Deployment Guide for Cisco Catalyst 9800 Wireless Controller for Cloud on Google Cloud Platform

First Published: March 12, 2020

Cisco Systems, Inc. www.cisco.com

Table of Contents

Introduction

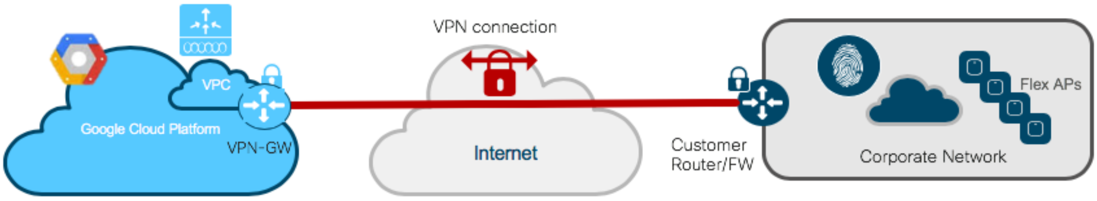
The IOS XE based Cisco Catalyst Wireless Controller for Cloud(C9800-CL) sets the standard for Infrastructure as a Service (IaaS) secure wireless network services with maximum performance in the Google Cloud Platform (GCP) cloud, bringing the world's most popular networking wireless platform to GCP.

Cisco Cloud Wireless LAN Controller (C9800-CL) combines the advantages and flexibility of a GCP public cloud with the customization and features richness customers usually get with on-Prem deployments.

C9800-CL scales up to 6000 Access Points and 64,000 clients with all Enterprise and Service Provider grade differentiating features like Zero Touch AP provisioning, High Availability, Application Visibility & Control, and more. All this at ZERO cost software.

Supported deployment mode

Starting with Cisco IOS-XE version 16.12.1, the Cisco Catalyst Wireless Controller for Cloud shall be supported as an IaaS solution on Google Cloud. The Cisco Catalyst Wireless Controller for Cloud supports the following deployment scenario: the WLC is available in GCP Virtual Private Network (VPC) connected to the customer enterprise network via a managed VPN. The VPN can be terminated either on the GCP Gateway Router or on a GCP based Cisco CSR. The only deployment mode supported is Flex Central Authentication and Local Switching for IPv4 and IPv6 clients with fall back to Local Authentication.



Prerequisites

Before we launch C9800-CL on GCP, the following prerequisites (in any order) should be met:

- You must have a GCP account.
- VPC with subnets defined and firewall configured.
- SSH key for password-less authentication. Here is the link that explain how to deal with public and private keys: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#createsshkeys
- The VPN connection must be established between the enterprise/branch and your VPC in GCP. (Instructions are in a section below)

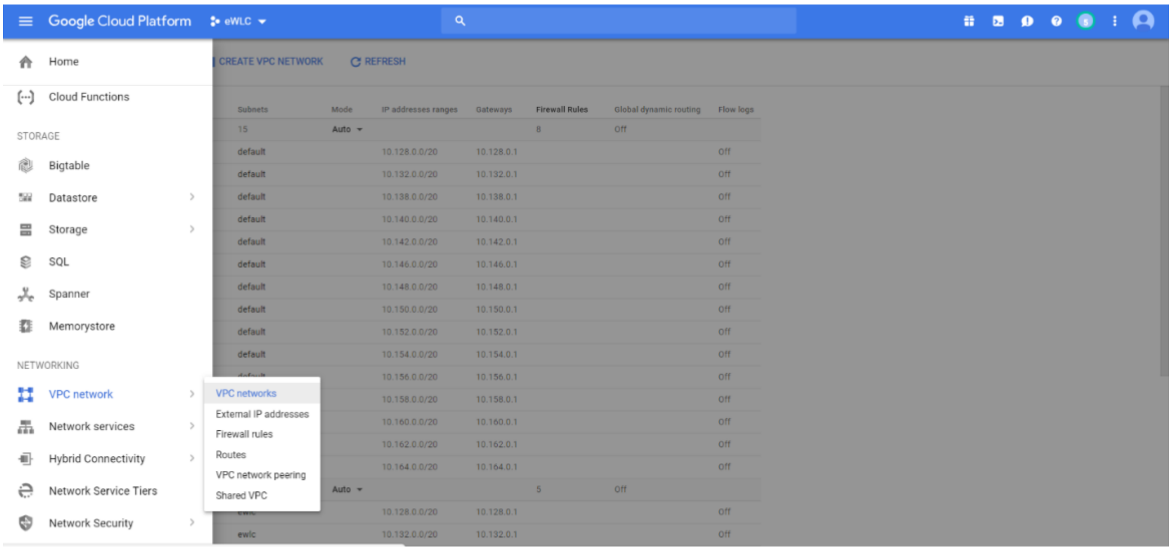
GCP Networking

Virtual Private Cloud or VPC

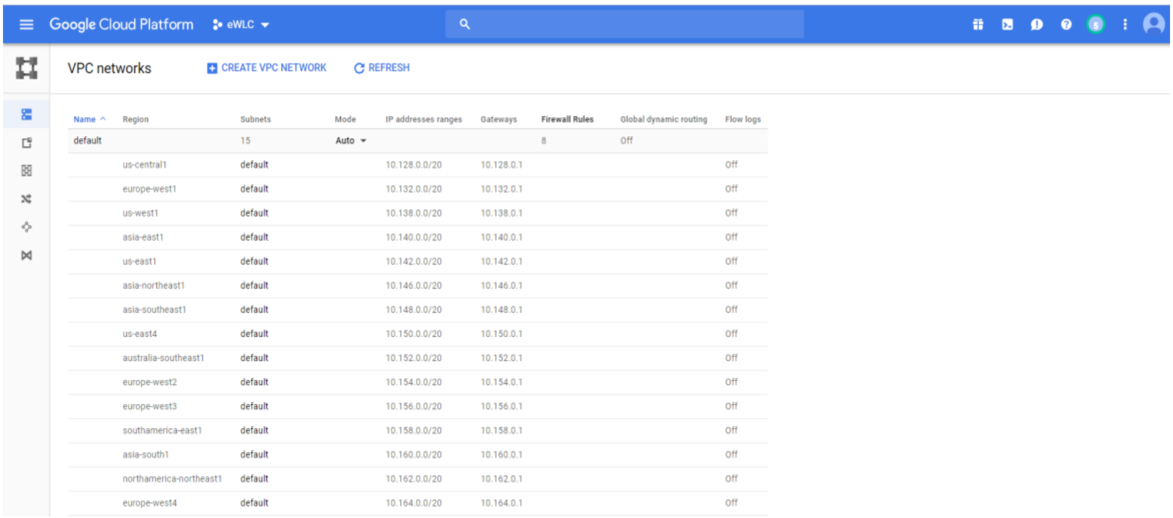
You can think of a VPC network the same way you'd think of a physical network, except that it is virtualized within GCP. GCP by default creates a 'default' VPC. It is recommended that we create a new VPC according to the requirements.

Steps to create a VPC:

- Go to VPC network -> VPC networks



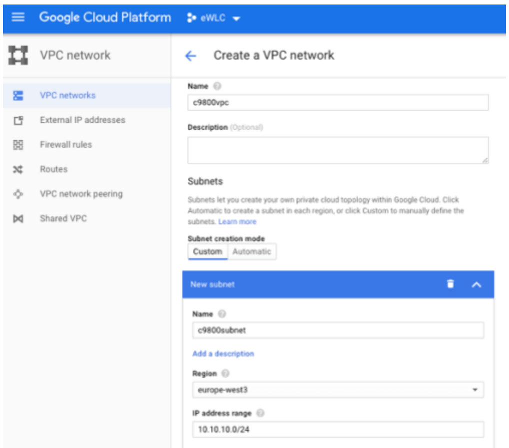
- Click on 'Create VPC Network' on the top



VPC networks

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
default		15	Auto			8	Off	
	us-central1	default		10.128.0.0/20	10.128.0.1			Off
	europe-west1	default		10.132.0.0/20	10.132.0.1			Off
	us-west1	default		10.138.0.0/20	10.138.0.1			Off
	asia-east1	default		10.140.0.0/20	10.140.0.1			Off
	us-east1	default		10.142.0.0/20	10.142.0.1			Off
	asia-northeast1	default		10.146.0.0/20	10.146.0.1			Off
	asia-southeast1	default		10.148.0.0/20	10.148.0.1			Off
	us-east4	default		10.150.0.0/20	10.150.0.1			Off
	australia-southeast1	default		10.152.0.0/20	10.152.0.1			Off
	europe-west2	default		10.154.0.0/20	10.154.0.1			Off
	europe-west3	default		10.156.0.0/20	10.156.0.1			Off
	southamerica-east1	default		10.158.0.0/20	10.158.0.1			Off
	asia-south1	default		10.160.0.0/20	10.160.0.1			Off
	northamerica-northeast1	default		10.162.0.0/20	10.162.0.1			Off
	europe-west4	default		10.164.0.0/20	10.164.0.1			Off

- Fill in the details as per requirements. You can find more about creating VPC at: https://cloud.google.com/vpc/docs/using-vpc



Create a VPC network

Name: c9800vpc

Description (Optional)

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode: Custom | Automatic

New subnet

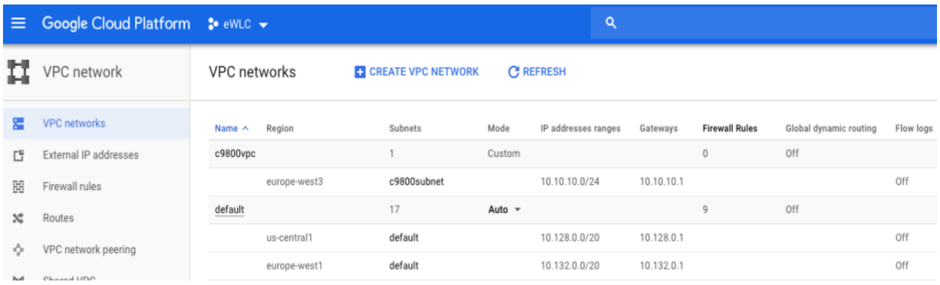
Name: c9800subnet

Add a description

Region: europe-west3

IP address range: 10.10.10.0/24

- You can find your VPC created as shown in the image below. We created a new VPC named ‘c9800vpc’.



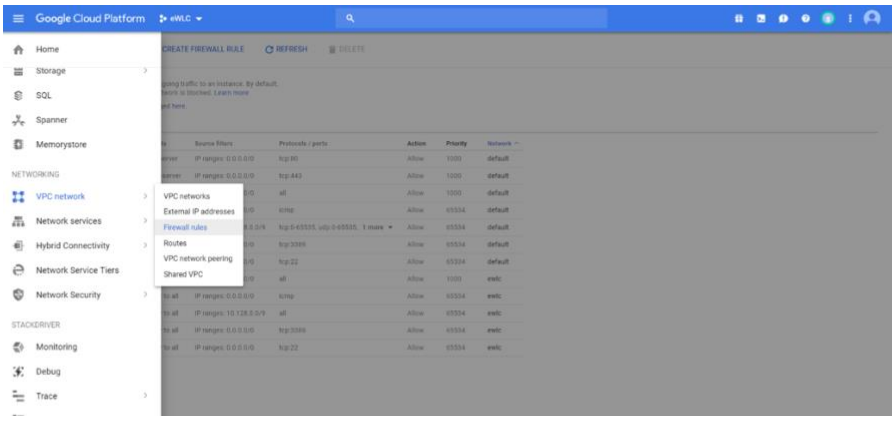
VPC networks

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing	Flow logs
c9800vpc		1	Custom			0	Off	
	europe-west3	c9800subnet		10.10.10.0/24	10.10.10.1			Off
default		17	Auto			9	Off	
	us-central1	default		10.128.0.0/20	10.128.0.1			Off
	europe-west1	default		10.132.0.0/20	10.132.0.1			Off

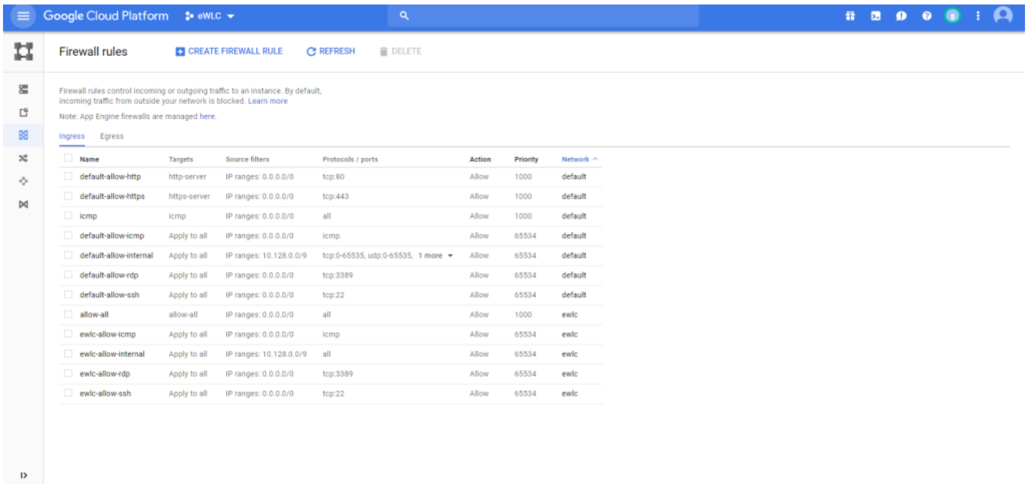
Firewall Rules

We need to instruct GCP to allow communication on required ports/protocols. GCP has 2 default rules which are not shown on the dashboard. All egress (outgoing) traffic are allowed and all ingress (incoming) are blocked. These rules can be overwritten by creating a higher priority firewall routes. To connect to the C9800-CL instance once it is up and running, we need to allow SSH and HTTP/HTTPS communication by adding the ingress firewall rules. Steps to create a firewall rule for SSH:

- Go to VPC Network -> Firewall rules



- Click on the ‘Create Firewall Rule’ on the top left side.



Firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed here.

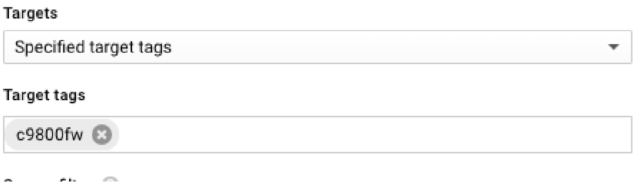
Ingress Egress

Name	Targets	Source filters	Protocols / ports	Action	Priority	Network
default-allow-http	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default
default-allow-https	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default
icmp	icmp	IP ranges: 0.0.0.0/0	all	Allow	1000	default
default-allow-icmp	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535, udp:0-65535, 1 more	Allow	65534	default
default-allow-rdp	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
default-allow-ssh	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default
allow-all	allow-all	IP ranges: 0.0.0.0/0	all	Allow	1000	ewlc
ewlc-allow-icmp	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	ewlc
ewlc-allow-internal	Apply to all	IP ranges: 10.128.0.0/9	all	Allow	65534	ewlc
ewlc-allow-rdp	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	ewlc
ewlc-allow-ssh	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	ewlc

- Provide the name, description, priority as per your requirement.

- Direction of the traffic is Ingress, Action of match is 'Allow'.

- Target: you can either select all instances in the network (as seen below) or select targets as 'Specified target tags' and enter a tag in the "Targets" text box (c9800fw in this case).



Targets

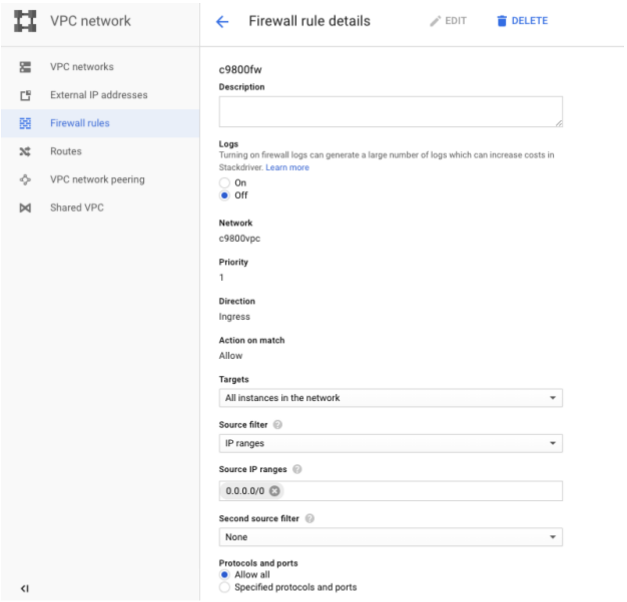
Specified target tags

Target tags

c9800fw

- Enter 0.0.0.0/0 to allow traffic for all IPs. You change this step to allow only a specific IP.

- Select 'Allow all' in Protocols and Ports. You can always change it later to restrict the access



Firewall rule details

c9800fw

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

○ On
● Off

Network
c9800vpc

Priority
1

Direction
Ingress

Action on match
Allow

Targets
All instances in the network

Source filter
IP ranges

Source IP ranges
0.0.0.0/0

Second source filter
None

Protocols and ports
● Allow all
○ Specified protocols and ports

- Click 'Create'

Establishing a VPN connection using the GCP VPN router

As stated in the earlier sections, the only supported mode is with a managed VPN.

This means you need a router/firewall in your enterprise or branch network to set up a VPN to the VPC in GCP. General documentation for VPN in GCP can be found here: https://cloud.google.com/vpn/docs/concepts/overview

Specific instructions on how to setup a VPN connection between GCP and a cisco ISR router can be found here: https://cloud.google.com/community/tutorials/using-cloud-vpn-with-cisco-asr

Launching the Cisco Catalyst C9800-CL image on Google Cloud

Information about launch Cisco Catalyst C9800-CL on Google Cloud Engine

Launching a Cisco Catalyst 9800 occurs directly from the Google Cloud Platform Marketplace. Cisco Catalyst 9800 will be deployed on a Google Compute Engine(GCE) Instance (VM).

Supported AMI type and scale

The Cisco Catalyst 9800 Wireless Controller supports the following profiles. Each profile supports a different AP and client count that fits your needs:

Table 1 : 9800-CL Profiles

vCPUs	RAM	Disk	# of NIC	AP Count	Client Count
4	8	8	1	1000	10000
6	16	8	1	3000	32000
10	32	8	1	6000	64000

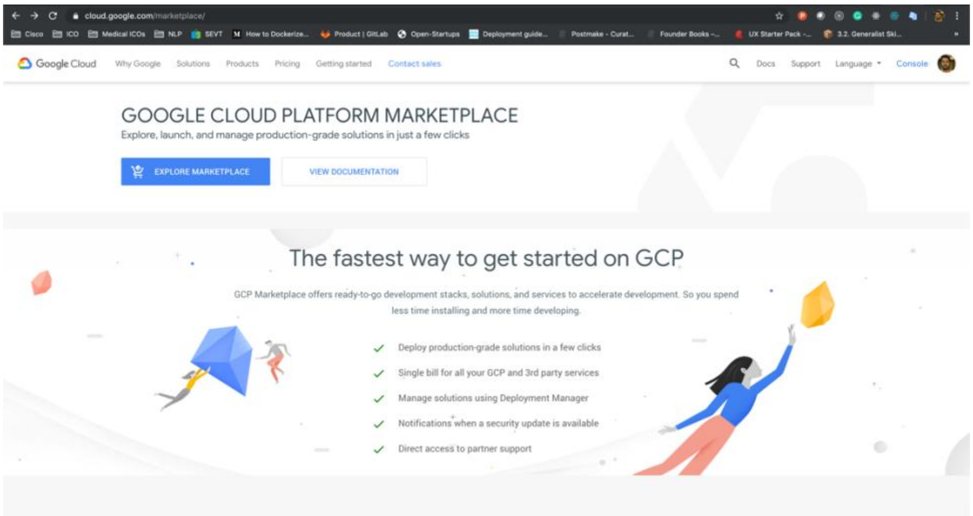
Licensing

The Cisco Catalyst 9800 Wireless Controller for GCP is purchased and on the GCP Marketplace using the Bring Your Own License (BYOL) model. After you deploy the C9800-CL in GCP you would have to purchase the DNA subscription licenses for APs using the Smart Licensing mode from Cisco.com.

Launching a 9800-CL from the Google Cloud Platform Marketplace using a Solution Template

Please refer to the Prerequisites section before you get started.

1. Head over to the Google Cloud Platform Marketplace (https://cloud.google.com/marketplace/)



GOOGLE CLOUD PLATFORM MARKETPLACE

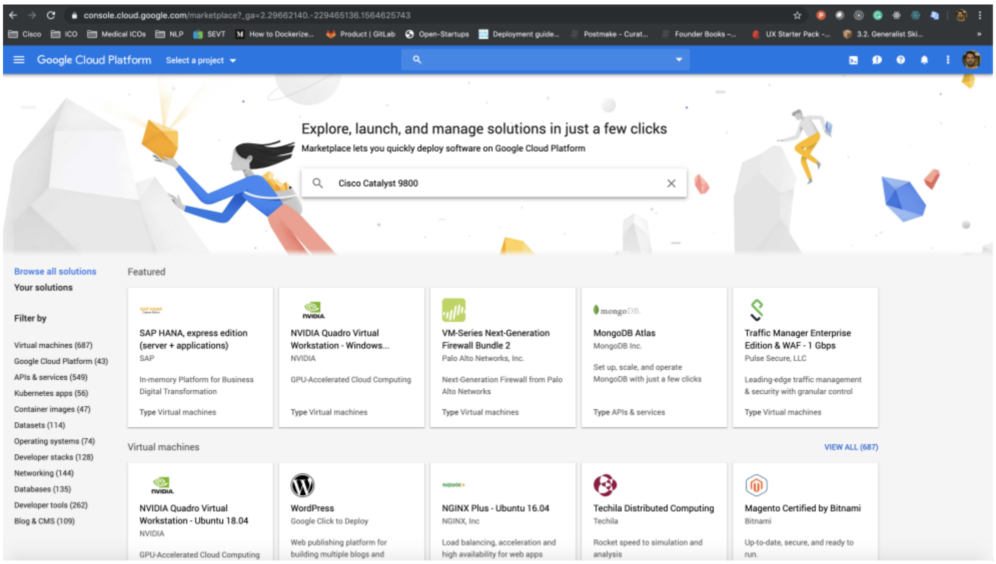
Explore, launch, and manage production-grade solutions in just a few clicks

The fastest way to get started on GCP

GCP Marketplace offers ready-to-go development stacks, solutions, and services to accelerate development. So you spend less time installing and more time developing.

- ✓ Deploy production-grade solutions in a few clicks
- ✓ Single bill for all your GCP and 3rd party services
- ✓ Manage solutions using Deployment Manager
- ✓ Notifications when a security update is available
- ✓ Direct access to partner support

2. Click “Explore Marketplace”. In the next page, search for “Cisco Catalyst 9800”.



Explore, launch, and manage solutions in just a few clicks

Marketplace lets you quickly deploy software on Google Cloud Platform

Cisco Catalyst 9800

Featured

SAP HANA, express edition (server + applications)
SAP
In-memory Platform for Business Digital Transformation
Type Virtual machines

NVIDIA Quadro Virtual Workstation - Windows...
NVIDIA
GPU-Accelerated Cloud Computing
Type Virtual machines

VM-Series Next-Generation Firewall Bundle 2
Palo Alto Networks, Inc.
Next-Generation Firewall from Palo Alto Networks
Type Virtual machines

MongoDB Atlas
MongoDB Inc.
Set up, scale, and operate MongoDB with just a few clicks
Type APIs & services

Traffic Manager Enterprise Edition & WAF - 1 Gbps
Pulse Secure, LLC
Leading-edge traffic management & security with granular control
Type Virtual machines

Virtual machines

NVIDIA Quadro Virtual Workstation - Ubuntu 18.04
NVIDIA
GPU-Accelerated Cloud Computing

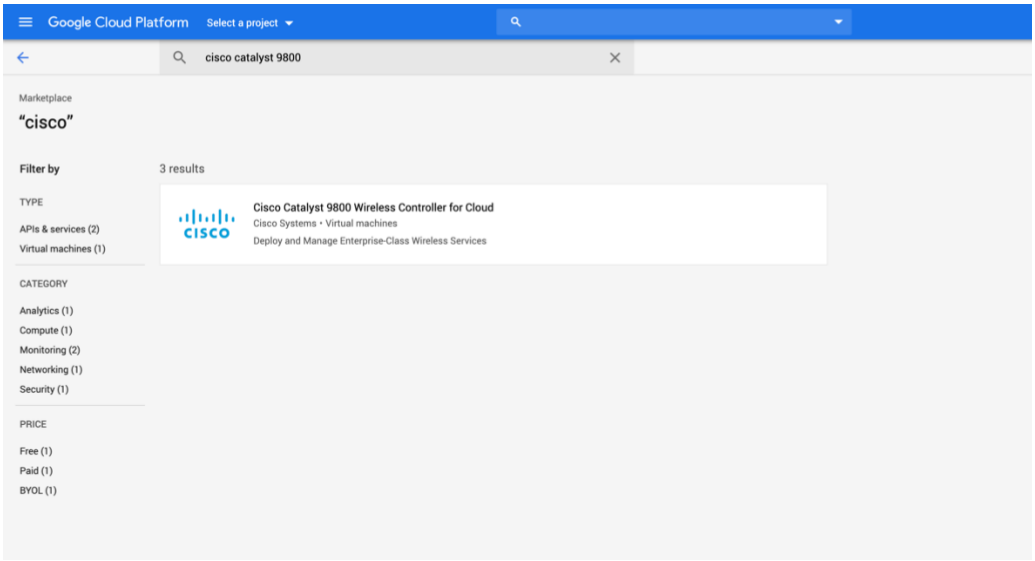
WordPress
Google Click to Deploy
Web publishing platform for building multiple blogs and

NGINX Plus - Ubuntu 16.04
NGINX, Inc
Load balancing, acceleration and high availability for web apps

Techila Distributed Computing
Techila
Rocket speed to simulation and analysis

Magento Certified by Bitnami
Bitnami
Up-to-date, secure, and ready to run.

3. Amongst the search results, please select the Cisco Catalyst 9800 Wireless controller for Cloud



Marketplace

"cisco"

Filter by

TYPE

APIs & services (2)
Virtual machines (1)

CATEGORY

Analytics (1)
Compute (1)
Monitoring (2)
Networking (1)
Security (1)

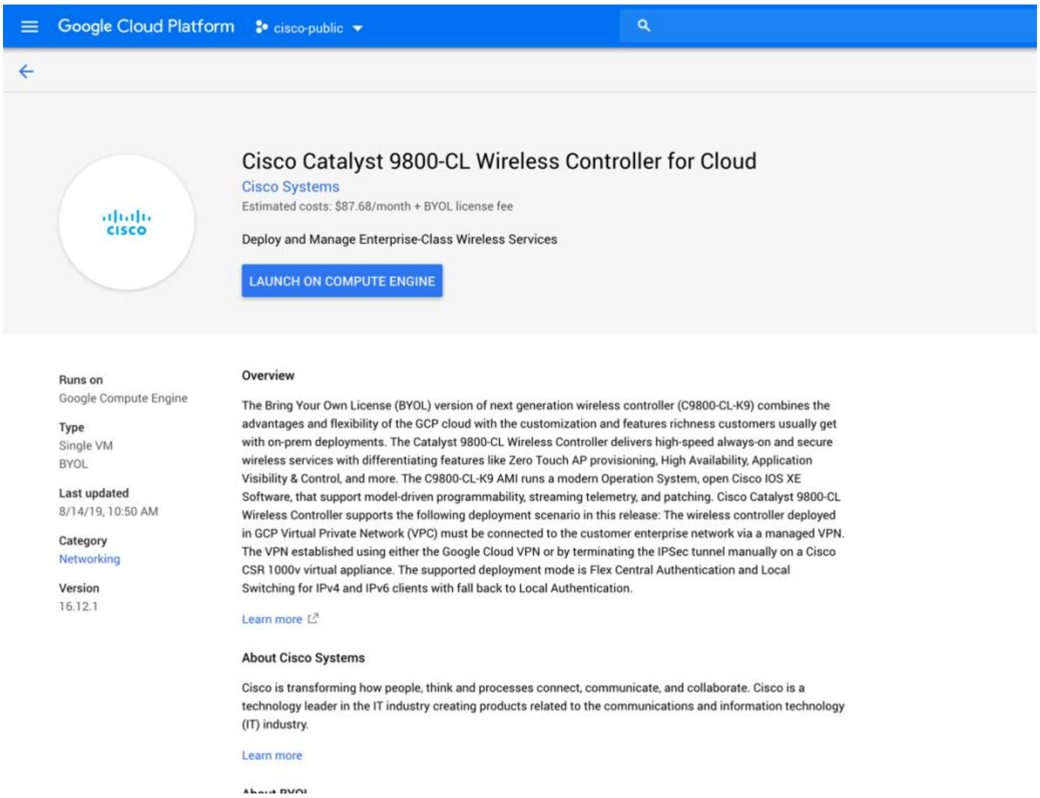
PRICE

Free (1)
Paid (1)
BYOL (1)

3 results

Cisco Catalyst 9800 Wireless Controller for Cloud
Cisco Systems • Virtual machines
Deploy and Manage Enterprise-Class Wireless Services

4. This will take you to the Product's page. Click "Launch on Compute Engine". This will open the VM configuration process.



Cisco Catalyst 9800-CL Wireless Controller for Cloud
Cisco Systems
Estimated costs: $87.68/month + BYOL license fee

Deploy and Manage Enterprise-Class Wireless Services

Runs on
Google Compute Engine

Type
Single VM
BYOL

Last updated
8/14/19, 10:50 AM

Category
Networking

Version
16.12.1

Overview

The Bring Your Own License (BYOL) version of next generation wireless controller (C9800-CL-K9) combines the advantages and flexibility of the GCP cloud with the customization and features richness customers usually get with on-prem deployments. The Catalyst 9800-CL Wireless Controller delivers high-speed always-on and secure wireless services with differentiating features like Zero Touch AP provisioning, High Availability, Application Visibility & Control, and more. The C9800-CL-K9 AMI runs a modern Operation System, open Cisco IOS XE Software, that support model-driven programmability, streaming telemetry, and patching. Cisco Catalyst 9800-CL Wireless Controller supports the following deployment scenario in this release: The wireless controller deployed in GCP Virtual Private Network (VPC) must be connected to the customer enterprise network via a managed VPN. The VPN established using either the Google Cloud VPN or by terminating the IPSec tunnel manually on a Cisco CSR 1000v virtual appliance. The supported deployment mode is Flex Central Authentication and Local Switching for IPv4 and IPv6 clients with fall back to Local Authentication.

Learn more

About Cisco Systems

Cisco is transforming how people, think and processes connect, communicate, and collaborate. Cisco is a technology leader in the IT industry creating products related to the communications and information technology (IT) industry.

Learn more

About BYOL

5. In the Product configuration page, please enter the values as shown here:

   a. Deployment name : Choose a name for the deployment.
   b. Hostname : This is the 9800-CL's Hostname. Enter an appropriate alphanumeric value.
   c. Instance SSH Key : Specify a SSH public key. This is the key that will be used to do a password-less login to the wireless controller. Use "gcp-user" (default username) as the username to login with this key.
   d. Username : Specify a Username. This is the 9800-CL's username that will be used to login to the wireless controller (via HTTPS, SSH, etc.)
   e. Password : Specify the Password to be configured on the 9800-CL. This is the password that will be used along with the username (configured in step d) to login to the 9800 controllers.

f. Zone : Select the zone where you would like to deploy the 9800-CL

g. Machine Type:

h. As mentioned earlier, the 9800-CL supports 3 different scales. Depending on your need, please click "Customize" and enter the required number of vCPUs, RAM as per the : 9800-CL Profiles.

i. Boot Disk:

   i. Boot Disk Type : Select "SSD Persistent Disk"

   ii. Boot Disk Size in GB : Please select the right boot disk type as per the table at : : 9800-CL Profiles

   ***Note** : The minimum boot-disk size supported by GCP (as on the date this document was created) is 10GB. Please select 10GB.*

j. Networking:

   i. Network : From the dropdown, choose the network that was created earlier.

   ii. Subnetwork : From the dropdown, choose the subnetwork created earlier.

k. External IP : Choose "None"

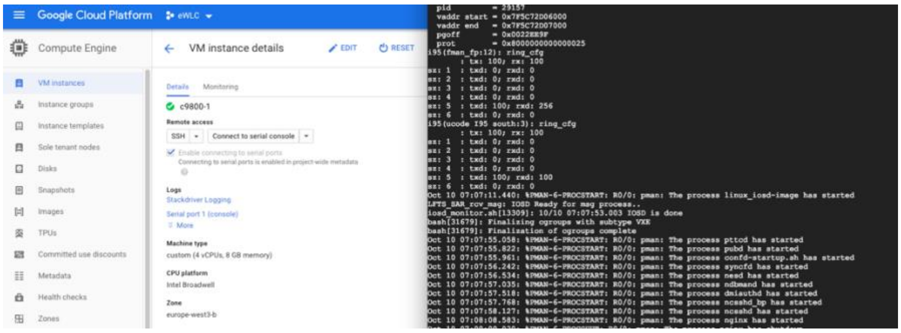
l. IP Forwarding : Choose "Yes"

m. Click Deploy

6. After successful deployment, the system displays a message that the 9800-CL instance has been deployed. Please verify the IP address of the controller.

Accessing the Cisco C9800-CL instance in GCP

After you have created the instance you can watch the initial boot by connecting to the serial console. Click on the newly created instance and then click on connect serial console:



c9800-1

Remote access

☑ Enable connecting to serial ports
Connecting to serial ports is enabled in project-wide metadata

Logs

Machine type
custom (4 vCPUs, 8 GB memory)

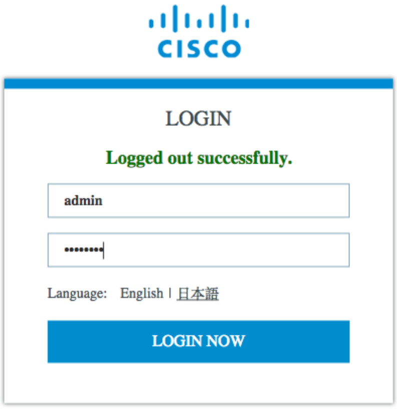
CPU platform
Intel Broadwell

Zone
europe-west3-b

```
  pid          = 29157
  vaddr start  = 0x7F5C72D06000
  vaddr end    = 0x7F5C72D07000
  pgoff        = 0x0022EE9F
  prot         = 0x8000000000000025
i95(fman_fp:12): ring_cfg
        : tx: 100; rx: 100
sz: 1   : txd: 0; rxd: 0
sz: 2   : txd: 0; rxd: 0
sz: 3   : txd: 0; rxd: 0
sz: 4   : txd: 0; rxd: 0
sz: 5   : txd: 100; rxd: 256
sz: 6   : txd: 0; rxd: 0
i95(ucode I95 south:3): ring_cfg
        : tx: 100; rx: 100
sz: 1   : txd: 0; rxd: 0
sz: 2   : txd: 0; rxd: 0
sz: 3   : txd: 0; rxd: 0
sz: 4   : txd: 0; rxd: 0
sz: 5   : txd: 100; rxd: 100
sz: 6   : txd: 0; rxd: 0
Oct 10 07:07:11.440: %PMAN-6-PROCSTART: R0/0: pman: The process linux_iosd-image has started
LFTS_SAR_rcv_msg: IOSD Ready for msg process..
iosd_monitor.sh[13309]: 10/10 07:07:53.003 IOSD is done
bash[31679]: Finalizing cgroups with subtype VXE
bash[31679]: Finalization of cgroups complete
Oct 10 07:07:55.058: %PMAN-6-PROCSTART: R0/0: pman: The process pttcd has started
Oct 10 07:07:55.822: %PMAN-6-PROCSTART: R0/0: pman: The process pubd has started
Oct 10 07:07:55.961: %PMAN-6-PROCSTART: R0/0: pman: The process confd-startup.sh has started
Oct 10 07:07:56.242: %PMAN-6-PROCSTART: R0/0: pman: The process syncfd has started
Oct 10 07:07:56.534: %PMAN-6-PROCSTART: R0/0: pman: The process nesd has started
Oct 10 07:07:57.035: %PMAN-6-PROCSTART: R0/0: pman: The process ndbmand has started
Oct 10 07:07:57.518: %PMAN-6-PROCSTART: R0/0: pman: The process dmiauthd has started
Oct 10 07:07:57.768: %PMAN-6-PROCSTART: R0/0: pman: The process ncsshd_bp has started
Oct 10 07:07:58.127: %PMAN-6-PROCSTART: R0/0: pman: The process ncsshd has started
Oct 10 07:08:08.583: %PMAN-6-PROCSTART: R0/0: pman: The process nginx has started
```

Once the instance is booted (3-4 mins), you can connect to C9800-CL using SSH or https://.

The recommendation is to login via HTTPs and access the DAY 0 interface to configure the instance with the important parameters to allow APs and Client to join. Browse to the IP of the instance and login using the credentials that you have defined during bootstrap:



LOGIN

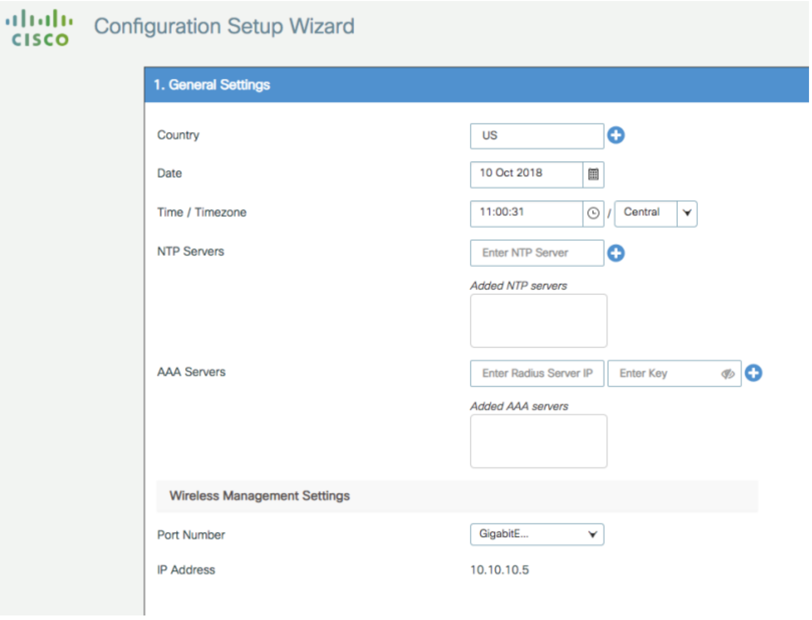
Logged out successfully.

admin

••••••••

Language: English | 日本語

Since the instance is not configured, once logged in you will be redirected to the DAY 0 page:



Configuration Setup Wizard

1. General Settings

Country	US
Date	10 Oct 2018
Time / Timezone	11:00:31 / Central
NTP Servers	Enter NTP Server
	Added NTP servers
AAA Servers	Enter Radius Server IP · Enter Key
	Added AAA servers

Wireless Management Settings

Port Number	GigabitE...
IP Address	10.10.10.5

To login to the controller using SSH, please use the following command.

1. With SSH-Key

```
ssh gcp-user@<Private IP address of the 9800-CL>
```

2. Password based

```
ssh <username>@<Private IP address of the 9800-CL>
The “username” was configured during the 9800-CL setup process.
```

Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright