AWS VPN Connection Procedure

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>March 19, 2019</td>
<td>Technical Operations</td>
</tr>
</tbody>
</table>

1. Purpose

Amazon makes the process of setting up a hardware VPN simple on AWS. As of August 2017, the cost of one VPN connection with single redundancy is $0.05/hour. The AWS VPN gives the user 2 tunnels with separate internal IP addresses for redundancy. When it is time for a customer to connect to the VPN, they give a few pieces of information to HSX, which HSX uses to automatically generate a document for the other party’s network team with connection information.

2. Scope

All employees, interns, contractors, members, participants, and third parties who may have access or exposure to HSX information assets are required to comply with this process.

3. Procedure

Creating a VPN

Note: Before starting, use the HSX VPN Connection Checklist to get the information needed from the connecting entity including the IP address, and VPN hardware specifications including manufacturer, model, and version number.

1. HSX connects to VPNs by linking the internal HSX AWS network with the client’s network, instead of a client to server connection. An AWS hardware VPN is the best way to do this, as it fully manages capacity and redundancy automatically.

2. Go to the VPC section of the AWS console. The navigation frame on the left side of the page will have a heading called “VPN Connections”. Click on Virtual Private Gateways.
3. Click “Create Virtual Private Gateway”. Give the virtual private gateway a name related to its function.

4. Next, click “Customer Gateways” on the left navigation column.

5. Create a new customer gateway. This represents the virtual point of contact to the outside party. Use the gateway address provided to you by the client where prompted.

6. Click on “VPN Connections” on the left side navigation column, then click the blue “Create VPN Connection” button.

7. The form on this page creates a hardware VPN that connects to client private networks. Give the VPN a suitable name and associate the virtual gateway and customer gateway (click the “Existing” radio button as shown below. Select the “Static” radio button. In the form that appears below, enter the IP prefixes (in CIDR notation) that the VPC can use to allocate IPs to VPN clients.
Click the blue “Create VPN Connection” button on the bottom right to launch the VPN.

8. Click on the new VPN on the VPN Connections page. Add the necessary static routes this VPN will use, in CIDR notation.

9. Add the necessary IPs to the route table and point them to the virtual gateway.
Ensure there is a subnet for related groups of VPN connections and an adequate supply of addresses. Associate subnets with the relevant route table. If this is not specified, it will use the route table designated as “Main”.

Connecting HSX to Client VPNs

1. Amazon engineered their VPN system to simplify the connection process. Once the VPN is fully set up in an HSX VPC, HSX must use the client’s hardware VPN information collected by project managers.

2. AWS VPC automatically generates a document that the client’s network engineers will use to finalize the connection. From the VPC web console, click on “VPN Connections” under the VPN Connections heading.

3. Select the VPN you wish to connect, and click “Download Configuration”

4. Using the information about the client’s VPN hardware, select the vendor (e.g. Cisco or Juniper), select the platform (e.g. SRX or ASA), and select the version (e.g. ASA 9.x or JunOS 11.0)
5. Click download to save the automatically generated configuration document. Send this to the client so their network engineers can use it to configure their hardware VPN.

4. Definitions

Refer to the HSX glossary for all definitions.

5. References

<table>
<thead>
<tr>
<th>Procedure Owner</th>
<th>Technical Operations</th>
<th>Contact</th>
<th>Approved By</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian Wells</td>
<td></td>
<td><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Approved By Brian Wells

Approval Date March 19, 2019
<table>
<thead>
<tr>
<th>Date Procedure In Effect</th>
<th>Version #</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 6, 2017</td>
<td>1.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Previous Approval Date</th>
<th>Last Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 6, 2017</td>
<td>October 26, 2023</td>
</tr>
</tbody>
</table>

- Encryption
- Endpoint protection
- Information security
- Network protections
- Remote Access