访问控制列表

访问控制列表 (ACL) 在许多不同的功能中使用。作为访问规则应用到接口或全局应用时，这些列表可允许或拒绝通过设备的流量。对于其他功能，ACL 可选择功能所适用的流量，执行匹配服务而非控制服务。

以下各节介绍ACL的基本信息以及如何配置和监控ACL。访问规则中将更加详细地介绍访问规则、全局应用或应用到接口的 ACL。

关于 ACL

访问控制列表(ACL)通过一个或多个特征识别流量，包括源和目标IP地址、IP协议、端口、EtherType及其他参数，视 ACL 类型而定。ACL 可用于各种功能。ACL 由一个或多个访问控制条目 (ACE) 组成。

ACL 类型

ASA 使用以下类型的 ACL：

- 扩展 ACL - 扩展 ACL 是您将使用的主要类型。这些 ACL 用于访问规则以允许和拒绝通过设备的流量，并在许多功能中用于流量匹配，包括服务策略、AAA 规则、WCCP、僵尸网络流量过滤器、VPN 组和 DAP 策略。请参阅配置扩展 ACL， 第 7 页。
- EtherType ACL - EtherType ACL 仅适用于桥接组成员接口上的非 IP 第 2 层流量。可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。通过 EtherType ACL，可以控制设备上的非 IP 流量。请参阅配置 EtherType ACL， 第 18 页。

- Webtype ACL - Webtype ACL 用于过滤无客户端 SSL VPN 流量。这些 ACL 可基于 URL 或目标地址拒绝访问。请参阅配置 Webtype ACL，第 15 页。
- 标准 ACL - 标准 ACL 只能基于目标地址识别流量。使用这种 ACL 的功能较少：路由映射和 VPN 过滤器。由于 VPN 过滤器还允许扩展访问列表，限制将标准 ACL 用于路由映射。请参阅配置标准 ACL，第 14 页。

下表列出 ACL 的一些常见用途及使用的类型。

表 *1: ACL* 类型和常见用途

ACL 用途	ACL 类型	说明
控制 IP 流量的网络接入（路由和透明模式）	扩展	ASA 不允许任何流量从较低安全性接口传送到较高安全性接口，除非流量经扩展 ACL 显式许可。在路由模式下，必须使用 ACL 来允许桥接组成员接口与同一个桥接组外部接口之间的流量。 **注释** 要接入 ASA 接口执行管理访问，也无需允许主机 IP 地址的 ACL。只需根据一般操作配置指南配置管理访问即可。
识别 AAA 规则的流量	扩展	AAA 规则使用 ACL 识别流量。
为给定用户增强 IP 流量的网络接入控制	扩展，按用户从 AAA 服务器下载	可以配置 RADIUS 服务器来下载要应用于用户的动态 ACL，或者服务器可以发送 ASA 上已配置的 ACL 的名称。
VPN 访问和过滤	扩展 标准	用于远程访问和站点间 VPN 的组策略使用标准或扩展 ACL 进行过滤。远程访问 VPN 还将扩展 ACL 用于客户端防火墙配置和动态访问策略。
识别用于模块化策略框架的流量类映射的流量。	扩展	可使用 ACL 来识别类映射中的流量，该类映射用于支持模块化策略框架的功能。支持模块化策略框架的功能包括 TCP 和一般连接设置及检测。
对于桥接组成员接口，控制非 IP 流量的网络接入	EtherType	可配置 ACL，以便基于属于桥接组成员的任何接口的 EtherType 来控制流量。
识别路由过滤和重分布	标准 扩展	各种路由协议将标准 ACL 用于 IPv4 地址（扩展 ACL 用于 IPv6 地址）的路由过滤和重分布（通过路由映射）。
无客户端 SSL VPN 过滤	Webtype	可以配置 Webtype ACL 以过滤 URL 和目标。

ACL 名称

每个 ACL 都有一个名称或数字 ID，如 outside_in、OUTSIDE_IN 或 101。名称限于不超过 241 个字符。请考虑全部使用大写字母，以便在查看运行配置时更方便地查找名称。

制定一个可帮助您识别 ACL 的预期用途的命名约定。例如，ASDM 使用约定 *interface-name_purpose_direction*，如“outside_access_in”，用于在入站方向应用于“外部”接口的 ACL。

一般来说，ACL ID 为数字。标准 ACL 的范围曾为 1 - 99 或 1300 - 1999。扩展 ACL 的范围曾为 100-199 或 2000-2699。ASA 不会执行这些范围，但若要使用编号，您可能希望遵循这些规则，以便与运行 IOS 软件的路由器保持一致。

访问控制条目顺序

ACL 由一个或多个 ACE 组成。除非明确将 ACE 插入给定行，否则为给定 ACL 名称输入的每个 ACE 都将附加到 ACL 的末尾。

ACE 的顺序非常重要。当 ASA 决定转发数据包还是丢包时，ASA 会按条目的列出顺序对照每个 ACE 检测数据包。找到匹配项后，不再检查更多 ACE。

因此，如果将一条更具体的规则放在一条更通用的规则之后，则该更具体的规则可能永远不会被命中。例如，如果要允许网络 10.1.1.0/24，但要丢弃该子网上来自主机 10.1.1.15 的流量，则拒绝 10.1.1.15 的 ACE 必须排在允许 10.1.1.0/24 的 ACE 之前。如果允许 10.1.1.0/24 的 ACE 排在前面，则将允许 10.1.1.15，并且用以拒绝的 ACE 将永远不会被匹配。

在扩展 ACL 中，使用 **access-list** 命令上的 **line** *number* 参数将规则插入正确位置。使用 **show access-list** *name* 命令查看 ACL 条目及其行号以帮助确定要使用的正确行号。对于其他类型的 ACL，必须重新创建 ACL（或最好使用 ASDM）以更改 ACE 的顺序。

允许/拒绝与匹配/不匹配

访问控制条目“允许”或“拒绝”与规则匹配的流量。向用来决定允许流量通过ASA还是将其丢弃的功能应用 ACL（例如全局和接口访问规则）时，“允许”和“拒绝”是名副其实的“允许”和“拒绝”。

对于其他功能（例如服务策略规则），“允许”和“拒绝”实际上表示“匹配”或“不匹配”。在这些情况下，ACL 选择的是应接收该功能服务的流量，例如，应用检查或重定向到服务模块。“被拒绝的”流量即为不匹配 ACL 的流量，因而将不会接收该服务。

访问控制隐式拒绝

用于通过型访问规则的ACL在末尾有隐式拒绝语句。因此，对于那些应用于接口的流量控制ACL，如果未明确允许某个类型的流量，则该流量将被丢弃。例如，如果除一个或多个特定地址以外，要允许所有用户通过 ASA 访问网络，则需要拒绝这些特定地址，再允许所有其他地址。

对于控制传入流量的管理（控制平面）ACL，接口的管理规则集末尾没有隐式拒绝。而是由正则访问控制规则对任何未匹配管理访问规则的连接进行评估。

对于用于为某项服务选择流量的 ACL，必须明确“允许”流量；对于该服务，任何未“被允许的”流量都不会被匹配接受服务；“被拒绝的”流量将绕过该服务。

对于 EtherType ACL，ACL 末尾处的隐式拒绝不会影响 IP 流量或 ARP 流量；例如，如果您允许 EtherType 8037，则 ACL 末尾处的隐式拒绝此时将不阻止您先前使用扩展 ACL 允许的任何 IP 流量（或者隐式允许的从较高安全性接口流向较低安全性接口的 IP 流量）。但是，如果通过 EtherType ACE 明确拒绝所有流量，则 IP 和 ARP 流量将被拒绝；仅仍然允许物理协议流量，如自动协商。

使用 NAT 时用于扩展 ACL 的 IP 地址

使用 NAT 或 PAT 时，您将转换地址或端口，通常是在内部和外部地址之间进行映射。如果需要创建适用于已转换的地址或端口的扩展 ACL，则需要确定是要使用实际（未转换）地址或端口，还是要使用已映射地址或端口。具体要求因功能而异。

使用实际地址和端口意味着，如果 NAT 配置更改，则无需更改 ACL。

使用实际 IP 地址的功能

以下命令和功能可以在 ACL 中使用实际 IP 地址，即使接口上所示的地址是映射地址：

- 访问规则（由 **access-group** 命令引用的扩展 ACL）
- 服务策略规则（模块化策略框架 **match access-list** 命令）
- 僵尸网络流量过滤器流量分类（**dynamic-filter enable classify-list** 命令）
- AAA 规则（**aaa ... match** 命令）
- WCCP（**wccp redirect-list group-list** 命令）

例如，如果已为内部服务器 (10.1.1.5) 配置 NAT，以使该服务器在外部拥有公共可路由的 IP 地址 209.165.201.5，则用于允许外部流量访问内部服务器的访问规则需要引用该服务器的真实 IP 地址 (10.1.1.5)，而非映射地址 (209.165.201.5)。

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
hostname(config)# access-group OUTSIDE in interface outside
```

使用映射的 IP 地址的功能

以下功能使用 ACL，但是这些 ACL 使用接口上可见的映射值：

- IPsec ACL
- **capture** 命令 ACL
- 每用户 ACL
- 路由协议 ACL

- 所有其他功能 ACL。

基于时间的 ACE

可以将时间范围对象应用到扩展 ACE 和 Webtype ACE，以便规则仅在特定时期内处于活动状态。通过这些类型的规则，可以区分在一天中某些时间点可接受但在其他时间点不可接受的活动。例如，可以在工作时间内提供附加限制，而在下班后或在午餐时间则不限制。相反，基本上可以在非工作时间关闭网络。

您无法创建具有完全相同的协议、源、目标的基于时间的规则，以及不包含时间范围对象的规则服务条件。非基于时间的规则始终会覆盖重复的基于时间的规则，因为它们是冗余。

注释 用户可能会在指定结束时间后遇到约 80 至 100 秒的延迟，以使 ACL 处于非活动状态。例如，如果指定的结束时间是 3:50，因为结束时间包含在内，所以将在 3:51:00 与 3:51:59 之间的任何时间点选取命令。选取命令后，ASA 将完成当前正在运行的所有任务，然后使用该命令来停用 ACL。

访问控制列表的许可

访问控制列表不需要特殊许可证。

但是，要使用 **sctp** 作为条目中的协议，必须拥有运营商许可证。

ACL 准则

防火墙模式

- 扩展 ACL 和标准 ACL 均支持路由和透明防火墙模式。
- Webtype ACL 仅支持路由模式。
- EtherType ACL 仅支持路由和透明模式下的桥接组成员接口。

故障转移和集群

配置会话未在故障转移或集群设备间同步。在会话中进行更改时，将在故障转移和集群设备中正常地进行更改。

IPv6

- 扩展 ACL 和 Webtype ACL 允许 IPv4 和 IPv6 地址混合使用。
- 标准 ACL 不允许 IPv6 地址。

- EtherType ACL 不包含 IP 地址。

其他准则

- 指定网络掩码时，方法与思科 IOS 软件 **access-list** 命令不同。ASA 使用网络掩码（例如使用 255.255.255.0 作为 C 类掩码）。思科 IOS 掩码使用通配符位（例如 0.0.0.255）。
- （仅限扩展 ACL）以下功能使用 ACL，但无法接受带有身份防火墙（指定用户或组名称）、FQDN（完全限定域名）或思科 TrustSec 值的 ACL：
  - VPN **crypto map** 命令
  - VPN **group-policy** 命令，**vpn-filter** 除外
  - WCCP
  - DAP

配置 ACL

以下各节介绍如何配置各种类型的 ACL。请阅读有关 ACL 基本信息的章节以了解总体情况，然后阅读有关特定类型 ACL 的章节了解详细信息。

基本 ACL 配置和管理选项

ACL 由一个或多个具有相同 ACL ID 或名称的访问控制条目 (ACE) 组成。要创建新的 ACL，只需使用新的 ACL 名称创建 ACE 即可，该 ACE 将成为新 ACL 中的第一条规则。

使用 ACL 时，可执行下列操作：

检查 ACL 内容并确定行号和命中计数

使用 **show access-list** *name* 命令查看 ACL 的内容。每一行是一个 ACE，并且包括行号，如果想要将新条目插入扩展 ACL 中，则需要了解这些信息。信息还包括每个 ACE 的命中次数，即为流量匹配规则的次数。例如：

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

添加 ACE

添加 ACE 的命令为 **access-list** *name* [**line** *line-num*] *type parameters*。行号参数仅适用于扩展 ACL。如果在命令中包含行号，ACE 将插入 ACL 中的该位置，而且该位置的 ACE 及其余 ACE 将向

下移动（即，在行号处插入 ACE 不会取代该行上的旧 ACE）。如果不包含行号，ACE 将被添加到 ACL 末尾。可用参数因 ACL 类型而异；请参阅每个 ACL 类型的特定主题以了解详细信息。

向 ACL 中添加注释（除 webtype 之外的所有类型）

使用 **access-list** *name* [**line** *line-num*] **remark** *text* 命令向 ACL 中添加备注，以帮助说明 ACE 的用途。最佳实践是在 ACE 之前插入备注；如果在 ASDM 中查看配置，备注将与备注后面的 ACE 关联。可以在 ACE 之前输入多个备注以包含一个扩展注释。每条备注限制在 100 个字符以内。可以包含前导空格以帮助引出备注。如果不包含行号，备注将被添加到 ACL 末尾。例如，可以在添加每个 ACE 之前添加备注：

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

编辑或移动 ACE 或备注

无法编辑或移动 ACE 或备注。相反，必须使用所需的值在正确位置创建新的 ACE 或备注（使用行号），然后删除旧的 ACE 或备注。由于只能将 ACE 插入扩展 ACL，如果需要编辑或移动 ACE，则需要重新建立标准 ACL、Webtype ACL 或 EtherType ACL。使用 ASDM 能更容易地重新组织较长的 ACL。

删除 ACE 或备注

使用 **no access-list** *parameters* 命令删除 ACE 或备注。使用 **show access-list** 命令查看您必须输入的参数字符串：字符串必须完全匹配 ACE 或备注才能将其删除，**line** *line-num* 参数除外，该参数对于 **no access-list** 命令为可选参数。

删除整个 ACL，包括备注

使用 **clear configure access-list** *name* 命令。务必要谨慎使用该命令！该命令不会要求您进行确认。如果未包含名称，ASA 中的每个访问列表都会被删除。

重命名 ACL

使用 **access-list** *name* **rename** *new_name* 命令。

将 ACL 应用到策略

创建一个 ACL，就其本身不对流量执行任何操作。必须将 ACL 应用到策略。例如，可以使用 **access-group** 命令将扩展 ACL 应用到接口，从而拒绝或允许通过接口的流量。

配置扩展 ACL

扩展 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。扩展 ACL 是最复杂且功能丰富的一类 ACL，可以用于许多功能。扩展 ACL 最显著用途是作为访问组被全局应用或应用到接口，以确定将被拒绝或允许通过设备的流量。但是，扩展 ACL 还可用于确定要向其提供其他服务的流量。

由于扩展 ACL 非常复杂，以下各节集中描述创建 ACE 以提供特定类型的流量匹配。前几节介绍关于基于地址的基本 ACE 以及 TCP/UDP ACE 的基本信息，为其余各节提供了基础。

添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配

基本的扩展 ACE 基于源地址和目标地址（包括 IPv4 和 IPv6 地址及完全限定域名 (FQDN)，如 www.example.com）来匹配流量。事实上，每种类型的扩展 ACE 都必须包含源地址和目标地址的一些规格，因此，本主题介绍最基本的扩展 ACE。

提示　提示：若要基于 FQDN 匹配流量，必须为每个 FQDN 创建一个网络对象。

要添加 ACE 以进行 IP 地址或 FQDN 匹配，请使用以下命令：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument source_address_argument dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

示例：

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

选项有：

- *access_list_name* - 新的或现有 ACL 的名称。
- 行号 - **line** *line_number* 选项指定插入 ACE 的行号，否则 ACE 将被添加到 ACL 的末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- 协议 - *protocol_argument* 指定 IP 协议。如果使用指定协议和端口的网络服务对象，则应在此参数中指定 **ip**。
  - *name* 或 *number* - 指定协议名称或编号。指定 **ip** 以应用于所有协议。
  - **object-group** *protocol_grp_id* - 指定使用 **object-group protocol** 命令创建的协议对象组。
  - **object** *service_obj_id* - 指定使用 **object service** 命令创建的服务对象。如果需要，该对象可以包含端口或 ICMP 类型和代码规范。
  - **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。
- Source Address、Destination Address - *source_address_argument* 指定将从其发送数据包的 IP 地址或 FQDN，*dest_address_argument* 指定将向其发送数据包的 IP 地址或 FQDN：
  - **host** *ip_address* - 指定 IPv4 主机地址。
  - *ip_address mask* - 指定 IPv4 网络地址和子网掩码，例如 10.100.10.0 255.255.255.0。
  - *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。
  - **any**、**any4** 和 **any6** - **any** 指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。

- **interface** *interface_name* - 指定 ASA 接口的名称。使用接口名称（而非 IP 地址）基于接口是流量的源还是目标来匹配流量。
- **object** *nw_obj_id* - 指定使用 **object network** 命令创建的网络对象。
- **object-group** *nw_grp_id* - 指定使用 **object-group network** 命令创建的网络对象组。
- **object-group-network-service***name* - 指定网络服务对象的名称。

- Logging - **log** 参数设置 ACE 与网络访问连接匹配时的日志记录选项（使用 **access-group** 命令应用的 ACL）。如果未在 **log** 选项中输入任何参数，则将以默认间隔（300 秒）启用默认级别 (6) 的系统日志消息 106100。日志选项是：
  - *level* - 在 0 和 7 之间的严重级别。默认值为 6（信息性）。如果为活动 ACE 更改此级别，则新级别应用于新连接；现有连接继续记录在原来的级别中。
  - **interval** *secs* - 各系统日志消息之间的时间间隔（以秒为单位），从 1 到 600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。
  - **disable** - 禁用所有 ACE 日志记录。
  - **default** - 为被拒绝的数据包启用消息 106023 日志记录。此设置与不包括 **log** 选项相同。
- Time Range - **time-range** *time_range_name* 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包括时间范围，则 ACE 始终为活动状态。
- Activation - 使用 **inactive** 选项，在不删除 ACE 的情况下禁用 ACE。要重新启用 ACE，请输入完整的 ACE，无需含 inactive 关键字。

添加扩展 ACE 以执行基于端口的匹配

如果在 ACE 中指定服务对象，则服务对象可包含符合端口规范的协议，例如 TCP/80。或者，也可以直接在ACE中指定端口。对于基于端口的匹配，您可以将基于端口的协议的特定类型的流量作为匹配目标，而不是将该协议的所有流量作为匹配目标。

注释 如果使用指定协议和端口的网络服务对象，则不应按本主题所述指定端口。指定 **ip** 作为协议，以便可以匹配对象中定义的协议/端口。

如果协议为 **tcp**、**udp** 或 **sctp**，基于端口的扩展 ACE 只是基本的地址匹配 ACE。若要添加端口规范，请使用以下命令：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**] [**time-range** *time-range-name*] [**inactive**]

示例：

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument 选项指定源端口或目标端口。如果不指定端口，则与所有端口匹配。可用参数包括：

- *operator port* - *port* 可以是整数或端口名称。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**。

注释 DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC 和 Talk 都需要一个对 TCP 的定义和一个对 UDP 的定义。TACACS+ 需要一个对 TCP 上的端口 49 的定义。

- **object-group** *service_grp_id* - 指定使用 **object-group service** {**tcp** | **udp** | **tcp-udp**} 命令创建的服务对象组。请注意，建议不要再使用这些对象类型。

  无法指定建议的通用服务对象，其中协议和端口在对象内定义为端口参数。您可以将这些对象指定为协议参数的一部分，如添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页中所述。

有关其他关键字的说明以及如何使用服务对象指定协议和端口，请参阅添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页。

添加扩展 ACE 以执行基于 ICMP 的匹配

要匹配 ICMP 流量，请使用 ICMP 协议关键字之一：**icmp** 或 **icmp6**。 **icmp** 协议仅匹配 IPv4 地址，而 **icmp6** 协议仅匹配 IPv6 地址。确保网络地址与所选的协议相匹配，否则 ACE 将无法匹配任何连接。

如果在 ACE 中指定服务对象，则服务对象可包含 ICMP/ICMP6 协议 ICMP 类型和代码规格。或者，也可以直接在 ACE 中指定 ICMP 类型和代码。例如，可以将 ICMP 回应请求流量 (ping) 作为目标。

ICMP 扩展 ACE 只是基本的地址匹配 ACE，其中协议为 **icmp** 或 **icmp6**。由于这些协议具有类型和代码值，可以将类型和代码规格添加到 ACE。

要添加 ACE 以进行 IP 地址或 FQDN 匹配（其中协议为 ICMP 或 ICMP6），请使用以下命令：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} *source_address_argument dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

示例：

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

```
hostname(config)# access-list abc extended permit icmp any any echo
```

icmp_argument 选项指定 ICMP 类型和代码。

- *icmp_type* [*icmp_code*] - 按名称或编号指定 ICMP 类型，以及用于该类型的可选 ICMP 代码。如果不指定代码，则使用所有代码。
- **object-group** *icmp_grp_id*- 为使用（已弃用）**object-group icmp-type** 命令创建的 ICMP/ICMP6 指定对象组。

  无法指定建议的通用服务对象，其中协议和端口在对象内定义为 ICMP 参数。您可以将这些对象指定为协议参数的一部分，如添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页中所述。

有关其他关键字的说明，请参阅添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页。

添加扩展 ACE 执行基于用户的匹配（身份防火墙）

基于用户的扩展 ACE 只是基本的地址匹配 ACE，可以在源匹配条件中包含用户名或用户组。通过基于用户身份创建规则，可以避免将规则与静态主机或网络地址相关联。例如，如果为 user1 定义规则，且身份防火墙功能将该用户映射到某一天分配 10.100.10.3 但下一天分配 192.168.1.5 的主机，则基于用户的规则将仍然适用。

由于仍必须提供源地址和目标地址，因此请扩展源地址以包含将分配给用户（通常通过 DHCP）的可能地址。例如，无论分配什么 IP 地址，用户“LOCAL\user1 any”都将匹配 LOCAL\user1 用户，而“LOCAL\user1 10.100.1.0 255.255.255.0”仅在地址处于 10.100.1.0/24 网络上时匹配该用户。

通过使用组名称，可以基于整个类别的用户（如学生、教师、管理人员、工程师等）定义规则。

要添加 ACE 以进行用户或组匹配，请使用以下命令：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

示例：

```
hostname(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument 选项指定除源地址之外还要为其匹配流量的用户或组。可用参数包括以下各项：

- **object-group-user** *user_obj_grp_id* - 指定使用 **object-group user** 命令创建的用户对象组。
- **user** {[*domain_nickname*\]*name* | **any** | **none**} - 指定用户名。指定 **any** 以将所有用户与用户凭证匹配，或指定 **none** 以匹配未映射到用户名的地址。这些选项对于将 **access-group** 与 **aaa authentication match** 策略结合特别有用。
- **user-group** [*domain_nickname*\\]*user_group_name* - 指定用户组名称。请注意分隔域名和组名的双斜号 \\。

有关其他关键字的说明，请参阅添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页。

提示 可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。

添加扩展 ACE 执行基于安全组的匹配（思科 TrustSec）

安全组（思科 TrustSec）扩展 ACE 只是基本的地址匹配 ACE，可以在源或目标匹配条件中包含安全组或标签。通过基于安全组创建规则，可以避免将规则与静态主机或网络地址相关联。由于您仍必须提供源地址和目标地址，因此请扩展地址以包含将分配给用户（通常通过 DHCP）的可能地址。

提示 在添加这种类型的 ACE 之前，请配置思科 TrustSec。

要添加 ACE 以进行安全组匹配，请使用以下命令：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

示例：

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument 选项指定除源地址或目标地址之外还要为其匹配流量的安全组。可用参数包括以下各项：

- **object-group-security** *security_obj_grp_id* - 指定使用 **object-group security** 命令创建的安全对象组。
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} - 指定安全组名称或标签。

有关其他关键字的说明，请参阅添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配，第 8 页。

提示 可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。

扩展 ACL 的示例

以下 ACL 允许所有主机（将 ACL 应用到的接口）通过 ASA：

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下 ACL 阻止 192.168.1.0/24 上的主机访问 209.165.201.0/27 网络以获取基于 TCP 的流量。允许所有其他地址。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

如果要仅限制对选定主机的访问，则输入一个受限制的允许 ACE。默认情况下，除非明确允许，否则拒绝所有其他流量。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

以下 ACL 限制所有主机（将 ACL 应用到的接口）访问地址为 209.165.201.29 的网站。允许所有其他流量。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下使用对象组的 ACL 限制内部网络中的多台主机访问多台 Web 服务器。允许所有其他流量。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

以下示例会临时禁用允许流量从一个网络对象组 (A) 流向另一个网络对象组 (B) 的 ACL：

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

要实施基于时间的 ACE，请使用 **time-range** 命令来定义一周和一天中的特定时间。然后，使用 **access-list extended**命令将该时间范围绑定到 ACE。以下示例将“Sales”ACL 中的 ACE 绑定到名为“New_York_Minute”的时间范围。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

以下示例显示同时包含 IPv4 和 IPv6 的 ACL：

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

将地址转换为扩展 ACL 对象的示例

以下未使用对象组的正常 ACL 限制内部网络上的多台主机访问若干 Web 服务器。允许所有其他流量。

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

如果创建两个网络对象组，一个用于内部主机，另一个用于 Web 服务器，则可以简化并轻松地修改配置来添加更多主机：

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group
web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

配置标准 ACL

标准 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。标准 ACL 用于有限数量的功能，例如路由映射或 VPN 过滤器。标准 ACL 仅使用 IPv4 地址，并且仅定义目标地址。

要添加标准访问列表条目，请使用以下命令：

access-list *access_list_name* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address mask*}

示例：

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

选项有：

- 名称 - *access_list_name* 参数指定 ACL 的编号名称。标准 ACL 的传统编号是 1 - 99 或 1300 - 1999，但可以使用任意名称或编号。如果 ACL 不存在，则创建新的 ACL，否则，将条目添加到 ACL 末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- 目的地址 - **any4** 关键字与所有 IPv4 地址匹配。**host** *ip_address* 参数与主机 IPv4 地址匹配。*ip_address ip_mask* 参数与 IPv4 子网匹配，例如 10.1.1.0 255.255.255.0。

配置 Webtype ACL

Webtype ACL 用于过滤无客户端 SSL VPN 流量，限制用户对特定网络、子网、主机和 Web 服务器的访问。如果不定义过滤器，将允许所有连接。Webtype ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。

通过 Webtype ACL，可以基于 URL 或目标地址来匹配流量。单个 ACE 不能混用这些规格。以下各节介绍每种类型的 ACE。

添加 Webtype ACE 以执行 URL 匹配

要基于用户正尝试访问的 URL 匹配流量，请使用以下命令：

access-list *access_list_name* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*] [**inactive**]

示例：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

选项有：

- *access_list_name* - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- URL - 关键字 **url** 指定要匹配的 URL。使用 **url any** 与所有基于 URL 的流量匹配。否则，请输入 URL 字符串，它可以包括通配符。以下是指定 URL 时的一些提示和限制：
  - 指定 **any** 将匹配所有 URL。
  - “Permit url any”会允许具有格式 protocol://server-ip/path 的所有 URL，并会阻止与此模式不匹配的流量，例如端口转发。应该有一个 ACE 允许连接至所需端口（如果是 Citrix，为端口 1494），从而避免发生隐式拒绝。
  - 具有“permit url any”的 ACL 不影响智能隧道和 ICA 插件，因为它们仅与 smart-tunnel:// 和 ica:// 类型匹配。
  - 可以使用这些协议：cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel:// 和 smtp://。也可以在协议中使用通配符；例如，htt* 与 http 和 https

匹配，星号（*）与所有协议匹配。例如，*://*.example.com 与传输到 example.com 网络的基于 URL 的任何类型的流量匹配。

- 如果指定 smart-tunnel:// URL，则可以仅包括服务器名称。URL 无法包含路径。例如，smart-tunnel://www.example.com 可接受，但是不接受 smart-tunnel://www.example.com/index.html。
- 星号（*）与零个字符或任何数量的字符匹配。要与任何 http URL 匹配，请输入 http://*/*。
- 问号（?）完全匹配任意字符。
- 方括号（[]）是范围运算符，与范围中的任何字符匹配。例如，要与 http://www.cisco.com:80/ 和 http://www.cisco.com:81/ 匹配，请输入 **http://www.cisco.com:8[01]/**。

- Logging - **log** 参数可设置当 ACE 匹配数据包时的日志记录选项。如果未在 **log** 选项中输入任何参数，则将以默认间隔（300 秒）启用默认级别 (6) 的系统日志消息 106102。日志选项是：
  - *level* - 在 0 和 7 之间的严重级别。默认值为 6。
  - **interval** *secs* - 各系统日志消息之间的时间间隔（以秒为单位），从 1 到 600。默认值为 300。
  - **disable** - 禁用所有 ACL 日志记录。
  - **default** - 对消息 106103 启用日志记录。此设置与不包括 **log** 选项相同。
- Time Range - **time-range** *time_range_name* 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包括时间范围，则 ACE 始终为活动状态。
- Activation - 使用 **inactive** 选项，在不删除 ACE 的情况下禁用 ACE。要重新启用 ACE，请输入完整的 ACE，无需含 inactive 关键字。

添加 Webtype ACE 以执行 IP 地址匹配

可以基于用户正尝试访问的目标地址来匹配流量。除了 URL 规格之外，Webtype ACL 可以同时包含 IPv4 和 IPv6 地址。

要添加 Webtype ACE 以进行 IP 地址匹配，请使用以下命令：

access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *time_range_name*]] [**inactive**]]

示例：

```
hostname(config)# access-list acl_company webtype permit tcp any
```

有关此处未说明的关键字的说明，请参阅添加 Webtype ACE 以执行 URL 匹配，第 15 页。此类型 ACE 的特定关键字和参数包括以下各项：

- **tcp** - TCP 协议。Webtype ACL 仅匹配 TCP 流量。
- Destination Address - *dest_address_argument* 指定将向其发送数据包的 IP 地址。

- **host** *ip_address* - 指定 IPv4 主机地址。
- *dest_ip_address mask* - 指定 IPv4 网络地址和子网掩码，例如 10.100.10.0 255.255.255.0。
- *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。
- **any**、**any4** 和 **any6** - **any** 指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。

- *operator port* - 目标端口。如果不指定端口，则与所有端口匹配。*port* 可以是表示 TCP 端口号的整数或端口名称。*operator* 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**。

Webtype ACL 的示例

以下示例展示如何拒绝对特定公司 URL 的访问：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

以下示例显示如何 拒绝对特定网页的访问：

```
hostname(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

以下示例显示如何 拒绝通过端口 8080 对特定服务器上任何 URL 的 HTTP 访问：

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

以下示例显示如何 在 webtype ACL 中使用通配符。

- 以下示例匹配 http://www.example.com/layouts/1033 等 URL：

  ```
  access-list VPN-Group webtype permit url http://www.example.com/*
  ```

- 以下示例匹配 http://www.example.com/ 和 http://www.example.net/ 等 URL：

  ```
  access-list test webtype permit url http://www.example.*
  ```

- 以下示例匹配 http://www.example.com 和 ftp://wwz.example.com 等 URL：

```
access-list test webtype permit url *://ww?.e*co*/
```

- 以下示例匹配 http://www.cisco.com:80 和 https://www.cisco.com:81 等 URL：

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上一个示例中的范围操作符“[]”指定在该位置可能出现 **0** 或 **1**。

- 以下示例匹配 http://www.example.com 和 http://www.example.net 等 URL：

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

上一个示例中的范围操作符“[]”指定该范围（从 **a** 到 **z**）内的任何字符都可能出现。

- 以下示例匹配文件名或路径中包含“cgi”的 http 或 https URL。

```
access-list test webtype permit url htt*://*/*cgi?*
```

注释 要匹配任意 http URL，必须输入 **http://*/***，而非 http://*。

以下示例显示如何强制 Webtype ACL 禁用对特定 CIFS 共享的访问。

在此场景中，我们有一个包含名为“Marketing_Reports”和“Sales_Reports”的两个子文件夹的“shares”根文件夹。我们希望明确拒绝访问“shares/Marketing_Reports”文件夹。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

但是，由于 ACL 末尾的隐式“deny all”，上述 ACL 使所有子文件夹 变得都不可访问（“shares/Sales_Reports”和“shares/Marketing_Reports”），包括 根文件夹（“shares”）。

要解决此问题，请添加一个新的 ACL 来 允许访问根文件夹和其余的子文件夹：

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

配置 EtherType ACL

EtherType ACL 适用于桥接组成员接口上的非 IP 第 2 层流量。可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。使用 EtherType ACL，可以控制非 IP 流量跨桥接组的流动。请注意，802.3 格式的帧不是由 ACL 处理，因为这些帧使用的是长度字段，而非类型字段。

要添加 EtherType ACE，请使用以下命令：

access-list *access_list_name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-multicast** | **mpls-unicast** | *hex_number*}

示例：

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

选项有：

- *access_list_name* - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝数据包。如果条件匹配，**permit** 关键字可允许数据包。
- Traffic Matching Criteria - 可以使用以下选项匹配流量：
  - **any**- 匹配所有第 2 层流量。
  - **bpdu**- 默认允许的桥接协议数据单元 (dsap 0x42)。此关键字将转换为 **dsap bpdu**。
  - **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} - IEEE 802.2 逻辑链路控制 (LLC) 数据包的目的服务无线接入点地址。包括要允许或拒绝的十六进制格式地址，范围介于 0x01 到 0xff 之间。也可以使用以下关键字来为通用值创建规则：
    - **bpdu** 对于 0x42，桥接协议数据单元。
    - **ipx** 对于 0xe0，互联网数据包交换 (IPX) 802.2 LLC。
    - **isis** 对于 0xfe，中间系统到中间系统 (IS-IS)。
    - **raw-ipx** 对于 0xff，原始 IPX 802.3 格式。
  - **eii-ipx**- 以太网 II IPX 格式，EtherType 0x8137。
  - **ipx**- 互联网数据包交换 (IPX)。此关键字是为 **dsap ipx**、**dsap raw-ipx** 和 **eii-ipx** 配置三条单独规则的快捷方式。
  - **isis**- 中间系统到中间系统 (IS-IS)。此关键字将转换为 **dsap isis**。
  - **mpls-multicast**- MPLS 组播。
  - **mpls-unicast**- MPLS 单播。
  - *hex_number* - 16 位十六进制数字（0x600 到 0xffff）可识别的任何 EtherType。请参阅 http://www.ietf.org/rfc/rfc1700.txt 上的 RFC 1700“分配的编号”，以获取 EtherType 列表。

EtherType ACL 的示例

以下示例显示如何配置 EtherType ACL，包括如何将 ACL 应用到接口。

例如，以下示例 ACL 允许源自内部接口的常见 EtherType 流量：

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
```

```
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

以下示例通过 ASA 允许一些 EtherType，但会拒绝所有其他 EtherType：

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

以下示例将拒绝 EtherType 0x1256 的流量，但允许两个接口上的所有其他流量：

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

在隔离配置会话中编辑 ACL

在编辑用于访问规则或任何其他用途的ACL时，更改会立即实施并影响流量。通过访问规则，可以启用事务性提交模型，以确保新规则仅在规则编译完成后变为活动状态，但编译发生在编辑的每个 ACE 之后。

如果想进一步隔离编辑 ACL 的影响，可在“configuration session”中进行更改，这是一种独立模式，在该模式下允许在明确提交更改前编辑多个ACE和对象，这样可确保更改设备行为前完成预期的所有更改。

开始之前

- 可以编辑由 access-group 命令引用的 ACL，但无法编辑由任何其他命令引用的 ACL。也可以编辑未引用的 ACL 或创建新的 ACL。
- 可以创建或编辑对象和对象组，但如果在会话中创建一个对象或对象组，则无法在同一会话中进行编辑。如果对象未按预期方式定义，则必须提交更改，然后编辑对象，或丢弃整个会话并重新开始。
- 编辑由 access-group 命令（访问规则）引用的 ACL 时，在提交会话时使用事务性提交模型。因此，ACL 将在新的 ACL 替换旧版本之前被完全编译。

过程

步骤 1 启动会话。

```
hostname#configure session session_name
hostname(config-s)#
```

如果 *session_name* 已存在，将打开该会话。否则，将创建一个新的会话。

使用 **show configuration session** 命令查看现有会话。一次最多可让 3 个会话处于活动状态。如果需要删除旧的未使用的会话，请使用 **clear configuration session** *session_name* 命令。

如果因为现有会话正在别处进行编辑而无法打开，则可以清除指示会话正在进行编辑的标记。该操作仅在确定会话实际上并未进行编辑时执行。使用 **clear session** *session_name* **access** 命令重置标记。

步骤 2 （仅限未提交的会话。）进行更改。可以将以下基本命令与其任一参数配合使用：

- **access-list**
- **object**
- **object-group**

步骤 3 决定如何处理会话。可用的命令取决于之前是否已提交会话。可能的命令如下：

- **exit** - 简单地退出会话而不提交或放弃更改，以便稍后返回。
- **commit** [**noconfirm** [**revert-save** | **config-save**]] -（仅限未提交的会话。）可提交更改。系统将询问您是否要保存会话。可以保存复原会话 (**revert-save**)，其可以让您使用 **revert** 命令撤消更改，或者可以保存配置会话 (**config-save**)，其包括在会话中所做的所有更改（允许您根据需要重新提交相同的更改）。如果保存复原或配置会话，将提交更改，但会话保持活动状态。可以打开会话，复原或重新提交更改。可以通过选中 **noconfirm** 选项（也可同时选中所需的保存选项）避免提示。
- **abort** -（仅限未提交的会话。）可放弃更改并删除会话。如果要保持会话，请退出会话并使用 **clear session** *session_name* **configuration** 命令，该命令清空会话而不删除会话。
- **revert** -（仅限已提交的会话。）取消所做更改，将配置返回到提交会话前的状态并删除会话。
- **show configuration session** [*session_name*] - 可显示会话中所做的更改。

监控 ACL

要监控 ACL，请输入以下其中一个命令：

- **show access-list** [*name*] - 显示访问列表，包括每个 ACE 的行号和匹配数。纳入 ACL 名称，否则将看到所有访问列表。
- **show running-config access-list** [*name*] - 显示当前运行的访问列表配置。纳入 ACL 名称，否则将看到所有访问列表。

ACL 的历史记录

功能名称	版本	说明
扩展 ACL、标准 ACL、Webtype ACL	7.0(1)	将 ACL 用于控制网络接入或指定供许多功能操作的流量。扩展访问控制列表用于通过设备的访问控制和其他几种功能。标准 ACL 用于路由映射和 VPN 过滤器。Webtype ACL 用于无客户端 SSL VPN 过滤。EtherType ACL 控制第 2 层非 IP 流量。 引入了以下命令：**access-list extended**、**access-list standard**、**access-list webtype** 和 **access-list ethertype**。
扩展 ACL 中的实际 IP 地址	8.3(1)	使用 NAT 或 PAT 时，对于几种功能，ACL 中不再使用映射地址和端口。必须为这些功能使用实际、未转换的地址和端口。使用实际地址和端口意味着，如果NAT配置更改，则无需更改ACL。
支持在扩展 ACL 中使用身份防火墙	8.4(2)	现在可以将身份防火墙用户和组用于源和目标。可以将身份防火墙 ACL 与访问规则、AAA 规则配合使用，并可将其用于 VPN 身份验证。 修改了以下命令：**access-list extended**。
IS-IS 流量的 EtherType ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式下，ASA 现在可使用 EtherType ACL 控制 IS-IS 流量。 修改了以下命令：**access-list ethertype** {**permit** | **deny**} **isis**。
支持在扩展ACL中使用思科TrustSec	9.0(1)	现在可以将思科 TrustSec 安全组用于源和目标。可以将身份防火墙 ACL 与访问规则配合使用。 修改了以下命令：**access-list extended**。
为 IPv4 和 IPv6 统一扩展 ACL 和 Webtype ACL	9.0(1)	扩展 ACL 和 Webtype ACL 现在支持 IPv4 和 IPv6 地址。甚至可以为源和目标同时指定 IPv4 和 IPv6 地址。更改了 **any** 关键字以表示 IPv4 和 IPv6 流量。添加了 **any4** 和 **any6** 关键字以分别表示纯 IPv4 和纯 IPv6 流量。特定于 IPv6 的 ACL 已弃用。现有 IPv6 ACL 已迁移到扩展 ACL。有关迁移的详细信息，请参阅版本说明。 修改了以下命令： **access-list extended**、**access-list webtype**。 删除了以下命令：**ipv6 access-list**、**ipv6 access-list webtype** 和 **ipv6-vpn-filter**。
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**。

功能名称	版本	说明
用于编辑 ACL 和对象的配置会话。 向前引用访问规则中的对象和ACL。	9.3(2)	现在，可以在单独的配置会话中编辑 ACL 和对象。还可以向前引用对象和 ACL，也就是说，可以为尚未存在的对象或 ACL 配置规则和访问组。 引入了 **clear configuration session**、**clear session**、**configure session**、**forward-reference** 和 **show configuration session** 命令。
流控制传输协议 (SCTP) 的 ACL 支持	9.5(2)	现在，您可以使用 **sctp** 协议（包括端口规范）创建 ACL 规则。 修改了以下命令：**access-list extended** 。
对 IEEE 802.2 逻辑链路控制数据包的目标服务无线接入点地址的 Ethertype 规则支持。	9.6(2)	现在，您可以为 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址编写 Ethertype 访问控制规则。添加此支持后，**bpdu** 关键字与预期流量不再匹配。我们重写了 **dsap 0x42** 的 **bpdu** 规则。 修改了以下命令：**access-list ethertype**
在路由模式下，桥接组成员接口上支持 Ethertype 规则，桥接组虚拟接口 (BVI) 上支持扩展访问规则。	9.7(1)	现在，您可以创建 Ethertype ACL，并在路由模式下将它们应用于桥接组成员接口。除成员接口之外，您还可以向桥接虚拟接口 (BVI) 应用扩展访问规则。 修改了以下命令： **access-group**、**access-list ethertype** 。
EtherType 访问控制列表更改。	9.9(1)	EtherType 访问控制列表现在支持以太网 II IPX (EII IPX)。此外，在 DSAP 关键字中增加了新关键字，以支持通用 DSAP 值：BPDU (0x42)、IPX (0xE0)、Raw IPX (0xFF) 和 ISIS (0xFE)。因此，现有的使用 BPDU 或 ISIS 关键字的 EtherType 访问控制条目将被自动转换为使用 DSAP 规范，并且 IPX 的规则将被转换为 3 条规则（DSAP IPX、DSAP Raw IPX 和 EII IPX）。此外，使用 IPX 作为 EtherType 值的数据包捕获已被弃用，因为 IPX 对应于 3 个单独的 EtherType。 修改了以下命令：**access-list ethertype** 添加了新的关键字 **eii-ipx** 和 **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}；**capture ethernet-type** 不再支持关键字 **ipx**。
支持扩展 ACL 中的网络服务对象。	9.17(1)	您可以在扩展 ACL 和访问控制规则中使用网络服务对象作为源和目标条件。 我们更改了以下命令：**access-list extended**。

功能名称	版本	说明
始终启用 ACL 和对象的转发引用。此外，默认情况下，为访问控制启用对象组搜索。	9.18(1)	在配置访问组或访问规则时，可以引用尚不存在的 ACL 或网络对象。 此外，默认情况下，为 新 部署的访问控制启用对象组搜索。升级设备将继续禁用此命令。如果要启用它（推荐），必须手动执行此操作。 我们删除了 **forward-reference enable** 命令，并将 **object-group-search access-control** 的默认设置更改为启用。

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。