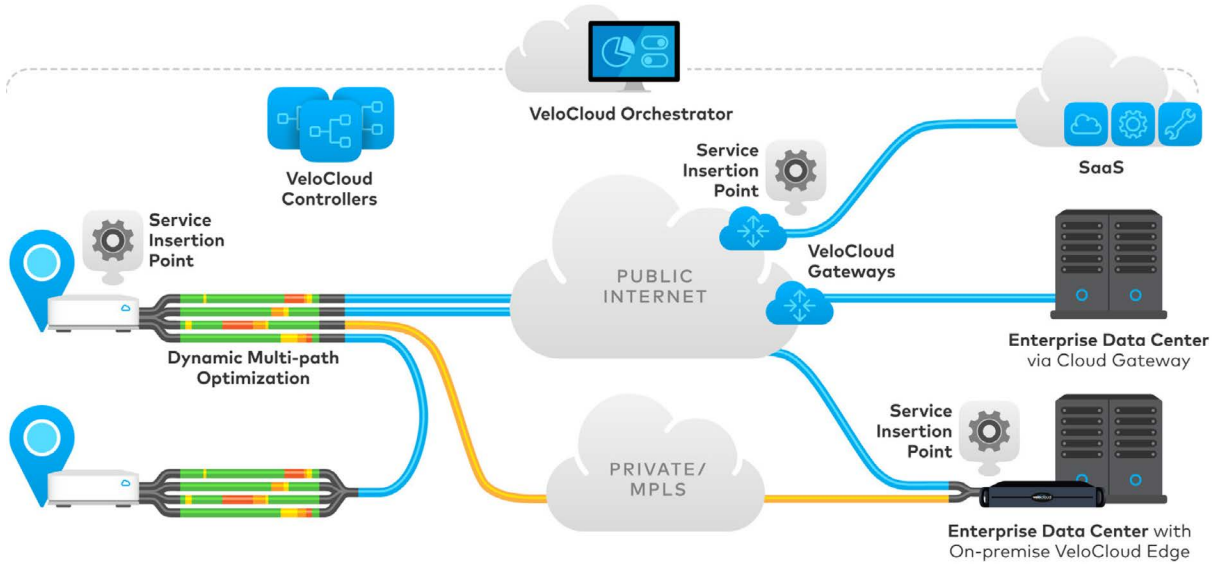


All EFS related security events are reported in a dedicated Security Dashboard available in VCO. The Security Dashboard provides an enterprise-wide threat landscape overview and logging, allowing for quick identification of attacking sources and affected edges.



Security Service Insertion Options

The VeloCloud SD-WAN supports multiple options for inserting security services into the network, accommodating a wide range of customer requirements for secure SD-WAN deployments. Security services can be inserted at cloud and on-premise sites.

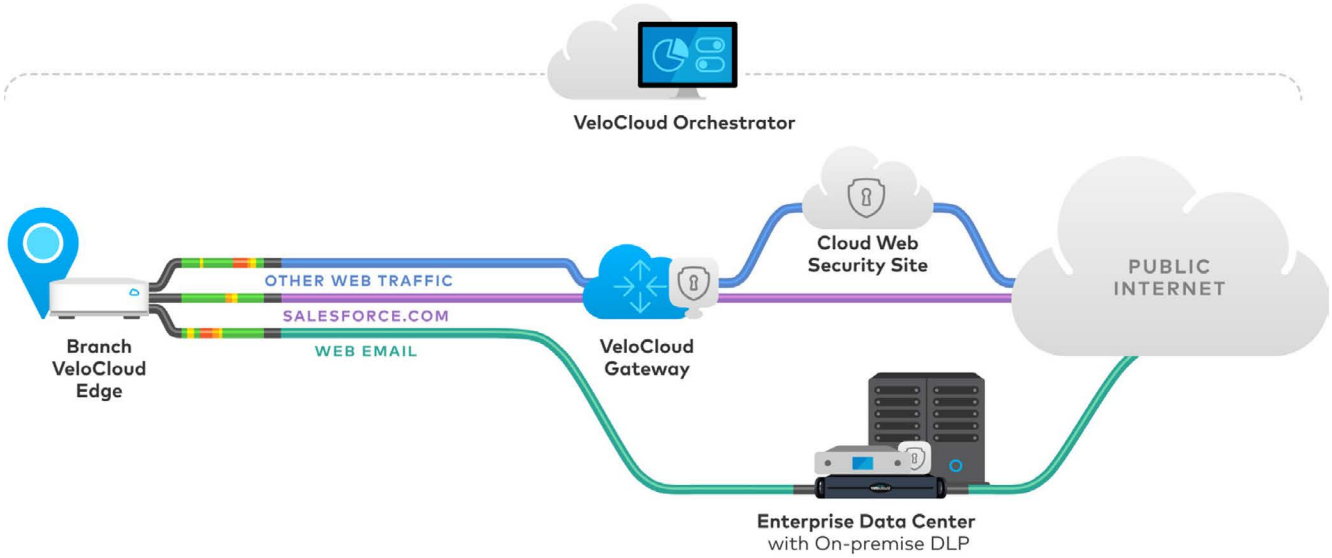


Cloud Web Security Service Insertion

In traditional WANs, deploying distributed security services such as firewalls across an enterprise network is challenging. Some common issues encountered include:

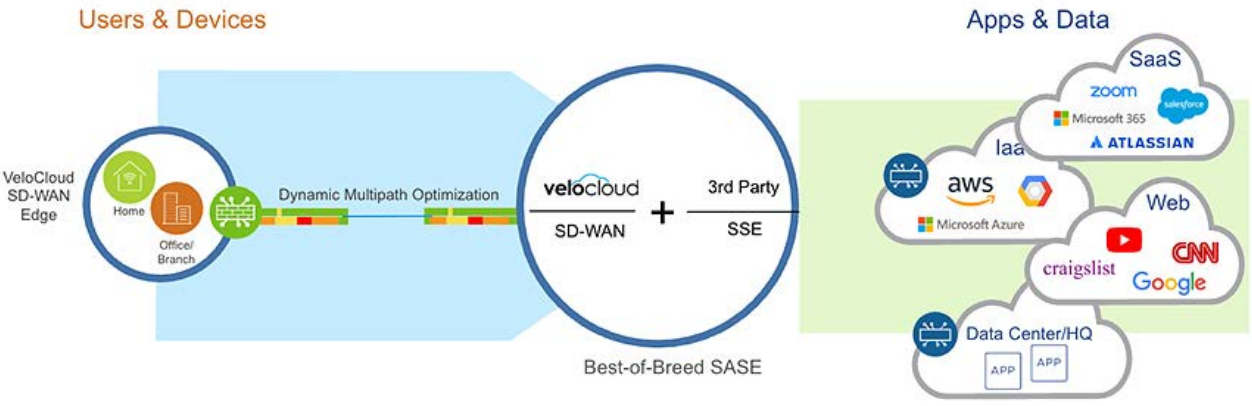
Complex and Cumbersome Integration

With branch office sites connecting directly to the Internet, customers want to leverage cloud-based security services to protect their branch networks. However, integration with well-known cloud web security vendors is complex and cumbersome to manage, requiring a VPN tunnel from each branch site to the cloud web security site.



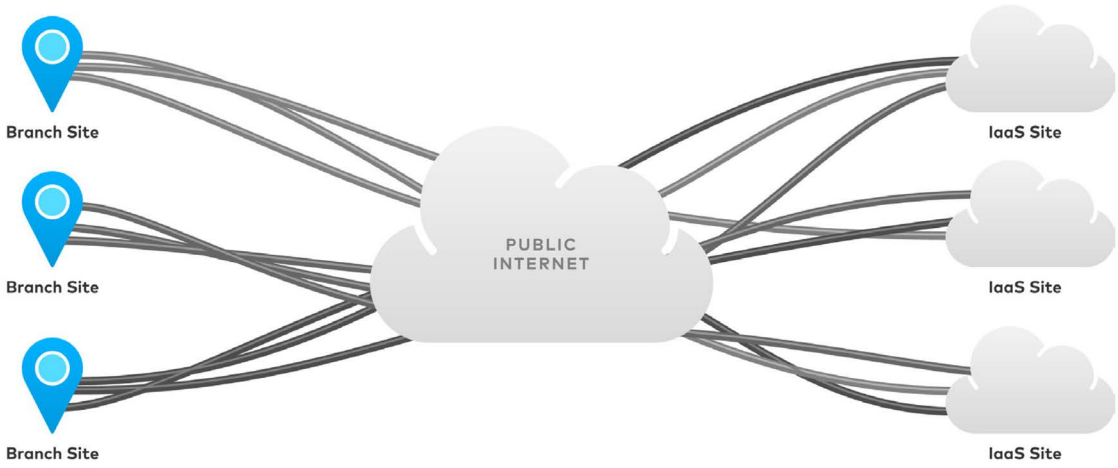
With the VeloCloud SD-WAN, customers can integrate cloud web security in a matter of minutes. Integration is enabled by establishing an IKE/IPsec tunnel from the VCG to the Cloud Web Security Gateway. All branch sites already connect to the VCG over VCMP tunnels. The VCG forwards Internet-bound traffic from the branch sites to be filtered by the cloud web security infrastructure as shown above.

VeloCloud leverages a Best-of-Breed SASE strategy by combining its industry-leading SD-WAN with seamless integration of leading Security Service Edge (SSE) solutions. This enables secure, reliable, and optimized connectivity for users—regardless of location—to applications across the edge, cloud, and data center. The solution enhances user experience, simplifies operations, and supports compliance risk mitigation.

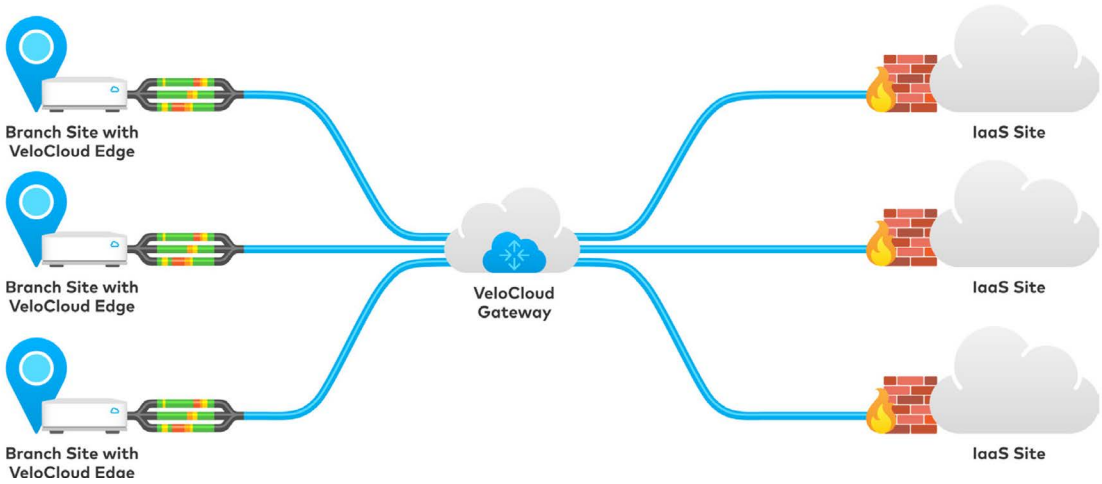


IPsec Tunnel Scalability and Optimization

When customers desire not to backhaul SaaS/IaaS traffic through their data center, traffic flows from each branch site to each IaaS instance requires a separate VPN tunnel. This creates onerous VPN configurations and management: N sites, with tunnels to each of N IaaS instances, results in NxN tunnels to manage.



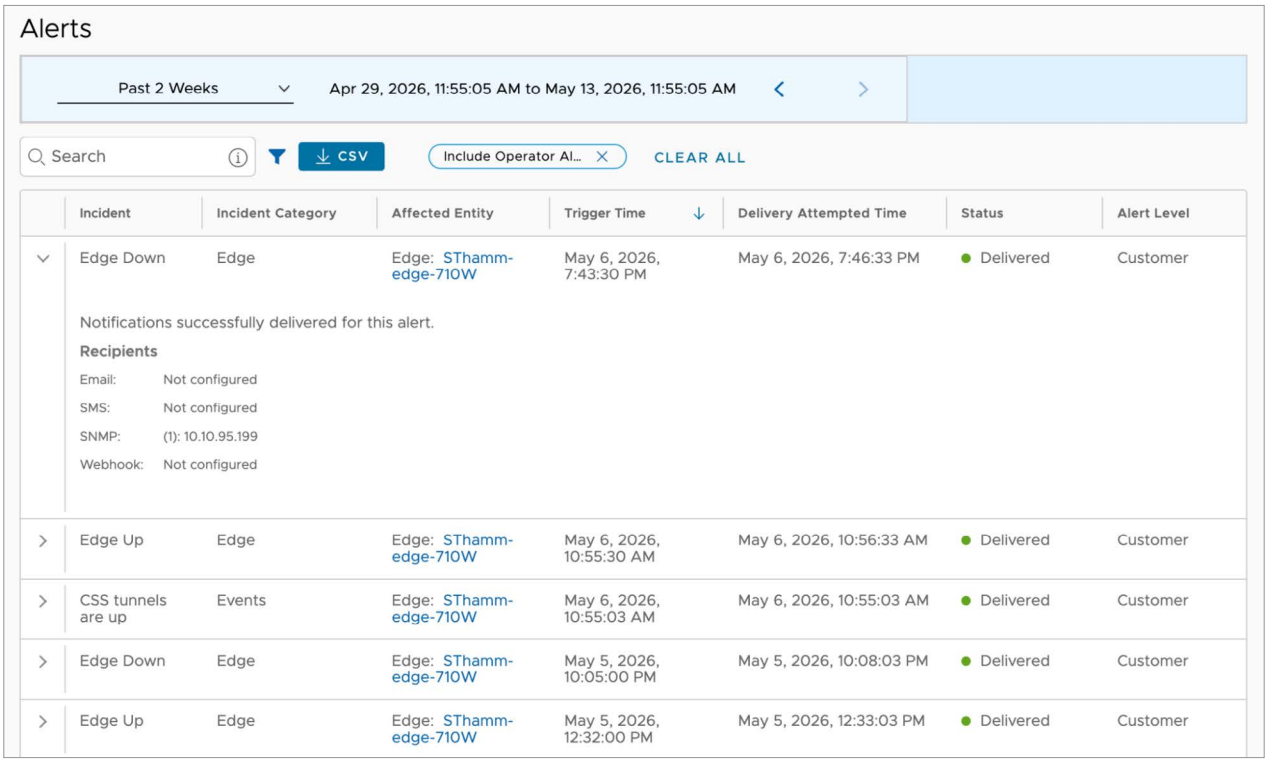
With the VeloCloud SD-WAN solution, tunnels are automatically established from each branch site to the cloud-based VCG. The VCG establishes a single tunnel to the IaaS instance and forwards all branch traffic to the SaaS site. Instead of building individual branch VPN tunnels to each SaaS application, customers now only need a single VPN tunnel to carry all branch traffic to the application. This reduces the NxN tunnel nightmare to just N tunnels from the branches to the VCG and a single tunnel from the VCG to the SaaS site.



Alerts and Logging

Security Alerts and Notifications

The VCO generates alerts to notify the administrator of specific events, such as when VCE or Link status changes to down/up, a VCE fails over from active to standby, or when a VPN tunnel between the VCG and the third party VPN gateway fails and cannot be re-established. Additionally, the VCO generates an alert if it receives no keepalive from an edge for an extended period of time. Alerts can be sent in the form of email or an SMS message to a cell phone.



Firewall Logs

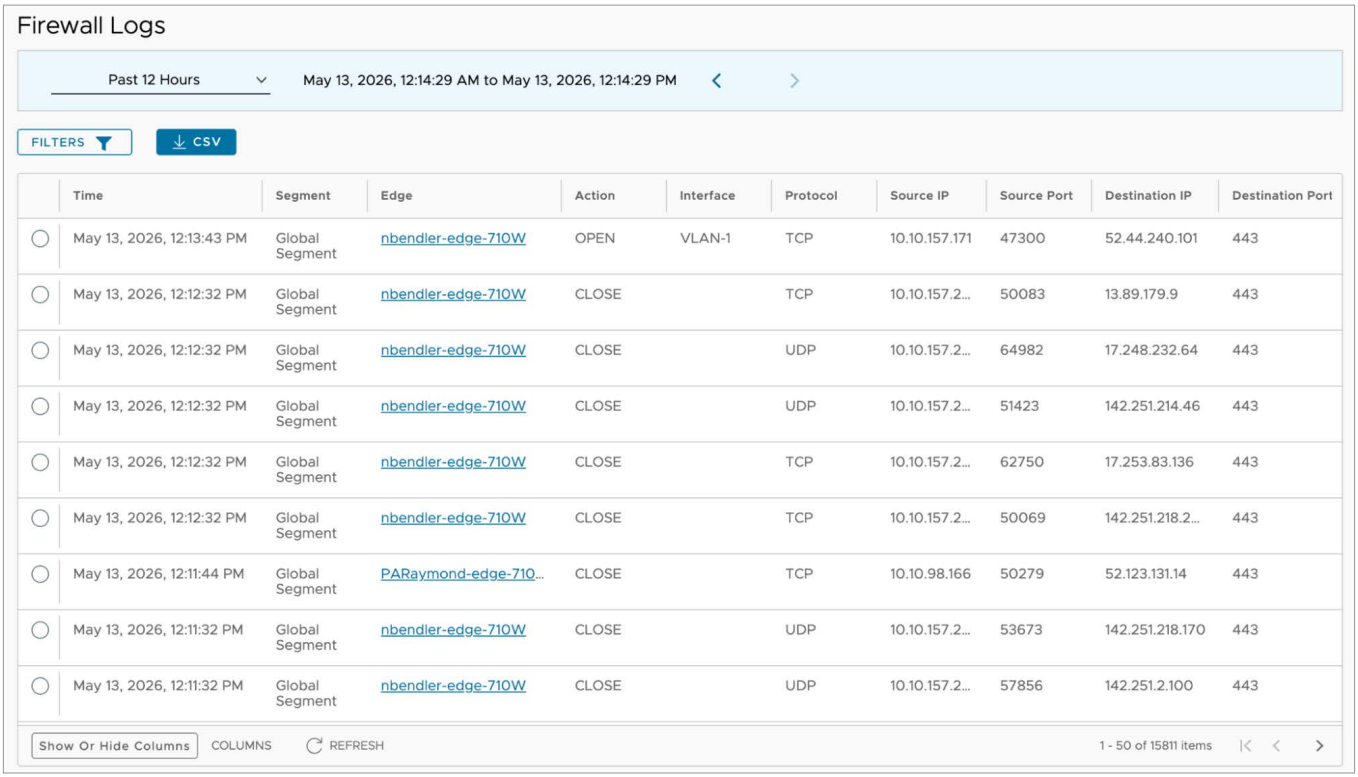
The integrated VCE firewall can be configured to generate logs when traffic is permitted or denied. The traffic could be traversing the VCE, or it could be destined to the VCE. Firewall logs can be enabled/disabled per VCE for a customer, and is displayed on the VCO on a per customer basis. It is recommended to enable logging only for deny events as the logs for permit events could be voluminous and quickly overrun available VCO storage.

Event Logs

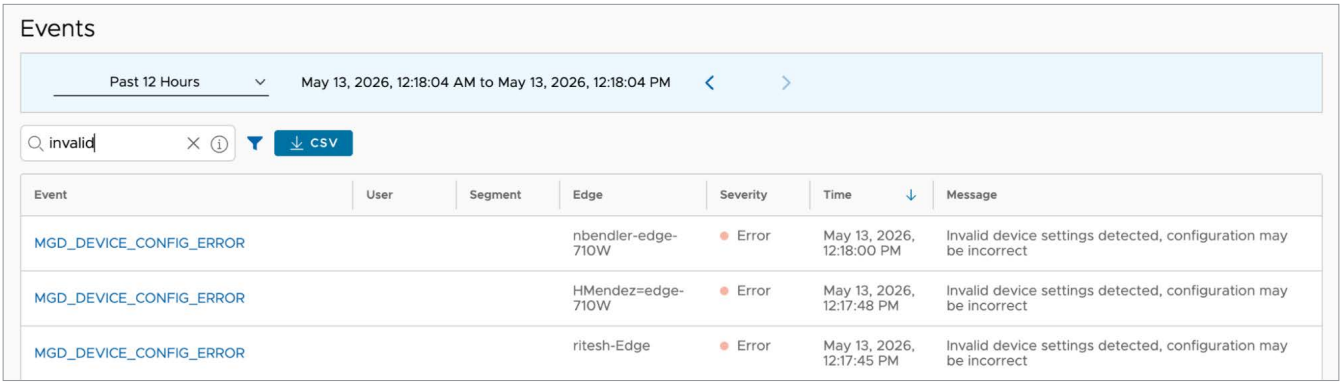
Event logs are useful to create an audit trail of user activity. Logs also provide a historical record of user activity and VCE and Link states. Events logged at the VCO include events such as:

- User Login: An administrator user has logged into the VCO
- User Created: An administrator user has been created
- Profile Updated: An administrator user has updated a profile or edge configuration
- Configuration Applied: A new configuration was applied to an edge
- Edge Provisioned: An edge was created on the VCO (but is not yet activated)

- Edge Activated: An edge was activated
- Link Up / Link Down: Link status has changed to up or down
- Edge Up / Edge Down: Edge status has changed to up or down



Certain events are seen only by the Operator, for example, gateway and orchestrator related events. Certain events are not service impacting, but require further investigation as they may become service impacting if unresolved. Certain events impact or degrade SD-WAN service quality and require immediate attention. VCO APIs can be used programmatically to retrieve event logs and post the events to standard log collectors. A detailed list of events retrievable via API can be made available by your VeloCloud point of contact.



External Logging

VeloCloud supports external logging via Syslog or VeloCloud Orchestrator hosted log storage. You can forward event logs and firewall logs from your Enterprise Edges and the Orchestrator directly to external SIEM collectors. This enables organizations to retain network access events and other types of network security related events in long term storage for compliance and auditing purposes.

Infrastructure Security

Device Security

The VCO/VCG/VCE run custom Linux environments with up-to-date, hardened kernels. Periodic external security assessments are also performed. Critical security vulnerabilities, when discovered, are immediately patched. Non-critical security patches are scheduled as part of regular software upgrades.

Software Security

The VCO/VCG/VCE are subjected to periodic vulnerability scans and fuzz testing, using well known tools to ensure that the software is not vulnerable to attacks and exploits. Some test details for the components include:

- **VCO/VCG/VCE Software Security:** Weekly scans are performed on VCO/ VCG/VCE using the Qualys Express Lite tool. Vulnerabilities identified are assessed and patched based on the criticality of the scan result. There are three categories of scan results: Confirmed Vulnerability, Potential Vulnerability, and Information gathered. Service impacting vulnerabilities are fixed and patched within 24 hours of identifying the issue.
- **VCE Software Security:** VCEs undergo intensive fuzz tests using the Codenomicon Defensics tool. These tests are executed as part of the QA infrastructure for every software release. In these tests, application packets are deliberately malformed and delivered to the VCE to see if a failure occurs. Defects detected in these tests are fixed prior to the software being released.

VCG and VCO Physical and Network Access

The VCG and VCO run in secure SSAE Type II Data Centers and Tier 1 Cloud Data Centers. Only VeloCloud operations personnel with secure tokens have access to the VCG to perform maintenance.

Network ports are locked down to the maximum possible level: for the VCG, only UDP 2426 traffic is permitted; for the VCO, only TLS1.2 (TCP/443) traffic is permitted. All other ports are locked and any traffic to these ports is silently discarded.

VCO Data Security

Data such as configurations, logs and events are stored by the VCO. The VCO runs in a secure cloud data center and employs strict Role-Based Access Control mechanisms that restrict VCO access to authorized users.

The certificates and keys of the integrated VCO-CA are stored in a secure database encrypted using an AES-128 bit key. This encryption key is not stored in any persistent storage and is provided by the operator on orchestrator startup.

Security Patch Distribution

VeloCloud constantly monitors security issues that might impact the VCO/VCG/VCE. Security patches with critical fixes are immediately pushed from the VCO to the VCE's and VCG's. Non-critical patches are distributed once a month.

Security Certifications and Compliance

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2, is a U.S. government computer security standard used to approve cryptographic modules. VeloCloud software is in the process of attaining FIPS 140-2 certification and is listed on the NIST website as one of the vendors with software Implementation Under Test (IUT):
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140IUT.pdf

PCI Compliance

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of requirements developed to help companies ensure the security of credit-card-holder data. Merchants who store, process, and/or transmit card-holder data must meet the minimum levels of security defined in the PCI DSS security standard. The VeloCloud SD-WAN solution helps enterprises meet these requirements.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989