Site-to-Site IPsec VPN

HOW TO GUIDE

Part No. TME-08-2014-30 Rev. B

Table of Contents

1. Overview

This guide provides an overview of the configuration steps required to establish site-to-site IPsec VPN tunnels between RFS X000 Controllers running WiNG 5.3 or higher firmware. This guide aims to provide the reader with the necessary information required to understand each of the IPsec configuration elements and apply them to create a working configuration. This guide does not provide configuration for third-party devices nor does it provide any details implementing X.509 certificates for authentication. These topics are out of the scope of this guide.

Note: The RFS X000 Wireless Controllers running WiNG 5.1 or WiNG 5.2 support a legacy IPsec VPN implementation that is not covered in this guide. Configuration examples for legacy VPN operation are covered in a separate guide.

1.1 Platform Support

The following table provides a matrix of WiNG 5 platform and minimum WiNG 5 release required to support the new implementation of IPsec which was introduced in WiNG 5.3.0. This table also provides the maximum number of IPsec Security Associations (SAs) supported by each platform:

WiNG 5 Platform	Version Support	Maximum IPsec Tunnels (SAs)
NX 9XX0	Not Supported	▨
NX 45XX	WiNG 5.4.2 and Above	128
NX 65XX	WiNG 5.4.2 and Above	128
RFS 7000	WiNG 5.3 and Above	512 (Base License) 1,024 (Advanced Security License)
RFS 6000	WiNG 5.3 and Above	256 (Base License) 512 (Advanced Security License)
RFS 4000	WiNG 5.3 and Above	256
AP 8131	WiNG 5.4.2 and Above	128
AP 71x1	WiNG 5.3 and Above	128
AP 6532	WiNG 5.3 and Above	64
AP 6522	WiNG 5.4 and Above	64
AP 6521	Not Supported	▨
AP 6511	Not Supported	▨
AP 650	Yes	64
AP 622	WiNG 5.4 and Above	64
AP 621	Not Supported	▨

Table 1.1 – WiNG 5 Platform and Release Support

1.2 Configuration Parameters

1.2.1 Global Configuration Parameters (Profile or Device)

The following table provides an overview of the global Internet Key Exchange (IKE) and IP Security (IPsec) parameters and default values which are assigned to each supported device profile by default. These parameters and values can be modified in the device profile or assigned directly to each device as overrides:

Global Configuration Parameter	Description
`crypto <ikev1|ikev2> dpd-keepalive <10-3600>`	Defines the global dead peer detection (DPD) interval in seconds for IKEv1 or IKEv2 in absence of traffic. Default value is ***30*** seconds.
`crypto <ikev1|ikev2> dpd-retries <1-100>`	Defines the global dead peer detection (DPD) retry interval for IKEv1 or IKEv2. Default value is ***5*** retries.
`crypto <ikev1|ikev2> nat-keepalive <10-3600>`	Defines the global NAT keepalive interval in seconds for IKEv1 or IKEv2. Default value is ***20*** seconds.
`crypto ikev2 cookie-challenge-threshold <1-100>`	Start cookie challenge after half open IKEv2 security associations (SAs) cross this limit. Default threshold value is ***5*** SAs.
`crypto ipsec security-association lifetime seconds <120-86400>|kilobytes <500-2147483646>`	Defines the global security association (SA) lifetime in seconds or kilobytes before the SA is expired. Default lifetime is ***3,600*** seconds and ***4,608,000*** bytes. Can be overridden in the crypto map.

Table 1.2.1 – Global Parameters

1.2.2 IKE Parameters (Profile or Device)

Internet Key Exchange (IKEv1 or IKEv2) is the protocol used to set up a security association (SA) between peers in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP and uses X.509 certificates or pre-shared keys for authentication and Diffie Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. The IKE protocol uses UDP port 500 by default and UDP port 4500 when a NAT device is detected between the peers (i.e. NAT traversal).

IKE consists of two phases:

- Phase 1 – Establishes a secure authenticated communication channel by using the Diffie Hellman key exchange algorithm to generate a shared secret key to encrypt further IKE communications. This negotiation results in one single bi-directional ISAKMP Security Association (SA). The authentication can be performed using a pre-shared key, or public key encryption. Phase 1 operates in either Main Mode or Aggressive Mode. Main Mode protects the identity of the peers while Aggressive Mode does not.
- Phase 2 – The IKE peers use the secure channel established in phase 1 to negotiate Security Associations (SA) on behalf of IPsec. The negotiation results in a minimum of two unidirectional security associations (one inbound and one outbound). The number of IPsec SAs is dependent on the number of source / destination networks and how the IP Access Control lists are defined.

IKEv2 (RFC 4306) builds upon IKEv1 and addresses various issues and limitations such as consolidating RFCs, improving NAT and firewall traversal support. In addition IKEv2 simplifies the message exchange (one 4 way message exchange vs. 8 separate mechanisms), provides reliability and state management and adds Denial of Server (DoS) attack resilience.

Note: An IPsec VPN tunnel can use Internet Key Exchange (IKE) version 1 or version 2 to establish the security associations (SAs) so you must select which IKE implementation you wish to use before defining the crypto parameters on the WiNG 5 device.

Note: When establishing site-to-site IPsec tunnels between WiNG 5 devices, it is recommended that IKEv2 be utilized whenever possible as IKEv2 provides many advantages and benefits over IKEv1. IKEv1 should only be implemented for IPsec VPN deployments requiring compatibility with older WiNG devices or implementations using third-party VPN gateways, routers, hosts or clients that do not support IKEv2.

1.2.2.1 IKEv1 Policies

The following table provides an overview of the IKEv1 policy parameters and default values. The WiNG 5 configuration includes a default IKEv1 policy named ***ikev1-default*** in each supported device profile that includes a ***default*** proposal, parameters and values. User defined IKE policies may also be optionally defined in a device profile or directly to devices as overrides:

Profile / Device Syntax
`crypto ikev1 policy <policy-name>`

Parameter	**Description**
`dpd-keepalive <10-3600>`	Defines the dead peer detection (DPD) interval for the IKEv1 policy in seconds in absence of traffic. Default value is ***30*** seconds.
`dpd-retries <1-100>`	Defines the global dead peer detection (DPD) retry interval for the IKEv1 policy. Default value is ***5*** retries.
`isakmp-proposal <name> encryption <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>`	Defines the ISAKMP proposal used to establish the security associations (SAs) for the IKEv1 policy. The default proposal uses aes-256 encryption, Diffie Hellman group 2 and SHA 1 hashing.
`lifetime <600-86400>`	Defines IKEv1 security association (SA) lifetime in seconds for the IKEv1 policy. Default lifetime is ***86,400*** seconds.
`mode <main|aggressive>`	Defines the IKEv1 mode used for the proposal. Default value is ***main***.

Table 1.2.2.1 – IKEv1 Policy Parameters

Each IKEv1 policy can include multiple proposals supporting different encryption, group and hashing values which the peers can negotiate. The ***ikev1-default*** policy includes a ***default*** proposal supporting AES 256 encryption, Diffie Hellman Group 2 and SHA 1 hashing. Additional proposals can be added to the ***ikev1-default*** policy or user defined policy as required to support peers with different encryption capabilities such as deployments with a mixture of encryption, keying and hashing schemes. The peers will negotiate the strongest proposal based on each peer's capabilities.

The following provides an example IKEv1 policy with multiple proposals which can be assigned to a device profile or directly to a device as an override. A separate proposal needs to be defined for each encryption, authentication and keying algorithm that needs to be supported:

IKEv1 Policy Example (Profile or Device)

```
crypto ikev1 policy IKEV1-POLICY
  isakmp-proposal aes256-group2-sha encryption aes-256 group 2 hash sha
  isakmp-proposal 3des-group2-sha encryption 3des group 2 hash sha
```

1.2.2.2 IKEv1 Peers

The following table provides an overview of the IKEv1 peer parameters which defines the identity and authentication parameters and IKEv1 policy used to establish a security association (SA). IKEv2 peers can be defined in each supported device profile or directly to supported device as overrides:

Profile / Device Syntax

```
crypto ikev1 peer <peer-name>
```

Parameter	Description
`ip {address <ip-address>}|{fqdn <host.domain.com>}`	IP address or fully qualified domain name (FQDN) of the remote peer. Note can be ***0.0.0.0*** at the hub for remote peers using dynamic IP addressing.
`remote-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <value>}`	Defines the remote identity which is provided by the remote peer. The local identity can be none, IP address, FQDN, email or DN.
`local-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <value>}`	Defines the local identity which is provided to the remote peer. The local identity can be none, IP address, FQDN, email or DN.
`authentication {rsa|psk <pre-shared-key>}`	Defines the authentication used by both peers for the security association (SA). Authentication can use RSA certificates or pre-shared keys.
`use ikev1-policy <policy-name>`	Assigns the IKEv1 policy to the IKEv1 peer that determines the security association (SA) parameters and proposals supported by the peers.

Table 1.2.2.2 – IKEv1 Peer Parameters

Each IKEv1 peer entry must include the IP address or FQDN of the remote peer, the authentication mode and an IKEv1 policy. A profile or device can include a single peer entry supporting multiple remote peers (wildcard IP address) or separate peer entries for each remote peer. This configuration will vary depending on if the peer is statically or dynamically addressed.

For the security association (SA) to be successfully established the IP address or FQDN of one or both of the peers must be known. For example in a hub and spoke environment the hub must have a static IP address while the spokes can be statically or dynamically addressed. In a static → dynamic IP environment, the security association (SA) can only be initiated from the dynamically addressed device.

Note: If dynamic IP addressing is used by both peers, a dynamic DNS service must be employed so that the FQDN of each peer resolves to the dynamic IP address assigned to each peer. As WiNG 5 does not natively support a dynamic DNS client, the client for the service must be installed on a host at each site.

The following provides an IKEv1 peer examples for a hub and spoke deployment with statically addressed devices with pre-shared key authentication and a user defined IKEv1 policy. Each hub and spoke device has a peer entry defined with the IP address of the remote peer and the respective pre-shared key:

IKEv1 Peer Example – Statically Addressed Hub (Profile or Device)

```
crypto ikev1 peer SPOKE1 ip
 address 76.7.10.20
 authentication psk 0 hellomoto1
 use ikev1-policy IKEV1-POLICY
crypto ikev1 peer SPOKE2 ip
 address 76.7.20.99
 authentication psk 0 hellomoto2
 use ikev1-policy IKEV1-POLICY
```

IKEv1 Peer Example – Statically Addressed Spoke1 (Profile or Device)

```
crypto ikev1 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto1
 use ikev1-policy IKEV1-POLICY
```

IKEv1 Peer Example – Statically Addressed Spoke2 (Profile or Device)

```
crypto ikev1 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto2
 use ikev1-policy IKEV1-POLICY
```

The following provides an IKEv1 peer examples for a hub and spoke deployment with a statically addressed hub and dynamically addressed spokes with pre-shared key authentication and a user defined IKEv1 policy. As the IP addresses of the remote spokes are unknown, the peer entry on the hub has a wildcard IP addressed and common pre-shared key defined. Each spoke has an identical peer entry using the hub IP address and common pre-shared key:

IKEv1 Peer Example – Statically Addressed Hub (Profile or Device)

```
crypto ikev1 peer SPOKES ip
 address 0.0.0.0 authentication
 psk 0 hellomoto
 use ikev1-policy IKEV1-POLICY
```

IKEv1 Peer Example – Dynamically Addressed Spoke1 (Profile or Device)

```
crypto ikev1 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto
 use ikev1-policy IKEV1-POLICY
```

IKEv1 Peer Example – Dynamically Addressed Spoke2 (Profile or Device)

```
crypto ikev1 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto
 use ikev1-policy IKEV1-POLICY
```

1.2.2.3 IKEv2 Policies

The following table provides an overview of the IKEv2 policy parameters and default values. The WiNG 5 configuration includes a default IKEv2 policy named ***ikev2-default*** in each supported device profile that includes a ***default*** proposal, parameters and values. User defined IKE policies may also be optionally defined in a device profile or directly to devices as overrides:

Profile / Device Syntax

```
crypto ikev2 policy <policy-name>
```

Parameter	Description
dpd-keepalive <10-3600>	Defines the dead peer detection (DPD) interval for the IKEv1 policy in seconds in absence of traffic. Default value is ***30*** seconds.
isakmp-proposal <name> encryption <des|3des|aes|aes-192|aes-256> group <1|2|5> hash <md5|sha>	Defines the ISAKMP proposal used to establish the security associations (SAs) for the IKEv2 policy. The default proposal uses aes-256 encryption, Diffie Hellman group 2 and SHA 1 hashing.
lifetime <600-86400>	Defines IKEv1 security association (SA) lifetime in seconds for the IKEv2 policy. Default lifetime is ***86,400*** seconds.
sa-per-acl	When enabled for site-to-site deployments this parameter creates a single security association (SA) for all rules in the ACL. Disabled by default.

Table 1.2.2.3 – IKEv2 Policy Parameters

Each IKEv2 policy can include multiple proposals supporting different encryption, group and hashing values which the peers can negotiate. The ***ikev2-default*** policy includes a ***default*** proposal supporting AES 256 encryption, Diffie Hellman Group 2 and SHA 1 hashing. Additional proposals can be added to the ***ikev2-default*** policy or user defined policy as required to support peers with different encryption capabilities such as deployments with a mixture of encryption, keying and hashing schemes. The peers will negotiate the strongest proposal based on each peer's capabilities.

The following provides an example IKEv2 policy with multiple proposals which can be assigned to a device profile or directly to a device as an override. A separate proposal needs to be defined for each encryption, authentication and keying algorithm that needs to be supported:

IKEv2 Policy Example (Profile or Device)

```
crypto ikev2 policy IKEV2-POLICY
  isakmp-proposal aes256-group2-sha encryption aes-256 group 2 hash sha
  isakmp-proposal 3des-group2-sha encryption 3des group 2 hash sha
```

1.2.2.4 IKEv2 Peers

The following table provides an overview of the IKEv2 peer parameters which defines the identity and authentication parameters and IKEv2 policy used to establish a security association (SA). IKEv2 peers can be defined in each supported device profile or directly to supported device as overrides:

Profile / Device Syntax
`crypto ikev2 peer <peer-name>`

Parameter	**Description**
`ip {address <ip-address>}|{fqdn <host.domain.com>}`	IP address or fully qualified domain name (FQDN) of the remote peer. Note can be ***0.0.0.0*** at the hub for remote peers using dynamic IP addressing.
`remote-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <value>}`	Defines the remote identity which is provided by the remote peer. The local identity can be none, IP address, FQDN, email or DN.
`local-identity {address <ip>| fqdn <value>| email <value>| string <value> |dn <value>}`	Defines the local identity which is provided to the remote peer. The local identity can be none, IP address, FQDN, email or DN.
`authentication {rsa|psk <pre-shared-key>} local`	Defines the authentication used by the local peer for the security association (SA). Authentication can use RSA certificates or pre-shared keys.
`authentication {rsa|psk <pre-shared-key>} remote`	Defines the authentication used by the remote peer for the security association (SA). Authentication can use RSA certificates or pre-shared keys.
`use ikev1-policy <policy-name>`	Assigns the IKEv1 policy to the IKEv1 peer that determines the security association (SA) parameters and proposals supported by the peers.

Table 1.2.2.4 – IKEv2 Peer Parameters

Each IKEv2 peer entry must include the IP address or FQDN of the remote peer, the authentication mode and an IKEv2 policy. A profile or device can include a single peer entry supporting multiple remote peers (wildcard IP address) or separate peer entries for each remote peer. This configuration will vary depending on if the peer is statically or dynamically addressed.

For the security association (SA) to be successfully established the IP address or FQDN of one or both of the peers must be known. For example in a hub and spoke environment the hub must have a static IP address while the spokes can be statically or dynamically addressed. In a static → dynamic IP environment, the security association (SA) can only be initiated from the dynamically addressed device.

ⓘ *Note: If dynamic IP addressing is used by both peers, a dynamic DNS service must be employed so that the FQDN of each peer resolves to the dynamic IP address assigned to each peer. As WiNG 5 does not natively support a dynamic DNS client, the client for the service must be installed on a host at each site.*

The following provides an IKEv2 peer examples for a hub and spoke deployment with statically addressed devices with pre-shared key authentication and a user defined IKEv2 policy. Each hub and spoke device has a peer entry defined with the IP address of the remote peer and the respective pre-shared keys. Note that in this example each device has unique load and remote pre-shared keys:

IKEv2 Peer Example – Statically Addressed Hub (Profile or Device)

```
crypto ikev2 peer SPOKE1
 ip address 76.7.10.20
 authentication psk 0 hellomoto1 local
 authentication psk 0 hellomoto1 remote
 use ikev2-policy IKEV2-POLICY
crypto ikev2 peer SPOKE2
 ip address 76.7.20.99
 authentication psk 0 hellomoto2 local
 authentication psk 0 hellomoto2 remote
 use ikev2-policy IKEV2-POLICY
```

IKEv2 Peer Example – Statically Addressed Spoke1 (Profile or Device)

```
crypto ikev2 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto1 local
 authentication psk 0 hellomoto1 remote
 use ikev2-policy IKEV2-POLICY
```

IKEv2 Peer Example – Statically Addressed Spoke2 (Profile or Device)

```
crypto ikev2 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto2 local
 authentication psk 0 hellomoto2 remote
 use ikev2-policy IKEV2-POLICY
```

The following provides an IKEv2 peer examples for a hub and spoke deployment with a statically addressed hub and dynamically addressed spokes with pre-shared key authentication and a user defined IKEv2 policy. As the IP addresses of the remote spokes are unknown, the peer entry on the hub has a wildcard IP addressed and common pre-shared key defined. Each spoke has an identical peer entry using the hub IP address and common pre-shared key:

IKEv2 Peer Example – Statically Addressed Hub (Profile or Device)

```
crypto ikev2 peer SPOKES
 ip address 0.0.0.0
 authentication psk 0 hellomoto local
 authentication psk 0 hellomoto remote
 use ikev2-policy IKEV2-POLICY
```

IKEv2 Peer Example – Dynamically Addressed Spoke1 (Profile or Device)

```
crypto ikev2 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto local
 authentication psk 0 hellomoto remote
 use ikev2-policy IKEV2-POLICY
```

IKEv2 Peer Example – Dynamically Addressed Spoke2 (Profile or Device)

```
crypto ikev2 peer HUB
 ip address 76.7.100.11
 authentication psk 0 hellomoto local
 authentication psk 0 hellomoto remote
 use ikev2-policy IKEV2-POLICY
```

1.2.3 Transform Sets

Transform sets are used to determine how the IP packets (i.e. site-to-site traffic) are protected between the IPsec peers. Once the IKE security association (SA) has been successfully established, the WiNG 5 device uses the rules in the IP Access Control List (ACL) to determine which IP packets are eligible to be protected over the IPsec security association (SA). Traffic that is permitted for the peer is protected using the parameters defined in the transform set assigned to the specific crypto map the peer is using.

The following table provides an overview of the transform set parameters and default values. The WiNG 5 configuration includes a default transform set named ***default*** in the supported device profiles that supports encapsulating security payload (ESP), AES 256 bit encryption, SHA1-HMAC authentication and tunnel mode. Transform sets can be defined in a device profile or directly to a device as an override on supported platforms:

Profile / Device Syntax

```
crypto ipsec transform-set <name> <esp-null|esp-des|esp-3des|esp-aes|esp-aes-192|aes-256>
<md5|sha> <esp-md5-hmac|esp-sha-hmac>
```

Parameter	Description
`mode <transport|tunnel>`	Determines how the payload of the IP packets are encrypted and authenticated: ▪ Transport Mode – Only the payload is encrypted and authenticated. The IP header is neither modified nor encrypted. ▪ Tunnel Mode (default) – The entire IP packet is encrypted and authenticated. The packet is encapsulated into a new IP packet with a new IP header.

Table 1.2.3 – Transform Set Parameters

Note: Authentication Header (AH) is not supported in WiNG 5.3 and above.

Each transform set can be assigned a single encryption algorithm, authentication algorithm and tunnel mode. If multiple algorithms need to be supported in the deployment, separate transform sets needs to be defined for each encryption, authentication and tunnel mode that needs to be supported. The transform sets can be assigned to the switched virtual interface (SVI) using crypto maps which share a common name but a different sequence ID

The following provides example transform sets supporting different encryption, authentication algorithms and tunnel mode which can be assigned to a device profile or directly to a device as an override:

Transform Set Examples (Profile or Device)

```
crypto ipsec transform-set ESP-AES-256-SHA1 esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA1 esp-3des esp-sha-hmac
```

1.2.4 IP Access Control Lists

IP Access Control Lists (ACLs) contain one or more permit rules to determine which IP packets are forwarded and secured by the crypto module. The IP packets which are permitted by the ACL are protected while IP packets that are not matched are ignored. How the IP packets are protected between the IPsec peers is determined by the transform set assigned to the specific crypto map the peer is using.

For site-to-site IPsec VPN each peer will need an ACL defined with one or more permit rules to determine the source and destination of the IP packets which are to be protected between the IPsec peers. Each rule may permit a specific host or subnet and may optionally contain specific protocols and ports.

The number of permit rules required for each peer will vary depending on the specific hosts and/or subnets that need to communicate at each site. For each source / destination pair an IPsec security association (SA) will be established between each peer when traffic matching the permit rule is received by the crypto module on the WiNG device. Each IPsec SA is bi-directional and can support traffic from for multiple hosts. Traffic matching additional permit rules will establish additional IPsec SAs as required.

The number of IPsec SAs that are established can be potentially minimized if required when contiguous blocks of addresses reside at each site. For example consider if traffic at site 1 with networks 192.168.10.0/24 and 192.168.11.0/24 and site 2 with networks 192.168.20.0/24 and 192.168.21.0/24. If permit rules were defined for each network up to four IPsec SAs could be established between the peers (one per source / destination pair). Alternatively you can create a single permit rule at each site using a /23 mask which will reduce the rule complexity in each IP ACL but also reduce the number of IPsec SAs that can be established between each peer.

The following provides example IP ACLs and rules for a three site hub and spoke deployment for traffic that needs to be protected between the hub and spoke sites. The hub site consists of two /24 networks (192.168.10.0/24 and 192.168.11.0/24) which needs to communicate with two /24 networks at the spoke 1 site (192.168.20.0/24 and 192.168.21.0/24) and two /24 networks at the spoke 2 site (192.168.30.0/24 and 192.168.31.0/24). Using the native /24 mask length for each permit rule results in four rules being required per ACL and two IPsec SAs being established per site:

IP Access List Example – Hub

```
ip access-list SPOKE1
 permit ip 172.16.10.0/24 172.16.20.0/24 rule-precedence 10
 permit ip 172.16.10.0/24 172.16.21.0/24 rule-precedence 11
 permit ip 172.16.11.0/24 172.16.20.0/24 rule-precedence 20
 permit ip 172.16.11.0/24 172.16.21.0/24 rule-precedence 21
```

```
ip access-list SPOKE2
 permit ip 172.16.10.0/24 172.16.30.0/24 rule-precedence 10
 permit ip 172.16.10.0/24 172.16.31.0/24 rule-precedence 11
 permit ip 172.16.11.0/24 172.16.30.0/24 rule-precedence 20
 permit ip 172.16.11.0/24 172.16.31.0/24 rule-precedence 21
```

IP Access List Example – Spoke 1

```
ip access-list HUB
 permit ip 172.16.20.0/24 172.16.10.0/24 rule-precedence 10
 permit ip 172.16.20.0/24 172.16.11.0/24 rule-precedence 10
 permit ip 172.16.21.0/24 172.16.10.0/24 rule-precedence 10
 permit ip 172.16.21.0/24 172.16.11.0/24 rule-precedence 10
```

IP Access List Example – Spoke 2

```
ip access-list HUB
 permit ip 172.16.30.0/24 172.16.10.0/24 rule-precedence 10
 permit ip 172.16.30.0/24 172.16.11.0/24 rule-precedence 10
 permit ip 172.16.31.0/24 172.16.10.0/24 rule-precedence 10
 permit ip 172.16.31.0/24 172.16.11.0/24 rule-precedence 10
```

The following provides example IP ACLs and rules which have be optimized for the above example. As the /24 networks at each site are contiguous, the number of rules per ACL has been reduced to one greatly simplifying the IP ACLs at each site. Additionally as a result of the ACL reduction the number IPsec SAs between each site has also been reduced to one:

IP Access List Example – Hub

```
ip access-list SPOKE1
 permit ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
```

```
ip access-list SPOKE2
 permit ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
```

IP Access List Example – Spoke 1

```
ip access-list HUB
 permit ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
```

IP Access List Example – Spoke 2

```
ip access-list HUB
 permit ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
```

*Note: When tunneling traffic destined to the public Internet, the ACL rules must use the wildcard **any** as the destination host will be unknown. The IP ACL remote site must include a permit rule with the destination network set to **any** while the hub site (where the Internet service resides) must include a permit rule with the source network set to **any**.*

1.2.5 Crypto Maps

Crypto Maps are assigned to public switched virtual interfaces (SVIs) and are used to select the IP packets that need to be protected (IP ACL), determines how the IP packets are protected (Transform Set) and which peer the traffic needs to be forwarded to (IKEv1 or IKEv2 Peer).

The following table provides an overview of the crypto map parameters and default values. Crypto Maps can be defined in supported devices profiles or directly to supported devices as overrides. Each Crypto Map entry includes a name and sequence ID allowing a single Crypto Map on an SVI to support multiple IPsec peers protecting traffic using common or different security and authentication algorithms:

Profile / Device Syntax
`crypto map <name> <1-1000> <ipsec-isakmp|ipsec-manual>`

Parameter	Description
`local-endpoint-ip <ip-address>`	Advanced parameter that allows you to specify a specific IPv4 address as the tunnel endpoint address instead of the switched virtual interface (SVI) address.
`peer <1-3> <ikev1|ikev2> <ike-peer-name>`	Assigns one or more IKE peers to the crypto map. For high-availability up to three peers can be defined. The first peer is always preferred until it becomes unreachable.
`pfs <2|5|14>`	When enabled Perfect Forward Security (PFS) ensures that if an attacker breaks a key the attacker is not able to derive any other key. When enabled an attacked will need to break each IPsec SA individually. WiNG 5 supports the following Diffie Hellman primes modulas groups: ▪ 2 – Diffie Hellman Group 2 (1024-bit) ▪ 5 – Diffie Hellman Group 5 (1536-bit) ▪ 14 – Diffie Hellman Group 14 (2048-bit)
`security-association inactivity-timeout <120-86440>`	Defines the IPsec security association (SA) inactivity timeout value in seconds. This is used to determine how long the IPsec SA is maintained when no traffic is detected. Default value is ***900*** seconds.
`security-association lifetime seconds <120-86400>|kilobytes <500-2147483646>`	Overrides the global security association (SA) lifetime in seconds before the IPsec SA is expired. Default global lifetime is ***3,600*** seconds and ***4,608,000*** bytes.
`security-association level perhost`	Specifies that separate IPsec security associations (SAs) are requested for each source/destination host pair. Disabled by default.
`transform-set <transform-set-name>`	Assigns the transform set to the crypto map which determines the algorithms used to secure the IP packets between the peers.
`use ip-access-list <ip-acl-name>`	Assigns the IP Access Control List (ACL) to the crypto map which determines which traffic is secured between the peers.

Table 1.2.5 – Transform Set Parameters

The specific Crypto Map configuration for each device will depend on the number of peers and the encryption and authentication algorithms that need to be supported. For example the hub and spoke deployment covered in section 2 uses a single Crypto Map entry per site where the hub site uses a single IKE Peer (wildcard peer IP address) and IP ACL for all spoke sites.

Alternatively individual Crypto Maps with separate IKE Peers and IP ACLs may be deployed if each site requires different credentials or requires different security and authentication algorithms. This may be required if site-to-site IPsec VPN tunnels need to be established to legacy or third-party devices.

The following provides example Crypto Maps for a two-site deployment where each peer supports encryption and authentication algorithms. In this example the device at the spoke 1 site supports AES 256 bit encryption while due to certain constraints the device at the spoke 2 site can only support triple DES (3DES) encryption. The Crypto Map for each site shares a common name but unique sequence ID. The Crypto Map name is then assigned to the public SVI on each device where the IKE and IPsec SAs will be established:

Crypto Map Example – Hub (Profile or Device)

```
crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list SPOKE1
  peer 1 ikev2 SPOKE1
  transform-set ESP-AES-256-SHA1
crypto map IPSEC 2 ipsec-isakmp
  use ip-access-list SPOKE2
  peer 1 ikev2 SPOKE2
  transform-set ESP-3DES-SHA1
```

Crypto Map Example – Spoke1 (Profile or Device)

```
crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list HUB
  peer 1 ikev2 HUB
  transform-set ESP-AES-256-SHA1
```

Crypto Map Example – Spoke2 (Profile or Device)

```
crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list HUB
  peer 1 ikev2 HUB
  transform-set ESP-3DES-SHA1
```

2. Configuration Example

2.1 Site-to-Site IPsec VPN Example (IKEv1 or IKEv2)

For this scenario site-to-site IPsec VPN tunnels using IKEv1 or IKEv2 will be established form two remote branch sites to a main headquarter site. Each site has an RFS X000 Wireless Controller deployed that provides Wireless LAN, IP routing, NAT and firewall services for each site. The headquarters site is statically addressed while the remote branch sites obtain dynamic IP addressing from their service providers. Each branch site will initiate a site-to-site IPsec VPN tunnel to the main headquarters site when hosts at each branch attempt to access hosts at the headquarters site.

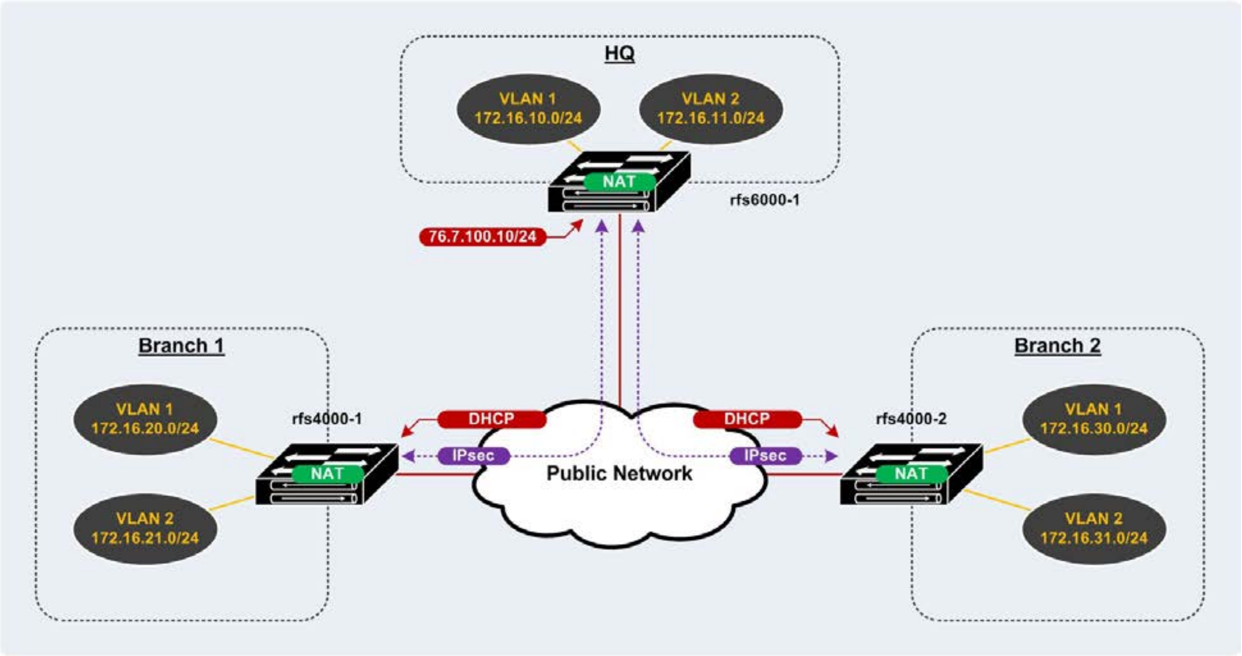

Figure 2.1 – Site-to-Site IPsec VPN Example Topology

2.1.1 Configuration Steps

The following section provides an overview of the configuration parameters, peers and policies required to create site-to-site IPsec VPN tunnels in WiNG 5.3 and higher. All the configuration parameters can be assigned to the device profile or directly to individual devices as overrides.

A site-to-site IPsec VPN tunnel requires an IKE policy, IKE Peer, Transform Set, IP Access Control List (ACL) and Crypto Map to be defined. The following steps are required to establish a site-to-site IPsec VPN tunnel on a WiNG 5 device:

1. Create a user defined IKEv1/IKEv2 Policy or use the default IKEv1/IKEv2 Policy.
2. Create IKEv1/IKEv2 Peer(s).
3. Create a user defined Transform Set or use the default Transform Set.
4. Create an IP Access Control List (ACL) and rules.
5. Create a Crypto Map referencing the ACL, IKE Peer and Transform Set.
6. Assign the Crypto Map to a public Switched Virtual Interface (SVI).

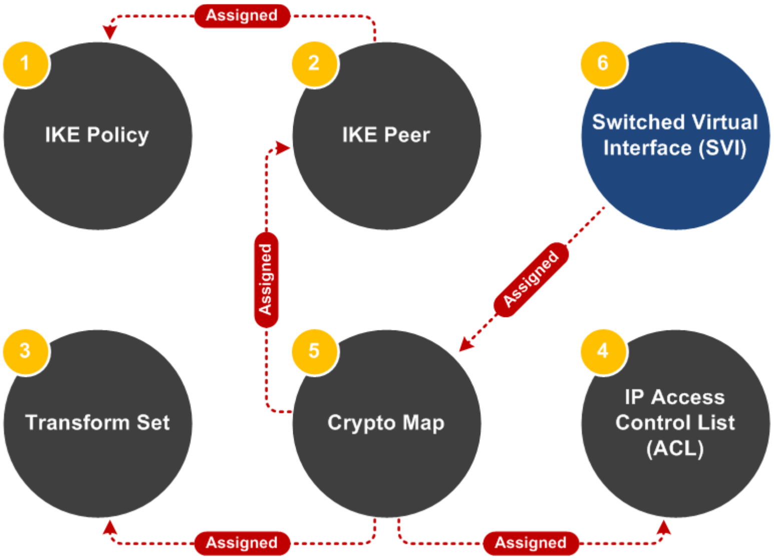

Figure 2.1.1 – Site-to-Site IPsec VPN Configuration Steps

2.1.2 Internet IP Access Control List (ACL)

Each site includes an IP Access Control List (ACL) named ***INTERNET-IN*** which is applied to all inbound traffic received by the RFS X000 Controllers public switched virtual interfaces (SVI). The IP ACL includes rules that permits IKE, NAT-T and ESP protocols but denies and logs all other inbound traffic. The IP ACLs ensure that only inbound IPsec traffic can be received by the interface:

HQ, Branch 1 and Branch 2

```
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
```

2.1.3 Network Address Translation (NAT)

Each RFS X000 Controller is directly connected to the Internet and is configured to provide many-to-one NAT translation to provide hosts at each site access the Internet. The NAT rule on each device references an IP Access Control List (ACL) named ***NAT*** that determines which internal traffic is NATed to the public switched virtual interface (SVI) on each device. As site-to-site IPsec VPN tunnels are also being deployed, special rules need to be applied to each ACL so that traffic destined to the IPsec VPN tunnel is excluded from being NATed to the Internet.

For this example each site includes two contiguous networks which are NATed to the public Internet. As the networks at each site are contiguous, the networks at each site will be summarized into a single /23 block to reduce the number of permit rules required for each IP ACL:

- HQ - 172.16.10.0/24 and 172.16.11.0/24 (summarized as 172.16.10.0/23)
- Branch 1 – 172.16.20.0/24 and 172.16.21.0/24 (summarized as 172.16.20.0/23)
- Branch 2 – 172.16.30.0/24 and 172.16.31.0/24 (summarized as 172.16.30.0/23)

Note: As the networks at each site are contiguous, the IP Access Control list entries use summarized addresses to reduce the number of permit and deny rules required in each Access Control List. In this example each site has two contiguous /24 networks which are summarized as a single /23 network.

2.1.3.1 IP Access Control Lists (ACLs)

The RFS X000 Controller in the HQ is assigned an IP Control Access List (ACL) named ***NAT*** that includes two deny statements that ignores IPsec VPN traffic from the 172.16.10.0/23 (HQ) networks destined to the remote 172.16.20.0/23 (Branch 1) and 172.16.30.0/23 (Branch 2) networks. The ACL also includes a permit statement allowing internal host traffic from the 172.16.10.0/23 (HQ) networks to be NATed to the Internet:

HQ

```
!
ip access-list NAT
 deny ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 deny ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
 permit ip 172.16.10.0/23 any rule-precedence 100
!
```

The RFS X000 Controller in Branch 1 is assigned an IP Control Access List (ACL) named ***NAT*** that includes one deny statement that ignores IPsec VPN traffic from 172.16.20.0/23 (Branch 1) networks destined to the 172.16.10.0/23 (HQ) networks. The ACL also includes a permit statement allowing internal host traffic from the 172.16.20.0/23 (Branch 1) networks to be NATed to the Internet:

Branch 1

```
!
ip access-list NAT
 deny ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.20.0/23 any rule-precedence 100
!
```

The RFS X000 Controller in Branch 2 is assigned an IP Control Access List (ACL) named ***NAT*** that includes one deny statement that ignores IPsec VPN traffic from 172.16.30.0/23 (Branch 2) networks destined to the 172.16.10.0/23 (HQ) networks. The ACL also includes a permit statement allowing internal host traffic from the 172.16.30.0/23 (Branch 2) networks to be NATed to the Internet:

Branch 2

```
!
ip access-list NAT
 deny ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.30.0/23 any rule-precedence 100
!
```

2.1.3.2 Switched Virtual Interfaces (SVIs)

For NAT to function on an RFS X000 Controller, each switched virtual interface (SVI) must be defined as a NAT inside or outside interface. In this deployment each RFS X000 Controller has two internal SVIs for internal traffic (VLAN 1 and VLAN 2) and a public SVI (VLAN 4094) which connects each RFS X000 Controller to the public Internet. The designation of each SVI as a NAT inside or outside determines how the traffic is processed and translated by the NAT module.

Each public SVI (VLAN 4094) is also assigned the IP Control Access List (ACL) named ***INTERNET-IN*** which is applied to all inbound traffic. The ACL permits IKE and IPsec traffic but denies and logs all other inbound traffic. As the WiNG 5 firewall is fully stateful aware, all outbound traffic (and the associated return flows) will be permitted.

Note: All SVIs in this example are assigned directly to each devices configuration as overrides.

The RFS X000 Controller in the HQ has two internal SVIs (VLAN 1 and VLAN 2) defined with the static IP addresses 172.16.10.1/24 and 172.16.11.1/24 marked as NAT inside interfaces. In addition the RFS X000 Controller has a public SVI (VLAN 4094) with the static IP address 76.7.100.10/24 which is marked as a NAT outside interface. When the NAT rule is defined, traffic received by the NAT inside interfaces destined to the public Internet will be NATed to the static public IP address assigned to the NAT outside interface:

HQ

```
!
interface vlan1
  ip address 172.16.10.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.11.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address 76.7.100.10/24
  use ip-access-list in INTERNET-IN
  ip nat outside
!
```

The RFS X000 Controller in Branch 1 has two internal SVIs (VLAN 1 and VLAN 2) defined with the static IP addresses 172.16.20.1/24 and 172.16.21.1/24 marked as NAT inside interfaces. In addition the RFS X000 Controller has a public SVI (VLAN 4094) configured to dynamically obtain IP addressing from the ISP. When the NAT rule is defined, traffic received by the NAT inside interfaces destined to the public Internet will be NATed to the dynamic public IP address assigned to the NAT outside interface:

Branch 1:

```
!
interface vlan1
  ip address 172.16.20.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.21.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
!
```

The RFS X000 Controller in Branch 2 has two internal SVIs (VLAN 1 and VLAN 2) defined with the static IP addresses 172.16.30.1/24 and 172.16.31.1/24 marked as NAT inside interfaces. In addition the RFS X000 Controller has a public SVI (VLAN 4094) configured to dynamically obtain IP addressing from the ISP. When the NAT rule is defined, traffic received by the NAT inside interfaces destined to the public Internet will be NATed to the dynamic public IP address assigned to the NAT outside interface:

Branch 2

```
!
interface vlan1
  ip address 172.16.30.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.31.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
```

2.1.3.3 NAT Rule (Profile or Override)

Each RFS X000 Controller has a many-to-one NAT rule defined that translates RFC 1918 private addresses assigned to the internal networks to static or dynamic IP address on the public SVI. Traffic destined to the Internet from each site will appear to originate from the public IP address assigned to each RFS X000 Controller. The RFC 1918 private IP addresses used on the internal networks at each site will be unreachable and hidden from the public Internet.

The NAT rule on each device references the IP Access Control List (ACL) named ***NAT*** which determines which traffic is translated to the public SVI and which traffic (i.e. IPsec) is ignored. The ACL rules tell the RFS X000 Controller to translate internal traffic destined to the Internet to the Controllers public SVI while ignoring traffic that is destined to the IPsec VPN tunnel.

Note: The NAT rules in this example are assigned directly to each devices configuration as overrides.

HQ, Branch 1 and Branch 2

```
!
ip nat inside source list NAT interface vlan4094 overload
!
```

2.1.4 IPsec

Each RFS X000 Controller is configured to support site-to-site IPsec VPN tunnels allowing hosts on the Branch 1 and Branch 2 sites to communicate with the centralized services at the HQ. The RFS X000 Controller in the HQ is assigned a static public IP address which terminates the remote IPsec VPN tunnels initiated from the RFS X000 Controllers at the Branch 1 and Branch 2 sites. Hosts in the Branch 1 and Branch 2 sites will be able to communicate with hosts in the HQ (and vice versa), however hosts in Branch 1 and Branch 2 will not be able to communicate as no IPsec VPN tunnel will be established between the branch sites.

The IPsec VPN tunnels in this example will utilize default WiNG 5 global values as well as the default IKE policies and transform sets. Additionally each peer will utilize pre-shared key authentication using a common pre-shared key.

2.1.4.1 IPsec Access Control Lists (ACLs)

Each site includes an IP Access Control list named ***IPSEC*** to determine which IP traffic is to be encapsulated and forwarded over the IPsec VPN tunnel. Each IP ACL includes the necessary permit rules that match the source and destination host(s) / network(s) for the traffic that is to be protected by the RFS X000 Controller at each site. IPv4 traffic that does not match a permit rule is ignored and will not be secured by the IPsec VPN tunnel.

Note: As the networks at each site are contiguous, the IP Access Control list entries use summarized addresses to reduce the number of permit rules required in each IP ACL and reduce the number of overall IPsec security associations established between sites. In this example each site has two contiguous /24 networks which are summarized as a single /23 network.

The RFS X000 Controller in the HQ is assigned an IP Control Access List (ACL) named ***IPSEC*** that includes two permit statements that matches traffic from the 172.16.10.0/23 (HQ) networks destined to the remote 172.16.20.0/23 (Branch 1) and 172.16.30.0/23 (Branch 2) networks:

HQ

```
!
ip access-list IPSEC
 permit ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 permit ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
!
```

The RFS X000 Controller in Branch 1 is assigned an IP Control Access List (ACL) named ***IPSEC*** that includes one permit statement that matches traffic from the 172.16.20.0/23 (Branch 1) networks destined to the remote 172.16.10.0/23 (HQ) networks:

Branch 1

```
!
ip access-list IPSEC
 permit ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
!
```

The RFS X000 Controller in Branch 2 is assigned an IP Control Access List (ACL) named ***IPSEC*** that includes one permit statement that matches traffic from the 172.16.30.0/23 (Branch 2) networks destined to the remote 172.16.10.0/23 (HQ) networks:

Branch 2

```
!
ip access-list IPSEC
 permit ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
!
```

2.1.4.2 IKE Policies (Profile or Override)

By default WiNG 5.3 and above includes a default IKEv1 policy named ***ikev1-default*** and an IKEv2 policy named ***ikev2-default*** assigned to each supported platforms profile. Each IKE policy includes a default proposal that supports 256 bit AES encryption, Diffie Hellman Group 2 key exchange and SHA1 authentication.

The default IKE policies will be utilized by the RFS X000 Controllers in the HQ, Branch 1 and Branch 2 sites to authenticate the remote peers, exchange cryptographic keys and establish the IPsec security associations (SAs). As both policies are pre-defined by default, no additional configuration is required unless the values of the default proposal need to be modified or a user defined IKE policy is preferred.

2.1.4.2.1 Default IKEv1 Policy

The following provides an example of the default IKEv1 policy (including default values) which is assigned to each supported WiNG 5 devices profile by default. A user defined IKEv1 policy can also be defined and assigned to each supported devices profile or directly to each device as an override:

HQ, Branch 1 and Branch 2

```
!
crypto ikev1 policy ikev1-default
  dpd-keepalive 30
  dpd-retries 5
  lifetime 86400
  isakmp-proposal default encryption aes-256 group 2 hash sha
  mode main
!
```

2.1.4.2.2 Default IKEv2 Policy

The following provides an example of the default IKEv2 policy (including default values) which is assigned to each supported WiNG 5 devices profile by default. A user defined IKEv2 policy can also be defined and assigned to each supported devices profile or directly to each device as an override:

HQ, Branch 1 and Branch 2

```
!
crypto ikev2 policy ikev2-default
  dpd-keepalive 30
  lifetime 86400
  isakmp-proposal default encryption aes-256 group 2 hash sha
!
```

2.1.4.3 IKE Peers (Profile or Override)

Each RFS X000 Controller will have an IKEv1 or IKEv2 peer named ***IPSEC*** defined which determines the IP address of the remote peer, the pre-shared key used for authentication and the IKE policy used for the security association and key exchange.

In this example the Branch 1 and Branch 2 sites are dynamically addressed and will initiate the IPsec VPN tunnel to the HQ which has a fixed public IP address. As the IP addresses for the Branch 1 and Branch 2 sites are unknown, the HQ cannot initiate the tunnel to the Branch 1 or Branch 2 sites.

For this configuration example an IKEv1 or IKEv2 peer needs to be defined on each RFS X000 Controller and examples will be provided for each. The IKE peers can either be assigned to the device profile or directly to each device as an override.

Note: For this configuration example either an IKEv1 or IKEv2 peer should be defined but not both. As a best practice it’s recommended that IKEv2 peers be defined for deployments consisting of all WiNG 5.3 or higher devices. IKEv1 peers should only be defined to support environments with legacy WiNG or third-party devices which can only support IKEv1.

2.1.4.3.1 IKEv1 Peer Example

The RFS X000 Controller in the HQ has a single IKEv1 peer defined with a wildcard IP address ***0.0.0.0*** to support the dynamically addressed Branch 1 and Branch 2 sites. The Branch 1 and Branch 2 sites will initiate the security association to the HQ to establish the IPsec VPN tunnel. The IKEv1 peer will define a common pre-shared-key ***hellomoto*** for authentication and will utilize the default IKEv1 policy:

HQ

```
!
crypto ikev1 peer IPSEC ip
  address 0.0.0.0 authentication
  psk 0 hellomoto
  use ikev1-policy ikev1-default
!
```

The RFS X000 Controllers in Branch 1 and Branch 2 have a single IKEv1 peer defined with the peer IP address set to the RFS X000 Controller in the HQ public IP address (***76.7.100.10***). The IKEv1 peer will define a common pre-shared-key ***hellomoto*** for authentication and will utilize the default IKEv1 policy:

Branch 1 and Branch 2

```
!
crypto ikev1 peer IPSEC ip
  address 76.7.100.10
  authentication psk 0 hellomoto
  use ikev1-policy ikev1-default
!
```

Note: In this example the Branch 1 and Branch 2 sites utilize dynamic IP addresses on their public SVI interfaces; as such a common pre-shared key must be employed across all sites. If each site is assigned a static public IP address, separate peer entries and pre-shared keys can be deployed for each site.

2.1.4.3.2 IKEv2 Peer Example

The RFS X000 Controller in the HQ has a single IKEv2 peer defined with a wildcard IP address ***0.0.0.0*** to support the dynamically addressed Branch 1 and Branch 2 sites. The Branch 1 and Branch 2 sites will initiate the security association to the HQ to establish the IPsec VPN tunnel. The IKEv2 peer will define a common pre-shared-key ***hellomoto*** for authentication and will utilize the default IKEv2 policy:

HQ

```
!
ip address 0.0.0.0
  no remoteid
  no localid
  authentication psk 0 hellomoto local
  authentication psk 0 hellomoto remote
  use ikev2-policy ikev2-default
!
```

The RFS X000 Controllers in Branch 1 and Branch 2 have a single IKEv2 peer defined with the peer IP address set to the RFS X000 Controller in the HQ public IP address (***76.7.100.10***). The IKEv2 peer will define a common pre-shared-key ***hellomoto*** for authentication and will utilize the default IKEv2 policy:

Branch 1 and Branch 2

```
!
crypto ikev2 peer IPSEC
  ip address 76.7.100.10
  no remoteid
  no localid
  authentication psk 0 hellomoto local
  authentication psk 0 hellomoto remote
  use ikev2-policy ikev2-default
!
```

Note: In this example the Branch 1 and Branch 2 sites utilize dynamic IP addresses on their public SVI interfaces; as such a common pre-shared key must be employed across all sites. If each site is assigned a static public IP address, separate peer entries and pre-shared keys can be deployed for each site.

2.1.4.4 Transform Set (Profile or Override)

Each WiNG 5 supporting IPsec includes a default transform set named ***default***. The default transform set supports ESP with 256 bit AES encryption, SHA authentication and tunnel encapsulation.

The default transform set will be utilized by the RFS X000 Controllers in the HQ, Branch 1 and Branch 2 sites to secure the IP packets forwarded to the HQ. As the transform set is pre-defined by default, no additional configuration is required unless the encryption and authentication values need to be modified which requires a user defined transform set to be assigned.

HQ, Branch 1 and Branch 2

```
!
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  mode tunnel
!
```

2.1.4.5 Crypto Map (Profile or Override)

Each RFS X Controller will have a crypto map defined named ***IPSEC*** that will be assigned to each Controllers public SVI (VLAN 4094). In this example each crypto map will include a single entry (sequence 1) as only one peer entry resides on each device. Each crypto map includes:

1. The IP Access Control List (ACL) name that determines which IP packets are to be protected by each device.
2. The IKEv1 *OR* IKEv2 peer name used to establish the security associations and key exchange.
3. The transform set that determines how the IP packets are secured between the sites.

2.1.4.5.1 IKEv1 Crypto Map Example

The following provides an example crypto map named ***IPSEC*** using the ACL named ***IPSEC***, IKEv1 peers named ***IPSEC*** and the transform set named ***default***:

HQ, Branch 1 and Branch 2

```
!
crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev1 IPSEC
  transform-set default
!
```

2.1.4.5.2 IKEv2 Crypto Map Example

The following provides an example crypto map named ***IPSEC*** using the ACL named ***IPSEC***, IKEv2 peers named ***IPSEC*** and the transform set named ***default***:

HQ, Branch 1 and Branch 2

```
!
crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev2 IPSEC
  transform-set default
!
```

2.1.4.6 Switched Virtual Interfaces

The crypto map named ***IPSEC*** is assigned to each of the RFS X000 Controllers public SVI (VLAN 4094) for which the IPsec VPN tunnel is terminated on. Crypto maps can be assigned to a switched virtual interface (SVI) using the device profile or directly to the device as an override:

HQ

```
!
interface vlan4094
  description PUBLIC
  ip address 76.7.100.10/24
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
!
```

Branch 1 and Branch 2

```
!
interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
!
```

2.1.4.7 Crypto Scope (Profile or Override)

To permit remote management access into the RFS X000 Controllers at each site, the ***plain-text-deny-acl-scope*** parameter must be changed from ***global*** to ***interface***. While the default value will not affect the operation of the IPsec VPN tunnel it will restrict which devices are able to manage the RFS X000 Controllers at each site. The crypto scope can be modified device profile or directly on the device as an override:

HQ, Branch 1 and Branch 2

```
!
crypto plain-text-deny-acl-scope interface
!
```

2.2 Verification

The following section provides an overview of the steps required to validate IKE and IPsec operation of the configuration outlined in the previous section. It’s important to note that the IPsec security associations (SAs) will only be established if active traffic from the branch or hub site is being forwarded.

Note: You can optionally maintain active IPsec security associations (SAs) by enabling Critical Resource Monitoring (CRM) on one or more Access Points at the remote site. CRM can be configured to monitor one or more devices through the IPsec VPN tunnel which will ensure the IPsec SAs between each site are maintained when no host traffic is present at the site.

2.2.1.1 IKE Security Associations

In this example the remote RFS X000 Controllers will automatically establish IKE security associations (SA) to the RFS X000 Controller at the hub site. An IPsec SA cannot be established between peers until an IKE SA has been formed. If the IKE SA is not present, the configuration on each device needs to be verified.

The following CLI command displays the active IKE SAs on the RFS X000 Controllers deployed at the hub and branch sites. In this example the two branch peers have successfully established an IKEv2 SA to the hub site. The hub site will display two IKE SAs while each branch will display a single IKE SA. Note that the IKE version, peer and local address information is provided as well as the encryption, hashing and keying algorithms used by each SA:

HQ

```
rfs6000# show crypto ike sa
```

```
--------------------------------------------------------------------------------
IKE VERSION      : IKEv2
Peer Address     : 76.7.100.254      Local Address   : 76.7.100.10
Encryption Algo  : AES_CBC_256
Hash Algo        : HMAC_SHA1_96
DH Group         : MODP_1024
IKE Lifetime     : 23 Hrs 58 Mins 17 Secs
IKE State        : ESTABLISHED
--------------------------------------------------------------------------------
IKE VERSION      : IKEv2
Peer Address     : 76.7.100.252      Local Address   : 76.7.100.10
Encryption Algo  : AES_CBC_256
Hash Algo        : HMAC_SHA1_96
DH Group         : MODP_1024
IKE Lifetime     : 23 Hrs 58 Mins 12 Secs
IKE State        : ESTABLISHED
--------------------------------------------------------------------------------
```

Branch 1

```
rfs4000-1# show crypto ike sa
```

```
-------------------------------------------------------------------------------
IKE VERSION     : IKEv2
Peer Address    : 76.7.100.10      Local Address   : 76.7.100.254
Encryption Algo : AES_CBC_256
Hash Algo       : HMAC_SHA1_96
DH Group        : MODP_1024
IKE Lifetime    : 23 Hrs 57 Mins 55 Secs
IKE State       : ESTABLISHED
-------------------------------------------------------------------------------
```

Branch 2

```
rfs4000-2# show crypto ike sa
```

```
-------------------------------------------------------------------------------
IKE VERSION     : IKEv2
Peer Address    : 76.7.100.10      Local Address   : 76.7.100.252
Encryption Algo : AES_CBC_256
Hash Algo       : HMAC_SHA1_96
DH Group        : MODP_1024
IKE Lifetime    : 23 Hrs 59 Mins 46 Secs
IKE State       : ESTABLISHED
-------------------------------------------------------------------------------
```

2.2.1.2 IPsec Security Associations (SAs)

The following CLI command displays the active IPsec SAs on the RFS X000 Controllers deployed at the hub and branch sites. It’s important to note that the number of IPsec SAs will vary depending on the permit rules defined in the IP Access Control Lists (ACLs) at each site. Additionally the IPsec SAs will only be established if hosts at the branch sites are attempting to access resources at the headquarters site. The IPsec SAs will not establish if not traffic is present on the network!

In this configuration example each site has two /24 networks which have been summarized into a single /23 network. As such a single IPsec SA will be established between each site where the hub site will display two IPsec SAs and each branch site will display a single IPsec SA. If each of the /24 networks was defined separately as permit rules in the IP ACLs, a potential of four IPsec SAs would be established between each site (one IPsec SA per source / destination network):

HQ

```
rfs6000# show crypto ipsec sa
```

```
-----------------------------------------------------------------------------
Peer Address        : 76.7.100.253    Local Address       : 76.7.100.10
Protocol            : ESP
SPI In              : C5015CAE        SPI Out             : C08A4CAE
Encryption Algo     : AES-CBC-256     MAC Algo            : HMAC-SHA1-96
Mode                : tunnel
Lifetime configured : 1 Hrs 0 Mins 0 Secs, 4608000 KBytes
Lifetime Remaining  : 0 Hrs 57 Mins 30 Secs, 4607999 KBytes
-----------------------------------------------------------------------------
Peer Address        : 76.7.100.254    Local Address       : 76.7.100.10
Protocol            : ESP
SPI In              : CCC09CAA        SPI Out             : C5212CAE
Encryption Algo     : AES-CBC-256     MAC Algo            : HMAC-SHA1-96
Mode                : tunnel
Lifetime configured : 1 Hrs 0 Mins 0 Secs, 4608000 KBytes
Lifetime Remaining  : 0 Hrs 57 Mins 4 Secs, 4607997 KBytes
----------------------------------------------------------------------------------
```

Branch 1

```
rfs4000-1# show crypto ipsec sa
```

```
-----------------------------------------------------------------------------
Peer Address        : 76.7.100.10     Local Address       : 76.7.100.254
Protocol            : ESP
SPI In              : C5212CAE        SPI Out             : CCC09CAA
Encryption Algo     : AES-CBC-256     MAC Algo            : HMAC-SHA1-96
Mode                : tunnel
Lifetime configured : 1 Hrs 0 Mins 0 Secs, 4608000 KBytes
Lifetime Remaining  : 0 Hrs 56 Mins 28 Secs, 4607997 KBytes
----------------------------------------------------------------------------------
```

Branch 2

```
rfs4000-2# show crypto ipsec sa
```

```
--------------------------------------------------------------------------------
Peer Address        : 76.7.100.10     Local Address       : 76.7.100.253
Protocol            : ESP
SPI In              : C08A4CAE        SPI Out             : C5015CAE
Encryption Algo     : AES-CBC-256     MAC Algo            : HMAC-SHA1-96
Mode                : tunnel
Lifetime configured : 1 Hrs 0 Mins 0 Secs, 4608000 KBytes
Lifetime Remaining  : 0 Hrs 56 Mins 43 Secs, 4607999 KBytes
-------------------------------------------------------------------------------------
```

3. Appendix

3.1 Configuration File Examples

3.1.1 Site-to-Site IPsec VPN (IKEv1)

rfs6000-1 - HQ

```
!
! Configuration of RFS6000 version 5.4.1.0-020R
!
!
version 2.1
!
!
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 permit ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
!
ip access-list NAT
 deny ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 deny ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
 permit ip 172.16.10.0/23 any rule-precedence 100
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
```

```
!
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.10.0/24
  address range 172.16.10.100 172.16.10.254
  domain-name tmelabs.local
  default-router 172.16.10.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.11.0/24
  address range 172.16.11.100 172.16.11.254
  domain-name tmelabs.local
  default-router 172.16.11.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs6000 default-rfs6000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge6
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge7
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge8
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
!
```

```
rf-domain default
 no country-code
!
rfs6000 00-23-68-64-43-5A
 use profile default-rfs6000
 use rf-domain default
 hostname rfs6000-1
 license AP <string>
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 crypto ikev1 peer IPSEC ip
  address 0.0.0.0 authentication
  psk 0 hellomoto use ikev1-
  policy ikev1-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev1 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface me1
  ip address 192.168.0.1/24
 interface ge7
  switchport mode access
  switchport access vlan 4094
 interface ge8
  switchport mode access
  switchport access vlan 4094
 interface vlan1
  ip address 172.16.10.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.11.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address 76.7.100.10/24
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload
!
!
End
```

rfs4000-1 – Branch 1

```
!
! Configuration of RFS4000 version 5.4.1.0-020R
!
!
version 2.1
!
!
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
!
ip access-list NAT
 deny ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.20.0/23 any rule-precedence 100
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
```

```
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.20.0/24
  address range 172.16.20.100 172.16.20.254
  domain-name tmelabs.local
  default-router 172.16.20.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.21.0/24
  address range 172.16.21.100 172.16.21.254
  domain-name tmelabs.local
  default-router 172.16.21.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface radio1
 interface radio2
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 router ospf
!
rf-domain default
 no country-code
!
rfs4000 00-23-68-22-9D-E4
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 crypto ikev1 peer IPSEC ip
  address 76.7.100.10
  authentication psk 0 hellomoto
  use ikev1-policy ikev1-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev1 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface ge5
  description PUBLIC
  switchport mode access
  switchport access vlan 4094
 interface vlan1
  ip address 172.16.20.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.21.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload
!
!
End
```

rfs4000 – Branch 2

```
!
! Configuration of RFS4000 version 5.4.1.0-020R
!
!
version 2.1
!
!
ip access-list INTERNET-IN
```

```
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
!
ip access-list NAT
 deny ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.30.0/23 any rule-precedence 100
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.30.0/24
  address range 172.16.30.100 172.16.30.254
  domain-name tmelabs.local
  default-router 172.16.30.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.31.0/24
  address range 172.16.31.100 172.16.31.254
  domain-name tmelabs.local
  default-router 172.16.31.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface radio1
 interface radio2
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 router ospf
!
rf-domain default
 no country-code
!
rfs4000 5C-0E-8B-1A-FE-A0
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-2
 license AP DEFAULT-6AP-LICENSE
 crypto ikev1 peer IPSEC ip
  address 76.7.100.10
  authentication psk 0 hellomoto
  use ikev1-policy ikev1-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev1 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface ge5 description
  PUBLIC switchport mode
  access switchport access
  vlan 4094
 interface vlan1
  ip address 172.16.30.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.31.1/24
  ip nat inside
 interface vlan4094
```

```
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload
!
!
end
```

3.1.2 Site-to-Site IPsec VPN (IKEv2)

rfs6000-1 - HQ

```
!
! Configuration of RFS6000 version 5.4.1.0-020R
!
!
version 2.1
!
!
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 permit ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
!
ip access-list NAT
 deny ip 172.16.10.0/23 172.16.20.0/23 rule-precedence 10
 deny ip 172.16.10.0/23 172.16.30.0/23 rule-precedence 20
 permit ip 172.16.10.0/23 any rule-precedence 100
!
```

```
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.10.0/24
  address range 172.16.10.100 172.16.10.254
  domain-name tmelabs.local
  default-router 172.16.10.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.11.0/24
  address range 172.16.11.100 172.16.11.254
  domain-name tmelabs.local
  default-router 172.16.11.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs6000 default-rfs6000
```

```
autoinstall configuration
autoinstall firmware
crypto ikev1 policy ikev1-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ikev2 policy ikev2-default
 isakmp-proposal default encryption aes-256 group 2 hash sha
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
crypto ikev1 remote-vpn
crypto ikev2 remote-vpn
crypto auto-ipsec-secure
interface me1
interface up1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge1
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge2
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge3
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge4
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge5
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge6
 ip dhcp trust
 qos trust dscp
 qos trust 802.1p
interface ge7
 ip dhcp trust
 qos trust dscp
```

```
  qos trust 802.1p
 interface ge8
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
!
rf-domain default
 no country-code
!
rfs6000 00-23-68-64-43-5A
 use profile default-rfs6000
 use rf-domain default
 hostname rfs6000-1
 license AP <string>
 license AAP <string>
 license ADVANCED-WIPS <string>
 license ADSEC <string>
 crypto ikev2 peer IPSEC
  ip address 0.0.0.0
  authentication psk 0 hellomoto local
  authentication psk 0 hellomoto remote
  use ikev2-policy ikev2-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev2 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface me1
  ip address 192.168.0.1/24
 interface ge7
  switchport mode access
  switchport access vlan 4094
 interface ge8
  switchport mode access
  switchport access vlan 4094
 interface vlan1
```

```
  ip address 172.16.10.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.11.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address 76.7.100.10/24
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload!
!
End
```

rfs4000-1 – Branch 1

```
!
! Configuration of RFS4000 version 5.4.1.0-020R
!
!
version 2.1
!
!
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
!
ip access-list NAT
 deny ip 172.16.20.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.20.0/23 any rule-precedence 100
!
firewall-policy default
```

```
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.20.0/24
  address range 172.16.20.100 172.16.20.254
  domain-name tmelabs.local
  default-router 172.16.20.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.21.0/24
  address range 172.16.21.100 172.16.21.254
  domain-name tmelabs.local
  default-router 172.16.21.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface radio1
 interface radio2
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 router ospf
!
```

```
rf-domain default
 no country-code
!
rfs4000 00-23-68-22-9D-E4
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-1
 license AP DEFAULT-6AP-LICENSE
 crypto ikev2 peer IPSEC
  ip address 76.7.100.10
  authentication psk 0 hellomoto local
  authentication psk 0 hellomoto remote
  use ikev2-policy ikev2-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev2 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface ge5
  description PUBLIC
  switchport mode access
  switchport access vlan 4094
 interface vlan1
  ip address 172.16.20.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.21.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload
!
```

```
!
End
```

rfs4000 – Branch 2

```
!
! Configuration of RFS4000 version 5.4.1.0-020R
!
!
version 2.1
!
!
ip access-list INTERNET-IN
 permit udp any any eq 500 rule-precedence 10
 permit udp any any eq 4500 rule-precedence 20
 permit proto esp any any rule-precedence 30
 deny ip any any log rule-precedence 100
!
ip access-list IPSEC
 permit ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
!
ip access-list NAT
 deny ip 172.16.30.0/23 172.16.10.0/23 rule-precedence 10
 permit ip 172.16.30.0/23 any rule-precedence 100
!
firewall-policy default
 no ip dos tcp-sequence-past-window
!
!
mint-policy global-default
!
meshpoint-qos-policy default
!
wlan-qos-policy default
 qos trust dscp
 qos trust wmm
!
radio-qos-policy default
!
ap300 default-ap300
 interface radio1
 interface radio2
!
```

```
dhcp-server-policy default
 dhcp-pool vlan1
  network 172.16.30.0/24
  address range 172.16.30.100 172.16.30.254
  domain-name tmelabs.local
  default-router 172.16.30.1
  dns-server 208.67.220.220 208.67.222.222
 dhcp-pool vlan2
  network 172.16.31.0/24
  address range 172.16.31.100 172.16.31.254
  domain-name tmelabs.local
  default-router 172.16.31.1
  dns-server 208.67.220.220 208.67.222.222
!
!
management-policy default
 no http server
 https server
 ssh
 user admin password 0 Zebra role superuser access all
!
l2tpv3 policy default
!
profile rfs4000 default-rfs4000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface radio1
 interface radio2
 interface up1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge5
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 router ospf
!
rf-domain default
 no country-code
!
rfs4000 5C-0E-8B-1A-FE-A0
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-2
 license AP DEFAULT-6AP-LICENSE
 crypto ikev2 peer IPSEC
  ip address 76.7.100.10
  authentication psk 0 hellomoto local
  authentication psk 0 hellomoto remote
  use ikev2-policy ikev2-default
 crypto map IPSEC 1 ipsec-isakmp
  use ip-access-list IPSEC
  peer 1 ikev2 IPSEC
  security-association inactivity-timeout 900
  transform-set default
 crypto plain-text-deny-acl-scope interface
 interface ge5
  description PUBLIC
  switchport mode access
  switchport access vlan 4094
 interface vlan1
  ip address 172.16.30.1/24
  ip nat inside
 interface vlan2
  ip address 172.16.31.1/24
  ip nat inside
 interface vlan4094
  description PUBLIC
  ip address dhcp
  ip dhcp client request options all
  use ip-access-list in INTERNET-IN
  ip nat outside
  crypto map IPSEC
 use dhcp-server-policy default
 logging on
 logging console warnings
 logging buffered warnings
 ip nat inside source list NAT interface vlan4094 overload
!
!
End
```