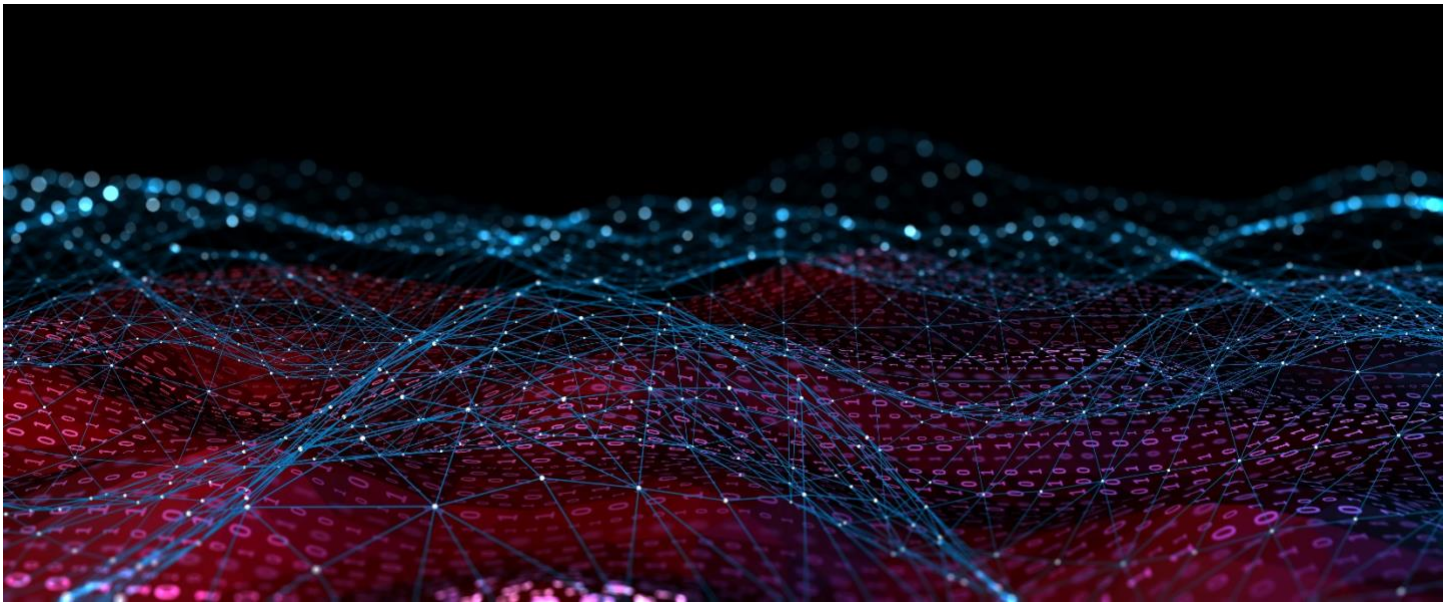
DOCUMENT: DEPLOYMENT GUIDE



Solution: Secure Access Services Edge (SASE) ▪ **Module**: Cyber Gateway ▪ **Use Case**: Secure Private (Internet) Access

Cyber Gateway Deployment Guide

Adjacent to the internal applications running in a public cloud, data center, or on-premises server, Exium places a small piece of software called Cyber Gateway (CGW), deployed as a VM or bare metal, which is used to extend a highly secure Zero Trust Path out to the Intelligent Cybersecurity Mesh.

What is Cyber Gateway?

The Cyber Gateway (CGW) is a key piece of software in our security architecture. Its deployment is required for Secure Private Access and SD-WAN services.

The CGW must be deployed in the data center (or virtual private cloud) that is hosting the applications that you want to enable for remote access. Once the CGW is deployed, our zero-trust network access capabilities can be configured to enable access to these apps.

The CGW can also be deployed in an-office location to connect that office to your network (SD-WAN).

We can help you determine where you should deploy the CGW in your environment.

Technical Requirements

The CGW requires a single virtual machine (VM) or bare metal (BM) machine to deploy. We recommend a 2-vCPU machine with at least 4 GB RAM for initial testing. Please consult the table below. The CGW requires access to the internet and must be able to reach the internal applications that require secure private access.

vCPU	*RAM*	*HDD*	*Type*	*OS*	*Supported Bandwidth*
4	8GB	50GB	VM / BM	Ubuntu	400 Mbps
2	4GB	50GB	VM / BM	Ubuntu	200 Mbps

EXIUM

Deployment Instructions

Pre-requisites

a) Create a Workspace, if not already done
b) Create a user group in the Workspace admin console that requires secure private access (if different from admin)
c) Add more users to the user group created, as and if needed.
d) Create CGW and add Trust Paths in the Workspace admin console
e) Associate the user group with the Trust Path created

Steps to bring up CGW VM

1) Download Ubuntu server 20.04 ISO image click here
2) Please select openssh-server option while installing Ubuntu server components
3) CGW VM Creation (Refer only one from below list)
   Note: Follow steps mentioned in below link to create VM but select above downloaded 20.04 ISO during installation
   a. Create Ubuntu on VMWare Hypervisor click here
   b. Create Ubuntu on Hyper-V click here
   c. Create Ubuntu on KVM click here
   d. Create Ubuntu on AWS EC2 click here
   e. Create Ubuntu on GCP click here
   f. Create Ubuntu on Azure click here
   g. In case machine is bare metal, skip VM creation and continue from step 4
4) Recommended Resources:
   a. Minimum 2 vCPU, 4 GB RAM, 20 GB HDD
5) Networking setup:
   a. Internet must be accessible and UDP ports 4500 and 500 need to be whitelisted
      i. Check CGW has internet access (ping 8.8.8.8)
      ii. Check DNS resolution works (ping google.com)
   b. Check internal/private application servers are accessible from CGW VM.
      i. Ping internal/private application server IP to verify connectivity
6) Install SSH server using below command (skip if already installed):

```
sudo apt-get install openssh-server
```

Steps to install CGW software

1) Login via SSH using VM IP address or continue with VM console
2) Execute below command:

```
sudo apt update; sudo apt install curl; curl -s https://clientreleases.s3.us-west-1.amazonaws.com/cgw/xcgw_install.sh | bash /dev/stdin workspace_name,cgw_name
```

Note: Above command will install CGW application and use provided workspace and CGW names. It will login automatically and connect the service. Before executing the command replace workspace_name and cgw_name words with actual values.