Google Compute Engine Configuration

GCE Setup for VNS3
2016
Table of Contents

Requirements 3
Step 1: GCE VNS3 Image Delivery 9
Step 2: GCE Network Setup 16
Step 3: Launching a VNS3 Controller 19
VNS3 Configuration Document Links 21
Requirements
Requirements

• You have a Google cloud account where you can control the API access and Service Accounts so Cohesive Networks can delivery a VNS3 Image to your account.

• Ability to configure a client (whether desktop based or cloud based) to use OpenVPN client software.

• You have a compliant IPsec firewall/router networking device:
  Preferred Most models from Cisco Systems*, Juniper, Watchguard, Dell SONICWALL, Netgear, Fortinet, Barracuda Networks, Check Point*, Zyxel USA, McAfee Retail, Citrix Systems, Hewlett Packard, D-Link, WatchGuard, Palo Alto Networks, OpenSwan, pfSense, and Vyatta.
  Best Effort Any IPsec device that supports: IKE1 or IKE2, AES256 or AES128 or 3DES, SHA1 or MD5.
  *Known Exclusions Checkpoint R65+ requires native IPSec connections as Checkpoint does not conform to NAT-Traversal Standards and Cisco ASA 8.4(2)-8.4(4) bugs prevent a stable connection from being maintained.
Google Compute Cloud surfaces some advanced network controls to the user such as network routing. This guide covers a very generic VNS3 GCE setup. If you need specific help with project planning, POCs, or audits, contact our professional services team via sales@cohesive.net for details.

This guide uses Cisco’s Adaptive Security Device Controller UI. Setting up your IPsec Extranet device may have a different user experience than what is shown here. All the information entered in this guide will be same regardless of your UI or cmd line setup.

Please review the VNS3 Support Plans and Contacts before sending support inquiries.
Firewall Considerations

VNS3 Controller instances use the following TCP and UDP ports.

- **UDP port 1194**
  For client VPN connections; must be accessible from all servers that will join VNS3 topology as clients.

- **UDP 1195-1203***
  For tunnels between Controller peers; must be accessible from all peers in a given topology.

- **TCP port 8000**
  HTTPS admin interface; must be accessible from hosts where you will want to obtain runtime status or configure peering, also needs to be open to and from the Controllers at least for the peering process, and needs to be accessible when downloading credentials for installation on overlay network clients.

- **UDP port 500**
  UDP port 500 is used the phase 1 or IKE (Internet Key Exchange) component of an IPsec VPN connection.

- **ESP Protocol 50 and possibly UDP port 4500**
  Protocol 50 is used for phase 2 or ESP (Encapsulated Security Payload) component of an IPsec VPN connection only when negotiating with native IPsec. UDP port 4500** is used for the phase 2 or ESP (Encapsulated Security Payload) component of an IPsec VPN connection when using NAT-Traversal Encapsulation.

*VNS3:vpn and VNS3:net Lite Edition will not require UDP ports 1195-1197 access as it is not licensed for Controller Peering.

** Some public cloud providers require IPsec connections to use NAT-Traversal encapsulation on UDP port 4500
Sizing Considerations

Image Size and Architecture

VNS3 Controller Images are available as 64bit images to allow the greatest flexibility for your use-case. We recommend Controller instances be launched with at least 512MB of RAM. Smaller sizes are supported but the performance will depend on the use-case.

Clientpack Key Size

VNS3 Controllers currently generate 1024 bit keys for connecting the clients to the overlay network via the “clientpacks”. Smaller or larger encryption keys can be provided upon request (from 64 bit to 2048 bit). Future releases of VNS3 will provide the user control over key size and cipher during initialization and configuration.
Remote Support

Note that TCP 22 (ssh) is not required for normal operations. Each VNS3 Controller is running a restricted SSH daemon, with access limited only to Cohesive for debugging purposes controlled by the user via the Remote Support toggle and key exchange generation.

In the event Cohesive needs to observe runtime state of a VNS3 Controller in response to a tech support request, we will ask you to open Security Group access to SSH from our support IP range and Enable Remote Support via the Web UI.

Cohesive will send you an encrypted passphrase to generate a private key used by Cohesive Support staff to access your Controller. Access to the restricted SSH daemon is completely controlled by the user. Once the support ticket has been closed you can disable remote support access and invalidate the access key.
Step 1: GCE VNS3 Image Delivery
VNS3 Image Availability in GCE

Google Compute Engine currently does not have Image sharing semantics. In order to provide a VNS3 Image to your GCE account you will need to provide a temporary service account for our use. Cohesive Networks will use this service account to deliver the VNS3 image to you.

You will also need three of the Google APIs enabled for your account. If you are using Google Compute Engine, these should already be enabled. These are the Google Cloud Storage API, Google Cloud Storage JSON API, Google Compute Engine API.
Create a Service Account for Use by Cohesive Networks

1) In the GCE Developer’s Console, select your project

2) From the left-side “APIs & Auth” menu, select “Credentials”

3) Under the OAuth heading, click “CREATE NEW CLIENT ID”, and select Service account on the pop-up window.
Create a Service Account for Use by Cohesive Networks

Your service account private key will download to the Downloads directory specified by your Web Browser. It will be a file of the form (for example)

“2c91976353f8264bb5b6926d9b295a03e62bb9bb-privatekey.p12”

GCE will generate a new Service Account for you with a public key fingerprint matching the name of the key file that was downloaded.

Send the key file and the contents of the service account window to Cohesive Networks.
Cohesive Networks will deliver the VNS3 image to your account using the service account information.

You can leave the service account active for Cohesive Networks’s use to provide image updates in the future. Or you can delete the service account which will revoke any keys generated for it.

Remove your service account after you’ve received VNS3 unless you want to keep it active for future images from Cohesive Networks.
Ensure necessary GCE APIs are enabled

Please ensure that the Google Cloud Storage API, Google Cloud Storage JSON API, and the Google Compute Engine API are enabled for your account or Cohesive Networks will not be able to push the VNS3 Image to your GCE Account.
Send the Keys to Cohesive Networks

Please provide the key file and service account information to Cohesive Networks. They will notify you when the VNS3 Image appears to be delivered to your account.

Any questions please contact your Account Manager, or email support@cohesive.net.
Step 2: GCE Network Setup
Configure Network from the GCE Console.

Click **Networks** in the left column menu under the Compute Engine section. Select the Default network.

The default settings allow inbound connections on all ports from servers launched in the Default network and allow outbound connections on all ports to all routes (0.0.0.0/0).

Add the following Firewall rules:

- TCP port 8000 from your public IP (you can find your IP address by navigating to http://whatismyip.com)

- UDP port 500 from the IP of your Datacenter-based IPsec Device

- UDP port 4500 from the IP of your Datacenter-based IPsec Device (NAT-Traversal encapsulation is required for all IPsec connection to GCE)
An alternative to just using the Default network is to separate the Controllers from the Client Servers into two networks. To do this we recommend creating two networks: vns3-mgr and vns3-client. Note: no rules are needed in the vns3-client network by default.

Initially you will only need to add the following Firewall rules to the vns3-mgr network:

- TCP port 8000 from your public IP (you can find your IP address by navigating to http://whatismyip.com)
- UDP port 500 from the IP of your Datacenter-based IPsec Device
- UDP port 4500 from the IP of your Datacenter-based IPsec Device (NAT-Traversal encapsulation is required for all IPsec connection to GCE)
- UDP port 1194 from the vns3-client network IP range
Step 3: Launching a VNS3 Controller Instance
Launch a VNS3 Controller

Launch a VNS3 instance from the GCE Console.

Click **VM Instances** in the left column menu under the Compute Engine section.

Click the **New Instance** button at the top of the VM Instance page and fill out the fields as follows:

- **Name**: vns3-mgr1 or some variation
- **Metadata**: leave blank
- **Zone**: select where you want to run your instances
- **Machine Type**: select a size that will support your use case, g1-small or larger is recommended
- **Boot source**: New form images
- **Image**: select the VNS3 image that Cohesive Networks delivered to your account
- **Network**: select either default or vns3-mgr depending on the network option you choose.
- **External IP**: you can choose to use an ephemeral IP but Cohesive Networks recommend assigning a Static IP which will speed recovery in the event you need to relaunch the VNS3 Controller or during operational windows for upgrades.
VNS3 Configuration Document Links
VNS3 Configuration Document Links

VNS3 Product Resources - Documentation | Add-ons

VNS3 Configuration Instructions
Instructions and screenshots for configuring a VNS3 Controller in a single or multiple Controller topology. Specific steps include, initializing a new Controller, generating clientpack keys, setting up peering, building IPsec tunnels, and connecting client servers to the Overlay Network.

VNS3 Administration Document
Covers the administration and operation of a configured VNS3 Controller. Additional detail is provided around the VNS3 Firewall, all administration menu items, upgrade licenses, other routes and SNMP traps.

VNS3 Docker Instructions
Explains the value of the VNS3 3.5 Docker integration and covers uploading, allocating and exporting application containers.

VNS3 Troubleshooting
Troubleshooting document that provides explanation issues that are more commonly experienced with VNS3.