About the Cisco Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the Ciso Secure Firewall Management Center (management center) so it can be used in access control rules.

The following topics provide background about the dynamic attributes connector:

About the Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in Secure Firewall Management Center (management center) access control rules.

Supported connectors

We currently support:

Table 1: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS	AWS security groups	AWS service tags	Azure	Azure Service Tags	Cisco Cyber Vision	Generic Text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall Management Center 7.4	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

More information about connectors:

- Amazon Web Services (AWS)

For more information, see a resource like Tagging AWS resources on the Amazon documentation site.

See Amazon Web Services Connector—About User Permissions and Imported Data.

- GitHub

  For more information, see Create a GitHub Connector.

- Google Cloud

  For more information, see Setting Up Your Environment in the Google Cloud documentation.

- Microsoft Azure

  For more information, see this page on the Azure documentation site.

  See Azure Connector—About User Permissions and Imported Data.

- Microsoft Azure service tags

  For more information, see a resource like Virtual network service tags on Microsoft TechNet.

- Office 365 IP addresses

  For more information, see Office 365 URLs and IP address ranges on docs.microsoft.com.

- VMware categories and tags managed by vCenter and NSX-T

  For more information, see a resource like vSphere Tags and Attributes in the VMware documentation site.

- Webex IP addresses

  For more information, see Create a Webex Connector.

- Zoom IP addresses

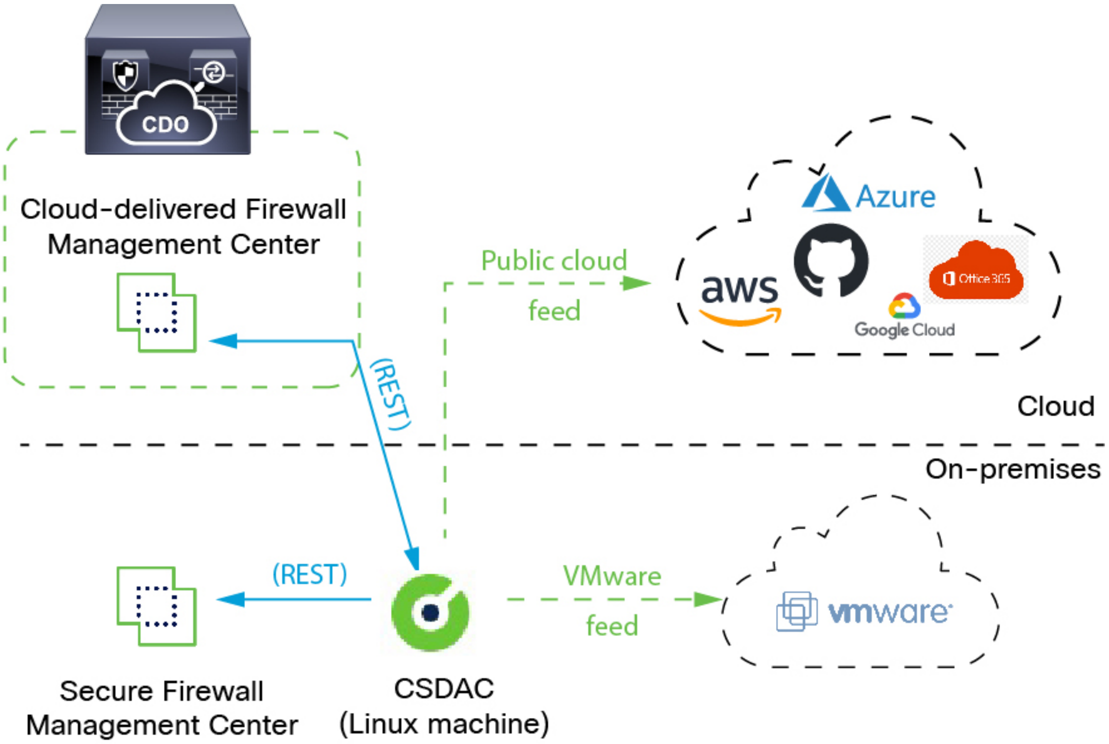
  For more information, see Create a Zoom Connector.

How It Works

Network constructs such as IP address are not reliable in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

You can collect these tags and attributes using dynamic attributes connector Docker containers running on an Ubuntu, CentOS, or Red Hat Enterprise Linux virtual machine. Install the dynamic attributes connector on the Ubuntu host using an Ansible collection.

The following figure shows how the system functions at a high level.



- Install the dynamic attributes connector on a supported Linux virtual machine.

  For more information, see Supported Operating Systems and Third-Party Software.

- The system supports certain public cloud providers.

  This topic discusses supported *connectors* (which are the connections to those providers).

- The *adapter* defined by the dynamic attributes connector receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.

  You can create the following types of adapters:

  - *On-Prem Firewall Management Center* for an on-premises Management Center device.

    This type of Management Center device might be managed by Cisco Defense Orchestrator (CDO) or it might be a standalone.

  - *Cloud-delivered Firewall Management Center* for devices managed by CDO.