IPsec Site-to-Site VPN Configuration Guide, Addendum 1801

November 2018

Supporting AT&T Vyatta Network Operating System

Copyright Statement

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.

About This Guide

This addendum describes IPsec Virtual Feature Point (VFP) VPN, which was added to 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) in release 1801.

IPsec Site-to-Site VPN Configuration Options

The AT&T Vyatta Router supports the following configuration options for IPsec site-to-site VPNs:

- **Policy-based with no associated, visible interface**: A policy-based configuration supports the IETF standards for IPsec.
  - Traffic is directed to a specified VPN tunnel according to a defined policy, and the same policy applies to all the traffic going through that tunnel.
  - It is relatively easy to deploy and is compatible with other vendor policy-based IPsec VPNs.
  - This type of configuration is suitable when you do not need to conserve tunnel resources or configure many security policies to filter traffic through the tunnel. For example, it can be used for a VPN to connect a branch office to corporate headquarters
- **Virtual Feature Point (VFP) Interfaces**: VFP is a new feature of vRouter. A key benefit of VFP is its flexibility.
  - VFP can be deployed with a peer that is configured for policy-based IPsec VPN, because its IKE negotiation to establish the IPsec tunnel is indistinguishable from the IKE negotiation used with policy-based IPsec. One peer can use basic policy-based IPsec and the other peer can use the *enhanced* policy-based IPsec with VFP.
  - When you use VFP, you can apply interface-dependent features such as network address translation (NAT) and firewalls to packets traversing the IPsec tunnel. Thus, it allows you to take advantage of features available to route-based IPsec VPNs while maintaining compatibility with policy-based IPsec VPNs.
- **Virtual Tunnel Interfaces (VTI**): 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.
  - It allows you to configure a route-based VPN, *not* a policy-based VPN.
  - Like VFP, VTI allows you to apply interface-dependent features.
  - The IKE negotiation is different than it is without VTI. Therefore, VTI should be applied on both ends of the connection. We do not recommend connecting a VTI peer to a peer that is not using VTI.
  - VTI is compatible with third party VTI VPN connections and might be required for connectivity with public cloud offerings.
- **GRE Tunnel**: Protected by IPsec: GRE tunnels can be included within IPsec, allowing you to take advantage of the multi-protocol flexibility of GRE while having the encryption protection of IPsec.
  - Interface-dependent features (such as NAT, uRPF, firewall) can be specified for the GRE tunnel.
  - This type of configuration requires that both peers are configured for a GRE tunnel protected by IPsec.

IPsec Site-to-Site VPN with a Virtual Feature Point Interface

The virtual feature point (VFP) is a new feature of vRouter. It can be used with an IPsec site-to-site VPN to provide both granularity and flexibility.

Configuring a VFP Interface for an IPsec VPN

To configure a VFP interface for a VPN tunnel, use the following command:

```
set security vpn ipsec site-to-site peer <peer> tunnel <number> uses <vfpN>
```

The VFP interface supports the following keywords after "`set interfaces virtual-feature-point <vfpN>:`

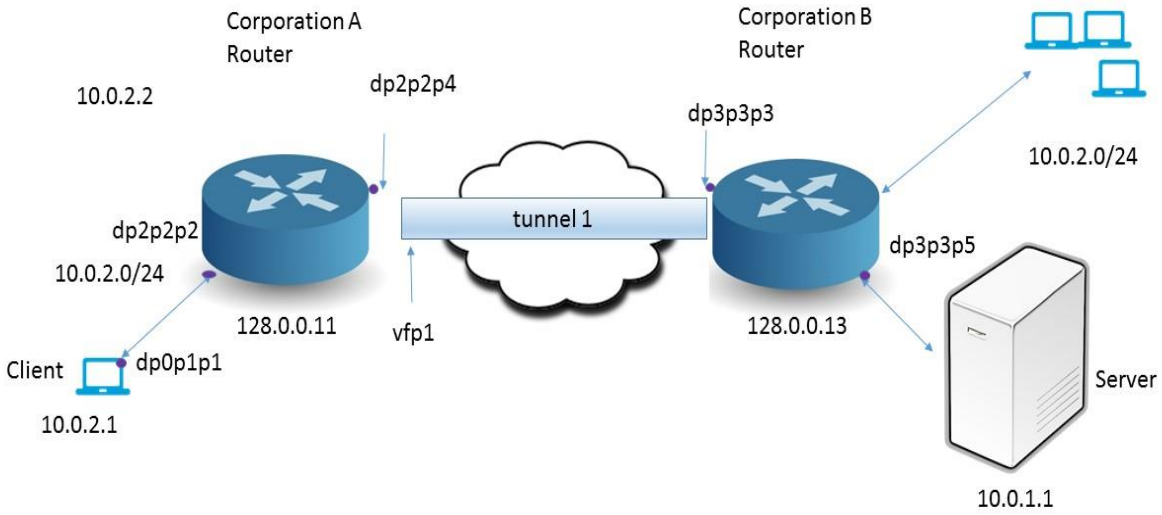
```
description
ip unnumbered
ipv6 unnumbered
ip tcp-mss
ipv6 tcp-mss
firewall
policy route policy-based
disable
address
mtu
```

Configuring an IPsec Virtual Feature Point Site-to-Site VPN to Handle Overlapping IP Addresses

In this sample configuration, a client (10.0.2.1) within the Corporation-A private network wants to access a server (10.0.1.0) within the Corporation-B private network. For security, a site-to-site VPN connection is configured from Corporation-A to Corporation-B.

However, it happens that both Corporation-A and Corporation-B are using the same IP range of addresses within their private networks. Thus, Corporation-A's client is assigned to IP address range 10.0.2.1/24, but Corporation-B reserves IP address range 10.0.2.0/24 for its own internal purposes. So if the Corporation-A client sent a packet to the server in Corporation-B, the connection might be misinterpreted as coming from one of Corporation-B's own internal addresses.

To avoid conflicts with Corporation-B's internal-use IP addresses, the Corporation-A Router translates its client's address to a different address (10.0.3.0/1/24) when it sends packets to Corporation-B. Corporate A router uses the virtual feature point (VFP) interface to apply the SNAT policy specifically on its client's traffic heading through the VPN to the server within the Corporation-B network, and it verifies that the responses from the server are translated back to the actual source address of the client. The Corporation-B router uses standard policy-based IPsec; it does not need a VFP interface.



Configuring the Corporation-A Client

The following table provides the steps and commands to configure the client within the Corporation-A network:

Corporation-A Client: Configuration Parameters Step	Command
Specify the interface that connects the Corporation-A client to the Corporation-A Router.	`vyatta@CORPA-client#set interfaces dataplane dp0p1p1 address 10.0.2.1/24`
Sets the default static route from Corporation-A client to the Corporation-A Router as its next-hop.	`vyatta@CORPA-client#set protocols static route 0.0.0.0/0 next-hop 10.0.2.2`

Before we go into the specifics of configuring the routers for this particular type of IPsec VPN configuration, we must configure the ESP group and the IKE group that will be used by both routers for this VPN site-to-site connection.

Configuring an ESP group on the Corporation-A Router

The following table provides the steps and commands to configure ESP group, `esp1`. The same ESP group and the same parameters must be used by both the Corporation-A Router and the Corporation-B Router for this IPsec site-to-site VPN connection.

Corporation-A Router: ESP Group Configuration Parameters	
Step	Command
Set the lifetime for the whole ESP group.	`vyatta@CORPA# set security vpn ipsec esp-group esp1 lifetime 600`
Set the authentication mode.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 authentication mode pre-shared-secret`
Set the pre-shared secret.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 authentication pre-shared-secret HelloDolly`
Specify the default ESP group for all tunnels.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 default-esp-group esp1`

Configuring an IKE Group on the Corporation-A Router

The following table provides the steps and commands to configure an IKE group, ike1. The same IKE group and the same parameters must be used by both the Corporation-A Router and the Corporation-B Router for this IPsec site-to-site VPN connection.

Corporation-A Router: IKE Group Configuration Parameters	
Step	Command
Set the lifetime for the whole IKE group	`vyatta@CORPA#set security vpn ipsec ike-group ike1 lifetime 3000`
Set the IKE group encryption cipher for proposal 1	`vyatta@CORPA#set security vpn ipsec ike-group ike1 proposal 1 encryption aes256`
Specify that this IKE group applies to the connection from this router to Corporation-B router.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 ike-group ike1`

Configuring the Corporation-A Router Interfaces

The following table provides the steps and commands to configure the interface addresses on the Corporation-A router:

Corporation-A Router: Interfaces Addressing Configuration Parameters	
Step	Command
Specify the interface that connects the Corporation-A Router to this Corporation-A client.	`vyatta@CORPA#set interfaces dataplane dp2p2p2 address 10.0.2.2/24`
Specify the interface that provides connectivity from the Corporation-A Router through the Internet to the other end of the IPsec tunnel.	`vyatta@CORPA#set interfaces dp2p2p4 address 128.0.0.11/24`

Ensure that there is an interface with a usable address for the virtual feature point (VFP) interface by specifying a loopback address.	`vyatta@CORPA#set interfaces loopback lo1 address 169.254.0.1/32`
Create the VFP interface. Ensure that it is IPv4-enabled by setting it to unnumbered and associating it with the loopback address. No traffic is actually sourced from this address. It is simply a way of enabling interface-dependent features on the VFP.	`vyatta@CORPA#set interfaces virtual-feature-point vfp1 ip unnumbered donor-interface lo1`

Configuring a Site-to-Site Connection from the Corporation-A Router to Corporation-B Router

The following table provides the steps and commands to configure a site-to-site connection from the Corporation-A Router to the Corporation-B Router:

Corporation-A Router: Site-to-Site Connection Configuration Parameters Step	Command
Specify the IP address of the Corporate B Router as the peer for this site-to-site connection. Specify the IP address of Corporate A Router as the local IP address.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 local-address 128.0.0.11`
Specify the subnet that will appear to be the source address of traffic that originates from Corporation-A client going to the Corporation-B server.	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 tunnel 1 local prefix 10.0.3.0/24`
Creates a tunnel configuration to Corporation-B Router specifies the IP address of the Corporation-B server as the specific remote address.	`vyatta@CORPA# set security vpn ipsec site-to-site peer 128.0.0.13 tunnel 1 remote prefix 10.0.1.0/24`
Specify a virtual feature point interface to be associated with this tunnel	`vyatta@CORPA#set security vpn ipsec site-to-site peer 128.0.0.13 tunnel 1 uses vfp1`

Configuring SNAT for VFP on the Corporation-A Router

The following table provides the steps and commands to configure SNAT for VFP on the Corporation-A Router:

NOTE: You do not need to configure a VFP on the peer router. The Corporation-B router in this example can be configured with a standard POLICY-BASED configuration.

Corporation-A Router: SNAT for VFP Configuration Parameters	
Step	Command
Specify SNAT for packets coming into the router from client `10.0.2.0/24`,	`vyatta@CORPA#set service nat source rule 10 source address 10.0.2.0/24`
Translates addresses coming in from that client to `10.0.3.0/24`.	`vyatta@CORPA#set service nat source rule 10 translation address 10.0.3.0/24`
Ties packets that have been translated to `10.0.3.0/24` to the VFP interface as they pass through the VPN tunnel.	`vyatta@CORPA#set service nat source rule 10 outbound-interface vfp1`

Configuring Corporation-A Router for Policy-Based IPsec on VFP

The following table provides the steps and commands to configure the policy-based IPsec on the Corporation-A router:

Corporation-A Router: Policy-Based IPsec Configuration Parameters	
Step	Command
Specifies that this VPN is going to use policy rule 10, which has been defined for traffic heading to Corporation-B	`vyatta@CORPA# set policy route policy-based toCorpB rule 10 action accept`
Specifies that the policy applies to traffic originating from the Corporation-A client.	`vyatta@CORPA# set policy route policy-based toCorpB rule 10 source address 10.0.2.0/24`
Specifies that the policy applies to traffic going to the Corporation-B server	`vyatta@CORPA# set policy route policy-based toCorpB rule 10 destination address 10.0.1.0/24`
Specifies that this policy is defined in table 50.	`vyatta@CORPA# set policy route policy-based toCorpB rule 10 table 50`
Specifies that the default route of this table is to through the VFP interface.	`vyatta@CORPA#set protocols static table 50 interface-route 0.0.0.0/0 next-hop-interface vfp1`
Specifies the interface used to forward traffic matching this policy.	`vyatta@CORPA# set interfaces dataplane dp2p2p2 policy route policy-based toCorpB`

Configuring the Interfaces on Corporation-B Router

The following table provides the steps and commands to configure the interfaces on the Corporation-B router:

Corporation-B Router: Interfaces Configuration Parameters	
Step	Command
Specify the interface that connects the Corporation-B router to the server within its network.	`vyatta@CORPB#set interfaces dataplane dp3p3p5 address 10.0.1.1/24`
Specify the interface that provides connectivity from the Corporation-B router through the Internet to the other end of the IPsec tunnel.	`vyatta@CORPB#set interfaces dataplane dp3p3p3 address 128.0.0.13/24`

Configuring an ESP group on the Corporation-B Router

The following table provides the steps and commands to configure the ESP group, `esp1`, on the Corporation-B router:

Note: Use the same ESP group values here that you set for the ESP group on the Corporation-A router.

Corporation-B Router: ESP Group Configuration Parameters	
Step	Command
Set the lifetime for the whole ESP group to match the setting being used by the Corporation-A router.	`vyatta@CORPB# set security vpn ipsec esp-group esp1 lifetime 600`
Set the ESP group encryption cipher to match the settings being used by the Corporation-A router..	`vyatta@CORPB#set security vpn ipsec esp-group esp1 proposal 1 encryption aes256`
Set the authentication mode to match the authentication mode set on the Corporation-A router and specify the IP address of the Corporation-A router.	`vyatta@CORPB#set security vpn ipsec site-to-site peer 128.0.0.11 authentication mode pre-shared-secret`
Set the pre-shared secret to match the secret set on the Corporation-A router and specify the IP address of the Corporation-A router.	`vyatta@CORPB#set security vpn ipsec site-to-site peer 128.0.0.11 authentication pre-shared-secret HelloDolly`
Specify the default ESP group for all tunnels to match the one specified on the Corporation-A router and specify the IP address of the Corporation-A router.	`vyatta@CORPB#set security vpn ipsec site-to-site peer 128.0.0.11 default-esp-group esp1`

Configuring an IKE group on the Corporation-B Router

The following table provides the steps and commands to configure the IKE group, ike1 on the Corporation-B router:

NOTE: Use the same IKE values that you set for the IKE on the Corporation-A router.

Corporation-B Router: IKE Group Configuration Parameters Step	Step
Set the IKE group encryption cipher to match the settings being used by the Corporation-A router.	`vyatta@CORPB#set security vpn ipsec ike-group ike1 proposal 1 encryption aes256`
Set the lifetime for the whole IKE group to match the setting used by the Corporation-A router.	`vyatta@CORPB#set security vpn ipsec ike-group ike1 lifetime 3000`

Configuring the site-to-site connection from the Corporation-B Router to the Corporation-A Router

The following table provides the steps and commands to configure the site-to-site connection from the Corporation-B router to the Corporation-A router:

Corporation-B Router: Site-to-Site Connection Configuration Parameters Step	Command
Specify that this connection is going to IP address 128.0.0.11 and is using the same IKE group as the Corporation-A router.	`vyatta@CORPB# set security vpn ipsec site-to-site peer 128.0.0.11 ike-group ike1`
Specify that this connection is going to IP address 128.0.0.11 and is using the same ESP group as Corporation-A router	`vyatta@CORPB# set security vpn ipsec site-to-site peer 128.0.0.11 default-esp-group esp1`
Specify the address of the Corporation-B router as the local address.	`vyatta@CORPB# set security vpn ipsec site-to-site peer 128.0.0.11 local-address 128.0.0.13`
Specify the address of Corporation-B server as the local prefix.	`vyatta@CORPB# set security vpn ipsec site-to-site peer 128.0.0.11 tunnel 1 local prefix 10.0.1.0/24`
Specify the translated address that was sent from the Corporation-A router to the Corporate B router in place of the	`vyatta@CORPB# set security vpn ipsec site-to-site peer 128.0.0.11 tunnel 1 remote prefix 10.0.3.0/24`

Corporation-B Router: Site-to-Site Connection Configuration Parameters	
Step	Command
actual client address as the remote prefix.	

Configuring Corporation-B Server

The following table provides the steps and command to configure the server's connection to the Corporation-B router:

Corporation-B Server: Configuration Parameters	
Step	Command
Specify the interface that connects the server to the Corporate B Router.	`vyatta@CORPB-server# set interfaces dataplane dp4p4p2 address 10.0.1.1/24`
Specifies the default static route from the server to the Corporation-B Router as its next-hop.	`vyatta@ CORPB-server# set protocols static route 0.0.0.0/0 next-hop 10.0.1.2`

Verification

To confirm that the configuration is working properly, perform the following tasks:

Show IKE sessions

```
VYATTA@CORPA:~$ SHOW VPN IKE SA

PEER ID / IP                            LOCAL ID / IP
------------                            -------------
128.0.0.13                              128.0.0.11

    STATE    ENCRYPT        HASH    D-H GRP  A-TIME  L-TIME IKEV
    -----  ------------  --------  -------  ------  ------ ----
    UP       AES256         SHA1       5         0       3000    1
```

Show established ESP connections

```
vyatta@CORPA:~$ show vpn ipsec sa

Peer ID / IP                            Local ID / IP
------------                            -------------
128.0.0.13                              128.0.0.11

Tunnel  Id       State  Bytes Out/In   Encrypt       Hash      DH A-Time  L-Time ---
-  ----------  -----  -------------  ------------  --------  -- ------  ------
    1   3         up     0.0/0.0        aes256        sha1      5  451     1500
```

```
vyatta@CORPA:~$ show vpn ipsec sa detail peer 128.0.0.13

------------------------------------------------------------------
Peer IP:                128.0.0.13
Peer ID:                128.0.0.13
Local IP:               128.0.0.11
Local ID:               128.0.0.11
NAT Traversal:          no
NAT Source Port:        n/a
NAT Dest Port:          n/a

    Tunnel 1:
        State:                  up
        Id:                     5
        Inbound SPI:            cee5e0bb
        Outbound SPI:           ca01d0b1
        Encryption:             aes256
        Hash:                   sha1
        DH Group:               5

        Local Net:              10.0.3.0/24
        Local Protocol:         all
        Local Port:             all

        Remote Net:             10.0.1.0/24
        Remote Protocol:        all
        Remote Port:            all

        Inbound Bytes:          252.0
        Outbound Bytes:         252.0

        Inbound Blocked:        no
        Outbound Blocked:       no

        Active Time (s):        318
        Lifetime (s):           1500
```

Show SNAT rules

```
vyatta@CORPA:~$ show nat source

------------------------
NAT Rulesets Information
------------------------
SOURCE
rule    intf            match                           translation
----    ----            -----                            -----------
10      vfp1          from 10.0.2.0/24        dynamic any -> 10.0.3.1-10.0.3.254
```

Show seen SNAT translations

```
vyatta@CORPA:~$ show nat source translations

Pre-NAT                 Post-NAT                Prot    Timeout

10.0.2.1:4323           10.0.3.1:4323           icmp    57
```

Show NAT sessions

```
vyatta@CORPA:~$ show session table
TCP state codes: SS - SYN SENT, SR - SYN RECEIVED, ES - ESTABLISHED, FW - FIN WAIT,
CW - CLOSE WAIT, CG - CLOSING, LA - LAST ACK, TW - TIME WAIT, CL - CLOSED

CONN ID    Source      Destination      Protocol          TIMEOUT
Intf          Parent
1       10.0.2.1:4323  10.0.1.1:4323     icmp [1] ES       15     vfp1    0
```

Viewing IPsec logs

To display the entire IPsec log:

```
show log vpn ipsec
```

To display the tail end of the log:

```
mnonitor vpn ipsec
```