**SBIT Documentation**

Randal McClure

February 28, 2018

Table of Contents

[**Introduction** 3](#_Toc507616437)

[**Important Notes** 4](#_Toc507616438)

[**Before…** 5](#_Toc507616439)

[**Create an IAM User:** 5](#_Toc507616440)

[**Create a Key Pair:** 6](#_Toc507616441)

[**Configuring AWS CLI:** 7](#_Toc507616442)

[**During…** 8](#_Toc507616443)

[**Required Information (from user):** 8](#_Toc507616444)

[**After…** 12](#_Toc507616445)

[**Configure Palo Alto Firewall:** 12](#_Toc507616446)

[**Customize Configuration:** 14](#_Toc507616447)

[*Change your public IP:* 15](#_Toc507616448)

[*Change the Peer Addresses and Pre-Shared Keys:* 15](#_Toc507616449)

[*Double Check the Inside Tunnel IPs:* 16](#_Toc507616450)

[**Create GlobalProtect VPN:** 18](#_Toc507616451)

[*Generate Certificates:* 18](#_Toc507616452)

[*Create an SSL/TLS Service Profile:* 19](#_Toc507616453)

[*Create an Authentication Profile:* 20](#_Toc507616454)

[*Configure a GlobalProtect Portal:* 20](#_Toc507616455)

[*Create a GlobalProtect Gateway:* 22](#_Toc507616456)

[*Create GlobalProtect Users:* 23](#_Toc507616457)

[*Commit Configuration Changes:* 23](#_Toc507616458)

[*Test GlobalProtect VPN:* 24](#_Toc507616459)

[**Additional Actions** 25](#_Toc507616460)

[**Creating Additional Users in Active Directory:** 25](#_Toc507616461)

[**Creating Additional Groups in Active Directory:** 26](#_Toc507616462)

[**Adding Users to Groups:** 27](#_Toc507616463)

[**Creating Mailboxes for Users:** 27](#_Toc507616464)

[**General Environment Documentation** 28](#_Toc507616465)

[**Server Documentation:** 28](#_Toc507616466)

[**AWS Network Documentation:** 30](#_Toc507616467)

# **Introduction**

SBIT: The Small Business IT Server Builder is an automation solution that builds an entire small business server environment in the Amazon Web Services cloud. This environment contains several features that a small business might need or find useful. The following features provide a launching point for many small businesses:

* Active Directory Domain Services
* File Servers
* An Exchange Server
* A Site-to-Site VPN
* (Optional) A Remote Access VPN.

The goal of SBIT is to allow small businesses and start-ups to defer the cost of building a server infrastructure until after the business has reached its break even point, or as long as possible. By automating the creation and subsequent configuration of these features in the cloud, a small business doesn’t need to pay upfront for server hardware nor for an expensive IT professional to build and manage the business’ environment. SBIT could also be used to create a testing environment for software developers.

Users of SBIT will download the SBIT files, extract them, then follow the instructions included in this document to create their server environment. For a general overview of these steps, a user must create an AWS account, create a few prerequisite objects in AWS, execute the SBIT script, complete a few final steps, and, optionally, follow the instructions to create a Remote Access VPN. More detail on these steps can be found later in this document. The instructions creating either VPN connection type have been created and tested for a Palo Alto VM-Series PanOS version 8.0.0 firewall. A list of other supported firewalls can be found at: https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#DevicesTested

# **Important Notes**

The following important notes reference the current build of SBIT. Most of these notes detail current limitations or known bugs. (Many of these notes are for the developer.)

* SBIT has only been tested in the **us-east-2** region of AWS. Most of the components include the parameters for other regions, but the functionality has not been implemented.
* SBIT only supports 2 Domain Controllers. The number entered here isn’t used by the script.
* SBIT only supports 2 File Servers. The number entered here isn’t used by the script.
* The number entered for File Server Storage may not validate properly.
* The file servers don’t actually make second drives. The script is written, but not implemented. It was once implemented but removed because testing was much too expensive and there were other issues that needed to be fixed before continuing. This may be implemented before the presentation.
* Passwords entered into SBIT are NOT secured. SBIT does not display the password, but the password may be transmitted in cleartext and may be stored in AWS instance log files if errors occur.
* The user’s public IP can technically reside behind a device performing NAT, however this functionality is untested and not recommended.

# **Before…**

Before using SBIT, you must create an account with Amazon Web Services. You can do thing by going to **https://aws.amazon.com/** and clicking on **Sign-Up**. Once you have an account there are a few tasks that you must complete before running the SBIT script.

## **Create an IAM User:**

Before execution of SBIT, users should create a separate IAM user with administrative access:

1. Log in to your AWS console.
2. Scroll down to the section titled **Security, Identity & Compliance** and click on the **IAM** link.
3. In the Navigation Pane on the left, click **Groups**.
4. Click the **Create New Group** Button.
5. Give the group a meaningful name (for example, ‘Administrators’). Click Next.
6. In the search/filter box, type ‘AdministratorAccess’ and tick the box next to **AdministratorAccess** in the list. Click **Next**.
7. Click **Create Group**.
8. In the Navigation Pane, click **Users**.
9. Click **Add User**.
10. Give the user a name.
11. Under **Select AWS Access Type**, tick both boxes.
12. Give the user a custom password.
13. Untick **Require password reset**. Click **Next**.
14. Click **Add user to group**.
15. Tick the box next to the group you created in Steps 3-7. Click **Next**.
16. Verify the information and click **Create User**.
17. Make a note of the user’s **Access Key** and **Secret Key**. These are needed to use SBIT.

Note: Keep these stored in a safe place; if the secret key is lost or otherwise compromised, you will have to generate a new user.

1. Click **Close**.

## **Create a Key Pair:**

1. Log into your AWS Console.
2. Find the **Compute** section and click the **EC2** link.
3. In the Navigation Pane, under **Network and Security**, click **Key Pairs**.
4. Click **Create Key Pair**.
5. Give the key pair a name. The name has little impact but should be meaningful.

Note: Be sure to download the key file as you CANNOT download it later. This will be the last time you can download the key file. The key file must be stored in a secure location. If the key file is lost, you must regenerate a new key and must use the AWS Console to reconfigure all instances to use the new key.

1. The name of this key pair will need to be entered when running SBIT.

Note: SBIT will use this one key pair to secure access to all instances. Again, all instances will use the same key file to secure access.

## **Configuring AWS CLI:**

After a separate IAM account has been created and enabled for programmatic access, the Access and Secret Access Keys must be configured in the AWS CLI.

1. Install Python 3.6.4 onto the computer from which SBIT will be run.
2. Follow Amazon’s online documentation to install the AWS CLI.
3. Install Boto3 (the Python SDK for AWS).
4. Once these three things are installed, open a **Command Prompt**. This can be done by pressing the Windows key and typing **cmd**.
5. When the Command Prompt opens, type **aws configure** and press enter.
6. Enter the Access Key, Secret Key, AWS Region, and Output Format when prompted.

Note: The AWS Region determines where the instances created by SBIT will be placed. This should generally be the nearest AWS region to your on-site location. The output type determines how information is returned to the user and is more or less unimportant to the execution of SBIT.

1. When finished, you can close the Command Prompt.

# **During…**

## **Required Information (from user):**

Before execution of SBIT, users must have the following information available. The SBIT script will ask for all of the following information. (Actual prompt text is included in italics.)

**Domain name:**

*Enter your Domain Name (Ex. "example.com"):*

* If you want the domain name to be accessible by the public, for a web server for example, you should purchase a domain name from any reputable domain name registrars. I purchased my domain from GoDaddy.
* If you do not want the domain to be accessible by the public and the domain will be entirely private, you can choose any domain name that you would like, within the standard domain naming rules.

Note: At the current stage of development on SBIT, this domain can be anything. Currently, there are no components that need public DNS records, therefore you don’t need to worry about someone else having your domain name.

**NetBIOS Name of the Domain:**

*Enter the NetBIOS name of the domain (Ex. "EXAMPLE"):*

* This is a shortened version of the domain name and is required for certain steps in SBIT. This name is typically the domain name in all capital letters without the root domain attached.
  + For example, the ‘example.com’ domain name might have ‘EXAMPLE’ as the NetBIOS name.

**Key Pair name:**

*Enter the name of the Key Pair (used when accessing instances):*

* You will need the key pair in order to access instances. You must have this in order to manage your servers.
* The key pair must be created before the script is executed. See Create a Key pair

**Number of Domain Controllers:**

*How many Domain Controllers? [Leave blank to use default of 2]:*

* Default: 2
* Can be anywhere between 2 and 8,
  + Two provides redundancy and availability, enough for most very small businesses
  + Four provides even more redundancy
  + More than 4 is likely overkill for most target businesses, save those with extremely high employee counts
* This number will be split across two availability zones

**Number of File Servers:**

*How many File Servers? [Leave blank to use default of 2]:*

* Default: 2
* Can be anywhere between 2 and 4
* These will be split across two availability zones

**File Server Storage:**

*How much storage would you like (in GiBs) on file servers?:*

* The size of the second volume (“extra drives”) which will be added to file servers, specifically for shares
* Can be between 10 (GiB) and 1500 (GiB), no default

**Exchange Server Storage:**

*How much storage would you like (in GiBs) on the Exchange server?:*

* This parameter determines the size of the root volume (the size of the C drive). This is needed as the default size of 30GB is not enough to install Exchange.

Note: 33 is the minimum number that should be entered here. Much more should be entered if the environment is to be used in actual production. 33GB is only enough for basic testing and should not be used in a production deployment.

**Instance Types:**

*Enter the instance type to use for Domain Controllers [Default: t2.micro]:*

*Enter the instance type to use for File Servers [Default: t2.micro]:*

*Enter the instance type to use for Exchange servers [Default: r4.large]:*

* DCs, File, and Exchange servers can be set independently
* Instance type determines resources available to server (memory, CPU, etc.) as well as cost.
* Type r4.large is the lowest recommended size for Exchange servers. I have tested with smaller (cheaper) instances, but the Exchange installation or configuration fails, or problems arise without enough resources.
* Type t2.micro lies within the free tier. For the first year of AWS use, users are granted up to 750 hours of free t2.micro use per month. Charges for other services or licenses may still apply.

**Domain Administrator Username and Password:**

*Enter a username for the domain administrator account (separate account from the default "Administrator" account):*

*Enter a password for the domain administrator account:*

* Domain Admin user will be added to domain and given domain admin permissions
* Safer/more secure than using default Admin account

Note: Without this secondary domain admin user, I would need to halt script execution after the Active Directory was configured and ask the user for the default Windows password of the DC1 domain controller instance. This is because the DC1 default password is the password of the default Domain Administrator account. This secondary user allows me to gather information once, and only once, from the user.

**Domain Restore Mode Password:**

*Enter a password for Active Directory Restore Mode:*

* Required for Active Directory
* Allows users to put domain in “Restore Mode” in case of server impairment or possible attack.

**Static, Publicly-Routable IP Address:**

*Enter the public IP of the firewall:*

* This can typically be obtained from an ISP. This component is required to create the site-to-site VPN, which gives the on-premise network access to the SBIT environment.
* This IP CANNOT be a private IP (see RFC 1918).
* This IP can reside behind a device performing NAT translation.

# **After…**

## **Configure Palo Alto Firewall:**

Before anything may be done with the firewall, you must have access to the device to manage it. Follow these steps to get access to the web console and import a pre-built configuration. The pre-built configuration sets up a site-to-site VPN between your firewall and AWS, giving you access to your servers.

Note: These instructions have been tested with the Palo Alto VM-Series Firewall. The steps should be identical for physical devices; however, they have not been tested on such devices.

1. Connect the firewall device to the network. You should follow the manufacturer’s instruction on how best to do this.
2. Connect to the device, either through the console port on the device, or via SSH session. If using the VM-Series firewall, you can simply use your hypervisor’s built-in virtual desktop connection (Note: The name of this feature may differ based on the hypervisor.)
   1. The default Palo Alto admin credentials are as follows:
      1. Username: **admin**
      2. Password: **admin**
3. Run the following commands in the firewall’s command line:

**configure**

**set deviceconfig system type static**

**set deviceconfig system ip-address 10.0.52.2 netmask 255.255.255.0 default-gateway 10.0.52.1**

These commands configure the device with an IP address so that it can be managed through the web console.

1. Go to **https://10.0.52.2/** and log in with the Username and Password from above.
2. Click **OK** to ignore the warning. The warning says that you should change the default administrator password. We will do this in an upcoming step.
3. If a series of welcome popups appear, click **Close**.
4. Click **Device** on the top navigation bar.
5. In the action pane, click the **Operations** subtab.
6. Click **Import named configuration snapshot**.
7. Click browse and navigate to the SBIT folder and select the **SBIT-PA-config.xml** file. Click **Open**, then **OK**.
8. When the import is complete, click **Load named configuration snapshot**.
9. Click the dropdown arrow and select the **SBIT-PA-config.xml** file that you just imported.
10. Leave the *Decryption Key* field empty and click **OK**.
11. Click **Administrators** in the left navigation pane. Click **admin** in the action pane. Enter **#Disaster8dR** as the *Old Password*. Enter a new password for the **admin** user. This password should be at least 8 characters in length and should contain at least one uppercase letter, lowercase letter, number, and symbol.
12. You may want to create another administrative user. To do this, click **Add** in the bottom left corner of the action pane.
13. Click **Commit** in the upper right corner of the console and click **OK** to apply the changes.

Note: Once the changes have been committed, you should disable DHCP on any wireless routers (or similar devices running the DHCP service). Part of the above configuration creates a DHCP server that integrates with SBIT. Any other DHCP servers must be disabled or network connectivity issues may arise.

## **Customize Configuration:**

Before the firewall can properly communicate with the AWS environment created by SBIT, you must change a few fields with your custom information.

1. Log into your AWS management console and navigate to the **Console Home**.
2. Scroll down to the section titled **Networking & Content Delivery**.
3. Click **VPC**.
4. In the navigation pane on the left, find the **VPN Connections** section and select **VPN Connections**.
5. Check the box to select **SBIT VPN Connection**.
6. Click **Download Configuration**.
7. Select **Palo Alto Networks** for the *Vendor*.
8. Select **PA Series** for the *Platform*.
9. Select **PANOS 7.0+** for the *Software*.
10. Click **Download** and save the configuration information in the SBIT folder. This file will henceforth be called the AWS VPN Configuration file.

You will need some of the information contained in this configuration file for the VPN connection. (I recommend using Notepad++, or some other text editor that displays line numbers, as I will be referencing the line numbers of specific information in the following steps.)

### *Change your public IP:*

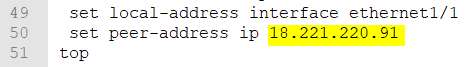
1. Go to **https://10.0.52.2**/ and log in with the **admin** username and password.
2. Click **Objects** in the top navigation bar.
3. Click **Addresses** in the left navigation pane.
4. Click **External Interface Address** and change **69.27.22.232/24** to your public IP and subnet. You should have acquired this information from your ISP (or from whomever you were assigned your public IP).

### *Change the Peer Addresses and Pre-Shared Keys:*

1. Go to **https://10.0.52.2**/ and log in with the **admin** username and password.
2. Click **Network** in the top navigation bar.
3. Expand the **Network Profiles** section in the left navigation pane.
4. Click **IKE Gateways**.
5. Click **SBIT-Ike-GW-0**.
6. Replace the **Pre-shared Key** and **Confirm Pre-shared Key** with the string of random characters found at the end of *Line 47* of the AWS VPN Configuration file you downloaded earlier.



1. Replace the **Peer IP Address** with the IP address found on *Line 50* in the AWS VPN Configuration file.



1. Click **OK**.
2. Click **SBIT-Ike-GW-1**.
3. Replace the **Pre-shared Key** and **Confirm Pre-shared Key** with the string of random characters found at the end of *Line 188* of the AWS VPN Configuration file you downloaded earlier. (See example figure for step 6.)
4. Replace the **Peer IP Address** with the IP address found on *Line 191* in the AWS VPN Configuration file. (See example figure for step 7.)
5. Click **OK**.
6. Click **Commit** in the top right corner of the console and click **OK** to apply the changes.

### *Double Check the Inside Tunnel IPs:*

1. Go to **https://10.0.52.2**/ and log in with the **admin** username and password.
2. Click **Network** in the top navigation bar.
3. Click **Interfaces** in the left navigation pane.
4. Click the **Tunnel** tab.
5. Ensure that the **IP Address** column for **tunnel.1** is the same IP as the one found on *Line 88* of the AWS VPN Configuration file.

If these IPs are identical, you can skip steps 6-20. If these IPs are not the same, continue with step 6.

1. Click **tunnel.1**, then click the **IPv4** tab.
2. Click the IP in the box and replace it with the IP found on *Line 88* in the AWS VPN Configuration File, leaving the **/30** appended to the end.
3. Click **OK**.
4. Click **tunnel.2**, then click the **IPv4** tab.
5. Click the IP in the box and replace it with the IP found on *Line* 229 in the AWS VPN Configuration File, leaving the **/30** appended to the end.
6. Click **OK**.
7. Click **Policies** in the top navigation bar.
8. Click **Policy Based Forwarding** in the left navigation pane.
9. Click **SBIT-AWS-Routing-Policy-0**, then click the **Forwarding** tab.
10. Change the **Next Hop** and **IP Address** fields to the IP address found on *Line 146* in the AWS VPN Configuration file.
11. Click **OK**.
12. Click **SBIT-AWS-Routing-Policy-1**, then click the **Forwarding** tab.
13. Change the **Next Hop** and **IP Address** fields to the IP address found on *Line 287* in the AWS VPN Configuration file.
14. Click **OK**.
15. Click **Commit** in the upper right corner of the console to save the changes.

You can monitor the state of the tunnels to make sure the connection has been established properly. Click **Network** in the top navigation bar, then **IPSec Tunnels** in the left navigation pane. The circle in the **Status** tab will turn green when the connection is active and working. It may take a few moments for the status to turn green after the changes have been committed.

## **Create GlobalProtect VPN:**

Follow the next steps if your business would like (or needs) a Remote Access VPN into your network. Palo Alto’s implementation of this type of VPN is called GlobalProtect.

For convenience, a configuration file (like **SBIT-PA-config.xml**) called **SBIT-GP-Demo.xml** is included in the SBIT files. This configuration has a sample GlobalProtect VPN pre-configured for you to explore. This configuration will not work if implemented in production, rather it is included for you to reference as you follow these steps. You can follow the same steps as in the section called *Configure Palo Alto Firewall*, replacing **SBIT-PA-config.xml** with **SBIT-GP-Demo.xml**, to view this configuration. It might help to review this configuration to get a general idea of what to expect with these steps. Once familiar, switch the configuration yet again back to **SBIT-PA-config.xml**, then continue with the following steps.

### *Generate Certificates:*

1. Click the **Device** tab in the top navigation bar.
2. Expand **Certificate Management** in the left navigation pane and click **Certificates**.
3. Click **Generate** at the bottom of the action pane to create what is called a Certificate Authority Certificate (CA Cert).
4. Enter a meaningful name. (I called it *SBIT-GP-VPN-CA* in the demo.)
5. Enter your domain name into the *Common Name* field.
6. Check the **Certificate Authority** box.
7. Leave the *Signed By* field blank.
8. Click **Generate** to generate the certificate.
9. Click **Generate** at the bottom of the action pane to create what is called a Server Certificate (Server Cert).
10. Give this second certificate a meaningful name. (I called it *SBIT-GP-VPN-Cert* in the demo.)
11. Enter your public IP in the *Common Name* field.
12. Select the **CA Cert** (created in Step 3) for the *Signed By* field.
13. Uncheck the **Certificate Authority** box.
14. Click **Generate** to generate the certificate.

### *Create an SSL/TLS Service Profile:*

1. Click the **Device** tab in the top navigation bar.
2. Expand **Certificate Management** in the left navigation pane and click **SSL/TLS Service Profile**.
3. Click **Add** at the bottom of the action pane.
4. Give the profile a meaningful name. (I called it *SBIT-GP-VPN-Cert-Profile*)
5. Select the **Server Cert** (created in Step 9 of the *Generate Certificates* section) in the *Certificate* field.
6. Click **OK** to save the SSL/TLS Service Profile.

### *Create an Authentication Profile:*

1. Click the **Device** tab in the top navigation bar.
2. Click **Authentication Profile** in the left navigation bar.
3. Click **Add** at the bottom of the action pane.
4. Enter a meaningful name. (I called it *Local DB Auth Profile* in the demo.)
5. Click the **Authentication** tab.
6. In the *Type* field, select **Local Database**.
7. Click the **Advanced** tab.
8. In the *Allow List* box, click **Add**.
9. Select **all**.
10. Click **OK** to save the Authentication Profile.

### *Configure a GlobalProtect Portal:*

1. Click the **Network** tab in the top navigation bar.
2. Expand the **GlobalProtect** section and click **Portals**.
3. Click **Add** at the bottom of the action pane.
4. Click the **General** tab.
5. Enter a meaningful name. (I called it *SBIT-GP-VPN-Portal* in the demo.)
6. In the *Network Settings* box, select **ethernet1/2** for the *Interface* field and **External Interface Address** for the *IPv4 Address* field.
7. Click the **Authentication** tab.
8. In the *Server Authentication* box, select the **SSL/TLS Service Profile** (created in the *Create an SSL/TLS Service Profile* section)
9. In the *Client Authentication* box, click **Add**.
10. Enter a meaningful name in the *Name* column. (I called it *SBIT-GP-VPN-client-auth* in the demo.)
11. In the *Authentication Profile* column, select the **Authentication Profile** (created in the *Create an Authentication Profile* section)
12. Click the **Agent** tab.
13. In the *Agent* (top) box, click **Add**.
14. Click the **Authentication** tab of the new window.
15. Enter a meaningful name. (I called it *SBIT-GP-agent-config* in the demo.)
16. Click the **External** tab of the new window.
17. In the *External Gateways* box, click **Add** in the top box.
18. Enter a meaningful name. (I called it *SBIT-GP-VPN-external-gateway* in the demo.)
19. Click the **IP** button (**FQDN** should NOT be selected).
20. In the *IPv4* box, enter your **Public IP**.
21. In the *Source Region* box, click **Add**, then select **Any**.
22. Click **OK** to create the gateway for the portal.
23. Click **OK** to create the agent configuration.
24. In the *Trusted Root CA* box, click **Add**.
25. Select the **CA Cert** (created in Step 3 of the *Generate Certificates* section)
26. Click **OK** to finish creating the GlobalProtect Portal.

### *Create a GlobalProtect Gateway:*

1. Click the **Network** tab in the top navigation bar.
2. Expand the **GlobalProtect** section and click **Gateways**.
3. Click **Add** in the bottom of the action pane.
4. Click the **General** tab.
5. Enter a meaningful name. (I called it *SBIT-GP-VPN-Gateway* in the demo.)
6. In the *Network Settings* box, select **ethernet1/2** for the *Interface* field and **External Interface Address** for the *IPv4 Address* field.
7. Click the **Authentication** tab.
8. In the *Server Authentication* box, select the **SSL/TLS Service Profile** (created in the *Create an SSL/TLS Service Profile* section)
9. In the *Client Authentication* box, click **Add**.
10. Enter a meaningful name in the *Name* column. (I called it *SBIT-GP-VPN-client-auth* in the demo.)
11. In the *Authentication Profile* column, select the **Authentication Profile** (created in the *Create an Authentication Profile* section)
12. Click the **Agent** tab.
13. Click the **Tunnel Settings** tab in the new window.
14. Check the box to enable **Tunnel Mode**.
15. Select **tunnel.3** for *Tunnel Interface*.
16. Click the **Client Settings** tab. Click **Add** in the box.
17. Click the **Authentication Override** tab.
18. Enter a meaningful name. (I called it *SBIT-GP-Gateway-client-config* in the demo.)
19. Click the **IP Pools** tab.
20. In the *IP Pool box*, click **Add**.
21. Type **192.168.0.50-192.168.0.250** in the field.
22. Click the **Split Tunnel** tab.
23. Click **Add** in the *Includes* box.
24. Type **0.0.0.0/0** in the field.
25. Click **OK** to finish creating the client configuration.
26. Click the **Network Services** tab.
27. Type **172.16.0.10** in the *Primary DNS* field and **172.16.1.10** in the *Secondary DNS* field.
28. Click OK to finish creating the GlobalProtect Gateway.

### *Create GlobalProtect Users:*

Before users can make use of the VPN, they must be added to the firewall’s local database.

1. Click the **Device** tab.
2. Expand the *Local User Database* section and click **Users**.
3. Click **Add** at the bottom of the action pane.
4. Enter the user’s **Username** and **Password**.
5. Click **OK** to create the user.

Users can be added at any time by following the steps below then clicking **Commit** at the top right corner of the console.

### *Commit Configuration Changes:*

1. Click **Commit** in the top right corner of the screen. Click **Commit** and wait for changes to be applied.

Note: Before committing your changes be sure to create Network Address Translation (NAT) rules and Security rules. These will allow your VPN users to access your network. Without these rules, your users will be able to “connect” to the network but will be denied access to all resources within the network.

### *Test GlobalProtect VPN:*

1. On a device connected to a separate network (simulating a remote user), open a browser and navigate to **https://<your public IP>/** (Ex. **https://69.27.22.232/)**.

Note: If a warning appears due to an “Incorrectly configured web page” or similar error, continue to the page or create an exception. This is due to the “self-signed” certificate we created.

1. Enter the **username** and **password** of a user created in the *Create GlobalProtect Users* section.
   1. If the login succeeds, the VPN configuration was successful. If the login fails, try to troubleshoot, check that all of your information is correct, and/or start over at the section titled *Configure Palo Alto Firewall*, skipping the command line steps.
2. Attempt to access a few resources in the network.
   1. If access succeeds, your Security and NAT rules work properly. If access fails, try to troubleshoot your Security and NAT rules. They may be blocking access to your resources inadvertently.

# **Additional Actions**

## **Creating Additional Users in Active Directory:**

It is highly unlikely that small businesses have only one employee. Therefore, additional users must be created. SBIT does not currently cannot to create these users automatically, so they will need to be created manually. Instructions can also be found on the Microsoft TechNet website.

1. Log into a domain controller with the username and password you created when running the SBIT script.
2. Open the **Active Directory Users and Computers** snap-in.

Note: One way this can be done is to press the Windows key and type ‘Active Directory Users and Computers’ and press **Enter**. Another way is to open the Server Manager, click **Tools** in the top right corner, then click **Active Directory Users and Computers**.

1. Expand the domain name.
2. Click on the **AWS OU** folder icon to navigate to the *AWS Organizational Unit*.
3. Click **Add User** (Icon looks like a single person) in the toolbar.
4. Fill in the user’s information, then click **Next**.
5. Enter the user’s password and confirm it.
6. Uncheck the **User must change password at next logon** box if the user should use the password entered in step 7. Leave the box checked if the password is generic and the user should create their password on their first logon.
7. Ensure the remaining boxes are unchecked. Click **Next**.
8. Confirm the information and click **Finish**.

## **Creating Additional Groups in Active Directory:**

Once you have more users, you may want to organize those users into groups. These groups can be used for assigning permissions to files and server administration tasks. SBIT does not currently cannot to create these users automatically, so they will need to be created manually. Instructions can also be found on the Microsoft TechNet website.

1. Log into a domain controller with the username and password you created when running the SBIT script.
2. Open the **Active Directory Users and Computers** snap-in.

Note: One way this can be done is to press the Windows key and type ‘Active Directory Users and Computers’ and press **Enter**. Another way is to open the Server Manager, click **Tools** in the top right corner, then click **Active Directory Users and Computers**.

1. Expand the domain name.
2. Click on the **AWS OU** folder icon to navigate to the *AWS Organizational Unit*.
3. Click **Add Group** (Icon looks like a group of people) in the toolbar.
4. Enter a **Group Name**.

Note: Leave the *pre-Windows 2000* field as-is. This field is needed for backwards compatibility but will likely not be needed.

1. In the *Group Scope* box, click the button next to **Global**.
2. In the *Group Type* box, click the button next to **Security**.
3. Click **OK** to create the group.

## **Adding Users to Groups:**

Groups are next to useless if users are not added to them. There are several ways to add users to groups. The following instructions detail one method of adding a single user to one or more groups. More methods can be found on the Microsoft TechNet website.

1. Log into a domain controller with the username and password you created when running the SBIT script.
2. Open the **Active Directory Users and Computers** snap-in.

Note: One way this can be done is to press the Windows key and type ‘Active Directory Users and Computers’ and press **Enter**. Another way is to open the Server Manager, click **Tools** in the top right corner, then click **Active Directory Users and Computers**.

1. Expand the domain name.
2. Click on the **AWS OU** folder icon to navigate to the *AWS Organizational Unit*.
3. Right-click on a user.
4. Select **Add to a Group…**
5. Enter the name of one or more groups, separated by a semi-colon.
6. Click **Check Names**. If there are any errors, check to make sure the name of the group is correct.
7. When the names are correct, click **OK**.

## **Creating Mailboxes for Users:**

After a user has been created, a mailbox must be created manually for that user. SBIT cannot currently do this automatically. These instructions detail how to create a mailbox for a single existing user. For other methods of adding mailboxes, see the Microsoft TechNet website.

1. While connected to the on-premises network, open a browser and navigate to **https://exch1.<your domain>/ecp/** (For example, **https://exch1.example.com/ecp/** ).
2. Log in with the administrator username and password you specified when running SBIT.
3. In the left navigation pane, click **Recipients**.
4. Click **Mailboxes** in the top navigation bar.
5. Click **Add Mailbox (+)** and select **User Mailbox**.
6. Enter an alias for the user.
7. Click the **Existing User** button.
8. Click **Browse**.
9. Select the user that needs a mailbox created, then click **OK**.
10. Click **Save**.
11. Test the mailbox by sending an email to and from the user.

# **General Environment Documentation**

The following information includes IP addresses, hostnames, roles, and other information about each server. Replace **example.com** with your custom domain name to maintain accuracy.

## **Server Documentation:**

DC1.example.com

IP Address: 172.16.0.10/24

Installed Roles:

* Active Directory Domain Services
* DNS

Users created by SBIT are located in the ‘AWS OU’ organizational unit. This organizational unit can be found directly under the domain in Active Directory Users and Computers.

DC2.example.com

IP Address: 172.16.1.10/24

Installed Roles:

* Active Directory Domain Services
* DNS

Users created by SBIT are located in the ‘AWS OU’ organizational unit. This organizational unit can be found directly under the domain in Active Directory Users and Computers.

FS1.example.com

IP Address: 172.16.0.20/24

Installed Roles:

* File Services
* File Server Resource Manager
* Distributed File System Namespace
* Distributed File System Replication

FS2.example.com

IP Address: 172.16.1.20/24

Installed Roles:

* File Services
* File Server Resource Manager
* Distributed File System Namespace
* Distributed File System Replication

EXCH1.example.com

IP Address: 172.16.0.30/24

Installed Roles:

* Exchange Server 2016 Mailbox Service (and all constituent components)
* Internet Information Services (specifically for Exchange, not recommended to use this server as an actual web server)

## **AWS Network Documentation:**

Virtual Private Cloud:

*Capstone VPC*

Subnet ID: 172.16.0.0/22

* This VPC houses the entire SBIT network and server environment.

Subnets:

*PrivSub1*

Subnet ID: 172.16.0.0/24

*PrivSub2*

Subnet ID: 172.16.1.0/24

*PubSub1*

Subnet ID: 172.16.2.0/24

NAT Gateway:

*NAT Gateway*

* This gateway creates additional cost as it requires an Elastic IP from Amazon. It is a small hourly charge but is required to allow SBIT to configure instances properly. This object should be safe to delete as long as SBIT completes successfully. Routes in each subnet’s route tables should be updated to remove the route to this gateway.

Developer’s Note: It’s feasible that the user could change the route to send all unknown (0.0.0.0/0) traffic to the VPN gateway. The environment would then relay through the on-premise environment for internet access.

Internet Gateway:

*InternetGW*

* This gateway provides internet access to any instances assigned a public IP address.
* This gateway is free but requires instances to have a public IP.
  + Instances can either have an ephemeral IP, which changes whenever the instance is rebooted, or an Elastic IP, which costs a little extra (same as the NAT gateway).
* This gateway is pretty much only used by instances in the PubSub1 public subnet.

Customer Gateway:

*SBIT Customer Gateway*

* This gateway is an object that represents the on-premise firewall.
* This object contains the user’s public IP address as found on the firewall.

Virtual Private Gateway:

*SBIT VPN Gateway*

* This object represents the Amazon side of the Site-to-Site VPN.

VPN Connection:

*SBIT VPN Connection*

* This object represents the VPN connection and tunnels (as seen by AWS).
* Information contained in this object:
  + Peer IP Addresses, used to configure the firewall
  + IP addresses used inside each VPN tunnel
  + Routes advertising what subnets in the on-premise network are accessible to the VPC