FortiManager - Fabric Connectors for GCP

Version 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

April 11, 2019
FortiManager 6.2 Fabric Connectors for GCP
02-620-00000-20190411

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-04-11	Initial release.

Creating fabric connectors for Google Cloud Platform

You can use FortiManager to create SDN fabric connectors for Google Cloud Platform, and then install the fabric connectors to FortiGates.

The fabric connectors in FortiManager define the type of connector and include information for FortiGate to communicate with and authenticate with the products. In some cases FortiGate units must communicate with products through the Fortinet SDN Connector, and in other cases FortiGate units communicate directly with the products.

FortiGate works with Fortinet SDN Connector to communicate with Google Cloud Platform.

For more information about Fortinet SDN Connector, see the Fortinet Document Library.

You cannot import a policy package for Fortinet SDN Connector from FortiGate to FortiManager.

Following is an overview of how to create fabric connectors for Google Cloud Platform by using FortiManager:

1. Create a fabric connector object for Google Cloud Platform. See Creating Fabric Connector objects for Google Cloud Platform on page 5.
2. Create dynamic firewall address objects. See Configuring dynamic firewall addresses for fabric connectors on page 1.
   You cannot import address names from Google Cloud Platform to FortiManager.
3. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for Google Cloud Platform. See Creating IP policies on page 7.
4. Install the policy package to FortiGate. See Installing policy packages on page 8.
   FortiGate communicates with Google Cloud Platform to dynamically populate the firewall address objects with IP addresses.

Creating Fabric Connector objects for Google Cloud Platform

With FortiManager, you can create a fabric connector for Google Cloud Platform (GCP), and then import address names from Google Cloud Platform to automatically create dynamic objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information and Fortinet SDN Connector to communicate with Google Cloud Platform and dynamically populate the objects with IP addresses.

When you create a fabric connector for Google Cloud Platform, you are specifying how FortiGate can communicate with Google Cloud Platform through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManagerwith ADOM version 6.2 or later.
  The method described in this topic for creating fabric connectors requires ADOM version 6.2 or later.
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Google Cloud Platform.

To create a fabric connector object for Google Cloud Platform:

1. Go to *Fabric View* > *Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Google Cloud Platform*, and click *Next*. The *Google Cloud Platform* screen is displayed.
4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Google Cloud Platform (GCP).
Project Name	Specify the Project Name for the SDN Connector.
Service Account Email	Specify the Service Account Email for the SDN Connector.
Private Key	Specify the Private Key for the Fortinet SDN Connector.
Update Interval (s)	Specify the update interval for the Fortinet SDN Connector. Select one of the following options: • Click *Use Default* to use the default interval. • Click *Specify* and specify the interval.
Status	Toggle *On* to enable the fabric connector object. Toggle *OFF* to disable the fabric connector object.

Importing address names to fabric connectors

After you configure a fabric connector, you can import address names from products, such as NSX and ACI, to the fabric connector, and dynamic firewall address objects are automatically created.

When you are importing address names from AWS, you must add filters to display the correct instances before importing address names.

You cannot import address names to fabric connectors created for Microsoft Azure and Nuage Virtualized Services Platform. You must manually create dynamic firewall address objects for these types of fabric connectors.

To import address names for NSX and ACI:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Security Fabric* > *Fabric Connectors*.
3. In the content pane, right-click the fabric connector, and select *Import*.
   The *Import SDN Connector* dialog box is displayed.
4. Select the address names, and click *Import*.
   The address names are imported and converted to dynamic firewall address objects that are displayed on the *Firewall Objects* > *Addresses* pane.

To import address names for AWS:

1. Go to *Policy & Objects* > *Object Configurations*.
2. In the tree menu, go to *Security Fabric* > *Fabric Connectors*.
3. In the content pane, right-click the fabric connector, and select *Import*.
   The *Import SDN Connector* dialog box is displayed.

4. Create a filter to select the correct AWS instances:
   a. Click *Add Filter*.
      The *Filter Generator* dialog box is displayed.

   b. Click *Add Filter*, and select a filter.
      A filtered list of instances is displayed.
   c. Click *OK*.
      The *Import SDN Connector* dialog box is displayed, and it contains the filter.
      You can add additional filters, or edit and delete filters.
   d. (Optional) Repeat this procedure to add additional filters.
5. Select the filters, and click *Import*.
   The address names are imported and converted to dynamic firewall address objects that are displayed on the *Firewall Objects* > *Addresses* pane. The name of the dynamic firewall address uses the following naming convention: `AWS-<random identifier>`. Use the *Details* column and the instance ID to identify the object.

Creating IP policies

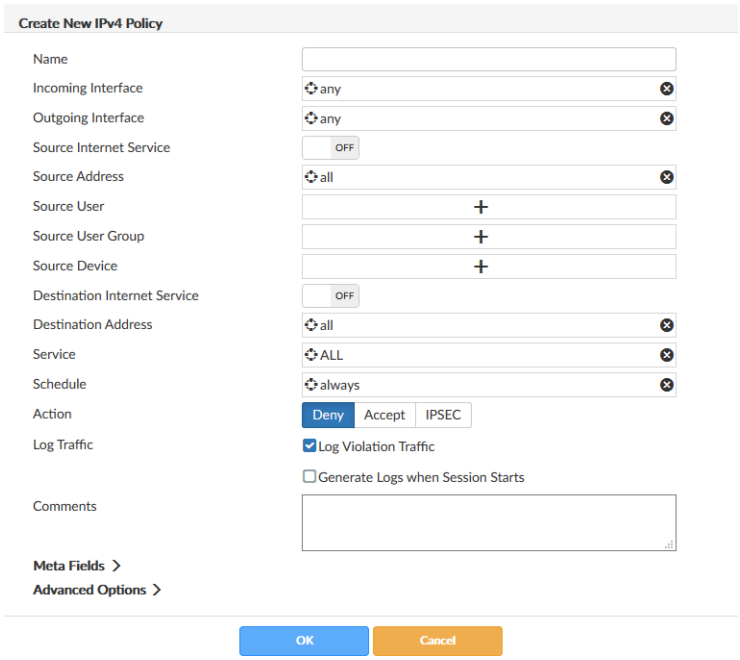
The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.

On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.



5. Complete the options.
6. Click *OK* to create the policy.
   You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Installing policy packages

When installing a policy package, objects that are referenced in the policy will be installed to the target device. Default or per-device mapping must exist or the installation will fail.

Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

To install a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.