访问控制的对象

对象指配置中可重用的组件。在 ASA 配置中可以定义和使用它们来代替内联 IP 地址、服务、名称等。可以使用对象轻松维护配置，因为只需要修改某一位置的对象，便可以使该对象在引用该对象的所有其他位置显示出来。如未使用对象，必要时必须逐一修改每项功能的参数，而不是一次性修改完成。例如，如果网络对象定义了 IP 地址和子网掩码，当要更改地址时，只需要在对象定义中进行更改，而无需在引用该 IP 地址的各项功能中逐一更改。

- 对象准则，第 1 页
- 配置对象，第 2 页
- 监控对象，第 15 页
- 对象的历史记录，第 16 页

对象准则

IPv6 准则

在以下限制条件下支持 IPv6：

- 可以在网络对象组中混合 IPv4 和 IPv6 条目，但不能将混合的对象组用于 NAT。

其他准则和限制

- 由于对象和对象组共享同一命名空间，对象名称必须唯一。当可能想要创建名为“Engineering”的网络对象组以及名为“Engineering”的服务对象组时，需要在至少其中一个对象组名称的末尾添加一个标识符（或“标签”），使其名称唯一。例如，可以使用名称“Engineering_admins”和“Engineering_hosts”，使对象组名称保持唯一，同时有助于进行识别。
- 对象名称限于 64 个字符，包括字母、数字和如下字符：.!@#$%^&()-_{}。对象名称区分大小写。

配置对象

以下各节介绍如何配置主要用于访问控制的对象。

配置网络对象和组

网络对象和组可以识别 IP 地址或主机名。可以使用访问控制列表中的这些对象来简化规则。

配置网络对象

网络对象可以包含主机、网络 IP 地址、IP 地址范围或完全限定域名 (FQDN)。

也可以启用对象的 NAT 规则（FQDN 对象除外）。有关配置对象 NAT 的详细信息，请参阅网络地址转换 (NAT)。

过程

步骤 1 使用对象名称创建或编辑网络对象：**object network** *object_name*

示例：

```
hostname(config)# object network email-server
```

步骤 2 使用以下命令之一将地址添加到对象。使用命令的 **no** 形式来删除对象。

- **host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** *start_address end_address* - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。
- **fqdn** [**v4** | **v6**] *fully_qualified_domain_name* - 完全限定域名，即主机的名称，例如 www.example.com。指定 **v4** 将地址限定于 IPv4，**v6** 将地址限定于 IPv6。如果未指定地址类型，则假定为 IPv4。

示例：

```
hostname(config-network-object)# host 10.2.2.2
```

步骤 3 （可选）添加说明：**description** *string*

配置网络对象组

网络对象组可以包含多个网络对象以及内联网络或主机。网络对象组可以同时包含 IPv4 和 IPv6 地址。

但是，无法使用包含 IPv4 和 IPv6 的混合对象组进行 NAT，也无法使用包含 FQDN 对象的对象组。

过程

步骤 1 使用对象名称创建或编辑网络对象组：**object-group network** *group_name*

示例：

```
hostname(config)# object-group network admin
```

步骤 2 使用以下一个或多个命令将对象和地址添加到网络对象组。使用命令的 **no** 形式来删除对象。

- **network-object host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **network-object** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络或主机的地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **network-object object** *object_name* - 现有网络对象的名称。
- **group-object** *object_group_name* - 现有网络对象组的名称。

示例：

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

步骤 3 （可选）添加说明：**description** *string*

示例

要创建包含三个管理员 IP 地址的网络组，请输入以下命令：

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

通过输入下列命令，为来自各部门的特权用户创建网络对象组：

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

然后按下述方法对所有三个组进行嵌套：

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

配置服务对象和服务组

服务对象和组可标识协议和端口。可以使用访问控制列表中的这些对象来简化规则。

配置服务对象

服务对象可以包含单个协议规范。

过程

步骤 1 使用对象名称创建或编辑服务对象：**object service** *object_name*

示例：

```
hostname(config)# object service web
```

步骤 2 使用以下命令之一将服务添加到对象。使用命令的 **no** 形式来删除对象。

- **service** *protocol* - IP 协议的名称或编号 (0-255)。指定 **ip** 以应用于所有协议。
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] - 适用于 ICMP 或 ICMP 版本 6 消息。或者，可以按名称或编号 (0-255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择性地为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则使用所有代码。
- **service** {**tcp** | **udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*] - 适用于 TCP、UDP 或 SCTP。或者，可以指定源端口、目标端口或两者。可以按名称或编号指定端口。操作符可以是以下任意一项：

- **lt** - 小于。
- **gt** - 大于。
- **eq** - 等于。
- **neq** - 不等于。
- **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

示例：

```
hostname(config-service-object)# service tcp destination eq http
```

步骤 3 （可选）添加说明：**description** *string*

配置服务组

服务对象组包括各种协议的组合，如果需要，包括使用协议的可选源端口和目标端口以及 ICMP 类型和代码。

开始之前

可以使用通用服务对象组来建立所有服务的模型（如本节所介绍）。不过，仍然可以配置 ASA 8.3(1) 版本之前可用的服务组对象的类型。上述旧版对象包括 TCP/UDP/TCP-UDP 端口组、协议组和 ICMP 组。这些组的内容与通用服务对象组（ICMP 组除外）中的关联配置等效，因为这些组不支持 ICMP6 或 ICMP 代码。如果仍希望使用这些旧版对象，请参阅 Cisco.com 命令参考中的 **object-service** 命令说明，获取详细的使用说明。

过程

步骤 1 使用对象名称创建或编辑服务对象组：**object-group service** *object_name*

示例：

```
hostname(config)# object-group service general-services
```

步骤 2 使用以下一个或多个命令将对象和服务添加到服务对象组。使用命令的 **no** 形式来删除对象。

- **service-object** *protocol* - IP 协议的名称或编号 (0-255)。指定 **ip** 以应用于所有协议。
- **service-object** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] - 适用于 ICMP 或 ICMP 版本 6 消息。或者，可以按名称或编号 (0-255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择性地为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则使用所有代码。

- **service-object** {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator port*] [**destination** *operator port*] - 适用于 TCP、UDP 或两者或适用于 SCTP。或者，可以指定源端口、目标端口或两者。可以按名称或编号指定端口。操作符可以是以下任意一项：
  - **lt** - 小于。
  - **gt** - 大于。
  - **eq** - 等于。
  - **neq** - 不等于。
  - **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。
- **service-object object** *object_name* - 现有服务对象的名称。
- **group-object** *object_group_name* - 现有服务对象组的名称。

示例：

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

步骤 3 （可选）添加说明：**description** *string*

示例

以下示例显示如何将 TCP 和 UDP 服务添加到服务对象组：

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示如何将多个服务对象添加到服务对象组：

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
```

```
hostname(config-service-object-group)# service-object object HTTPS
```

配置网络服务对象和组

网络服务对象或组定义了一个应用。应用可以由 DNS 域名（如 example.com）、IP 子网以及协议和端口（如 TCP/80）组成。因此，网络服务对象或组可以将不同网络和服务对象的内容合并为一个对象。

您可以在扩展ACL中使用网络服务对象组，以便与路由映射（在基于策略的路由选择中）、访问控制规则和 VPN 过滤器一起使用。请注意，不能在 ACL 中直接使用网络服务对象（而不是组）：必须先将对象放入组对象中，然后才能使用组对象。

使用域名规范时，系统会使用 DNS 监听来获取 IP 地址，这些 IP 地址是在连接开始前通过用户的 DNS 请求获得的。这样可以确保在连接开始时就有一个IP地址，以便路由映射和访问控制规则从第一个数据包开始就能正确处理连接。

网络服务对象的准则

- 如果在网络服务对象中包含 DNS 域名规范，则需要进行 DNS 检测。默认情况下，DNS 检测已启用。如果使用网络服务对象，请勿禁用它。
- DNS 监听只针对 UDP DNS 数据包，不针对 TCP 或 HTTP DNS 数据包。与完全限定域名对象不同，即使不在访问列表中使用该对象，也会立即监听网络服务域名规范。
- 不能在 DNS 检测策略映射中启用 dnscrypt；它与 DNS 监听不兼容，而 DNS 监听是为网络服务对象中使用的域获取 IP 地址所必需的。任何包含域规范的网络服务对象都将无法操作，相关的访问控制条目也将无法匹配。
- 您最多可以定义1024个网络服务组。但是，身份防火墙本地用户组也共享这一限制。每定义一个网络服务组，就可以少创建 2 个用户组。
- 网络服务组的内容可以重叠，但不能创建网络服务组的完整副本。
- 如果ACL中使用了网络服务对象或组，删除该对象只需清除对象内容即可。对象本身仍在配置中定义。

配置受信任的 DNS 服务器

如果在网络服务对象中配置域名，系统就会监听 DNS 请求/响应流量，以收集 DNS 域名的 IP 地址，并缓存结果。任何 DNS 请求/响应都可以被监听。

监听的记录包括 A、AAAA 和 MX。每个已解析名称的生存时间 (TTL) 都在一定范围内：最小 TTL 为 2 分钟，最大为 24 小时。这样可以确保缓存不会过时。

出于安全考虑，可以通过定义哪些 DNS 服务器应受信任来限制 DNS 监听的范围。指向非信任 DNS 服务器的任何DNS流量都会被忽略，也不会用于获取网络服务对象的映射。默认情况下，所有已配置和已学习的 DNS 服务器都是受信任的；只有在要限制受信任列表时才需要更改。

开始之前

DNS 监听依赖于 DNS 检查，默认情况下已启用。确保没有禁用检测。此外，DSN 监听与 **dnscrypt** 功能不兼容，因此请勿在 DNS 检测策略映射中启用该命令。

过程

步骤 1 使用 **show dns trusted-source detail** 命令确定已下载到数据路径以用于网络服务对象域解析的当前受信任服务器。

默认情况下，信任任何在 DNS 组中配置的 DNS 服务器，或通过 DHCP 客户端/服务器或中继配置的 DNS 服务器。此命令显示当前设置和受信任的服务器。

示例：

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 10.163.47.11: management : N/A
    DNS Server Configured: 10.37.137.85: management : N/A
    DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
  10.37.142.73/1
  10.37.137.85/1
  10.163.47.11/1
```

步骤 2 （可选。）添加或删除显式配置的受信任DNS服务器：

dns trusted-source *ip_list*

ip_list 是应信任的 DNS 服务器 IP 地址的列表，以空格分隔。您最多可以列出 12 个 IPv4 和 IPv6 地址。指定 **any** 以涵盖所有 DNS 服务器。使用命令的 **no** 形式来删除服务器。

步骤 3 （可选。）指定是否信任 DNS 服务器组中配置的服务器。

dns trusted-source configured-servers

配置的服务器是 DNS 组或 name-server 命令中指定的任何服务器。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 4 （可选。）指定是否要信任 DHCP 池中为通过设备接口上运行的 DHCP 服务器获取地址的客户端配置的 DNS 服务器。

dns trusted-source dhcp-pools

这些是使用 **dhcpd dns** 命令配置的服务器，因此仅为 IPv4。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 5 （可选。）指定通过 DHCP 客户端和 DHCP 服务器之间的 DHCP 中继消息监听所了解到的服务器是否被视为受信任的 DNS 服务器。

dns trusted-source dhcp-relay

默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 6 （可选。）指定通过 DHCP 客户端和 DHCP 服务器之间的消息监听所了解到的服务器是否被视为受信任的 DNS 服务器。

dns trusted-source dhcp-client

该选项适用于配置 **dhcpd auto_config** 命令时，使用从通过 DHCP 客户端获取 IP 地址的设备接口上获得的信息在内部接口上配置 DHCP 服务器。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

配置网络服务对象

网络服务对象定义了一个应用。它通过子网规范或更常见的DNS域名来定义应用的位置。您也可以选择包括协议和端口，以缩小应用的范围。

只能在网络服务组对象中使用这些对象；不能在访问控制列表条目(ACE)中直接使用网络服务对象。

过程

步骤 1 使用对象名称创建或编辑网络服务对象：

object network-service *object_name* [**dynamic**]

名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。**dynamic** 关键字意味着对象不会保存到运行配置，它将仅显示在 **show object** 输出中。 **dynamic** 关键字主要供外部设备管理器使用。

示例：

```
ciscoasa(config)# object network-service webex
```

步骤 2 使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **domain** *domain_name* [*service*] - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 www.example.com）或部分名称（例如 example.com），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 www.example.com、www1.example.com、long.server.name.example.com 等）。如果存在完全匹配的名称，则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时，才指定服务。默认情况下，与已解析 IP 地址的任何连接都与对象相匹配。

protocol [*operator port*]

其中：

- *protocol* 是连接中使用的协议，例如 tcp、udp、ip 等。使用 ? 查看协议列表。
- （仅限 TCP/UDP。）*operator* 为以下选项之一：
  - **eq** 等于指定的端口号。
  - **lt** 表示小于指定端口号的任何端口。
  - **gt** 表示大于指定端口号的任何端口。
  - **range** 表示两个指定端口之间的任何端口。
- （仅限 TCP/UDP。）*port* 是端口号 1-65535 或助记符，例如 www。使用 ? 查看助记符。对于范围，必须指定两个端口，并且第一个端口号要小于第二个端口号。

步骤 3 （可选。）添加思科定义的应用 ID。

app-id *number*

该编号是思科为特定应用分配的唯一编号，范围为 1-4294967295。此命令主要供外部设备管理器使用。

步骤 4 （可选）添加说明（最多 200 个字符）：**description** *string*

示例

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

配置网络服务对象组

网络服务组可以包含网络服务对象和明确的子网或域规范。您可以在访问控制列表条目 (ACE) 中使用网络服务对象，以实现基于策略的路由选择、访问控制和 VPN 过滤。

使用 network-service groups 可定义应以相同方式处理的应用的类别。例如，您可以创建一个组，定义其流量应导向互联网而不是指向企业中心的站点间 VPN 通道的应用程序。

对于网络服务对象组中包含的应用程序数量，没有任何限制，无论是显式还是通过引用网络服务对象。

过程

步骤 1 使用组名创建或编辑网络服务对象组：

object-group network-service *group_name* [**dynamic**]

名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。**dynamic** 关键字意味着组不会保存到运行配置中，而只会显示在 show object-group 输出中。 **dynamic** 关键字主要供外部设备管理器使用。

示例：

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

步骤 2 使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **network-service-member** *object_name* - 组中包含的网络服务对象的名称。如果名称中有空格，请用双引号括起来。
- **domain** *domain_name* [*service*] - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 www.example.com）或部分名称（例如 example.com），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 www.example.com、www1.example.com、long.server.name.example.com 等）。如果存在完全匹配的名称，则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时，才指定服务。默认情况下，与已解析 IP 地址的任何连接都与对象相匹配。

protocol [*operator port*]

其中：

- *protocol* 是连接中使用的协议，例如 tcp、udp、ip 等。使用 ? 查看协议列表。
- （仅限 TCP/UDP。）*operator* 为以下选项之一：
  - **eq** 等于指定的端口号。
  - **lt** 表示小于指定端口号的任何端口。
  - **gt** 表示大于指定端口号的任何端口。
  - **range** 表示两个指定端口之间的任何端口。
- （仅限 TCP/UDP。）*port* 是端口号 1-65535 或助记符，例如 www。使用 ? 查看助记符。对于范围，必须指定两个端口，并且第一个端口号要小于第二个端口号。

步骤 3 （可选）添加说明（最多 200 个字符）：**description** *string*

示例

使用之前定义的网络服务对象配置一组 SaaS 应用。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

配置本地用户组

可以创建本地用户组，通过将组列入扩展ACL中，在支持身份防火墙的功能中使用本地用户组，进而用于访问规则等。

对于 Active Directory 域控制器中全局定义的用户组，ASA 将向 Active Directory 服务器发送 LDAP 查询。ASA为基于身份的规则导入这些组。不过，ASA可能包含未全局定义的本地化网络资源，需要使用支持本地化安全策略的本地用户组。本地用户组可包含从 Active Directory 导入的嵌套组和用户组。ASA 可整合本地组和 Active Directory 组。

用户可以属于本地用户组和从 Active Directory 导入的用户组。

由于能够在 ACL 中直接使用用户名和用户组，因此只有在以下情况下才需配置本地用户组：

- 要创建 LOCAL 数据库中定义的一组用户。
- 要创建在 AD 服务器上所定义的单一用户组中未捕获的一组用户或用户组。

过程

步骤 1 使用对象名称创建或编辑用户对象组：**object-group user** *group_name*

示例：

```
hostname(config)# object-group user admins
```

步骤 2 使用以下一个或多个命令将用户和组添加到用户对象组。使用命令的 **no** 形式来删除对象。

- **user** [*domain_NETBIOS_name*\]*username* - 用户名。如果域名或用户名中有空格，必须用引号将域名和用户名引起来。域名可以是 LOCAL（适用于本地数据库中定义的用户）或 **user-identity domain** *domain_NetBIOS_name* **aaa-server** *aaa_server_group_tag* 命令中指定的 Active Directory (AD) 域名。添加 AD 域中定义的用户时，*user_name* 必须是 Active Directory sAMAccountName（唯一），而非公用名 (cn)（可能不唯一）。如果未指定域名，则使用默认域名，即 LOCAL 或 **user-identity default-domain** 命令中定义的域名。

- **user-group** [*domain_NETBIOS_name*\\]*username* - 用户组。如果域名或组名中有空格，必须用引号将域名和组名引起来。请注意分隔域名和组名的双反斜杠 \\。
- **group-object** *object_group_name* - 现有用户对象组的名称。

示例：

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\\managers
hostname(config-user-object-group)# group-object local-admins
```

步骤 3 （可选）添加说明：**description** *string*

配置安全组对象组

例如，通过在扩展 ACL 中包含组，可以创建用于支持 Cisco TrustSec 的功能的安全组对象组，然后该组又可用于访问规则等。

将 ASA 与思科 TrustSec 集成时，ASA 可从 ISE 中下载安全组信息。ISE 可以提供思科 TrustSec 标签到用户的身份映射以及思科 TrustSec 标签到服务器的资源映射，从而充当身份储存库。可以在 ISE 上集中调配和管理安全组 ACL。

不过，ASA 可能包含未全局定义的本地化网络资源，需要使用支持本地化安全策略的本地安全组。本地安全组可以包含下载自 ISE 的嵌套安全组。ASA 可整合本地和中心安全组。

要在ASA上创建本地安全组，需要创建本地安全对象组。本地安全对象组可以包含一个或多个嵌套的安全对象组或安全 ID 或安全组名称。另外，也可以创建 ASA 上不存在的新安全 ID 或安全组名称。

可以使用您在ASA上创建的安全对象组来控制对网络资源的访问。可以将安全对象组用作访问组或服务策略的一部分。

提示 如果创建的组包含ASA未知的标签或名称，使用该组的任何规则都将处于非活动状态，直到这些标签或名称在 ISE 中得到解析。

过程

步骤 1 使用对象名称来创建或编辑安全组对象组：**object-group security** *group_name*

示例：

```
hostname(config)# object-group security mktg-sg
```

步骤 2 使用以下一个或多个命令将对象添加到服务组对象组。使用命令的 **no** 形式来删除对象。

- **security-group** {**tag** *sgt_number* | **name** *sg_name*} - 安全组标签 (SGT) 或名称。标签为一个介于 1 和 65533 之间的数字，由 ISE 通过 IEEE 802.1X 身份验证、Web 身份验证或 MAC 身份验证绕行 (MAB) 分配给设备。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。此安全组表将 SGT 映射到安全组名称。有关有效标签和名称，请查阅 ISE 配置。
- **group-object** *object_group_name* - 现有安全组对象组的名称。

示例：

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

步骤 3 （可选）添加说明：**description** *string*

配置时间范围

时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。可以将这些对象用于 ACL 规则，从而对特定功能或资产提供基于时间的访问。例如，可以创建一条仅允许在工作时间内对特定服务器进行访问的访问规则。

注释 可以在时间范围对象中列入多个定期条目。如果为时间范围规定指定了绝对值和周期值，则只有在达到绝对起始时间后才开始评估周期值，而且在绝对结束时间到达后便不再对其进行评估。

创建时间范围并不会限制对设备的访问。该操作步骤仅定义时间范围。随后必须在访问控制规则中使用该对象。

过程

步骤 1 创建时间范围：**time-range** *name*

步骤 2 （可选。）为时间范围添加起始时间或结束时间（或两者）。

absolute [**start** *time date*] [**end** *time date*]

如果未指定起始时间，则默认当前时间为起始时间。

time 采用 24 小时格式 *hh*:*mm*。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。

date 的格式为：*day month year*，例如 **1 January 2014**。

步骤 3 （可选。）添加循环时间周期。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

可以为 *days-of-the-week* 指定以下值。请注意，只有为第一个参数指定了某一天时，才可以指定一个星期中的第二天。

- **Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday** 或 **Sunday**。可以为第一个 *days-of-the-week* 参数指定上述其中多个值（用空格隔开）。
- **daily**
- **weekdays**
- **weekend**

time 采用 24 小时格式 *hh*:*mm*。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。

可以重复该命令来配置多个循环时间段。

示例

以下示例表示从 2006 年 1 月 1 日上午 8:00 开始的绝对时间范围。由于未指定结束时间和日期，因此该时间范围无限期有效。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

以下示例表示工作日从上午 8:00 到下午 6:00 的每周定期时间范围：

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

以下示例确定时间范围的结束日期，且设置从上午 8 点到下午 5 点的工作日时间段，以及星期一、星期三和星期五与星期二和星期四不同的下午 5 点之后的时间。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

监控对象

要监控对象和组，请输入以下命令：

- **show access-list**

  显示访问列表条目。包括对象的条目也会基于对象内容展开显示单个条目。

- **show running-config object** [**id** *object_id*]

显示当前所有的对象。使用 **id** 关键字按名称查看单个对象。

- **show running-config object** *object_type*

  按类型（**network** 或 **service**）显示当前对象。

- **show running-config object-group** [**id** *group_id*]

  显示当前所有的对象组。使用 **id** 关键字按名称查看单个对象组。

- **show running-config object-group** *grp_type*

  按组类型显示当前对象组。

对象的历史记录

功能名称	平台 版本	说明
对象组	7.0(1)	对象组可简化 ACL 的创建和维护。 引入或修改了以下命令：**object-group** *protocol*、**object-group** *network*、**object-group** *service*、**object-group** *icmp_type*。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令：**class-map type regex**、**regex**、**match regex**。
对象	8.3(1)	引入了对象支持功能。 引入或修改了以下命令：**object-network**、**object-service**、**object-group**network、**object-group** service、**network object**、**access-list extended**、**access-list webtype**、**access-list remark**。
用于身份防火墙的用户对象组	8.4(2)	引入了用于身份防火墙的用户对象组。 引入了以下命令：**object-network user**、**user**。
用于 Cisco TrustSec 的安全组对象组	8.4(2)	引入了用于 Cisco TrustSec 的安全组对象组 引入了以下命令：**object-network security**、**security**。
IPv4 和 IPv6 混合网络对象组	9.0(1)	以前，网络对象组只能包含所有 IPv4 地址或所有 IPv6 地址。现在，网络对象组可以同时包含 IPv4 和 IPv6 地址。 **注释** 不能使用混合对象组进行 NAT。 修改了以下命令：**object-group network**。

功能名称	平台 版本	说明
用于按ICMP代码过滤ICMP流量的扩展 ACL 和对象增强	9.0(1)	现在可以根据 ICMP 代码允许/拒绝 ICMP 流量。 引入或修改了以下命令：**access-list extended**、**service-object**、**service**。
流控制传输协议 (SCTP) 的服务对象支持	9.5(2)	现在可以创建服务对象和组合特定 SCTP 端口。 修改了以下命令： **service-object**、**service**。
网络服务对象及其在基于策略的路由和访问控制中的使用。	9.17(1)	您可以配置网络服务对象并将其用于扩展访问控制列表，以便在基于策略的路由映射和访问控制组中使用。网络服务对象包括IP子网或 DNS 域名规范，以及（可选）协议和端口规范，它们实质上结合了网络和服务对象。此功能还包括定义受信任 DNS 服务器的功能，以确保任何 DNS 域名解析都从受信任来源获取 IP 地址。 添加或修改了以下命令： **access-list extended**、 **app-id**、 **clear configure object network-service**、 **clear configure object-group network-service**、 **clear dns ip-cache**、 **clear object**、 **clear object-group**、 **debug network-service**、 **description**、 **dns trusted-source**、 **domain**、 **network-service-member**、 **network-service reload**、 **object-group network-service**、 **object network-service**、 **policy-route cost**、 **set adaptive-interface cost**、 **show asp table classify**、 **show asp table network-service**、 **show dns trusted-source**、 **show dns ip-cache**、 **show object**、 **show object-group**、 **show running-config**、 **subnet**。
网络服务组支持	9.19(1)	您现在最多可以定义 1024 个网络服务组。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。