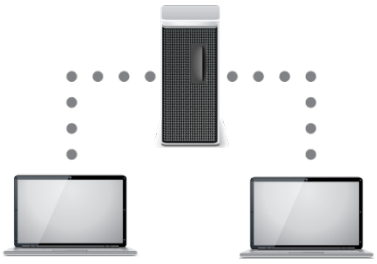
celestix

Celestix SecureAccess AWS Deployment Guide



SecureAccess

Table of Contents

1 Overview

The following sections describe an overview of the AWS components required to provision a SecureAccess server. Detailed deployment steps are described in sections 2 to 5.

1.1 AWS Account

If you haven't created an account already, setup an AWS account to utilize the various AWS resources that are needed to provision Celestix SecureAccess server. Once you have completed the account setup you will be presented with the AWS Management Console.

1.2 Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) is the networking layer for Amazon EC2. A Virtual Private Cloud is a virtual network logically isolated from other virtual networks in the AWS cloud.

- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC.
- You can configure your VPC by modifying its IP address range, create subnets, and configure route tables, network gateways, and security settings.

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.

If your account supports the EC2-VPC platform only, it comes with a default VPC that has a default subnet in each Availability Zone. If you have a default VPC and don't specify a subnet when you launch an instance, the instance is launched into your default VPC. You can launch instances into your default VPC without needing to know anything about Amazon VPC.

You can create your own VPC, and configure it as you need. This is known as a nondefault VPC. This gives you complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. Subnets that you create in your nondefault VPC and additional subnets that you create in your default VPC are called nondefault subnets.

1.3 Internet Gateway

An internet gateway enables your instances to connect to the internet through the Amazon EC2 network edge. You control how the instances that you launch into a VPC access resources outside the VPC.

Your default VPC includes an Internet gateway, and each default subnet is a public subnet. Each instance that you launch into a default subnet has a private IPv4 address and a public IPv4 address. These instances can communicate with the internet through the internet gateway.

1.4 Elastic IP addresses

An Elastic IP address is a static public IPv4 address associated with your AWS account and reachable from the Internet. With an Elastic IP address you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account. The public DNS hostname resolves to the public IPv4 address or the Elastic IP address of the instance outside the network of the instance and to the private IPv4 address of the instance from the network of the instance.

1.5 Security Groups

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance you can assign up to five security groups to the instance. A Security group acts at the instance level not subnet level. If you don't specify a security group at launch time, the instance will be automatically assigned to the default security group for the VPC. When you create a security group, it has no inbound rules. Therefore no traffic is allowed to the instance until inbound rules are added.

1.6 NAT Gateway or NAT instance

AWS offers two kinds of NAT devices – a NAT gateway or a NAT instance. A NAT gateway service is a managed service that does not require your administration efforts. A NAT instance is launched from a NAT AMI and requires basic settings to be configured. These devices are required only if you need resources in private network to connect to the Internet e.g. the scenario where you create VPC with Public and Private Subnets.

2 AWS Network & Security Configuration

2.1 Allocate Elastic IP address

1. An Elastic IP address is a public IPv4 address that you can allocate to your account. You can associate it to and from instances as you require, and it's allocated to your account until you choose to release it.
2. Navigate to the EC2 dashboard.
3. In the navigation pane under Network & Security choose Elastic IPs.
4. Choose Allocate new address.
5. On the Allocate new address page choose Allocate

2.2 Create a Security Group

1. Navigate to the EC2 dashboard.
2. In the navigation pane under Network & Security choose Security Groups.
3. Choose Create Security Group.

4. Specify a name and description for the security group – e.g. [Security group name: SecureAccess] [Description: Allow access to ports 3389 and 443 from anywhere].
5. For VPC, choose the VPC created in section 2.1.
6. For SecureAccess two rules need to be created – one rule to allow RDP (port 3389) access to the server and the other rule to allow access to HTTPS (port 443).
6. Select Inbound and choose Add Rule. For Type choose RDP. For Source choose Anywhere or choose Custom and enter specific IP addresses (in CIDR notation) to which RDP access is allowed.
7. Repeat the step for HTTPS rule – for Source select Anywhere.
8. Choose Create.

2.3 Create a Virtual Private Cloud (VPC)

1. In this step, you'll use the Amazon VPC wizard in the Amazon VPC console to create a VPC. The wizard performs the following steps for you:
2. Creates a VPC with a /16 IPv4 CIDR block (a network with 65,536 private IP addresses).
3. Attaches an Internet gateway to the VPC.
4. Creates a size /24 IPv4 subnet (a range of 256 private IP addresses) in the VPC.
5. Creates a custom route table, and associates it with your subnet, so that traffic can flow between the subnet and the Internet gateway.

To create a VPC wizard using the Amazon VPC wizard

1. Log in to AWS Management Console.
2. Open the Amazon VPC console listed in AWS Services under Networking and Content Delivery.
3. In the navigation bar, on the top-right, take note of the region in which you are creating the VPC. Ensure that you continue working in the same region as you cannot launch an instance into your VPC from a different region.
4. Choose Start VPC Wizard.
5. In the “Step 1: Select a VPC Configuration" wizard choose the option that suits your network requirement, and choose Select.
   Note: Select “VPC with Public and Private Subnets” if you plan to allow SecureAccess clients access to resources in the Private Subnet of the VPC in AWS. Select “VPC with Public and Private Subnets and Hardware VPN Access” if you plan to allow SecureAccess clients access to your corporate network.
6. In the Step 2 wizard, configure the VPC, Public and Private IPv4 CIDR blocks. (Note: Refer to the section “Setting up a test scenario” for detailed steps.)
7. For VPC name, Public subnet name and Private subnet name, you can name your VPC and subnets to help you identify them later in the console. You can specify your own IPv4 CIDR block range for the VPC and subnets, or you can leave the default values.

8. In step 5, if “VPC with Public and Private Subnets and Hardware VPN Access” is selected, refer to the VPC User Guide in AWS for details on how to configure the VPN connection between AWS and corporate network gateway.
9. In step 5, if you selected “VPC with Public and Private Subnets”, for Elastic IP Allocation ID there are two options:
    a. Use the default NAT gateway that is created in the public subnet
    b. Use a NAT instance that is created based on the instance type that you select.

For option (a) you must specify an Elastic IP address for your NAT gateway; if you don't have one you must first allocate one to your account. If you want to use an existing Elastic IP address, ensure that it's not currently associated with another instance or network interface. Refer section 2.1 for details on how to allocate an Elastic IP address.

For option (b) select the NAT instance type. The instance is automatically created.

10. Choose Create VPC. Navigate to Your VPCs in the VPC dashboard and verify the details.
11. In step 5, if you selected “VPC with Public and Private Subnets”, a security group has to be created to allow traffic from private subnet to the public subnet. Follow the steps in section 2.2 to create the security group. For Type select AllTraffic and for Source configure the private subnet.
6. Go to EC2 instances view and select the NAT instance (should be the one without a name). Assign a name to the NAT instance for better identification. Choose Actions menu and choose Networking->Change Security Groups. Check the security group and choose Assign Security Groups.

3 Provisioning Celestix SecureAccess

1. Navigate to the EC2 dashboard.
2. Click Launch Instance button on the middle pane.
3. In the “Step 1: Choose an Amazon Machine Image” wizard, under Quick Start select AWS Marketplace.
4. In the “Search AWS Marketplace Products” search box enter “Celestix SecureAccess” and press Enter key and choose Select.
5. Verify the product information and choose Continue.
6. In the “Step 2: Choose an Instance Type” wizard, select the appropriate instance configuration that corresponds to Celestix licence and choose “Next: Configure Instance Details”.
7. In “Step 3: Configure Instance Details” wizard, choose the VPC created in section 2.1 as Network, choose the public subnet for Subnet.
8. In the Network Interfaces configuration, set the primary IP to an IP address in the range of public subnet addresses. Choose “Next: Add Storage”.

9. In “Step 4: Add Storage”, modify the Size or Volume Type if required. Note that this will incur charges. Choose “Next: Add Tags”.
10. In “Step 4: Add Tags”, you can create tags to identify resources based on their purpose. For example you can create a tag with key=Purpose and Value=Testing to identify that this instance is for testing. Choose “Next: Configure Security Group”.
11. In “Step 5: Configure Security Group”, select security group created in section 2.2. A security group is a set of firewall rules that control the traffic for your instance. If you are creating a new security group, enter an appropriate name and description so that it can be identified when viewed in the instance details – e.g. [Security group name: SecureAccess] [Description: Allow access to ports 3389 and 443 from anywhere]. A rule for RDP access is added by default when the instance is launched.
12. Choose Add Rule. Under Type, select HTTPS. In the Source column, leave the default settings as [Custom 0.0.0.0/0,::/0]. You can modify the Source column of the RDP rule to allow access from specific IP addresses using the Custom or My IP options.
13. Choose Review and Launch. In “Step 7: Review Instance Launch”, review the instance launch details and Choose Launch.
14. In the “Select an existing key pair or create a new key pair” wizard, enter a name for the key pair and choose Download Key Pair. Store the key in a secure and accessible location. Without this key you cannot connect to the instance. You will be prompted for this key when you access the instance until the password is set during SecureAccess configuration.
15. Go to the Instances view and check the instance details. In the Name column set a name to the instance e.g. SecureAccess Server. This will be useful to identify the instance.
    7. Choose Actions menu and select Networking->Change Source/Dest. Check and then choose Yes, Disable.
16. Go to Elastic IPs. Select the IP address allocated in step 2.3. Under Actions choose Associate Address. Leave the Resource type as Instance. For Instance select the SecureAccess server instance. For Private IP choose the IP address set in step 8 of section 3. Choose Associate and then Close. Verify the association.
17. To check whether the instance is ready to configure select the instance. In the Status Checks column check whether “2/2 checks passed”. Choose Actions menu and choose Instance Settings->Instance Screenshot. A locked screen denotes that the SecureAccess server is ready for configuration.

3.1 Configure Routing Tables for SecureAccess

This configuration is required only if you plan to use a static address pool for VPN address assignment configured in step 6 of section 3.2.2.

1. Navigate to the VPC dashboard.
2. In the navigation pane choose Subnets.
3. Choose the private subnet.

4. Choose the Routing Table tab.
5. Choose the routing table name (displayed as a hyper link)
6. Select the Route Table ID and choose Routes tab.
7. Choose Edit and then choose Add another route.
8. For Destination, enter the network IP that identifies the pool of addresses that will be assigned to the VPN clients. The range of IPs that you specify during the SecureAccess Server configuration should belong to this network. For Target, specify the SecureAccess server instance and choose Save.
9. If you have resources in the Private subnet of VPC then you need to create inbound rules allowing access from this address pool. Otherwise the SecureAccess clients cannot access these resources. Refer to section 2.2 for more details.

3.2 Configure SecureAccess Server

1. Navigate to the EC2 dashboard.
2. In the navigation pane choose Instances and choose the SecureAccess server and note the Public DNS address.
3. Choose Connect button on the top. On the Connect to your instance dialog choose Get Password. Click Choose File and browse to the key that was downloaded in step 14 of section 3. Choose Decrypt Password and note the password.
4. Connect to the SecureAccess web UI at https://<public DNS>. Note: A certificate warning will be displayed because the site uses self-signed certificate. Accept the certificate to access the web UI.
5. Log in to the UI with user name as Administrator and password obtained in step 3. The Quick Setup wizard is displayed.

3.2.1 Quick Setup Wizard

1. In General Settings/Administrator Password, specify the new password. The UI prompts for login because the password changed. Use the new password to login.
2. In General Settings/ Date and Time set the Date, Time and Time Zone.
3. In General Settings/Network Interfaces, select the interface and choose Use the following IP settings. For IP Address set the IP address configured in step 8 of section 3. Configure the subnet mask, gateway and DNS addresses accordingly.
4. In General Settings/Hostname and Domain, change the Hostname and join the system to the domain.
5. Note: The system will be rebooted. Domain administrator credentials will be required to access the web UI after the reboot.
6. After reboot, the web UI refreshes and Alerts Email step is displayed. Configure the Alert Email settings. This step is optional and can be configured later in the Maintenance section.

7. The wizard is complete when the congratulations screen displays. Choosing Close displays the main dashboard. This completes the initial step.
8. Now it's time to install features. The following features are available.
9. Remote Access with VPN – configuration for SecureAccess VPN.
10. Network Policy Server – basic RADIUS authentication or RADIUS proxy; Can also serve as a NAP policy server.
11. In the main dashboard, navigate to SecureAccess|Features.
12. Click the toggle button to On for the Remote Access with VPN feature.
13. Click Apply to confirm.
14. The feature's status indicator will rotate while the system processes the request. A confirmation will display when the process is complete.
15. Configuration must be customized for an environment. There are two options:
16. Click the Wizard button to open the SecureAccess VPN configuration tool
17. Click Remote Access with VPN link to open the Remote Access console as an RDP application.

3.2.2 SecureAccess setup wizard

The wizard provides the steps to configure SecureAccess VPN settings. It covers the minimum functionality; however, an individual organization may need different or additional configuration.

Deployment assumptions

- Amazon VPC is created and network planning is complete
- SecureAccess server instance is provisioned into the public subnet created in the VPC
- The Remote Access with VPN feature is installed through the web UI
- Deployment is a single server
- Network Location Server to help the SecureAccess clients decide whether they are inside or outside the corporate network. This will be a server inside the corporate network and should not be accessible from Internet. If a separate resource cannot be allocated for this functionality, the default IIS site on port 80 i.e. http://<fqdn_of_secureaccess_server_name>. Security group of the instance should be configured to allow access to the port 80 from the internal network or the range of IPs configured for SecureAccess VPN clients.
- Necessary certificates have been acquired for VPN and NLS (optional)
- AD will be used for SecureAccess VPN authentication and authorization
- DNS needs to resolve to either the public host name of the SecureAccess server or the NAT device for the SecureAccess server.

1. Access the setup wizard through the web UI at SecureAccess | Features | Remote Access with VPN | Wizard.
2. In the Component Selection screen choose Configure VPN service. This option is selected by default. Choose Next.
   Note: During the quick setup wizard if the server is not joined to the domain, the error message “SecureAccess deployment cannot continue because the server does not belong to the domain.” displays.
3. In VPN/Basic screen specify the topology that matches your requirement. For Public address, enter the FQDN of the connection that clients will use to connect. Choose Next.
4. In the VPN/Advanced screen specify the network interfaces corresponding to the internal and/or external networks.
   Note: In step 3 if you select the topology as Edge or Behind an Edge (with two network adapters), then this view displays two network interfaces – Internal and External. If you select Edge (with one network adapter) then this view displays only Internal.
5. Provide your SSL certificate for SSTP. The certificate subject name should match the Public address configured in step 3. If the names do not match then the error message “VPN certificate must match public connection address.” displays.
6. In the VPN/Address Assignment screen, select the address assignment method. Choose Assign addresses from a static address pool. This pool should belong to the network IP that configured in step 8 of section 3.1.
   Note: Depending on the VPC scenario that you have created before provisioning SecureAccess server, if you have a DHCP server available in the private network of the VPC or plan to use the DHCP server in the corporate network choose Assign addresses automatically.
7. In the VPN/Authentication screen, select the authentication method. Choose Next.
8. The wizard configuration is complete when the Finish screen displays. Verify the configuration. If you need any modifications you can go back and do the necessary changes. Choose Next to save the configuration.
9. The configuration is successfully saved when the Congratulations screen displays.
10. Click on the logo on the top left of the web UI to display the main dashboard. Choose SecureAccess | Remote Access Dashboard and select the SecureAccess tab.
11. Download the SecureAccess client installers using the links provided in the Download Client section and distribute it to the users.