



WAZUH Deployment Guide

TABLE OF CONTENTS

- Overview
- Pre-requisite
- Key Points
- Steps of Configuration of WAZUH
- Steps of Configuration of VPN from Google Cloud to On Prem Office
- Steps of Configuration of VPN from On Prem Office to Google Cloud
- How to Deploy Agent
- How to View Dashboard.

Overview

WAZUH is an open-source security monitoring platform that offers intrusion detection, log management, vulnerability assessment, and compliance capabilities. It was designed to help organizations detect, respond to, and mitigate security threats across diverse IT environments, from traditional on-premises systems to cloud infrastructure. Overall, Wazuh enhances an organization's security posture by enabling continuous monitoring, detection, and response to potential threats and vulnerabilities. Its open-source nature allows for community-driven innovation and customization to meet specific security requirements.

Prerequisites

Hardware and OS requirement:

Hardware Requirements				Operating System
Agent	CPU	RAM	Storage (90 days)	Ubuntu 16.04, 18.04, 20.04, 22.04
1 - 25	4 vCPU	8 GB	50 GB	CentOS 7, 8
25 – 50	8 vCPU	8 GB	100 GB	RedHat Enterprise Linux 7, 8, 9
50 - 100	8 vCPU	8 GB	200 GB	Amazon Linux 2

Key points:

- The WAZUH server IP should be Static.
- WAZUH Dashboard password shouldn't include any special character.
- Need to allow internet connection to the WAZUH server.
- 1514,1515,1516,514,55000 and 443 ports should be allowed from the OpenVAS server.
- IPsec Site to Site VPN should be configured correctly from both ends.

Steps of Configuration of WAZUH

We need to create a VM in any appliance with the above-mentioned specification.

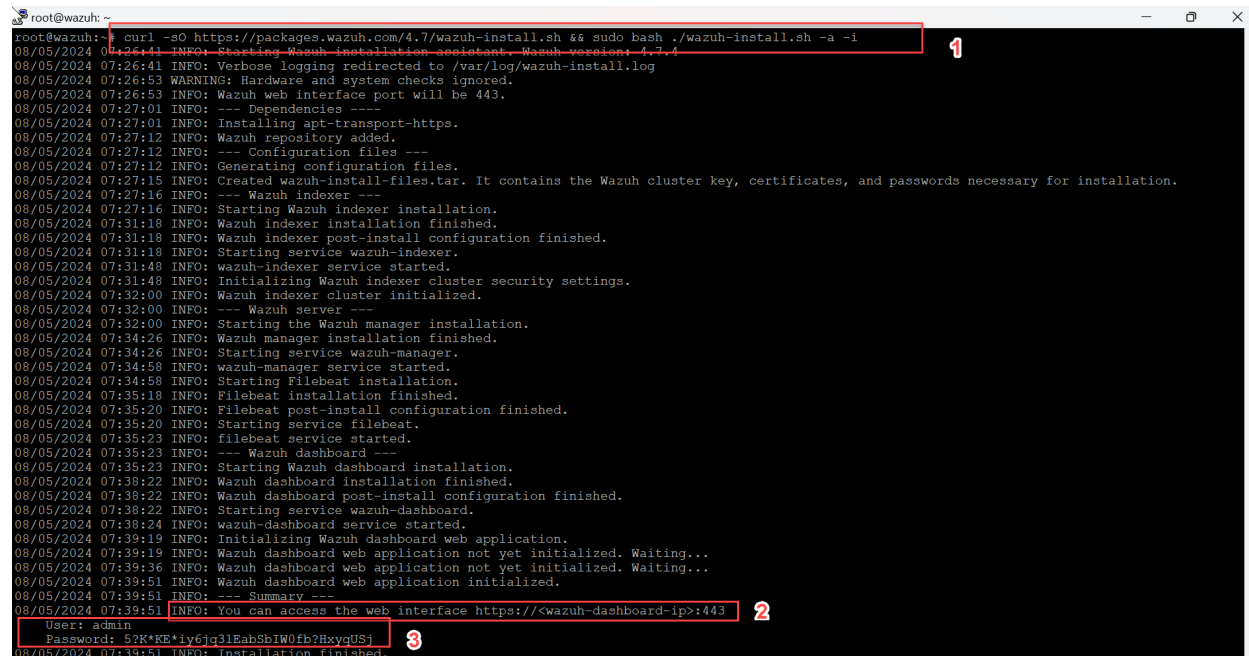
After the VM creation completed following Tasks should be done to install WAZUH server in it.

Task 1:

To begin, we can done WAZUH installation by using the following command:

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i
```

Once it is installed, we can view the below screen. Here Collect Dashboard Address, User Name and Password.



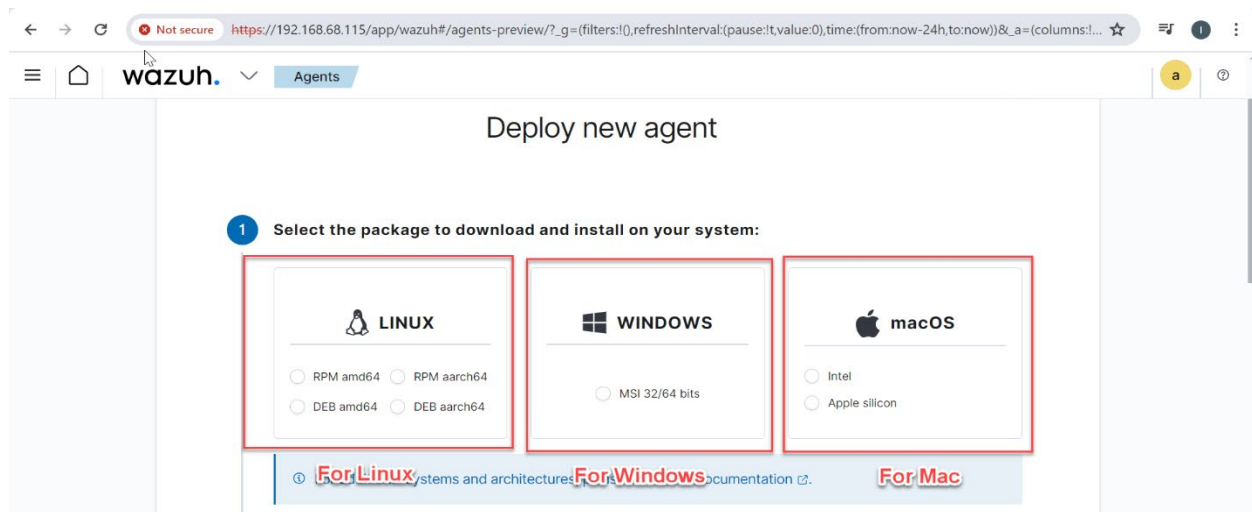
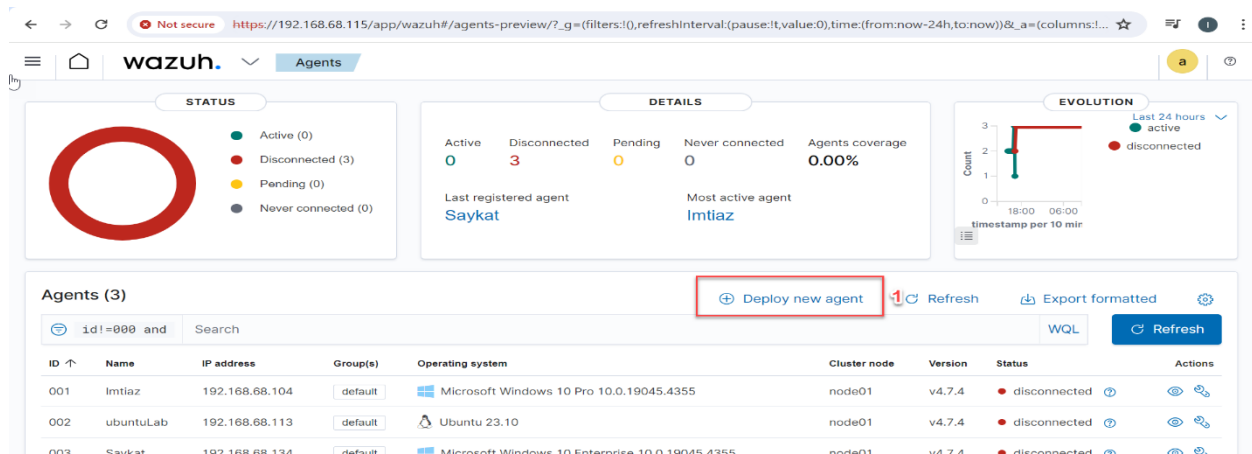
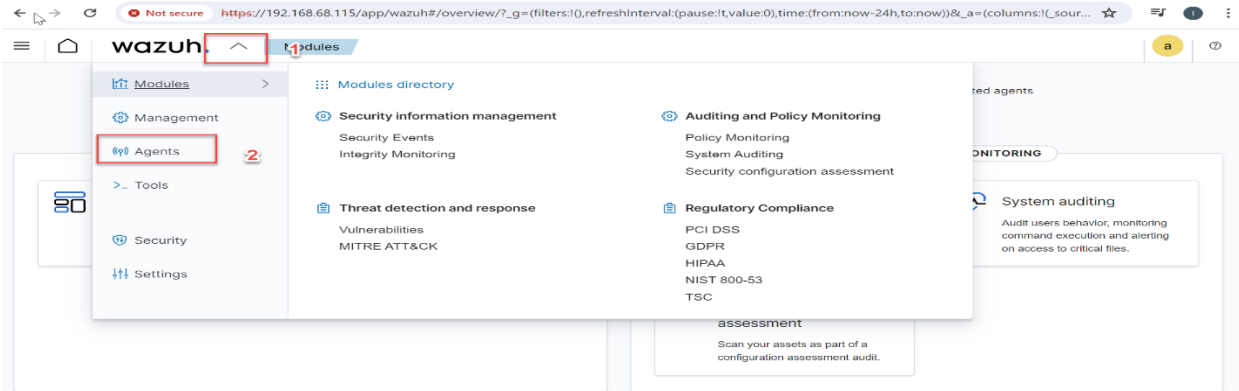
```
root@wazuh:~# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i
08/05/2024 07:25:41 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.4
08/05/2024 07:26:41 INFO: Verbose logging redirected to /var/log/wazuh-install.log
08/05/2024 07:26:53 WARNING: Hardware and system checks ignored.
08/05/2024 07:26:53 INFO: Wazuh web interface port will be 443.
08/05/2024 07:27:01 INFO: --- Dependencies ---
08/05/2024 07:27:01 INFO: Installing apt-transport-https.
08/05/2024 07:27:12 INFO: Wazuh repository added.
08/05/2024 07:27:12 INFO: --- Configuration files ---
08/05/2024 07:27:12 INFO: Generating configuration files.
08/05/2024 07:27:15 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
08/05/2024 07:27:16 INFO: --- Wazuh indexer ---
08/05/2024 07:27:16 INFO: Starting Wazuh indexer installation.
08/05/2024 07:31:18 INFO: Wazuh indexer installation finished.
08/05/2024 07:31:18 INFO: Wazuh indexer post-install configuration finished.
08/05/2024 07:31:18 INFO: Starting service wazuh-indexer.
08/05/2024 07:31:48 INFO: wazuh-indexer service started.
08/05/2024 07:31:48 INFO: Initializing Wazuh indexer cluster security settings.
08/05/2024 07:32:00 INFO: Wazuh indexer cluster initialized.
08/05/2024 07:32:00 INFO: --- Wazuh server ---
08/05/2024 07:32:00 INFO: Starting the Wazuh manager installation.
08/05/2024 07:34:26 INFO: Wazuh manager installation finished.
08/05/2024 07:34:26 INFO: Starting service wazuh-manager.
08/05/2024 07:34:58 INFO: wazuh-manager service started.
08/05/2024 07:34:58 INFO: Starting Filebeat installation.
08/05/2024 07:35:18 INFO: Filebeat installation finished.
08/05/2024 07:35:20 INFO: Filebeat post-install configuration finished.
08/05/2024 07:35:20 INFO: Starting service filebeat.
08/05/2024 07:35:23 INFO: filebeat service started.
08/05/2024 07:35:23 INFO: --- Wazuh dashboard ---
08/05/2024 07:35:23 INFO: Starting Wazuh dashboard installation.
08/05/2024 07:38:22 INFO: Wazuh dashboard installation finished.
08/05/2024 07:38:22 INFO: Wazuh dashboard post-install configuration finished.
08/05/2024 07:38:22 INFO: Starting service wazuh-dashboard.
08/05/2024 07:38:24 INFO: wazuh-dashboard service started.
08/05/2024 07:39:19 INFO: Initializing Wazuh dashboard web application.
08/05/2024 07:39:19 INFO: Wazuh dashboard web application not yet initialized. Waiting...
08/05/2024 07:39:36 INFO: Wazuh dashboard web application not yet initialized. Waiting...
08/05/2024 07:39:51 INFO: Wazuh dashboard web application initialized.
08/05/2024 07:39:51 INFO: --- Summary ---
08/05/2024 07:39:51 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: 5?K*KE*iy6jq3lEabSbIW0fb?HxyqUSj
08/05/2024 07:39:51 INFO: Installation finished.
```

After complete installation you can log in WAZUH Dashboard with provided user name and password.

Task 2:

Deploy An Agent to your Environment.

For Deploy any agent you have to follow below steps



The image consists of three vertically stacked screenshots of the Wazuh web interface, illustrating the process of installing a new agent.

Top Screenshot: The 'Agents' page shows a dropdown menu for selecting a group, with 'Default' selected. A red box highlights this dropdown, and a red annotation says '1. Select the Group'. Below this, a blue box contains the command to download and install the agent, with a red annotation '2. Copy this code and run it to you windows from power shell as an administrative privilege'. The command is: `Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile $(env:tmp)\wazuh-agent; msixec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.68.115' WAZUH_AGENT_NAME='ImtiazPC' WAZUH_REGISTRATION_SERVER='192.168.68.115'`. A blue box below the command lists requirements: 'You will need administrator privileges to perform this installation.' and 'PowerShell 3.0 or greater is required.' A note states: 'Keep in mind you need to run this command in a Windows PowerShell terminal.'

Middle Screenshot: This screenshot shows the same 'Agents' page, but the command box is now empty, and the requirements box is still visible.

Bottom Screenshot: The 'Agents' page shows the command box with the command: `NET START WazuhSvc`. A red box highlights this command, and a red annotation says '1. Run this command'. Below the command box, a blue box contains the requirements and the note. A red annotation '2. Close the Window' points to a 'Close' button in the bottom right corner.

Task 3:

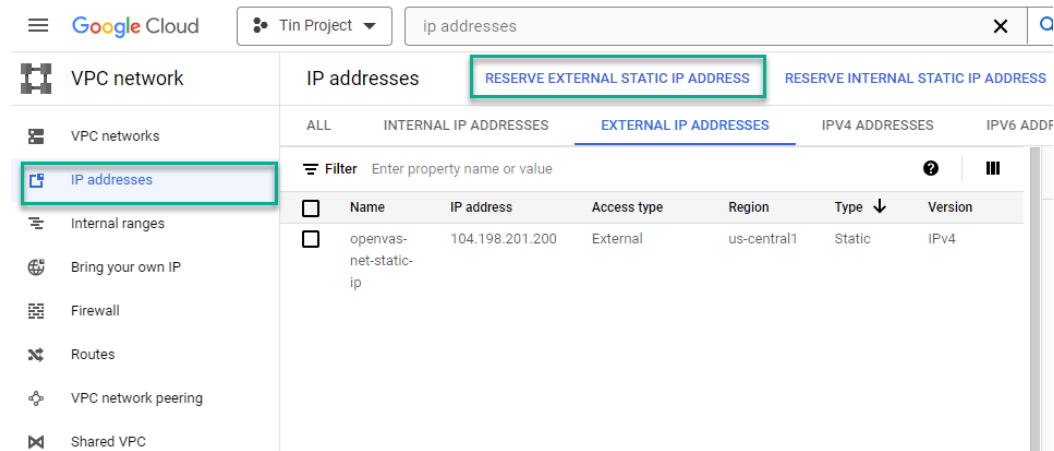
Steps of Configuration of VPN from Google Cloud to On Prem Office

Following three different task we need to complete to create a Google cloud VPN.

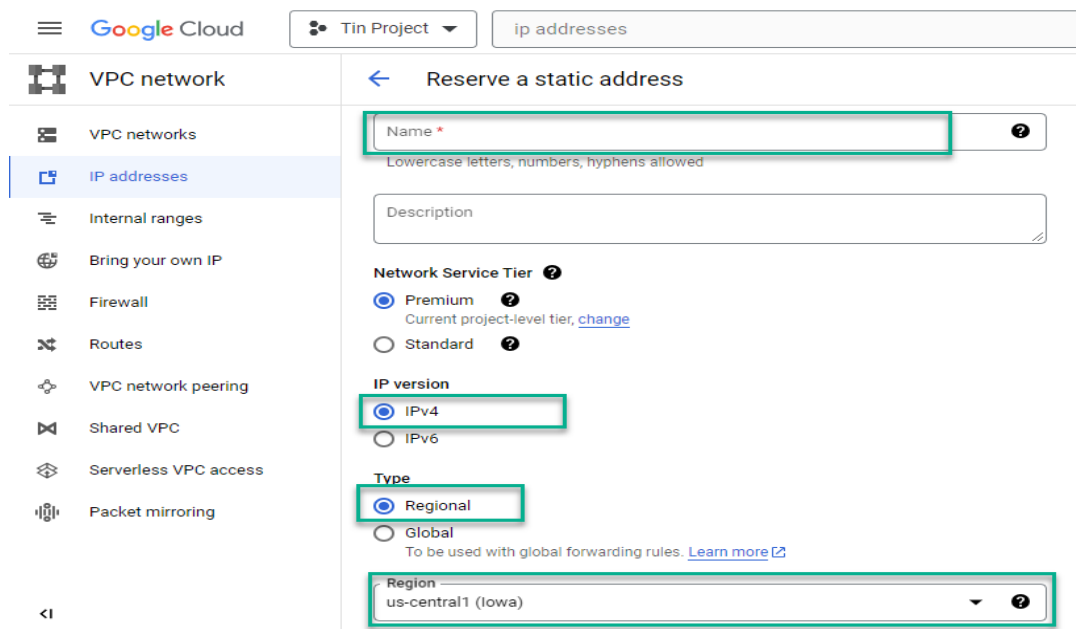
Task 1: Reserve static IP:

First, we must go to Google cloud console and perform following steps:

- Go to IP addresses.
- Click on Reserve External static IP address.



- Choose a name for the new address.
- Specify IPv4 address.
- Select the region to create the address in.
- Click Reserve to reserve the IP address.

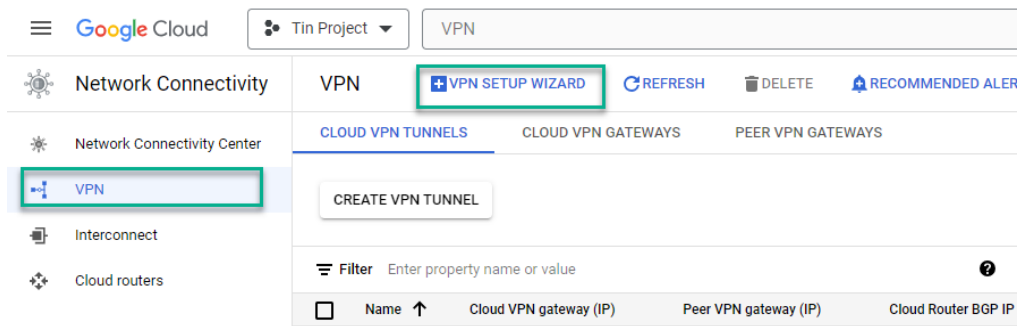


Task 2: Create VPN Gateway:

From Google cloud console we need to perform following steps:

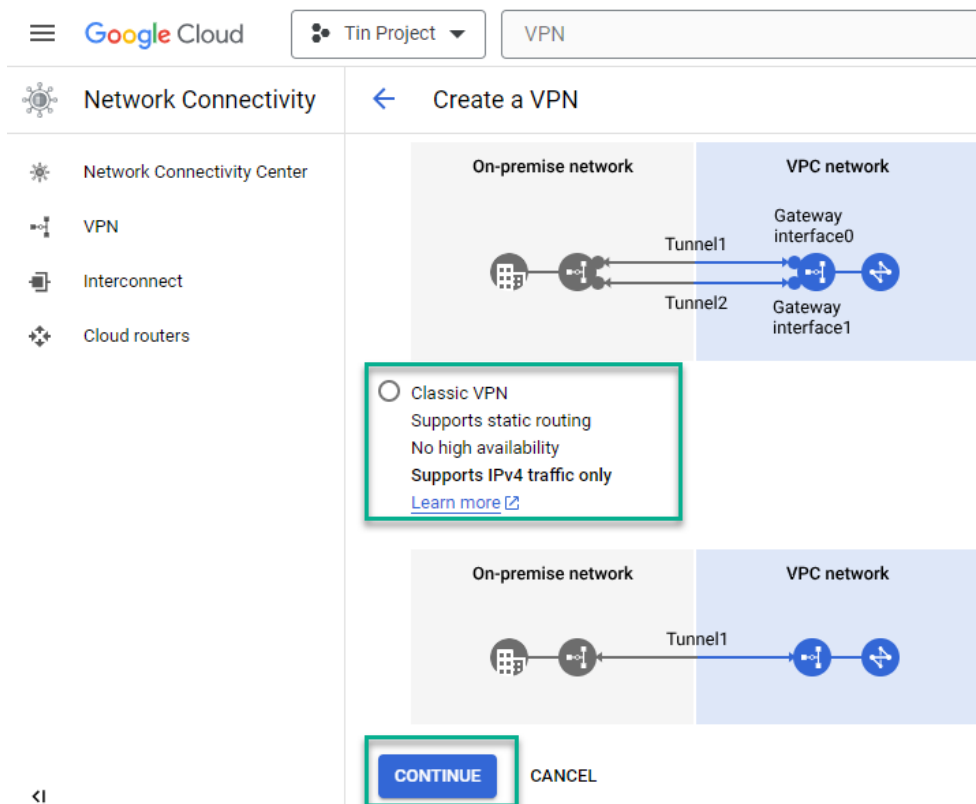
- Click Create VPN connection.

- Select the VPN setup wizard.



- Select the Classic VPN option button.

- Click Continue.



- On the Create a VPN connection page, specify the following gateway settings:

- Name: The name of the VPN gateway. The name cannot be changed later.
- Description: Optionally, add a description.
- Network: Specify an existing VPC network in which to create the VPN gateway and tunnel.
- Region: Choose a Google Cloud region where the gateway will be located.
- IP address: Select the reserved static external IP address.

Google Cloud

Tin Project

VPN

Network Connectivity

VPN

Interconnect

Cloud routers

Create a VPN connection

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPsec connectivity.[Learn more](#)

Google Compute Engine VPN gateway

Name *

vpn-1

Lowercase letters, numbers, hyphens allowed

Description

Network *

Region *

us-central1 (Iowa)

Region is permanent

IP address *

Task 3: Create Tunnel:

From the Tunnels section, specify the following settings:

- Name: The name of the VPN tunnel. The name cannot be changed later.
- Description: Optionally, type a description.
- Remote peer IP address: Specify the external IP address of the peer VPN gateway.
- IKE version: Choose the appropriate IKE version supported by the peer VPN gateway. IKEv2 is preferred.
- IKE pre-shared key: Click on Generate and copy **(This key will be needed when configure the counterpart tunnel on the peer VPN gateway)**.

Google Cloud | Tin Project | VPN

Network Connectivity

← Create a VPN connection

Tunnels ⓘ

You can have multiple tunnels to a single Peer VPN gateway.

New tunnel [trash] [up]

Name *
-tunnel-1 ⓘ
Lowercase letters, numbers, hyphens allowed

Description

Remote peer IP address * ⓘ

IKE version
IKEv2 ⓘ

IKE pre-shared key * [GENERATE AND COPY](#)
Enter your own key or generate one automatically

- Routing options: select Route based.
- Remote network IP ranges: provide a space-separated list of the IP address ranges used by the local traffic (DABS Office) VPN setup.
- Click Done.
- Click Create.

The screenshot shows the Google Cloud console interface for creating a VPN connection. The left sidebar lists 'Network Connectivity Center', 'VPN', 'Interconnect', and 'Cloud routers'. The main content area is titled 'Create a VPN connection'. Under 'Routing options', 'Route-based' is selected. Below this, the 'Remote network IP ranges' field is highlighted with a red box. A 'DONE' button is also highlighted with a red box. At the bottom, the 'CREATE' button is highlighted with a red box.

Steps of Configuration of VPN from On Prem Office to Google Cloud

We need to go to “https://unifi.ui.com/” and from one of the DABS Office Network go to VPN > Site to Site VPN> Create New, specified in the following settings.

- VPN Option: Site to Site VPN
- Name: Give a name of the VPN tunnel
- Pre-shared Key: Provide the Pre-shared key which was copied from Google Cloud VPN.
- Local Public IP: Keep the default gateway public IP.
- Remote Public IP: Provide the Public IP address of the Google Cloud VPN.
- VPN Type: Route based.
- Remote IP Range: Provide the IP address range used by the Google Cloud VPN.

< VPN Type OpenVPN IPsec

Name Give a name

Pre-Shared Key

Local IP Keep the default Public IP 1.....
[Enter IP Address manually](#)

Remote IP / Host Public IP address of the Google Cloud VPN

Network Configuration

VPN Type Route Based Policy Based

Remote Network(s) IP address range used by the Google Cloud VPN

- IKE Version: IKEv2.
- Keep other settings as default.
- Click Add.

< **Advanced** Auto Manual

Key Exchange Version IKEv1

IKE ✓ IKEv1
IKEv2

ESP Keep as default →

Local Authentication ID

Remote Authentication ID

Add Transmission Unit

DH Group 14 Lifetime 28800

Encryption AES-128 Hash SHA1

DH Group 14 Lifetime 3600

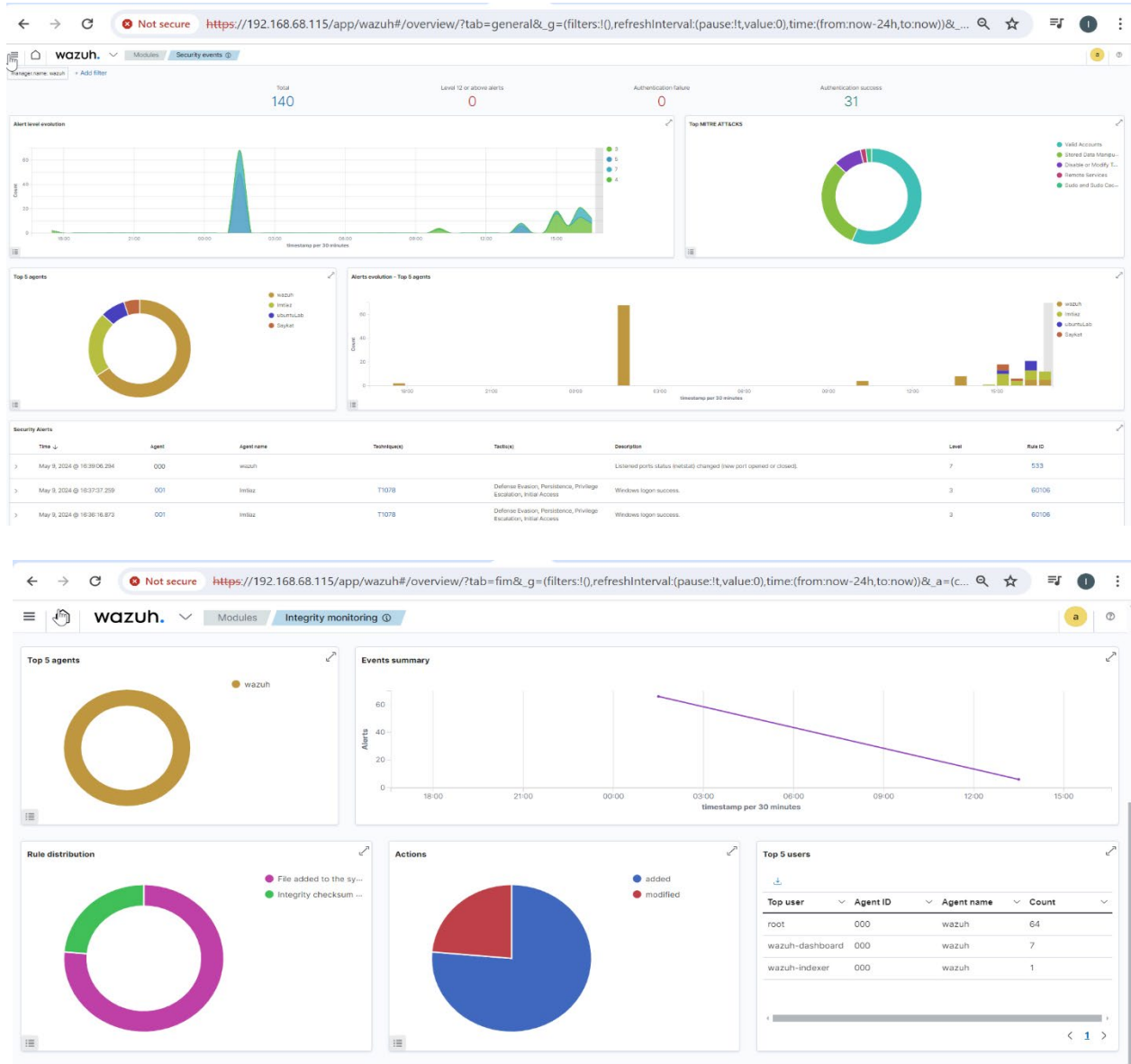
☒ Perfect Forward Secrecy (PFS)

☒ Auto 104.184.156.226

☒ Auto

☒ Auto 1417

How to View Dashboard



What we can do:

- Monitor your environment.
- Monitor your System Security Score.
- Monitor your Registry File
- Monitor your any File.
- Mitigate Any DDos attack.
- Monitor any vulnerability.
- And many more things...

END