Configure Geolocation-Based Firewall Rules for Network Access

Table 1: Feature History

Feature Name	Release Information	Description
Geolocation-Based Firewall Rules for Allowing or Denying Network Traffic Based on Geolocation	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature enables you to configure firewall rules for allowing or denying network traffic based on the source and destination location instead of IP addresses. This feature adds a new object group, geo, where you can specify countries and continents as objects in an Access Control List (ACL). An object group ACL simplifies policy creation in large networks, especially if the ACL changes frequently. New object-group and geo commands were added.

Overview of Geolocation-Based Firewall Rules

Geolocation-based firewall rules allow you to configure firewall rules for allowing or denying network traffic based on the specified source and destination locations.

A third-party database is used for geolocation-to-IP-address mapping. Use the **geo database update** command to update the geolocation database periodically to pick up the latest changes.

After you configure a geolocation-based firewall rule by specifying source and destination locations in Cisco SD-WAN Manager, the geolocation database is automatically enabled in the CLI. Alternatively, you can use the **geo database** command to enable the geolocation database.

For more information on the CLI commands, see Cisco IOS XE SD-WAN Qualified Command Reference.

This feature adds a new object group **geo**, where you can specify countries and continents as objects to use in Access Control Lists (ACLs). The new geo object group is then used in the ACL to enable geolocation-based firewall rules.

The geo object group is a collection of the following types of objects:

- Three-letter country code objects
- Two-letter continent code objects

An object group can contain a single object or multiple objects. You can nest other geolocation object groups using the **group-object** command.

Note You cannot configure nested geo object groups in Cisco SD-WAN Manager. You can configure nested geo object groups using only the CLI.

Data packets are classified using geolocation-based firewall rules instead of using IP addresses. When classifying the data packet, if a firewall rule has a geolocation-based filter, an IP address lookup occurs against the geolocation database to determine which country or continent is associated with the IP address.

Use-Case Scenario

A client (192.168.11.10) in a local area network (LAN) initiates traffic over Dedicated Internet Access (DIA) to a destination IP addresses belonging to France (FRA) and Germany (GBR). As per the security firewall policy, traffic to France should be inspected and that to Germany should be dropped.

Benefits of Geolocation-Based Firewall Rules

- You can restrict access to particular countries without needing to know the associated IP addresses for those countries.
- A geolocation can be a country, a continent, or a list containing both continents and countries.

  Note After you have chosen a continent in a security firewall rule, all IP addresses belonging to that particular continent code are inspected as part of the security firewall rule.

- You can add multiple geolocation lists or geolocations using a single policy.
- When you update a geo object group, all the policies that use that geo object group are automatically updated.

Prerequisites for Geo Object Groups

To associate a geo object with an ACL, the geo object group must be already defined with at least one object.

Restrictions for Geo Object Groups

- Empty geo object groups are not supported. Any empty geo object group is deleted in exiting global configuration mode. You cannot associate an empty object group with an ACL.

Note An empty geo object group is a geo object group that does not contain any references to countries. To empty a geo object group, you need to remove any references to countries within the geo object group.

- As long as a geo object group is in use inside the corresponding ACL or nested in another group, it can neither be deleted nor emptied.
- A geo object group can be associated only with extended IPv4 ACLs and not with IPv4 standard ACLs.

Configure Geolocation-Based Firewall Rules

To configure firewall rules, specify the source and destination locations in the security firewall policies in Cisco SD-WAN Manager.

There are two ways to configure geofiltering using Cisco SD-WAN Manager:

- Configure a geolocation list using **Configuration** > **Security** > **Custom Options**.
- Create or add a geolocation list or a geolocation to an existing firewall security policy.

  Prerequisite: You must have an existing security policy for the second bullet item.

Note If you add a geolocation list, you cannot add a geolocation.

Conversely, if you add a geolocation, you cannot add a geolocation list.

Note You cannot configure both a fully qualified domain name (FQDN) and a geo as a source data prefix and as a destination data prefix.

Configure a Geolocation List Using Configuration > Security > Custom Options

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. From the **Custom Options** drop-down menu, choose **Lists**.
3. Click **Geo Location** in the left pane.
4. Click **New Geo Location List**.
5. Enter a name for the geolocation list.

6. Choose one or more geolocations from the drop-down menu.

> **Note** If you choose a continent, you cannot choose any of the countries that are part of the continent. If you want to choose a list of countries, choose the appropriate countries from the list.

7. Click **Add**.

Create a Geolocation List or Add a Geolocation to an Existing Security Firewall Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Choose an existing security policy.
3. For the chosen policy, click **...**, and click **Edit**.

   The **Edit Security Policy** window displays.
4. Click **Firewall**.
5. For the desired policy you want to modify, click **...** and click **Edit**.

   The **Edit Firewall Policy** window displays.
6. Click **Add Rule/Rule Set Rule**.
7. From the drop-down menu, choose **Add Rule**.

   The **New Firewall** window displays.
8. Click **Source Data Prefix** to add a source geolocation list or new geolocations.
9. From the **Geo Location List** drop-down menu, choose a previously configured geolocation list.
10. Alternatively, to create a new geolocation list, choose **New Geo Location**.

    The **Geo Location List** dialog box displays.

    a. In the **Geo Location List Name** field, specify a name for the geolocation list.

    b. From the **Select Geo Location** drop-down menu, choose one or more locations.

    c. Click **Save**.
11. From the **Geo Location** drop-down menu, choose one or more locations.
12. Click **Save**.
13. Click **Destination Data Prefix** to add a destination geolocation list or new geolocations.
14. Repeat Step 9 through Step 12.
15. Click **Save Firewall Policy** to save the security firewall rule.
16. Click **Save Policy Changes**.

Configure Geolocation-Based Firewall Rules Using the CLI

1. Enable the geolocation database:

   ```
   Device(config)# geo database
   ```

2. View the status of the geodatabase:

   ```
   Device# show geo status
   Geo-Location Database is enabled
   File in use       : geo_ipv4_db
   File version      : 2134.ajkdbnakjsdn
   Number of entries : 415278
   ```

3. View the contents of the geodatabase file:

   ```
   Device# show geo file-contents info bootflash:geo_ipv4_db
   File version      : 2134.ajkdbnakjsdn
   Number of entries : 415278
   ```

4. Update the geodatabase for periodic updates:

   ```
   Device# geo database update bootflash:geo_ipv4_db
   ```

   Here, *geo_ipv4_db* is the name of the geodatabase file downloaded from the Cisco.com path and copied to the bootflash device or the hard disk.

5. Create a geo object group:

   ```
   Device(config)# object-group geo GEO_1
   ```

6. Add a continent to a geo group object:

   ```
   Device(config-geo-group)# continent EU
   ```

7. Add a country to a geo group object:

   ```
   Device(config-geo-group)# country GBR
   ```

8. View the geo object group:

   ```
   Device# show object-group name Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
   GEO object group Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
   country GBR
   ```

9. View detailed country information:

   ```
   Device# show platform hardware qfp active feature geo client alpha gbr
   Country alpha code: gbr
   Country numeric code: 826
   GEO country info:
   Country alpha code: gbr
   Continent alpha code: eu
   Continent numeric code: 5
   Country ref count: 0
   Country hit count: 13
   ```

10. Verify geodatabase status:

    ```
    Device# show platform hardware qf active feature geo client stats
    CPP client Geo DB stats
    -----------------------
    Enable received             : 1
    Modify received             : 0
    ```

```
Disable received            : 0
Enable failed               : 0
Modify failed               : 0
Disable failed              : 0
IPv4 table write failed     : 0
Persona write failed        : 0
Country table write failed  : 0
```

11. View the geodatabase file and memory information:

```
Device# show platform hardware qf active feature geo client info
Geo DB enabled
DB in use
  File name: /usr/binos/conf/geo_ipv4_db
  Number of entries installed: 415278
  Version: 2134.ajkdbnakjsdn
  Datapath PPE Address: 0x00000000f0d3b070
  Size (bytes): 6644448
  Exmem Handle: 0x009dcf0709080003
Country table
  Datapath PPE Address: 0x00000000f04bcc60
  Size (bytes): 16000
  Exmem Handle: 0x009550c609080003
```

12. View geodatabase table memory information:

```
Device# show platform hardware qf active feature geo datapath memory
Table-Name   Address       Size
--------------------------------
Country DB   0xf04bcc60    1000
IPV4 DB      0xf0d3b070    415278
```

For more information on the CLI commands, see Cisco IOS XE SD-WAN Qualified Command Reference.

Update the Geolocation Database Using the CLI

To ensure that you are using up-to-date geographical location data, we recommend that you update the geolocation database.

To update the geolocation database using the CLI:

On the CLI, use Secure Copy Protocol (SCP) or TFTP to copy the geolocation database to your Cisco IOS XE Catalyst SD-WAN device:

```
Device# copy scp: bootflash:
```

or

```
Device# copy tftp: bootflash:
```

Verify Geolocation-Based Firewall Rules Using the CLI

The following example shows how geo object groups are created for France and Germany:

```
platform inspect match-statistics per-filter
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
 country FRA
!
```

```
object-group network Zone1_to_Zone1-seq-Rule_1-network-src-og_
 host 192.168.11.10
!
object-group service Zone1_to_Zone1-seq-Rule_1-service-og_
 ip
!
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
 15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
 country GBR
```

The following example shows how a geo object group is defined under an extended ACL that is used in a security firewall class map:

```
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
 15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
 country GBR
!
object-group network Zone1_to_Zone1-seq-Rule_1-network-src-og_
 host 192.168.11.10
!
object-group service Zone1_to_Zone1-seq-Rule_1-service-og_
 ip
!
ip access-list extended Zone1_to_Zone1-seq-Rule_1-acl_
 15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_ geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
!
ip access-list extended Zone1_to_Zone1-seq-Rule_2-acl_
!
object-group geo Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
 country GBR
```

The following example shows when a geolocation is chosen as part of a security firewall rule either in a source or a destination data prefix from Cisco SD-WAN Manager, the geodatabase is added by default. If a geolocation is removed, the geodatabase is removed from the rule.

```
class-map type inspect match-all Zone1_to_Zone1-seq-1-cm_
 match access-group name Zone1_to_Zone1-seq-Rule_1-acl_
!
class-map type inspect match-all Zone1_to_Zone1-seq-11-cm_
 match access-group name Zone1_to_Zone1-seq-Rule_2-acl_
!
policy-map type inspect Zone1_to_Zone1
 ! first
 class Zone1_to_Zone1-seq-1-cm_
   inspect
 !
 class Zone1_to_Zone1-seq-11-cm_
   drop
 !
 class class-default
   drop
 !
parameter-map type inspect-global
 alert on
 log dropped-packets
 multi-tenancy
 vpn zone security
!
zone security Zone0
 vpn 0
!
zone security Zone1
 vpn 1
!
zone-pair security ZP_Zone1_Zone0_Zone1_to_Zone1 source Zone1 destination Zone0
 service-policy type inspect Zone1_to_Zone1
!
geo database
```

The following is a sample output of the **show policy-firewall config zone-pair** command used for validating geolocation configuration:

```
Device# show policy-firewall config zone-pair ZP_Zone1_Zone0_Zone1_to_Zone1

Zone-pair              : ZP_Zone1_Zone0_Zone1_to_Zone1
Source Zone            : Zone1
Destination Zone       : Zone0
Service-policy inspect : Zone1_to_Zone1
  Class-map : Zone1_to_Zone1-seq-1-cm_ (match-all)
  Match access-group name Zone1_to_Zone1-seq-Rule_1-acl_
Extended IP access list Zone1_to_Zone1-seq-Rule_1-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_1-service-og_ object-group
Zone1_to_Zone1-seq-Rule_1-network-src-og_geo-group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
  Action : inspect
  Parameter-map : Default
  Class-map : Zone1_to_Zone1-seq-11-cm_ (match-all)
  Match access-group name Zone1_to_Zone1-seq-Rule_2-acl_
Extended IP access list Zone1_to_Zone1-seq-Rule_2-acl_
  15 permit object-group Zone1_to_Zone1-seq-Rule_2-service-og_ object-group
Zone1_to_Zone1-seq-Rule_2-network-src-og_geo-group Zone1_to_Zone1-seq-Rule_2-geo-dstn-og_
  Action : drop log
  Parameter-map : Default
  Class-map : class-default (match-any)
    Match any
    Action : drop log
  Parameter-map : Default
```

The following is a sample output of the **show policy-map type inspect zone-pair sessions** command used for verifying inspected and dropped traffic:

```
show policy-map type inspect zone-pair sessions
  Zone-pair: ZP_Zone1_Zone0_Zone1_to_Zone1
  Service-policy inspect : Zone1_to_Zone1

    Class-map: Zone1_to_Zone1-seq-1-cm_ (match-all)
      Match: access-group name Zone1_to_Zone1-seq-Rule_1-acl_
      Inspect
        Established Sessions
         Session ID 0x0000000A (192.168.11.10:8)=>(2.10.1.1:14780) icmp SIS_OPEN.
          Created 00:00:03, Last heard 00
          Bytes sent (initiator:responder) [224:168]


    Class-map: Zone1_to_Zone1-seq-11-cm_ (match-all)
      Match: access-group name Zone1_to_Zone1-seq-Rule_2-acl_
      Drop
        13 packets, 1326 bytes

    Class-map: class-default (match-any)
```

```
Match: any
Drop
  0 packets, 0 bytes
```