OpenVAS Deployment documentation for XXX-COMPANY

At first, we have created a Google Cloud VM and setup OpenVAS in it after that done the following configuration for communication between OpenVAS VM and XXX-COMPANY Office.

Google Cloud VPN setup:

The following steps has been done to setup VPN from Google Cloud end to XXX-COMPANY end:

From the VPN Tunnels section, specified the following settings:

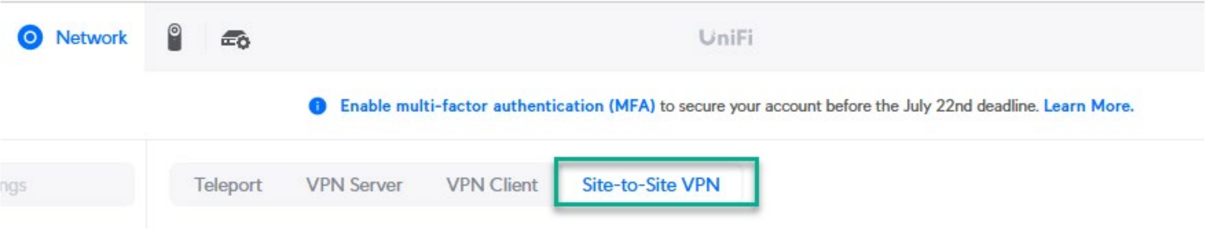
- **Name:** openvas-XXX-company-01.
- **Description:** This is the VPN tunnel to communicate from Google Cloud to the XXX-COMPANY office.
- **Remote peer IP address: xxx.xxx.xxx.xxx.**
- **IKE version:** IKEv2.
- **IKE pre-shared key:** L4dRTOsdgfL1JfbtsV5dsd5PhSIx2zGi.
- **Routing options:** Route based.
- **Remote network IP ranges:** 192.168.1.0/24.

XXX-COMPANY Office VPN setup:

The following steps has been done to setup VPN from XXX-COMPANY end to Google Cloud end:

From the XXX-COMPANY Burlingame Office Network option, specified the following settings:

VPN Option: Site to Site VPN



Enable multi-factor authentication (MFA) to secure your account before the July 22nd deadline. Learn More.

- **Name:** XXX-company-openvas-01
- **Pre-Shared key:** L4dRTOsdgfL1JfbzGitsV5dsd5PhSIx2
- **Local Public IP: xxx.xxx.xxx.xxx (Client Public IP address)**
- **Remote Public IP:** 104.198.201.200 (Google Cloud Public IP address)
- **VPN Type:** Route based.
- **Remote IP Range:** 192.168.0.0/24
- **IKE Version:** IKEv2
- **Encryption:** AES-128

After the above setup from Both ends VPN has been Established, then you can start the Vulnerability Scanning.