

Objects for Access Control

Objects are reusable components for use in your configuration. You can define and use them in ASA configurations in the place of inline IP addresses, services, names, and so on. Objects make it easy to maintain your configurations because you can modify an object in one place and have it be reflected in all other places that are referencing it. Without objects you would have to modify the parameters for every feature when required, instead of just once. For example, if a network object defines an IP address and subnet mask, and you want to change the address, you only need to change it in the object definition, not in every feature that refers to that IP address.

- Guidelines for Objects, on page 1
- Configure Objects, on page 2
- Monitoring Objects, on page 12
- History for Objects, on page 12

Guidelines for Objects

IPv6 Guidelines

Supports IPv6 with the following restrictions:

- You can mix IPv4 and IPv6 entries in a network object group, but you cannot use a mixed object group for NAT.

Additional Guidelines and Limitations

- Objects must have unique names, because objects and object groups share the same name space. While you might want to create a network object group named “Engineering” and a service object group named “Engineering,” you need to add an identifier (or “tag”) to the end of at least one object group name to make it unique. For example, you can use the names “Engineering_admins” and “Engineering_hosts” to make the object group names unique and to aid in identification.
- If you enter more than one item in source or destination address, or source or destination service, in an ACL or access rule, ASDM automatically creates an object group for them with the prefix DM_INLINE. These objects are not shown on the objects page, but they are defined on the device.
- Object names are limited to 64 characters, including letters, numbers, and these characters: .!@#$%^&()-_{}. Object names are case-sensitive.

Configure Objects

The following sections describe how to configure objects that are primarily used on access control.

Configure Network Objects and Groups

Network objects and groups identify IP addresses or host names. Use these objects in access control lists to simplify your rules.

Configure a Network Object

A network object can contain a host, a network IP address, a range of IP addresses, or a fully qualified domain name (FQDN).

You can also enable NAT rules on the object (excepting FQDN objects). For more information about configuring object NAT, see Network Address Translation (NAT).

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Network Objects/Group**.

Step 2 Do one of the following:

- Choose **Add > Network Object** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Configure the address for the object based on the object **Type** and **IP version** fields.

- **Host**—The IPv4 or IPv6 address of a single host. For example, 10.1.1.1 or 2001:DB8::0DB8:800:200C:417A.
- **Network**—The address of a network. For IPv4, include the mask, for example, **IP address** = 10.0.0.0 **Netmask** = 255.0.0.0. For IPv6, include the prefix, such as **IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60.
- **Range**—A range of addresses. You can specify IPv4 or IPv6 ranges. Do not include masks or prefixes.
- **FQDN**—A fully-qualified domain name, that is, the name of a host, such as www.example.com.

Step 4 Click **OK**, then click **Apply**.

You can now use this network object when you create a rule. If you edit an object, the change is inherited automatically by any rules using the object.

Configure a Network Object Group

Network object groups can contain multiple network objects as well as inline networks or hosts. Network object groups can include a mix of both IPv4 and IPv6 addresses.

However, you cannot use a mixed IPv4 and IPv6 object group for NAT, or object groups that include FQDN objects.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**.

Step 2 Do one of the following:

- Choose **Add > Network Object Group** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Add network objects to the group using any combination of the following techniques:

- **Existing Network Objects/Groups**—Select any already defined network object or group and click **Add** to include them in the group.
- **Create New Network Object Member**—Enter the criteria for a new network object and click **Add**.

Step 4 After you add all the member objects, click **OK**, then click **Apply**.

You can now use this network object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

Configure Service Objects and Service Groups

Service objects and groups identify protocols and ports. Use these objects in access control lists to simplify your rules.

Configure a Service Object

A service object can contain a single protocol specification.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Service Object/Group**.

Step 2 Do one of the following:

- Choose **Add > Service Object** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Choose the service type and fill in details as needed:

- Protocol—A number between 0-255, or a well-known name, such as **ip**, **tcp**, **udp**, **gre**, and so forth..
- ICMP, ICMP6—You can leave the message type and code fields blank to match any ICMP/ICMP version 6 message. You can optionally specify the ICMP type by name or number (0-255) to limit the object to

that message type. If you specify a type, you can optionally specify an ICMP code for that type (1-255). If you do not specify the code, then all codes are used.

- TCP, UDP, SCTP—You can optionally specify ports for the source, destination, or both. You can specify the port by name or number. You can include the following operators:
  - <—Less than. For example, <80.
  - >—Greater than. For example, >80.
  - **!=**—Not equal to. For example, !=80.
  - **-** (hyphen)—An inclusive range of values. For example, 100-200.

Step 4 Click **OK**, and then **Apply**.

Configure a Service Group

A service object group includes a mix of protocols, if desired, including optional source and destination ports for protocols that use them, and ICMP type and code.

Before you begin

You can model all services using the generic service object group, which is explained here. However, you can still configure the types of service group objects that were available prior to ASA 8.3(1). These legacy objects include TCP/UDP/TCP-UDP port groups, protocol groups, and ICMP groups. The contents of these groups are equivalent to the associated configuration in the generic service object group, with the exception of ICMP groups, which do not support ICMP6 or ICMP codes. If you still want to use these legacy objects, for detailed instructions, see the **object-service** command description in the command reference on Cisco.com.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Service Objects/Groups**.

Step 2 Do one of the following:

- Choose **Add > Service Group** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Add service objects to the group using any combination of the following techniques:

- **Existing Service/Service Group**—Select any already defined service, service object, or group and click **Add** to include them in the group.
- **Create New Member**—Enter the criteria for a new service object and click **Add**. If you give the object a name, when you apply changes, the new object is created and added to the group; otherwise, unnamed objects are members of this group only. You cannot name TCP-UDP objects; these are members of the group only.

Step 4 After you add all the member objects, click **OK**, then click **Apply**.

You can now use this service object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

Configuring Network-Service Objects and Groups

A network-service object or group defines an application. An application can consist of a DNS domain name (such as example.com), IP subnet, and optionally, protocol and port, such as TCP/80. Thus, a network-service object or group can combine the contents of separate network and service objects into a single object.

You can use the network-service object group in an extended ACL for use with routes maps (in policy-based routing), access control rules, and VPN filter. Note that you cannot directly use a network-service object (not group) in an ACL: you must first put objects in a group object, then you can use the group object.

When you use domain name specifications, the system uses DNS snooping to get the IP addresses that are obtained through the user's DNS request prior to the start of the connection. This ensures that an IP address is available at the start of a connection, so that the connection is handled correctly, by route maps and access control rules, from the first packet.

The Application Visibility and Control (AVC) service uses network-service objects and groups to define applications based on the contents of the Vulnerability Database. For more information, see Application Visibility and Control.

Guidelines for Network-Service Objects

- DNS inspection is required if you include DNS domain name specifications in a network-service object. DNS inspection is enabled by default. Do not disable it if you use network-service objects.
- DNS snooping is done on UDP DNS packets only, it is not done on TCP or HTTP DNS packets. Unlike fully-qualified domain name objects, network-service domain specifications are snooped immediately, even if you do not use the object in an access list.
- You cannot enable dnscrypt in the DNS inspection policy map; it is not compatible with the DNS snooping that is required to obtain IP addresses for domains used in network-service objects. Any network-service objects that include domain specifications will become inoperable and the related access control entries will not be matched.
- You can define a maximum of 1024 network-service groups. However, this limit is shared with identity firewall local user groups. For each network-service group defined, you can create 2 fewer user groups.
- The contents of network-service groups can overlap, but you cannot create a complete duplicate of a network-service group.
- If a network-service object or group is being used in an ACL, deleting the object simply clears the object contents. The object itself remains defined in the configuration.
- The **dynamic** keyword on an object or group indicates that the object will not be saved to the running configuration, it will be shown in the **show object** output only. Do not directly configure this keyword. It is primarily for use by external device managers. The Application Visibility and Control (AVC) system creates dynamic objects and groups.
- The **app-id** command for a network-service object defines a Cisco-assigned number for a particular application, in the range 1-4294967295. Do not directly configure this command. This command is

mainly for the use of external device managers. The Application Visibility and Control (AVC) system creates dynamic objects that include the app-id command.

Configure Trusted DNS Servers

If you configure domain names in network-service objects, the system snoops DNS request/response traffic to gather IP addresses for DNS domain names and caches the results. Any DNS request/response can be snooped.

The records snooped are A, AAAA, and MX. The time-to-live (TTL) of each resolved name is honored within limits: the minimum TTL is 2 minutes, the maximum is 24 hours. This ensures that the cache does not become stale.

For security reasons, you can limit the scope of DNS snooping by defining which DNS servers should be trusted. Any DNS traffic to non-trusted DNS servers is ignored and not used to obtain mappings for network-service objects. By default, all configured and learned DNS servers are trusted; you need to change this only if you want to limit the trusted list.



Note The key is that you define the DNS servers used by your clients as trusted servers.

Before you begin

DNS snooping depends on DNS inspection, which is enabled by default. Ensure that you do not disable the inspection. In addition, DSN snooping is incompatible with the **dnscrypt** feature, so do not enable that command in the DNS inspection policy map.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **DNS** > **DNS Client**.

Step 2 Under **Trusted DNS Server**, configure the options for determining which servers to trust.

a) (Optional.) Add or remove explicitly-configured trusted DNS servers.

- Click **Add** to add a new server, then select the IP type (IPv4 or IPv6), enter the IP address of the server, and click **OK**.
- Select a server and click **Edit** to change the address.
- Select a server and click **Delete** to remove it from the trusted server list.

b) Select or deselect the following options:

- **Any**—Trust every DNS server, snoop them all. This option is disabled by default.
- **Configured-Servers**—Whether servers configured in DNS server groups should be trusted. This option is enabled by default.
- **DHCP-Client**—Whether the servers that are learned by snooping messages between a DHCP client and DHCP server are considered trusted DNS servers. This option is enabled by default.

- **DHCP-Pools**—Whether the DNS servers that are configured in the DHCP pools for clients that obtain addresses through DHCP servers running on the device interfaces should be trusted. This option is enabled by default.
- **DHCP-Relay**—Whether the servers that are learned by snooping DHCP relay messages between a DHCP client and DHCP server are considered trusted DNS servers. This option is enabled by default.

Step 3 Click **Apply**.

Configure Network-Service Objects

A network-service object defines a single application. It defines the application location either by subnet specification or more commonly, DNS domain name. Optionally, you can include protocol and port to narrow the scope of the application.

You can use these objects in network-service group objects only; you cannot directly use a network-service object in an access control list entry (ACE).

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Network Services Objects/Groups**.

Step 2 Do one of the following:

- Choose **Add** > **Network Services Objects** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 (Not recommended.) Add the application ID in the **App-ID** field.

The number is a unique Cisco-assigned number for a particular application, in the range 1-4294967295. This option is mainly for the use of external device managers. You should not configure this value.

Step 4 Add one or more members to the object:

a) Select one of the following in **Create New Member**, then fill in the appropriate address information:

- **domain**—The DNS name, up to 253 characters. This can be fully-qualified (such as www.example.com) or partial (such as example.com), in which case the object matches all subdomains, that is, servers with the partial name (such as www.example.com, www1.example.com, long.server.name.example.com, and so forth). Connections will be matched against the longest name if an exact match is available. The domain name can resolve to multiple IP addresses.
- **subnet**—The address of a network. For IPv4 subnets, include the network address and mask, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix, such as 2001:DB8:0:CD30::/60. Enter the values in the appropriate fields.

b) Select one of the following in Service Type, then fill in the appropriate fields:

- **protocol**—The protocol used in the connection, such as tcp, udp, ip, and so forth. To make the object service-agnostic, simply enter **ip**.

- **tcp** or **udp**—Enter the port number, 1-65535 or a mnemonic, such as www. For a single port, simply enter the port number. For multiple ports, you can include the number after the following operators:
  - < means any port less than the specified port number.
  - > means any port greater than the specified port number.
  - **range** means any port between the two ports specified. The first port number must be lower than the second port number.

c) Click **Add** to add the network service to the object. To delete a service, select it an click **Delete**.
d) Repeat the process until the object contains all specifications that you require.

Step 5 Click **OK**.

Configure Network-Service Object Groups

Network-service groups can contain network-service objects and explicit subnet or domain specifications. You can use network-service objects in access control list entries (ACEs) for policy-based routing, access control, and VPN filter.

Use network-service groups to define a category of applications that should be handled in the same manner. For example, you could create a single group that defines the applications whose traffic should be directed to the Internet rather than to the site-to-site VPN tunnel to the corporate hub.

There is no limit to how many applications you include in a network-service object group, either explicitly or by reference to network-service objects.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Network Services Objects/Groups**.

Step 2 Do one of the following:

- Choose **Add** > **Network Services Groups** to add a new group object. Enter a name and optionally, a description.
- Choose an existing group and click **Edit**.

Step 3 To add an existing network-service object to the group:

a) Select **Existing Network-Services Objects**.
b) Click **Add** to add the object to the group. To delete an object, select it an click **Delete**.
c) Repeat the process until the group contains all objects that you require.

Step 4 To define one or more members directly in the group:

a) Select **Create New Network-Services Object Member**.
b) Select one of the following, then fill in the appropriate address information:

- **domain**—The DNS name, up to 253 characters. This can be fully-qualified (such as www.example.com) or partial (such as example.com), in which case the object matches all subdomains, that is, servers with the partial name (such as www.example.com, www1.example.com,

long.server.name.example.com, and so forth). Connections will be matched against the longest name if an exact match is available. The domain name can resolve to multiple IP addresses.

- **subnet**—The address of a network. For IPv4 subnets, include the network address and mask, for example, 10.0.0.0 255.0.0.0. For IPv6, include the address and prefix, such as 2001:DB8:0:CD30::/60. Enter the values in the appropriate fields.

c) Select one of the following in Service Type, then fill in the appropriate fields:

- **protocol**—The protocol used in the connection, such as tcp, udp, ip, and so forth. To make the object service-agnostic, simply enter **ip**.
- **tcp** or **udp**—Enter the port number, 1-65535 or a mnemonic, such as www. For a single port, simply enter the port number. For multiple ports, you can include the number after the following operators:
  - < means any port less than the specified port number.
  - > means any port greater than the specified port number.
  - **range** means any port between the two ports specified. The first port number must be lower than the second port number.

d) Click **Add** to add the network service to the group. To delete a service, select it an click **Delete**.
e) Repeat the process until the group contains all specifications that you require.

Step 5 Click **OK**.

Configure Local User Groups

You can create local user groups for use in features that support the identity firewall by including the group in an extended ACL, which in turn can be used in an access rule, for example.

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for identity-based rules. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups.

A user can belong to local user groups and user groups imported from Active Directory.

Because you can use usernames and user group names directly in an ACL, you need to configure local user groups only if:

- You want to create a group of users defined in the LOCAL database.
- You want to create a group of users or user groups that are not captured in a single user group defined on the AD server.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Local User Groups**.

Step 2 Do one of the following:

- Choose **Add** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Add users or groups to the object using any of these methods:

- **Select existing users or groups**—Select the domain that contains the user or group, then pick the user or group name from the lists and click **Add**. For long lists, use the Find box to help locate the user. The names are pulled from the server for the selected domain.
- **Manually type user names**—You can simply type in the user or group names in the bottom edit box and click **Add**. When using this method, the selected domain name is ignored, and the default domain is used if you do not specify one. For users, the format is *domain_name**username*; for groups, there is a double \\, *domain_name**group_name*.

Step 4 After you add all the member objects, click **OK**, then click **Apply**.

You can now use this user object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

Configure Security Group Object Groups

You can create security group object groups for use in features that support Cisco TrustSec by including the group in an extended ACL, which in turn can be used in an access rule, for example.

When integrated with Cisco TrustSec, the ASA downloads security group information from the ISE. The ISE acts as an identity repository, by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping. You provision and manage security group ACLs centrally on the ISE.

However, the ASA might have localized network resources that are not defined globally that require local security groups with localized security policies. Local security groups can contain nested security groups that are downloaded from the ISE. The ASA consolidates local and central security groups.

To create local security groups on the ASA, you create a local security object group. A local security object group can contain one or more nested security object groups or Security IDs or security group names. You can also create a new Security ID or security group name that does not exist on the ASA.

You can use the security object groups you create on the ASA to control access to network resources. You can use the security object group as part of an access group or service policy.

Tip If you create a group with tags or names that are not known to the ASA, any rules that use the group will be inactive until the tags or names are resolved with ISE.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Security Group Object Groups**.

Step 2 Do one of the following:

- Choose **Add** to add a new object. Enter a name and optionally, a description.
- Choose an existing object and click **Edit**.

Step 3 Add security groups to the object using any of these methods:

- **Select existing local security group object groups**—Pick from the list of objects already defined and click **Add**. For long lists, use the Find box to help locate the object.
- **Select security groups discovered from ISE**—Pick groups from the list of existing groups and click **Add**.
- **Manually add security tags or names**—You can simply type in the tag number or security group name in the bottom edit box and click **Add**. A tag is a number from 1 to 65533 and is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB) by the ISE. Security group names are created on the ISE and provide user-friendly names for security groups. The security group table maps SGTs to security group names. Consult your ISE configuration for the valid tags and names.

Step 4 After you add all the member objects, click **OK**, then click **Apply**.

You can now use this security group object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

Configure Time Ranges

A time range object defines a specific time consisting of a start time, an end time, and optional recurring entries. You use these objects on ACL rules to provide time-based access to certain features or assets. For example, you could create an access rule that allows access to a particular server during working hours only.



Note You can include multiple periodic entries in a time range object. If a time range has both absolute and periodic values specified, then the periodic values are evaluated only after the absolute start time is reached, and they are not further evaluated after the absolute end time is reached.

Creating a time range does not restrict access to the device. This procedure defines the time range only. You must then use the object in an access control rule.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Time Ranges**.

Step 2 Do one of the following:

- Choose **Add** to add a new time range. Enter a name and optionally, a description.
- Choose an existing time range and click **Edit**.

Step 3 Choose the overall start and end time.

The default is to start now and never end, but you can set specific dates and times. The time range is inclusive of the times that you enter.

Step 4 (Optional) Configure recurring periods within the overall active time, such as the days of the week or the recurring weekly interval in which the time range will be active.

a) Click **Add**, or select an existing period and click **Edit**.

b) Do one of the following:

- Click **Specify days of the week and times on which this recurring range will be active**, and choose the days and times from the lists.
- Click **Specify a weekly interval when this recurring range will be active**, and choose the days and times from the lists.

c) Click **OK**.

Step 5 Click **OK**, and then click **Apply**.

Monitoring Objects

For network, service, and security group objects, you can analyze the usage of an individual object. From their page in the **Configuration > Firewall > Objects** folder, click the **Where Used** button.

For network objects, you can also click the Not Used button to find objects that are not used in any rules or other objects. This display gives you a short-cut for deleting these unused objects.

History for Objects

Feature Name	Platform Releases	Description
Object groups	7.0(1)	Object groups simplify ACL creation and maintenance.
Regular expressions and policy maps	7.2(1)	Regular expressions and policy maps were introduced to be used under inspection policy maps. The following commands were introduced: **class-map type regex**, **regex**, **match regex**.
Objects	8.3(1)	Object support was introduced.
User Object Groups for Identity Firewall	8.4(2)	User object groups for identity firewall were introduced.
Security Group Object Groups for Cisco TrustSec	8.4(2)	Security group object groups for Cisco TrustSec were introduced.

Feature Name	Platform Releases	Description
Mixed IPv4 and IPv6 network object groups	9.0(1)	Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses. **Note** You cannot use a mixed object group for NAT.
Extended ACL and object enhancement to filter ICMP traffic by ICMP code	9.0(1)	ICMP traffic can now be permitted/denied based on ICMP code. We introduced or modified the following screens: Configuration > Firewall > Objects > Service Objects/Groups, Configuration > Firewall > Access Rule
Service object support for Stream Control Transmission Protocol (SCTP)	9.5(2)	You can now create service objects and groups that specific SCTP ports. We modified the add/edit dialog boxes for service objects and groups on the **Configuration** > **Firewall** > **Objects** > **Service Objects/Groups** page.
Network-service objects and their use in policy-based routing and access control.	9.17(1)	You can configure network-service objects and use them in extended access control lists for use in policy-based routing route maps and access control groups. Network-service objects include IP subnet or DNS domain name specifications, and optionally protocol and port specifications, that essentially combine network and service objects. This feature also includes the ability to define trusted DNS servers, to ensure that any DNS domain name resolutions acquire IP addresses from trusted sources. We added or modified the following screens. • **Configuration** > **Device Setup** > **Routing** > **Route Maps**, Add/Edit dialog boxes. • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**, Add/Edit dialog boxes. • **Configuration** > **Firewall** > **Objects** > **Network Services Objects/Groups**. • **Configuration** > **Device Management** > **DNS** > **DNS Client**.
Network-service groups support	9.19(1)	You can now define a maximum of 1024 network service groups.