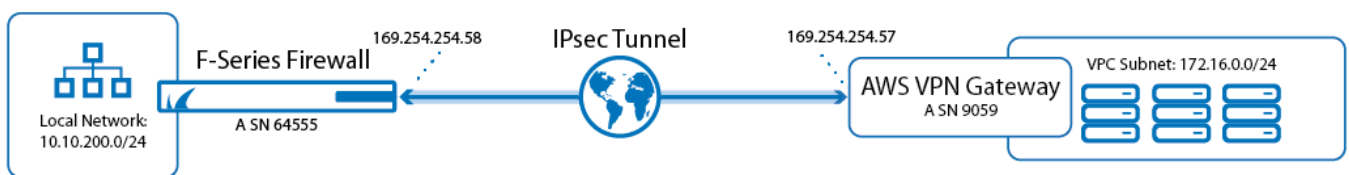




How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP

If you are using the Amazon Virtual Private Cloud, you can transparently extend your local network to the cloud by connecting both networks with a site-to-site IKEv1 IPsec VPN tunnel. The Amazon virtual private gateway uses one IKEv1 IPsec VPN tunnel in combination with BGP. The second IPsec tunnel offered by the AWS gateway is not used, as the identifier sent by AWS causes rekeying issues, that are not present when only one tunnel is used.

Additional Amazon AWS charges apply. For more information, see Amazon's monthly pricing calculator at <http://calculator.s3.amazonaws.com/calc5.html>.



Before You Begin

- Create an Amazon Virtual Private Cloud (VPC).

The local and remote (VPC) subnets must not overlap. E.g., if your local network is 10.0.1.0/24, do not use 10.0.0.0/16 for your VPC.

- Create at least one subnet in the VPC.
- Create and configure the Amazon Routing Table.

Step 1. Create the Amazon VPN Gateway

Step 1.1 Create a Virtual Private Gateway

The Amazon virtual private gateway is the VPN concentrator on the remote side of the IPsec VPN connection.

1. Go to the [Amazon VPC Management Console](#).
2. In the left menu, click **Virtual Private Gateways**.
3. Click **Create Virtual Private Gateway**.
4. Enter the **Name tag** for the VPN gateway.
5. Click **Yes, Create**.
6. Select the newly created virtual private gateway, and click **Attach to VPC**.
7. Select your VPC from the **VPC** list, and click **Yes, Attach**.

The virtual private gateway is now available.



VPC Dashboard

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Virtual Private Gateway Delete Virtual Private Gateway Attach to VPC Detach from VPC

Search Virtual Private Gateways...

Name	ID	State	Type	VPC
Techilb Virtual Private Gateway	vgw-eaac9b9e	attached	ipsec.1	vpc-7ae90b1f (172.16.0.0/16)...

Step 1.2. Add Your Customer Gateway Configuration

The Amazon customer gateway is your Barracuda NextGen Firewall F-Series on your end of the VPN connection. Specify your external IP address and routing type in the customer gateway configuration:

1. Go to the [Amazon VPC Management Console](#).
2. In the left menu, click **Customer Gateway**.
3. Click **Create Customer Gateway**.
4. Enter the connection information for your Barracuda Firewall:
 - o **Name Tag** - Enter a name for your device (e.g., My Barracuda NextGen Firewall F-Series).
 - o **Routing** - Select **Dynamic**.
 - o **IP Address** - Enter your external **IP Address**. To look up your external IP address, go to **CONTROL > Network**.

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and can't be behind a device performing network address translation (NAT). For dynamic routing also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name tag: My Barracuda NG Firewall

Routing: Dynamic

BGP ASN: 64555

IP Address: 54.229.1.87

Cancel Yes, Create

5. Click **Yes, Create**.

Your Barracuda NextGen Firewall F-Series is now configured in the AWS cloud and can be used to configure VPN connections.

VPC Dashboard

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Customer Gateway Delete Customer Gateway

Search Customer Gateways...

Name	ID	State	Type	IP Address	BGP ASN
My Barracuda NG Firewall	cgw-c56751b1	available	ipsec.1	54.229.172.87	64555

Step 1.3. Create a VPN Connection

Create a VPN connection with the customer gateway and the virtual private gateway that you just created. Then download the VPN configuration file because it contains all the necessary information for configuring the VPN connection on the Barracuda NextGen Firewall F-Series.

How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP



The Amazon VPN configuration file is different for every VPN connection.

1. Go to the [Amazon VPC Management Console](#).
2. In the left menu, click **VPN Connections**.
3. Click **Create VPN Connection**.
4. In the **Create VPN Connection** window, enter the configuration information for your VPN connection:
 - o **Name tag** - Enter a name for your VPN connection (e.g., NG2AWSCLoud).
 - o **Virtual Private Gateway** - Select the virtual private gateway created in [Step 1](#).
 - o **Routing Options** - Select **Dynamic (requires BGP)**.

Create VPN Connection
? X

Select the Virtual Private Gateway and Customer Gateway that you would like to connect via a VPN connection. You must have entered the Virtual Private Gateway and your Customer Gateway information already.

Name tag i

Virtual Private Gateway v

Customer Gateway Existing
 New

v

Specify the routing for the VPN Connection ([Help me choose](#))

Routing Options **Dynamic (requires BGP)**
 Static

VPN connection charges apply once this step is complete. [View Rates](#)

Cancel
Yes, Create

5. Click **Yes, Create**.
6. Click **Download Configuration**.
7. Select generic vendor and platform settings for the configuration file:
 - o **Vendor** - Select **Generic**.
 - o **Platform** - Select **Generic**.
 - o **Software** - Select **Vendor Agnostic**.

Download Configuration
? X

Please choose the configuration to download based on your type of customer gateway.

Vendor: v i

Platform: v i

Software: v i

Cancel
Yes, Download

8. Click **Yes, Download**, and save the vpn- .txt file.

[Click here to see an example Amazon VPN configuration file](#)

Amazon Web Services Virtual Private Cloud VPN Connection Configuration

```

=====
= AWS utilizes unique identifiers to manipulate the configuration of a VPN
Connection. Each VPN Connection is assigned a VPN Connection Identifier and is
associated with two other identifiers, namely the Customer Gateway Identifier
and the Virtual Private Gateway Identifier. Your VPN Connection ID : vpn-YOUR-

```



VPN-CONNECTION-ID Your Virtual Private Gateway ID : vgw-YOUR-VIRTUAL-PRIVATE-GATEWAY-ID Your Customer Gateway ID : cgw-YOUR-CUSTOMER-GATEWAY-ID A VPN Connection consists of a pair of IPsec tunnel security associations (SAs). It is important that both tunnel security associations be configured. IPsec Tunnel #1

```
=====
= #1: Internet Key Exchange Configuration Configure the IKE SA as follows -
Authentication Method : Pre-Shared Key - Pre-Shared Key : YOUR-PRESHARED-KEY -
Authentication Algorithm : sha1 - Encryption Algorithm : aes-128-cbc - Lifetime
: 28800 seconds - Phase 1 Negotiation Mode : main - Perfect Forward Secrecy :
Diffie-Hellman Group 2 #2: IPsec Configuration Configure the IPsec SA as
follows: - Protocol : esp - Authentication Algorithm : hmac-sha1-96 -
Encryption Algorithm : aes-128-cbc - Lifetime : 3600 seconds - Mode : tunnel -
Perfect Forward Secrecy : Diffie-Hellman Group 2 IPsec Dead Peer Detection
(DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your
endpoint as follows: - DPD Interval : 10 - DPD Retries : 3 IPsec ESP
(Encapsulating Security Payload) inserts additional headers to transmit
packets. These headers require additional space, which reduces the amount of
space available to transmit application data. To limit the impact of this
behavior, we recommend the following configuration on your Customer Gateway: -
TCP MSS Adjustment : 1387 bytes - Clear Don't Fragment Bit : enabled -
Fragmentation : Before encryption #3: Tunnel Interface Configuration Your
Customer Gateway must be configured with a tunnel interface that is associated
with the IPsec tunnel. All traffic transmitted to the tunnel interface is
encrypted and transmitted to the Virtual Private Gateway. The Customer Gateway
and Virtual Private Gateway each have two addresses that relate to this IPsec
tunnel. Each contains an outside address, upon which encrypted traffic is
exchanged. Each also contain an inside address associated with the tunnel
interface. The Customer Gateway outside IP address was provided when the
Customer Gateway was created. Changing the IP address requires the creation of
a new Customer Gateway. The Customer Gateway inside IP address should be
configured on your tunnel interface. Outside IP Addresses: - Customer Gateway :
YOUR-EXTERNAL-IP - Virtual Private Gateway : VIRTUAL-PRIVATE-NETWORK-EXTERNAL-
IP Inside IP Addresses - Customer Gateway : 169.254.254.58/30 - Virtual Private
Gateway : 169.254.254.57/30 Configure your tunnel to fragment at the optimal
size: - Tunnel interface MTU : 1436 bytes #4: Border Gateway Protocol (BGP)
Configuration: The Border Gateway Protocol (BGPv4) is used within the tunnel,
between the inside IP addresses, to exchange routes from the VPC to your home
network. Each BGP router has an Autonomous System Number (ASN). Your ASN was
provided to AWS when the Customer Gateway was created. BGP Configuration
Options: - Customer Gateway ASN : 64555
```

Step 2. Configure the IPsec Tunnel on the firewall

Create a next-hop-interface and then configure one IPsec site-to-site VPN tunnel using the settings for the IPsec Tunnel #1. Use the IP addresses provided in the Amazon generic VPN configuration file you downloaded at the end of Step 1.

Step 2.1. Create VPN Next-hop Interfaces

For each IPsec tunnel, a VPN next-hop interface must be created. Use the IP addresses provided in the Amazon generic VPN configuration file you downloaded at the end of Step 1.

[Click here to see the relevant part of an example Amazon VPN configuration file](#)

[...]

How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP



IPSec Tunnel #1

```

[...]
```

```

#3: Tunnel Interface Configuration
[...]
```

Inside IP Addresses

- Customer Gateway : 169.254.254.58/30
- Virtual Private Gateway : 169.254.254.57/30

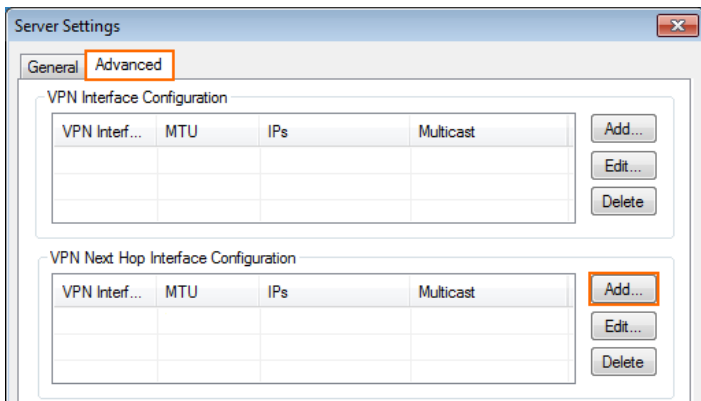
Configure your tunnel to fragment at the optimal size:

- Tunnel interface MTU : 1436 bytes

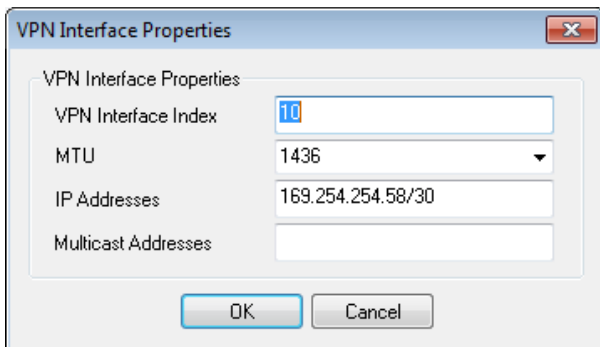
```

[...]
```

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings** .
2. Click **Lock**.
3. Click on **Click here for Server Settings**.
4. Click on the **Advanced** tab.



5. Create a VPN next hop interface for each IPsec tunnel by clicking **Add** in the **VPN Next Hop Interface Configuration** section.
 1. In the **VPN Interface Properties** window enter:
 - **VPN Interface Index** - Enter a number between 0 and 99. Each interface index number must be unique. E.g., IPsec tunnel1: 10
 - **MTU** - Enter 1436.
 - **IP Addresses** - Enter the **Inside IP Address** for the **Customer Gateway** provided by Amazon. E.g, IPsec tunnel1: 169.254.254.58/30
 2. Click **OK**.



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

Step 2.2. Configure Two Site-to-Site IPsec Tunnels

Configure a site-to-site IPsec tunnel using the VPN next-hop interface.

[Click here to see the relevant part of an example Amazon VPN configuration file](#)



Amazon Web Services

Virtual Private Cloud

[...]

IPSec Tunnel #1

=====

#1: Internet Key Exchange Configuration

Configure the IKE SA as follows

- Authentication Method : Pre-Shared Key
- Pre-Shared Key : YOUR-PRESHARED-KEY
- Authentication Algorithm : sha1
- Encryption Algorithm : aes-128-cbc
- Lifetime : 28800 seconds
- Phase 1 Negotiation Mode : main
- Perfect Forward Secrecy : Diffie-Hellman Group 2

#2: IPSec Configuration

Configure the IPSec SA as follows:

- Protocol : esp
- Authentication Algorithm : hmac-sha1-96
- Encryption Algorithm : aes-128-cbc
- Lifetime : 3600 seconds
- Mode : tunnel
- Perfect Forward Secrecy : Diffie-Hellman Group 2

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:

- DPD Interval : 10

[...]

#3: Tunnel Interface Configuration

[...]

Outside IP Addresses:

- Customer Gateway : YOUR-EXTERNAL-IP-ADDRESS
- Virtual Private Gateway : AMAZON-VPN-GATEWAY-IP-ADDRESS-TUNNEL-2

[...]

Configure your tunnel to fragment at the optimal size:

- Tunnel interface MTU : 1436 bytes

[...]

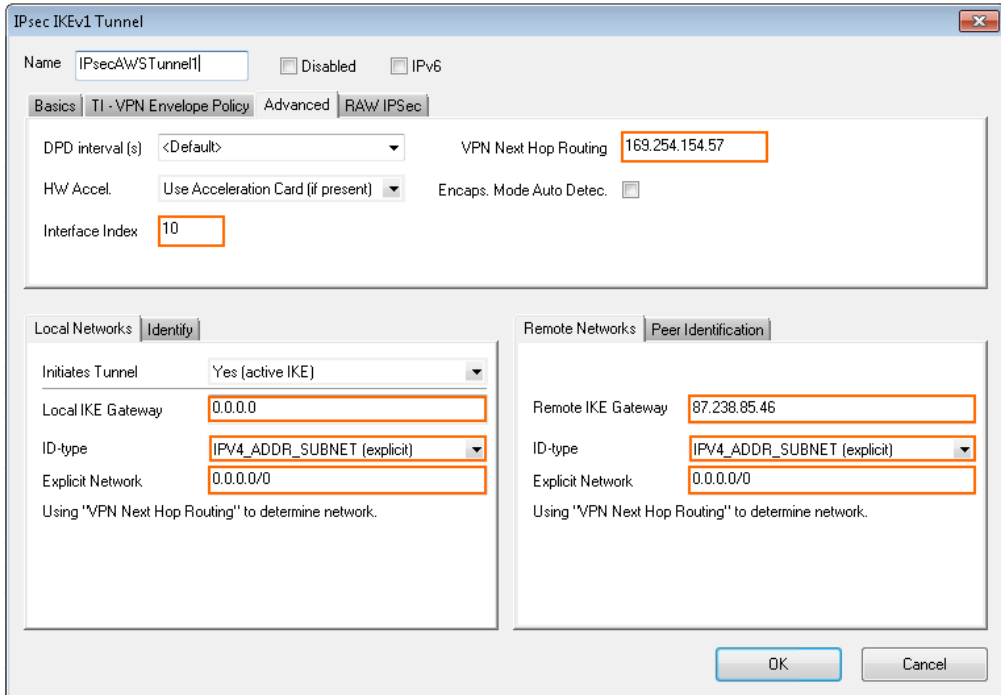
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Site to Site** .
2. Click on the **IPsec IKEv1 Tunnels** tab.
3. Click **Lock**.
4. For each IPsec tunnel, right-click and click **New IPsec IKEv1 tunnel**.
 1. Enter the IPsec tunnel configurations:
 1. Enter a **Name**. E.g, IPsec Tunnel 1: IPsecAWSTunnel1
 2. Enter the **Phase 1** and **Phase 2** settings:

	Phase 1	Phase 2
Encryption	AES	AES
Hash Meth.	SHA	SHA
DH-Group	Group2	Group 2
Lifetime(sec)	28800	3600
Perfect Forward Secrecy		Enable

3. In the **Local Network s** tab:

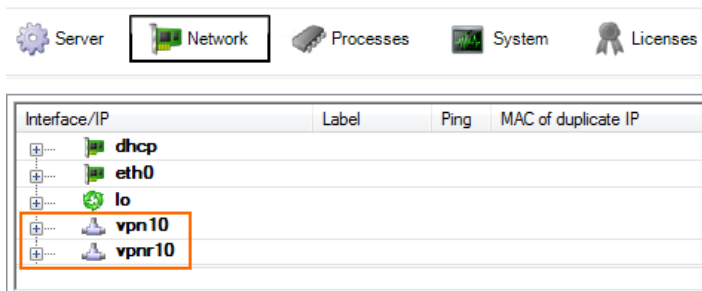


- **Local IKE Gateway** - Enter your external IP address. If you are using a dynamic WAN interface enter 0.0.0.0
 - **ID-type** - Select **IPv4_ADDR_SUBNET (explicit)**,
 - **Explicit Network** - Enter 0.0.0.0/0.
 - **Network Address** - Enter the **Inside IP Address** of the **Customer Gateway** (without the /30) and click **Add**. E.g., IPsec tunnel 1 169.254.254.58
4. In the **Remote Networks** tab:
 - **Remote IKE Gateway** - Enter the **Outside IP Address** of the **Virtual Private Gateway** .
 - **ID-type** - Select **IPv4_ADDR_SUBNET (explicit)**,
 - **Explicit Network** - Enter 0.0.0.0/0.
 5. In the **Peer Identification** tab:
 - **Shared Secret** - Enter the Amazon **Pre-Shared Key**.
 6. In the **Advanced** tab:
 - **DPD intervals (s)** - Enter 10.
 - **Interface Index** - Enter the **VPN Next Hop Interface index** number you entered in step 1.1. E.g., IPsec tunnel 1 10
 - **VPN Next Hop Routing** - Enter the **Inside IP address** of the **Virtual Private Gateway**. E.g., IPsec tunnel 1 169.254.254.57
 7. Click **OK**.



5. Click **Send Changes** and **Activate**.

You now have the VPN next-hop interface listed in the **Interfaces/IPs** section on the **CONTROL > Network** page and the VPN tunnels on the **CONTROL > VPN > STATUS**.



Tunnel	Name	Type	Group	I...	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client
IPSEC	IPsecAWSTunnel1-169.254.254.57-169.25...				ACTIVE	37	5	50m 19s	87.238.85.42	Access Granted	50m 19s	Unknown

Step 3. Configure the BGP Service

Configure BGP routing to learn the subnets on the other side of the VPN tunnels. The BGP route propagated by the second (backup) IPsec tunnel is artificially elongated so traffic is routed per default over the first IP tunnel, as suggested by Amazon.

[Click here to see the relevant part of an example Amazon VPN configuration file](#)

```
[...]IPSec Tunnel #1
```

```
=====
[...] #4: Border Gateway Protocol (BGP) Configuration: [...] BGP Configuration
Options: - Customer Gateway ASN : YOUR-ASN-NUMBER (e.g., 64555) - Virtual Private
Gateway ASN : 9059 - Neighbor IP Address : 169.254.254.57 - Neighbor Hold Time : 30
[...]
```

Step 3.1. Configure Routes to be Advertised via BGP

Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. (optional) To propagate the management network, set **Advertise Route** to **yes**.
4. In the left menu, click on **Routing**.
5. Double-click on the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3.2. Configure the BGP Routes

Configure the BGP setting for the BGP service on the Barracuda NextGen Firewall F-Series.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. Select **yes** from the **Run BGP Router** list.
3. Select **advertise-learn** from the **Operations Mode** list.

Operational Setup

Run OSPF Router	no	
Run RIP Router	no	
Run BGP Router	yes	
Hostname		
Operation Mode	advertise-learn	
Router ID	10.10.200.101	

4. In the left menu, click **BGP Router Setup**.
5. Enter the **AS Number** (e.g., 64555).
6. In the **Networks** table, add the local network(s)(e.g., 10.10.200.0/24).



BGP Router Configuration

AS Number:

Terminal Password:

Current:

New:

Confirm:

Strength:

Networks:

Name	Network Prefix
LocalNetwork	10.10.200.0/24

7. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
8. Click the **Set** button for the **Advanced Settings**. The **Advanced Settings** window opens.
9. Set the **Hold timer** to 30 seconds.
10. Set the **Keep Alive Timer** to 10 seconds.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

Step 3.3. Add a BGP Neighbor for the IPsec Tunnel

To dynamically learn the routing of the neighboring network, set up a BGP neighbor for the VPN next-hop interface.

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
2. Click **Lock**.
3. For each IPsec tunnel, click the plus sign (+) next to the **Neighbors** table to add a new neighbor.
4. Enter a **Name** for the neighbor. E.g., **AWS1** and **AWS2**
5. In the **Neighbors** window, configure the following settings in the **Usage and IP** section:
 - **Neighbor IPv4** – Enter the inside IP Address of the Virtual Private Gateway (remote address for the VPN next hop interface on the NextGen Firewall F-Series) E.g., IPsec Tunnel 1: 169.254.254.57
 - **OSPF Routing Protocol Usage** – Select **no**.
 - **RIP Routing Protocol Usage** – Select **no**.
 - **BGP Routing Protocol Usage** – Select **yes**.
6. In the **BGP Parameters** section, configure the following settings:
 - **AS Number**: Enter the ASN for the remote network: 9059
 - **Update Source**: Select **Interface.vpnr**
 - **Update Source Interface**: Enter the vpnr interface for the IPsec tunnels. E.g., IPsec Tunnel 1: vpnr10



Usage and IP	
Neighbor IPv4	169.254.254.57
Active	yes
OSPF Routing Protocol Usage	no
RIP Routing Protocol Usage	no
BGP Routing Protocol Usage	yes

OSPF Parameters	
Neighbor Priority	
Dead Neighbor Poll Interval	

BGP Parameters	
AS Number	9059
Description	
Peer Group Affiliation	
Update Source	Interface
Update Source Interface	vpnr10
Update Source IPv4 Address	
Peer Filtering For Input	Set... Clear NOTSET: No section present
Peer Filtering For Output	Set... Clear NOTSET: No section present

7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 4. Create an Access Rule for VPN Traffic

To allow traffic to and from the VPN networks, a pass access rule is needed. You also need to set the **Clear DF bit** and **Force Maximum Segment Size** settings according to the Amazon configuration file in the advanced firewall rule settings. You also need to set **Reverse Interface (Bi-directional)** to **Any** to allow return traffic using a different VPN tunnel than was used to initiate the connection.

[Click here to see the relevant part of an example Amazon VPN configuration file](#)

[...] IPSec ESP (Encapsulating Security Payload) inserts additional headers to transmit packets. These headers require additional space, which reduces the amount of space available to transmit application data. To limit the impact of this behavior, we recommend the following configuration on your Customer Gateway: - TCP MSS Adjustment : 1387 bytes - Clear Don't Fragment Bit : enabled [...]

1. Create a **Pass** access rule:
 - **Bi-Directional** - Enable.
 - **Source** - Select the local network(s) you are propagating via BGP.
 - **Service** - Select the service you want to have access to the remote network or **ALL** for complete access.
 - **Destination** - Select the remote VPC subnet(s).
 - **Connection Method** - Select **Original IP**.



2. In the left menu, click on **Advanced**.
3. In the **TCP Policy** section, set **Force MSS (Maximum Segment Size)** to 1350.

TCP Policy

Generic TCP Proxy	OFF
Syn Flood Protection (Forward)	Server Default
Syn Flood Protection (Reverse)	Server Default
Accept Timeout (s)	10
Last ACK Timeout (s)	10
Retransmission Timeout (s)	300
Halfside Close Timeout (s)	30
Disable Nagle Algorithm	
Force MSS (Maximum Segment Size)	1350
Generic IPS Patterns	-NONE-
Port Protocol Protection Policy	Use Matching Service Settings
Raw TCP mode	No

4. In the **Miscellaneous** section, set **Clear DF Bit** to **Yes**.

Miscellaneous

Authentication	No Inline Authentication
IP Counting Policy	Default Policy
Time Restriction	
Clear DF Bit	Yes
Set TOS Value	0 (TOS unchanged)
Prefer Routing over Bridging	No
Color	RGB(0,0,0)

5. In the **Dynamic Interface Handling** section, set **Reverse Interface (Bi-directional)** to **Any**.

Dynamic Interface Handling

Source Interface	Matching
Continue on Source Interface Mismatch	No
Reverse Interface (Bi-directional)	Any
Interface Checks After Session Creation	Enabled

6. Click **OK**.
7. Move the access rule up in the rule list, so that it is the first rule to match the firewall traffic.
8. Click **Send Changes** and **Activate**.

You now have two IPsec VPN tunnels connecting your F-Series firewalls to the Amazon AWS cloud. Per default, the first IPsec tunnel is chosen. It may take some time for BGP to learn the new routes, in case of a failure.



IPsec Tunnels are connected

Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info
IPSEC	IPsecAWSTunnel1-169.254.254.57-169.25...				ACTIVE	1	1	4m 31s	87.238.85.42	Access Granted

BGP Configuration (CONTROL > NETWORK > BGP)

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
Local						
> 10.10.200.0/24	0.0.0.0	0		32768	Local	IGP
AS 9059						
Neighbor: 169.254.254.57						
172.16.0.0	169.254.254.61			0	9059	IGP

AWS VPN status in the Amazon AWS management interface

vpn-00665074 | NG2AWSCloud

Summary

Tunnel Details

Static Routes

Tags

VPN Tunnel	IP Address	Status	Status Last Changed	Details
Tunnel 1	87.238.85.46	UP	2014-05-27 17:38 UTC+2	1 BGP ROUTES
Tunnel 2	87.238.85.42	DOWN	2014-05-27 17:38 UTC+2	

