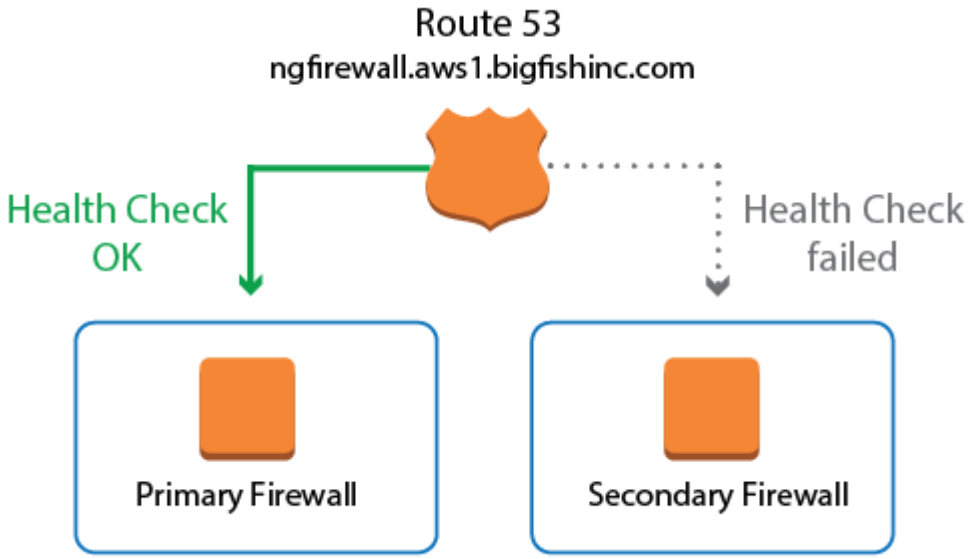
How to Configure Route 53 for F-Series Firewalls in AWS

If you are running multiple stacks in different AWS regions, or multiple deployments in a single region, you must configure AWS Route 53 to access your services behind the NextGen Firewalls. Also use Route 53 if you are using UDP-based services since the Elastic Load Balancer supports only TCP connections. To always route traffic to the active firewall in the HA cluster, define two record sets with a failover policy. The record set for the first firewall is combined with a health check. As long as the health check is valid, the DNS name for the firewall is resolved to the primary firewall. When the virtual server fails over to the secondary firewall, the health check for the primary firewall fails, and after the TTL of the DNS record has expired, the DNS name for the firewall cluster resolves to the IP address in the secondary record set. When the primary firewall is active again, the health check will again show a healthy state and the DNS record will point to the IP address of the primary firewall.



Alternative

If you are not using Elastic IP addresses for your firewalls, you can also use the DNS name of the firewall for the health check and create a CNAME DNS record.

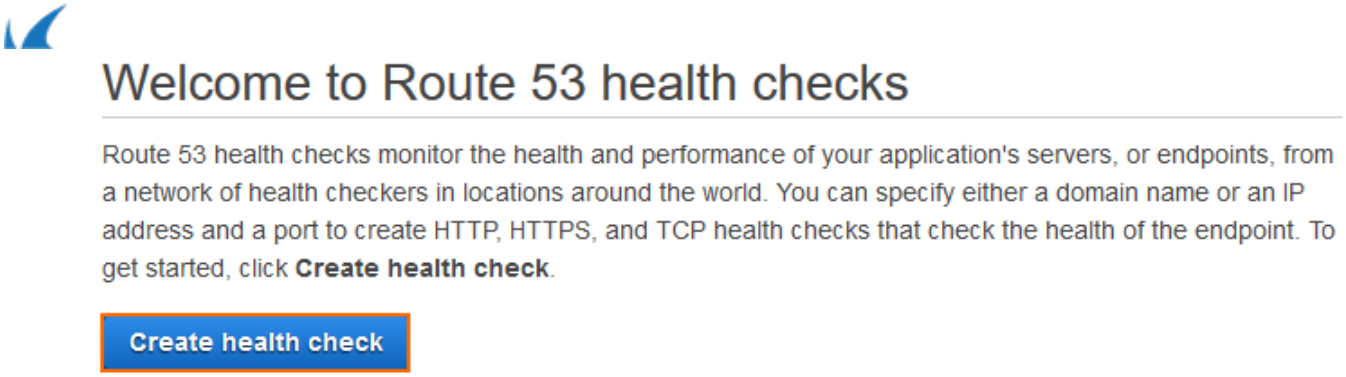
Before you begin

- Set up a domain or subdomain in Route 53 and create a public hosted zone.
- Deploy a high availability cluster. For more information, see How to Configure a High Availability Cluster in AWS using the Web Portal.
- Look up the DNS names, and public or Elastic IP address for the primary and secondary firewalls.

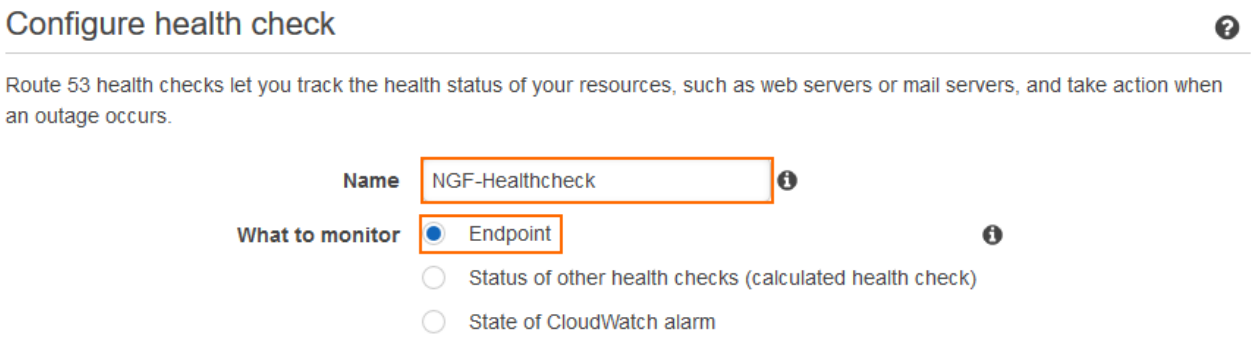
Step 1. Create a Route 53 heath check for the primary firewall

Configure the health check for a service running on the virtual server, such as the VPN service. Do not create a check for box-level services because these services will not fail over to the secondary firewall.

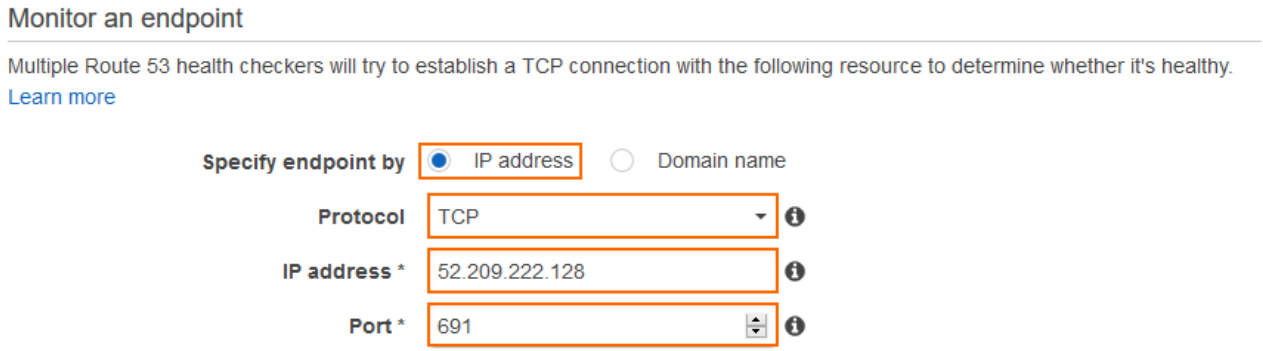
1. Log into the AWS console.
2. Click **Services** and select **Route 53**.
3. In the left menu, click **Health checks**.
4. Click **Create health check**.



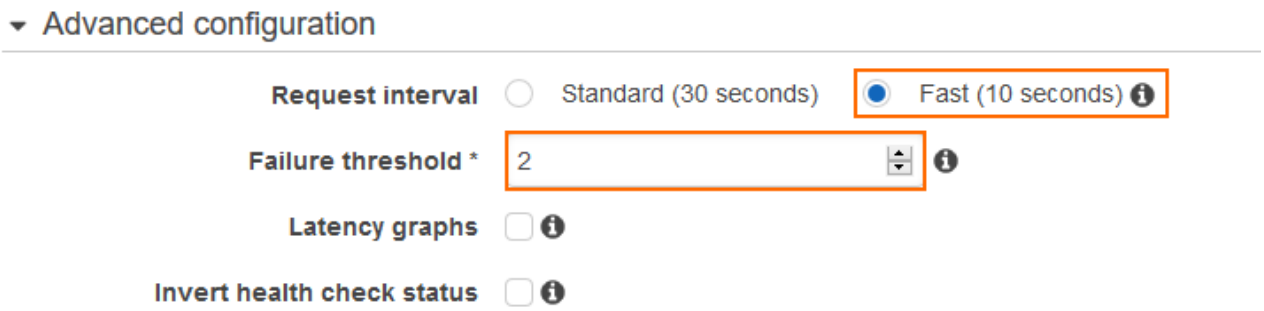
5. Enter a **Name**.
6. From the **What to monitor** list select **Endpoint**.



7. Configure the service to be monitored:
   - **Specify and endpoint by** – Select **IP address**.
   - **Protocol** – Select **TCP**.
   - **IP address** – Enter the public IP address for the primary firewall.
   - **Port** – Enter 691 to monitor the VPN service. The VPN service must be running on your virtual server. Alternatively, you can also select another port on your firewall.

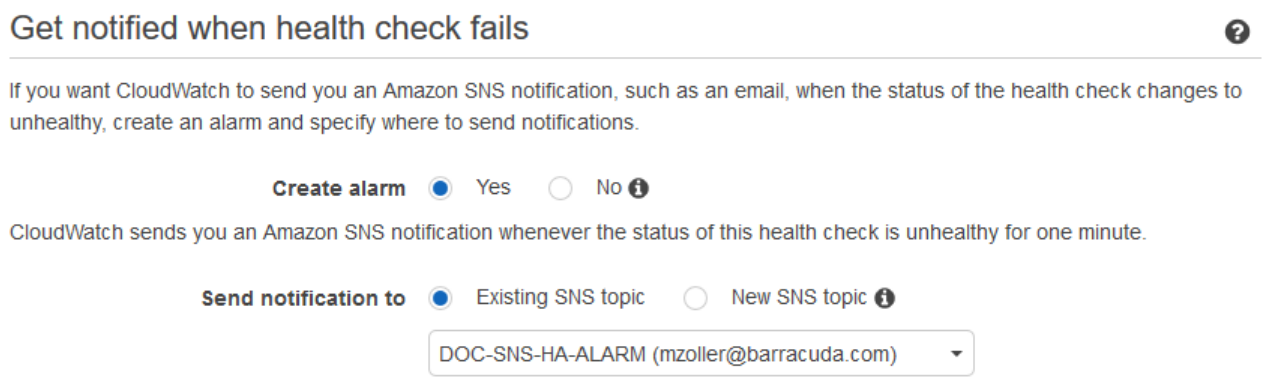


8. (optional) Expand the **Advanced configuration** section and adjust the following settings to improve failover times:
   - **Request interval** – Select **Fast (10 seconds)**.
   - **Failure threshold** – Select **2**.



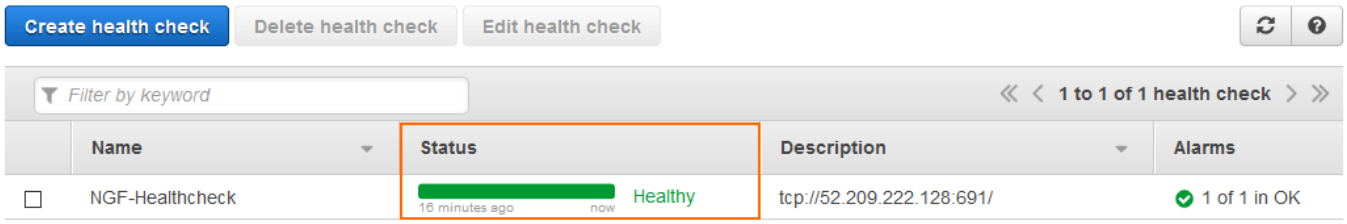
9. Click **Next**.
10. (optional) Set **Create alarm** to **yes** and select an **Existing SNS topic** or create a **New SNS topic** to

receive a notification.



11. Click **Create health check**.

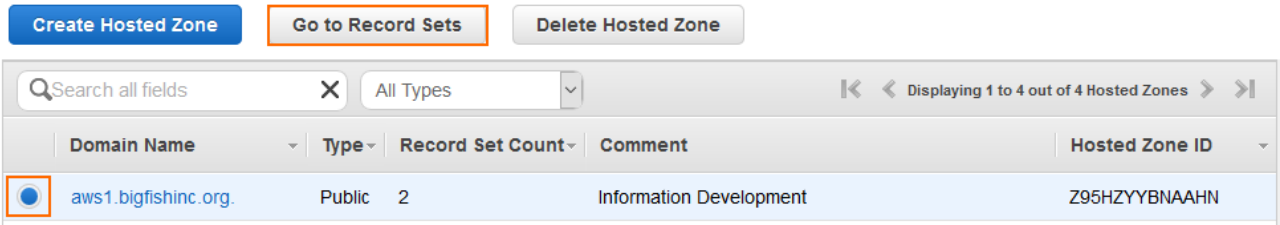
The health check is now active. Depending on the request interval and failover threshold, the **Status** of the health check changes from **Unknown** to **Healthy**.



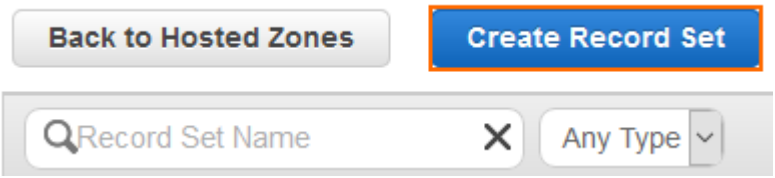
Step 2. Create a failover record set for the primary firewall

Create the DNS record for the primary firewall. Use a **failover** routing policy and add the health check you just created as a condition.

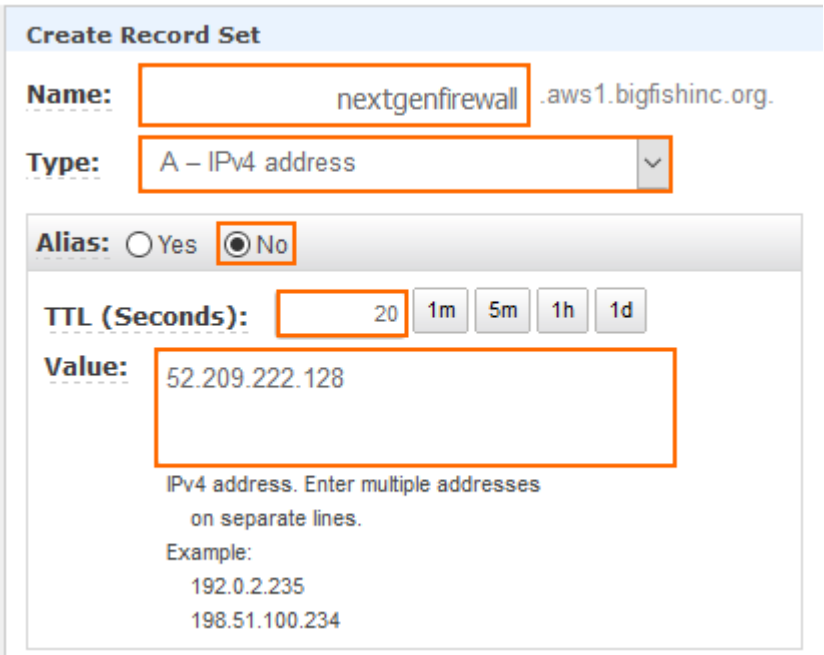
1. Log into the AWS console.
2. Click **Services** and select **Route 53**.
3. In the left menu, click **Hosted zones**.
4. Select your **Domain Name** and click **Go to Record Sets**.



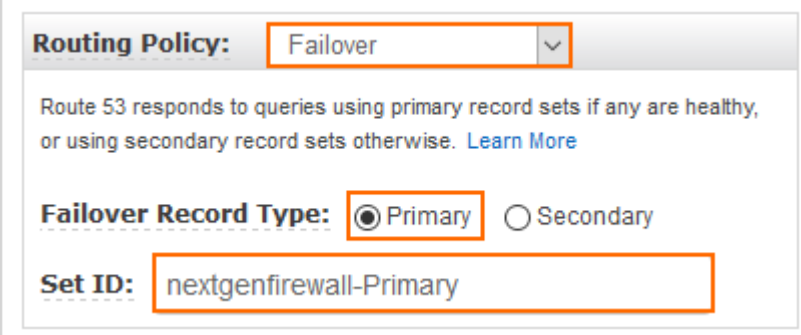
5. Click **Create Record Set**.



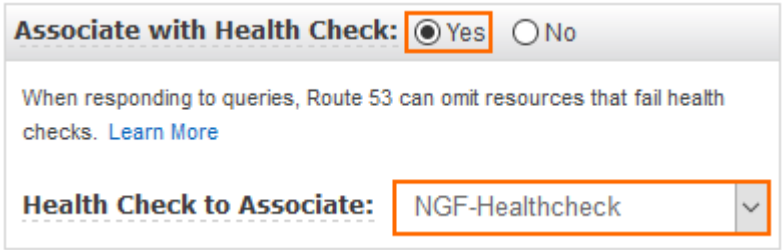
6. In the right column, create the record set:
   - **Name** – Enter the DNS name.
   - **Type** – Select **A - IPv4 address**.
   - **Alias** – Select **No**.
   - **TTL (Seconds)** – Set the number of seconds the DNS records can be cached by non-authoritative DNS servers.
   - **Value** – Enter the EIP or public IP address for the primary firewall.



7. In the right column, configure the **Routing Policy**:
   - **Routing Policy** – Select **Failover**.
   - **Failover Record Type** – Select **Primary**.
   - **Set ID** – Enter a unique ID to differentiate from other failover record sets using the same name and type.



8. In the right column, configure the **Health Check**:
   - **Associate with Heath Check** – Select **yes**.
   - **Health Check to Associate** – Select the health check created in step 1.



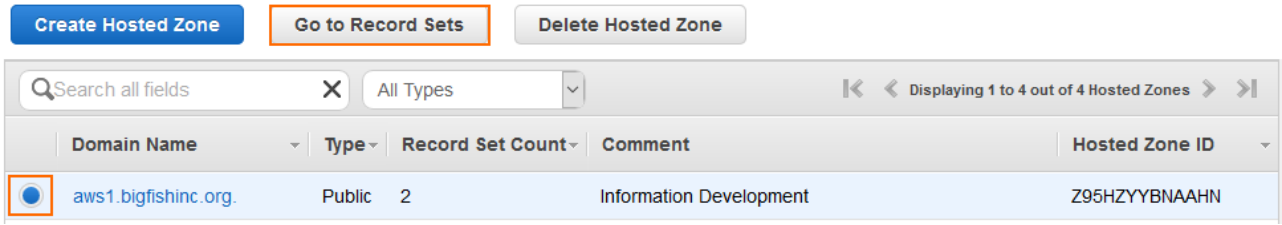
9. Click **Create**.

The record set for the primary firewall is now listed with the other DNS records of this hosted zone.

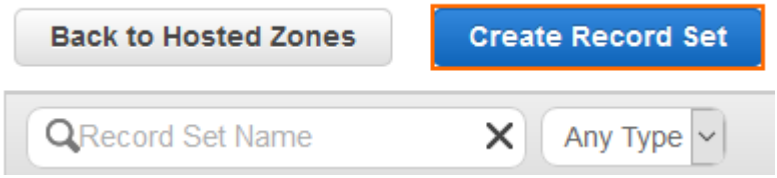
Step 3. Create a failover record set for the secondary firewall

Create the DNS record for the secondary firewall. Use a **failover** routing policy.

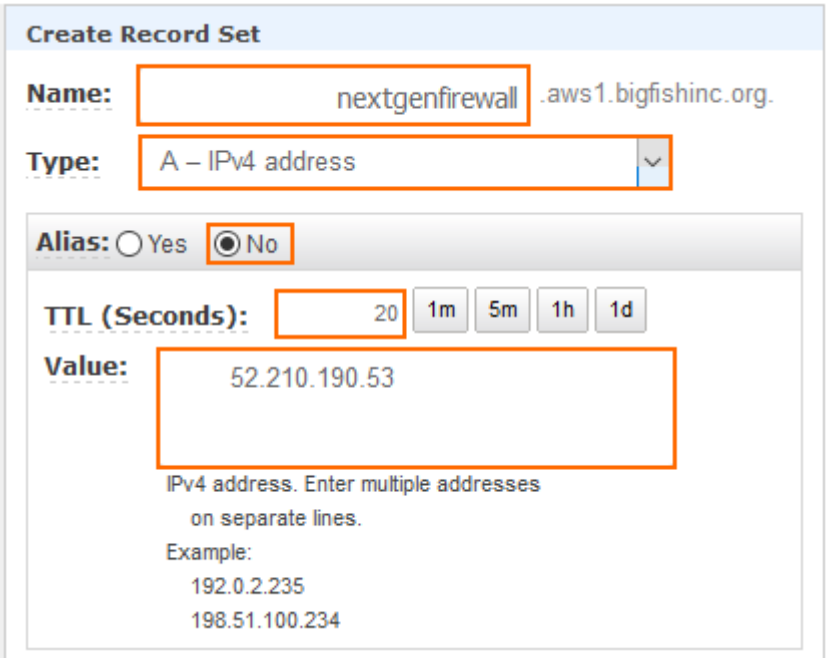
1. Log into the AWS console.
2. Click **Services** and select **Route 53**.
3. In the left menu, click **Hosted zones**.
4. Select your **Domain Name** and click **Go to Record Sets**.



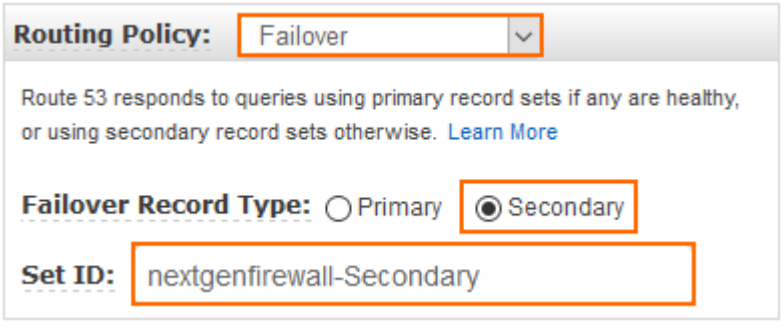
5. Click **Create Record Set**.



6. In the right column, create the record set:
   - **Name** – Enter the DNS name you used for the primary firewall.
   - **Type** – Select **A - IPv4 address**.
   - **Alias** – Select **No**.
   - **TTL (Seconds)** – Set the number of seconds the DNS records can be cached by non-authoritative DNS servers.
   - **Value** – Enter the EIP or public IP address for the secondary firewall.



7. In the right column, configure the **Routing Policy**:
   - **Routing Policy** – Select **Failover**.
   - **Failover Record Type** – Select **Secondary**.
   - **Set ID** – Enter a unique ID to differentiate from other failover record sets using the same name and type.



8. In the right column, configure the **Health Check**:

- **Associate with Heath Check** – Select **No**.

9. Click **Create**.

Both record sets for the primary and secondary firewalls are now listed in the hosted zone.

Figures