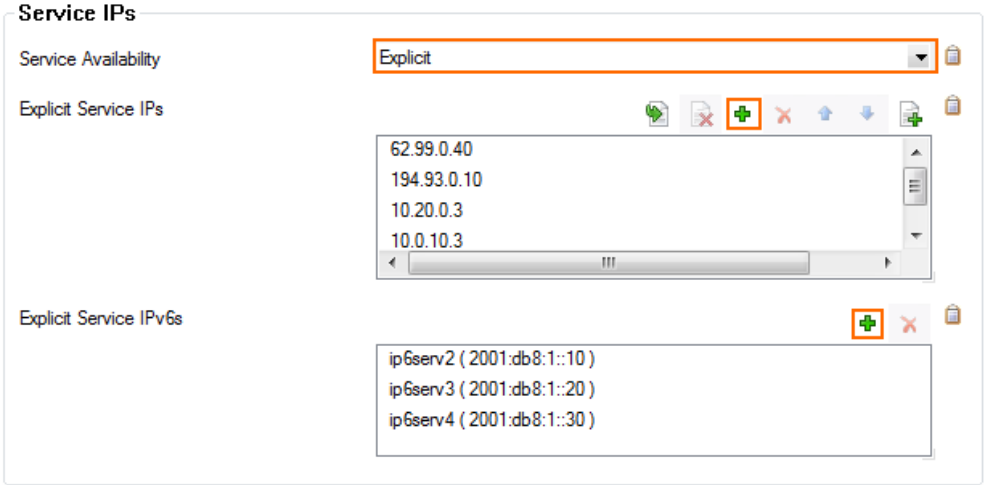
How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel

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 the F-Series Firewall and the third-party IKEv2 IPsec gateway.

Step 1. Configure the VPN Service Listeners

Configure the IPv4 and IPv6 listener addresses for the VPN service.

1. Go to **CONFIGURATION > Configuration Tree> Box > Virtual Server > your virtual server > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** list, select the source for the IPv4 listeners:
   - **First+Second-IP** – The VPN service listens on the first and second virtual server IPv4 address.
   - **First-IP** – The VPN service listens on the first virtual server IPv4 address.
   - **Second-IP** – The VPN service listens on the second virtual server IPv4 address.
   - **Explicit** – For each IP address, click **+** and enter the IPv4 addresses in the **Explicit Service IPs** list.
4. Click **+** to add an entry to the **Explicit IPv6 Service IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 virtual server IP addresses.

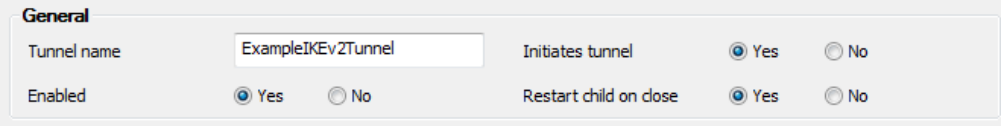


6. Click **Send Changes** and **Activate**.

Step 2. 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.

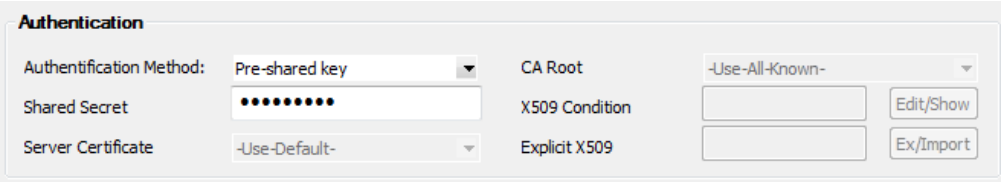


8. Select the **Authentication Method**:

   - **Pre-shared key** – Enter the **Shared Secret** to use a shared passphrase to authenticate.

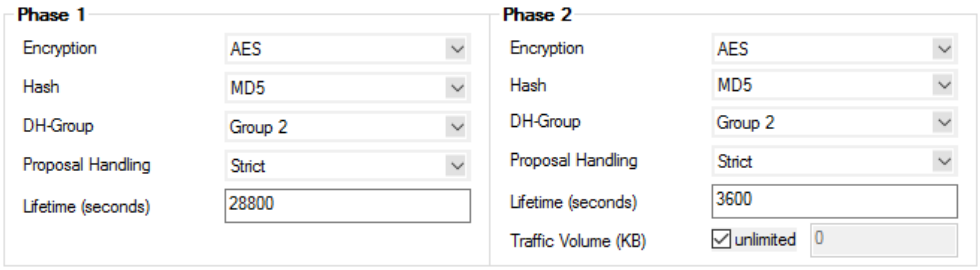
     The shared secret can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).

   - **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.

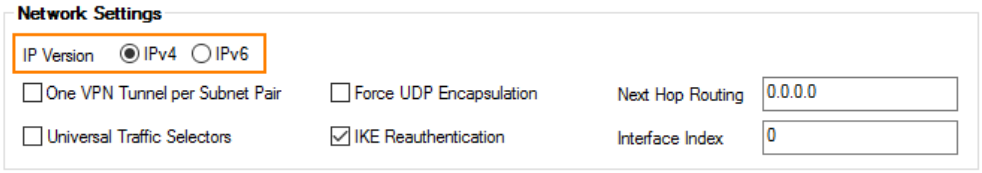


9. Select the **Phase 1** settings:
   - **Encryption** – Select the encryption algorithm: **AES**, **3DES**, **Blowfish**, or **AES256**.
   - **Hash** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, or **SHA512**.
   - **DH-Group** – Select the Diffie-Hellman Group. Supported groups are: 1, 2, 5, 14 - 30.
   - **Proposal Handling**
     - **Strict** – The effective encryption is strictly determined by the proposed set of **Encryption**, **Hash** and **Group**. The communication partner must agree with the proposed set; otherwise, no communication will be established due to a missing common encryption agreement.
     - **Negotiate** – This option lets a communication partner decrease the strength of the encryption if it cannot support the proposed encryption from the initiator.
   - **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed. Default: 28800
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.
    - **Proposal Handling**
      - **Strict** – The effective encryption is strictly determined by the proposed set of **Encryption**, **Hash** and **Group**. The communication partner must agree with the proposed set; otherwise, no communication will be established due to a missing common encryption agreement.
      - **Negotiate** – This option lets a communication partner decrease the strength of the encryption if it cannot support the proposed encryption from the initiator.
    - **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed. Default: 3600.
    - **Traffic Volume (KB**) – Enter the number of KB after which the IPsec SA is re-keyed.

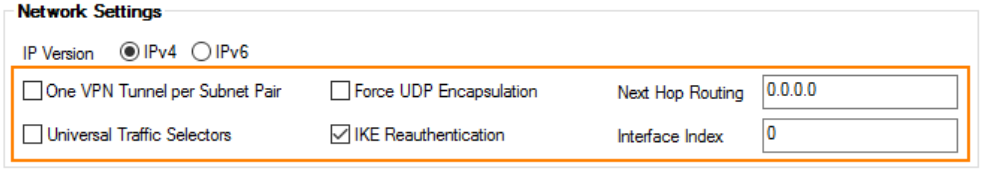
- **Unlimited** – Click the check box to keep the traffic volume from being a trigger for re-keying.



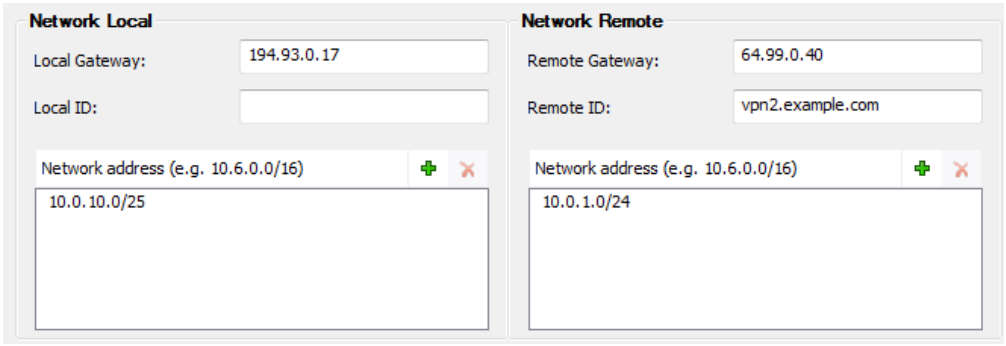
11. Select the IP version of the local listener and the remote gateway.
    - **IP Version** – Click **IPv4** or **IPv6** to match the **Local Gateway** and **Remote Gateway** IP address IP versions.



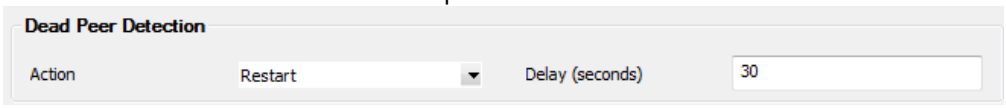
12. (optional) Select **Advanced Network Settings**
    - **One VPN Tunnel per Subnet Pair** – Creates a dedicated security association for each subnet pair. This is needed if the remote device is a Cisco ASA.
    - **Force UDP Encapsulation** – Use UDP encapsulation (4500) for ESP traffic even if no NAT is detected.
    - **Universal Traffic Selector** – Instruct peer to route all traffic into tunnel. This is needed if the remote device is a Checkpoint firewall.
    - **IKE Reauthentication** – Re-authenticate during every IKE re-keying. This setting must be disabled if the remote device is a Microsoft Azure Dynamic VPN Gateway.
    - **Next Hop Routing** – Sets the next hop IP address for routed VPN traffic.
    - **Interface Index** – The number of the virtual interface to be used for routed VPN.



13. Enter the **Network Local** settings:
    - **Local Gateway** – Enter the external IP address of the 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**.
14. Enter the **Network Remote** settings:
    - **Remote Gateway** – Depending on the setting of **Initiate Tunnel**, this edit field accepts different input:
      - **Initiate Tunnel = Yes** – The input must be a hostname or IP address. No network IPs in CIDR notation are allowed.
      - **Initiate Tunnel = No** – The input must be an IP address or network address. If the remote appliance is using dynamic IP addresses, enter `0.0.0.0/0`.
    - **Remote ID** – Enter a unique ID. VPN tunnels without remote ID will not establish successfully.
    - **Network Address** – Add the IP address of the remote network, and click **Add**.



15. 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.



16. Click **OK**.
17. Click **Send Changes and Activate**.

Step 3. Create an IPsec Tunnel on the Remote Appliance

C onfigure 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.

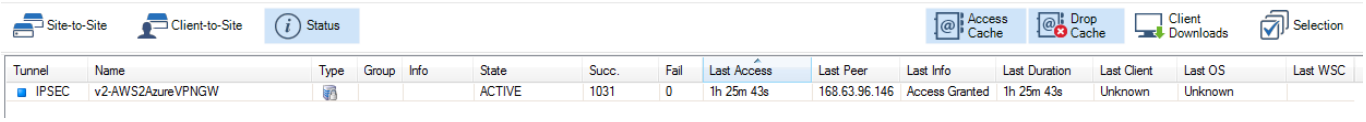
Step 4. Create Access Rules for VPN Traffic

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

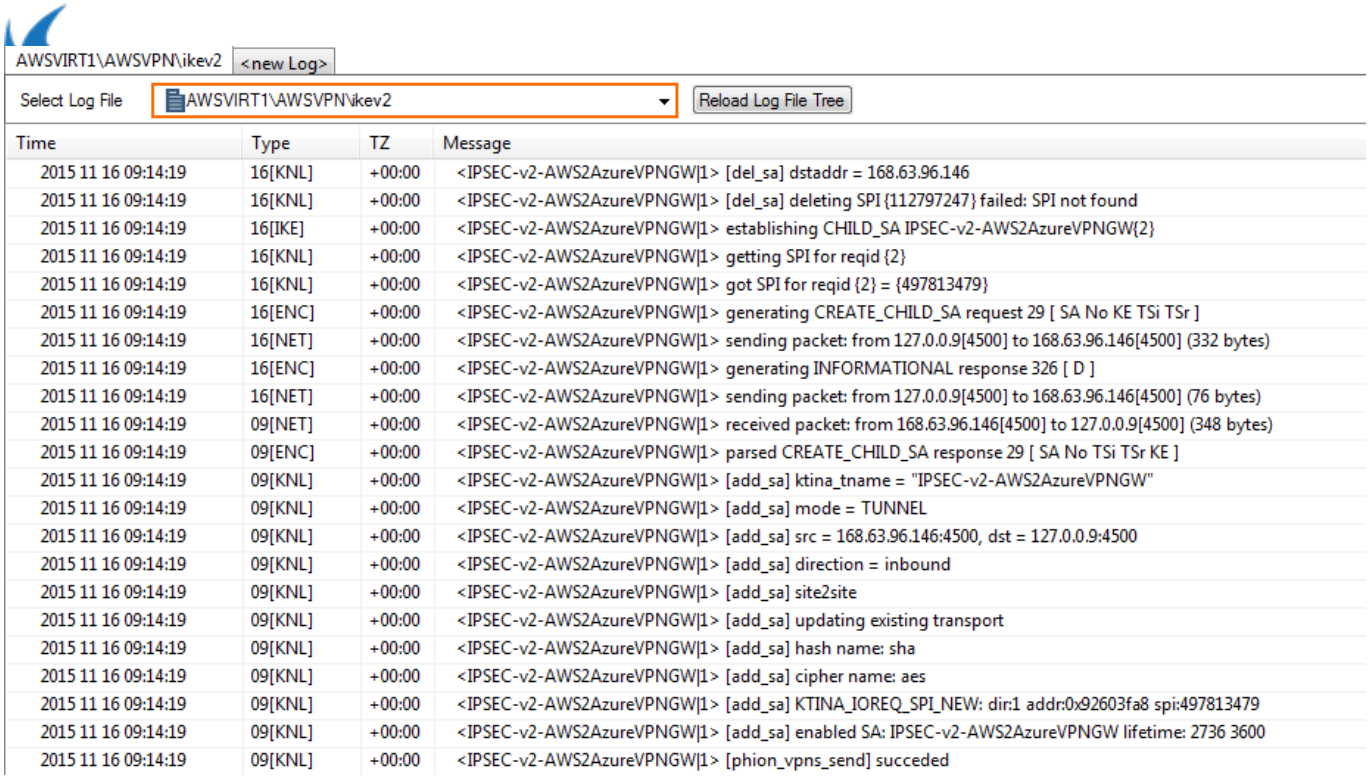
For more information, see How to Create Access Rules for Site-to-Site VPN Access.

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**.



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



AWSVIRT1\AWSVPN\ikev2 <new Log>

Select Log File: AWSVIRT1\AWSVPN\ikev2 | Reload Log File Tree

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