# pr - pz

# pre-fill-username

要从客户端证书中提取用户名以用于身份验证和授权，请在**pre-fill-username**隧道组 webvpn-attributes 模式下使用该命令。要从配置中删除属性，请使用此命 **no**令的形式。

**pre-fill-username** {**client** | **clientless**}
**no pre-fill-username**

## Syntax Description

| | |
|---|---|
| **client**<br>**ssl-client** | 为 AnyConnect VPN 客户端连接启用此功能。在 9.8(1)+ 中，请使用 **client** 关键字。 |
| **clientless** | 为无客户端连接启用此功能。 |

## Command Default

没有默认值或行为。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Tunnel-group webvpn-attributes 配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(4) | 添加了此命令。 |
| 9.8(1) | 关键字 **ssl-client** 已更改为 **client**。 |

## 使用指南

该命令允 **pre-fill-username**许使用从命令中指定的证书字段中提取的 **username-from-certificate**用户名作为用户名/密码认证和授权的用户名。如要使用证书功能中的此预填充用户名，必须配置这两个命令。

要启用此功能，您还必须在 tunnel-group general-attributes 模式下配置 **username-from-certificate** 命令。

## CR_Examples

以下示例以全局配置模式输入，创建一个名为 remotegrp 的 IPsec 远程访问隧道组，并指定 SSL VPN 客户端的身份验证或授权查询的名称必须来自数字证书：

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
```

```
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **pre-fill-username** | 启用预填充用户名功能。 |
| **show running-config tunnel-group** | 显示指示的隧道组配置。 |
| **tunnel-group general-attributes** | 指定命名的隧道组的常规属性。 |
| **username-from-certificate** | 指定证书中用作授权用户名的字段。 |

# preempt

要使故障转移组在首选设备上变成活动状态，请在故障转移组配置模式下使用 **preempt** 命令。要取消抢占，请使用此命 **no**令的形式。

**preempt** [*delay*]
**no preempt** [*delay*]

## Syntax Description

*seconds* 对等设备抢占之前的等待时间（以秒为单位）。有效值范围为 1 至 1200 秒。

## Command Default

默认情况下，没有延迟。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 故障转移组配置 | • 是 | • 支持 | — | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.0(1) | 较早的软件版本中允许“同时”启动，以便故障转移组无需 **preempt** 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障转移组在要启动的第一台设备上都变为主用状态。 |

## 使用指南

将 **primary** 或 **secondary** 首选项分配给故障转移组可指定在设置 **preempt** 命令时故障转移组在哪个设备上将变为主用状态。两个故障转移组都会在第一个启动的单元上变为活动状态（即使看起来它们同时启动，但一个单元会先变为活动状态），无论该组的 **primary**或 **secondary**设置如何。当另一台设备上线时，将第二台设备作为优先级的任何故障转移组都不会在第二台设备上变为活动状态，除非故障转移组使用 **preempt** 命令进行了配置，或者使用 **nofailoveractive** 命令手动强制到另一台设备请参阅如果使用该命令配置了故障转移 **preempt**组，则故障转移组将在指定单元上自动变为活动状态。

注释 如果启用状态故障转移，则抢占会延迟，直到连接从当前处于主用状态的故障转移组所在的设备中复制为止。

## CR_Examples

以下示例配置了故障转移组 1，其中主设备为较高优先级，并配置了故障转移组 2，其中辅助设备为较高优先级。两个故障转移组均使用 **preempt** 命令配置为 100 秒的等待时间，因此，在设备变为可用 100 秒后，两个组将在其首选设备上自动变为主用状态。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **failovergroup** | 定义主用/主动故障转移的故障转移组。 |
| **primary** | 为正在配置的故障转移组的故障转移对中的主设备提供优先级。 |
| **secondary** | 为正在配置的故障转移组的故障转移对中的辅助设备提供优先级。 |

# prefix-list

OSPFv2、EIGRP 和 BGP 协议全部在全局配置模式下使用 **prefix-list** 命令。要删除前缀列表条目，请使用此命令的 **no** 形式。

**prefix-list***prefix-list-name* [**seq***seq_num*] {**permit** | **deny**} *network*/*len* [**ge***min_value*] [**le***max_value*]
**no prefix-list***prefix-list-name* [**seq***seq_num*] {**permit** | **deny**} *network*/*len* [**ge***min_value*] [**le***max_value*]

## Syntax Description

| | |
|---|---|
| / | 网络 和 *len* 值之间的必需分隔符。 |
| **deny** | 因条件匹配而拒绝访问。 |
| **ge***min_value* | （可选）指定要匹配的最小前缀长度。 *min_value* 参数的值必须大于 *len* 参数的值并小于或等于 *max_value* 参数（如果有）。 |
| **le***max_value* | （可选）指定要匹配的最大前缀长度。 *max_value* 参数的值必须大于或等于 *min_value* 参数（如果有）的值，或者，如果 *min_value* 参数不存在，则该值必须大于 *len* 参数的值。 |
| *len* | 网络掩码的长度。有效值为 0 至 32。 |
| 网络 | 网络地址。 |
| **permit** | 允许访问匹配条件。 |
| *prefix-list-name* | 前缀列表的名称。前缀列表名称不能包含空格。 |
| **seq***seq_num* | （可选）将指定序列号应用于正在创建的前缀列表。 |

## Command Default

如果未指定序列号，则系统将为前缀列表中的第一个条目分配序列号 5，并且每个后续条目的序列号都将增加 5。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.0(1) | 增加了多情景模式支持。 |

| 版本 | 修改 |
| --- | --- |
| 9.2(1) | 添加了对 BGP 的支持。 |

## 使用指南

**prefix-list** 命令是 ABR 类型 3 LSA 过滤命令。ABR 类型 3 LSA 过滤扩展了 ABR 的功能，即在不同 OSPF 区域之间运行 OSPF 过滤类型 3 LSA。一旦配置了前缀列表，则只有指定的前缀才会从一个区域发送到另一个区域。所有其他前缀都限用于各自的 OSPF 区域。可以向传入或传出 OSPF 区域的流量或者同时为该区域的传入和传出流量应用此类型的区域过滤。

当前缀列表的多个条目与给定前缀相匹配时，将使用具有最低序列号的条目。ASA 从前缀列表的顶部开始搜索具有最小序列号的条目。创建匹配后，ASA 不会浏览列表中的其余项。为提高效率，可能需要手动为最常用的匹配或拒绝项分配较低的序列号来将其置于列表顶部附近。

默认情况下，系统会自动生成序列号。可以使用 **noprefix-listsequence-number** 命令抑制这些警报。序列号以 5 为增量生成。前缀列表中生成的第一个序列号为 5。该列表中的下一个条目的序号为 10，以此类推。如果为某个条目指定了值，但不为后续条目指定值，则生成的序列号将以 5 为增量从指定的值开始增加。例如，如果指定前缀列表中第一个条目的序号为 3，然后另外两个条目未指定序号，则为这两个条目自动生成的序号为 8， 13.

您可以使用 **ge**和关 **le**键字来指定比 *network*/*len*参数更具体的前缀匹配的前缀长度范围。既未指定 **ge** 也未指定 **le** 关键字时，假定完全匹配。如果仅指定了 **ge** 关键字，则范围为 *min_value* 到 32。如果仅指定了 **le**关键字，则范围为 *len* 到 *max_value* 。

*min_value* 和 *max_value* 参数的值必须满足以下条件：

*len* < *min_value* <= *max_value* <= 32

使用命令的 **no** 形式可从前缀列表中删除特定条目。使用 **clearconfigureprefix-list** 命令来删除前缀列表。clear **configureprefix-list** 命令还会从配置中删除关联的 **prefix-listdescription** 命令（如果有）。

## CR_Examples

以下示例拒绝默认路由 0.0.0.0/0：

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

以下示例允许使用前缀 10.0.0.0/8：

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

以下示例显示如何在前缀为 192/8 的路由中接受最多 24 位的掩码长度：

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

以下示例显示如何拒绝前缀为 192/8 的路由中掩码长度大于 25 位的路由：

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

以下示例显示如何在所有地址空间中允许 8 至 24 位的掩码长度：

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

以下示例显示如何在所有地址空间中拒绝长度超过 25 位的掩码：

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

以下示例显示如何拒绝前缀为 10/8 的所有路由：

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

以下示例显示如何拒绝前缀为 192.168.1/24 的路由的所有长度大于 25 位的掩码：

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

以下示例显示如何允许所有前缀为 0/0 的路由：

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearconfigureprefix-list** | 从运行配置中删除 **prefix-list** 命令。 |
| **prefix-listdescription** | 用于输入前缀列表的说明。 |
| **prefix-listsequence-number** | 启用前缀列表顺序编号。 |
| **showrunning-configprefix-list** | 显示正在 **prefix-list**运行的配置中的命令。 |

# 前缀列表说明

要向前缀列表添加说明，请在全局配置模式下使用 **prefix-list description** 命令。要删除前缀列表描述，请使用此 **no**命令的形式。

**prefix-list***prefix-list-name***description***text*
**no prefix-list***prefix-list-name***description** [ *text* ]

## Syntax Description

| | |
|---|---|
| *prefix-list-name* | 前缀列表的名称。 |
| 文本 | 前缀列表说明的文本。最多可以输入80个字符。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

对于特定前缀列表名称，可以按任意顺序输入**prefix-list** 和 **prefix-listdescription**命令。在输入前缀列表说明之前，不需要创建前缀列表。在配置中， **prefix-listdescription** 命令将始终显示在关联前缀列表之前的行中，无论您输入命令的顺序如何。

如果为已有说明的前缀列表条目输入 **prefix-listdescription** 命令，新说明将替换原始说明。

使用此命令的 **no** 形式时，无需输入文本说明。

## CR_Examples

以下示例为名为 MyPrefixList 的前缀列表添加说明。 **showrunning-configprefix-list** 命令显示，虽然前缀列表说明已添加到运行配置，但前缀列表本身尚未配置。

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **clearconfigureprefix-list** | 从运行配置中删除 **prefix-list** 命令。 |
| **prefix-list** | 定义 ABR 3 类 LSA 筛选的前缀列表。 |
| **showrunning-configprefix-list** | 显示正在 **prefix-list**运行的配置中的命令。 |

# 前缀列表序列号

要启用前缀列表序列编号，请在全局配置模式下使用 **prefix-listsequence-number** 命令。要禁用前缀列表序列编号，请使用此命令的 **no** 形式。

**prefix-list sequence-number**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下，启用前缀列表序列编号。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

配置中 **no**仅出现此命令的形式。当配置中使用此命令的 **no** 形式时，系统会从配置中的 **prefix-list** 命令中删除序列号（包括手动配置的序列号），并且不会为新的前缀列表条目分配序列号。

启用前缀列表序列编号后，系统将使用默认编号方法为所有前缀列表条目分配序列号（从 5 开始，每个数字加5）。如果在禁用编号之前手动为前缀列表条目分配了序号，则会恢复手动分配的编号。在自动编号禁用时，手动分配的序列号也会恢复，即使在编号禁用时它们不会显示。

## CR_Examples

以下示例禁用前缀列表序列编号：

```
ciscoasa(config)# no prefix-list sequence-number
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **prefix-list** | 定义 ABR 3 类 LSA 筛选的前缀列表。 |
| **showrunning-configprefix-list** | 显示正在 **prefix-list**运行的配置中的命令。 |

# prf

要在 AnyConnect IPsec 连接的 IKEv2 安全关联 (SA) 中指定伪随机函数 (PRF)，请在 IKEv2 策略配置模式下使用 prf 命令。要删除该命令并使用默认设置，请使用此命令的 no 形式：

**prf** {**md5** | **sha** | **sha256** | **sha384** | **sha512**}
**no prf** {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

## Syntax Description

| | |
|---|---|
| **md5** | 指定 MD5 算法。 |
| **sha** | （默认）指定安全散列算法 SHA 1。 |
| sha256 | 指定具有 256 位摘要的安全散列算法 SHA 2。 |
| **sha384** | 指定具有 384 位摘要的安全散列算法 SHA 2。 |
| **sha512** | 指定具有 512 位摘要的安全散列算法 SHA 2。 |

## Command Default

默认值为 **sha**(SHA 1)。

## 使用指南

IKEv2 SA 是在第 1 阶段使用的密钥，用于使 IKEv2 对等体能够在第 2 阶段安全通信。输入 crypto ikev2 policy 命令后，使用该命令选择 **prf**用于构建 SA 中使用的所有加密算法的密钥材料的伪随机函数。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.4(1) | 添加了此命令。 |
| 8.4(2) | 添加了 sha256、sha384 和 sha512 关键字以提供 SHA 2 支持。 |

## CR_Examples

以下示例进入 IKEv2 策略配置模式并将 PRF 设置为 MD5：

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| encryption | 为 AnyConnect IPsec 连接指定 IKEv2 SA 中的加密算法。 |
| group | 在 IKEv2 SA 中为 AnyConnect IPsec 连接指定 Diffie-Hellman 群。 |
| **integrity** | 为 AnyConnect IPsec 连接指定 IKEv2 SA 的 ESP 完整性算法。 |
| lifetime | 指定 AnyConnect IPsec 连接的 IKEv2 SA 的 SA 生命周期。 |

# primary

要在使用 **preempt** 命令时设置故障转移组的首选设备，请在故障转移组配置模式下使用 **primary** 命令。要恢复默认值，请使用此命 **no**令的形式。

**primary**
**no primary**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

如果未为故障转移组指定 **primary** 或 **secondary** ，则故障转移组默认为 **primary**。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 故障转移组配置 | • 是 | • 支持 | — | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.0(1) | 较早的软件版本中允许“同时”启动，以便故障转移组无需 **preempt** 命令即可在首选设备上变为主用状态。但此功能现已更改，以使两个故障转移组在要启动的第一台设备上都变为主用状态。 |

## 使用指南

将 **primary** 或 **secondary** 首选项分配给故障转移组可指定在设置 **preempt** 命令时故障转移组在哪个设备上将变为主用状态。两个故障转移组都会在第一个启动的单元上变为活动状态（即使看起来它们同时启动，但一个单元会先变为活动状态），无论该组的 **primary**或 **secondary**设置如何。当另一台设备上线时，将第二台设备作为优先级的任何故障转移组都不会在第二台设备上变为活动状态，除非故障转移组使用 **preempt** 命令进行了配置，或者使用 **nofailoveractive** 命令手动强制到另一台设备请参阅如果使用该命令配置了故障转移 **preempt**组，则故障转移组将在指定单元上自动变为活动状态。

## CR_Examples

以下示例配置了故障转移组 1，其中主设备为较高优先级，并配置了故障转移组 2，其中辅助设备为较高优先级。两个故障转移组均使用 **preempt** 命令进行配置，因此，当设备变得可用时，两个组将在其首选设备上自动变为主用状态。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
```

```
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **failovergroup** | 定义主用/主动故障转移的故障转移组。 |
| **preempt** | 当设备变得可用时，强制故障转移组在其首选设备上变为主用状态。 |
| **secondary** | 给予辅助设备高于主设备的优先级。 |

# priority（类别）

要启用 QoS 优先级排队，请在类配置模式下使用 **priority**命令。对于不能容忍延迟的关键流量，例如 IP 语音 (VoIP)，您可以识别低延迟排队 (LLQ) 的流量，以便始终以最低速率传输。要删除优先级要求，请使用此命 **no**令的形式。

注释 ASA 服务模块不支持此命令。

**priority**
**no priority**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

无默认行为或变量。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 类配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

LLQ 优先级排队使您可以在处理其他流量之前优先处理某些流量（例如，像语音和视频之类的延迟敏感型流量）。

ASA 支持两种类型的优先级排队：

- 标准优先级排队——标准优先级排队在 **priority-queue** 接口上使用 LLQ 优先级队列（参见命令），而所有其他流量都进入“尽力而为”队列。由于队列大小有限制，队列可以填满和溢出。如果队列已满，任何额外的数据包无法进入队列，并将丢弃。这称为 尾部丢 弃。为了避免队列填满，您可以增加队列缓冲区的大小。还可以优化允许进入传输队列的数据包的最大数。这些选项使您能够控制优先级排队的延迟和稳定性。LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

- 分层优先级排队 - 分层优先级排队用在启用流量整形队列（ **shape** 命令）的接口上。可以对整形的流量的子集进行优先级排序。不使用标准优先级队列。请参阅以下有关分层优先级排队的准则：
- 优先级数据包始终排在整形队列的开头，因此它们始终先于其他未优先排队的数据包传输。
- 优先级数据包永远不会从整形队列中丢弃，除非优先级流量的持续速率超过整形速率。
- 对于 IPsec 加密的数据包，只能根据 DSCP 或优先级设置来匹配流量。
- 优先级流量分类不支持 IPsec-over-TCP。

### 使用模块化策略框架配置 QoS

要启用优先级排队，请使用模块化策略框架。您可以使用标准优先级排队或分层优先级排队。

对于标准优先级排队，请执行以下任务：

**1.—class-map**确定您想要执行优先级排队的流量。

**2.policy-map**- 确定与每个类映射关联的操作。

- **a.—class**确定您想要执行操作的类映射。
- **b.priority**- 为类映射启用优先级排队。

**3.service-policy**- 向接口或全局分配策略映射。

对于分层优先级排队，请执行以下任务：

**1.—class-map**确定您想要执行优先级排队的流量。

**2.policy-map** (for priority queuing) - 标识与每个类映射关联的操作。

- **a.—class**确定您想要执行操作的类映射。
- **b.priority**- 为类映射启用优先级排队。如果要分层使用，只能在此策略映射中包含 priority 命令。

**3.policy-map** （适用于流量整形）- 标识与 **class-default** 类映射关联的操作。

- **a.—classclass-default**确定您想要执行操作的 **class-default**类映射。
- **b.shape**- 将流量整形应用到类映射。
- **c.service-policy**- 调用您在其中配置了 **priority** 命令的优先级排队策略映射，以便将优先级排队应用于整形流量子集。

**4.service-policy**- 向接口或全局分配策略映射。

## CR_Examples

以下是策略映射配置模式下的 **priority** 命令的示例：

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
```

```
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

## Related Commands

| | |
|---|---|
| **class** | 指定要用于流量分类的类映射。 |
| **clearconfigurepolicy-map** | 删除所有策略映射配置，但如果策略映射正在用于服务策略命令，则不会删除该策略映射。 |
| **policy-map** | 配置策略；即流量类与一个或多个操作的关联。 |
| **showrunning-configpolicy-map** | — 确定您想要执行操作的类映射。 |

# priority（集群组）

要设置此设备在 ASA 集群中主设备选举的优先级，请在集群组配置模式下使用 **priority** 命令。要删除优先级，请使用此 **no**命令的形式。

**priority***priority_number*
**no priority** [*priority_number*]

## Syntax Description

| | |
|---|---|
| *priority_number* | 设置此单元在主单元选举中的优先级，介于 1 和 100 之间，其中 1 为最高优先级。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 集群组配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 9.0(1) | 添加了此命令。 |

## 使用指南

集群成员通过集群控制链路进行通信来选举主单元，如下所示：

**1.** 当为设备启用集群（或当设备首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。

**2.** 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。

**3.** 如果某设备在 45 秒后未收到另一个具有较高优先级的设备的响应，则该设备会成为主设备。

注释 如果多个单元并列最高优先级，则使用集群单元名称，然后序列号来确定主单元。

**4.** 如果稍后有优先级更高的设备加入群集，则该设备不会自动成为主设备；现有主设备将一直作为主设备，除非它停止响应，届时将选举新的主设备。

注释 您可以使用命令手动强制某个单元成为主单元**clustermasterunit**。对集中功能而言，如果强制更改主设备，则所有连接都将断开，而您必须在新的主设备上重新建立连接。有关集中功能的列表，请参阅配置指南。

## CR_Examples

以下示例将优先级设置为 1（最高）：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clacpsystem-mac** | 使用跨网以太网通道时，ASA 使用 cLACP 与邻居交换机协商以太网通道。 |
| cluster group | 命名集群并进入集群配置模式。 |
| **cluster-interface** | 指定集群控制链路接口。 |
| **clusterinterface-mode** | 设置集群接口模式。 |
| **conn-rebalance** | 启用连接再均衡。 |
| **console-replicate** | 启用从从属设备到主设备的控制台复制。 |
| **enable(clustergroup)** | 启用集群。 |
| **health-check** | 启用集群健康检查功能，包括单元健康监控和接口健康监控。 |
| **key** | 为集群控制链路上的控制流量设置身份验证密钥。 |
| **local-unit** | 为集群成员命名。 |
| **mtucluster-interface** | 指定集群控制链路接口的最大传输单元。 |
| **priority(clustergroup)** | 设置此单元在主单元选举中的优先级。 |

# priority（VPN负载均衡）

要设置参与虚拟负载均衡集群的本地设备的优先级，请在 VPN 负载均衡模式下使用 **priority**命令。要恢复默认优先级规范，请使用此命 **no**令的形式。

**priority***priority*
**no priority**

## Syntax Description

| | |
|---|---|
| *priority* | 您要分配给此设备的优先级，取值范围为 1 到 10。 |

## Command Default

默认优先级取决于设备型号：

| 型号编号 | 默认优先级 |
|---|---|
| 5520 | 5 |
| 5540 | 7 |

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| VPN 负载均衡 | — | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

必须先使用 **vpnload-balancing**命令进入 VPN 负载均衡模式。

此命令设置加入虚拟负载均衡集群的本地设备的优先级。

优先级必须是介于 1（最低）到 10（最高）之间的整数。

在主设备选择过程中，优先级会作为一种方式来确定VPN负载均衡集群中的哪台设备会成为集群的主设备或主设备。有关主设备选择过程的详细信息，请参阅 CLI 配置指南 。

命令的 **no** 形式可将指定的优先级恢复为默认值。

## CR_Examples

以下是一个 VPN 负载均衡命令序列示例，其中包含一条 **priority** 命令，该命令将当前设备的优先级设置为 9：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **vpnload-balancing** | 进入 VPN 负载均衡模式。 |

# priority-queue

要在接口上创建标准优先级队列以与**priority**命令配合使用，请在全局配置模式下使用**priority-queue**命令。要删除队列，请使用此 **no**命令的形式。

注释 ASA 5580万兆以太网接口不支持此命令。（ASA 5585-X上的优先级队列支持十千兆以太网接口。）ASA 5512-X 至 ASA 5555-X 管理接口也不支持此命令。ASA 服务模块不支持此命令。

**priority-queue***interface-name*
**no priority-queue***interface-name*

## Syntax Description

| | |
|---|---|
| *interface-name* | 指定要启用优先级队列的物理接口的名称，或者对于 ASA 5505 或 ASASM，指定 VLAN 接口的名称。 |

## Command Default

默认情况下，优先级排队处于禁用状态。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 8.2(3)/8.4(1) | ASA 5585-X增加了对十千兆以太网接口的支持。 |

## 使用指南

LLQ 优先级排队使您可以在处理其他流量之前优先处理某些流量（例如，像语音和视频之类的延迟敏感型流量）。

ASA 支持两种类型的优先级排队：

- 标准优先级排队——标准优先级排队在您使用命令创建的接口上使用LLQ优先级**priority-queue**队列，而所有其他流量进入“尽力而为”队列。由于队列大小有限制，队列可以填满和溢出。如果队列已满，任何额外的数据包无法进入队列，并将丢弃。这被称为 尾部丢弃。为了避免队列填满，您可以增加队列缓冲区大小（ **queue-limit**命令）。您还可以微调允许进入传输队列的最大数据包数量（ **tx-ring-limit**命令）。这些选项使您能够控制优先级排队的延迟和稳定性。LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

- 分层优先级排队 - 分层优先级排队用在启用了流量整形队列的接口上。可以对整形的流量的子集进行优先级排序。不使用标准优先级队列。

注释 仅在 ASA 5505 上，在一个接口上配置优先级队列会覆盖所有其他接口上的相同配置；所有接口上仅存在最后应用的配置。此外，如果从一个接口删除优先级队列配置，则该配置也会从所有接口删除。要解决此问题，请仅在一个接口上配置 priority-queue 命令。如果不同的接口需要对 queue-limit 和/或 tx-ring-limit 命令进行不同的设置，请在任何一个接口上使用所有队列限制中的最大者和所有 tx-ring-limits 中最小者（CSCsi13132）。

## CR_Examples

以下示例为名为 test 的接口配置优先级队列，指定队列限制为 30,000 个数据包，传输队列限制为 256 个数据包。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **queue-limit** | 指定在优先级队列丢弃数据前可排入该队列的最大数据包数。 |
| **tx-ring-limit** | 设置可在任何给定时间在以太网传输驱动器中排队的数据包的最大数量。 |
| **policy-map** | 配置策略；即流量类与一个或多个操作的关联。 |
| **clearconfigurepriority-queue** | 删除当前优先级队列配置。 |
| **showrunning-config[all]priority-queue** | 显示当前优先级队列配置。如果指定 **all** 关键字，此命令将显示所有当前优先级队列、队列限制和 tx-ring-limit 配置值。 |

# privilege

要配置与命令授权一起使用的命令权限级别（仅限本地、RADIUS 和 LDAP（映射）），请在全局配置模式下使用 **privilege** 命令。要不允许配置，请使用此命 **no**令的形式。

**privilege** ［**show** ｜**clear** ｜**configure**］**level***level* ［**mode***cli_mode*］ **command**命令
**no privilege**［ **show** ｜**clear** ｜**configure**］**level***level* ［**mode***cli_mode* ］**command**命令

## Syntax Description

| | |
|---|---|
| **clear** | （可选）仅为 clear 形式设置命令的权限。如果不使用、或 **configureclearshow**关键字，则该命令的所有形式都会受到影响。 |
| **command**命令 | 指定您正在配置的命令。您只能配置主命令的权限级别。例如可以配置所 **aaa**有命令的级别，但不能配置某条命 **aaaauthentication**令和某条命令的 **aaaauthorization** 级别。 |
| **configure** | （可选）仅为命令的配置形式设置权限。命令的配置形式通常是导致配置更改的形式，或者是以未修改的命令形式（无 **show**或 **clear** 前缀），或者是以 **no** 形式。如果不使用、或**configureclearshow**关键字，则该命令的所有形式都会受到影响。 |
| **level**级别 | 指定特权级别；有效值为 0 至 15。较低特权级别数字表示较低特权级别。 |
| **mode***cli_mode* | （可选）如果可以在多个 CLI 模式下输入命令，例如用户执行/特权 EXEC 模式、全局配置模式或命令配置模式，则可以分别设置这些模式的权限级别。如果不指定模式，则该命令的所有版本都使用同一级别。请参阅以下模式：<br>• **exec** - 指定用户 EXEC 模式和特权 EXEC 模式。<br>• —**configure**指定全局配置模式， **configureterminal**使用命令访问。<br>• *command_config_mode* - 指定命令配置模式，在全局或其他命令配置模式下使用命令名称进行访问。<br>例如， **mac-address**该命令可以在全局配置模式和接口配置模式下输入。mode 关键字用于为每种模式单独设置级别。<br>如果在为 命令设置级别，则无法使用此命令 |
| **show** | （可选）仅为 show 形式的命令设置权限。如果不使用、或**configureclearshow**关键字，则该命令的所有形式都会受到影响。 |

## Command Default

默认情况下，会为以下命令分配 0 级权限，所有其他命令均处于级别 15。

- **showchecksum**
- **showcurpriv**
- **enable**
- **help**

- **showhistory**
- **login**
- **logout**
- **pager**
- **showpager**
- **clearpager**
- **quit**
- **showversion**

如果将任何配置模式命令移动到低于 15 的 **configure** 级别，请确保也将该命令移动到该级别，否则用户将无法进入配置模式。

要查看所有权限级别，请参阅 **showrunning-configallprivilegeall** 命令。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 增加了对具有 Cisco VSA CVPN3000-Privilege-Level 的 RADIUS 用户的支持。如果使用 **ldapmap-attributes**命令将 LDAP 属性映射到 CVPN3000-Privilege-Level，则支持 LDAP 用户。 |

## 使用指南

当您配置 **privilege** 命令时，[ **aaaauthorizationcommandLOCAL** 命令允许您设置 ASA 命令的权限级别。即使命令使用 **LOCAL** 关键字，此关键字也将启用本地、RADIUS 和 LDAP（映射）授权。

## CR_Examples

例如，命令有 **filter**以下形式：

- **filter**（以 **configure**选项表示）
- **showrunning-configfilter**
- **clearconfigurefilter**

您可以为每种形式分别设置权限级别，或通过忽略此选项为所有形式设置同一权限级别。例如，分别设置每个表单，如下所示：

```
ciscoasa(config)# privilegeshowlevel5commandfilter
ciscoasa(config)# privilegeclearlevel10commandfilter
ciscoasa(config)# privilegecmdlevel10commandfilter
```

或者，您可以将所有过滤命令设置为同一级别：

```
ciscoasa(config)# privilegelevel5commandfilter
```

该命令将 **showprivilege**显示中的各个表单分开。

以下示例显示 **mode** 关键字的使用。该 **enable**命令必须从用户 EXEC 模式输入，而在 **enablepassword**配置模式下可访问的命令需要最高权限级别。

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

以下示例显示了两种模式下的 **mac-address** 命令以及 show、clear 和 cmd version 的不同级别：

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearconfigureprivilege** | 从配置中删除特权命令语句。 |
| **showcurpriv** | 显示当前权限级别。 |
| **showrunning-configprivilege** | 显示命令的权限级别。 |

# profile

要创建或编辑报障配置文件，请在报障配置模式下使用 **profile** 命令。要删除一个或所有已配置的报障配置文件，请使用此命令的 **no** 形式指定一个或所有配置文件。您可以通过首先输入命令来访问 call-home配置 **call-home**模式。

**profile***profile-name*
**no profile**{*profile-name* | **all**}

## Syntax Description

| | |
|---|---|
| *profile-name* | 配置文件名称，最长 20 个字符。 |
| **all** | 包括所有已配置的配置文件。 |

## Command Default

已提供默认配置文件。 **CiscoTAC** 默认配置文件包含一组要监控的预定义组（诊断、环境、清单、配置和遥测）以及预定义的目标邮件地址和 HTTPS URL。最初配置 Smart Call Home 时，系统将自动创建默认配置文件。目标邮件地址为 callhome@cisco.com，目标 URL 为 https://tools.cisco.com/its/service/oddce/services/DDCEService。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 报障配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 8.2(1) | 我们引入了此命令。 |
| 8.2(2) | 添加了关键字all。 |
| 9.3(2) | 我们为智能软件许可添加了 **License** 配置文件。 |
| 9.6(2) | 引入了 **destinationaddresshttp**的 reference-identity 选项。 |

## 使用指南

以下命令用于模板配置模式。

### 启用或禁用配置文件

要启用 call-home 配置文件，请在 call-home-profile 配置模式下使用 **active**命令。要禁用 call-home 配置文件，请在 call-home-profile 配置模式下使用 **noactive**命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home**模 **profile**式。默认设置为启用。

active

no active

### 将配置文件命令设置为默认值

要将 call home 配置文件设置恢复为默认值，请在 call-home-profile 配置模式下使用 default 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home**模 **profile**式。您也可以从该模式重置报障配置模式设置。使用命令帮助、 **default?**确定和重置所有报障配置文件和常规设置。

**default**{**activedestinationemail-subjectsubscribe-to-alert-group**}

### 目标类型、地址和设置

要为 Smart Call Home 消息接收方设置目标地址、引用标识、消息格式和传输方法，请在 call-home-profile 配置模式下使用 **destination** 命令。要删除目标参数或将其重置为默认值，请使用 **nodestination**或 **default** 命令。

默认的邮件格式为 XM，默认的邮件大小为 5MB（0 表示无限制），默认传输方式为邮件。您必须指定以前配置的引用标识。这用于在连接时验证报障服务器的证书。它仅适用于 http 目标。

**destinationaddress**{**e-mail***e-mail-address***http***http-url*}
**nodestinationaddress**{**e-mailhttp**[**all**]}
**destinationaddresshttp***http-url***reference-identity**引用 *ID* 名称
**nodestinationaddresshttp***http-url***reference-identity**引用 *ID* 名称
**destinationaddress**{**e-mail***e-mail-address***http***http-url*}**msg-format**{**short-textlong-textxml**}
**nodestinationaddress**{**e-mail***e-mail-address***http***http-url*}**msg-format**{**short-textlong-textxml**}
**destinationmessage-size-limit***max-size*
**nodestinationmessage-size-limit***max-size*
**destinationpreferred-msg-format**{**short-textlong-textxml**}
**nodestinationpreferred-msg-format**{**short-textlong-textxml**}
**destinationtransport-method**{**e-mailhttp**}
**nodestinationtransport-method**{**e-mailhttp**}

### 配置邮件主题

要设置 call-home 邮件的邮件主题前缀或后缀，请在 call-home-profile 配置模式下使用 **email-subject** 命令。要清除这些字段，请使用 **noemail-subject** 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home**模 **profile**式。

**email-subject**{**appendprepend**}*chars*
**noemail-subject**{**appendprepend**}*chars*

### 订阅警报组

要订用警报组，请在 call-home-profile 配置模式下使用 s**ubscribe-to-alert-group** 命令。要清除这些订用，请使用 no s**ubscribe-to-alert-group** 命令。您可以通过首先输入 then 命令来访问 call-home-profile 配置 **call-home**模 **profile**式。

- [编号] 订阅警报组警报组名称[严重性|灾难性] | 灾难 | | 突发事件警报 | 警报| 严重 |错误 |警告 |通知 | 通知信息 | debug}] - 订阅具有指定严重性级别的组的事件。alert-group-name：系统日志、诊断、环境或威胁都是有效值。

- [no] subscribe-to-alert-group syslog [{严重性{灾难性| | 灾难 | | 突发事件警报 | 警报| 严重 |错误 |警告 |通知 | 通知信息 |调试} | message start [-end]}] - 订阅具有严重性级别或消息 ID 的系统日志。start-[end]：一个系统日志消息 ID 或一系列系统日志消息 ID。

注释 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。因此，请仅将调试用于解决特定问题或在与 Cisco 技术支持人员进行故障排除会话期间使用。另外，在网络流量较低和用户较少的时期使用它。在这些期间进行调试可以降低增加影响系统使用的处理开销的可能性。

- [no] subscribe-to-alert-group inventory [periodic {每日 | 重复每月 day_of_ month | 每月week day_of_week [hh:mm]] - 订阅资产事件。day_of_ month：星期几，1-31。day_of_week：星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）.hh, mm ： 24 小时制、一天的小时数和分钟数。
- [no] subscribe-to-alert-group configuration [export full | [no] subscribe-to-alert-group configuration [export full]最小值] [周期 {每日 | 周期每月 day_of_ month | 每月week day_of_week [hh:mm]] - 订用配置事件。full：要导出运行配置、启动配置、功能列表、访问列表中的元素数量以及多模式中情景名称的配置。minimum：要导出的配置-仅限功能列表、访问列表中的元素数量以及多模中的情景名称。day_of_ month：星期几，1-31。day_of_week：星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六） ).hh、mm：一天中的小时和分钟，采用 24 小时制。
- [no] subscribe-to-alert-group遥测定期{每小时| | 每日 |每月 day_of_ month | 每月week day_of_week [hh:mm] -订用遥测周期性事件。day_of_month：月份中的日期，1-31。day_of_week：星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）.hh, mm ： 24 小时制、一天的小时数和分钟数。
- [no] subscribe-to-alert-group snapper period {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]} — 订阅快照定期事件。minutes：间隔时间（分钟）。day_of_month：每月的某一天，1-31。day_of_week：星期几（星期日、星期一、星期二、星期三、星期四、星期五、星期六）。hh, mm：一天的小时和分钟，以 24 小时制表示。

**Related Commands**

| 命令 | 说明 |
|---|---|
| call-home | 使用户进入报障配置模式 |
| **showcall-home** | 显示 Call Home 配置信息。 |
| reference-identity | 配置引用标识对象。 |

# prompt

要自定义 CLI 提示符，请在全局配置模式下使用 prompt 命令。要恢复默认提示，请使用此命令的 no 形式。

**prompt**{ ［**hostname**］ ［**context** ］［**domain**］ ［**slot**］ ［**state**］ ［**priority**］［**cluster-unit** ］
**no prompt**［ **hostname**］ ［**context**］ ［**domain** ］［**slot** ］［**state**］ ［**priority** ］［**cluster-unit** ］

## Syntax Description

| | |
|---|---|
| **cluster-unit** | 显示集群设备名称。集群中的每台设备都有一个唯一的名称。 |
| **context** | （仅限多种模式）显示当前上下文。 |
| **domain** | 显示域名。 |
| **hostname** | 显示主机名。 |
| **priority** | 显示故障转移优先级 pri（主要）或 sec（辅助）。使用命令设置优先 **failoverlanunit** 级。 |
| **state** | 显示设备的流量传递状态或角色。<br>对于故障转移，关 **state**键字显示以下值：<br>• act - 已启用故障转移，设备正在传递流量。<br>• stby - 已启用故障转移，设备未在传递流量，并且处于备用、故障或其他非活动状态。<br>• actNoFailover - 未启用故障转移，设备正在传递流量。<br>• stbyNoFailover - 未启用故障转移，设备未在传递流量。这可能会在待机设备上存在阈值以上的接口故障时发生。<br>对于聚类，关 **state**键字显示以下值：<br>• control node<br>• data node<br>例如，如果您设置 **prompthostnamecluster-unitstate**，那么在提示符“ciscoasa/cl2/data>”中，主机名是 ciscoasa，单元名称是 cl2，状态名称是 data |

## Command Default

默认提示符是主机名。在多情景模式下，主机名后跟当前情景名称 (*hostname* /*context* )。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 全局配置 | • 是 | • 支持 | • 支持 | — | • 是 |

**Command History**

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |
| 9.0(1) | 该 **cluster-unit** 选项已添加。已更新集群的 **state** 关键字。 |
| 9.19(1) | 对于集群， **state** 显示已从 **主设备** 和 **从属设备** 更改为 **控制节点** 和 **数据节点**。 |

**使用指南**

输入关键字的顺序确定提示符中各元素的顺序（各元素以斜线 (/) 分隔）。

在多情景模式中，您可以在登录到系统执行空间或管理情景时查看扩展的提示符。在非管理情景中，您仅可看到默认提示符，即主机名和情景名称。

利用为提示符添加信息这项功能，可以大体了解在您有多个模块时登录哪一台 ASA。故障转移起价你，如果两台 ASA 具有相同的主机名，则此功能非常有用。

**CR_Examples**

以下示例显示提示中可用于故障转移的所有可用元素：

```
ciscoasa(config)# prompt hostname context slot state priority
```

提示符更改为以下字符串：

```
ciscoasa/admin/pri/act(config)#
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| 清除配置提示 | 清除配置的提示。 |
| **showrunning-configprompt** | 显示配置的提示。 |

# propagate sgt

要在接口上启用安全组标记（称为 **sgt**）的传播，请在 cts 手动接口配置模式下使用 **propagatesgt** 命令。要在接口上禁用安全组标记（称为 **sgt**）的传播，请使用此命令的 **no** 形式。

**propagatesgt**
**nopropagatesgt**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下，传送被启用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Cts 手动接口配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.3(1) | 添加了此命令。 |

## 使用指南

此命令可在 CTS 第 2 层 SGT 实施中启用和禁用安全组标记的传播。

**限制**

- 仅支持物理接口、VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI、TVI 和 VNI。

## CR_Examples

以下示例启用第 2 层 SGT 实施接口并指示未传播 SGT：

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

## Related Commands

| 命令 | 说明 |
|---|---|
| cts manual | 启用第 2 层 SGT 强制并进入 cts 手动接口配置模式。 |

| 命令 | 说明 |
| --- | --- |
| **policystaticsgt** | 将策略应用于手动配置的 CTS 链接。 |

# protocol

要为 IKEv2 连接指定 IPsec 提议的协议和加密类型，请在 IPsec 提议配置模式下使用 **protocol** 命令。如要删除协议和加密类型，请使用该命令的 no 形式：

**protocol**
**esp**{**encryption**{**des**|**3des**|**aes**|**aes-192**|**aes-256**|**aes-gcm**|**aes-gcm-192**|**aes-gcm-256**|**aes-gmac**|**aes-gmac-192**|**aes-gmac-256**|**null**} |**integrity**{**md5**|**sha-1**|**sha-256**|**sha-384**|**sha-512** |**null**}
**no protocol**
**esp**{**encryption**{**des**|**3des**|**aes**|**aes-192**|**aes-256**|**aes-gcm**|**aes-gcm-192**|**aes-gcm-256**|**aes-gmac**|**aes-gmac-192**|**aes-gmac-256**|**null**} |**integrity**{**md5**|**sha-1**|**sha-256**|**sha-384**|**sha-512** |**null**}

## Syntax Description

| | |
|---|---|
| esp | 指定封装安全有效负载 (ESP) IPsec 协议（当前唯一支持的 IPsec 协议）。 |
| **des** | 为 ESP 指定 56 位 DES-CBC 加密。 |
| **3des** | （默认）为 ESP 指定三重 DES 加密算法。 |
| **aes** | 为 ESP 指定带有 128 位密钥加密的 AES。 |
| **aes-192** | 为 ESP 指定带有 192 位密钥加密的 AES。 |
| **aes-256** | 为 ESP 指定带有 256 位密钥加密的 AES。 |
| **aes-gcm** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **aes-gcm-192** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **aes-gcm-256** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **aes-gmac** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **aes-gmac-192** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **aes-gmac-256** | 指定要使用的 AES-GCM 或 AES-GMAC 算法。 |
| **null** | 不对 ESP 使用加密。 |
| integrity | 指定 IPsec 协议的完整性算法。 |
| **md5** | 指定ESP完整性保护的md5算法。 |
| **sha-1** | （默认）指定美国联邦信息处理标准 (FIPS) 中定义的安全散列算法 (SHA) SHA-1，用于 ESP 完整性保护。 |
| **sha-256** | 指定要用作 IPsec 完整性算法的算法。 |
| **sha-384** | 指定要用作 IPsec 完整性算法的算法。 |
| **sha-512** | 指定要用作 IPsec 完整性算法的算法。 |

| | |
|---|---|
| **null** | 选择是否将 AES-GCM/GMAC 配置为加密算法。 |

**Command Default**

IPsec 提议的默认设置是加密类型 3DES 和完整性类型 SHA-1。

**Command Modes**

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| IPsec 提议配置 | • 是 | • 支持 | • 支持 | — | — |

**Command History**

| 版本 | 修改 |
|---|---|
| 8.4(1) | 添加了此命令。 |
| 9.0(1) | 添加了对 AES-GCM 或 AES-GMAC 算法的支持。增加了选择要用作 IPsec 完整性算法的算法的功能。 |

**使用指南**

IKEv2 IPsec 提议可以有多个加密和完整性类型。使用此命令可指定类型，这将允许对等体根据需要进行选择。

如果将 AES-GMC/GMAC 配置为加密算法，则必须选择空完整性算法。

**CR_Examples**

以下示例创建 IPsec 提议 proposal_1，配置 ESP 加密类型 DES 和 3DES，并指定用于完整性保护的加密算法 MD5 和 SHA-1：

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **cryptoikev2enable** | 在 IPsec 对等体通信的接口上启用 ISAKMP IKEv2 协商。 |
| **cryptoipsecikev2ipsec-proposal** | 创建 IPsec 提案并进入 IPsec 提案配置模式，您可以在其中为提案指定多种加密和完整性类型。 |
| **showrunning-configipsec** | 显示所有转换集的配置。 |
| **cryptomapsettransform-set** | 指定要在加密映射条目中使用的转换集。 |
| **cryptodynamic-mapsettransform-set** | 指定要在动态加密映射条目中使用的转换集。 |
| **showrunning-configcryptomap** | 显示加密映射配置。 |

| 命令 | 说明 |
| --- | --- |
| show running-config crypto dynamic-map | 显示动态加密映射配置。 |

# protocol-enforcement

要启用域名、标签长度和格式检查（包括压缩和循环指针检查），请在参数配置模式下使用**protocol-enforcement**命令。要禁用协议执行，请使用此命 **no** 令的形式。

**protocol-enforcement**
**no protocol-enforcement**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下启用协议实施。配置**inspectdns**后，即使未定义**policy-maptypeinspectdns**，也可以启用此功能。要禁用，必须在策略映射配置中明确声明**noprotocol-enforcement**。如果未配置**inspectdns**，则不执行 NAT 重写。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

在某些情况下，即使禁用了 命令，协议实施仍会执行。当出于其他目的（例如DNS资源记录分类、NAT 或 TSIG 检查）需要解析 DNS 资源记录时，会发生这种情况。

## CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用协议实施：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-enforcement
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class** | 在策略映射中标识类映射名称。 |
| **class-maptypeinspect** | 创建检查类映射以匹配特定于应用的流量。 |
| **policy-map** | 创建第 3/4 层策略映射。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configpolicy-map** | 显示所有当前的策略映射配置。 |

# protocol http

要将 HTTP 指定为用于检索 CRL 的允许分发点协议，请在 ca-crl 配置模式下使用 **protocolhttp**命令。要将 HTTP 作为允许的 CRL 检索方法删除，请使用此命令的 **no** 形式。

**protocol http**
**no protocol http**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认设置是允许 HTTP。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Ca-crl 配置 | • 是 | • 支持 | • 支持 | • 支持 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

如果使用此命令，请务必将 HTTP 规则分配给公共接口过滤器。CRL 分发点的内容根据权限确定检索方法（HTTP、LDAP 和/或 SCEP）。

## CR_Examples

以下示例进入 ca-crl 配置模式，并允许 HTTP 作为检索信任点集中式 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **crlconfigure** | 进入 ca-crl 配置模式。 |
| **cryptocatrustpoint** | 进入 trustpoint 配置模式。 |
| **protocolldap** | 指定 LDAP 作为 CRL 的检索方法。 |
| **protocolscep** | 指定 SCEP 作为 CRL 的检索方法。 |

# protocol ldap

要将 LDAP 指定为用于检索 CRL 的分发点协议，请在 ca-crl 配置模式下使用 **protocolldap**命令。CRL 分发点的内容根据权限确定检索方法（HTTP、LDAP 和/或 SCEP）。

要将 LDAP 协议作为允许的 CRL 检索方法删除，请使用此命令的 **no** 形式。

**protocol ldap**
**no protocol ldap**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认设置是允许 LDAP。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| crl 配置 | • 是 | • 支持 | • 支持 | • 支持 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## CR_Examples

以下示例进入 ca-crl 配置模式，并允许 LDAP 作为检索信任点集中式 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **crlconfigure** | 进入 ca-crl 配置模式。 |
| **cryptocatrustpoint** | 进入 trustpoint 配置模式。 |
| **protocolhttp** | 指定 HTTP 作为 CRL 的检索方法 |
| **protocolscep** | 指定 SCEP 作为 CRL 的检索方法 |

# protocol-object

要将协议对象添加到协议对象组，请在协议配置模式下使用 protocol-object 命令。要删除端口对象，请使用此命令的 **no** 形式。

**protocol-object***protocol*
**no protocol-object***protocol*

## Syntax Description

| | |
|---|---|
| protocol | 协议名称或编号。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 协议配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## 使用指南

**protocol-object** 命令与 **object-group** 命令配合使用，以在协议配置模式下定义协议对象。

可以使用 *protocol* 参数指定 IP 协议名称或编号。udp 协议编号为 17，tcp 协议编号为 6，egp 协议编号为 47。

## CR_Examples

以下示例显示如何定义协议对象：

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **clearconfigureobject-group** | 从配置中删除所有对象组命令。 |
| **group-object** | 添加网络对象组。 |
| **network-object** | 向网络对象组添加网络对象。 |
| **object-group** | 定义对象组以优化您的配置。 |
| **showrunning-configobject-group** | 显示当前对象组。 |

# protocol scep

要指定 SCEP 作为用于检索 CRL 的分发点协议，请在 crl 配置模式下使用 **protocolscep**命令。CRL 分发点的内容根据权限确定检索方法（HTTP、LDAP 和/或 SCEP）。

要将 SCEP 协议从允许的 CRL 检索方法中删除，请使用此命令的 **no** 形式。

**protocol scep**
**no protocol scep**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认设置是允许 SCEP。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Crl 配置 | • 是 | • 支持 | • 支持 | • 支持 | • 支持 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |

## CR_Examples

以下示例进入 ca-crl 配置模式，并允许 SCEP 作为检索信任点集中器的 CRL 的分发点协议：

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **crlconfigure** | 进入 ca-crl 配置模式。 |
| **cryptocatrustpoint** | 进入 trustpoint 配置模式。 |
| **protocolhttp** | 指定 HTTP 作为 CRL 的检索方法。 |
| **protocolldap** | 指定 LDAP 作为 CRL 的检索方法。 |

# protocol shutdown

要禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接关系并清除 IS-IS LSP 数据库，请在 **protocolshutdown**路由器 isis 配置模式下使用该命令。要重新启用 IS-IS 协议，请使用此命令的 **no** 形式

**protocol shutdown**
**no protocol shutdown**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

此命令没有默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 路由器 isis 配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(1) | 添加了此命令。 |

## 使用指南

此命令允许您禁用特定路由实例的 IS-IS 协议，而无需删除任何现有的 IS-IS 配置参数。输入该命令后，IS-IS **protocolshutdown**协议继续在 ASA 上运行，并且可以使用当前的 IS-IS 配置，但 IS-IS 不会在任何接口上形成任何邻接关系，并且还会清除 IS-IS LSP 数据库。

如果要禁用特定接口的 IS-IS 协议，请使用该 **isisprotocolshutdown**命令。

## CR_Examples

以下示例为特定路由实例禁用 IS-IS 协议：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

## Related Commands

# protocol-violation

要定义 HTTP 和 NetBIOS 检测中发生协议违规时的操作，请在参数配置模式下使用 **protocol-violation** 命令来定义检测的操作。要禁用此功能，请使用此**no** 命令的形式。

**protocol-violationaction**［**drop**［**log**］ ｜**log**］
**no protocol-violationaction**［**drop**［**log**］ ｜**log**］

## Syntax Description

| | |
|---|---|
| 丢弃 | 指定丢弃不符合协议的数据包。 |
| *log* | 指定记录协议违规。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |

## 使用指南

可以在 HTTP 或 NetBIOS 策略映射中配置此命令。当 HTTP 或 NetBIOS 解析器无法在消息的前几个字节中检测到有效的 HTTP 或 NetBIOS 消息时，将发出系统日志。例如，当分块编码格式错误且无法解析消息时，会发生这种情况。

## CR_Examples

以下示例显示如何在策略映射中设置针对协议违规的操作：

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **class** | 在策略映射中标识类映射名称。 |
| **class-maptypeinspect** | 创建检查类映射以匹配特定于应用的流量。 |

| 命令 | 说明 |
| --- | --- |
| **policy-map** | 创建第 3/4 层策略映射。 |
| **showrunning-configpolicy-map** | 显示所有当前的策略映射配置。 |

# proxy-auth

要将隧道组标记为特定代理身份验证隧道组，请在 webvpn 配置模式下使用 **proxy-auth** 命令。

**proxy-auth**[**sdi**]

## Syntax Description

| | |
|---|---|
| **sdi** | 将 RADIUS/TACACS SDI 代理消息解析为本机 SDI 指令。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Webvpn 配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |

## 使用指南

使用 **proxy-auth** 命令启用将 aaa-server 代理身份验证文本消息解析为本地协议指令。

# proxy-auth_map sdi

要将 RADIUS 代理服务器返回的 RADIUS 质询消息映射到本地 SDI 消息，请在 aaa-server 配置模式下使用 **proxy-auth_mapsdi** 命令。

**proxy-auth_mapsdi**［**sdi_message**］［**radius_challenge_message**］

## Syntax Description

| | |
|---|---|
| **radius_challenge_message** | 指定用于映射特定 SDI 消息的 RADIUS 质询消息，可以是以下任意消息：<br>• new-pin-meth - 新的 PIN 码方式，[默认值] 是否要输入自己的 PIN 码<br>• new-pin-reenter - 重新输入新 PIN，[默认] 重新输入 PIN：<br>• new-pin-req - 请求的新 PIN，[默认] 输入新的字母数字 PIN<br>• new-pin-sup - 提供的新 PIN 码，[默认值] 请记住您的新 PIN 码<br>• new-pin-sys-ok - 接受新 PIN，[默认值] 接受新 PIN<br>• next-ccode-and-reauth - 在更改令牌时重新进行身份验证，[默认]使用下一个卡代码的新 PIN<br>• 下一个代码 - 提供不带 PIN 的令牌代码，[默认] 输入下一个密码<br>• ready-for-sys-pin - 接受系统生成的 PIN，[默认值] 接受系统生成的 PIN |
| sdi_message | 指定本地 SDI 消息。 |

## Command Default

ASA 上的默认映射对应于思科 ACS 上的默认设置（包括系统管理、配置和 RSA SecureID 提示），这些设置也与 RSA 身份验证管理器上的默认设置同步。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| AAA服务器配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |

## 使用指南

要启用对来自 RADIUS 代理的 RADIUS 质询消息的解析和映射，您必须在隧道组配置模式下启用 **proxy-auth** 命令。然后将使用默认映射值。您可以使用 **proxy-auth_map** 命令更改默认映射值。

远程用户通过 Secure Client 连接到 ASA，并尝试使用 RSA SecurID 令牌进行身份验证。ASA 可配置为使用 RADIUS 代理服务器，而 ASA 则与关于该身份验证的 SDI 服务器进行通信。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。当 ASA 直接与 SDI 服务器通信时的消息文本与 ASA 通过 RADIUS 代理通信时的消息文本不同。

因此，为了作为 的本地 SDI 服务器出现 Secure Client，ASA 必须解释来自 RADIUS 服务器的消息。此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。否则，向远程客户端用户显示的提示可能不适用于身份验证期间所需的操作。可 Secure Client 能无法响应，并且身份验证可能会失败。

## Related Commands

| 命令 | 说明 |
|---|---|
| **proxy-auth** | 启用来自 RADIUS 代理的 RADIUS 质询消息的解析和映射。 |

# proxy-bypass

要将 ASA 配置为执行最小内容重写并指定要重写的内容类型（外部链路和/或 XML），请在 webvpn 配置模式下使用 **proxy-bypass** 命令。要禁用代理绕过，请使用命 **no**令的形式。

**proxy-bypassinterface***interfacename* { **port***portnumber* | **path-mask***path mask* } **target***url* [ **rewrite** { **link** | **xml** | **none** ] }
**no proxy-bypassinterface***interfacename* { **port***portnumber* | **path-mask***path mask* } **target***url* [ **rewrite** { **link** | **xml** | **none** ] }

## Syntax Description

| | |
|---|---|
| 主机 | 标识要将流量转发到的主机。使用主机 IP 地址或主机名。 |
| interface | 标识用于代理绕行的 ASA 接口。 |
| *interfacename* | 通过名称指定 ASA 接口。 |
| **link** | 指定绝对外部链接的重写。 |
| **none** | 指定不重写。 |
| 路径掩码 | 指定要匹配的模式。 |
| 路径掩码 | 指定要匹配的模式，可以包含正则表达式。您可以使用以下通配符：<br>* - 匹配所有内容。此通配符不能单独使用。它必须附带字母数字字符串。<br>? —匹配任意单个字符。<br>[!seq] — 匹配任何不按顺序的字符。<br>[seq] — 匹配序列中的任意字符。<br>最多 128 个字节。 |
| **port** | 确定为代理绕行保留的端口。 |
| 端口数值 | 指定为代理绕行保留的高位端口。端口范围为 20000-21000。一个端口只能用于一个代理绕行规则。 |
| **rewrite** | （可选）指定其他重写规则：无或 XML 和链接的组合。 |
| **target** | 标识要将流量转发到的远程服务器。 |
| *url* | 以 **http(s)://***Fully_qualified_domain_name*[:*port*] 格式输入URL。最多 128 个字节。HTTP 的端口为 80，HTTPS 的端口为 443，除非您指定其他端口。 |
| **xml** | 指定重写 XML 内容。 |

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| WebVPN 配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |

## 使用指南

将代理绕行用于可更好地抑制内容重写的应用和 Web 资源。proxy-bypass 命令确定如何处理通过 ASA 传输的特定 Web 应用。

您可以多次使用此命令。配置条目的顺序并不重要。接口和路径掩码或接口和端口将唯一标识代理绕行规则。

如果您使用端口而不是路径掩码来配置代理旁路，则根据您的网络配置，您可能需要更改防火墙配置以允许这些端口访问 ASA。使用路径掩码可避免此限制。但请注意，路径掩码可能会发生变化，因此您可能需要使用多个路径掩码语句来穷尽所有可能性。

路径是 URL 中 .com 或 .org 或其他类型域名之后的任何内容。例如，在 URL www.example.com/hrbenefits 中，*hrbenefits* 就是路径。同样，对于 URL www.example.com/hrinsurance，*hrinsurance* 就是路径。如果要对所有 hr 站点使用代理绕过，则可以使用 * 通配符来避免多次使用该命令，如下所示：/hr*。

## CR_Examples

以下示例显示如何将 ASA 配置为使用端口 20001 进行 webvpn 接口上的代理旁路（使用 HTTP 及其默认端口 80）将流量转发至 example.com 并重写 XML 内容。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

下一个示例显示如何配置 ASA 以在外部接口上将路径掩码用于代理绕行，使用 HTTP 及其默认端口 443 将流量转发到 example.com，并重写 XML 和链接内容。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **apcf** | 指定用于特定应用的非标准规则。 |
| rewrite | 确定流量是否通过 ASA。 |

# proxy-ldc-issuer

要颁发 TLS 代理本地动态证书，请在 crypto ca trustpoint 配置模式下使用 proxy-ldc- issuer 命令。要删除配置，请使用此命令 **no**的形式。

**proxy-ldc-issuer**
**no proxy-ldc-issuer**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Crypto ca trustpoint 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

使用 proxy-ldc- issuer 命令可颁发 TLS 代理本地动态证书。proxy-ldc- issuer 命令授予加密信任点作为本地 CA 的角色来颁发 LDC，该命令可从 crypto ca trustpoint 配置模式访问。

proxy-ldc-issuer 命令为该信任点定义了本地 CA 角色，以便为 TLS 代理颁发动态证书。此命令只能在使用“enrollment self”的信任点下配置。

## CR_Examples

以下示例显示如何创建内部本地CA来签署电话的LDC。此本地CA创建为启用了 proxy-ldc-issuer 的常规自签名信任点。

```
ciscoasa(config)# crypto ca trustpoint ldc_server
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| ctl-provider | 定义CTL提供程序实例，然后进入提供程序配置模式。 |
| **servertrust-point** | 指定要在 TLS 握手期间呈现的代理信任点证书。 |
| **showtls-proxy** | 显示 TLS 代理。 |
| tls-proxy | 定义 TLS 代理实例并设置最大会话数。 |

# proxy paired

要为 Azure 网关负载均衡器 (GWLB) 将 VNI 接口设置为 ASA Virtual 的配对代理模式，请在接口配置模式下使用 **proxy paired** 命令。要删除代理，请使用此命 **no**令的形式。

**proxy paired**
**no proxy paired**

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.19(1) | 添加了此命令。 |

## 使用指南

在 Azure 服务链中，ASA 虚拟充当透明网关，可以拦截互联网和客户服务之间的数据包。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

## CR_Examples

以下示例为 Azure GWLB 配置 VNI 1 接口：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **debug vxlan** | 调试 VXLAN 流量。 |
| **encapsulation vxlan** | 将 NVE 实例设置为 VXLAN 封装。 |

| 命令 | 说明 |
| --- | --- |
| **external-port** | 设置外部 VXLAN 端口。 |
| **external-segment-id** | 指定 VNI 接口的 VXLAN 外部段 ID。 |
| **inspect vxlan** | 强制遵守标准 VXLAN 报头格式。 |
| **interface vni** | 创建用于 VXLAN 标记的 VNI 接口。 |
| **internal-port** | 设置内部 VXLAN 端口。 |
| **internal-segment-id** | 指定 VNI 接口的 VXLAN 内部段 ID。 |
| **nve** | 指定网络虚拟化终端实例。 |
| **peer ip** | 手动指定对等 VTEP IP 地址。 |
| **show interface vni** | 显示VNI接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。 |
| **show nve** | 显示NVE接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。 |
| **source-interface** | 指定 VTEP 源接口。 |
| **vtep-nve** | 将 VNI 接口与 VTEP 源接口相关联。 |
| **vxlan port** | 设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。 |

# proxy-server (已弃用)

要为以下项下的电话代理功能配置 HTTP 代理（该功能已写入 IP 电话的配置文件）：<proxyServerURL>标记，请在电话代理配置模式下使用 **proxy-server** 命令。要从电话代理中删除 HTTP 代理配置，请使用此命令的 **no**形式。

**proxy-server address***ip_addresslisten_port* [ *ifc* ] **interface**
**no proxy-server address***ip_addresslisten_port* [ *ifc* ] **interface**

## Syntax Description

| | |
|---|---|
| **interface***ifc* | 在 ASA 上指定 HTTP 代理所在的接口。 |
| *ip_address* | 指定 HTTP 代理的 IP 地址。 |
| 侦听端口 | 指定HTTP代理的侦听端口。如果未指定，则默认为8080。 |

## Command Default

如果未指定侦听端口，则默认情况下会将端口配置为 8080。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 电话代理配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(4) | 命令已添加。 |
| 9.4(1) | 此命令与所 **phone-proxy**有模式命令一起已被弃用。 |

## 使用指南

为电话代理设置代理服务器配置选项，可以在 DMZ 或外部网络上使用 HTTP 代理，其中的所有 IP 电话 URL 都将定向到电话上服务的代理服务器。此设置容纳不允许返回公司网络的非安全 HTTP 流量。

根据 IP 电话和 HTTP 代理服务器所在位置，输入的 *ip_address* 应该是全局 IP 地址。

如果代理服务器位于 DMZ 中而 IP 电话位于网络外部，则 ASA 会查找以查看是否存在 NAT 规则，并使用全局 IP 地址写入配置文件。

当主机名可由 ASA 解析为 IP 地址（例如，配置了 DNS 查找）时，您可以在 *ip_address* 参数中输入主机名，因为 ASA 会将主机名解析为 IP 地址。

默认情况下，“企业参数”下配置的电话 URL 参数在 URL 中使用 FQDN。如果 HTTP 代理的 DNS 查找无法解析 FQDN，则可能需要更改这些参数以使用 IP 地址。

要确保代理服务器 URL 已正确写入 IP 电话配置文件，请在以下路径下检查 IP 电话上的 URL：设置 (Settings) =“设备配置”(Device Configuration) =“HTTP 配置”(HTTP configuration) =“代理服务器 URL”(Proxy Server URL)。

电话代理不会检查此流向代理服务器的 HTTP 流量。

如果 ASA 位于 IP 电话和 HTTP 代理服务器的路径中，请使用现有的调试技术（例如系统日志和捕获）对代理服务器进行故障排除。

使用电话代理时，您只能配置一个代理服务器，您可以在其中选择一个代理服务器。配置代理服务器

## CR_Examples

以下示例显示如何使 **proxy-server** 用命令为电话代理配置 HTTP 代理服务器：

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **phone-proxy** | 配置电话代理实例。 |

# proxy single-arm

要为 VXLAN VNI 接口启用单臂代理，请在接口配置模式下使用 **proxy single-arm**命令。要禁用代理，请使用此命 **no**令的形式。

**proxy single-arm**
**no proxy single-arm**

此命令没有任何参数或关键字。

## Command Default

无默认行为或值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | • — | • 是 | • — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.17(1) | 我们添加了此命令。 |

## 使用指南

AWS网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA virtual支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。此使用案例要求您将 VNI 接口配置为单臂代理。另请确保启用 **same-security-traffic permit intra-interface**，以允许流量从 VTEP 源接口流出。

## CR_Examples

以下示例将 VNI 接口配置为单臂代理：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **debugvxlan** | 调试 VXLAN 流量。 |

| 命令 | 说明 |
| --- | --- |
| **encapsulationgeneve** | 将 NVE 实例设置为 Geneve 封装。 |
| **interfacevni** | 创建用于 VXLAN 标记的 VNI 接口。 |
| **nve** | 指定网络虚拟化终端实例。 |
| **nve-only** | 将 VXLAN 源接口指定为仅限 NVE。 |
| **showinterfacevni** | 显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。 |
| **shownve** | 显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。 |
| **source-interface** | 指定 VTEP 源接口。 |
| **vtep-nve** | 将 VNI 接口与 VTEP 源接口相关联。 |

# ptp domain

要指定 ISA 3000 上所有 PTP 端口的域编号，请在特权 EXEC 或全局配置模式下使用 **ptpdomain** 命令。域编号，范围为 0 至 255；默认值为 0。在与配置的域不同的域上接收到的数据包将被视为常规多播数据包，并且不会经过任何 PTP 处理。要将域号重置为默认值 0，请使用此命令的 **no**形式。

**ptp domain***domain_num*
**no ptp domain**

注释 此命令仅在 Cisco ISA 3000 设备上可用。

## Syntax Description

| | |
|---|---|
| **domain***domain_num* | 为 ISA 3000 上所有启用 PTP 的端口指定域编号。 |

## Command Default

默认 **ptpdomain**数量为 0。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | • 支持 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.7(1) | 添加了此命令。 |

## 使用指南

该命令也 **ptpdomain** 可在全局配置模式下使用。

## CR_Examples

以下示例展示如何使用 **ptpdomain**命令将 PTP 域编号设置为 127：

```
ciscoasa# ptp domain 127
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **showptpport** | 显示PTP接口/端口信息。 |

# ptp enable

要在 ISA 3000 的接口上启用 PTP，请在接口配置模式下使用该 **ptpenable**命令。使用 **ptpmode** 命令指定将启用 PTP 的模式。要禁用接口上的 PTP，请使用此命 **no**令的形式。出入该接口的 PTP 数据包将像常规组播数据包一样处理。

**ptp enable**
**no ptp enable**

注释 此命令仅在 Cisco ISA 3000 设备上可用。

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下，在透明模式下对所有 ISA 3000 接口启用 PTP。在路由模式下，必须添加必要的配置以确保允许 PTP 数据包通过设备。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 接口配置 | • 是 | • 支持 | • 支持 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.7(1) | 添加了此命令。 |

## 使用指南

该命令只能在接口配置模式下输入。

仅允许在物理接口上使用此命令。不允许在子接口、其他虚拟接口或管理接口上使用此类型。

加入父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。

如果未在任何模式下启用 PTP，则接受此命令，但不会产生任何效果。将发出警告。

## Related Commands

| 命令 | 说明 |
|---|---|
| **showptpclock** | 显示PTP时钟属性。 |

# ptp 模式

要在 ISA 3000 上指定 PTP 时钟模式，请在特权 EXEC 或全局配置模式下使用 **ptpmode** 命令。要在所有接口上禁用 PTP，请使用此命 **no**令的形式。

**ptp modee2etransparent**
**no ptp mode**

注释 此命令仅在 Cisco ISA 3000 设备上可用。

## Syntax Description

| | |
|---|---|
| **e2etranparent** | 在 ISA 3000 上所有启用 PTP 的接口上启用端到端透明模式。 |

## Command Default

默认情况下，端到端透明模式已禁用。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | • 支持 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.7(1) | 添加了此命令。 |

## 使用指南

禁用端到端透明模式时，系统将像处理任何其他组播数据包一样处理所有 PTP 数据包。这相当于 转发 模式。

该命令也 **ptpmode** 可在全局配置模式下使用。

## CR_Examples

以下示例展示如何使用 **ptpmode**命令将 PTP 时钟模式设置为端到端透明模式：

```
ciscoasa# ptp mode e2etranparent
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **showptpinternal-info** | 显示 PTP 统计数据和计数器信息。 |

# public-key

要指定思科 Umbrella 所需的证书验证的 DNSCrypt 提供程序公钥，请在 Umbrella 配置模式下使用 **public-key** 命令。使用此命 **no**令的形式可以删除密钥并使用默认密钥。

**public-key***dnscrypt_key*
**no public-key** [*dnscrypt_key*]

## Syntax Description

| | |
|---|---|
| *dnscrypt_key* | Cisco Umella 服务器用于 DNSCrypt 的公钥。只有在用于 Cisco Umbrella 的 DNS 检测策略映射中启用 dnscrypt 时，此项才与密钥相关。<br><br>密钥是一个 32 字节的十六进制值。在 ASCII 中输入十六进制值，每个 2 字节使用一个冒号分隔符。密钥长度为 79 个字节。从思科 Umbrella 获取此密钥。 |

## Command Default

将使用默认密钥。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Umbrella 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.10(1) | 添加了此命令。 |

## 使用指南

如果想要在 DNS 检测策略映射中启用 DNSCrypt DNS，则可以选择配置用于证书验证的 DNSCrypt 提供商公钥。如果未配置密钥，则使用当前分布分发的默认公钥进行验证。

仅当 Cisco Umbrella 更改其用于 DNSCrypt 加密的公钥时，才需要配置密钥。

## CR_Examples

以下示例配置与 Cisco Umbrella 配合使用的公钥。示例还显示如何在默认 DNS 检测策略映射（该映射用于全局 DNS 检测）中启用 DNSCrypt。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)#
public-keyB735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
```

```
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **dnscrypt** | 为设备和思科 Umbrella 之间的连接启用 DNScrypt 加密。 |
| **inspectdns** | 启用 DNS 检测。 |
| **policy-maptypeinspectdns** | 创建 DNS 检测策略映射。 |
| **timeoutedns** | 配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。 |
| **token** | 确定在思科 Umbrella 中注册时所需的 API 令牌。 |
| **umbrella-global** | 配置思科 Umbrella 全局参数。 |

# publish-crl

要允许其他 ASA 验证本地 CA 颁发的证书的吊销状态，请在 ca-server 配置模式下使用 **publish-crl** 命令允许直接从 和 ASA 上的接口下载 CRL。要使 CRL 不可下载，请使用此命令的 **no** 形式。

[**no**] **publish-crlinterface***interface* [**port***portnumber*]

## Syntax Description

| | |
|---|---|
| **interface***interface* | 指定用于接口的 *nameif* ，例如gigabitethernet0/1。有关详细信息，请参阅 interface 命令。 |
| **port***portnumber* | （可选）指定接口设备期望在其上下载 CRL 的端口。端口号可以在 1-65535 范围内。 |

## Command Default

默认状 **publish-crl**态为 。 **nopublish** TCP 端口 80 是 HTTP 的默认端口。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| Ca-server配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |

## 使用指南

默认情况下，CRL 不可访问。您必须在需要的接口和端口上启用对 CRL 文件的访问。

TCP 端口 80 是 HTTP 默认端口号。如果配置非默认端口（端口 80 除外），请确保 **cdp-url** 配置包含新端口号，以便其他设备知道要访问此特定端口。

CRL 分发点 (CDP) 是 CRL 在本地 CA ASA 上的位置。您使用 **cdp-url** 命令配置的 URL 会嵌入到任何已颁发的证书中。如果没有为 CDP 配置特定位置，则默认 CDP URL 为：http://hostname.domain/+CSCOCA+/asa_ca.crl。

如果在同一接口上启用无客户端 SSL VPN，则 HTTP 重定向和 CRL 下载请求将由同一 HTTP 侦听程序处理。侦听程序检查传入 URL，如果其与使用 **cdp-url** 命令配置的 URL 匹配，则下载 CRL 文件。如果 URL 与 **cdp-url** 命令不匹配，则连接将重定向到 HTTPS（如果启用了 HTTP 重定向）。

## CR_Examples

在 ca-server 配置模式下输入的 **publish-crl** 命令示例启用外部接口的端口 70 以进行 CRL 下载：

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **cdp-url** | 为自动生成的 CRL 指定特定位置。 |
| **showinterface** | 显示接口的运行时间状态和统计信息。 |

# pwd

要显示当前工作目录，请在特权 EXEC 模式下使用 **pwd**命令。

**pwd**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

根目录 (/) 为默认值。

## Command Modes

下表展示可输入命令的模式：

| 命令模式 | 防火墙模式 | | 安全情景 | | |
|---|---|---|---|---|---|
| | 路由 | 透明 | 一个 | 多个 | |
| | | | | 情景 | 系统 |
| 特权 EXEC | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0 | 添加了此命令。 |

## 使用指南

此命令在功能上与 **dir** 命令类似。

## CR_Examples

以下示例显示如何显示当前工作目录：

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **cd** | 将当前工作目录更改为指定的目录。 |
| **dir** | 系统随即会显示目录的内容。 |
| **more** | 显示文件的内容。 |

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。