

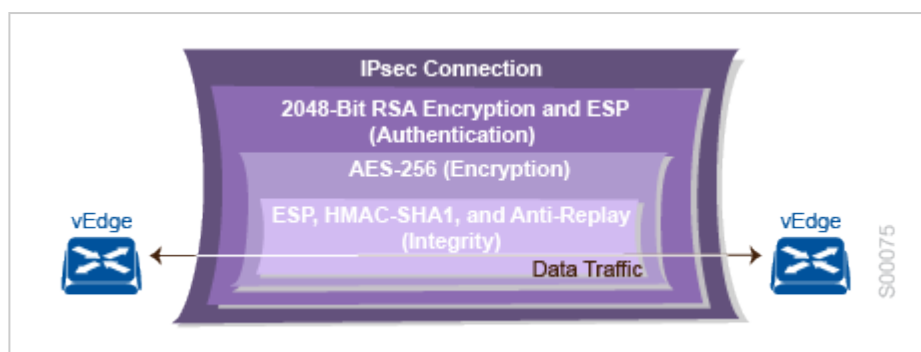
Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the vEdge routers in the Viptela overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone would be able to sniff the traffic, and it would be easy to implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Viptela data plane is the security of the control plane. Because the control plane is secure—all devices are validated, and control traffic is encrypted and cannot be tampered with—we can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of vEdge routers.

The data plane provides the infrastructure for sending data traffic among the vEdge routers in the Viptela overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Viptela data plane implements the key security components of authentication, encryption, and integrity in the following ways:

- **Authentication**—As mentioned above, the Viptela control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:
 - RSA encryption with 2048-bit keys.
 - Two standard protocols from the IPsec security suite framework, Encapsulation Security Payload (ESP) and Authentication Header (AH), are used to authentication the origin of data traffic.
- **Encryption**—The standard ESP protocol protects the data packet's payload, and the standard AH protocol protects both the payload and the non-mutable header fields. Key exchange encryption is done using the AES-256 cipher.
- **Integrity**—To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:
 - The ESP protocol encapsulates the payload of data packets.
 - The HMAC-SHA1 algorithm, which is used by the IPsec AH protocol, combines a keyed-hash authentication code with SHA-1 cryptography to ensure data integrity. AH encapsulates the non-mutable fields in the outer IP header and the payload of data packets. You can configure the integrity methods supported on each vEdge router, and this information is exchanged in the router's TLOC properties. If two vEdge peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.



- The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

Data Plane Authentication and Encryption

Before a pair of vEdge routers can exchange data traffic, they establish an IPsec connection between them, which they use as a secure communications channel, and then the routers authenticate each other over this connection. As with the control plane, the data plane uses keys to perform Viptela device authentication.

In a traditional IPsec environment, key exchange is handled by the Internet Key Exchange (IKE) protocol. IKE first sets up secure communications channels between devices and then establishes security associations (SAs) between each pair of devices that want to exchange data. IKE uses a Diffie-Hellman key exchange algorithm to generate a shared key that encrypts further IKE communication. To establish SAs, each device (n) exchanges keys with every other device in the network and creates per-pair keys, generating a unique key for each remote device. This scheme means that in a fully meshed network, each device has to manage n^2 key exchanges and (n-1) keys. As an example, in a 1,000-node network, 1,000,000 key exchanges are required to authenticate the devices, and each node is responsible for maintaining and managing 999 keys.

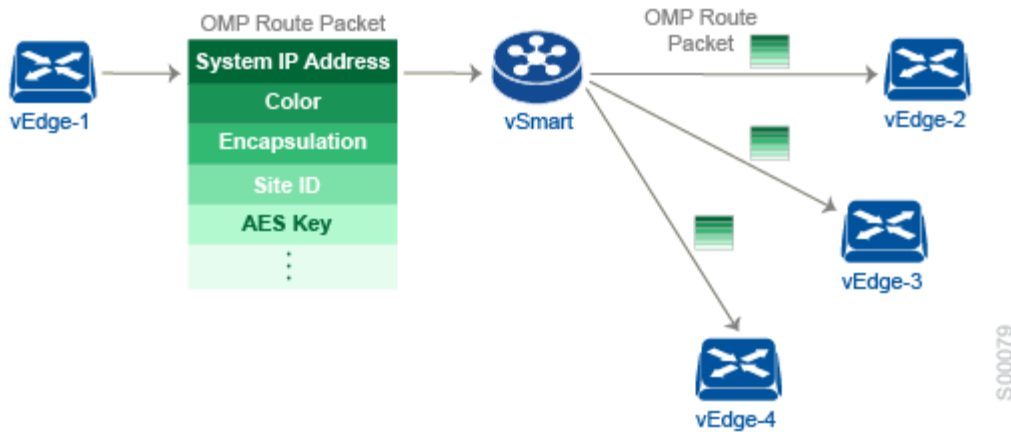
The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- The handshaking required to set up the communications channels is both time consuming and resource intensive.
- The processing required for the key exchange, especially in larger networks, can strain network resources and can take a long time.

The Viptela implementation of data plane authentication and encryption establishes SAs between each pair of devices that want to exchange data, but it dispenses with IKE altogether. Instead, to provide a scalable solution to data plane key exchange, the Viptela solution takes advantage of the fact that the DTLS control plane connections in the Viptela overlay network are known to be secure. Because the Viptela control plane establishes authenticated, encrypted, and tamperproof connections, there is no need in the data plane to set up secure communications channels to perform data plane authentication.

In the Viptela network, data plane encryption and key generation are done by AES-256, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each vEdge router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the vEdge router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other vEdge routers in the network. In this way, the AES keys for all the vEdge routers are distributed across the network. Even though the key exchange is symmetric, Viptela devices use it in an asymmetric fashion. The result is a simple and scalable key exchange process that does not use per-pair keys.





If control policies configured on a vSmart controller limit the communications channels between network devices, the reachability advertisements sent by the vSmart controller contain information only for the vEdge routers that they are allowed to exchange data with. So, a vEdge router learns the keys only for those vEdge routers that they are allowed to communicate with.

To further strengthen data plane authentication and encryption, vEdge routers regenerate their AES keys aggressively (by default, every 24 hours). Also, the key regeneration mechanism ensures that no data traffic is dropped when keys change.

In the Viptela overlay network, the liveness of SAs between vEdge router peers is tracked by monitoring BFD packets, which are periodically exchanged over the IPsec connection between the peers. IPsec relays the connection status to the vSmart controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the vSmart controller learns that the connection has been lost.

The Viptela IPsec software has no explicit SA idle timeout, which specifies the time to wait before deleting SAs associated with inactive peers. Instead, an SA remains active as long as the IPsec connection between two vEdge routers is up, as determined by the periodic exchange of BFD packets between them. Also, the frequency with which SA keys are regenerated obviates the need to implement an implicit SA idle timeout.

In summary, the Viptela data plane authentication offers the following improvements over IKE:

- Because only $n + 1$ keypaths are required rather than the n^2 required by IKE, the Viptela solution scales better as the network grows large.
- Keys are generated and refreshed locally, and key exchange is performed over a secure control plane.
- No key server is required, and thus there is no need to worry about high availability requirements of a key server.

Data Plane Integrity

A number of components contribute to the integrity of data packets in the Viptela data plane:



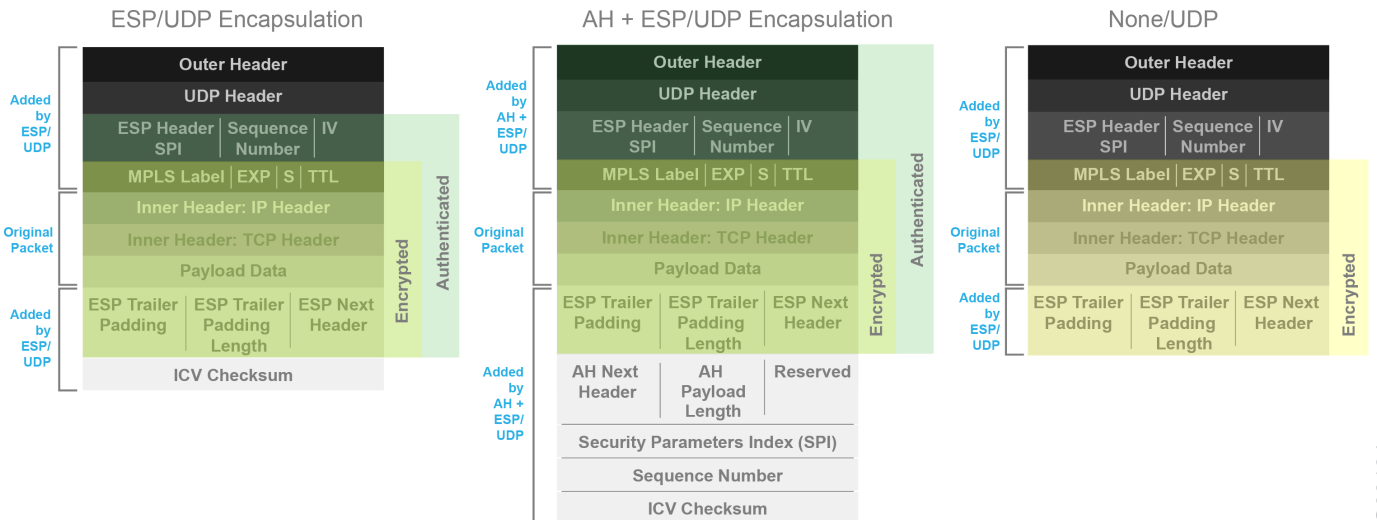
- ESP, which is the standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets.
- AH, which is the standard IPsec authentication protocol, protects (via authentication) the entire data packet, including the inner and outer headers, data packet payload, and ESP trailer.
- Anti-replay, which is also part of the standard IPsec software suite, provides a mechanism to number all data packets and to ensure that receiving routers accept only packets with unique numbers.

The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet's payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet's payload and inner header fields and places the resultant hash (also called a digest) into a 12-byte HMAC-SHA1 field at the end of the packet. (A hash is a one-way compression.) The receiving device performs the same checksum and compares its calculated hash with that in the packet. If the two checksums match, the packet is accepted. Otherwise, it is dropped. In the figure below, the left stack illustrates the ESP/UDP encapsulation. ESP encrypts and authenticates the inner headers, payload, MPLS label (if present), and ESP trailer fields, placing the HMAC-SHA1 hash in the ICV checksum field at the end of the packet. The outer header fields added by ESP/UDP are neither encrypted nor authenticated.

A second component that contributes to data packet integrity is AH, the standard IPsec authentication protocol, which protects all fields in a data packet via authentication. AH performs a checksum process similar to that done by ESP, except that instead of calculating the checksum over just the payload and inner IP header fields, it calculates it over all the fields in the packet—the payload, the inner header, and all the non-mutable fields in the outer IP header. AH places the resultant HMAC-SHA1 hash into the last field of the packet. As with ESP, AH on the receiving device performs the same checksum, and accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by AH, in combination with ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now AH authenticates the entire packet—the outer IP and UDP headers, the ESP header, the MPLS label (if present), the original packet, and the ESP trailer—and places its calculated HMAC-SHA1 hash into the ICV checksum field at the end of the packet.

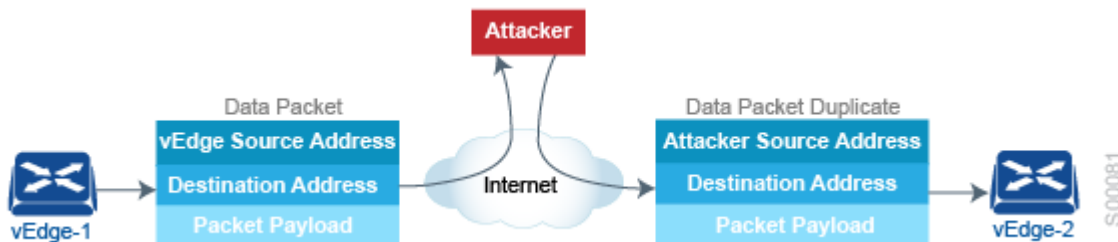
For situations in which data packet authentication is not required, you can disable data packet authentication altogether. In this case, data packets are processed just by ESP, which encrypts the original packet, the MPLS label (if present), and the ESP trailer. This scheme is illustrated in the right stack in the figure below.





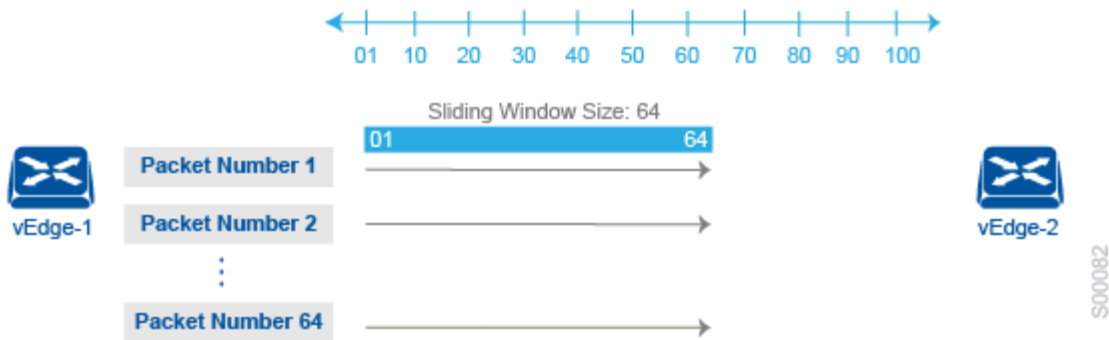
S00194

Note that Viptela devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the HMAC-SHA1 digest. Both are distributed as part of the TLOC properties for a vEdge router. Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this type of attack, an adversary tampers with the data traffic by inserting a copy of a message that was previously sent by the source. If the destination cannot distinguish the replayed message from a valid message, it may authenticate the adversary as the source or may incorrectly grant to the adversary unauthorized access to resources or services.

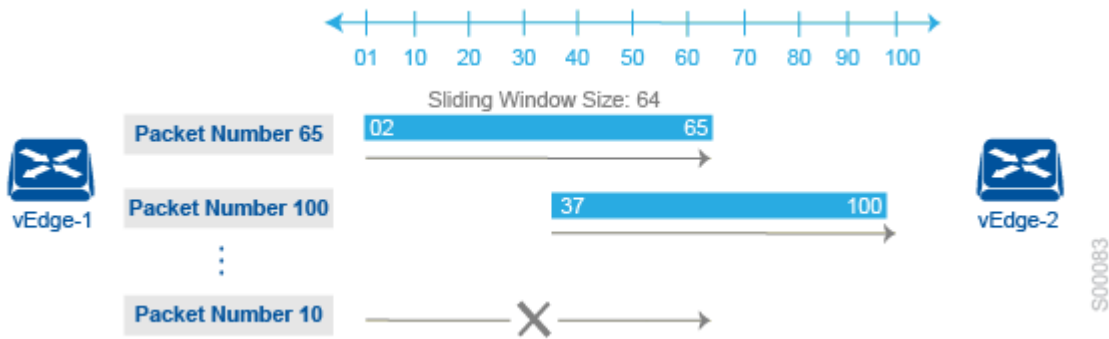


As a counter to such attacks, the Viptela overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, and it drops all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.



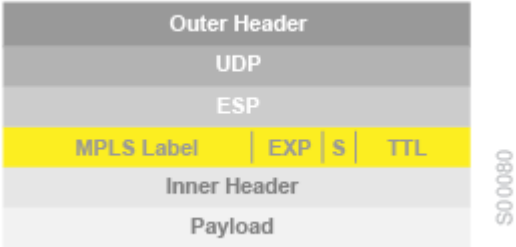


When the destination receives a packet whose sequence number is larger than the highest number in the sliding window, it slides the window to the right, thus changing the range of valid sequences numbers it will accept. This scheme protects against an MITM type of attack because, by choosing the proper window size, you can ensure that if a duplicate packet is inserted into the traffic stream, its sequence number will either be within the current range but will be a duplicate, or it will be smaller than the lowest current value of the sliding window. Either way, the destination will drop the duplicate packet. So, the sequence numbering combined with a sliding window provide protection against MITM type of attacks and ensure the integrity of the data stream flowing within the IPsec connection.



Carrying VPN Information in Data Packets

For enterprise-wide VPNs, Viptela devices support MPLS extensions to data packets that are transported within IPsec connections. The figure to the right shows the location of the MPLS information in the data packet header. These extensions provide the security for the network segmentation (that is, for the VPNs) that is needed to support multi-tenancy in a branch or segmentation in a campus. The Viptela implementation uses IPsec UDP-based overlay network layer protocol encapsulation as defined in [RFC 4023](#). The security is provided by including the Initialization Vector (IV) at the beginning of the payload data in the ESP header. The IV value is calculated by the AES-256 cipher block chaining



(CBC).

Additional Information

[Configuring Security Parameters](#)

[Control Plane Security Overview](#)

[Security Overview](#)



https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/SD-WAN_Release_16.3/05Security/01Security_Ov...

Created on: Wed, 19 May 2021 05:59:50 GMT

Generated by: Anonymous