访问规则

本章介绍如何使用访问规则控制通过或流向ASA的网络访问。在路由和透明防火墙模式下均可使用访问规则控制网络访问。在透明模式下，可同时使用访问规则（适用于第 3 层流量）和 EtherType 规则（适用于第 2 层流量）。

注释 要访问 ASA 接口进行访问管理，亦无需允许主机 IP 地址的 访问规则。只需根据一般操作配置指南配置管理访问即可。

控制网络访问

访问规则决定允许哪些流量通过 ASA。有多个不同的规则层，这些规则层共同实施访问控制策略：

- 分配至接口的扩展访问规则（第 3+ 层流量）- 可于入站和出站方向应用单独的规则集 (ACL)。扩展访问规则根据源和目标流量条件允许或拒绝流量。
- 分配至桥接虚拟接口（BVI、路由模式）的扩展访问规则（第 3+ 层流量）- 如果命名了 BVI，可以在入站和出站方向应用单独的规则集，也可以向桥接组成员接口应用规则集。当 BVI 和成员接口都有访问规则时，处理顺序取决于方向。入站时，首先评估成员访问规则，然后是 BVI 访问规则。出站时，首先考虑 BVI 规则，然后是成员接口规则。
- 全局分配的扩展访问规则 - 可创建用作默认访问控制的单个全局规则集。全局规则在接口规则之后应用。

- 管理访问规则（第 3+ 层流量）- 可应用单个规则集以覆盖接口处定向的流量，这通常是管理流量。在 CLI 中，这些是“控制平面”访问组。对于在设备处定向的 ICMP 流量，也可配置 ICMP 规则。
- 分配至接口（仅限桥接组成员接口）的 EtherType 规则（第 2 层流量）- 可以在入站和出站方向应用单独的规则集。EtherType 规则控制针对非 IP 流量的网络访问。EtherType 规则根据 EtherType 允许或拒绝流量。此外，还可以对桥接组成员接口应用扩展访问规则来控制第 3+ 层流量。

一般规则信息

以下主题提供有关访问规则和 EtherType 规则的一般信息。

接口访问规则和全局访问规则

可将访问规则应用于特定接口，也可将访问规则全局应用于所有接口。可结合接口访问规则配置全局访问规则，在此情况下，特定入站接口访问规则始终在通用全局访问规则之前得以处理。全局访问规则仅适用于入站流量。

入站和出站规则

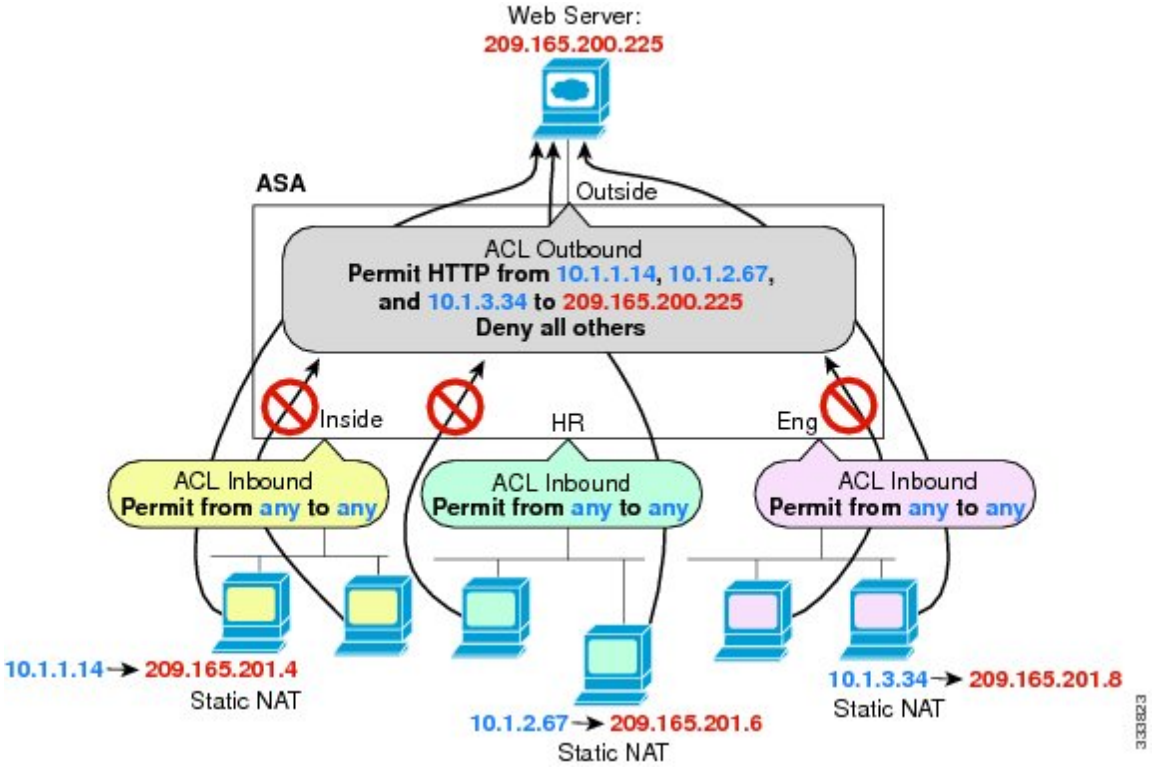
可根据流量的方向配置访问规则：

- 入站 - 入站访问规则在流量进入接口时应用于流量。全局访问规则和管理访问规则始终为入站规则。
- 出站 - 出站规则在流量离开接口时应用于流量。

注释 “入站”和“出站”指在接口上对通过接口进入 ASA 或离开 ASA 的流量应用 ACL。这些术语不是指流量从较低安全性接口至较高安全性接口的移动（通常称为入站），或者流量从较高安全性接口至较低安全性接口的移动（通常称为出站）。

出站 ACL 非常有用，例如，如果您想要仅允许内部网络上的某些主机访问外部网络上的某个网络服务器，可创建仅允许指定主机的单个出站 ACL，而不是创建多个入站 ACL 以限制访问。（请参阅下图。）出站 ACL 会阻止任何其他主机到达外部网络。

图 *1:* 出站 ***ACL***



请见以下适用于本示例的命令：

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225
 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225
 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225
 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

规则顺序

规则顺序非常重要。当 ASA 决定转发数据包还是丢弃数据包时，ASA 会按适用 ACL 中列出规则的顺序对照每个规则检测数据包。发现某个匹配后，将不再检查其他规则。例如，如在起始处创建的访问规则显式允许某接口的所有流量，系统将不检查更多的规则。

隐式允许

默认情况下，允许从较高安全性接口流向较低安全性接口的单播 IPv4 和 IPv6 流量。其中，包括路由模式下标准路由接口与桥接虚拟接口 (BVI) 之间的流量。

对于桥接组成员接口，这种从较高安全性接口到较低安全性接口之间的隐式允许仅适用于同一桥接组内的接口。桥接组成员接口与路由接口或不同桥接组的成员之间不存在隐式允许。

默认情况下，桥接组成员接口（路由或透明模式）还允许以下流量：

- 两个方向上的 ARP 流量。（可使用 ARP 检测控制 ARP 流量，但不能通过访问规则控制该流量。）
- 两个方向上的 BPDU 流量。（您可以使用 Ethertype 规则控制这些流量。）

对于其他流量，需要使用扩展访问规则（IPv4 和 IPv6）或 EtherType 规则（非 IP）。

隐式拒绝

ACL 列表的末尾有隐式拒绝，因此，除非您显式允许流量，否则流量无法通过。例如，如果除特定地址以外，要允许其他所有用户通过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 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）。然而，如果您使用EtherType规则显式拒绝所有流量，则将拒绝 IP 和 ARP 流量，仅物理协议流量（如自动协商流量）仍得以允许。

如果配置全局访问规则，则全局规则之后的隐式拒绝得以处理。请参阅以下操作顺序：

1. 接口访问规则。
2. 对于网桥组成员接口，网桥虚拟接口 (BVI) 访问规则。
3. 全局访问规则。
4. 隐式拒绝。

NAT 和访问规则

在确定访问规则匹配时，访问规则始终将使用真实IP地址，即使您已配置NAT。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)。

相同安全级别的接口和访问规则

每个接口都有一个安全级别，在考虑访问规则之前要进行安全级别检查。因此，即使您在访问规则中允许某个连接，它也可能因接口级的同一安全级别检查而被阻止。您可能需要确保您的配置允许相同安全级别的连接，以便在做出允许/拒绝决定时始终考虑您的访问规则。

- 相同安全级别的入口和出口接口之间的连接要接受相同安全流量接口间检查。

  要允许这些连接，请输入 **same-security-traffic permit inter-interface** 命令。

  要允许这些连接，依次选择**配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)**，然后选择**启用两个或多个配置了相同安全级别的接口之间的流量**

(Enable traffic between two or more interfaces which are configured with the same security levels) 选项。

- 具有相同入口和出口接口的连接要接受相同安全流量的接口间检查。

  要允许这些连接，请输入 **same-security-traffic permit intra-interface** 命令。

  要允许这些连接，依次选择**配置 (Configuration)** > **设备设置 (Device Setup)** > **接口设置 (Interface Settings)** > **接口 (Interfaces)**，然后选择**启用连接到同一接口的两台或多台主机之间的流量 (Enable traffic between two or more hosts connected to the same interface)** 选项。

扩展访问规则

本节介绍有关扩展访问规则的信息。

用于返回流量的扩展访问规则

对于路由和透明模式下的 TCP、UDP 和 SCTP 连接，ASA 允许建立的双向连接的所有返回流量，无需使用访问规则来允许返回流量。

不过，对于 ICMP 等无连接协议，ASA 会建立单向会话，所以您需要使用访问规则来允许两个方向的 ICMP（通过向源接口和目标接口应用 ACL），或者需要启用 ICMP 检测引擎。ICMP 检测引擎将 ICMP 会话视为双向连接。例如，要控制 ping 操作，请指定 **echo-reply (0)**（ASA 到主机）或 **echo (8)**（主机到 ASA）。

允许广播和组播流量

在路由防火墙模式下，即便访问规则（包括不支持的动态路由协议和 DHCP）中允许广播和组播流量，它们也会受到阻拦。必须配置动态路由协议或 DHCP 中继，才能允许这些流量。

对于在透明或路由防火墙模式下属于同一桥接组成员的接口，可以使用访问规则允许任何 IP 流量通过。

注释 由于这些特殊类型的流量无传输连接，所以需要向入站和出站接口应用访问规则，才能允许返回流量通过。

下表列出了在同一桥接组成员的接口之间可使用访问规则允许的常见流量类型。

表 *1:* 在同一个桥接组成员之间应用访问规则的特殊流量

流量类型	协议或端口	说明
DHCP	UDP 端口 67 和 68	如果启用 DHCP 服务器，则 ASA 不会传送 DHCP 数据包。
EIGRP	协议 88	—
OSPF	协议 89	—

流量类型	协议或端口	说明
组播流	UDP 端口因应用而异。	组播流始终以 D 类地址为目标（224.0.0.0 至 239.x.x.x）。
RIP（v1 或 v2）	UDP 端口 520	—

管理访问规则

您可以配置访问规则来控制流向 ASA 的管理流量。传入管理流量的访问控制规则（由 **http**、**ssh** 或 **telnet** 等命令定义）的优先级高于使用 **control-plane** 选项应用的管理访问规则。因此，系统允许此类允许的管理流量传入，即使被所有传入 ACL 明确拒绝。

与正则访问规则不同，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。

或者，可使用 ICMP 规则控制流向设备的 ICMP 流量。使用正则扩展访问规则可控制通过设备的 ICMP 流量。

EtherType 规则

本节介绍 EtherType 规则。

支持的 EtherType 和其他流量

EtherType 规则控制以下方面：

- 一个 16 位十六进制数字标识的 EtherType，包括常见类型 IPX 和 MPLS 单播或组播。
- 以太网 V2 帧。
- 默认情况下允许的 BPDU。BPDU 采用 SNAP 封装，ASA 专用于处理 BPDU。
- 中继端口（思科专有）BPDU。中继 BPDU 在负载内包含 VLAN 信息，因此，如果允许 BPDU，ASA 将使用出站 VLAN 修改负载。
- 中间系统到中间系统 (IS-IS)。
- IEEE 802.2 逻辑链路控制数据包。可以根据目标服务无线接入点地址来控制访问。

不支持以下类型的流量：

- 802.3 格式化帧 - 规则将不处理这些帧，因为它们使用长度字段而不是类型字段。

返回流量的 EtherType 规则

因为 EtherType 是无连接的，所以，如果想要在两个方向上允许流量通过，则需要在两个接口上都应用规则。

允许 MPLS

如果允许MPLS，请确保已通过ASA建立标签分发协议和标记分发协议TCP连接，方法是将两个连接到 ASA 的 MPLS 路由器配置为使用 ASA 接口上的 IP 地址作为 LDP 或 TDP 会话的路由器 ID。（LDP 和 TDP 允许 MPLS 路由器协商用于转发数据包的标签（地址）。）

在思科 IOS 路由器上，输入协议、LDP 或 TDP 的相应命令。*interface* 为连接到 ASA 的接口。

mpls ldp router-id *interface* **force**

或

tag-switching tdp router-id *interface* **force**

面向访问规则的许可

访问控制规则无需专用许可证。

但是，要使用 **sctp** 作为规则中的协议，您必须拥有运营商许可证。

访问控制准则

IPv6 准则

支持 IPv6。源和目标地址可能包括 IPv4 和 IPv6 地址的任意混合。

每用户 ACL 准则

- 每用户 ACL 使用 **timeout uauth** 命令中的值，但该值可被 AAA 每用户会话超时值覆盖。
- 如果由于每用户 ACL 而拒绝流量，则将记录系统日志消息 109025。如果允许流量，则将不生成系统日志消息。每用户 ACL 中的 **log** 选项将不产生影响。

其他准则和限制

- 随着时间的推移，访问规则列表可能会增长到包含许多过时的规则。最终，访问组的ACL可能会非常大，以至于影响整体系统性能。如果您发现系统在发送系统日志消息、进行故障转移同步通信、建立和维护 SSH/HTTPS 管理访问连接等方面遇到问题，可能需要修剪访问规则。通常，您应主动维护规则列表，以删除过时的规则、永远不会命中的规则、无法再解析的 FQDN 对象等。另请考虑实施对象组搜索。
- 新部署默认启用对象组搜索。

  通过启用对象组搜索可降低搜索访问规则所需的内存，但此规则会影响查询性能及增加CPU使用量。已启用的对象组搜索不会展开网络或服务对象，而是根据这些组定义搜索匹配的访问规则。可以使用 **object-group-search access-control** 命令设置此选项。

可以使用 **object-group-search threshold** 命令启用阈值，以有助于防止性能下降。使用阈值运行时，对于每个连接，将根据网络对象匹配源和目标 IP 地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。配置规则以防止过多的匹配项。

注释 对象组搜索仅适用于网络和服务对象。它不适用于安全组或用户对象。如果 ACL 包括安全组，请勿启用此功能。结果可能是非活动的 ACL 或其他意外行为。

- 可使用访问组的事务提交模型，从而提高系统性能和可靠性。但是，如果使用 FQDN 对象来处理解析经常变化的主机名，则不建议使用事务提交，因为访问组编译可能永远无法完全解析。有关详细信息，请参阅常规操作配置指南中的基本设置章节。使用 **asp rule-engine transactional-commit access-group** 命令。
- 在 ASDM 中，规则描述基于出现在 ACL 中规则之前的访问列表注释，对于在 ASDM 中创建的新规则，任何描述均将配置为相关规则之前的注释。然而，ASDM 中的数据包跟踪器匹配在 CLI 中在匹配规则之后配置的注释。
- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须配置适用于数据接口的 DNS。

  请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

  - 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的内部 DNS 服务器。
  - 有些 FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

    建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备 DNS 缓存中已解析和可用地址的可能性很低。
  - 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的 DNS 服务器与您所配置的不同，基于 FQDN 的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
  - 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。

配置访问控制

以下主题解释如何配置访问控制。

配置访问组

应先创建 ACL，然后才能创建访问组。

要将 ACL 绑定至接口，或将其全局应用，请使用以下命令：

access-group *access_list* { {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global**}

对接口特定的访问组：

- 指定扩展或 EtherType ACL 名称。可为每个 ACL 类型、每个接口、每个方向配置一个 **access-group** 命令，并配置一个控制平面 ACL。控制平面 ACL 必须是扩展 ACL。Ethertype ACL 仅可用于网桥组成员接口。对于路由模式下的网桥组，可为网桥虚拟接口 (BVI) 和每个网桥组成员接口上的每个方向指定扩展 ACL。
- **in** 关键字会将 ACL 应用于入站流量。 **out** 关键字会将 ACL 应用于出站流量。
- 指定 **interface** 名称。
- Per-user-override 关键字（仅适用于入站扩展 ACL）允许为用户授权下载的动态用户 ACL 覆盖分配给该接口的 ACL。例如，如果接口 ACL 拒绝来自 10.0.0.0 的所有流量，但动态 ACL 允许来自 10.0.0.0 的所有流量，则动态 ACL 将覆盖该用户的接口 ACL。

  默认情况下，将不针对接口 ACL 匹配 VPN 远程访问流量。但是，如果使用 **no sysopt connection permit-vpn** 命令关闭此旁路，则该行为取决于是否存在应用于组策略的 **vpn-filter**，以及是否设置 **per-user-override** 选项：

  - No **per-user-override**, no **vpn-filter** - 针对接口 ACL 匹配流量。
  - No **per-user-override**, **vpn-filter** - 依次针对接口 ACL 和 VPN 过滤器匹配流量。
  - **per-user-override**、**vpn-filter** - 仅针对 VPN 过滤器匹配流量。
- **control-plane** 关键字指定扩展 ACL 是否适用于传入流量。

  与正则访问规则不同，接口的管理（控制平面）规则集的末尾没有任何隐式拒绝。相反，与管理访问规则不匹配的任何连接都通过正则访问控制规则进行评估。

对于全局访问组，指定 **global** 关键字，以将扩展 ACL 应用于所有接口的入站方向流量。

示例

以下示例展示如何使用 **access-group** 命令：

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside
```

access-list 命令允许任何主机使用端口 80 访问主机地址。**access-group** 命令指定 **access-list** 命令适用于传入外部接口的流量。

配置 ICMP 访问规则

默认情况下，您可以使用 IPv4 或 IPv6 将 ICMP 数据包发送到任何接口，以下情况例外：

- ASA 不响应定向至广播地址的 ICMP 回显请求。

- ASA 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

为了保护设备免受攻击，您可以使用 ICMP 规则将接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为 ICMP 不可到达消息类型（类型 3）授予权限。拒绝 ICMP 不可达消息会禁用 ICMP 路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。

过程

步骤 1 创建适用于 ICMP 流量的规则。

icmp {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name*

如果未指定 *icmp_type*，该规则将适用于所有类型。可输入编号或名称。要控制 ping 操作，请指定 echo-reply (0) (ASA-to-host) 或 echo (8) (host-to-ASA)。

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ip_address mask*)。

步骤 2 创建适用于 ICMPv6 (IPv6) 流量的规则。

ipv6 icmp {**permit** | **deny**} {**host** *ipv6_address* | *ipv6-network*/*prefix-length* | **any**} [*icmp_type*] *interface_name*

如果未指定 *icmp_type*，该规则将适用于所有类型。

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ipv6-network*/*prefix-length*)。

步骤 3 （可选。）设置对 ICMP Unreachable 消息的速率限制，以便 ASA 显示在跟踪路由输出中。

icmp unreachable rate-limit *rate* **burst-size** *size*

速率限制可为 1-100，1 为默认值。突发大小可以是 1-10。发送的回复数量为突发大小，但在达到速率限制之前不会发送后续回复。

示例：

要允许跟踪路由通过 ASA（作为其中一跳显示 ASA），需要增加速率限制并在服务策略中启用 **set connection decrement-ttl** 命令。例如，以下策略可增加速率限制并减小通过 ASA 的所有流量的生存时间 (TTL) 值。

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```

```
set connection decrement-ttl
```

示例

以下示例展示，如何允许除处于 10.1.1.15 的主机之外的所有主机使用 ICMP 流量侦测内部接口：

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

以下示例显示如何允许地址为 10.1.1.15 的主机仅使用 ping 连接内部接口：

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

以下示例显示如何在外部接口上拒绝所有 ping 请求并允许所有数据包太大的消息（以支持路径 MTU 发现）：

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

以下示例显示如何允许主机 2000:0:0:4::2 或前缀 2001::/64 的主机使用 ping 连接外部接口：

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

监控访问规则

要监控网络访问，请输入以下命令：

- **clear access-list** *id* **counters**

  清除访问列表的命中计数。

- **show access-list** [*name*]

  显示访问列表，包括每个 ACE 的行号和命中次数。纳入 ACL 名称，否则将看到所有访问列表。

- **show running-config access-group**

  显示与接口绑定的当前 ACL。

评估访问规则的系统日志消息

使用系统日志事件查看器，如 ASDM 中的查看器，查看与访问规则相关的消息。

如果使用默认日志记录，则只会看到与显式拒绝的流对应的系统日志消息 106023。将不记录与规则列表末尾的“隐式拒绝”条目匹配的流量。

如果已连接 ASA，则拒绝数据包的系统日志消息数可能非常大。我们建议您转而启用使用系统日志消息 106100 的日志记录，该记录提供每条规则（包括允许规则）的统计信息，且可使您限制所生成的系统日志消息的数量。或者，可禁用给定规则的所有日志记录。

当您对消息 106100 启用日志记录时，如果数据包与某个 ACE 匹配，ASA 会创建一个流条目来跟踪特定间隔内收到的数据包数。ASA 会在首次计数和每个间隔结束时都生成一条系统日志消息，标识该间隔内计数的总数以及最后一次计数的时间戳。在每个间隔结束时，ASA 会将计数数额重置为 0。如果在一个间隔内没有数据包匹配，ASA 将删除该流条目。为规则配置日志记录时，可控制间隔，甚至可控制每条规则的日志消息的严重性级别。

流是按源与目标 IP 地址、协议和端口定义的。由于对于相同两台主机之间的新连接而言源端口可能不同，且为该连接创建了新的流，因此，可能看不到相同的流递增。

不需要针对 ACL 检查属于已建立连接的已允许数据包；仅初始数据包将得以记录并纳入命中计数中。对于无连接的协议（如 ICMP），所有数据包均得以记录，即使它们是被允许的数据包，且所有已拒绝数据包均得以记录。

有关这些消息的详细信息，请参阅系统日志消息指南。

提示 当您对消息 106100 启用日志记录时，如果数据包与某个 ACE 匹配，ASA 会创建一个流条目来跟踪特定间隔内收到的数据包数。ASA 包含的 ACE 日志记录流最大为 32 K。在任何时间点，都可能有大量的流同时存在。为了防止无限制地占用内存和 CPU 资源，ASA 会限制并发拒绝流的数量；由于拒绝流可能意味着正在发生攻击，所以该限制仅应用于拒绝流（不应用于允许流）。达到该限制时，ASA 在现有流到期前不会对日志记录创建新的拒绝流，并会发出消息 106101。可使用 **access-list alert-interval** *secs* 命令控制发出此消息的频率，并使用 **access-list deny-flow-max** *number* 命令控制缓存的拒绝流的最大数量。

允许或拒绝网络访问的配置示例

以下是一些允许或拒绝网络访问的典型配置示例。

扩展 ACL 示例

以下示例为内部服务器 1 添加网络对象，为服务器执行静态 NAT 以及为内部服务器 1 启用来自外部的访问。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12
```

```
hostname(config)# access-list outside_access extended permit tcp any object inside-server1
 eq www
hostname(config)# access-group outside_access in interface outside
```

以下示例允许所有主机在 inside 和 hr 网络之间进行通信，但仅允许特定主机访问外部网络：

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

以下示例使用对象组来允许内部接口上的特定流量：

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

EtherType 示例

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
```

访问规则的历史记录

功能名称	平台版本	说明
接口访问规则	7.0(1)	使用 ACL 通过 ASA 控制网络访问。 引入了以下命令：**access-group**。
全局访问规则	8.3(1)	引入了全局访问规则。 修改了以下命令： **access-group.**
标识防火墙的支持	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 传输 IS-IS 流量。 修改了以下命令：**access-list ethertype** {**permit** | **deny**} **isis**。
对 TrustSec 的支持	9.0(1)	现可将 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**。
适用于 IPv4 和 IPv6 的统一 ACL	9.0(1)	ACL 现支持 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**、**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**。
基于访问组规则引擎的事务提交模型	9.1(5)	一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。 引入了以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**。

功能名称	平台版本	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 config-session**、**clear session**、**configure session**、**forward-reference** 和 **show config-session** 命令。
流控制传输协议 (SCTP) 的访问规则支持	9.5(2)	现在，您可以使用 **sctp** 协议（包括端口规范）创建访问规则。 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**。
现在，对象组搜索阈值将默认禁用。	9.12(1)	在以前，如果您启用对象组搜索功能，此功能将受阈值限制，这是为了防止性能出现下降。该阈值现在默认将被禁用。您可以使用 **object-group-search threshold** 命令启用该阈值。 添加了以下命令：**object-group-search threshold**。

功能名称	平台版本	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。
对象组搜索优化。	9.22(1)	对象组搜索功能得到了增强，可在评估访问控制规则以匹配连接时减少对象查找时间，并减少 CPU 开销。配置对象组搜索没有任何变化，优化行为会自动进行。 我们在设备 CLI 或增强的命令输出中添加了以下命令：**clear asp table network-object**、**debug ac logs**、**packet-tracer**、**show access-list**、**show asp table network-group**、**show object-group**。

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。