

---

## Security Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing. There are multiple problems with the traditional ways of securing networks, including:

- Very little emphasis is placed on ensuring the authenticity of the devices involved in the communication.
- Securing the links between a pair of devices involves tedious and manual setup of keys and shared passwords.
- Scalability and high availability solutions are often at odds with each other.

---

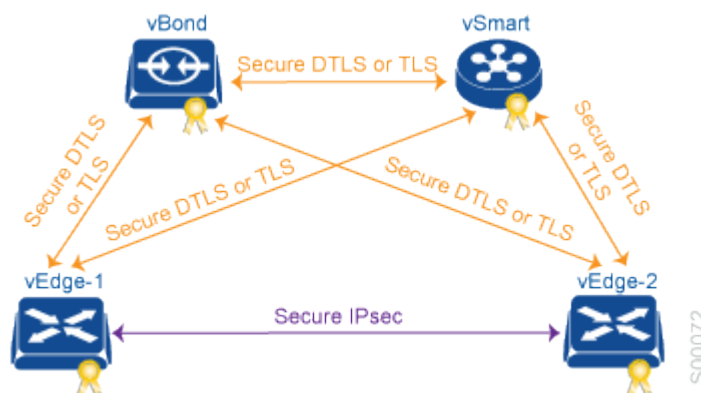
## Viptela Security Components

The Viptela solution takes a fundamentally different approach to security, basing its core design around the following precepts:

- Authentication—The solution ensures that only authentic devices are allowed to send traffic to one another.
- Encryption—All communication between each pair of devices is automatically secure, completely eliminating the overhead involved in securing the links.
- Integrity—No group keys or key server issues are involved in securing the infrastructure.

These three components—authentication, encryption, and integrity—are key to securing the Viptela network infrastructure.

The articles on [Control Plane Security Overview](#) and [Data Plane Security Overview](#) examine how authentication, encryption, and integrity are implemented throughout the Viptela overlay network. The security discussion refers to the following illustration of the components of the Viptela network—the vSmart controller, the vBond orchestrator, and the vEdge routers. The connections between these devices form the control plane (in orange) and the data plane (in purple), and it is these connections that need to be protected by appropriate measures to ensure the security of the network devices and all network traffic.



---

## Security Provided by NAT Devices

While the primary purpose of NAT devices is to allow devices with private IP addresses in a local-area network (LAN) to communicate with devices in public address spaces, such as the Internet, NAT devices also inherently provide a level of security, functioning as hardware firewalls to prevent unwanted data traffic from passing through the Viptela edge routers and to the LAN networks in the service-side networks connected to the vEdge router.

To enhance the security at branch sites, you can place the vEdge router behind a NAT device. The vEdge router can interact with NAT devices configured with the following Session Traversal Utilities for NAT (STUN) methods, as defined in [RFC 5389](#):

- Full-cone NAT, or one-to-one NAT—This method maps an internal address and port pair to an external address and port. Any external host can send packets to LAN devices behind the vEdge router by addressing them to the external address and port.
- Address-restricted cone NAT, or restricted-cone NAT—This method also maps an internal address and port to an external address and port. However, an external host can send packets to the internal device only if the external address (and any port at that address) has received a packet from the internal address and port.
- Port-restricted cone NAT—This method is a stricter version of restricted-cone NAT, in which an external host can send packets to the internal address and port only if the external address and port pair has received a packet from that internal address and port. The external device must send packets from the specific port to the specific internal port.
- Symmetric NAT—With this method, each request from the same internal IP address and port to an external IP address and port is mapped to a unique external source IP address and port. If the same internal host sends a packet with the same source address and port but to a different destination, the NAT device creates a different mapping. Only an external host that receives a packet from an internal host can send a packet back. vEdge routers support symmetric NAT only on one side of the WAN tunnel. That is, only one of the NAT devices at either end of the tunnel can use symmetric NAT.

When a vEdge router operates behind a NAT device running symmetric NAT, only one of the NAT devices at either end of the tunnel can use symmetric NAT. The vEdge router that is behind a symmetric NAT cannot establish a BFD tunnel with a remote vEdge router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT.

To allow a vEdge router to function behind a symmetric NAT, you must configure the vManage NMS and vSmart controller control connections to use TLS. DTLS control connections do not work through a symmetric NAT.

---

## Additional Information

[Control Plane Security Overview](#)

[Data Plane Security Overview](#)

