How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel

https://campus.barracuda.com/doc/46208905/

The Barracuda NextGen Firewall F-Series can establish IPsec VPN tunnels to any standard compliant IKEv2 IPsec VPN gateway. The Site-to-Site IPsec VPN tunnel must be configured with identical settings on both F-Series Firewalls and the third-party IKEv2 IPsec gateway.

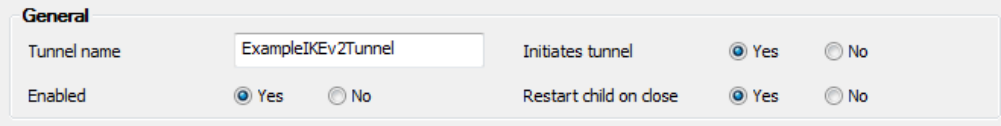
In this article:

Before You Begin

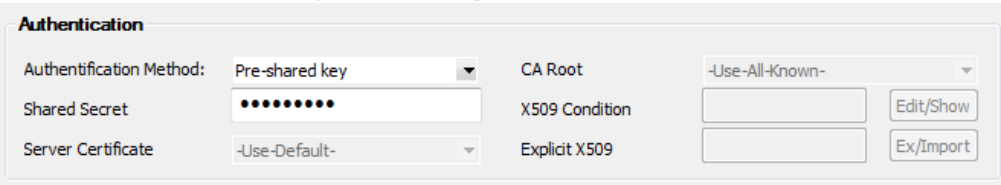
Create a VPN and Firewall service. For more information, see How to Configure Services.

Step 1. Create an IKEv2 IPsec Tunnel on the F-Series Firewall

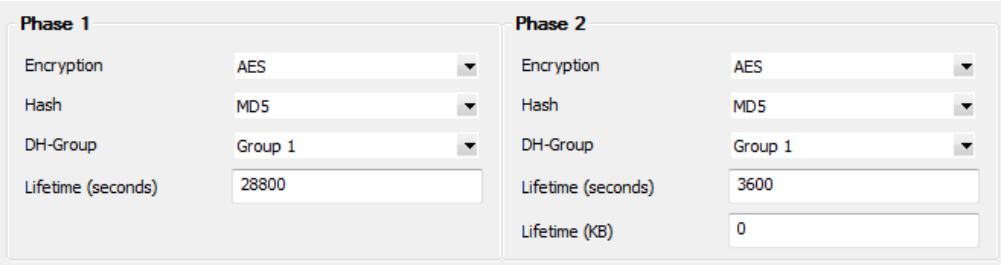
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click the **IPsec IKEv2 Tunnels** tab.
3. Click **Lock**.
4. Right-click the table and select **New IKEv2 Tunnel**. The **IKEv2 Tunnel** window opens.
5. Enter a **Tunnel Name**.
6. Set **Initiates Tunnel:**
   - **yes** – The firewall is the active unit and continuously attempts to connect to the remote VPN gateway until a VPN tunnel is established.
   - **no** – The firewall is the passive unit and waits for connection attempts from the remote VPN gateway.
7. Set **Restart child on close**:
   - **yes** – Restart the connection if the tunnel terminates unexpectedly.
   - **no** – Close the VPN connection if the tunnel terminates unexpectedly.



8. Select the **Authentication Method**:
   - **Pre-shared key** – Enter the **Shared Secret** to use a shared passphrase to authenticate.
   - **CA certificate** – Select a **Server Certificate**, **CA Root** certificate, and enter a **X509 Condition** to use certificate authentication.
   - **X509 certificate (explicit)** – Select a **Server Certificate** and import an **Explicit X509** certificate.
   - **Box SCEP certificate (CA signed)** – Enter a **Shared Secret**, **CA Root** certificate, **X509 Condition**, and upload an **Explicit X509** certificate to use SCEP to authenticate.

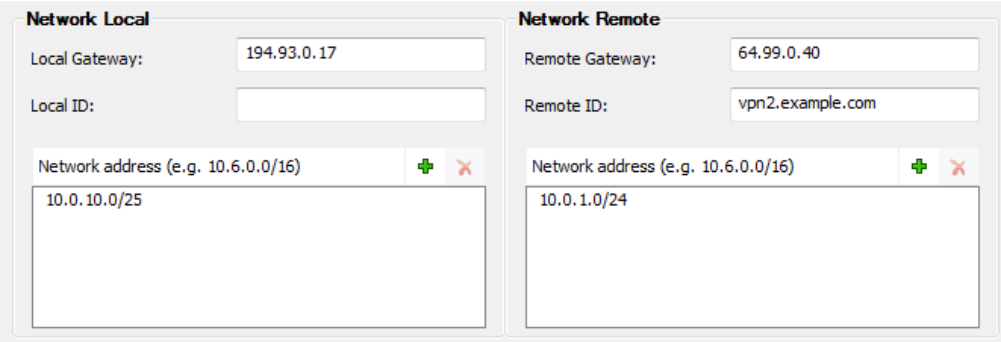


9. Select the **Phase 1** settings:
   - **Encryption** – Select the encryption algorithm: **AES**, **3DES**, **Blowfish**, or **AES256**.
   - **Hash** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, or **SHA512**.
   - **DH-Group** – Select the Diffie-Hellman Group. Supported groups are: 1, 2, 5, 14 - 30.
   - **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed. Default: `3600`
10. Select the **Phase 2** settings:
    - **Encryption** – Select the encryption algorithm: **AES**, **3DES**, **Blowfish**, or **AES256**.
    - **Hash** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, or **SHA512**.
    - **DH-Group** – Select the Diffie-Hellman Group. Supported groups are: 1, 2, 5, 14 - 30.
    - **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed. Default: `3600`.
    - **Lifetime (KB**) – Enter the number of KB after which the IPsec SA is re-keyed.

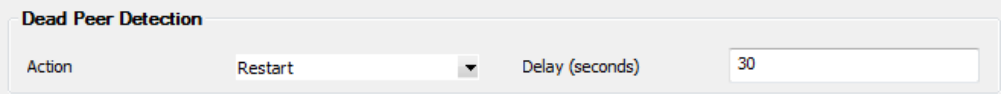


11. Enter the **Network Local** settings:
    - **Local Gateway** – Enter the external IP address of the F-Series Firewall. If you are using a dynamic WAN IP address, enter `0.0.0.0`.
    - **Local ID**– Enter an IP address, FQDN, email or a distinguished name if left blank the local gateway IP is used.
    - **Network Address** – Add the local networks you want to reach through the VPN tunnel, and click **Add**.
12. Enter the **Network Remote** settings:
    - **Remote Gateway** – Enter the external IP address of the third-party appliance. If the remote appliance is using dynamic IP addresses, enter `0.0.0.0`.

- **Remote ID** – Enter a unique ID.
- **Network Address** – Add the IP address of the remote network, and click **Add**.



13. Enter the **Dead Peer Detection** settings:
    - **Action**:
      - **None** – Disable DPD.
      - **Clear** – Connection with the dead peer is stopped, routes removed.
      - **Hold** – Connection is put in hold state.
      - **Restart** – Connection is restarted.
    - **Delay (seconds)** – Enter the number of seconds, after which an empty INFORMATIONAL message is sent to check if the remote peer is still available.



14. Click **OK**.
15. Click **Send Changes and Activate**.

Step 2. Create an IPsec Tunnel on the Remote Appliance

Configure the remote F-Series Firewall or third-party VPN gateway with the same settings. Only the local and remote networks and the IP address for the remote VPN gateway must be interchanged.

Step 3. Create Access Rules for VPN Traffic

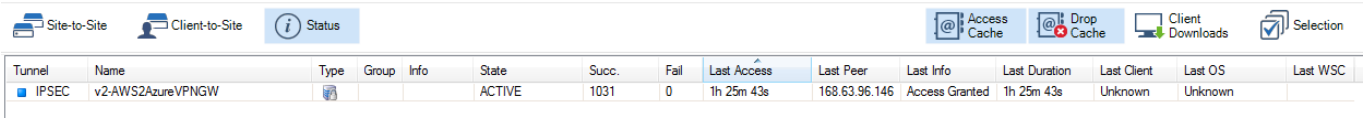
To allow traffic in and out of the VPN tunnel, create a PASS access rule.

For more information, see How to Create Access Rules for Site-to-Site VPN Access.

Monitoring a VPN Site-to-Site Tunnel

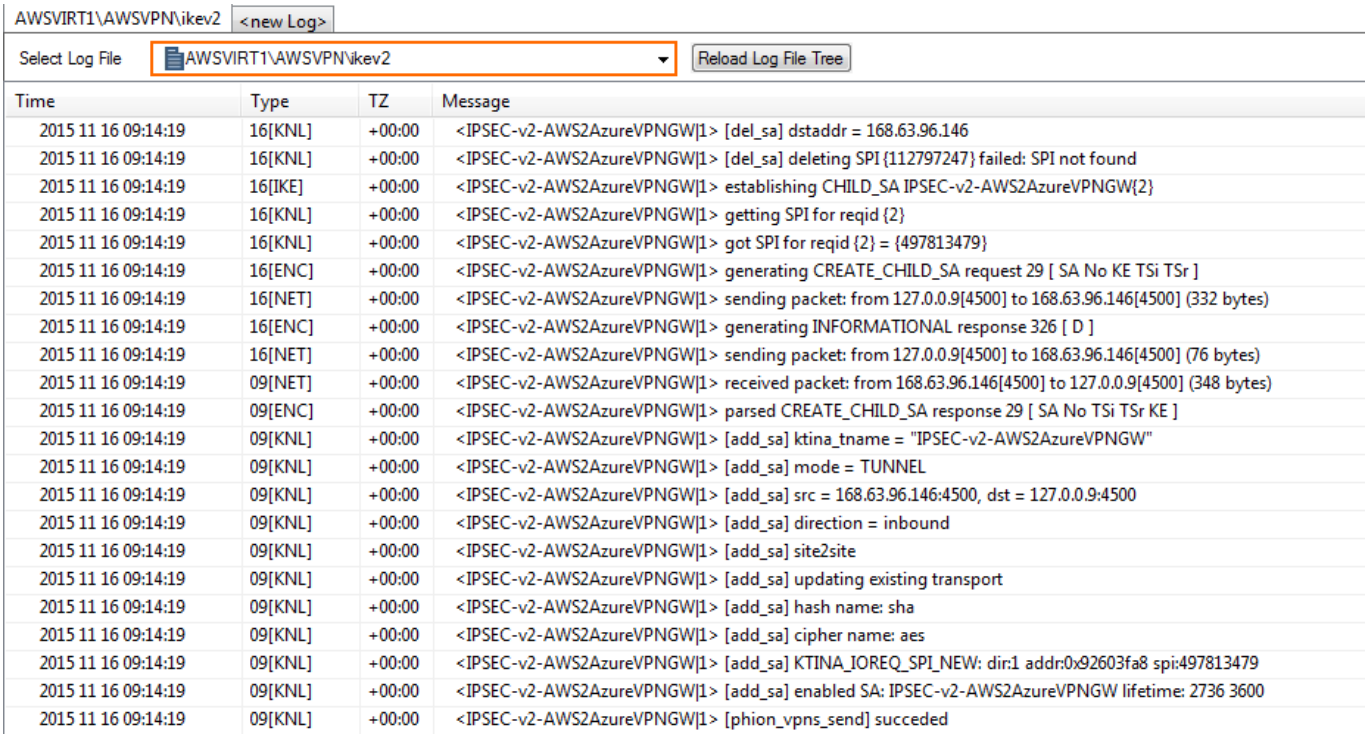
To verify that the VPN tunnel was initiated successfully and traffic is flowing, go to **VPN > Site-to-**

Site or **VPN > Status**.



Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client	Last OS	Last WSC
IPSEC	v2-AWS2AzureVPNGW				ACTIVE	1031	0	1h 25m 43s	168.63.96.146	Access Granted	1h 25m 43s	Unknown	Unknown	

Go to **LOGS** and select the **//IKEv2** log file



Time	Type	TZ	Message
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [del_sa] dstaddr = 168.63.96.146
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [del_sa] deleting SPI {112797247} failed: SPI not found
2015 11 16 09:14:19	16[IKE]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> establishing CHILD_SA IPSEC-v2-AWS2AzureVPNGW{2}
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> getting SPI for reqid {2}
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> got SPI for reqid {2} = {497813479}
2015 11 16 09:14:19	16[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> generating CREATE_CHILD_SA request 29 [SA No KE TSi TSr]
2015 11 16 09:14:19	16[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> sending packet: from 127.0.0.9[4500] to 168.63.96.146[4500] (332 bytes)
2015 11 16 09:14:19	16[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> generating INFORMATIONAL response 326 [D]
2015 11 16 09:14:19	16[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> sending packet: from 127.0.0.9[4500] to 168.63.96.146[4500] (76 bytes)
2015 11 16 09:14:19	09[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> received packet: from 168.63.96.146[4500] to 127.0.0.9[4500] (348 bytes)
2015 11 16 09:14:19	09[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> parsed CREATE_CHILD_SA response 29 [SA No TSi TSr KE]
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] ktina_tname = "IPSEC-v2-AWS2AzureVPNGW"
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] mode = TUNNEL
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] src = 168.63.96.146:4500, dst = 127.0.0.9:4500
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] direction = inbound
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] site2site
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] updating existing transport
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] hash name: sha
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] cipher name: aes
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] KTINA_IOREQ_SPI_NEW: dir:1 addr:0x92603fa8 spi:497813479
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [add_sa] enabled SA: IPSEC-v2-AWS2AzureVPNGW lifetime: 2736 3600
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW|1> [phion_vpns_send] succeded

Figures

1. ipsec_IKEv2.png
2. S2S_IKEv2_01.png
3. S2S_IKEv2_02.png
4. S2S_IKEv2_03.png
5. S2S_IKEv2_04.png
6. S2S_IKEv2_05.png
7. S2S_IKEv2_monitor.png
8. S2S_IKEv2_logfile.png