IPsec Site-to-Site VPN Configuration Guide, 17.2.0

November 2017

Supporting AT&T Vyatta Network Operating System

Contents

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Copyright Statement

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners.

The training materials and other content provided herein for assistance in training on the Vyatta vRouter may have references to Brocade as the Vyatta vRouter was formerly a Brocade product prior to AT&T's acquisition of Vyatta. Brocade remains a separate company and is not affiliated to AT&T.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

About This Guide

This guide describes how to configure site-to-site IPsec VPNs on AT&T products that run on the AT&T Vyatta Network Operating System (referred to as a virtual router, vRouter, or router in the guide).

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

IPsec VPN Overview

Benefits of IPsec VPNs

An IPsec Virtual Private Network (VPN) is a virtual network that operates across the public network, but remains "private" by establishing encrypted tunnels between two or more end points. VPNs provide:

- Data integrity: Data integrity ensures that no one has tampered with or modified data while it traverses the network. Data integrity is maintained with hash algorithms.
- Authentication: Authentication guarantees that data you receive is authentic; that is, that it originates from where it is supposed to, and not from someone masquerading as the source. Authentication is also ensured with hash algorithms.
- Confidentiality: Confidentiality ensures data is protected from being examined or copied while transiting the network. Confidentiality is accomplished using encryption.

An IP Security (IPsec) VPN secures communications and access to network resources for site-to-site access using encryption, authentication, and key management protocols. On a properly configured VPN, communications are secure, and the information that is passed is protected from attackers.

The AT&T Vyatta vRouter currently supports site-to-site IPsec VPN connectivity on both IPv4 and IPv6 networks (IPv4 traffic over IPv4 IPsec tunnels, and IPv6 traffic over IPv6 IPsec tunnels). Site-to-site VPN connections are normally established between two (or more) VPN gateways and provide connectivity for user hosts, servers, and other devices at each location. Connectivity is normally based on IP source and destination network pairs, allowing multiple hosts to share the same tunnel between locations.

Site-to-site VPNs enable enterprises to create low-cost connectivity between offices. These site-to-site VPNs frequently replace more expensive WAN technologies such as private lines or Frame Relay.

IPsec architecture

IPsec is a suite of protocols designed to provide end-to-end security at the network layer (Layer 3), using encryption and authentication techniques. From the point of view of IP networking equipment, encrypted packets can be routed just like any other ordinary IP packets. The only devices that require an IPsec implementation are the IPsec endpoints.

There are three main components of the IPsec architecture. These are:

- The Authentication Header (AH) protocol
- The Encapsulating Security Payload (ESP) protocol
- The Internet Key Exchange (IKE) protocol, formerly referred to as ISAKMP/Oakley

Of these, the AT&T Vyatta vRouter currently supports ESP, which encrypts the packet payload and prevents it from being monitored, and IKE (IKEv1 and IKEv2), which provides a secure method of exchanging cryptographic keys and negotiating authentication and encryption methods.

The set of IPsec parameters describing a connection is called a security policy. The security policy describes how both endpoints will use security services, such as encryption, hash algorithms, and Diffie-Hellman groups, to communicate securely.

The IPsec peers negotiate a set of security parameters, which must match on both sides. Then they create a security association (SA). An IPsec SA describes the connection in one direction. For packets to travel in both directions in a connection, both an inbound and an outbound SA are required.

IPsec forwarding architecture

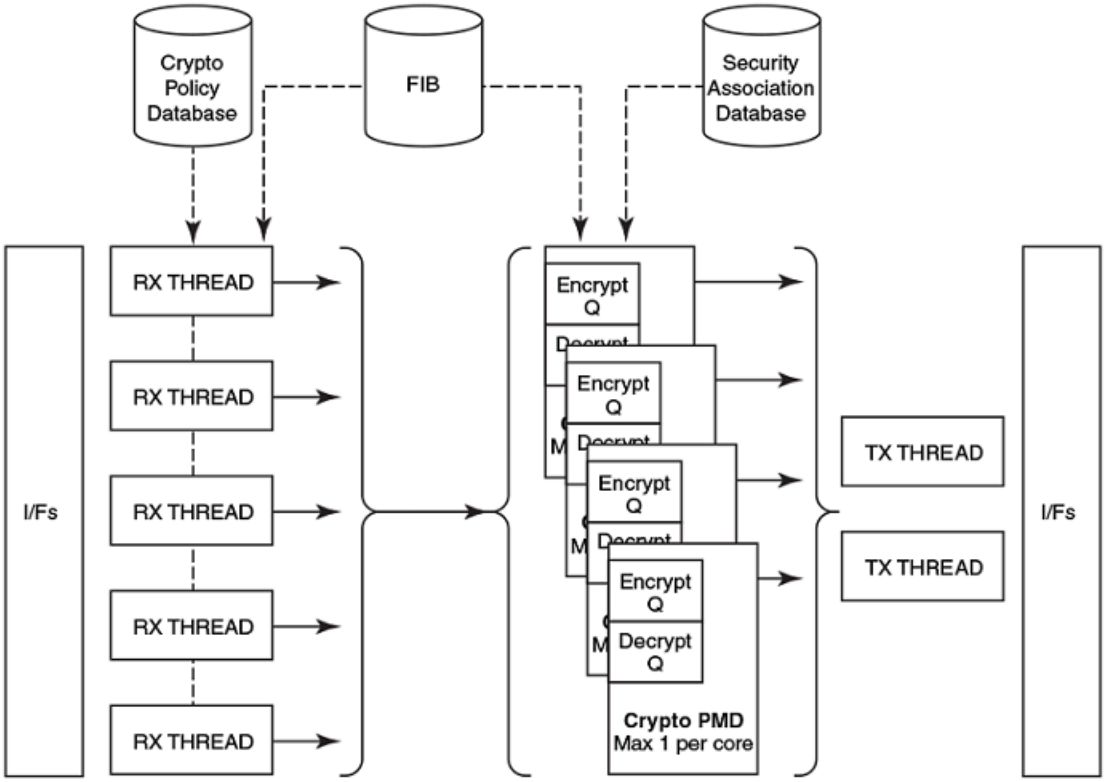
Enables multiple processor cores to be purposed and operated as crypto engines simultaneously.

This feature parallelizes the existing support for IPsec in the AT&T Vyatta vRouter data plane, enabling multiple processor cores to be purposed and operated as crypto engines simultaneously. A crypto engine represents a

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

processing element within the AT&T Vyatta vRouter data plane, providing encryption and decryption support for one or more IPsec Security Associations.

Figure 1: Multiple crypto engines overview



Each data plane core can support one crypto engine. All data plane cores that are not associated with interfaces are suitable for crypto engine allocation. If no eligible cores are available, all cores are considered available for crypto engine allocation. A crypto engine is created and associated with a core on demand that is driven by the creation of each Security Association which is then bound to the crypto engine. After crypto engines have been allocated to all eligible cores, Security Associations are bound to the existing crypto engines by using an allocation mechanism that considers the number of Security Associations already allocated to a particular crypto engine and whether the new Security Association is replacing an existing one. A Security Association can be associated with no more than one crypto engine; therefore, the maximum performance of a Security Association is limited by the core to which the individual crypto engine is bound.

Following cryptographic processing, the transformed packet is passed to IP forwarding on the crypto engine. In a tunnel-stitching scenario, this passage could result in the packet being forwarded to and processed on another crypto engine.

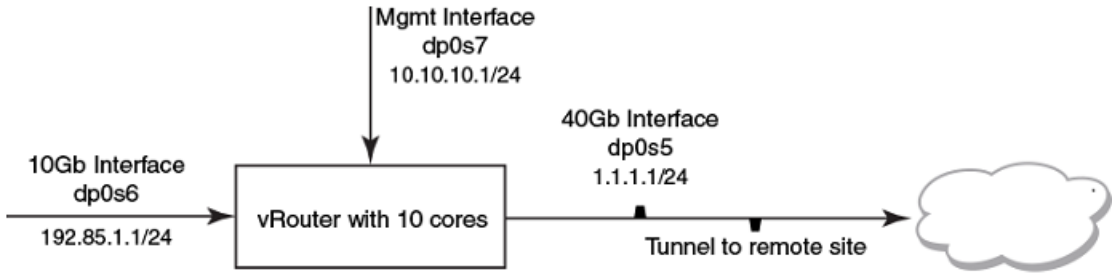
Controlling IPsec crypto cores to obtain better performance

The following examples to illustrate how Crypto engines are mapped to dataplane cores, and how that can be controlled by the user from CLI, in order to get the desired aggregate throughput.

Note: The CLI for exposing dataplane core usage is: "monitor dataplane".

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Figure 2: Controlling IPsec crypto cores



Example: Example 1

In this example, we have an AT&T Vyatta vRouter with 10 cores with IPsec site-to-site tunnels to a single remote network. With the default dataplane core assignment, this results in a single free core, which can be used as a crypto engine, which results in sub-optimal IPsec forwarding performance, as all crypto SAs are assigned to a single core.

```
set interfaces dataplane dp0s5 address '1.1.1.1/24'
set interfaces dataplane dp0s6 address '192.85.1.1/24'
set interfaces dataplane dp0s7 address 10.10.10.1/24'
set security vpn ipsec esp-group ESP lifetime '86400'
set security vpn ipsec esp-group ESP pfs disable'
set security vpn ipsec esp-group ESP proposal 1 encryption 'aes128gcm128'
set security vpn ipsec esp-group ESP proposal 1 hash 'null'
set security vpn ipsec ike-group IKE ike-version '2'
set security vpn ipsec ike-group IKE lifetime '86400'
set security vpn ipsec ike-group IKE proposal 1 dh-group '2'
set security vpn ipsec ike-group IKE proposal 1 encryption 'aes256'
set security vpn ipsec ike-group IKE proposal 1 hash 'sha2_512'

set security vpn ipsec site-to-site peer 1.1.1.5 authentication mode 'pre-shared-secret'
set security vpn ipsec site-to-site peer 1.1.1.5 authentication pre-shared-secret 'test'
set security vpn ipsec site-to-site peer 1.1.1.5 default-esp-group 'ESP'
set security vpn ipsec site-to-site peer 1.1.1.5 ike-group 'IKE'
set security vpn ipsec site-to-site peer 1.1.1.5 local-address '1.1.1.1'
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 1 local prefix '192.85.1.0/24'
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 1 protocol 'all'
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 1 remote prefix '196.85.1.0/24'
```

The following `monitor dataplane` and `show dataplane` command output shows that there is a single core for all crypto traffic and the AT&T Vyatta vRouter total crypto throughput is limited to 1.3 Mpps.

```
Dataplane CPU activity

Core Interface    RX Rate   TX Rate  Idle
-----------------------------------------------------
1    dp0s7              0             250 µs
2    dp0s7              0             250 µs
3    dp0s6           1.5M             1 µs
4    dp0s6           1.5M             3 µs
5    dp0s5              0             250 µs
6    dp0s5              0             250 µs
7    dp0s5              0             250 µs
8    dp0s5           1.5M             10 µs
9    [crypt]                   1.3M   0 µs
```

```
                  RX                  TX                Slow Path
Interface         Packets Rate        Packets Rate      In      Out
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
------------------------------------------------------------------------------
[crypt]                                333087232 1.3M
dp0s5            397954426 1.5M                               3       11
dp0s6            780658237 2.9M                              51        6
dp0s7                    0 0                                  0        7
```

As dp0s7 is just for low volumes of traffic, this can be limited to a single core, and dp0s5 can be reduced to just 2 cores as the 40Gb link it underutilized, and dp0s6 remains with 2 cores via the configuration.

```
set interfaces dataplane dp0s7 cpu-affinity 1
set interfaces dataplane dp0s5 cpu-affinity 2-3
set interfaces dataplane dp0s6 cpu-affinity 4-5
```

Following a reboot, we now see that the cpu assignment matched our configuration, and we now have 2 crypt processes and the AT&T Vyatta vRouter total crypto throughput is increased 2.8 Mpps.

```
Dataplane CPU activity

Core Interface    RX Rate   TX Rate  Idle
------------------------------------------------------------

1    dp0s7               0              250 µs
     dp0s7               0              250 µs
2    dp0s5               0              250 µs
     dp0s5               0              250 µs
3    dp0s5               0              250 µs
     dp0s5           1.5M               10 µs
4    dp0s6           1.5M               1 µs
5    dp0s6           1.5M               0 µs
8    [crypt]                    1.3M   0 µs
9    [crypt]                    1.5M   0 µs
```

```
vyatta@dut-1:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.5                                 1.1.1.1

Tunnel Id         State Bytes Out/In  Encrypt      Hash     DH A-Time L-Time
------ ---------- ----- ------------- ------------ -------- -- ------ ------
1      1          up    10.0G/9.7G    aes128gcm128 null     2 11     86400
```

```
vyatta@dut-1:~$ show dataplane

                   RX                    TX                  Slow Path
Interface          Packets Rate          Packets Rate        In      Out
------------------------------------------------------------------------------
[crypt]                                1796307664 2.8M
dp0s5           3304762213 1.5M                              36       40
dp0s6           3845688861 2.9M                              30        7
dp0s7                    0 0                                  0        6
```

Further performance improvements can be made by splitting the traffic across multiple tunnels whose crypt processes can run on the other 2 free cores. In this example, the customer's traffic profile is split between TCP and other protocols, better performance can be obtained by creating a second tunnel, (which will create a second pair of SAs, and therefore a second pair of crypt processes)

```
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 2 local prefix '192.85.1.0/24'
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 2 remote prefix '196.85.1.0/24'
set security vpn ipsec site-to-site peer 1.1.1.5 tunnel 2 protocol tcp
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Now we see that there are 4 crypto processes and the AT&T Vyatta vRouter total crypto through-put is increased to 5.4 Mpps.

```
Dataplane CPU activity

Core Interface    RX Rate   TX Rate  Idle
-------------------------------------------------------
1    dp0s7               0              250 µs
     dp0s7               0              250 µs
2    dp0s5               0              250 µs
     dp0s5               0              250 µs
3    dp0s5               0              250 µs
     dp0s5            2.6M              10 µs
4    dp0s6            1.5M              0 µs
5    dp0s6            1.5M              1 µs
6    [crypt]                     1.3M   0 µs
7    [crypt]                     1.3M   0 µs
8    [crypt]                     1.4M   0 µs
9    [crypt]                     1.3M   0 µs
```

```
vyatta@dut-1:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.5                                 1.1.1.1

Tunnel Id         State Bytes Out/In  Encrypt      Hash     DH A-Time L-Time
------ ---------- ----- ------------- ------------ -------- -- ------ ------
1      5          up    40.9G/34.0G   aes128gcm128 null     2 106    86400
2      6          up    21.4G/17.0G   aes128gcm128 null     2 105    86400
```

```
vyatta@dut-1:~$ show dataplane
                   RX                    TX                  Slow Path
Interface          Packets Rate          Packets Rate        In      Out
-------------------------------------------------------------------------------
[crypt]                                  5549204792 5.4M
dp0s5           2770036752 2.6M                                31       36
dp0s6           3219935397 2.9M                                30        7
dp0s7                    0 0                                    0        6
```

If there were initially no free cores, rather than a single one, on an AT&T Vyatta vRouter with 9 cores, the crypt processes would share the cores with the dataplane forwarding threads, as shown below.

```
Dataplane CPU activity

Core Interface    RX Rate   TX Rate  Idle
-------------------------------------------------------
1    dp0s7               0              250 µs
     [crypt]                     1.3M   0 µs
2    dp0s7               0              250 µs
     [crypt]                     1.5M   0 µs
3    dp0s5               0              250 µs
4    dp0s5               0              250 µs
5    dp0s5               0              250 µs
6    dp0s5            1.5M              7 µs
7    dp0s6            1.5M              0 µs
8    dp0s6            1.5M              1 µs
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Example: Example 2

In the following example, the CPU cycles for the crypt process have to be shared with that on the dataplane forwarding, however, as in this case the dp0s7 interface is receiving no traffic, the performance matches that of a dedicated core as shown in the previous example, and the AT&T Vyatta vRouter total crypto throughput is 2.8 Mpps.

```
vyatta@dut-1:~$ show dataplane
                  RX                   TX                 Slow Path
Interface         Packets Rate         Packets Rate       In      Out

-------------------------------------------------------------------------------

[crypt]                                500745504 2.8M
dp0s5           271005437 1.5M                              3       10
dp0s6           537440476 2.9M                             53        7
dp0s7                   0 0                                 0        7
```

Performance can be improved by creating a second tunnel for the TCP traffic resulting in total crypto throughput of 4.3 Mpps. Here the performance does not match that of the dedicated cores, as core 6 is now doing both packet forwarding and crypt processing.

```
Dataplane CPU activity
Core Interface    RX Rate   TX Rate  Idle
-----------------------------------------------------
1    dp0s7               0              250 µs
2    dp0s7               0              250 µs
3    dp0s5               0              250 µs
     [crypt]                    1.3M   0 µs
4    dp0s5               0              250 µs
     [crypt]                    1.4M   0 µs
5    dp0s5               0              250 µs
     [crypt]                  796.8K   2 µs
6    dp0s5           2.3M               0 µs
     [crypt]                  796.8K   0 µs
7    dp0s6           1.5M               2 µs
8    dp0s6           1.5M               1 µs
```

```
vyatta@dut-1:~$ show dataplane
                  RX                   TX                 Slow Path
Interface         Packets Rate         Packets Rate       In      Out
-------------------------------------------------------------------------------
[crypt]                               410930913 4.3M
dp0s5            665245216 2.3M                            10       15
dp0s6           1166023120 2.9M                            53        7
dp0s7                   0 0                                 0        7
```

IPsec phase 1 and phase 2

The establishment of an IPsec connection takes place in two phases, called IKE phases:

- In IKE Phase 1, the two endpoints authenticate one another and negotiate keying material. This results in an encrypted tunnel used by Phase 2 for negotiating the ESP security associations.
- In IKE Phase 2, the two endpoints use the secure tunnel created in Phase 1 to negotiate ESP SAs. The ESP SAs are what are used to encrypt the actual user data that is passed between the two endpoints.

IKE Phase 1 establishes an ISAKMP SA (typically called an IKE SA). The IKE protocol is used to dynamically negotiate and authenticate keying material and other security parameters required to provide secure

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

communications. IKE itself uses a combination of four protocols (including ISAKMP and Oakley) to dynamically manage keys in the context of IPsec.

If the IKE Phase 1 negotiation is successful, then the ISAKMP SA is established. The ISAKMP SA essentially contains the information from the “winning proposal” of the negotiation, recording the security encryption and keying material that was successfully negotiated. This creates a secure “control channel” where keys and other information for protecting Phase 2 negotiation are maintained. The ISAKMP SA encrypts only Phase 2 ESP security association negotiations, plus any IKE messages between the two endpoints.

An ISAKMP SA is maintained for a pre-determined lifetime. This lifetime is configured, not negotiated or passed between peers. The configured lifetime may be different between peers. When the configured lifetime expires, a new ISAKMP SA is negotiated.

IKE Phase 2 negotiations are also managed by the IKE protocol. Using the encryption provided by the security association, the security policy is used to try and negotiate a Phase 2 SA. The security policy includes information about the communicating hosts and subnets, as well as the ESP information for providing security services for the connection, such as encryption cipher and hash algorithm. If the IKE Phase 2 negotiation process is successful, a pair of ESP SAs (typically called IPsec SAs) is established—one inbound and one outbound—between the two endpoints. This is the encrypted VPN “tunnel” between the two endpoints. At this point, the user data can be exchanged through the encrypted tunnel.

Between any two IPsec VPN peers, there can be just one control channel for exchanging Phase 2 keying material. This means that between any two peers there will be just one ISAKMP SA on each peer.

However, between two VPN peers, any number of security policies can be defined. For example, you can define a security policy that creates a tunnel between two hosts, and a different security policy that creates a tunnel between a host and a subnet, or between two subnets. Since multiple tunnels can exist between two peers, this means that multiple IPsec SAs can be active at any time between two peers.

IKE key exchange

To be able to create an ISAKMP SA, the two devices must agree on all of the following:

- The encryption algorithm
- The strength of the encryption key (Diffie-Hellman group)
- The authentication method
- The hash algorithm
- The authentication material (pre-shared secret)

All of this information is contained in an IKE Phase 1 proposal. A VPN gateway can be configured multiple Phase 1 proposals. Note that the SA lifetime is not negotiated.

During an IKE key exchange, one device (the initiator) sends the first packet in the exchange. This first packet consists of all the Phase 1 proposals configured for this VPN peer, in a sequence. This set of proposals informs the other gateway of what security and authentication policies it supports. The second device (the responder) inspects the set of proposals and returns the policy representing strongest security policy that both devices can agree on. If this process is successful, both devices agree on the parameter and the ISAKMP SA is established.

Once the ISAKMP SA has been established, the two devices can use this SA to encrypt the Phase 2 traffic where the two endpoints try to negotiate an IPsec SA for each matching security policy that has been configured between the two endpoints. Only after the IPsec SAs have been established can IPsec traffic be passed.

Different devices initiate IKE negotiation differently. Many VPN devices bring up VPN tunnels only on demand. These devices monitor traffic to see if it is “interesting”—that is, to see if it matches a configured security policy. Once the device receives traffic matching a specific security policy, the device will attempt to negotiate an IPsec SA that will be used to encrypt that traffic.

Other devices, including the AT&T Vyatta vRouter, will attempt to initiate Phase 2 negotiations as soon as a correct policy configuration is entered. If both endpoints behave in this way, a race condition can occur, where duplicate IPsec SAs are created.

Encryption ciphers

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Ciphers are used to encrypt data, so that it cannot be read or monitored during transit. The AT&T Vyatta vRouter supports the following encryption ciphers.

Table 1: Supported encryption ciphers

Cipher	Description
AES	The Advanced Encryption Standard (AES) is a U.S. government standard that was developed to take the place of DES, which has become easier to break by using the more powerful computers available today. AES can run very quickly for a block cipher and can be implemented in a relatively small space. It has a block length that varies between 192 and 256 bits, and a key length that ranges between 128 and 256 bits in increments of 32 bits. The AT&T Vyatta vRouter supports AES with a 128-bit key and a 256-bit key. The AT&T Vyatta vRouter also supports the AES options with 128-bit or 256-bit Galois/Counter Mode (GCM), which provides improved efficiency and performance.
3DES	Triple-DES is a variant of the Data Encryption Standard (DES). DES was formerly the most commonly used cipher, but in recent years has been compromised and is no longer recommended as a first choice. The AT&T Vyatta vRouter supports only Triple-DES. Triple-DES is an iterative block cipher in which DES is used in three consecutive iterations on the same block of text and either two or three keys are used. The resulting cipher text is much harder to break than DES. Using two keys yields 112-bits key strength; using three keys yields 168-bits key strength.

Hash algorithms

A hash function is a cryptographic algorithm that is used for message authentication. A hash function takes a message of arbitrary length and produces an output of fixed length, called a message digest or fingerprint. Hash functions are used to verify that messages have not been tampered with.

The AT&T Vyatta vRouter supports the following hash functions.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 2: Supported hash functions

Cipher	Description
MD5	MD5 is the most recent version of message digest algorithm. MD5 takes a message of arbitrary length and produces a 128-bit condensed digital representation, called a message digest. It is often used when a large file must be compressed and encrypted, then signed with a digital signature. Message digest is quite fast and efficient compared with SHA-1 because it uses primitive operations and produces a shorter message. However, it is not as secure as SHA, and has reportedly been compromised in some ways, though not yet in ways that make it insecure.
SHA-1	SHA stands for Secure Hash Algorithm, also known as the Secure Hash Standard. The SHA hash functions are five one-way cryptographic algorithms for computing a message digest. SHA-1 is an extension of the original SHA, and is the standard hash algorithm supported by the U.S. government. SHA-1 takes a message of arbitrary length (the message must be smaller than 2^64 bits) and produces a 160-bit message digest. SHA-1 is slower than MD5, but it is more secure because the additional bits in the message digest provide more protection from brute-force attacks.
SHA-2	SHA-2 is a stronger algorithm than SHA-1 with a longer hash value. The AT&T Vyatta vRouter supports 256-bit, 384-bit, and 512-bit SHA-2 algorithms, which are used to calculate a 128-bit hash message authentication code (HMAC) to verify the message.

Pre-shared keys

A preshared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a character string agreed upon beforehand by both parties as the key for authenticating the session. It generates a hash such that each VPN endpoint can authenticate the other.

Note that the pre-shared secret, although an ordinary character string, is not a “password.” It actually generates a hashed key to form a fingerprint that proves the identity of each endpoint. This means that long, complex character strings are more secure than short strings. Choose complex pre-shared secrets and avoid short ones, which can be more easily compromised by an attack.

The preshared secret is not passed during IKE negotiation. It is configured on both sides, and must match on both sides.

A preshared secret is an example of symmetric cryptography: the key is the same on both sides. Symmetric encryption algorithms are less computationally intensive than asymmetric algorithms, and are, therefore, faster. However, in symmetric cryptography, the two communicating parties must exchange keys in advance. Doing this securely can be a problem.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

A preshared secret and a digital signature are the most common methods of IKE authentication. A preshared secret is an easy and effective way to quickly set up authentication with little administrative overhead. However, it has several drawbacks.

- If a preshared key is captured and no one is aware of it, the attacker has access to your network as long as that key is in use.
- A preshared secret is manually configured, so it should be regularly changed. However, this task often falls off the list of busy network administrators. Using preshared key values with remote users is equivalent to giving them a password to your network.

Note: You should restrict the use of pre-shared keys to smaller, low-risk environments.

Digital signatures

Along with pre-shared key, RSA digital signatures are the most common means of IKE authentication.

An RSA digital signature is based on a cryptographic key that has two parts: a public part and a private part. One part (the public key) is widely shared, and may even be publicly distributed. The other part (the private key) remains secret. These keys are mathematically related but are independent, so that neither key is derivable from the other.

The key is used as input to a hash function; together, the key and the hash function form a signing function that, when applied to a document, creates a digital signature.

An RSA key can be used either to encrypt or authenticate, and this is based on two facts:

- Data encrypted with the agent's public key can only be decrypted by the agent, using the private key. This means that any peer can send information securely by encrypting it with the public key and forwarding it to the agent.
- Data processed with a hash function can be encrypted with the signer's private key—such data is said to be digitally signed. Since anyone with the public key can verify the digital signature, this communication can be accepted as authentically coming from the agent.

Note: RSA1 keys are not supported in AT&T Vyatta Network Operating System.

The algorithms that encrypt using RSA keys are very secure but extremely slow—so slow that it would be impracticable to encrypt an entire set of data using them. Instead, the agent produces a digital signature for the data, as follows:

1. A hash function is applied to the data to generate a message digest. The message digest is much shorter than the original data, and any peer possessing the same hash function can produce the identical message digest.
2. The private key is used to encrypt the message digest. This encrypted message digest is the digital signature.
3. The original message and the digital signature are all sent to the peer in an encrypted packet. (The encryption of the packet is independent of the digital signature.)
4. When the peer receives the packet, it decrypts the packet. Then it uses the sending agent's public key to decrypt the digital signature. This recovers the message digest.
5. The peer applies the hash function to the original message (which was also sent in the packet) and compares the resulting message digest to the message digest recovered from the digital signature.

   Info:

   When the system generates an RSA digital signature, it stores it in a file. The file that contains the digital signature contains both the public key part and the private key part of the digital signature. When you view the RSA key, by looking at VPN configuration or by using the `show vpn ike rsa-keys` command, only the public key is displayed (along with any public keys configured for VPN peers). It is the public key that you should share with the other VPN peer.

   By default, the RSA digital signature file for the local host is stored in the `/config/ipsec.d/rsa-keys/localhost.key` directory. When the key is required to authenticate the VPN peer, the system looks for the key in this directory. You can change the location and name of the file through configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

You can have only one RSA digital signature configured for the local host. If you generate a new key, it overwrites the previous key.

- If the message digests match, the peer can accept the communication as authentic.
- If the message digests do not match, the peer must consider the communication to have been tampered with, or corrupted in some other way, and reject it.

Diffie-Hellman groups

Diffie-Hellman key exchange is a cryptographic protocol for securely exchanging encryption keys over an insecure communications channel, such as the Internet. Diffie-Hellman key exchange was developed in 1976 by Whitfield Diffie and Martin Hellman. It is based on two facts.

- Asymmetric encryption algorithms are much more secure than symmetric algorithms, which require that two parties exchange secret keys in advance.
- However, asymmetric algorithms are much slower and much more computationally expensive than symmetric algorithms.

In a Diffie-Hellman key exchange, asymmetric cryptography is used at the outset of the communication (IKE Phase 1) to establish a shared key. After the key has been exchanged, it can then be used symmetrically to encrypt subsequent communications (IKE Phase 2).

Diffie-Hellman key exchange uses a group of standardized global unique prime numbers and generators to provide secure asymmetric key exchange. The original specification of IKE defined four of these groups, called Diffie-Hellman groups or Oakley groups. Since then, additional groups have been added.

The AT&T Vyatta vRouter supports the following Diffie-Hellman groups. Groups 19 and 20, introduced with IKEv2, are based on elliptic curve cryptography and provide higher security than the other modular exponentiation (MODP) groups.

Table 3: Supported Diffie-Hellman groups

Diffie-Hellman Group	Description
2	MODP with a 1024-bit modulus.
5	MODP with a 1536-bit modulus.
14	MODP with a 2048-bit modulus.
15	MODP with a 3027-bit modulus.
16	MODP with a 4096-bit modulus.
17	MODP with a 6144-bit modulus.
18	MODP with a 8192-bit modulus.
19	256-bit elliptic curve group.
20	384-bit elliptic curve group.

IPsec modes

IPsec, in general, supports two modes of operation: *aggressive mode* and *main mode*.

Aggressive mode

Aggressive mode was created to reduce latency during Phase 1 negotiation but it is vulnerable to attack. For this reason, the AT&T Vyatta vRouter does not support aggressive mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Main mode

Under ordinary conditions, establishing the ISAKMP SA requires several packets to be sent and received:

- The first two messages determine communications policy.
- The next two messages exchange Diffie-Hellman public data.
- The last two messages authenticate the Diffie-Hellman exchange.

This is the normal method of establishing a successful Phase 1 connection, and it is called *main mode*. This method provides the most security and privacy, because authentication information is not exchanged until a full Diffie-Hellman exchange has been negotiated and encryption has been enabled. The AT&T Vyatta vRouter supports main mode.

Perfect forward secrecy

In Perfect Forward Secrecy (PFS), the private key is used to generate a temporary key (the session key) that is used for a short time and then discarded. Subsequent keys are independent of any previously created keys. This way, if a key is compromised, it does not affect any further keys, or compromise the security of data protected by other keys.

PFS provides a way to optimize both efficiently and security. Reasonably-sized keys are much more computationally efficient than large keys, but are also less secure. In PFS, you can use reasonably-sized keys and refresh them frequently.

Committing VPN configuration changes

An IPsec VPN connection includes multiple components, some of which are interdependent. For example, a VPN connection configuration requires a valid IKE group configuration, a valid ESP group configuration, and a valid tunnel configuration. In addition, the interface specified in the connection must be enabled for IPsec VPN. When you commit a VPN configuration, the AT&T Vyatta vRouter performs a full verification on the configuration. If any required component is missing or incorrectly specified, the commit will fail.

For an IPsec VPN site-to-site connection configuration to successfully commit, all the following must be correctly configured:

- The interface and IP address must already be configured.
- The interface must be enabled for IPsec VPN.
- The peer must be configured.
- The IKE group specified in the peer configuration must be defined.
- The tunnel must be configured.
- The ESP group specified in the tunnel must be defined.
- The local IP address specified for the peer must be configured on the VPN-enabled interface.
- The `peer-address` type, `local-address` type, `tunnel local prefix` network type, and `tunnel remote prefix` network type, must all match. They must all be IPv4 or all be IPv6.

In addition, note that modifying global parameters (such as `auto-update` or `nat-traversal`) requires an IPsec restart, and therefore restarts all tunnels.

Adding, modifying, or deleting a tunnel restarts only the modified tunnel. Modifying an existing IKE group or ESP group restarts any tunnel using the group. Changing authentication information (pre-shared key or RSA signature) does not result in a tunnel restart.

Supported standards for IPsec VPN

The AT&T Vyatta vRouter implementation of IPsec complies with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC 2412, The OAKLEY Key Determination Protocol
- RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4478, Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
- RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7815, Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Virtual Tunnel Interface Overview

This chapter provides a brief overview of virtual tunnel interfaces.

Virtual tunnel interfaces

A virtual tunnel interface provides a termination point for a site-to-site IPsec VPN tunnel and allows it to behave like other routable interfaces. In addition to simplifying the IPsec configuration, it enables many common capabilities to be used because the endpoint is associated with an actual interface.

Traffic being routed to a virtual tunnel interface is encrypted prior to being sent through the tunnel. Traffic arriving from a virtual tunnel interface is decrypted prior to its exposure to the routing system.

The virtual tunnel interface on the AT&T Vyatta vRouter is compatible with third party VTI/route-based VPN connections and is sometimes required for connectivity with public cloud offerings.

Benefits of virtual tunnel interfaces

The virtual tunnel interface provides the following benefits over non-VTI IPsec VPN connections:

1. They are capable of having traffic routed to them.
2. They are capable of passing routing protocols over them.
3. They do not require local or remote subnets to be specified.
4. They operate as if the peer interfaces are directly connected.

Restrictions and limitations

The virtual tunnel interface has the following restrictions and limitations:

- Supports IPv4 address, and not IPv6.
- Allows unicast and multicast IP traffic only.
- The AT&T Vyatta vRouter uses *fwmark* in the kernel sk_buff to uniquely identify virtual tunnel interfaces (as well as entities associated with other features). For this purpose, the AT&T Vyatta vRouter uses *fwmark* greater than or equal to 0x7FFF FFFF. If you intend to use *fwmark* directly for another purpose, you should not use values greater than or equal to 0x7FFF FFFF.
- It is not possible to use both of these tunnel types between the same tunnel endpoints, because the virtual tunnel interface and IP-in-IP tunnels use the same IP protocol type.
- The virtual tunnel interface does not support Time to Live (TTL) and Type of Service (ToS).
- The IPsec mode must be configured as tunnel. See security vpn ipsec esp-group <name> mode <mode> *(page 24)*.
- Unlike other site-to-site IPsec VPN tunnels, the local and remote proxies are implicitly 0.0.0.0/0 so the remote and local subnets do not need to be specified explicitly.
- IPsec injects tunnel related routes into the Linux kernel. You can also configure static routes for the same prefixes. For example, on a VTI tunnel, with a remote prefix of 30.1.1.0/24 you can configure a static default route (for 0.0.0.0/0) pointing to any interface of your choice.

  Note: You can configure static routes for backup purposes by using the same address prefixes. To configure a static route, it must point to a backup path of that prefix that is encrypted. If the IPsec tunnel goes down, the static route becomes active.

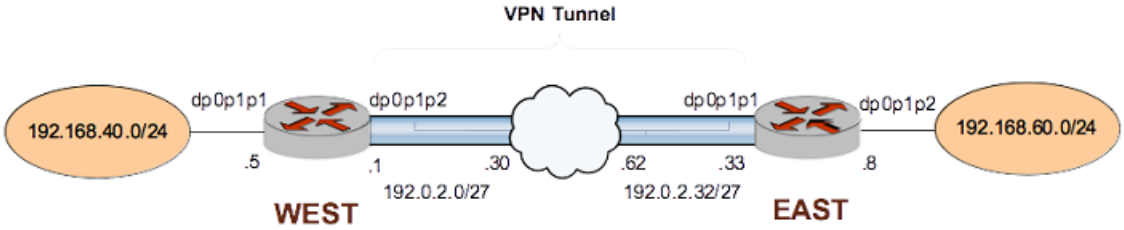
© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

IPsec Site-to-Site VPN Configuration

Basic site-to-site connection

This section presents a sample configuration for a basic IPsec tunnel between WEST and EAST AT&T Vyatta vRouters on an IPv4 network. First WEST is configured, and then EAST. When you have finished, these peers will be configured as shown in the following section.

Figure 3: Basic site-to-site IPsec VPN connection



Before you begin:

- In this set of examples, we assume that you have two AT&T Vyatta vRouters, with host names configured WEST and EAST. (The example systems are configured with the host name in upper case.)
- Any data plane interface used for IPsec VPN must already be configured. In this example, you need dp0p1p2 on WEST and dp0p1p1 on EAST, plus internal subnet information.
- The interface must be configured with the IP address you want to use as the source IP for packets sent to the peer VPN gateway. In this example, IP address 192.0.2.1 is defined on dp0p1p2 of WEST, and 192.0.2.33 is defined on dp0p1p1 of EAST. In examples where the interface is configured as a DHCP client, the interface address is set to `dhcp`.

  Note: The sending and receiving of ICMP redirects is disabled when IPsec VPN is configured.

  Note: In the AT&T Vyatta vRouter, a data plane interface is an abstraction that represents the underlying physical or virtual Ethernet interface of the system.The terms Ethernet interface and data plane interface are synonymous in this guide.

Configure WEST

This section presents the following topics:

Configure an IKE group on WEST

The IKE group allows you to pre-define a set of one or more proposals to be used in IKE Phase 1 negotiation, after which the ISAKMP security association (SA) can be set up. For each proposal in the group, the following information is defined:

- Cipher to encrypt packets during IKE Phase 1
- Hash function to authenticate packets during IKE Phase 1

The IKE group also has a configured lifetime, which is the duration of the ISAKMP SA. When the lifetime of the ISAKMP SA expires, a new Phase 1 negotiation takes place, and new encryption, hash, and keying information is established in a new pair of ISAKMP SAs.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

The lifetime is an attribute of the IKE group as a whole. If the IKE group contains multiple proposals, the lifetime applies regardless of which proposal in the group is accepted.

The following procedure creates IKE group IKE-1W on WEST. This IKE group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm.
- Proposal 2 uses AES-256 with 128-bit GCM as the encryption cipher.

The IKE version is specified as version 2.

The lifetime of a proposal from this IKE group is set to 3600 seconds.

To create this IKE group, perform the following steps on WEST in configuration mode.

Table 4: Configuring an IKE group on WEST

Step	Command
Create the configuration node for proposal 1 of IKE group IKE-1W.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1`
Specify the IKE version (v2).	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W ike-version 2`
Set the encryption cipher for proposal 1.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 encryption aes256`
Set the hash algorithm for proposal 1.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 hash sha1`
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of IKE group IKE-1W.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 2 encryption aes256gcm128`
Set the hash algorithm for proposal 2.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 2 hash null`
Set the lifetime for the whole IKE group.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W lifetime 3600`

View the configuration for the IKE group. Don't commit yet.	`vyatta@WEST# show security vpn ipsec ike-group IKE-1W`
	`ike-version 2`
	`proposal 1 {`
	`encryption aes256`
	`hash sha1`
	`}`
	`proposal 2 {`
	`encryption aes256gcm128`
	`hash null`
	`}`
	`lifetime 3600`

Configure an ESP group on WEST

Encapsulated Security Payload (ESP) is an authentication protocol that provides authentication for IP packets, and it also encrypts them.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

The ESP protocol negotiates a unique number for the session connection, called the Security Parameter Index (SPI). It also starts a numbering sequence for the packets and negotiates the hashing algorithm that authenticates packets.

The AT&T Vyatta vRouter allows you to pre-define multiple ESP configurations. Each configuration is known as an ESP group. An ESP group includes the Phase 2 proposals, which contain the parameters that are needed to negotiate an IPsec security association:

- Cipher to encrypt user data across the IPsec tunnel
- Hashing function to authenticate packets in the IPsec tunnel
- Lifetime of the IPsec security association

The following procedure creates ESP group ESP-1W on AT&T Vyatta vRouter WEST. This ESP group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses Triple-DES as the encryption cipher and MD5 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 1800 seconds.

To create this ESP group, perform the following steps on WEST in configuration mode.

Table 5: Configuring an ESP group on AT&T Vyatta vRouter WEST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1W.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1`
Set the encryption cipher for proposal 1.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 encryption aes256`
Set the hash algorithm for proposal 1.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 hash sha1`
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of ESP group ESP-1W.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 2 encryption 3des`
Set the hash algorithm for proposal 2.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 2 hash md5`
Set the lifetime for the whole ESP group.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W lifetime 1800`

View the configuration for the ESP group. Don't commit yet.	`vyatta@WEST# show security vpn ipsec esp-group ESP-1W`
	
	`proposal 1 {`
	`encryption aes256`
	`hash sha1`
	`}`
	`proposal 2 {`
	`encryption 3des`
	`hash md5`
	`}`
	`lifetime 1800`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Create the connection to EAST

In defining a site-to-site connection, you specify IPsec policy information (most of which is pre-configured as an IKE and ESP group) and the routing information for the two endpoints of the IPsec tunnel.

The local endpoint is the AT&T Vyatta vRouter. The remote endpoint is the peer VPN gateway—this gateway can be another AT&T Vyatta vRouter, or it can be another IPsec-compliant router, an IPsec-capable firewall, or a VPN concentrator. For each end of the tunnel, you define the IP address and subnet mask of the local and remote subnets or hosts.

In all, you must specify the following:

- IP address of the remote peer.
- Authentication mode that the peers use to authenticate one another. The AT&T Vyatta vRouter supports peer authentication by pre-shared secret (pre-shared key, or PSK), so you must also supply the character string to use to generate the hashed key. Digital signatures and X.509 certificates are also supported.
- IKE group to use in the connection.
- ESP group to use in the connection.
- IP address on this AT&T Vyatta vRouter to use for the tunnel. This IP address must be pre-configured on the interface that is enabled for VPN.
- Communicating subnet or host for each end of the tunnel. You can define multiple tunnels for each VPN peer, and each tunnel can use a different security policy.

When supplying a preshared secret, keep the following in mind:

A preshared secret, or pre-shared key (PSK), is a method of authentication. The secret, or key, is a character string agreed upon beforehand by both parties as the key for authenticating the session. It generates a hash such that each VPN endpoint can authenticate the other.

Note that the pre-shared secret, although an ordinary character string, is not a “password.” It actually generates a hashed key to form a fingerprint that proves the identity of each endpoint. This means that long, complex character strings are more secure than short strings. Choose complex pre-shared secrets and avoid short ones, which can be more easily compromised by an attack.

The preshared secret is not passed during IKE negotiation. It is configured on both sides, and must match on both sides.

A preshared secret is an example of symmetric cryptography: the key is the same on both sides. Symmetric encryption algorithms are less computationally intensive than asymmetric algorithms, and are, therefore, faster. However, in symmetric cryptography, the two communicating parties must exchange keys in advance. Doing this securely can be a problem.

A preshared secret and a digital signature are the most common methods of IKE authentication. A preshared secret is an easy and effective way to quickly set up authentication with little administrative overhead. However, it has several drawbacks.

- If a preshared key is captured and no one is aware of it, the attacker has access to your network as long as that key is in use.
- A preshared secret is manually configured, so it should be regularly changed. However, this task often falls off the list of busy network administrators. Using preshared key values with remote users is equivalent to giving them a password to your network.

Note: You should restrict the use of pre-shared keys to smaller, low-risk environments.

The following example defines a site-to-site connection to EAST.

- This connection is configured with a single tunnel:
  - Tunnel 1 communicates between 192.168.40.0/24 on WEST and 192.168.60.0/24 on EAST, using ESP group ESP-1W.
- WEST uses IP address 192.0.2.1 on dp0p1p2.
- EAST uses IP address 192.0.2.33 on dp0p1p1.
- The IKE group is IKE-1W.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- The authentication mode is pre-shared secret. The pre-shared secret is “test_key_1”.

To configure this connection, perform the following steps on AT&T Vyatta vRouter WEST in configuration mode.

Table 6: Creating a site-to-site connection from WEST to EAST

Step	Command
Create the node for EAST and set the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit security vpn ipsec site-to-site peer 192.0.2.33`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Provide the string that will be used to generate encryption keys.	`vyatta@WEST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@WEST# set local-address 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Create a tunnel configuration, and provide the local subnet for this tunnel.
 	
Note: When configuring an IPsec site-to-site tunnel, if the local IP address is not configured for the configured local prefix subnet, IPsec fails to install the kernel route. A workaround is to configure the local IP address on a loopback or a data plane interface.
	`vyatta@WEST# set tunnel 1 local prefix 192.168.40.0/24`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Provide the remote subnet for the tunnel.	`vyatta@WEST# set tunnel 1 remote prefix 192.168.60.0/24`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
Return to the top of the configuration tree.	`vyatta@WEST# top`
Now commit the configuration.	`vyatta@WEST# commit`

View the configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer 192.0.2.33`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.40.0/24`
	`}`
	`remote {`
	`prefix 192.168.60.0/24`
	`}`
	`}`

View data plane interface dp0p1p2 address configuration. `local-address` is set to this address.	`vyatta@WEST# show interfaces dataplane dp0p1p2 address`
	
	`address 192.0.2.1/27`

Configure EAST

This section presents the following examples:

- Configure an IKE group on EAST *(page 30)*
- Configure an ESP group on EAST *(page 31)*
- Create the connection to WEST *(page 32)*

Configure an IKE group on EAST

The following procedure creates IKE group IKE-1E on EAST. This IKE group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm.
- Proposal 2 uses AES-256 with 128-bit GCM as the encryption cipher.

The IKE version is specified as version 2. IKEv2 is required for the AES encryption with 128-bit GCM.

The lifetime of a proposal from this IKE group is set to 3600.

Note that these parameters correspond to those set in IKE-1W on WEST. You must ensure, in defining proposals, that the encryption ciphers and hash algorithms are such that the two peers will be able to agree on at least one combination.

To create this IKE group, perform the following steps on EAST in configuration mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 7: Configuring an IKE group on EAST

Step	Command
Create the configuration node for proposal 1 of IKE group IKE-1E.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E proposal 1`
Specify the IKE version (v2).	`vyatta@WEST# set security vpn ipsec ike-group IKE-1E ike-version 2`
Set the encryption cipher for proposal 1.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E proposal 1 encryption aes256`
Set the hash algorithm for proposal 1.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E proposal 1 hash sha1`
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of IKE group IKE-1E.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E proposal 2 encryption aes256gcm128`
Set the hash algorithm for proposal 2.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E proposal 2 hash null`
Set the lifetime for the whole IKE group.	`vyatta@EAST# set security vpn ipsec ike-group IKE-1E lifetime 3600`

View the configuration for the IKE group. Don't commit yet.	`vyatta@EAST# show security vpn ipsec ike-group IKE-1E`
	`ike-group 2`
	`proposal 1 {`
	`encryption aes256`
	`hash sha1`
	`}`
	`proposal 2 {`
	`encryption aes256cgm128`
	`hash null`
	`}`
	`lifetime 3600`

Configure an ESP group on EAST

The following procedure creates ESP group ESP-1E on EAST. This ESP group contains two proposals:

- Proposal 1 uses AES-256 as the encryption cipher and SHA-1 as the hash algorithm
- Proposal 2 uses Triple-DES as the encryption cipher and MD5 as the hash algorithm

The lifetime of a proposal from this ESP group is set to 1800 seconds.

To create this ESP group, perform the following steps on EAST in configuration mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 8: Configuring an ESP group on EAST

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1E.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E proposal 1`
Set the encryption cipher for proposal 1.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E proposal 1 encryption aes256`
Set the hash algorithm for proposal 1.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E proposal 1 hash sha1`
Set the encryption cipher for proposal 2. This also creates the configuration node for proposal 2 of ESP group ESP-1E.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E proposal 2 encryption 3des`
Set the hash algorithm for proposal 2.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E proposal 2 hash md5`
Set the lifetime for the whole ESP group.	`vyatta@EAST# set security vpn ipsec esp-group ESP-1E lifetime 1800`

View the configuration for the ESP group. Don't commit yet.	`vyatta@EAST# show security vpn ipsec esp-group ESP-1E`
	
	`proposal 1 {`
	`encryption aes256`
	`hash sha1`
	`}`
	`proposal 2 {`
	`encryption 3des`
	`hash md5`
	`}`
	`lifetime 1800`

Create the connection to WEST

The following table defines a site-to-site connection to WEST. In this example:

- This connection is configured with a single tunnel:
  - Tunnel 1 communicates between 192.168.60.0/24 on EAST and 192.168.40.0/24 on WEST, using ESP group ESP-1E.
- EAST uses IP address 192.0.2.33 on dp0p1p1.
- WEST uses IP address 192.0.2.1 on dp0p1p2.
- The IKE group is IKE-1E.
- The authentication mode is pre-shared secret. The pre-shared secret is “test_key_1.”

To configure this connection, perform the following steps on EAST in configuration mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 9: Creating a site-to-site connection from EAST to WEST

Step	Command
Create the node for WEST and set the authentication mode.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@EAST# edit security vpn ipsec site-to-site peer 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Provide the string that will be used to generate encryption keys.	`vyatta@EAST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify the default ESP group for all tunnels.	`vyatta@EAST# set default-esp-group ESP-1E`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify the IKE group.	`vyatta@EAST# set ike-group IKE-1E`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@EAST# set local-address 192.0.2.33`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@EAST# set tunnel 1 local prefix 192.168.60.0/24`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Provide the remote subnet for the tunnel.	`vyatta@EAST# set tunnel 1 remote prefix 192.168.40.0/24`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Return to the top of the configuration tree.	`vyatta@EAST# top`
Now commit the configuration.	`vyatta@EAST# commit`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1E`
	`ike-group IKE-1E`
	`local-address 192.0.2.33`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.60.0/24`
	`}`
	`remote {`
	`prefix 192.168.40.0/24`
	`}`
	`}`

View data plane interface dp0p1p1 address configuration. `local-address` is set to this address.	`vyatta@EAST# show interfaces dataplane dp0p1p1 address`
	
	`address 192.0.2.33/27`

RSA digital signature authentication

This section presents the following topics:

In this set of examples, you modify the VPN connection configured in the previous set of examples between WEST and EAST (Basic site-to-site connection *(page 25)*). The site-to-site connection created in that set of examples used pre-shared keys for authentication. This set of examples modifies the connection to use RSA digital signatures for authentication.

Generate a digital signature on WEST

In this example, you generate WEST's digital signature. This signature will have two parts: a public part (the public key) and a private part (the private key). The public key will be shared with EAST; the private key will remain secret.

To generate an RSA digital signature for system WEST, perform the following steps in operational mode.

Table 10: Generating a digital signature on WEST

Step	Command
Generate the key.	`vyatta@WEST> generate vpn rsa-key`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
The system warns you that the existing RSA key file will be overwritten. You have the opportunity to exit the key generation process by pressing <Ctrl>+c.	`A local RSA key file already exists and will be overwritten` `<CTRL>C to exit: 8`

The system indicates the location of the file where the key will be written, generates the key, and displays the fingerprint.	`Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key`
	
	`Your new local RSA key has been generated.`
	`RSA key fingerprint:`
	`9d:0d:16:3d:93:e1:95:6f:91:a7:18:35:f3:af:f5:ed`

Generate a digital signature on EAST

In this example, you generate EAST's digital signature. This signature will have two parts: a public part (the public key) and a private part (the private key). The public key will be shared with WEST; the private key will remain secret.

To generate an RSA digital signature for system EAST, perform the following steps in operational mode.

Table 11: Generating a digital signature on EAST

Step	Command
Generate the key.	`vyatta@EAST> generate vpn rsa-key`
The system warns you that the existing RSA key file will be overwritten. You have the opportunity to exit the key generation process by pressing <Ctrl>+c.	`A local RSA key file already exists and will be overwritten` `<CTRL>C to exit: 5`
The system indicates the location of the file where the key will be written.	`Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key`

The system indicates the location of the file where the key will be written, generates the key, and displays the fingerprint.	`Your new local RSA key has been generated.`
	`RSA key fingerprint:`
	`74:83:53:c1:2e:11:7b:ba:c5:6e:5a:ee:b1:7a:6d:7b`
	
	`vyatta@EAST>`

Record EAST's public key on WEST

In this example, you record the public key you have obtained from EAST. The key is then saved under a name that you can refer to in site-to-site configuration.

A digital signature can be typed in manually, but digital signatures are lengthy and difficult to type. It is generally easier to copy the digital signature into the clipboard of your system and then paste it into the configuration. You do this in a number of ways; for example:

- Receive the public key from the operator of the VPN peer in an e-mail—perhaps an e-mail protected by a PGP signature. Copy the key text into your clipboard.
- From an X.509 certificate, provided by a Certificate Agency.
- Connect to the VPN peer directly through a Telnet or SSH control session. View the public portion of the key using a `show` command, select the text, and copy the key text into your clipboard.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

The following procedure pastes EAST's public key into RSA configuration. The name “EAST-key” is used as the identifier of the key.

Before you begin, copy EAST's public key into your clipboard. To obtain the public key for EAST, run the `show vpn ike rsa-keys` command on EAST.

If you are in operational mode on WEST, enter configuration mode now and perform the following steps:

Table 12: Record EAST's public key on WEST

Step	Command
Specify a name for EAST's public key and paste EAST's public key into the configuration.	`vyatta@WEST# set security vpn rsa-keys rsa-key-name EAST-key rsa-key 0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1`
Commit the configuration.	`vyatta@WEST# commit`
View the configuration for RSA keys. Since you have not changed the configuration for the local host's key, it does not display.	`vyatta@WEST# show security vpn rsa-keys` `rsa-key-name EAST-key {` `rsa-key 0sAQOVBIJL+rIkpTuwh8FPeceAF0bhgLr++W51bOAIjFbRDbR8gX3Vlz6wiUbMgGwQxWlYQiqsCeacicsfZx/amlEn9PkSE4e7tqK/JQo40L5C7gcNM24mup1d+0WmN3zLb9Qhmq5q3pNJxEwnVbPPQeIdZMJxnb1+lA8DPC3SIxJM/3at1/KrwqCAhX3QNFY/zNmOtFogELCeyl4+d54wQljA+3dwFAQ4bboJ7YIDs+rqORxWd3l3I7IajT/pLrwr5eZ8OA9NtAedbMiCwxyuyUbznxXZ8Z/MAi3xjL1pjYyWjNNiOij82QJfMOrjoXVCfcPn96ZN+Jqk+KknoVeNDwzpoahFOseJREeXzkw3/lkMN9N1` `}`  `vyatta@WEST#`

Modify WEST's connection to EAST

The following procedure modifies the connection from WEST to EAST to use RSA digital signatures for authentication. In this example:

- The authentication mode is changed from pre-shared secret to RSA digital signatures.
- EAST's public key is specified as the remote key, under the identifier configured in the previous step (see Record EAST's public key on WEST *(page 35)*).

To modify the site-to-site connection to use RSA configuration, perform the following steps:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 13: Configure WEST for RSA authentication

Step	Command
Remove the pre-shared key.	`vyatta@WEST# delete security vpn ipsec site-to-site peer 192.0.2.33 authentication pre-shared-secret`
Change the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication mode rsa`
Provide the identifier for EAST's digital signature.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication rsa-key-name EAST-key`
Commit the configuration.	`vyatta@WEST# commit`

View the modified configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer 192.0.2.33`
	
	`authentication {`
	`mode rsa`
	`rsa-key-name EAST-key`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.40.0/24`
	`}`
	`remote {`
	`prefix 192.168.60.0/24`
	`}`
	`}`

View data plane interface dp0p1p2 address configuration. local-address is set to this address.	`vyatta@WEST# show interfaces dataplane dp0p1p2 address address 192.0.2.1/27`

Record WEST's public key on EAST

The following procedure pastes WEST's public key into RSA configuration. The name “WEST-key” is used as the identifier of the key.

Before you begin, copy WEST's public key into your clipboard. To obtain the public key for WEST, run the `show vpn ike rsa-keys` command on WEST.

If you are in operational mode on EAST, enter configuration mode now and perform the following steps:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 14: Record WEST's public key on EAST

Step	Command

Specify a name for WEST's public key and paste WEST's public key into the configuration.	`vyatta@EAST# set security vpn rsa-keys rsa-key-name WEST-key rsa-key 0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQqMZyVMInoQKUU/T0iKSK/0NSH9Ldrr8yQUFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjKGaOkFgLREtVJD3pRzTloTkPepRUtW1bmYev2H7tajSO0K0`
	
	`rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL+EkKfyEl9RagKxRW82XJbgY4LG77K2YDN90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FMpdaUYcbY31o/5PedUutJCK5RMwl+IJGaxrKf1OmCQfzXlkM09ijZx8kzPIlBk`
	
	`5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX00t3ZLfKu+/wX595J`

Commit the configuration.	`vyatta@EAST# commit`

View the configuration for RSA keys.
Since you have not changed the configuration for the local host's key, it does not display.
	`vyatta@EAST# show security vpn rsa-keys`
	
	`rsa-key-name WEST-key {`
	
	`rsa-key 0sAQPEOQvukvkv1ofuO8gEKp7IFFZz4lQqMZyVMInoQKUU/T0iKSK/0NSH9Ldrr8yQUFayzKag6wM7ASXWXKyt0LS1Gn8tJVsjKGaOkFgLREtVJD3pRzTloTkPepRUtW1bmYev2H7tajSO0K0`
	
	`rqu+7nlocZI0ppMAyF6CS+Wd5W1JBpVGL+EkKfyEl9RagKxRW82XJbgY4LG77K2YDN90Wd2GgMY3kf+YJLIzFEt/xRbh2/380FMpdaUYcbY31o/5PedUutJCK5RMwl+IJGaxrKf1OmCQfzXlkM09ijZx8kzPIlBk`
	
	`5hulZrbUWjzBJdFcwFAyPM3yCuv3+ndFX00t3ZLfKu+/wX595J`
	`}`
	
	`vyatta@EAST#`

Modify EAST's connection to WEST

The following procedure modifies the connection from EAST to WEST to use RSA digital signatures for authentication.

In this example:

- The authentication mode is changed from pre-shared secret to RSA digital signatures.
- WEST's public key is specified as the remote key, under the identifier configured in the previous step (see Record WEST's public key on EAST *(page 37)*).

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

To modify the site-to-site connection to use RSA configuration, perform the following steps:

Table 15: Configure EAST for RSA authentication

Step	Command
Remove the pre-shared key.	`vyatta@EAST# delete security vpn ipsec site-to-site peer 192.0.2.1 authentication pre-shared-secret`
Change the authentication mode.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication mode rsa`
Provide the identifier for WEST's digital signature.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication rsa-key-name WEST-key`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication {`
	`mode rsa`
	`rsa-key WEST-key`
	`}`
	`default-esp-group ESP-1E`
	`ike-group IKE-1E`
	`local-address 192.0.2.33`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.60.0/24`
	`}`
	`remote {`
	`prefix 192.168.40.0/24`
	`}`
	`}`

View data plane interface dp0p1p1 address configuration. local-address is set to this address.	`vyatta@EAST# show interfaces dataplane dp0p1p1 address`
	
	`address 192.0.2.33/27`

X.509 certificate authentication

In this set of examples, you modify the VPN connection configured in the basic set of examples between WEST and EAST (Basic site-to-site connection *(page 25)*). The site-to-site connection created in that set of examples used pre-shared keys for authentication. This set of examples modifies the configuration to use X.509 certificates for authentication.

In general, the procedure for obtaining the files required to authenticate using X.509 certificates is as follows:

1. Generate the private key and a certificate signing request (CSR) (based on the public key). This can be accomplished using the `generate vpn x509 key-pair <name>` command (for example, `generate vpn x509 key-pair west`, where `west.key` is the private key and `west.csr` is the certificate signing request file—both created in `/config/auth`).

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

2. Send the CSR file (for example, `west.csr`) to the certificate authority (CA) and receive back a server certificate (for example, `west.crt`), the CA certificate (for example, `ca.crt`), and potentially, a certificate revocation list (CRL) file. This procedure varies according to the CA being used.

   Info:

   At this point, the configuration can be modified to use these files.

Modify WEST's connection to EAST

The following procedure modifies the connection from WEST to EAST to use X.509 certificates for authentication. In this example:

- The authentication mode is changed from pre-shared secret to X.509 certificates.
- The certificate for the peer is identified using its Distinguished Name information. This is the information prompted for when creating the certificate signing request (CSR) file on the peer.
- The locations of the CA certificate, the server certificate, and the private key file for the server are specified.

To modify the site-to-site connection to use X.509 certificate authentication, perform the following steps:

Table 16: Configure WEST for x.509 certificate authentication

Step	Command
Remove the pre-shared key.	`vyatta@WEST# delete security vpn ipsec site-to-site peer 192.0.2.33 authentication pre-shared-secret`
Change the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication mode x509`
Specify the 'distinguished name' of the certificate for the peer.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication remote-id “C=US, ST=CA, O=ABC Company, CN=east, emailAddress=root@abc.com”`
Specify the location of the CA certificate.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication x509 ca-cert-file /config/auth/ca.crt`
Specify the location of the server certificate.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication x509 cert-file /config/auth/west.crt`
Specify the location of the server key file.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication x509 key file /config/auth/west.key`
Specify the password for the server key file.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication x509 key password testpwd-west`
Commit the configuration.	`vyatta@WEST# commit`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the modified configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer 192.0.2.33`
	
	`authentication {`
	`mode x509`
	`remote-id “C=US, ST=CA, O=ABC Company, CN=east, emailAddress=root@abc.com”`
	`x509 {`
	`ca-cert-file /config/auth/ca.crt`
	`cert-file /config/auth/west.crt`
	`key {`
	`file /config/auth/west.key`
	`password testpwd-west`
	`}`
	`}`
	`}`

	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.40.0/24`
	`}`
	`remote {`
	`prefix 192.168.60.0/24`
	`}`
	`}`

View data plane interface dp0p1p2 address configuration. `local-address` is set to this address.	`vyatta@WEST# show interfaces dataplane dp0p1p2 address address 192.0.2.1/27`

Modify EAST's connection to WEST

The following procedure modifies the connection from EAST to WEST to use X.509 certificates for authentication.

In this example:

- The authentication mode is changed from pre-shared secret to X.509 certificates.
- The certificate for the peer is identified using its 'distinguished name' information. This is the information prompted for when creating the certificate signing request (CSR) file.
- The locations of the CA certificate, the server certificate, and the private key file for the server are specified.

To modify the site-to-site connection to use X.509 certificate authentication, perform the following steps:

Table 17: Configure EAST for x.509 certificate authentication

Step	Command
Remove the pre-shared key.	`vyatta@EAST# delete security vpn ipsec site-to-site peer 192.0.2.1 authentication pre-shared-secret`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
Change the authentication mode.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication mode x509`
Specify the 'distinguished name' of the certificate for the peer.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication remote-id “C=US, ST=CA, O=ABC Company, CN=west, emailAddress=root@abc.com”`
Specify the location of the CA certificate.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication x509 ca-cert-file /config/auth/ca.crt`
Specify the location of the server certificate.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication x509 cert-file /config/auth/east.crt`
Specify the location of the server key file.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication x509 key file /config/auth/east.key`
Specify the password for the server key file.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication x509 key password testpwd-east`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication {`
	`mode x509`
	`remote-id “C=US, ST=CA, O=ABC Company, CN=west,`
	
	`emailAddress=root@abc.com”`
	`x509 {`
	`ca-cert-file /config/auth/ca.crt`
	`cert-file /config/auth/east.crt`
	`key {`
	`file /config/auth/east.key`
	`password testpwd-east`
	`}`
	`}`
	`}`

View data plane interface dp0p1p1 address configuration. local-address is set to this address.	`vyatta@EAST# show interfaces dataplane dp0p1p1 address address 192.0.2.33/27`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Suite B configuration

NSA Suite B set of cryptographic algorithms that the National Security Agency is using as part of an effort to modernize its cryptography. Suite B supports interoperability for unclassified information and most classified information.

The AT&T Vyatta vRouter supports the following Suite B configurations from RFC 6379:

- Suite-B-CGM-128
- Suite-B-CGM-256

This section shows how to configure Suite B cryptography for IPsec and includes an interoperability example with Cisco IOS.

Table 18: Configuring Suite-B-GCM-128

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1W.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1`
Set the encryption cipher.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 encryption aes128gcm128`
Set the hash algorithm.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 hash null`
Set the IKE version.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W ike-version 2`
Set the encryption cipher.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 encryption aes128`
Set the hash algorithm.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 hash sha2_256`
Set the Diffie-Hellman group.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 dh-group 19`

View the configuration.	`vyatta@WEST# show security vpn ipsec`
	`esp-group`
	`  ESP-1W {`
	`  proposal 1 {`
	`  encryption aes128gcm128`
	`  hash null`
	`  }`
	`ike-group`
	`  IKE-1W {`
	`  ike-version 2`
	`  proposal 1 {`
	`  encryption aes128`
	`  hash sha2_256`
	`  dh-group 19`
	`  }`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 19: Configuring Suite-B-GCM-256

Step	Command
Create the configuration node for proposal 1 of ESP group ESP-1W.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1`
Set the encryption cipher.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 encryption aes256gcm128`
Set the hash algorithm.	`vyatta@WEST# set security vpn ipsec esp-group ESP-1W proposal 1 hash null`
Set the IKE version.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W ike-version 2`
Set the encryption cipher.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 encryption aes256`
Set the hash algorithm.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 hash null`
Set the Diffie-Hellman group.	`vyatta@WEST# set security vpn ipsec ike-group IKE-1W proposal 1 dh-group 20`

View the configuration.	`vyatta@WEST# show security vpn ipsec`
	`esp-group`
	`  ESP-1W {`
	`  proposal 1 {`
	`  encryption aes256gcm128`
	`  hash null`
	`  }`
	`ike-group`
	`  IKE-1W {`
	`  ike-version 2`
	`  proposal 1 {`
	`  encryption aes256`
	`  hash null`
	`  dh-group 20`
	`  }`

Interoperability with Cisco IOS

The following sample configurations can be adapted as needed for interoperability with Cisco IOS. Note that the example values might not be suitable for all security policies, and that the security policy must be applied to the appropriate interface.

AT&T Vyatta vRouter

```
set security vpn ipsec esp-group ESP-G1 lifetime '3600'
set security vpn ipsec esp-group ESP-G1 proposal 1 encryption 'aes128gcm128'
set security vpn ipsec esp-group ESP-G1 proposal 1 hash 'null'
set security vpn ipsec ike-group IKE-G1 ike-version '2'
set security vpn ipsec ike-group IKE-G1 lifetime '3600'
set security vpn ipsec ike-group IKE-G1 proposal 1 dh-group '19'
set security vpn ipsec ike-group IKE-G1 proposal 1 encryption 'aes128'
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
set security vpn ipsec ike-group IKE-G1 proposal 1 hash 'sha2_256'
set security vpn ipsec site-to-site peer 192.168.3.3 authentication mode 'pre-shared-secret'
set security vpn ipsec site-to-site peer 192.168.3.3 authentication pre-shared-secret 'password'
set security vpn ipsec site-to-site peer 192.168.3.3 default-esp-group 'ESP-G1'
set security vpn ipsec site-to-site peer 192.168.3.3 ike-group 'IKE-G1'
set security vpn ipsec site-to-site peer 192.168.3.3 local-address '192.168.2.1'
set security vpn ipsec site-to-site peer 192.168.3.3 tunnel 1 local prefix '192.168.1.1/24'
set security vpn ipsec site-to-site peer 192.168.3.3 tunnel 1 remote prefix '192.168.4.3/24'
```

Cisco IOS

```
crypto ikev2 proposal 1
 encryption aes-cbc-128
 integrity sha256
 group 19
!
crypto ikev2 policy IKE-G1
 match fvrf any
 proposal 1
!
crypto ikev2 profile IKE-G1
 match identity remote any
 authentication remote pre-share key password
 authentication local pre-share key password
 lifetime 3600
!
crypto ipsec transform-set ESP-G1 esp-gcm
 mode tunnel
!
crypto ipsec profile 192.168.2.1
 set transform-set ESP-G1
 set pfs group19
 set ikev2-profile IKE-G1
!
crypto map vyatta 101 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set ESP-G1
 set pfs group19
 set ikev2-profile IKE-G1
 match address 101
!
access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
!
interface GigabitEthernet2
 ip address 192.168.3.3 255.255.255.0
 crypto map vyatta
```

VPN connection to a peer with a dynamic IP address

This section presents the following topics:

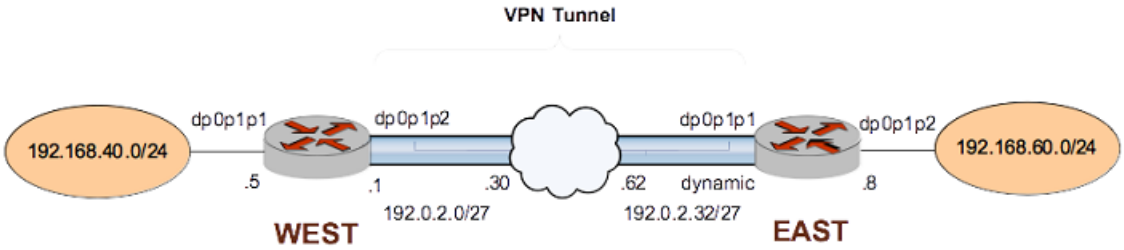
This section presents a sample configuration for a connection between WEST and EAST, where EAST has a dynamic IP address (it is configured as a DHCP client). In this example:

- EAST has a dynamic IP address from WEST's point of view.
- WEST retains its fixed IP address.

When you have finished, these systems will be configured as shown in Figure 1 *(page 46)*.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Figure 4: IPsec VPN connection with dynamic IP address



Before you begin:

- This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section Basic site-to-site connection *(page 25)*. Only the relevant changes to that configuration are presented here.

Configure WEST

The following table defines configuration changes for a new site-to-site connection to EAST. The main change is the IP address specification of the peer. This is set to 0.0.0.0 to represent “any” IP address. Because the IP address of the peer is unknown, WEST will not initiate connections to the peer. It will only receive connections from the peer.

To configure this connection, perform the following steps on WEST in configuration mode.

Table 20: Creating a site-to-site connection to a peer with a dynamic IP address

Step	Command
Delete the previous configuration.	`vyatta@WEST# delete security vpn ipsec site-to-site peer 192.0.2.33`
Create the node for EAST and set the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer 0.0.0.0 authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit security vpn ipsec site-to-site peer 0.0.0.0`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Provide the string that will be used to generate encryption keys.	`vyatta@WEST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@WEST# set local-address 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@WEST# set tunnel 1 local prefix 192.168.40.0/24`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Provide the remote subnet for the tunnel.	`vyatta@WEST# set tunnel 1 remote prefix 192.168.60.0/24`
	
	`[edit security vpn ipsec site-to-site peer 0.0.0.0]`

Return to the top of the configuration tree.	`vyatta@WEST# top`
Commit the configuration.	`vyatta@WEST# commit`

View the configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer 0.0.0.0`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.40.0/24`
	`}`
	`remote {`
	`prefix 192.168.60.0/24`
	`}`
	`}`

View data plane interface dp0p1p2 address configuration. local-address is set to this address.	`vyatta@WEST# show interfaces dataplane dp0p1p2 address`
	
	`address 192.0.2.1/27`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Configure EAST

The connection from EAST to WEST only requires a minor change from that configured in the section Basic site-to-site connection *(page 25)*.

- WEST retains its fixed IP, so no modification is required to the remote peer IP address.
- EAST has a dynamic local IP, so that must change. The *dhcp-interface* option specifies the DHCP client interface.

To configure this connection, perform the following steps on EAST in configuration mode.

Table 21: Specify that the local IP is dynamic

Step	Command

Remove the existing `local-address` configuration so that doesn't conflict with the `dhcp-interface` configuration that will be set.	`vyatta@EAST# delete security vpn ipsec site-to-site peer 192.0.2.1 local-address`
	
	`[edit]`

Specify the DHCP client interface to use for the connection.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 dhcp-interface dp0p1p1`
	
	`[edit]`

Commit the configuration.	`vyatta@EAST# commit`

View the configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1E`
	`dhcp-interface dp0p1p1`
	`ike-group IKE-1E`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.60.0/24`
	`}`
	`remote {`
	`prefix 192.168.40.0/24`
	`}`
	`}`

View data plane interface dp0p1p1 address configuration. It is set to dhcp which configures it as a DHCP client. This is the setting required by dhcp-interface.	`vyatta@EAST# show interfaces dataplane dp0p1p1`
	
	`address dhcp`

VPN connection to a peer using dynamic DNS

This section presents the following topics:

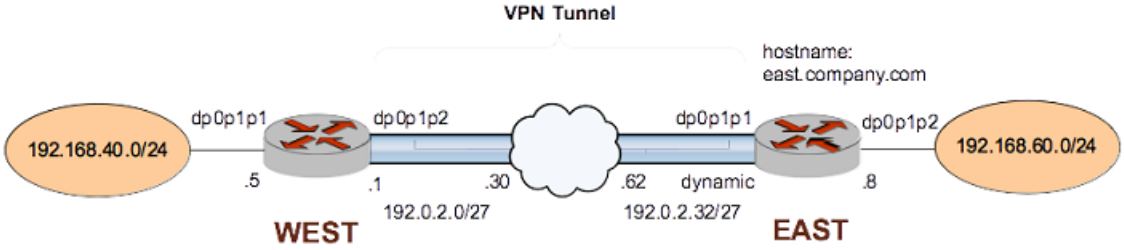
© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

This section presents a sample configuration for a connection between WEST and EAST, where EAST has a dynamic IP address (it is configured as a DHCP client) and is configured for dynamic DNS. In this example:

- EAST has a dynamic IP address from WEST's point of view but WEST can initiate connections to EAST because EAST's hostname remains constant even though its IP address may change.
- WEST retains its fixed IP address.

When you have finished, these systems will be configured as shown in the following figure.

Figure 5: IPsec VPN connection with dynamic IP address and dynamic DNS



Before you begin:

- This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section Basic site-to-site connection *(page 25)*. Only the relevant changes to that configuration are presented here.

Configure WEST

The following table defines configuration changes for a new site-to-site connection to EAST.

- The main change is the IP address specification of the peer. This is set to the hostname for EAST: “east.company.com”. This is the hostname that is configured on EAST with the dynamic DNS provider. Because the IP address for EAST can be resolved, WEST can either initiate IPsec connections to, or receive IPsec connections from EAST.
- The other important change is to configure **auto-update** so that if EAST's IP address changes, the IPsec connection to EAST will be restarted automatically.

To configure this connection, perform the following steps on WEST in configuration mode.

Table 22: Creating a site-to-site connection to a peer with a dynamic IP address and using dynamic DNS

Step	Command
Delete the previous configuration.	`vyatta@WEST# delete security vpn ipsec site-to-site peer 192.0.2.33`
Create the node for EAST and set the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer east.company.com authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit security vpn ipsec site-to-site peer east.company.com`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

Provide the string that will be used to generate encryption keys.	`vyatta@WEST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@WEST# set local-address 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Create a tunnel configuration, and provide the local subnet for this tunnel.	`vyatta@WEST# set tunnel 1 local prefix 192.168.40.0/24`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Provide the remote subnet for the tunnel.	`vyatta@WEST# set tunnel 1 remote prefix 192.168.60.0/24`
	
	`[edit security vpn ipsec site-to-site peer east.company.com]`

Return to the top of the configuration tree.	`vyatta@WEST# top`
Commit the configuration.	`vyatta@WEST# commit`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer east.company.com`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.40.0/24`
	`}`
	`remote {`
	`prefix 192.168.60.0/24`
	`}`
	`}`

View data plane interface dp0p1p2 address configuration. local-address is set to this address.	`vyatta@WEST# show interfaces dataplane dp0p1p2 address`
	
	`address 192.0.2.1/27`

Specify that the IPsec connection should be refreshed every 60 seconds - in case the peer's IP address changes. If this happens, the new IP address will be resolved via the dynamic DNS service provider.	`vyatta@WEST# set security vpn ipsec auto-update 60`
	
	`[edit]`

Commit the configuration.	`vyatta@WEST# commit`

View the configuration.	`vyatta@WEST# show security vpn ipsec auto-update`
	
	`auto-update 60`

Configure EAST

The connection from EAST to WEST only requires a minor change from that configured in the section Basic site-to-site connection *(page 25)*.

- WEST retains its fixed IP, so no modification is required to the remote peer IP address.
- EAST has a dynamic local IP, so that must change. The **dhcp-interface** option specifies the DHCP client interface.
- EAST is also configured for dynamic DNS, in this case with service provider DynDNS. See the “Configuring Dynamic DNS” section in the AT&T Vyatta Network Operating System Services Configuration Guide for details on configuring a system for dynamic DNS.

To configure this connection, perform the following steps on EAST in configuration mode.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 23: Specify that the local IP is dynamic

Step	Command

Remove the existing local-address configuration so that doesn't conflict with the dhcp-interface configuration that will be set.	`vyatta@EAST# delete security vpn ipsec site-to-site peer 192.0.2.1 local-address`
	
	`[edit]`

Specify the DHCP client interface to use for the connection.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 dhcp-interface dp0p1p1`
	
	`[edit]`

Commit the configuration.	`vyatta@EAST# commit`

View the configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1E`
	`dhcp-interface dp0p1p1`
	`ike-group IKE-1E`
	`tunnel 1 {`
	`local {`
	`prefix 192.168.60.0/24`
	`}`
	`remote {`
	`prefix 192.168.40.0/24`
	`}`
	`}`

View data plane interface dp0p1p1 address configuration. It is set to dhcp which configures it as a DHCP client. This is the setting required by dhcp-interface.	`vyatta@EAST# show interfaces dataplane dp0p1p1`
	
	`address dhcp`

Display the dynamic DNS configuration on EAST:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 24: Display the dynamic DNS configuration

Step	Command

View the dynamic DNS configuration.	`vyatta@EAST# show service dns dynamic`
	
	`interface dp0p1p1 {`
	`  service dyndns {`
	`  host-name east.company.com`
	`  login test`
	`  password testpassword`
	`  }`
	`}`

GRE tunnel protected with IPsec

GRE, IP-in-IP, and SIT tunnels are not encrypted, and provide no security outside of a simple password-like key that is exchanged in clear text in each packet. This means that GRE, IP-in-IP, and SIT tunnels, on their own, do not provide adequate security for production environments.

At the same time, IPsec policy-based tunnels cannot directly route non-IP or multicast protocols, and IPsec also has limitations from an operations point of view. Using tunnel interfaces in conjunction with IPsec VPN provides secure, routable tunnel connections between gateways, that have some advantages over traditional IPsec policy-based tunnel mode connections:

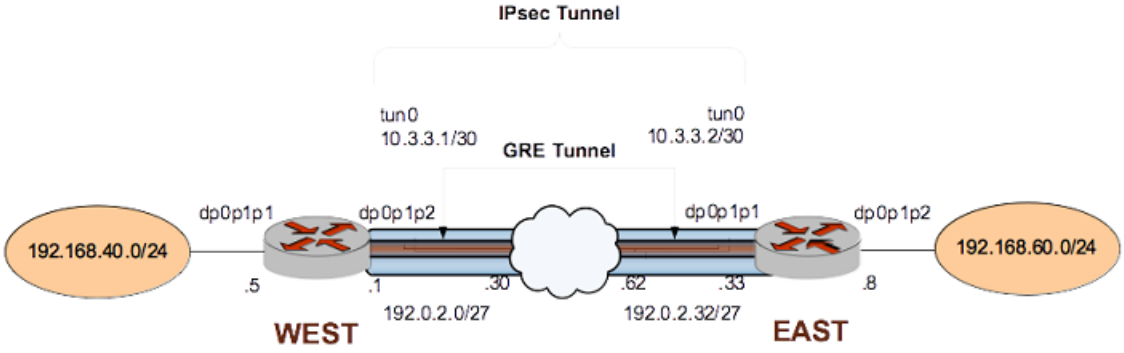
- Support for standard operational commands such as `show interfaces` and `show route`
- Support for operational tools such as `traceroute` and SNMP
- Dynamic tunnel failover using routing protocols
- Simplified IPsec policies and troubleshooting

For secure routable tunnels, GRE, IP-in-IP, and SIT tunnel interfaces should be used in conjunction with an IPsec connection, so that the IP tunnel can be protected by the IPsec tunnel.

This set of examples configures a GRE tunnel between EAST to WEST and protects it within an IPsec tunnel between the same endpoints.

When you have finished, WEST and EAST will be configured as shown in the following figure.

Figure 6: GRE tunnel protected by an IPsec tunnel



Configure WEST

This section presents the following examples:

- Defining the GRE tunnel on WEST *(page 54)*
- Defining the IPsec tunnel on WEST *(page 54)*

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- Defining a static route on WEST *(page 56)*

Defining the GRE tunnel on WEST

For details on GRE tunnels, refer to AT&T Vyatta Network Operating System Tunnels Configuration Guide.

The following procedure defines WEST's end of the GRE tunnel. In this example:

- The tunnel interface tun0 on router WEST is assigned the IP address 10.3.3.1/30.
- The encapsulation type is set to GRE.
- The IP address on the local side of the GRE tunnel (`local-ip`) is set to that of the local data plane interface (192.0.2.1).
- The IP address of the other end of the GRE tunnel (`remote-ip`) is set to the address of the remote system (192.0.2.33).
- Multicast is enabled in order to allow routing protocols to be carried on the GRE tunnel.

To create the tunnel interface and the tunnel endpoint on WEST, perform the following steps in configuration mode.

Table 25: Defining the GRE tunnel from WEST to EAST

Step	Command
Create the GRE tunnel interface, and specify the IP address to be associated with it.	`vyatta@WEST# set interfaces tunnel tun0 address 10.3.3.1/30`
Assign a brief description for the GRE tunnel interface.	`vyatta@WEST# set interfaces tunnel tun0 description “GRE tunnel to router EAST”`
Specify the encapsulation mode for the tunnel.	`vyatta@WEST# set interfaces tunnel tun0 encapsulation gre`
Allow multicast protocols (e.g., routing protocols) to be carried over the tunnel.	`vyatta@WEST# set interfaces tunnel tun0 multicast enable`
Specify the local IP address for the GRE tunnel.	`vyatta@WEST# set interfaces tunnel tun0 local-ip 192.0.2.1`
Specify the remote IP address for the GRE tunnel.	`vyatta@WEST# set interfaces tunnel tun0 remote-ip 192.0.2.33`
Commit the configuration.	`vyatta@WEST# commit`

View the modified configuration.	`vyatta@WEST# show interfaces tunnel tun0`
	
	`address 10.3.3.1/30`
	`description “GRE tunnel to router EAST”`
	`encapsulation gre`
	`local-ip 192.0.2.1`
	`multicast enable`
	`remote-ip 192.0.2.33`

Defining the IPsec tunnel on WEST

The following procedure creates the IPsec tunnel from WEST to EAST.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- WEST uses IP address 192.0.2.1 on dp0p1p2.
- EAST uses IP address 192.0.2.33 on dp0p1p1.
- The IKE group is IKE-1W.
- The preshared secret is “test_key_1”.
- All GRE traffic will be passed through the tunnel.

This examples assumes that you have already configured the following:

- IKE group IKE-1W (see Configure an IKE group on WEST *(page 25)*)
- ESP group ESP-1W (see Configure an ESP group on WEST *(page 26)*)

To create the IPsec tunnel from WEST to EAST, perform the following steps on WEST in configuration mode.

Table 26: Defining the IPsec tunnel from WEST to EAST

Step	Command
Define the site-to-site connection to EAST. Set the authentication mode.	`vyatta@WEST# set security vpn ipsec site-to-site peer 192.0.2.33 authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit security vpn ipsec site-to-site peer 192.0.2.33`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Provide the string that will be used to authenticate the peers.	`vyatta@WEST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify the default ESP group for all tunnels.	`vyatta@WEST# set default-esp-group ESP-1W`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify the IKE group.	`vyatta@WEST# set ike-group IKE-1W`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@WEST# set local-address 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify that only GRE traffic will pass through the tunnel.	`vyatta@WEST# set tunnel 1 protocol gre`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Return to the top of the configuration hierarchy.	`vyatta@WEST# top`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
Commit the configuration.	`vyatta@WEST# commit`

View the modified configuration.	`vyatta@WEST# show security vpn ipsec site-to-site peer 192.0.2.33`
	
	`authentication`
	`  mode pre-shared-secret`
	`  pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1W`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`tunnel 1 {`
	`  protocol gre`
	`}`

Defining a static route on WEST

The following procedure creates the static route for traffic destined for the far end of the GRE tunnel.

Note: Routing protocols can be used to specify how to get to the remote network. This method simply provides the minimal requirement to achieve this.

- Send traffic destined for 192.168.60.0/24 to the far end of the GRE tunnel at 10.3.3.2.

To create the static route, perform the following steps on WEST in configuration mode.

Table 27: Defining a static route on WEST

Step	Command
Create the static route.	`vyatta@WEST# set protocols static route 192.168.60.0/24 next-hop 10.3.3.2`
Commit the configuration.	`vyatta@WEST# commit`

View the modified configuration.	`vyatta@WEST# show protocols static route`
	
	`192.168.60.0/24 {`
	`  next-hop 10.3.3.2`
	`}`

Configure EAST

This section presents the following examples:

- Defining the GRE tunnel on EAST *(page 56)*
- Defining the IPsec tunnel on EAST *(page 57)*
- Defining a static route on EAST *(page 59)*

Defining the GRE tunnel on EAST

For details on GRE tunnels, refer to AT&T Vyatta Network Operating System Tunnels Configuration Guide.

The following procedure defines EAST's end of the GRE tunnel. In this example:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- The tunnel interface tun0 on router EAST is assigned the IP address 10.3.3.2/30.
- The encapsulation type is set to GRE.
- The IP address on the local side of the GRE tunnel (`local-ip`) is set to that of the local data plane interface (192.0.2.33).
- The IP address of the other end of the GRE tunnel (`remote-ip`) is set to the address of the remote system (192.0.2.1).

To create the tunnel interface and the tunnel endpoint on EAST, perform the following steps in configuration mode.

Table 28: Defining the GRE tunnel from EAST to WEST

Step	Command
Create the GRE tunnel interface, and specify the IP address to be associated with it.	`vyatta@EAST# set interfaces tunnel tun0 address 10.3.3.2/30`
Assign a brief description for the GRE tunnel interface.	`vyatta@EAST# set interfaces tunnel tun0 description “GRE tunnel to router WEST”`
Specify the encapsulation mode for the tunnel.	`vyatta@EAST# set interfaces tunnel tun0 encapsulation gre`
Allow multicast protocols (e.g., routing protocols) to be carried over the tunnel.	`vyatta@EAST# set interfaces tunnel tun0 multicast enable`
Specify the local IP address for the GRE tunnel.	`vyatta@EAST# set interfaces tunnel tun0 local-ip 192.0.2.33`
Specify the remote IP address for the GRE tunnel.	`vyatta@EAST# set interfaces tunnel tun0 remote-ip 192.0.2.1`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration.	`vyatta@EAST# show interfaces tunnel tun0`
	
	`address 10.3.3.2/30`
	`description “GRE tunnel to router WEST”`
	`encapsulation gre`
	`local-ip 192.0.2.33`
	`multicast enable`
	`remote-ip 192.0.2.1`

Defining the IPsec tunnel on EAST

The following procedure creates the IPsec tunnel from EAST to WEST.

- EAST uses IP address 192.0.2.33 on dp0p1p1.
- WEST uses IP address 192.0.2.1 on dp0p1p2.
- The IKE group is IKE-1E.
- The preshared secret is “test_key_1”.
- All GRE traffic will be passed through the tunnel.

This examples assumes that you have already configured the following:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- IKE group IKE-1E (see Configure an IKE group on EAST *(page 30)*)
- ESP group ESP-1E (see Configure an ESP group on EAST *(page 31)*)

To create the IPsec tunnel from EAST to WEST, perform the following steps on EAST in configuration mode.

Table 29: Defining the IPsec tunnel from EAST to WEST

Step	Command
Define the site-to-site connection to WEST. Set the authentication mode.	`vyatta@EAST# set security vpn ipsec site-to-site peer 192.0.2.1 authentication mode pre-shared-secret`

Navigate to the node for the peer for easier editing.	`vyatta@EAST# edit security vpn ipsec site-to-site peer 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Provide the string that will be used to authenticate the peers.	`vyatta@EAST# set authentication pre-shared-secret test_key_1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify the default ESP group for all tunnels.	`vyatta@EAST# set default-esp-group ESP-1E`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify the IKE group.	`vyatta@EAST# set ike-group IKE-1E`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Identify the IP address on this AT&T Vyatta vRouter to be used for this connection.	`vyatta@EAST# set local-address 192.0.2.33`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify that only GRE traffic will pass through the tunnel.	`vyatta@EAST# set tunnel 1 protocol gre`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Return to the top of the configuration hierarchy.	`vyatta@EAST# top`
Commit the configuration.	`vyatta@EAST# commit`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the modified configuration.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`default-esp-group ESP-1E`
	`ike-group IKE-1E`
	`local-address 192.0.2.33`
	`tunnel 1 {`
	`protocol gre`
	`}`

View data plane interface dp0p1p1 address configuration. `local-address` is set to this address.	`vyatta@EAST# show interfaces dataplane dp0p1p1 address address 192.0.2.33/27`

Defining a static route on EAST

The following procedure creates the static route for traffic destined for the far end of the GRE tunnel.

Note: Routing protocols can be used to specify how to get to the remote network. This method simply provides the minimal requirement to achieve this.

- Send traffic destined for 192.168.40.0/24 to the far end of the GRE tunnel at 10.3.3.1.

To create the static route, perform the following steps on EAST in configuration mode.

Table 30: Defining a static route on EAST

Step	Command
Create the static route.	`vyatta@EAST# set protocols static route 192.168.40.0/24 next-hop 10.3.3.1`
Commit the configuration.	`vyatta@EAST# commit`

View the modified configuration.	`vyatta@EAST# show protocols static route`
	
	`192.168.40.0/24 {`
	`next-hop 10.3.3.1`
	`}`

Basic site-to-site connection using a virtual tunnel interface

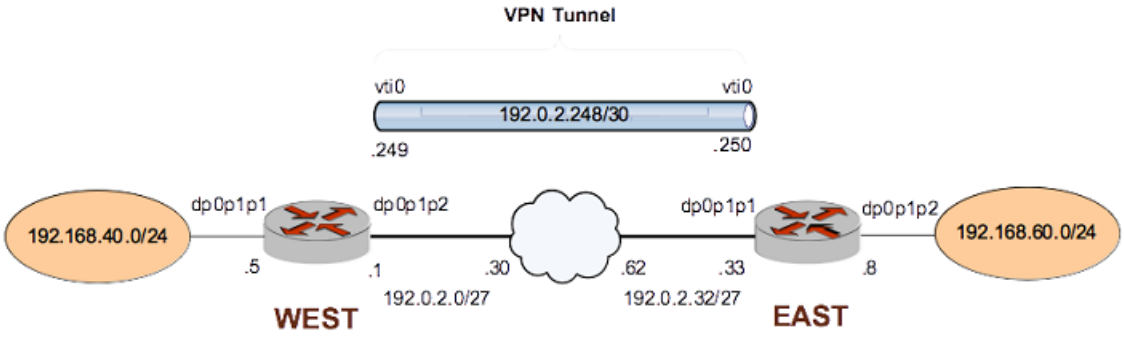
This section presents a sample configuration for a connection between WEST and EAST, where a virtual tunnel interface is bound to each end of an IPsec VPN connection. When configured in this way, the VPN can be treated like any other routable interface.

Note: IPv6 is not supported for this use case.

When the configuration is complete, the systems are configured as shown in the following figure.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Figure 7: IPsec VPN connection with virtual tunnel interfaces



This example assumes that you have already configured a basic site-to-site connection using a preshared key between WEST and EAST, as explained in the section Basic site-to-site connection *(page 25)*. Only the relevant changes to that configuration are presented here.

Configure WEST

The following table defines configuration required to create a virtual tunnel interface on WEST.

To configure this interface, perform the following steps on WEST in configuration mode.

Table 31: Creating a virtual tunnel interface on WEST

Step	Command

Create the vti interface and assign it an IP address.	`vyatta@WEST# set interfaces vti vti0 address 192.0.2.249/30`
	
	`[edit]`

Commit the configuration.	`vyatta@WEST# commit`

View the configuration.	`vyatta@WEST# show interfaces vti`
	
	`vti0 {`
	`address 192.0.2.249/30`
	`}`

The following table defines configuration changes for a new site-to-site connection to EAST.

The main changes from the basic site-to-site configuration are that the tunnel specification and default-esp-group specification are removed, and that the VPN is bound to the virtual tunnel interface created above.

To configure this connection, perform the following steps on WEST in configuration mode.

Table 32: Binding the VPN connection to the virtual tunnel interface

Step	Command

Navigate to the node for the peer for easier editing.	`vyatta@WEST# edit security vpn ipsec site-to-site peer 192.0.2.33`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

Delete the default-esp-group specification from the previous configuration.	`vyatta@WEST# delete default-esp-group`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Delete the tunnel specification from the previous configuration.	`vyatta@WEST# delete tunnel`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Bind the VPN tunnel to the vti0 interface.	`vyatta@WEST# set vti bind vti0`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Specify the ESP group for the tunnel.	`vyatta@WEST# set vti esp-group ESP-1W`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.33]`

Return to the top of the configuration tree.	`vyatta@WEST# top`
Commit the configuration.	`vyatta@WEST# commit`

View the configuration for the site-to-site connection.	`vyatta@WEST# show security vpn ipsec site-to-site peer 192.0.2.33`
	
	`authentication {`
	`  mode pre-shared-secret`
	`  pre-shared-secret test_key_1`
	`}`
	`ike-group IKE-1W`
	`local-address 192.0.2.1`
	`vti {`
	`  bind vti0`
	`  esp-group ESP-1W`
	`}`

Configure EAST

The following table defines configuration required to create a virtual tunnel interface on EAST.

To configure this interface, perform the following steps on EAST in configuration mode.

Table 33: Creating a virtual tunnel interface on EAST

Step	Command

Create the vti interface and assign it an IP address.	`vyatta@EAST# set interfaces vti vti0 address 192.0.2.250/30`
	
	`[edit]`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
Commit the configuration.	`vyatta@EAST# commit`

View the configuration.	`vyatta@EAST# show interfaces vti`
	
	`vti0 {`
	`address 192.0.2.250/30`
	`}`

The following table defines configuration changes for a new site-to-site connection to WEST.

- The main changes from the basic site-to-site configuration are that the tunnel specification and default-esp-group specification are removed, and that the VPN is bound to the virtual tunnel interface created above.

To configure this connection, perform the following steps on EAST in configuration mode.

Table 34: Binding the VPN connection to the virtual tunnel interface

Step	Command

Navigate to the node for the peer for easier editing.	`vyatta@EAST# edit security vpn ipsec site-to-site peer 192.0.2.1`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Delete the default-esp-group specification from the previous configuration.	`vyatta@EAST# delete default-esp-group`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Delete the tunnel specification from the previous configuration.	`vyatta@EAST# delete tunnel`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Bind the VPN tunnel to the vti0 interface.	`vyatta@EAST# set vti bind vti0`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Specify the ESP group for the tunnel.	`vyatta@EAST# set vti esp-group ESP-1E`
	
	`[edit security vpn ipsec site-to-site peer 192.0.2.1]`

Return to the top of the configuration tree.	`vyatta@EAST# top`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command
Commit the configuration.	`vyatta@EAST# commit`

View the configuration for the site-to-site connection.	`vyatta@EAST# show security vpn ipsec site-to-site peer 192.0.2.1`
	
	`authentication {`
	`mode pre-shared-secret`
	`pre-shared-secret test_key_1`
	`}`
	`ike-group IKE-1E`
	`local-address 192.0.2.33`
	`vti {`
	`bind vti0`
	`esp-group ESP-1E`
	`}`

Basic site-to-site connection over IPv6

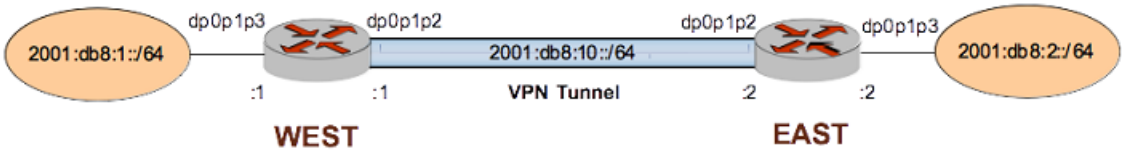
For the most part, configuring IPsec over IPv6 is the same as configuring IPsec over IPv4. There are three differences to note when configuring IPsec over IPv6.

1. IPv6 addresses are used instead of IPv4 addresses for all arguments that require IP addresses.
2. Hostnames cannot be used. They can only be used when configuring IPsec over IPv4.
3. The `any` keyword cannot be used as the `local-address`. It can only be used when configuring IPsec over IPv4.

Info:

The following example creates a basic site-to-site IPsec connection from WEST to EAST over IPv6.

Figure 8: Basic site-to-site IPsec VPN connection over IPv6



Configure WEST

The following example configuration is for the WEST system.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Table 35: Basic site-to-site IPsec VPN connection over IPv6 - WEST

Step	Command

View the data plane interface configuration on WEST.	`vyatta@WEST# show interfaces dataplane`
	
	`dataplane dp0p1p2 {`
	`address 2001:db8:10::1/64`
	`duplex auto`
	`hw-id 00:15:5d:00:d5:33`
	`speed auto`
	`}`
	`dataplane dp0p1p3 {`
	`address 2001:db8:1::1/64`
	`duplex auto`
	`hw-id 00:15:5d:00:d5:34`
	`speed auto }`
	`}`
	`[edit]`

View the IPv6 IPsec configuration on WEST.	`vyatta@WEST# show security vpn`
	
	`vpn {`
	`ipsec {`
	`esp-group ESP-1W {`
	`lifetime 3600`
	`mode tunnel`
	`pfs enable`
	`proposal 1 {`
	`encryption aes128`
	`hash sha1`
	`}`
	`}`
	`ike-group IKE-1W {`
	`lifetime 28800`
	`proposal 1 {`
	`encryption aes128`
	`hash sha1`
	`}`
	`}`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the IPv6 IPsec configuration on WEST.	logging {
	log-modes all
	}
	nat-traversal disable
	site-to-site {
	peer 2001:db8:10::2 {
	authentication {
	mode pre-shared-secret
	pre-shared-secret test123
	}
	connection-type initiate
	default-esp-group ESP-1W
	ike-group IKE-1W
	local-address 2001:db8:10::1
	tunnel 1 {
	allow-nat-networks
	disable
	allow-public-networks
	disable
	local {
	prefix
	2001:db8:1::/64
	}
	remote {
	prefix
	2001:db8:2::/64
	}
	}
	}
	}
	}
	}
	[edit]

Configure EAST

The following example configuration is for the EAST system.

Table 36: Basic site-to-site IPsec VPN connection over IPv6 - EAST

Step	Command

View the data plane interface configuration on EAST.	vyatta@EAST# show interfaces dataplane
	
	dataplane dp0p1p2 {
	address 2001:db8:10::2/64
	duplex auto
	hw-id 00:15:5d:00:d5:35
	speed auto
	}
	dataplane dp0p1p3 {
	address 2001:db8:2::2/64
	duplex auto
	hw-id 00:15:5d:00:d5:36
	speed auto }
	}
	[edit]

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Step	Command

View the IPv6 IPsec configuration on EAST.	vyatta@EAST# show security vpn
	
	vpn {
	ipsec {
	esp-group ESP-1E {
	lifetime 3600
	mode tunnel
	pfs enable
	proposal 1 {
	encryption aes128
	hash sha1
	}
	}
	ike-group IKE-1E {
	lifetime 28800
	proposal 1 {
	encryption aes128
	hash sha1
	}
	}

	logging {
	log-modes all
	}
	nat-traversal disable
	site-to-site {
	peer 2001:db8:10::1 {
	authentication {
	mode pre-shared-secret
	pre-shared-secret test123
	}
	connection-type initiate
	default-esp-group ESP-1E
	ike-group IKE-1E
	local-address 2001:db8:10::2
	tunnel 1 {
	allow-nat-networks
	disable
	allow-public-networks
	disable
	local {
	prefix
	2001:db8:2::/64
	}
	remote {
	prefix
	2001:db8:1::/64
	}
	}
	}
	}
	}
	}
	[edit]

Restrictions and limitations

The virtual tunnel interface has the following restrictions and limitations:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- IPsec injects tunnel related routes into the Linux kernel. You can also configure static routes for the same prefixes. For example, on a non-vti interface with a remote prefix of 30.1.1.0/24, you can configure a static route for 30.1.1.0/24 pointing to any interface of your choice.

  Note: You can configure static routes for backup purposes by using the same address prefixes. To configure a static route, it must point to a backup path of that prefix which is also encrypted. If the IPsec tunnel goes down, the static route becomes active.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

IPsec Site-to-Site VPN Commands

generate vpn rsa-key

Generates a pair of RSA public and private keys.

Syntax:

```
generate vpn rsa-key [ F4 ] [ bits bits ]
```

bits

Bit-length of the generated key, in 16-bit increments. The length ranges from 1024 through 4096. The default length is 2192.

F4

When specified, sets the public exponent to 65537. When absent, sets the public exponent to 3.

Operational mode

Use this command to generate a pair of RSA public and private keys. This command is available only to users with administrative privileges.

> **Note:** A larger exponent makes brute-force attacks on public keys more difficult, so AT&T recommends using the F4 option.

RSA key pairs authenticate identities of hosts or users and securely exchange a random one-time key, which is then used for a session as the symmetrical encryption key. The public key or keys (more than one public key can be derived from the private key component) are shared with the peer that requests communication with the holder of the private key. Due to this potential one-to-many relationship, the private key is typically generated by and stored on the server, and the public key or keys are distributed to one or more clients.

The RSA key pair for the local host is generated by using this command in operational mode. After the key pair is generated, it is stored at the location that is specified by the `local-key rsa-key-name` option. By default, this location is the `localhost.key` file in the `/config/ipsec.d/rsa-keys/` directory.

You can change the name and location of the key file by using security vpn rsa-keys *(page 114)*.

The following example shows how to extract the public key in an exportable form. The public key can be extracted in the format that is used in RFC-2537, RSA/MD5 KEYs and SIGs in the Domain Name System (DNS), as the credentials of a peer by extracting it from the `localhost.key` file. You can then paste it into the appropriate configuration parameter on the peer.

```
vyatta@WEST:~$ generate vpn rsa-key
Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key

Your new local RSA key has been generated.
RSA key fingerprint: d0:75:1b:c9:36:c7:3a:48:0a:d8:11:06:41:90:57:cb
vyatta@WEST:~$ show vpn ike rsa-keys

Local public key (/opt/vyatta/etc/config/ipsec.d/rsa-keys/localhost.key):

0sAQOaH8PuqTqHW6kkm6hAM7Mt4juBt7tdOQAqiNfaHou72+T/1/
ztUmsnXzT7c7YGGQQ95eej9IDgBGmhnmGa9kXn/Upa7M8Te9bINNAkHT7DqSxflEYH2eVFT3/
Q0ZghCU8U51a66OqAbuXpfQxAZ6ujAxmGBS3FOC2b9GSRqyybGSLDoniRWSFZ12Yd5ckX4CprhJmryGU0mZn91eE5kQLiUfONPcEywCmi50RqKTcQsXgF
+d7K6CrJLALyOqtXEPW0kRmaqcZXhuwlOtDHgws2vUal7H
+vQCq6OjKuO8+3xvLNZxH3820z81PytcnAa8X7YmrsjIV8MfWGPobk6l27ZjGOo9ZG44nEAS3KX
```

The following example shows how to generate a pair of RSA public and private keys.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
vyatta@WEST:~$ generate vpn rsa-key bits 1024
Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key
Your new local RSA key has been generated.
RSA key fingerprint: 78:af:08:60:92:34:c6:02:94:a2:52:53:69:91:a0:91
```

generate vpn x509 key-pair <name> private-key

Generates an X.509 private key file and a certificate signing request file.

Syntax:

`generate vpn x509 key-pair` *name* **`private-key`** [**`ecdsa`** | **`rsa`**]

name

The name to be used for the X.509 private key file and certificate signing request file. The private key file will be called `/config/auth/name.key` and the certificate signing request file will be called `/config/auth/name.csr`.

Operational mode

Use this command to generate an X.509 private key file and a certificate signing request file. If **rsa** is specified, or no private key option is specified, an RSA key is generated. If **edcsa** is specified, an ECDSA key is generated.

The private key file is required for configuring a VPN for X.509 authentication (see security vpn ipsec site-to-site peer <peer> authentication x509 key file <file-name> *(page 100)*). The certificate signing request file must be sent to a certificate authority (CA). In return, the CA will provide a server certificate (e.g. `name.crt`), a CA certificate (e.g. `ca.crt`), and potentially, a certificate revocation list (.crl) file. This procedure varies according to the CA being used. The files returned are also used to configure a VPN for X.509 authentication (see security vpn ipsec site-to-site peer <peer> authentication x509 cert-file <file-name> *(page 98)* for specifying the server certificate, security vpn ipsec site-to-site peer <peer> authentication x509 ca-cert-file <file-name> *(page 97)* for specifying the CA certificate, and security vpn ipsec site-to-site peer <peer> authentication x509 crl-file <file-name> *(page 99)* for specifying the certificate revocation list).

This example generates an X.509 private key file and a certificate signing request file. The private key file will be called `/config/auth/name.key` and the certificate signing request file will be called `/config/auth/name.csr`.

```
vyatta@vyatta:~$ generate vpn x509 key-pair mykey
Generating a 1024 bit RSA private key
..............++++++
.................................................++++++
writing new private key to '/config/auth/mykey.key1'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:us
State Name []:ca
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) []:AT&T
Organizational Unit Name (eg, department) []:Pubs
Common Name (eg, Device hostname) []:sys05
Email Address []:admin@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password (optional) []:
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
writing RSA key
```

reset vpn ipsec-peer <peer>

Resets tunnels associated with the IPsec peer.

Syntax:

```
reset vpn ipsec-peer peer [ tunnel tunnel | vti ]
```

peer
The IPv4 or IPv6 address of the VPN peer.

tunnel
The tunnel to be reset. The numbers range from 0 through 4294967295.

vti
Reset the virtual tunnel interface associated with the peer.

Operational mode

Use this command to reset IPsec tunnels associated with the specified peer. Resetting IPsec tunnels will cause the tunnels to be torn down and re-established.

If the peer is 0.0.0.0, “any”, or @id, then the tunnel is torn down and re-loaded but a new connection is not initiated because the remote end could be multiple end-points.

If tunnel or vti is not specified, then all IPsec connections associated with the peer will be restarted.

reset vpn ipsec-profile <peer>

Resets tunnels for the specified IPsec profile.

Syntax:

```
reset vpn ipsec-profile profile [ tunnel tunnel ]
```

profile
The IPsec profile.

tunnel
The tunnel to be reset.

Operational mode

Use this command to reset IPsec tunnels associated with the specified profile. Resetting IPsec tunnels will cause the tunnels to be torn down and re-established.

If tunnel is not specified, then all IPsec connections associated with the profile will be reset.

reset vpn remote-access

Terminates remote access for VPN connections.

Syntax:

```
reset vpn remote-access { all | interface interface-name | user user-name }
```

interface-name
The interface for which remote acess is to be terminated. If an interface is not specified, the reset applies to all interfaces.

user-name
The user for whom remote acess is to be terminated. If a user name is not specified, the reset applies to all users.

Operational mode

Use this command to terminate remote VPN access. If **all** is specified, access is terminated for all users.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

restart vpn

Restarts the IPsec process.

Syntax:
```
restart vpn
```

Operational mode

Use this command to restart the IPsec process.

Restarting IPsec will cause all tunnels to be torn down and re-established.

The following example shows the output resulting from the `restart vpn` command.

```
vyatta@vyatta:~$ restart vpn
Restarting IPsec process...
vyatta@vyatta:~$
```

security vpn ipsec

Enables IPsec VPN functionality on the system.

Syntax:
```
set security vpn ipsec
```

Syntax:
```
delete security vpn ipsec
```

Syntax:
```
show security vpn ipsec
```

Configuration mode

```
security {
        vpn {
            ipsec
    }
}
```

Use this command to enable IPsec VPN functionality on the AT&T Vyatta vRouter.

Note: The sending and receiving of ICMP redirects is disabled when IPsec VPN is configured.

Use the `set` form of this command to enable IPsec VPN.

Use the `delete` form of this command to remove all IPsec VPN configuration and disable IPsec VPN functionality.

Use the `show` form of this command to view the IPsec VPN configuration.

security vpn ipsec auto-update <interval>

Specifies the interval to automatically refresh IPsec connections.

Syntax:
`set security vpn ipsec auto-update` *interval*

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
delete security vpn ipsec auto-update
```

Syntax:

```
show security vpn ipsec auto-update
```

IPsec connections are not refreshed periodically.

interval

The interval (seconds) in which to review IPsec connections for changes (for example, the IP address of a dynamic DNS peer changes) and restart them if changes are found. The number ranges from 30 through 65535.

Configuration mode

```
security {
        vpn {
            ipsec {
                auto-update interval
        }
    }
}
```

Use this command to specify the interval to automatically refresh IPsec connections. This is most useful for connections where the remote peer uses dynamic DNS to keep track of its address. Auto-update will review information pertaining to the connection at the specified interval and, if it is changed (for example, if the dynamic DNS peer's IP address has changed), will restart the connection.

Use the `set` form of this command to specify the interval at which to automatically refresh IPsec connections.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn ipsec esp-group <name>

Defines a named ESP configuration for IKE Phase 2 negotiations.

Syntax:

```
set security vpn ipsec esp-group name
```

Syntax:

```
delete security vpn ipsec esp-group
```

Syntax:

```
show security vpn ipsec esp-group
```

name

Multi-node. The name to be used to refer to the ESP configuration.

You can create multiple ESP configurations by creating multiple `esp-group` configuration nodes. At least one ESP configuration must be defined, for use in tunnel configuration.

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name
        }
    }
}
```

Use this command to define an ESP group.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

An ESP group lets you set the Encapsulating Security Payload (ESP) parameters required for IKE Phase 2 and the lifetime of the resulting IPsec security association.

Use the `set` form of this command to create and modify an ESP group.

Use the `delete` form of this command to remove ESP group configuration.

Use the `show` form of this command to view ESP group configuration.

security vpn ipsec esp-group compression

Enables or disables ESP compression for an ESP group.

Syntax:
```
set security vpn ipsec esp-group compression { disable | enable }
```

Syntax:
```
delete security vpn ipsec esp-group compression
```

Syntax:
```
show security vpn ipsec esp-group compression
```

{ disable | enable }
Enable or disable ESP compression. The default is disable.

Configuration mode

```
security {
    vpn {
        ipsec {
              esp-group esp1 {
                    compression enable
              }
        }
    }
}
```

Use the `set` form of this command to enable or disable ESP compression for an ESP group.

Use the `delete` form of this command to revert to the default compression configuration (disable).

Use the `show` form of this command to view the current compression configuration.

security vpn ipsec esp-group disable-strict-mode

Disables strict-mode proposal negotiation for an ESP group.

Syntax:
```
set security vpn ipsec esp-group disable-strict-mode
```

Syntax:
```
delete security vpn ipsec esp-group disable-strict-mode
```

Syntax:
```
show security vpn ipsec esp-group disable-strict-mode
```

Configuration mode

```
security {
        vpn {
            ipsec {
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
                esp-group group-name {
                   disable-strict-mode
                }
            }
        }
}
```

Use the `set` form of this command to disable strict mode proposal negotiation for an ESP group.

Use the `delete` form of this command to revert to the default behavior (use strict mode proposal negotiation).

Use the `show` form of this command to view the current strict mode configuration.

security vpn ipsec esp-group <name> lifetime <lifetime>

Specifies how long an ESP encryption key can stay in effect.

Syntax:

`set security vpn ipsec esp-group` *name* **`lifetime`** *lifetime*

Syntax:

`delete security vpn ipsec esp-group` *name* **`lifetime`**

Syntax:

`show security vpn ipsec esp-group` *name* **`lifetime`**

Keys stay in effect for 3,600 seconds (1 hour).

name

The name to be used to refer to the ESP configuration.

lifetime

The time, in seconds, that any key created during IKE Phase 2 negotiation can persist before the next negotiation is triggered. The numbers range from 30 through 86400 (that is, 24 hours). The default is 3600 (1 hour).

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name {
                    lifetime lifetime
                }
            }
    }
}
```

Use this command to specify the lifetime of a key.

Note: The lifetime of IKE security associations (SA) should be greater than the lifetime of ESP SA.

Use the `set` form of this command to specify the lifetime of a key.

Use the `delete` form of this command to remove the lifetime configuration.

Use the `show` form of this command to view the lifetime configuration.

security vpn ipsec esp-group <name> mode <mode>

Specifies the IPsec connection mode to be used.

Syntax:

`set security vpn ipsec esp-group` *name* **`mode`** *mode*

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Syntax:
```
delete security vpn ipsec esp-group name mode
```

Syntax:
```
show security vpn ipsec esp-group name mode
```

IPsec connections use tunnel mode.

name

The name to be used to refer to the ESP configuration.

mode

The IPsec connection mode. Supported values are as follows:

`tunnel`—Tunnel mode.

`transport`—Transport mode.

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name {
                        mode mode
                }
            }
    }
}
```

Use this command to specify the IPsec connection mode to be used.

Use the `set` form of this command to specify the IPsec connection mode to be used.

Use the `delete` form of this command to restore the default IPsec connection mode.

Use the `show` form of this command to view IPsec connection mode configuration.

security vpn ipsec esp-group <name> pfs <pfs>

Specifies whether or not Perfect Forward Secrecy (PFS) is used.

Syntax:
```
set security vpn ipsec esp-group name pfs pfs
```

Syntax:
```
delete security vpn ipsec esp-group name pfs
```

Syntax:
```
show security vpn ipsec esp-group name pfs
```

PFS is enabled and uses the Diffie-Hellman group defined in the ike-group.

name

The name to be used to refer to the ESP configuration.

pfs

Enables or disables Perfect Forward Secrecy. Supported values are as follows:

`enable`—Enables PFS using Diffie-Hellman group defined in the ike-group.

`dh-group2`—Enables PFS using Diffie-Hellman group 2.

`dh-group5`—Enables PFS using Diffie-Hellman group 5.

`dh-group14`—Enables PFS using Diffie-Hellman group 14.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

`dh-group15`—Enables PFS using Diffie-Hellman group 15.

`dh-group16`—Enables PFS using Diffie-Hellman group 16.

`dh-group17`—Enables PFS using Diffie-Hellman group 17.

`dh-group18`—Enables PFS using Diffie-Hellman group 18.

`dh-group19`—Enables PFS using Diffie-Hellman group 19.

`dh-group20`—Enables PFS using Diffie-Hellman group 20.

`disable`—Disables PFS.

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name {
                            pfs pfs
                }
            }
    }
}
```

Use this command to specify whether or not PFS will be used and, if used, which Diffie-Hellman group is to be used.

Note: Regardless of the setting of this parameter, if the far-end VPN peer requests PFS, the AT&T Vyatta vRouter will use PFS.

Note: If PFS or a Diffie-Hellman group is not configured for ESP, the default is to use the same Diffie-Hellman group that is used for the configured IKE proposal.

Use the `set` form of this command to specify whether or not PFS will be used.

Use the `delete` form of this command to restore default PFS configuration.

Use the `show` form of this command to view PFS configuration.

security vpn ipsec esp-group <name> proposal <num>

Defines an ESP group proposal for IKE Phase 2 negotiation.

Syntax:

```
set security vpn ipsec esp-group name  proposal num
```

Syntax:

```
delete security vpn ipsec esp-group proposal
```

Syntax:

```
show security vpn ipsec esp-group proposal
```

name

The name to be used to refer to the ESP configuration.

num

Multi-node. An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation.

You can define multiple proposals within a single ESP configuration by creating multiple `proposal` configuration nodes. Each must have a unique identifier.

Configuration mode

```
security {
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
        vpn {
            ipsec {
                esp-group name {
                            proposal num
                }
            }
    }
}
```

Use this command to define an ESP proposal for IKE Phase 2 negotiation.

Use the `set` form of this command to create an ESP proposal.

Use the `delete` form of this command to remove an ESP proposal and all its configuration.

Use the `show` form of this command to view ESP proposal configuration.

security vpn ipsec esp-group <name> proposal <num> encryption <cipher>

Specifies the encryption cipher for an ESP proposal.

Syntax:

```
set security vpn ipsec esp-group name proposal num encryption cipher
```

Syntax:

```
delete security vpn ipsec esp-group proposal num encryption
```

Syntax:

```
show security vpn ipsec esp-group proposal num encryption
```

The default is `aes128`.

name

The name to be used to refer to the ESP configuration.

proposal

An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation.

cipher

The encryption cipher to be proposed. Supported values are as follows:

`aes128`—Advanced Encryption Standard with a 128-bit key.

`aes256`—Advanced Encryption Standard with a 256-bit key.

`aes128gcm128`—128-bit AES with 128-bit Galois/Counter Mode (GCM).

`aes256gcm128`—256-bit AES with 128-bit Galois/Counter Mode (GCM).

`3des`—Triple-DES (Data Encryption Standard).

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name {
                        proposal num {
                        encryption cipher
                }
            }
        }
    }
}
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use this command to specify the encryption cipher to be proposed in an ESP proposal during IKE Phase 2 negotiation.

Use the `set` form of this command to specify the encryption cipher.

Use the `delete` form of this command to restore default encryption configuration.

Use the `show` form of this command to view ESP proposal encryption configuration.

security vpn ipsec esp-group <name> proposal <num> hash <hash>

Specifies the hash algorithm for an ESP proposal.

Syntax:

```
set security vpn ipsec esp-group name proposal num hash hash
```

Syntax:

```
delete security vpn ipsec esp-group proposal num hash
```

Syntax:

```
show security vpn ipsec esp-group proposal num hash
```

The default is *sha1*.

name

The name to be used to refer to the ESP configuration.

proposal

An integer uniquely identifying a proposal to be used in IKE Phase 2 negotiation.

hash

The hash algorithm to be used. Supported values are as follows:

`md5`— MD5 hash message authentication code (HMAC).

`null`— No separate authentication code.

`sha1`— SHA1 HMAC (default).

`sha1_160`—SHA1_160 bit hash.

`sha2_256`—SHA2_256_128 HMAC

`sha2_384`—SHA2_384_192 HMAC

`sha2_512`—SHA2_512_256 HMAC

Configuration mode

```
security {
        vpn {
            ipsec {
                esp-group name {
                        proposal num {
                            hash hash
                }
            }
        }
    }
}
```

Use this command to specify the hash algorithm to be proposed in an ESP proposal.

Use the `set` form of this command to specify the hash algorithm to be proposed.

Use the `delete` form of this command to restore default hash algorithm configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `show` form of this command to view ESP proposal hash algorithm configuration.

security vpn ipsec ike-group <name>

Defines a named IKE configuration for IKE Phase 1 negotiations.

Syntax:
`set security vpn ipsec ike-group` *name*

Syntax:
`delete security vpn ipsec ike-group`

Syntax:
`show security vpn ipsec ike-group`

name
Mandatory. Multi-node. The name to be used to refer to this IKE configuration.

You can create multiple IKE configurations by creating multiple `ike-group` configuration nodes.

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name
        }
    }
}
```

Use this command to configure a set of values for IKE configuration.

This configuration can be referred to as part of configuring a site-to-site configuration with a VPN peer, using security vpn ipsec profile <profile-name> authentication mode <mode> *(page 89)*.

Use the `set` form of this command to create an IKE group.

Use the `delete` form of this command to remove an IKE group and all its configuration.

Use the `show` form of this command to view IKE group configuration.

security vpn ipsec ike-group <name> dead-peer-detection

Defines the behavior if the VPN peer becomes unreachable.

Syntax:
`set security vpn ipsec ike-group` *name* **`dead-peer-detection`** [**`action`** *action* | **`interval`** *interval* | **`timeout`** *timeout*]

Syntax:
`delete security vpn ipsec ike-group` *name* **`dead-peer-detection`**

Syntax:
`show security vpn ipsec ike-group` *name* **`dead-peer-detection`**

Default values are used.

name
The name to be used to refer to this IKE configuration.

action
Specifies the action to be taken if the timeout interval expires. Supported values are as follows:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

`hold`—Queue packets until the tunnel comes back up. This is the default value.

`clear`—Delete the connection information.

`restart`—Attempt to restart the tunnel.

interval

The interval, in seconds, at which IKE keep-alive messages will be sent to VPN peers. The numbers range from 15 through 86400. The default is 30.

timeout

The interval, in seconds, after which if the peer has not responded the defined action will be taken. The numbers range from 30 through 86400. The default is 120.

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name {
                    dead-peer-detection {
                        action action
                        interval interval
                        timeout timeout
                    }
                }
            }
    }
}
```

Use this command to specify how the system should detect dead IPsec VPN peers.

Use the `set` form of this command to configure dead peer detection.

Use the `delete` form of this command to remove dead peer detection configuration.

Use the `show` form of this command to view dead peer detection configuration.

security vpn ipsec ike-group disable-strict-mode

Disables strict-mode proposal negotiation for an IKE group.

Syntax:

```
set security vpn ipsec ike-group disable-strict-mode
```

Syntax:

```
delete security vpn ipsec ike-group disable-strict-mode
```

Syntax:

```
show security vpn ipsec ike-group disable-strict-mode
```

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group group-name {
                   disable-strict-mode
                }
            }
        }
}
```

Use the `set` form of this command to disable strict mode proposal negotiation for an IKE group.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `delete` form of this command to revert to the default behavior (use strict mode proposal negotiation).

Use the `show` form of this command to view the current strict mode configuration.

security vpn ipsec ike-group <group-name> ike-version <version>

Specifies the version of IKE for a configuration.

Syntax:
`set security vpn ipsec ike-group` *group-name* **`ike-version`** *version*

Syntax:
`delete security vpn ipsec ike-group` *group-name* **`ike-version`**

Syntax:
`show security vpn ipsec ike-group` *group-name* **`ike-version`**

The default version is 1 (IKEv1).

group-name
The name to be used to refer to this IKE configuration (for example, IKE-E1).

`ike-version` ***version***

version

One of the following IKE versions:

- 1–Use IKEv1.
- 2–Use IKEv2.
- 2+1–Use IKEv2 when initiating, but accept any protocol version when responding.

Note: When configuring peer 1 with the 2+1 version and peer 2 with the 1 version, AT&T recommends that you configure **respond** as the connection-type for peer 1. Refer to the `security vpn ipsec site-to-site peer connection-type` command for more information.

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group group-name {
                    ike-version version
                }
            }
    }
}
```

Use this command to specify the version of IKE (1, 2, or 2+1) for a configuration.

Use the `set` form of this command to specify the version of IKE for a configuration.

Use the `delete` form of this command to restore the default version (1).

Use the `show` form of this command to view the current version.

security vpn ipsec ike-group <name> lifetime <lifetime>

Specifies how long an IKE group key can stay in effect.

Syntax:
`set security vpn ipsec ike-group` *name* **`lifetime`** *lifetime*

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Syntax:
```
delete security vpn ipsec ike-group name lifetime
```

Syntax:
```
show security vpn ipsec ike-group name lifetime
```

An IKE key stays in effect for 8 hours.

name
The name to be used to refer to this IKE configuration.

lifetime
The time, in seconds, that any key created during IKE Phase 1 negotiation can persist before the next negotiation is triggered. The numbers range from 30 through 86400 (that is, 24 hours). The default is 28800 (8 hours).

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name {
                    lifetime lifetime
                }
            }
    }
}
```

Use this command to specify the lifetime of an IKE key.

Note: The lifetime of IKE security associations (SA) should be greater than the lifetime of ESP SA.

Use the `set` form of this command to specify key lifetime.

Use the `delete` form of this command to restore the default key lifetime.

Use the `show` form of this command to view key lifetime configuration.

security vpn ipsec ike-group <name> proposal <num>

Specifies the IKE group proposal number.

Syntax:
```
set security vpn ipsec ike-group name proposal num
```

Syntax:
```
delete security vpn ipsec ike-group proposal
```

Syntax:
```
show security vpn ipsec ike-group proposal
```

name
The name to be used to refer to the IKE configuration.

proposal
Multi-node. An integer uniquely identifying an IKE proposal.

You can define up to 10 proposals within a single IKE configuration by creating multiple `proposal` configuration nodes. Each proposal must have a unique identifier.

Configuration mode

```
security {
        vpn {
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            ipsec {
                ike-group name {
                        proposal num {
                }
            }
        }
    }
}
```

Use this command to create an IKE proposal. The proposal will be used in IKE Phase 1 negotiation.

Use the `set` form of this command to create an IKE proposal.

Use the `delete` form of this command to remove an IKE proposal and all its configuration.

Use the `show` form of this command to view IKE proposal configuration.

security vpn ipsec ike-group <name> proposal <num> dh-group <group>

Specifies the group to be proposed for Diffie-Hellman key exchanges.

Syntax:

```
set security vpn ipsec ike-group name proposal num dh-group group
```

Syntax:

```
delete security vpn ipsec ike-group proposal num dh-group
```

Syntax:

```
show security vpn ipsec ike-group proposal num dh-group
```

name

The name to be used to refer to the IKE configuration.

proposal

An integer uniquely identifying an IKE proposal.

pfs

The Diffie-Hellman group used for key exchanges. Supported values are as follows:

`2`—Group 2.

`5`—Group 5.

`14`—Group 14.

`15`—Group 15.

`16`—Group 16.

`17`—Group 17.

`18`—Group 18.

`19`—Group 19.

`20`—Group 20.

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name {
                        proposal num {
                            dh-group group
                }
            }
        }
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
    }
}
```

Use this command to specify the Diffie-Hellman group used for key exchanges.

Use the `set` form of this command to specify the Diffie-Hellman group used for key exchanges.

Use the `delete` form of this command to revert to the default group.

Use the `show` form of this command to view the group configuration.

security vpn ipsec ike-group <name> proposal <num> encryption <cipher>

Specifies the encryption cipher to be proposed in IKE Phase 1 negotiation.

Syntax:

`set security vpn ipsec ike-group` *name* **`proposal`** *num* **`encryption`** *cipher*

Syntax:

`delete security vpn ipsec ike-group proposal` *num* **`encryption`**

Syntax:

`show security vpn ipsec ike-group proposal` *num* **`encryption`**

The default is `aes128`.

name

The name to be used to refer to the IKE configuration.

`proposal`

An integer uniquely identifying an IKE proposal.

cipher

The encryption cipher to be proposed. Supported values are as follows:

`aes128`—Advanced Encryption Standard with a 128-bit key.

`aes256`—Advanced Encryption Standard with a 256-bit key.

`aes128gcm128`—128-bit AES with 128-bit Galois/Counter Mode (GCM).

`aes256gcm128`—256-bit AES with 128-bit Galois/Counter Mode (GCM).

`3des`—Triple-DES (Data Encryption Standard).

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name {
                        proposal num {
                            encryption cipher
                }
            }
        }
    }
}
```

Use this command to specify the encryption cipher to be proposed in IKE Phase 1 negotiation.

Use the `set` form of this command to set the encryption cipher.

Use the `delete` form of this command to restore the default encryption cipher.

Use the `show` form of this command to view encryption cipher configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

security vpn ipsec ike-group <name> proposal <num> hash <hash>

Specifies the hash algorithm to be proposed.

Syntax:
`set security vpn ipsec ike-group` *name* **`proposal`** *num* **`hash`** *hash*

Syntax:
`delete security vpn ipsec ike-group proposal` *num* **`hash`**

Syntax:
`show security vpn ipsec ike-group proposal` *num* **`hash`**

The default is `sha1`.

name
The name to be used to refer to the IKE configuration.

`proposal`
An integer uniquely identifying an IKE proposal.

hash
The hash algorithm to be used. Supported values are as follows:

`md5`— MD5 hash message authentication code (HMAC).

`null`— No separate authentication code.

`sha1`— SHA1 HMAC (default).

`sha1_160`—SHA1_160 bit hash.

`sha2_256`—SHA2_256_128 HMAC

`sha2_384`—SHA2_384_192 HMAC

`sha2_512`—SHA2_512_256 HMAC

Configuration mode

```
security {
        vpn {
            ipsec {
                ike-group name {
                        proposal num {
                                hash hash
                }
            }
        }
    }
}
```

Use this command to specify the hash algorithm to be proposed in an IKE proposal.

Use the `set` form of this command to specify the hash algorithm to be proposed.

Use the `delete` form of this command to restore default hash algorithm configuration.

Use the `show` form of this command to view IKE proposal hash algorithm configuration.

security vpn ipsec logging

Specifies logging options for IPsec VPN.

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
set security vpn ipsec logging [ log-modes mode ]
```

Syntax:

```
delete security vpn ipsec logging [ log-modes ]
```

Syntax:

```
show security vpn ipsec logging [ log-modes ]
```

`log-modes` *mode*

Mandatory. Multi-node. The log mode to be used for IPsec log messages. Supported values are as follows:

`all`—Enables all logging options.

`raw`—Shows the raw bytes of messages.

`crypt`—Shows the encryption and decryption of messages.

`parsing`—Shows the structure of input messages.

`emitting`— Shows the structure of output messages.

`control`—Shows the decision-making process of the IKE daemon (Pluto).

`private`—Allows debugging output with private keys.

You can configure multiple log modes, by creating more than one `log-mode` configuration node.

Configuration mode

```
security {
        vpn {
            ipsec {
                logging {
                        log-modes mode
                }
            }
        }
    }
}
```

Use this command to define logging options for IPsec VPN.

When this command is set, the system uses the AT&T Vyatta vRouter's internal VPN logging daemon for IPsec log messages.

The IPsec process generates log messages during operation. You can direct the system to send IPsec log messages to syslog. The result will depend on how the system syslog is configured.

Keep in mind that in the current implementation, the main syslog file reports only messages of severity warning and above, regardless of the severity level configured. If you want to configure a different level of severity for log messages (for example, if you want to see debug messages during troubleshooting), you must configure syslog to send messages into a different file, which you define within syslog.

Configuring log modes is optional. When a log mode is not configured, IPsec log messages consist mostly of IPsec startup and shutdown messages. The log modes allow you to direct the system to inspect the IPsec packets and report the results.

Note that some log modes (for example, *all* and *control*) generate several log messages per packet. Using any of these options may severely degrade system performance.

VPN IPsec log messages use standard syslog levels of severity.

Use the `set` form of this command to specify logging modes for IPsec VPN.

Use the `delete` form of this command to remove the logging configuration.

Use the `show` form of this command to view the logging configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

security vpn ipsec nat-networks allowed-network <ipv4net>

This command is no longer required. Running this command has no effect on the configuration.

Syntax:
`set security vpn ipsec nat-networks allowed-network` *ipv4net* [**`exclude`** *ipv4net-exclude*]

Syntax:
`delete security vpn ipsec nat-networks allowed-network` *ipv4net* [**`exclude`** *ipv4net-exclude*]

Syntax:
`show security vpn ipsec nat-networks allowed-network` [*ipv4net* [**`exclude`**]]

ipv4net
Multi-node. An IPv4 network of private IP addresses that remote hosts behind a NAT device may use.

ipv4net-exclude
Multi-node. An IPv4 network to be excluded from the allowed network range. These are the RFC 1918 ("private") IP addresses being used on the network internal to this VPN gateway.

Configuration mode

```
security {
        vpn {
            ipsec {
                nat-networks {
                    allowed-network ipv4net {
                        exclude ipv4net-exclude
                }
            }
        }
    }
}
```

Use this command to specify RFC 1918 private IP addresses for remote networks that may reside behind a NAT device.

Unlike public IP addresses, private IP addresses may be re-used between sites. That means that private IP address ranges behind a NAT device at the far end of the VPN connection may overlap or be coextensive with private IP addresses on the internal network behind this VPN gateway, causing routing problems. For this reason, you must specify the allowed private network addresses that reside behind a NAT device, excluding internal network addresses.

The following table lists the three blocks of the IP address space that the Internet Assigned Numbers Authority (IANA) has reserved for private internets.

Table 37: IP addresses reserved for private networks

Network	Prefix
10.0.0.0-10.255.255.255	10.0.0.0/8
172.16.0.0-172.31.255.255	172.16.0.0/12
192.168.0.0-192.168.255.255	192.168.0.0/16

Use the `set` form of this command to specify the private network addresses that remote hosts behind a NAT device may use.

Use the `delete` form of this command to remove the configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `show` form of this command to view the configuration.

security vpn ipsec nat-traversal <state>

This command is no longer required. Running this command has no effect on the configuration.

Syntax:
`set security vpn ipsec nat-traversal` *state*

Syntax:
`delete security vpn ipsec nat-traversal`

Syntax:
`show security vpn ipsec nat-traversal`

state
Enables or disables RFC 3947 NAT Traversal. Supported values are as follows:

`enable`—Enables NAT Traversal.

`disable`—Disables NAT Traversal.

Configuration mode

```
security {
        vpn {
            ipsec {
                nat-traversal state
        }
    }
}
```

Use this command to direct the AT&T Vyatta vRouter to propose RFC 3947 NAT Traversal support during IKE negotiation.

Regardless of the setting of this parameter, if the far-end VPN peer requests NAT Traversal, the AT&T Vyatta vRouter will use NAT Traversal.

Use the `set` form of this command to specify whether the system proposes NAT traversal capability.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn ipsec profile <profile-name>

Defines an IPsec profile.

Syntax:
`set security vpn ipsec profile` *profile-name*

Syntax:
`delete security vpn ipsec profile` *profile-name*

Syntax:
`show security vpn ipsec profile` *profile-name*

profile-name
Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

Configuration mode

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
security {
        vpn {
            ipsec {
                profile profile-name
        }
    }
}
```

Use this command to define an IPsec configuration profile to associate with a pre-defined tunnel interface.

Use the `set` form of this command to define an IPsec configuration profile.

Use the `delete` form of this command to remove the profile configuration.

Use the `show` form of this command to view the profile configuration.

security vpn ipsec profile <profile-name> authentication mode <mode>

Defines an IPsec profile authentication mode.

Syntax:

`set security vpn ipsec profile` *profile-name* **`authentication mode`** *mode*

Syntax:

`delete security vpn ipsec profile` *profile-name* **`authentication mode`**

Syntax:

`show security vpn ipsec profile` *profile-name* **`authentication mode`**

profile-name

Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

mode

The authentication method to be used for this profile.

Supported values are as follows:

`pre-shared-secret`—Uses a pre-shared secret for authentication.

`x509`—Uses x509 certificates for authentication.

Configuration mode

```
security {
        vpn {
            ipsec {
                profile profile-name {
                    authentication {
                        mode mode
                }
            }
        }
    }
}
```

Use this command to specify the authentication method to use for an IPsec configuration profile.

Use the `set` form of this command to specify the authentication method to use for an IPsec configuration profile.

Use the `delete` form of this command to remove the authentication mode configuration.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `show` form of this command to view the authentication mode configuration.

security vpn ipsec profile <profile-name> authentication pre-shared-secret <secret>

Specifies the pre-shared secret used to authenticate the VPN peer.

Syntax:
`set security vpn ipsec profile` *profile-name* **`authentication pre-shared-secret`** *secret*

Syntax:
`delete security vpn ipsec profile` *profile-name* **`authentication pre-shared-secret`**

Syntax:
`show security vpn ipsec profile` *profile-name* **`authentication pre-shared-secret`**

profile-name
Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

secret
The pre-shared secret used to authenticate the VPN peer.

Configuration mode

```
security {
        vpn {
            ipsec {
                profile profile-name {
                    authentication {
                        pre-shared-secret secret
                }
            }
        }
    }
}
```

Use this command to specify the pre-shared secret used to authenticate the VPN peer.

Use the `set` form of this command to specify the pre-shared secret to use for an IPsec configuration profile.

Use the `delete` form of this command to remove the pre-shared secret configuration.

Use the `show` form of this command to view the pre-shared secret configuration.

security vpn ipsec profile <profile-name> bind tunnel <tunx>

Specifies the tunnel interface to associate the IPsec profile configuration with.

Syntax:
`set security vpn ipsec profile` *profile-name* **`bind tunnel`** *tunx*

Syntax:
`delete security vpn ipsec profile` *profile-name* **`bind tunnel`**

Syntax:
`show security vpn ipsec profile` *profile-name* **`bind tunnel`**

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

profile-name

Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

tunx

The name of the tunnel interface to associate the IPsec profile configuration with.

Configuration mode

```
security {
        vpn {
            ipsec {
                profile profile-name {
                        bind {
                            tunnel tunx
                }
            }
        }
    }
}
```

Use this command to specify the tunnel interface to associate the IPsec profile configuration with.

Use the `set` form of this command to specify the tunnel interface to associate the IPsec profile configuration with.

Use the `delete` form of this command to remove the bind configuration.

Use the `show` form of this command to view the bind configuration.

security vpn ipsec profile <profile-name> esp-group <name>

Specifies the ESP group to use for the IPsec profile configuration.

Syntax:

`set security vpn ipsec profile` *profile-name* **`esp-group`** *name*

Syntax:

`delete security vpn ipsec profile` *profile-name* **`esp-group`**

Syntax:

`show security vpn ipsec profile` *profile-name* **`esp-group`**

profile-name

Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

name

The name of the ESP group to be used for the IPsec profile configuration. The ESP group must have already been defined using security vpn ipsec esp-group <name> *(page 72)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                profile profile-name {
                        esp-group name
                }
            }
        }
    }
}
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use this command to specify the ESP group to use for the IPsec profile configuration.

Use the `set` form of this command to specify the ESP group to use for the IPsec profile configuration.

Use the `delete` form of this command to remove the ESP group configuration.

Use the `show` form of this command to view the ESP group configuration.

security vpn ipsec profile <profile-name> ike-group <name>

Specifies the IKE group to use for the IPsec profile configuration.

Syntax:

```
set security vpn ipsec profile profile-name ike-group name
```

Syntax:

```
delete security vpn ipsec profile profile-name ike-group
```

Syntax:

```
show security vpn ipsec profile profile-name ike-group
```

profile-name

Multi-node. The name of the IPsec configuration profile.

You can define more than one IPsec profile by creating multiple `profile` configuration nodes.

name

The name of the IKE group to be used for the IPsec profile configuration. The IKE group must have already been defined using security vpn ipsec ike-group <name> *(page 79)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                profile profile-name {
                ike-group name
            }
        }
    }
}
```

Use this command to specify the IKE group to use for the IPsec profile configuration.

Use the `set` form of this command to specify the IKE group to use for the IPsec profile configuration.

Use the `delete` form of this command to remove the IKE group configuration.

Use the `show` form of this command to view the IKE group configuration.

security vpn ipsec site-to-site peer <peer>

Defines a site-to-site connection between the AT&T Vyatta vRouter and another VPN gateway.

Syntax:

```
set security vpn ipsec site-to-site peer peer
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer
```

Syntax:

```
show security vpn ipsec site-to-site peer peer
```

peer

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Multi-node. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

You can define more than one VPN peer by creating multiple `peer` configuration nodes.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer
                }
            }
    }
}
```

Use this command to define a site-to-site connection with another VPN peer.

For peers that have a known IP address or hostname, specify the IP address or hostname (IPv4 networks only) of the peer. For those that have a known authentication ID (prefixed with "@") specify the authentication ID of the peer. For peers where the IP address is unknown—for example, in the scenario where there are multiple "road warrior" peers—specify 0.0.0.0 as the peer, meaning there are multiple possible peers.

Use the `set` form of this command to define a site-to-site connection with another VPN peer.

Use the `delete` form of this command to remove the peer configuration.

Use the `show` form of this command to view the peer configuration.

security vpn ipsec site-to-site peer <peer> authentication id <id>

Specifies local authentication credentials to send to the VPN peer.

Syntax:

`set security vpn ipsec site-to-site peer` *peer* **`authentication id`** *id*

Syntax:

`delete security vpn ipsec site-to-site peer` *peer* **`authentication id`**

Syntax:

`show security vpn ipsec site-to-site peer` *peer* **`authentication id`**

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

id

The local authentication credentials to send to the VPN peer. Can be specified if the `local-address` address for the peer is set to `any` (which means the external address of the interface is dynamic); ignored otherwise. Use the format *@ id* to specify the *id*.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                            id id
                    }
                }
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            }
        }
    }
}
```

Use this command to specify the local authentication credentials to send to the VPN peer.

When using IP address as the *id*, make sure the certificate has Subject Alternative Name with the IP address field. For example:

X509v3 extensions:

X509v3 Subject Alternative Name:

IP Address:192.0.71.1

Use the `set` form of this command to specify the local authentication credentials to send to the VPN peer.

Use the `delete` form of this command to remove the local authentication credentials.

Use the `show` form of this command to view the local authentication credentials.

security vpn ipsec site-to-site peer <peer> authentication mode <mode>

Specifies the authentication method to be used for the connection with the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication mode mode
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication mode
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication mode
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

mode

Specifies the authentication method to be used for this connection. Supported values are as follows:

`pre-shared-secret`—Uses a pre-shared secret for authentication.

`rsa`—Uses an RSA digital signature for authentication.

`x509`—Uses X.509 V.3 certificates for authentication.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                        mode mode
                    }
                }
            }
        }
    }
}
```

Use this command to specify the authentication method to be used for the connection to the VPN peer.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `set` form of this command to specify the authentication method to be used for the connection to the VPN peer.

Use the `delete` form of this command to remove the authentication method configuration.

Use the `show` form of this command to view the authentication method configuration.

security vpn ipsec site-to-site peer <peer> authentication pre-shared-secret <secret>

Specifies the pre-shared secret used to authenticate the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication pre-shared-secret secret
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication pre-shared-secret
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication pre-shared-secret
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

secret

Specifies the pre-shared secret to be used to authenticate the VPN peer.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        authentication {
                            pre-shared-secret secret
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify the pre-shared secret used to authenticate the VPN peer. The pre-shared-secret set here is only valid if the authentication mode is set to pre-shared-secret.

Use the `set` form of this command to specify the pre-shared secret used to authenticate the VPN peer.

Use the `delete` form of this command to remove the pre-shared secret configuration.

Use the `show` form of this command to view the pre-shared secret configuration.

security vpn ipsec site-to-site peer <peer> authentication remote-id <id>

Specifies the authentication credentials of the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication remote-id id
```

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
delete security vpn ipsec site-to-site peer peer authentication remote-id
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication remote-id
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

id

The authentication credentials of the remote VPN peer. The id can be an IP address, a hostname (IPv4 networks only), an authentication ID in the form @ *id* , or, for X.509, a string specifying the "distinguished name" of the certificate for the remote end of the tunnel.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                        remote-id id
                    }
                }
            }
        }
    }
}
```

Use this command to specify the authentication credentials of the VPN peer. The `remote-id` is an override to the default authentication - the peer IP address. The remote peer uses an authentication ID for authentication when its IP address is dynamic or it identifies itself with a different IP address or hostname (IPv4 networks only). An example of this is when the remote peer is behind a NAT device.

Another case where *remote-id* is required is for X.509 authentication. In this case, a string specifying the "distinguished name" of the certificate for the remote end of the tunnel is used. For example, the string "C=US, ST=CA, O=ABC Company, CN=test, emailAddress=root@abc.com" specifies the information included in the X.509 certificate for the peer.

When using IP address as the *id*, make sure the certificate has Subject Alternative Name with the IP address field. For example:

X509v3 extensions:

X509v3 Subject Alternative Name:

IP Address:192.0.71.1

Use the `set` form of this command to specify the authentication credentials of the VPN peer.

Use the `delete` form of this command to remove the remote peer authentication credentials.

Use the `show` form of this command to view the remote peer authentication credentials.

security vpn ipsec site-to-site peer <peer> authentication rsa-key-name <name>

Specifies the name of the digital signature used to authenticate the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication rsa-key-name name
```

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
delete security vpn ipsec site-to-site peer peer authentication rsa-key-name
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication rsa-key-name
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

name

The name of the digital signature used to authenticate the VPN peer.

To record an RSA digital signature for a VPN peer, use the `set` form of security vpn rsa-keys *(page 114)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        authentication {
                            rsa-key-name name
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify the name of the digital signature to use to authenticate the VPN peer. The `rsa-key-name` set here is only valid if the `authentication mode` is set to `rsa`.

Use the `set` form of this command to specify the name of the digital signature to use to authenticate the VPN peer.

Use the `delete` form of this command to remove the name of the digital signature.

Use the `show` form of this command to view the name of the digital signature.

security vpn ipsec site-to-site peer <peer> authentication x509 ca-cert-file <file-name>

Specifies the name of an X.509 Certificate Authority (CA) certificate file for IPsec authentication of the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication x509 ca-cert-file file-name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication x509 ca-cert-file
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication x509 ca-cert-file
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

file-name

The certificate file name. This parameter is mandatory if `authentication mode` is `x509`.

Configuration mode

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                        x509 {
                            ca-cert-file file-name
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify the name of an X.509 Certificate Authority (CA) certificate file. The X.509 CA certificate is used for IPsec authentication for the VPN peer.

Certificate and key files are assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the CA certificate file.

Use the `delete` form of this command to remove the name of the CA certificate file.

Use the `show` form of this command to display CA certificate file configuration.

security vpn ipsec site-to-site peer <peer> authentication x509 cert-file <file-name>

Specifies the name of the VPN server's certificate file for IPsec authentication of the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication x509 cert-file file-name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication x509 cert-file
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication x509 cert-file
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

file-name

The name of the VPN server's certificate file. This parameter is mandatory if `authentication mode` is `x509`.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                        x509 {
                            cert-file file-name
                        }
                    }
                }
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            }
        }
    }
}
```

Use this command to specify the name to the VPN server's certificate file. The VPN server's certificate certifies the identity of the VPN server.

Certificate and key files are assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the VPN server's certificate file.

Use the `delete` form of this command to remove the name of the VPN server's certificate file.

Use the `show` form of this command to display VPN server certificate file configuration.

security vpn ipsec site-to-site peer <peer> authentication x509 crl-file <file-name>

Specifies the name of an X.509 Certificate Revocation List (CRL) file for IPsec authentication of the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication x509 crl-file file-name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication x509 crl-file
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication x509 crl-file
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

file-name

The name of the CRL file.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    authentication {
                        x509 {
                            crl-file file-name
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify the name of a Certificate Revocation List (CRL) file.

A CRL is a time-stamped signed data structure issued by the Certificate Authority (CA) identifying revoked certificates. When the remote user attempts to log on to the system, the system checks both the remote user's certificate signature and also the CRL to make sure that the remote user's certificate serial number is not on the CRL. If it is, the login attempt will be refused.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the name of the CRL file.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `delete` form of this command to remove the name of the CRL file.

Use the `show` form of this command to display CRL file configuration.

security vpn ipsec site-to-site peer <peer> authentication x509 key file <file-name>

Specifies the name of the VPN server's private key file for IPsec authentication of the VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer authentication x509 key file file-name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer authentication x509 key file
```

Syntax:

```
show security vpn ipsec site-to-site peer peer authentication x509 key file
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

file-name

The name of the VPN server's private key file. This parameter is mandatory if `authentication mode` is `x509`.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        authentication {
                            x509 {
                                key {
                                    file file-name
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify the name of the VPN server's private key file. The VPN server's private key certifies the identity of the VPN server.

The file is assumed to be in `/config/auth` unless an absolute path is specified.

Use the `set` form of this command to specify the location of the VPN server's private key file.

Use the `delete` form of this command to remove the location of the VPN server's private key file.

Use the `show` form of this command to display VPN server private key file configuration.

security vpn ipsec site-to-site peer <peer> authentication x509 key password <password>

Specifies the password that protects the VPN server's private key.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Syntax:
`set security vpn l2tp remote-access ipsec-settings authentication x509 key password` *password*

Syntax:
`delete security vpn l2tp remote-access ipsec-settings authentication x509 key password`

Syntax:
`show security vpn l2tp remote-access ipsec-settings authentication x509 key password`

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

password
The password protecting the VPN server's private key file.

Configuration mode

```
security {
        vpn {
            l2tp {
                remote-access {
                    ipsec-settings {
                        authentication {
                            x509 {
                                key {
                                    password password
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify a password that protects the VPN server's private key.

Use the `set` form of this command to specify the password for the VPN server's private key.

Use the `delete` form of this command to remove the password for the VPN server's private key.

Use the `show` form of this command to display VPN servers private key password configuration.

security vpn ipsec site-to-site peer <peer> connection-type

Specifies the type of peer connection.

Syntax:
`set security vpn ipsec site-to-site peer` *peer* **`connection-type`** { **`initiate`** | **`respond`** }

Syntax:
`delete security vpn ipsec site-to-site peer` *peer* **`connection-type`**

Syntax:
`show security vpn ipsec site-to-site peer` *peer* **`connection-type`**

A connection to the remote peer is initiated by the local peer unless the remote peer is set to 0.0.0.0, @id, or any.

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

`initiate`

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Indicates that the connection to the remote peer will be initiated by the local peer unless the remote peer is set to `0.0.0.0`, `@id`, or `any`.This is the default behavior.

`respond`

Indicates that the local peer will not initiate a connection to the remote peer, but will respond to connections initiated by the remote peer.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer{
                        connection-type [initiate|respond]
                }
            }
        }
    }
}
```

Use this command to specify the type of peer connection.

Use the `set` form of this command to specify the type of peer connection.

Use the `delete` form of this command to return the connection type to its default behavior.

Use the `show` form of this command to view connection type configuration.

security vpn ipsec site-to-site peer <peer> default-esp-group <name>

Specifies a default ESP configuration to use for all tunnels to the peer.

Syntax:

`set security vpn ipsec site-to-site peer` *peer* **`default-esp-group`** *name*

Syntax:

`delete security vpn ipsec site-to-site peer` *peer* **`default-esp-group`**

Syntax:

`show security vpn ipsec site-to-site peer` *peer* **`default-esp-group`**

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

name

Specifies the named ESP configuration (ESP group) to be used by default for all connections. The ESP group must have already been defined, using security vpn ipsec esp-group <name> *(page 72)*.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    default-esp-group name
                }
            }
        }
    }
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
}
```

Use this command to specify a default ESP configuration to use for all tunnels to the peer. This setting can be overridden on a per-tunnel basis by using security vpn ipsec site-to-site peer <peer> tunnel <tunnel> esp-group <name> *(page 109)*.

Use the `set` form of this command to specify an ESP configuration to use for all connections by default.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn ipsec site-to-site peer <peer> description <desc>

Specifies a description for a VPN peer.

Syntax:

```
set security vpn ipsec site-to-site peer peer description desc
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer description
```

Syntax:

```
show security vpn ipsec site-to-site peer peer description
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

desc

A brief description for the VPN peer. If the description contains space characters, it must be enclosed in double quotes.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    description desc
                }
            }
        }
    }
}
```

Use this command to specify a description for the VPN peer.

Use the `set` form of this command to specify the description for the VPN peer.

Use the `delete` form of this command to remove the description for the VPN peer.

Use the `show` form of this command to view the description for the VPN peer.

security vpn ipsec site-to-site peer <peer> dhcp-interface <interface>

Specifies a DHCP client interface to use for the connection.

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
set security vpn ipsec site-to-site peer peer dhcp-interface interface
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer dhcp-interface
```

Syntax:

```
show security vpn ipsec site-to-site peer peer dhcp-interface
```

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

interface
The interface to use for the VPN connection (e.g. dp0p1p1). Note that the interface must be configured as a DHCP client.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer{
                        dhcp-interface interface
                }
            }
        }
    }
}
```

Use this command to specify a DHCP client interface to use for the connection. The connection will be automatically restarted if the IP address changes.

Note: This option cannot be used if security vpn ipsec site-to-site peer <peer> local-address <address> *(page 105)* is also set.

Use the `set` form of this command to specify a DHCP interface to use for the connection.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn ipsec site-to-site peer <peer> ike-group <group>

Specifies the named IKE configuration to be used for a peer connection.

Syntax:

```
set security vpn ipsec site-to-site peer peer ike-group group
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer ike-group
```

Syntax:

```
show security vpn ipsec site-to-site peer peer ike-group
```

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

group

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Mandatory. The named IKE configuration to be used for this connection. The IKE configuration must have already been defined, using security vpn ipsec ike-group <name> *(page 79)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer{
                        ike-group group
                }
            }
        }
    }
}
```

Use this command to specify a named IKE configuration (an IKE group) to be used for an IPsec peer connection.

Use the `set` form of this command to specify the IKE group.

Use the `delete` form of this command to remove IKE group configuration.

Use the `show` form of this command to view IKE group configuration.

security vpn ipsec site-to-site peer <peer> local-address <address>

Specifies the local IP address to be used as the source IP for packets destined for the remote peer.

Syntax:
`set security vpn ipsec site-to-site peer` *peer* **`local-address`** *address*

Syntax:
`delete security vpn ipsec site-to-site peer` *peer* **`local-address`**

Syntax:
`show security vpn ipsec site-to-site peer` *peer* **`local-address`**

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

address
Mandatory. The local IPv4 or IPv6 address to be used as the source IP for packets destined for the remote peer. If the physical interface has a dynamic IPv4 address, then the `local-address` must be set to `any`.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    local-address address
                }
            }
        }
    }
}
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use this command to specify the local IP address to be used as the source IP address for packets destined for the remote peer.

The address type must match that of the peer. For example, if the peer address is IPv4, then the local-address must also be IPv4.

The local-address must be set to any in cases where the local external IPv4 address is dynamic or unknown; for example, when the address is supplied by a PPPoE connection or DHCP server. If you use an address of *any*, you must set the local authentication ID using security vpn ipsec site-to-site peer <peer> authentication id <id> *(page 93)*.

When the *local-address* is set to *any*, the default route is used and the connection will not be automatically updated if the IP address changes (a reset vpn ipsec-peer <peer> *(page 70)* is required when the IP address changes). A better alternative for use with DHCP client interfaces is security vpn ipsec site-to-site peer <peer> dhcp-interface <interface> *(page 103)*.

> **Note:** The *local-address* option cannot be used if security vpn ipsec site-to-site peer <peer> dhcp-interface <interface> *(page 103)* is also set.

If the VPN tunnel is being clustered for high availability, the local-address attribute must be the cluster IP address, not the IP address configured for the physical interface. Otherwise, the local-address must be the address configured for the physical interface.

Use the `set` form of this command to specify the local IP address to be used as the source IP for packets destined for the remote peer.

Use the `delete` form of this command to remove local IP address configuration.

Use the `show` form of this command to view local IP address configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-nat-networks <state>

This command is no longer required. Running this command has no effect on the configuration.

Syntax:

```
set security vpn ipsec site-to-site peer peer tunnel tunnel allow-nat-networks state
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer tunnel tunnel allow-nat-networks
```

Syntax:

```
show security vpn ipsec site-to-site peer peer tunnel tunnel allow-nat-networks
```

A connection to a private network is not allowed (disabled).

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple tunnel configuration nodes within the peer configuration.

state

Allows connection to a defined network of private IP addresses on a per-tunnel basis. Supported values are as follows:

`enable`—Allow connection to the private network.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

`disable`—Do not allow connection to the private network.

This option is mandatory if the `allow-public-networks` is enabled; optional otherwise. The allowed private network must be defined by using security vpn ipsec nat-networks allowed-network <ipv4net> *(page 87)*.

If this option is enabled, any value set for the `remote prefix` option is ignored.

Configuration mode

```
security {
        vpn {
            ipsec {
            site-to-site {
                peer peer {
                    tunnel tunnel {
                        allow-nat-networks state
                    }
                }
            }
        }
    }
}
```

Use this command to specify whether or not a connection to a private network is allowed.

Use the `set` form of this command to specify whether or not a connection to a private network is allowed.

Use the `delete` form of this command to remove the configuration and return it to the default behavior.

Use the `show` form of this command to view the configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> allow-public-networks <state>

This command is no longer required. Running this command has no effect on the configuration.

Syntax:
`set security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`allow-public-networks`** *state*

Syntax:
`delete security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`allow-public-networks`**

Syntax:
`show security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`allow-public-networks`**

A connection to a public network is not allowed (disabled).

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

state

Allows connections to public IP addresses on a per-tunnel basis. Supported values are as follows:

`enable`—Allows connections to public networks.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

`disable`—Does not allow connections to public networks.

This option requires that the `allow-nat-networks` option be enabled, and that allowed NAT networks be specified by using security vpn ipsec nat-networks allowed-network <ipv4net> *(page 87)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        tunnel tunnel {
                            allow-public-networks state
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to specify whether or not a connection to a public network is allowed.

Use the `set` form of this command to specify whether or not a connection to a public network is allowed.

Use the `delete` form of this command to remove the configuration and return it to the default behavior.

Use the `show` form of this command to view the configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> disable

Disables a VPN tunnel without discarding configuration.

Syntax:
`set security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`disable`**

Syntax:
`delete security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`disable`**

Syntax:
`show security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel*

The VPN tunnel configuration is enabled.

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
                    peer peer {
                        tunnel tunnel {
                            disable
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to disable the VPN tunnel without discarding configuration. The tunnel can then be re-enabled at a later time without the need to redefine the configuration.

Use the `set` form of this command to disable the tunnel.

Use the `delete` form of this command to enable the tunnel.

Use the `show` form of this command to view the VPN tunnel configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> esp-group <name>

Specifies an ESP configuration to use for this tunnel.

Syntax:

```
set security vpn ipsec site-to-site peer peer tunnel tunnel esp-group name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer tunnel tunnel esp-group
```

Syntax:

```
show security vpn ipsec site-to-site peer peer tunnel tunnel esp-group
```

The ESP group specified by security vpn ipsec site-to-site peer <peer> default-esp-group <name> *(page 102)* will be used.

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

name

Specifies the named ESP configuration (ESP group) to be used for this connection. The ESP group must have already been defined, using security vpn ipsec esp-group <name> *(page 72)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        tunnel tunnel {
                            esp-group name
                        }
                    }
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            }
        }
    }
}
```

Use this command to specify an ESP configuration to use for this connection. It will override the ESP group specified by security vpn ipsec site-to-site peer <peer> default-esp-group <name> *(page 102)* which will be used by default.

Use the `set` form of this command to specify an ESP configuration to use for this connection.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> local

Defines local configuration options for the IPsec tunnel.

Syntax:

```
set security vpn ipsec site-to-site peer peer tunnel tunnel local [ port port | prefix prefix ]
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer tunnel tunnel local [ port | prefix ]
```

Syntax:

```
show security vpn ipsec site-to-site peer peer tunnel tunnel local [ port | prefix ]
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

port

Applicable only when the protocol is TCP or UDP. The local port to match. Only traffic from or to this port on the local subnet will travel through this tunnel. Supported formats are as follows:

port-name—Matches the name of an IP service; for example, `http`. You can specify any service name in the file `/etc/services`.

port-num—Matches a port number. The numbers range from 1 through 65535.

The default is `all`.

prefix

Mandatory. The local subnet to which the remote VPN gateway will have access. For IPv4, the format is an IPv4 network address, where network address `0.0.0.0/0` means any local subnet. For IPv6, the format is an IPv6 network address, where network address `0::0/0` means any local subnet.

Note: The address type (IPv4 or IPv6) must match that of the `remote prefix`.

The default is the subnet the `local-address` is on.

Configuration mode

```
security {
        vpn {
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            ipsec {
                site-to-site {
                    peer peer {
                        tunnel tunnel {
                            local {
                                port port
                                prefix prefix
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to define local configuration options for the IPsec tunnel.

Use the `set` form of this command to set the local tunnel characteristics.

Use the `delete` form of this command to remove local tunnel configuration.

Use the `show` form of this command to view local tunnel configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> protocol <protocol>

Specifies the protocol to match for traffic to enter the tunnel.

Syntax:
`set security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`protocol`** *protocol*

Syntax:
`delete security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`protocol`**

Syntax:
`show security vpn ipsec site-to-site peer` *peer* **`tunnel`** *tunnel* **`protocol`**

The default is `all`.

peer
Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel
Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

protocol
Any protocol literals or numbers listed in the file `/etc/protocols` can be used. The keywords `tcp_udp` (for both TCP and UDP) and `all` (for all protocols) are also supported.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        tunnel tunnel {
                            protocol protocol
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
                    }
                }
            }
        }
    }
}
```

Use this command to specify the protocol to match for traffic to enter the tunnel.

Use the `set` form of this command to specify the protocol.

Use the `delete` form of this command to remove protocol configuration.

Use the `show` form of this command to view protocol configuration.

security vpn ipsec site-to-site peer <peer> tunnel <tunnel> remote

Defines remote configuration options for the IPsec tunnel.

Syntax:

```
set security vpn ipsec site-to-site peer peer tunnel tunnel remote [ port port | prefix prefix ]
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer tunnel tunnel remote [ port | prefix ]
```

Syntax:

```
show security vpn ipsec site-to-site peer peer tunnel tunnel remote [ port | prefix ]
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address, an IPv6 address, a hostname (IPv4 networks only), an authentication ID, or `0.0.0.0`.

tunnel

Mandatory. Multi-node. An integer that uniquely identifies this tunnel configuration for this peer VPN gateway. Each tunnel corresponds to a distinct connection configuration. The numbers range from 0 through 4294967295.

A given VPN peer may have more than one tunnel configuration, but each peer must have at least one. To define more than one tunnel configuration for a peer, create multiple `tunnel` configuration nodes within the peer configuration.

port

Applicable only when the protocol is TCP or UDP. The remote port to match. Only traffic from or to this port on the remote subnet will travel through this tunnel. Supported formats are as follows:

port-name—Matches the name of an IP service; for example, `http`. You can specify any service name in the file `/etc/services`.

port-num—Matches a port number. The numbers range from 1through 65535.

The default is `all`.

prefix

Mandatory. The remote subnet behind the remote VPN gateway, to which the AT&T Vyatta vRouter will have access. For IPv4, the format is an IPv4 network address, where network address `0.0.0.0/0` means any subnet behind the remote VPN gateway. For IPv6, the format is an IPv6 network address, where network address `0::0/0` means any local subnet.

Note: The address type (IPv4 or IPv6) must match that of the `local prefix`.

This option is ignored if `allowed-nat-networks` is enabled.

The default is the subnet of the peer.

Configuration mode

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        tunnel tunnel {
                            remote {
                                port port
                                prefix prefix
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Use this command to define local configuration options for the IPsec tunnel.

Use the `set` form of this command to set the local tunnel characteristics.

Use the `delete` form of this command to remove local tunnel configuration.

Use the `show` form of this command to view local tunnel configuration.

security vpn ipsec site-to-site peer <peer> vti bind <vtix>

Binds the IPsec site-to-site VPN tunnel to a virtual tunnel interface.

Syntax:

`set security vpn ipsec site-to-site peer` *peer* **`vti bind`** *vtix*

Syntax:

`delete security vpn ipsec site-to-site peer` *peer* **`vti bind`**

Syntax:

`show security vpn ipsec site-to-site peer` *peer* **`vti bind`**

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address.

vtix

Mandatory. The virtual tunnel interface to bind the IPsec site-to-site VPN tunnel to. The virtual tunnel interface must have already been defined, using interfaces vti <vtix> *(page 125)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        vti {
                            bind vtix
                       }
                    }
                }
            }
        }
    }
}
```

Use this command to bind an IPsec site-to-site VPN tunnel to a virtual tunnel interface.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use the `set` form of this command to bind the IPsec site-to-site VPN tunnel to the specified virtual tunnel interface.

Use the `delete` form of this command to remove the bind to the virtual tunnel interface.

Use the `show` form of this command to view the bind configuration.

security vpn ipsec site-to-site peer <peer> vti esp-group <name>

Specifies the ESP configuration to use for the IPsec site-to-site VPN tunnel.

Syntax:

```
set security vpn ipsec site-to-site peer peer vti esp-group name
```

Syntax:

```
delete security vpn ipsec site-to-site peer peer vti esp-group
```

Syntax:

```
show security vpn ipsec site-to-site peer peer vti esp-group
```

peer

Mandatory. The address of the far-end VPN gateway. The format is an IPv4 address.

name

Mandatory. Specifies the named ESP configuration (ESP group) to be used for the connection. The ESP group must have already been defined, using security vpn ipsec esp-group <name> *(page 72)*.

Configuration mode

```
security {
        vpn {
            ipsec {
                site-to-site {
                    peer peer {
                        vti {
                            esp-group name
                    }
                }
            }
        }
    }
}
```

Use this command to specify an ESP configuration to use for this connection. It will override the ESP group specified by security vpn ipsec site-to-site peer <peer> default-esp-group <name> *(page 102)* which will be used by default.

Use the `set` form of this command to specify an ESP configuration to use for this VPN tunnel.

Use the `delete` form of this command to remove the configuration.

Use the `show` form of this command to view the configuration.

security vpn rsa-keys

Records RSA keys for the local host.

Syntax:

```
set security vpn rsa-keys [ local-key file file-name | rsa-key-name name rsa-key key ]
```

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
delete security vpn rsa-keys local-key file [ local-key file | rsa-key-name [ name rsa-key ] ]
```

Syntax:

```
show security vpn rsa-keys local-key file [ local-key file | rsa-key-name [ name rsa-key ] ]
```

file-name

Specifies the name and location of the file containing the RSA digital signature of the local host (both public key and private key). By default, the RSA digital signature for the local host is recorded in `/config/ipsec.d/rsa-keys/`.

name

A mnemonic name for the remote key. This is the name you refer to when configuring RSA configuration in site-to-site connections.

key

The RSA public key data for the remote peer.

Configuration mode

```
security {
        vpn {
            rsa-keys {
                local-key {
                    file file-name
        }
            rsa-key-name name {
                rsa-key key
        }
    }
}
```

Use this command to view or change the location of the file containing RSA key information for the local host, or to record an RSA public key for a remote host.

The RSA digital signature for the local host can be generated using generate vpn rsa-key *(page 68)* in operational mode. Once generated, the key is stored at the location specified by the *local-key rsa-key-name* option. By default, this is the *localhost.key* file in the `/config/ipsec.d/rsa-keys/` directory.

You must also enter the public key of the remote peer, as the *rsa-key-namenamersa-key* attribute. Digital signatures are lengthy, so to configure this value copy it as text into your clipboard and paste it into the configuration. Once recorded with a mnemonic name, you can refer to the RSA key by the name in site-to-site connection configurations.

Use the `set` form of this command to set RSA key configuration.

Use the `delete` form of this command to remove RSA key configuration.

Use the `show` form of this command to view RSA key configuration.

show vpn debug

Provides trace-level information about IPsec VPN.

Syntax:

```
show vpn debug [ detail | peer peer [ tunnel tunnel ] ]
```

detail

Provides extra verbose output at the trace level.

peer

Shows trace-level information for the specified VPN peer. The format is the IPv4 or IPv6 address of the peer.

tunnel

Shows trace-level information for the specified tunnel to the specified peer. The *tunnel* argument is an integer that uniquely identifies the tunnel to the specified peer. The numbers range from 0 through 4294967295.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Operational mode

Use this command to view trace-level messages for IPsec VPN.

This command is useful for troubleshooting and diagnostic situations.

The following example shows the output of the `show vpn debug` command.

```
vyatta@vyatta:~$ show vpn debug
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.4-1-amd64-vyatta, x86_64):
  uptime: 2 minutes, since Apr 06 10:24:47 2016
  malloc: sbrk 1204224, mmap 0, used 304432, free 899792
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes rc2 sha1 sha2 md5 random nonce x509 revocation constraints
 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac
 gcm attr kernel-netlink resolve socket-default connmark stroke vici updown
Listening IP addresses:
  10.18.170.212
Connections:
Security Associations (0 up, 0 connecting):
  none
vyatta@vyatta:~$
```

The following example shows the output of the `show vpn debug detail` command.

```
vyatta@vyatta:~$ show vpn debug detail
IPsec version
Linux strongSwan U5.3.5/K4.4.4-1-amd64-vyatta
Institute for Internet Technologies and Applications
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
IPsec working directory
/usr/lib/ipsec
IPsec status
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.4-1-amd64-vyatta, x86_64):
  uptime: 5 minutes, since Apr 06 10:24:47 2016
  malloc: sbrk 1744896, mmap 0, used 313328, free 1431568
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes rc2 sha1 sha2 md5 random nonce x509 revocation constraints
 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac
 gcm attr kernel-netlink resolve socket-default connmark stroke vici updown
Listening IP addresses:
  10.18.170.212
Connections:
Security Associations (0 up, 0 connecting):
  none
:...skipping...
IPsec version
Linux strongSwan U5.3.5/K4.4.4-1-amd64-vyatta
Institute for Internet Technologies and Applications
University of Applied Sciences Rapperswil, Switzerland
See 'ipsec --copyright' for copyright information.
IPsec working directory
/usr/lib/ipsec
IPsec status
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.4-1-amd64-vyatta, x86_64):
  uptime: 5 minutes, since Apr 06 10:24:47 2016
  malloc: sbrk 1744896, mmap 0, used 313328, free 1431568
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes rc2 sha1 sha2 md5 random nonce x509 revocation constraints
 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac
 gcm attr kernel-netlink resolve socket-default connmark stroke vici updown
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
--More--
```

show vpn ike rsa-keys

Displays RSA public keys recorded in the system.

Syntax:

```
show vpn ike rsa-keys
```

Operational mode

Use this command to display the public portion of all RSA digital signatures recorded on the system.

This will include the public portion of the RSA digital signature of the local host (the private portion will not be displayed), plus the public key configured for any VPN peer.

The following example shows output of the `show vpn ike rsa-keys` command, which displays the RSA digital signatures stored on router WEST. In this example:

- The public portion of the key for the local host is shown, but the private portion of the local key remains hidden in the RSA keys file.
- The RSA public key recorded for the VPN peer EAST is also shown.

```
vyatta@WEST> show vpn ike rsa-keys
Local public key:

0sMIIBMjANBgkqhkiG9w0BAQEFAAOCAR8AMIIBGgKCARMAqz26wqVVbstD/
ZBjdyXxfqxziunwR2PDX9n/8ee5+uri1mo4RBcTVCzZ
+r46Pc4UnMZG1TVajkdrPjUht45ycYuAIItxAh5v4ltY3FUOpRRsXu+JLtYjuZNX
+ZsGQsSoyiDaJMaJWj4nUxTleW0YhZtDS+TtA+CEs471y6ZkKJM36btGBqBypBBOhHBIEiFWxntKtzRilAnbfX
+ZngK2HBIuqXltYeVbDMuMKwJ9LGJCUGhaOn01QXy+0k1MA/SW2QJ5ea+qf1K2qXk/
PDNf0YDtOH1HnJdL6hMNDM46d6A1uYk83wRUsBXgCBdkRADYYCszahytc/1VtafI/fzn4S7/Cf6F4n9syegGm
+xUVKtpywIBAw==

================================================================================
Peer: 10.10.1.2  (ekey)

0sMIIBMjANBgkqhkiG9w0BAQEFAAOCAR8AMIIBGgKCARMAuQgX2ZPOsI9x33p6U7NEqSVD77pFySZlEQHzwHvEoyqZDlGMEbmNaquemP5JMrTc
+4quGAI3b6odkuLexhtZEZRHuFUmV0j3ceyj6Zw06lJgGtLvxTxBPG3QYHwkNANNN
+dT2w5y/5cjhPG4BZAXA8FulGMM0lv89ebPIDsBR8UA7h4qJU58YTbd3myyxuS+PLW96vVPHBv9/
BjuWciXjgYCOuBPVZyfAH8D9tp1k1

vyatta@WEST>
```

show vpn ike sa

Provides information about all currently active IKE (ISAKMP) security associations.

Syntax:

```
show vpn ike sa [ nat-traversal | peer peer ]
```

nat-traversal
: Displays all the IKE SAs that are using RFC 3947 NAT Traversal.

peer
: Shows IKE SA information for the specified VPN peer. The format is the IPv4 or IPv6 address of the peer.

  There will be at most one IKE SA per peer (except possibly during re-key negotiation).

Operational mode

Use this command to display information about IKE security associations (SAs).

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

The following example shows the output of the `show vpn ike sa` command.

```
vyatta@rtr1:~$ show vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
192.0.3.33                              192.0.3.1

    State    Encrypt       Hash    D-H Grp  A-Time  L-Time IKEv
    -----  ------------  --------  -------  ------  ------ ----
    up     aes256        sha1      14       0       86400   2
vyatta@rtr1:~$
```

show vpn ike secrets

Displays configured pre-shared secrets.

Syntax:

```
show vpn ike secrets
```

Operational mode

Use this command to display information about pre-shared secrets recorded in the system.

The following example shows the output of the `show vpn ike secrets` command.

```
vyatta@WEST> show vpn ike secrets
Local IP/ID                             Peer IP/ID
----------                              ----------
192.168.1.2                             1.1.1.2
N/A                                     192.168.2.2
    Secret: "secret"
Local IP/ID                             Peer IP/ID
-----------                             ----------
192.168.1.2                             192.168.2.2
N/A                                     192.168.2.2
    Secret: "secret"
```

show vpn ike status

Displays summary information about the IKE process.

Syntax:

```
show vpn ike status
```

Operational mode

Use this command to see the status of the IKE process.

The following example shows the output of the `show vpn ike status` command.

```
vyatta@west> show vpn ike status
IKE Process Running

PID: 5832

vyatta@west>
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

show vpn ipsec policy

Displays information about the configured IPsec policies.

Syntax:

```
show vpn ipsec policy
```

Operational mode

Use this command to display information about the configured IPsec policies.

The following example shows the output of the `show vpn ipsec policy` command.

```
vyatta@R1# show vpn ipsec policy
src 192.168.50.0/24 dst 192.168.70.0/24
        dir fwd priority 2883 ptype main
        tmpl src 192.0.3.1 dst 192.0.3.33
                proto esp reqid 1 mode tunnel
src 192.168.50.0/24 dst 192.168.70.0/24
        dir in priority 2883 ptype main
        tmpl src 192.0.3.1 dst 192.0.3.33
                proto esp reqid 1 mode tunnel
src 192.168.70.0/24 dst 192.168.50.0/24
        dir out priority 2883 ptype main
        tmpl src 192.0.3.33 dst 192.0.3.1
                proto esp reqid 1 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0 ptype main
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0 ptype main
src ::/0 dst ::/0
        socket in priority 0 ptype main
src ::/0 dst ::/0
        socket out priority 0 ptype main
src ::/0 dst ::/0
        socket in priority 0 ptype main
src ::/0 dst ::/0
        socket out priority 0 ptype main
vyatta@R1#
```

show vpn ipsec sa

Provides information about active IPsec security associations.

Syntax:

```
show vpn ipsec sa [ peer peer [ tunnel tunnel ] ]
```

peer

Shows active IPsec security associations for the specified VPN peer. The format is the IPv4 or IPv6 address of the peer.

tunnel

Shows active IPsec security associations for the specified tunnel to the specified peer. The *tunnel* argument is an integer that uniquely identifies the tunnel to the specified peer. The numbers range from 0 through 4294967295.

Operational mode

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Use this command to display information about remote VPN peers and IPsec security associations (SAs) currently in effect.

The following example shows the output of the `show vpn ipsec sa` command.

```
vyatta@rtr1:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
190.160.3.2                             190.160.2.1

    Tunnel  State  Bytes Out/In   Encrypt       Hash      DH A-Time  L-Time
    ------  -----  -------------  ------------  --------  -- ------  ------
    1       up     0.0/0.0        aes256        md5       5  6       1800
```

The following example shows the output of the `show vpn ipsec sa peer` command.

```
vyatta@rtr1:~$ show vpn ipsec sa peer 192.168.3.3
Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.3.3                             192.168.2.1

    Tunnel  State  Bytes Out/In     Encrypt       Hash    DH   A-Time  L-Time
    ------  -----  -------------  ------------  --------  --   ------  -----
    1       up     0.0/0.0        aes256        md5       5    61      1800
```

The following example shows the output of the `show vpn ipsec sa peer tunnel` command.

```
vyatta@rtr1:~$ show vpn ipsec sa peer 192.168.3.3 tunnel 1
Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.3.3                             192.168.2.1

    Tunnel  State  Bytes Out/In     Encrypt       Hash    DH  A-Time  L-Time
    ------  -----  -------------  ------------  --------  --  ------  -----
    1       up     0.0/0.0        aes256        md5       5   96      1800
```

show vpn ipsec sa detail

Provides detailed information about active IPsec security associations.

Syntax:

`show vpn ipsec sa` **`detail`** [**`peer`** *peer* [**`tunnel`** *tunnel*]]

peer

The peer to display information about.

tunnel

The tunnel to display information about. The number ranges from 0 through 4294967295.

Operational mode

Use this command to display detailed information about remote VPN peers and IPsec security associations (SAs) currently in effect.

The following example shows the output of the `show vpn ipsec sa detail` command.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
vyatta@WEST> show vpn ipsec sa detail
----------------------------------------------------------------------
Peer IP:                190.160.3.2
Peer ID:                190.160.3.2
Local IP:               190.160.2.1
Local ID:               190.160.2.1
NAT Traversal:          no
NAT Source Port:        500
NAT Dest Port:          500

    Tunnel 1:
        State:                  up
        Inbound SPI:            c76eac7d
        Outbound SPI:           c29b9e88
        Encryption:             aes256
        Hash:                   md5
        DH Group:               5

        Local Net:              190.160.1.0/24
        Local Protocol:         all
        Local Port:             all

        Remote Net:             190.160.4.0/24
        Remote Protocol:        all
        Remote Port:            all

        Inbound Bytes:          0.0
        Outbound Bytes:         0.0

        Inbound Blocked:        no
        Outbound Blocked:       no

        Active Time (s):        6
        Lifetime (s):           1800
vyatta@WEST>
```

The following example shows the output of the `show vpn ipsec sa detail peer` *peer* command for an x509 tunnel (note the “CA” information).

```
vyatta@WEST> show vpn ipsec sa detail peer  190.160.3.2
----------------------------------------------------------------------
Peer IP:                190.160.3.2
Peer ID:                190.160.3.2
Local IP:               190.160.3.1
Local ID:               190.160.3.1
NAT Traversal:          no
NAT Source Port:        500
NAT Dest Port:          500

    Tunnel 1:
        State:                  up
        Inbound SPI:            cadcb2d6
        Outbound SPI:           c4d66a6c
        Encryption:             aes256
        Hash:                   md5
        DH Group:               5

        Local Net:              192.85.1.0/24
        Local Protocol:         all
        Local Port:             all
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
        Remote Net:             193.85.1.0/24
        Remote Protocol:        all
        Remote Port:            all

        Inbound Bytes:          0.0
        Outbound Bytes:         0.0

        Inbound Blocked:        no
        Outbound Blocked:       no

        Active Time (s):        121
        Lifetime (s):           1800
```

show vpn ipsec sa nat-traversal

Provides information about all active IPsec security associations that are using NAT Traversal.

Syntax:

```
show vpn ipsec sa nat-traversal
```

Operational mode

Use this command to display information about all active IPsec security associations that are using RFC 3947 NAT Traversal.

show vpn ipsec sa statistics

Display statistics information about active IPsec security associations.

Syntax:

```
show vpn ipsec sa statistics [ peer peer [ tunnel tunnel ] ]
```

peer

The peer to display information about.

tunnel

The tunnel to display information about. The number ranges from 0 through 4294967295.

Operational mode

Use this command to see statistics for active IPsec security associations.

The following example shows the output of the `show vpn ipsec sa statistics` command.

```
vyatta@WEST> show vpn ipsec sa statistics

Peer ID / IP                            Local ID / IP
------------                            -------------
1.1.1.2                                 192.168.1.2


  Tun# Dir Source Network               Destination Network          Bytes
  ---- --- --------------               -------------------          -----
  1    in  192.168.2.2/32               192.168.1.2/32               0.0
  1    out 192.168.1.2/32               192.168.2.2/32               0.0
  2    in  n/a                          n/a                          0.0
  2    out n/a                          n/a                          0.0


Peer ID / IP                            Local ID / IP
------------                            -------------
192.168.2.2                             192.168.1.2
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
  Tun# Dir Source Network              Destination Network         Bytes
  ---- --- --------------              -------------------         -----
  1    in  n/a                         n/a                         0.0
  1    out n/a                         n/a                         0.0

vyatta@WEST>
```

show vpn ipsec state

Displays information about the current IPsec state.

Syntax:

```
show vpn ipsec state
```

Operational mode

Use this command to display information about the status about the current IPsec state.

The following example shows the output of the `show vpn ipsec state` command.

```
vyatta@R1# show vpn ipsec state
src 192.0.3.33 dst 192.0.3.1
        proto esp spi 0xcfa035e9 reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha1) 0x31c816ef1336fed43366d5023875f7e98b8e9e8f 96
        enc cbc(aes) 0x0cc8fbc4f29ee71945874cbd76a43a6302248a0eac75580ef85e2cfdee07a643
src 192.0.3.1 dst 192.0.3.33
        proto esp spi 0xc37c65f1 reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha1) 0xc7c7accc5ed51e4bb35457f0d98120975c3b8042 96
        enc cbc(aes) 0x1d5213116324811159de79f4a16754a04595ab8bffd5c30dd3327c0b4010b12b
src 192.0.3.33 dst 192.0.3.1
        proto esp spi 0xcc9fd53e reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha1) 0x886cfcb9a4d273fd4ebf1209297f49286db501d2 96
        enc cbc(aes) 0xbf5c202e635a512136bb7790c88ba9d7a40548e46c671b459e48b0506ad4e418
src 192.0.3.1 dst 192.0.3.33
        proto esp spi 0xcae3a9f1 reqid 1 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha1) 0xfb1374ffca9d4a7552c8a950c87b4f1784cfbd7a 96
        enc cbc(aes) 0x164be36fbeaf8762ebd4609c0cbe163e0df6da6273051657ee5ad600c1e521dd

vyatta@R1#
```

show vpn ipsec status

Displays information about the status of IPsec processes.

Syntax:

```
show vpn ipsec status
```

Operational mode

Use this command to display information about the status about running IPsec processes.

The information shown includes:

- The process ID
- The number of active tunnels
- The interfaces configured for IPsec

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

- The IP addresses of interfaces configured for IPsec

The following example shows the output of the `show vpn ipsec status` command.

```
vyatta@WEST> show vpn ipsec status
IPSec Process Running  PID: 5832

4 Active IPsec Tunnels

IPsec Interfaces:
  dp0p1p2 (10.6.0.55)


vyatta@WEST>
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Virtual Tunnel Interface Commands

clear interfaces vti counters

Clears statistics counters for virtual tunnel interfaces.

Syntax:
```
clear interfaces vti [ vtix ] counters
```

Clears counters for all virtual tunnel interfaces.

vtix

Clears statistics for the specified virtual tunnel interface.

Operational mode

Use this command to clear counters on virtual tunnel interfaces.

interfaces vti <vtix>

Defines a virtual tunnel interface.

Syntax:
```
set interfaces vti vtix
```

Syntax:
```
delete interfaces vti vtix
```

Syntax:
```
show interfaces vti vtix
```

vtix

Multi-node. The identifier for the virtual tunnel interface you are defining; for example `vti0`.

You can define multiple virtual tunnel interfaces by creating multiple `vti` configuration nodes.

Configuration mode

```
interfaces {
    vti vtix {
    }
}
```

Use this command to define a virtual tunnel interface.

Use the `set` form of this command to create a virtual tunnel interface.

Use the `delete` form of this command to remove a virtual tunnel interface.

Use the `show` form of this command to view virtual tunnel interface configuration.

interfaces vti <vtix> address <ip-address>

Sets an IP address and network prefix for a virtual tunnel interface.

Syntax:
```
set interfaces vti vtix address { ipv4 | ipv6 }
```

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
delete interfaces vti vtix address [ ipv4 | ipv6 ]
```

Syntax:

```
show interfaces vti vtix address
```

vtix

The identifier of the virtual tunnel interface. The identifiers range from **vti0** through **vti** *x*, where x is a positive integer.

ipv4

Defines an IPv4 address on this interface. The format is *ip-address* / *prefix* (for example, 192.168.1.77/24).

You can define multiple IP addresses for a single virtual tunnel interface, by creating multiple `address` configuration nodes.

ipv6

Defines an IPv6 address on this interface. The format is *ipv6-address* / *prefix* (for example, 2001:db8::/64).

You can define multiple IPv6 addresses for a single virtual tunnel interface, by creating multiple `address` configuration nodes.

Configuration mode

```
interfaces {
    vti vtix {
        address ipv4
    }
}
```

```
interfaces {
    vti vtix {
        address ipv6
    }
}
```

Use this command to set the IP address and network prefix for a virtual tunnel interface.

Note: You cannot configure IP addresses such as loopback addresses, or broadcast, or subnet-broadcast addresses on an interface.

Use the `set` form of this command to set the IP address and network prefix. You can set more than one IP address for the interface by creating multiple address configuration nodes.

Use the `delete` form of this command to remove IP address configuration.

Use the `show` form of this command to view IP address configuration.

interfaces vti <vtix> description <description>

Specifies a description for a virtual tunnel interface.

Syntax:

```
set interfaces vti vtix description description
```

Syntax:

```
delete interfaces vti vtix description
```

Syntax:

```
show interfaces vti vtix description
```

vtix

The identifier of the virtual tunnel interface. The identifiers range from **vti0** through **vti** *x*, where x is a positive integer.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

description
A mnemonic name or description for the virtual tunnel interface.

Configuration mode

```
interfaces {
    vti vtix {
            description description
    }
}
```

Use this command to set a description for a virtual tunnel interface.

Use the `set` form of this command to specify the description.

Use the `delete` form of this command to remove the description.

Use the `show` form of this command to view description configuration.

interfaces vti <vtix> disable

Disables a virtual tunnel interface without discarding configuration.

Syntax:
`set interfaces vti` *vtix* **`disable`**

Syntax:
`delete interfaces vti` *vtix* **`disable`**

Syntax:
`show interfaces vti` *vtix*

vtix
The identifier of the virtual tunnel interface. The identifier ranges from **vti0** through **vti** *x*, where x is a positive integer.

Configuration mode

```
interfaces {
    vti vtix {
            disable
    }
}
```

Use this command to disable a virtual tunnel interface without discarding configuration.

Use the `set` form of this command to disable the interface.

Use the `delete` form of this command to enable the interface.

Use the `show` form of this command to view virtual tunnel interface configuration.

interfaces vti <vtix> firewall <state>

Applies a firewall instance, or rule set, to an interface.

Syntax:
`set interfaces` **`vti`** *vtix* **`firewall`** { **`in`** *firewall-name* | **`l2`** *name* | **`out`** *firewall-name* }

Syntax:
`delete interfaces` **`vti`** *vtix* **`firewall`** [**`in`** *firewall-name* | **`l2`** *name* | **`out`** *firewall-name*]

Syntax:

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
show interfaces vti vtix firewall [ in | l2 | out ]
```

interface
A type of interface. For detailed keywords and arguments, refer to Supported Interface Types *(page 132)*.

in *firewall-name*
Applies a firewall rule set to inbound traffic on the specified interface.

l2
Applies a firewall rule set to bridge traffic.

out *firewall-name*
Applies a firewall rule set to outbound traffic on the specified interface.

Configuration mode

```
interfaces interface {
    vto vtix        firewall {
            in firewall-name
            l2 name
            out firewall-name
    }
}
```

Use this command to apply an IPv6 firewall instance, or rule set, to an interface.

A firewall has no effect on traffic traversing the system or destined to the system until a firewall rule set has been applied to an interface or a virtual interface by using this command.

To use the firewall feature, you must define a firewall rule set as a named firewall instance by using the `security firewall name` command. You then apply the firewall instance to interfaces, virtual interfaces, or both by using this command. After the instance is applied, the instance acts as a packet filter.

The firewall instance filters packets in one of the following ways, depending on what you specify when you apply it.

- *in* —If you apply the rule set as *in*, the firewall filters packets entering the interface.
- *out* —If you apply the rule set as *out*, the firewall filters packets leaving the interface.

For each interface, you can apply up to three firewall instances: one firewall *in* instance, one firewall *out* instance, and one firewall local instance.

Make sure the firewall instance you apply to an interface is already defined, or you may experience unintended results. If you apply a firewall instance that does not exist to an interface, the implicit firewall rule of *allow all* is applied.

Use the `set` form of this command to apply an IPv6 firewall instance, or rule set, to an interface.

Use the `delete` form of this command to delete an IPv6 firewall instance, or rule set, from an interface.

Use the `show` form of this command to display the configuration of an IPv6 firewall instance, or rule set, for an interface.

interfaces vti <vtix> mtu <mtu>

Sets the MTU for a virtual tunnel interface.

Syntax:
```
set interfaces vti vtix mtu mtu
```

Syntax:
```
delete interfaces vti vtix mtu
```

Syntax:
```
show interfaces vti vtix mtu
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

If this value is not set, the default MTU of 1500 is used.

vtix
The identifier of the virtual tunnel interface. The identifiers range from **vti0** through **vti** *x*, where x is a positive integer.

mtu
Sets the MTU, in octets, for the interface. The numbers range from 68 through 9000.

Configuration mode

```
interfaces {
    vti vtix {
        mtu mtu
    }
}
```

Use this command to set the maximum transmission unit (MTU) for an virtual tunnel interface.

During forwarding, IPv4 packets larger than the MTU are fragmented unless the “Don't Fragment” (DF) bit is set in the IP header. In that case, the packets are dropped and an ICMP “fragmentation needed” message is returned to the sender.

Use the `set` form of this command to specify the MTU.

Use the `delete` form of this command to remove MTU value and restore the default behavior.

Use the `show` form of this command to view MTU configuration.

monitor interfaces vti <vtix> traffic

Displays (captures) traffic on a virtual tunnel interface.

Syntax:
`monitor interfaces vti` *vtix* **`traffic`** [**`detail`** [**`filter filter-name`** | **`unlimited`** [**`filter filter-name`**]] | **`filter filter-name`** | **`save`** *filename* | **`unlimited`** [**`filter filter-name`**]]]

vtix
The identifier of an virtual tunnel interface. The identifiers range from `vti0` through `vtix`, where `x` is a non-negative integer.

`detail`
Provides detailed information about the monitored VRRP traffic.

filter-name
Applies the specific PCAP (packet capture) filter to traffic.

`unlimited`
Monitors an unlimited amount of traffic.

filename
Saves the monitored traffic to the specified file.

Operational mode

Use this command to capture traffic on a virtual tunnel interface. Type <Ctrl>+c to stop the output.

The following example shows captured data on interface vti0.

```
vyatta@vyatta:~$ monitor interfaces vti vti0 traffic
Capturing traffic on vti0 ...
  4.568357 192.168.1.254 -> 238.255.255.251 SSDP NOTIFY * HTTP/1.1
  4.568372 192.168.1.254 -> 238.255.255.251 SSDP NOTIFY * HTTP/1.1
...
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

show interfaces vti

Displays information and statistics about Virtual Tunnel interfaces.

Syntax:

```
show interfaces vti [ vtix ]
```

Information is displayed for all Virtual Tunnel interfaces.

vtix

Displays information for the specified Virtual Tunnel interface. The identifiers range from `vti0` through `vtix`, where x is a positive integer.

Operational mode

Use this command to view operational status of Virtual Tunnel interfaces.

The following example shows information for all Virtual Tunnel interfaces.

```
vyatta@vyatta:~$ show interfaces vti
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
vti2             100.0.0.1/24                   u/u
```

The following example shows information for interface vti2.

```
vyatta@vyatta:~$ show interfaces vti vti2
vti2: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ipip 12.0.0.1 peer 12.0.0.2
    inet 100.0.0.1/24 scope global vti2
    RX:  bytes    packets     errors    dropped    overrun      mcast
            84          1          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
            84          1          0          0          0          0
```

show interfaces vti detail

Displays detailed information about Virtual Tunnel interfaces.

Syntax:

```
show interfaces vti detail
```

Operational mode

Use this command to view detailed statistics and configuration information about Virtual Tunnel interfaces.

The following example shows the first screen of output for show interfaces vti detail.

```
vyatta@vyatta:~$ show interfaces vti detail
vti2: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ipip 12.0.0.1 peer 12.0.0.2
    inet 100.0.0.1/24 scope global vti2
    RX:  bytes    packets     errors    dropped    overrun      mcast
            84          1          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

```
            84          1          0          0          0          0
```

show interfaces vti <vtix> brief

Displays a brief status for an Virtual Tunnel interface.

Syntax:

`show interfaces vti` *vtix* **`brief`**

vtix

The identifier of an Virtual Tunnel interface. The identifiers range from `vti0` through `vtix`, where x is a positive integer.

Operational mode

Use this command to view the status of a virtual tunnel interface.

The following example shows brief status for interface vti2.

```
vyatta@vyatta:~$ show interfaces vti vti2 brief
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
vti2             100.0.0.1/24                   u/u
```


© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Supported Interface Types

The following table shows the syntax and parameters of supported interface types. Depending on the command, some of these types may not apply.

Interface Type	Syntax	Parameters
Bridge	`bridge` *brx*	*brx*: The name of a bridge group. The name ranges from br0 through br999.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Interface Type	Syntax	Parameters
Data plane	`dataplane` *interface-name*	*interface-name*: The name of a data plane interface. Following are the supported formats of the interface name: • `dp`*x*`p`*y*`p`*z*—The name of a data plane interface, where — `dp`*x* specifies the data plane identifier (ID). Currently, only dp0 is supported. — `p`*y* specifies a physical or virtual PCI slot index (for example, p129). — `p`*z* specifies a port index (for example, p1). For example, dp0p1p2, dp0p160p1, and dp0p192p1. • `dp`*x*`em`*y* —The name of a data plane interface on a LAN-on-motherboard (LOM) device that does not have a PCI slot, where `em`*y* specifies an embedded network interface number (typically, a small number). For example, dp0em3. • `dp`*x*`s`*y*—The name of a data plane interface in a system in which the BIOS identifies the network interface card to reside in a particular physical or virtual slot *y*, where *y* is typically a small number. For example, for the dp0s2 interface, the BIOS identifies slot 2 in the system to contain this interface. • `dp`*x*`P`*n*`p`*y*`p`*z* —The name of a data plane interface on a device that is installed on a secondary PCI bus, where `P`*n* specifies the bus number. You can use this format to name data plane interfaces on large physical devices with multiple PCI buses. For these devices, it is possible to have network interface cards installed on different buses with these cards having the same slot ID. The value of *n* must be an integer greater than 0. For example, dp0P1p162p1 and dp0P2p162p1.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Interface Type	Syntax	Parameters
Data plane vif	`dataplane` *interface-name* `vif` *vif-id* [`vlan` *vlan-id*]	*interface-name*: Refer to the preceding description. *vif-id*: A virtual interface ID. The ID ranges from 1 through 4094. *vlan-id*: The VLAN ID of a virtual interface. The ID ranges from 1 through 4094.
Loopback	`loopback lo` or `loopback lo`*n*	*n*: The name of a loopback interface, where *n* ranges from 1 through 99999.
OpenVPN	`openvpn` *vtunx*	*vtunx*: The identifier of an OpenVPN interface. The identifier ranges from vtun0 through vtun*x*, where *x* is a nonnegative integer.
Tunnel	`tunnel` *tunx* or `tunnel` *tunx* `parameters`	*tunx*: The identifier of a tunnel interface you are defining. The identifier ranges from tun0 through tun*x*, where *x* is a nonnegative integer.
Virtual tunnel	`vti` *vtix*	*vtix*: The identifier of a virtual tunnel interface you are defining. The identifier ranges from vti0 through vti*x*, where *x* is a nonnegative integer. **Note:** Before you can configure a vti interface, you must configure a corresponding vpn. **Note:** This interface does not support IPv6.
VRRP	*parent-interface* `vrrp vrrp-group` *group*	*parent-interface*: The type and identifier of a parent interface; for example, data plane dp0p1p2 or bridge br999. *group*: A VRRP group identifier. The name of a VRRP interface is not specified. The system internally constructs the interface name from the parent interface identifier plus the VRRP group number; for example, dp0p1p2v99. Note that VRRP interfaces support the same feature set as does the parent interface.

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

List of Acronyms

Acronym	Description
ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AMI	Amazon Machine Image
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
AWS	Amazon Web Services
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CCMP	AES in counter mode with CBC-MAC
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMVPN	dynamic multipoint VPN
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EBS	Amazon Elastic Block Storage
EC2	Amazon Elastic Compute Cloud
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Acronym	Description
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP Security
IPv4	IP Version 4
IPv6	IP Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISM	Internet Standard Multicast
ISP	Internet Service Provider
KVM	Kernel-Based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
MAC	medium access control
mGRE	multipoint GRE
MIB	Management Information Base
MLD	Multicast Listener Discovery
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
ND	Neighbor Discovery
NHRP	Next Hop Resolution Protocol
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PIM	Protocol Independent Multicast
PIM-DM	PIM Dense Mode
PIM-SM	PIM Sparse Mode
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

Acronym	Description
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PTMU	Path Maximum Transfer Unit
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RHEL	Red Hat Enterprise Linux
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, and Adleman
Rx	receive
S3	Amazon Simple Storage Service
SLAAC	Stateless Address Auto-Configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPT	Shortest Path Tree
SSH	Secure Shell
SSID	Service Set Identifier
SSM	Source-Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TBF	Token Bucket Filter
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
ToS	Type of Service
TSS	TCP Maximum Segment Size
Tx	transmit
UDP	User Datagram Protocol
VHD	virtual hard disk
vif	virtual interface
VLAN	virtual LAN
VPC	Amazon virtual private cloud
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network
WAP	wireless access point
WPA	Wired Protected Access

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.