# n


- nac-authentication-server-group (已弃用)， 第 3 页
- nac-policy (已弃用)， 第 5 页
- nac-settings (已弃用)， 第 7 页
- name (dynamic-filter blacklist 或 whitelist)， 第 9 页
- name（全局）， 第 12 页
- nameif， 第 14 页
- names， 第 16 页
- name-separator (pop3s, imap4s, smtps) (已弃用)， 第 18 页
- name-server， 第 20 页
- nat (global)， 第 22 页
- nat (object)， 第 33 页
- nat (vpn load-balancing)， 第 42 页
- nat-assigned-to-public-ip， 第 44 页
- nat-rewrite， 第 47 页
- nbns-server， 第 48 页
- neighbor (router eigrp)， 第 50 页
- neighbor (router ospf)， 第 52 页
- neighbor activate， 第 54 页
- neighbor advertise-map， 第 56 页
- neighbor advertisement-interval， 第 58 页
- neighbor default-originate， 第 60 页
- 邻居描述， 第 62 页
- neighbor disable-connected-check， 第 64 页
- neighbor distribute-list， 第 66 页
- neighbor ebgp-multihop， 第 68 页
- neighbor fall-over bfd (router bgp)， 第 70 页
- neighbor filter-list， 第 72 页
- neighbor ha-mode graceful-restart， 第 74 页
- neighbor local-as， 第 76 页
- neighbor maximum-prefix， 第 80 页

- neighbor next-hop-self， 第 82 页
- neighbor password， 第 84 页
- neighbor prefix-list， 第 87 页
- neighbor remote-as， 第 89 页
- neighbor remove-private-as， 第 91 页
- neighbor route-map， 第 93 页
- neighbor send-community， 第 95 页
- neighbor shutdown， 第 96 页
- neighbor timers， 第 98 页
- neighbor transport， 第 100 页
- neighbor ttl-security， 第 102 页
- neighbor update-source， 第 104 页
- neighbor version， 第 106 页
- neighbor weight， 第 108 页
- nem， 第 110 页
- netmod， 第 111 页
- network (address-family)， 第 113 页
- network (router eigrp)， 第 115 页
- network (router rip)， 第 116 页
- network-acl， 第 118 页
- network area， 第 120 页
- network-object， 第 122 页
- network-service-member， 第 124 页
- nis address， 第 125 页
- nis domain-name， 第 128 页
- nisp address， 第 131 页
- nisp domain-name， 第 134 页
- nop， 第 137 页
- nsf cisco， 第 139 页
- nsf cisco helper， 第 141 页
- nsf ietf， 第 143 页
- nsf ietf helper， 第 145 页
- nt-auth-domain-controller， 第 147 页
- ntp authenticate， 第 149 页
- ntp authentication-key， 第 151 页
- ntp server， 第 153 页
- ntp trusted-key， 第 155 页
- num-packets， 第 157 页
- nve， 第 159 页
- nve-only， 第 161 页

# nac-authentication-server-group (已弃用)

要标识用于网络准入控制安全状态验证的身份验证服务器组，请在 tunnel-group general-attributes 配置模式下使用 **nac-authentication-server-group** 命令。要从默认远程访问组继承身份验证服务器组，请访问要从中继承它的备用组策略，然后使用此命令的 **no**形式。

**nac-authentication-server-group***server-group*
**no nac-authentication-server-group**

## Syntax Description

| | |
|---|---|
| *server-group* | 姿态验证服务器组的名称，使用命令在 ASA 上配 **aaa-serverhost**置。该名称必须与该命令中指定的 server-tag 变量匹配。 |

## Command Default

此命令没有任何参数或关键字。

## 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 |
| 隧道组常规属性配置 | • 是 | • — | • 是 | • — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |
| 8.0(1) | 此命令已弃用。nac-policy-nac-framework 配置模式下的 **authentication-server-group** 命令取而代之。 |

## 使用指南

将至少一个访问控制服务器配置为支持 NAC。使用该 **aaa-server**命令命名 ACS 组。然后使用该 **nac-authentication-server-group**命令，对服务器组使用相同的名称。

## CR_Examples

以下示例将 acs-group1 标识为要用于 NAC 安全状态验证的身份验证服务器组：

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

以下示例从默认远程访问组继承身份验证服务器组。

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **aaa-server** | 创建 AAA 服务器或组的记录，并设置主机特定的 AAA 服务器属性。 |
| 调试 eap | 启用 EAP 事件日志记录以调试 NAC 消息传送。 |
| 调试 EOU | 启用 EAP over UDP (EAPoUDP) 事件日志记录以调试 NAC 消息传送。 |
| 调试 nac | 启用 NAC 事件的日志记录。 |
| **nac** | 在组策略上启用网络准入控制。 |

# nac-policy (已弃用)

注释 此命令的最后支持版本是版本 9.1(1)。

要创建或访问思科网络准入控制 (NAC) 策略并指定其类型，请在全局配置模式下使用 **nac-policy** 命令。要从配置中删除 NAC 策略，请使用此命令的 **no**形式。

**nac-policy***nac-policy-name***nac-framework**
**no nac-policy***nac-policy-name***nac-framework**

## Syntax Description

| | |
|---|---|
| *nac-policy-name* | NAC 策略的名称。输入最多 64 个字符的字符串，为 NAC 策略命名。该 **showrunning-confignac-policy**命令显示安全设备上已存在的每个 NAC 策略的名称和配置。 |
| **nac-framework** | 指定使用 NAC 框架为远程主机提供网络访问策略。网络上必须存在 Cisco 访问控制服务器才能为 ASA 提供 NAC 框架服务。<br>如果指定此类型，提示符表明您处于 config--nac-policy-nac-framework 配置模式。此模式允许配置 NAC 框架策略。 |

## Command Default

此命令没有默认设置。

## 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 |
|---|---|
| 8.0(2) | 添加了此命令。 |
| 9.1(2) | 此命令已弃用。 |

## 使用指南

对要分配给组策略的每个 NAC 设备使用此命令一次。然后使用 **nac-settings** 命令将 NAC 策略分配给每个适用的组策略。设置 IPsec 或思科 AnyConnect VPN 隧道后，ASA 应用与使用的组策略关联的 NAC 策略。

如果 NAC 策略已分配给一个或多个组策略，则无法使用 **nonac-policy***name* 命令将其删除。

## CR_Examples

以下命令创建并访问名为 nac-framework1 的 NAC 框架策略：

```
ciscoasa
(config)
# nac-policy nac-framework1 nac-framework
ciscoasa
(config-nac-policy-nac-framework)
```

以下命令删除名为 nac-framework1 的 NAC 框架策略：

```
ciscoasa
(config)
# no nac-policy nac-framework1
ciscoasa
(config-nac-policy-nac-framework)
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **showrunning-confignac-policy** | 显示 ASA 上每个 NAC 策略的配置。 |
| **shownac-policy** | 显示 ASA 上 NAC 策略使用统计信息。 |
| **clearnac-policy** | 重置 NAC 策略使用统计信息。 |
| **nac-settings** | 将 NAC 策略分配到组策略。 |
| **clearconfigurenac-policy** | 从正在运行的配置中删除所有NAC策略，分配给组策略的策略除外。 |

# nac-settings (已弃用)

注释 此命令的最后支持版本是版本 9.1(1)。

要将 NAC 策略分配给组策略，请在 **nac-settings**策略组配置模式下使用以下命令：

**nac-settings** { **value***nac-policy-name* | **none** }
**no nac-settings** { **value***nac-policy-name* | **none** }

## Syntax Description

| | |
|---|---|
| *nac-policy-name* | 要分配到组策略的 NAC 策略。您命名的 NAC 策略必须存在于 ASA 配置中。该 **showrunning-configNAC-policy**命令显示每个 NAC 策略的名称和配置。 |
| **none** | 从组策略中删除 nac - policy-name 并禁止此组策略使用 NAC 策略。组策略不会从默认组策略继承 nac-settings 值。 |
| **value** | 将要命名的 NAC 策略分配给组策略。 |

## Command Default

此命令没有任何参数或关键字。

## 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 |
| 组策略配置 | • 是 | • — | • 是 | • — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |
| 9.1(2) | 此命令已弃用。 |

## 使用指南

使用 **nac-policy** 命令指定 NAC 策略的名称和类型，然后使用此命令将策略分配给组策略。

该 **showrunning-configNAC-policy**命令显示每个 NAC 策略的名称和配置。

当您为 ASA 分配 NAC 策略时，ASA 会自动为组策略启用 NAC。

## CR_Examples

以下命令从组策略中删除 nac - policy-name。组策略从默认组策略继承了 nac -*settings*值：

```
ciscoasa(config-group-policy)
# no nac-settings
ciscoasa(config-group-policy)
```

以下命令从组策略中删除 nac - policy-name 并禁用此组策略使用 NAC 策略。组策略不会从默认组策略继承 nac-settings 值。

```
ciscoasa(config-group-policy)
# nac-settings none
ciscoasa(config-group-policy)
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **nac-policy** | 创建和访问思科 NAC 策略，并指定其类型。 |
| **showrunning-confignac-policy** | 显示 ASA 上每个 NAC 策略的配置。 |
| **shownac-policy** | 显示 ASA 上 NAC 策略使用统计信息。 |
| **showvpn-session_summary.db** | 显示 IPsec、WebVPN 和 NAC 会话的数量。 |
| **showvpn-session.db** | 显示有关 VPN 会话的信息，包括 NAC 结果。 |

# name (dynamic-filter blacklist 或 whitelist)

要将域名添加到僵尸网络流量过滤器黑名单或白名单，请在 dynamic-filter 黑名单或白名单配置模式下使用**name**命令。要删除名称，请使用**no**此命令的形式。静态数据库允许您通过要列入白名单或黑名单的域名或 IP 地址扩充动态数据库。

**name***domain_name*
**no name***domain_name*

## Syntax Description

| | |
|---|---|
| *domain_name* | 将名称添加到黑名单。可以多次输入此命令以获得多个条目。您最多可以添加 1000 个黑名单条目。 |

## 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 |
| 动态过滤器黑名单或白名单配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.2(1) | 添加了此命令。 |

## 使用指南

进入动态过滤器白名单或黑名单配置模式后，您可以使用 **address** 和 **name** [ 键，手动输入要标记为白名单中的好名称或黑名单中的不良名称的域名或 IP 地址（主机或子网）。 命令。

可以多次输入此命令以获得多个条目。您最多可以添加 1000 个黑名单条目和 1000 个白名单条目。

当您将域名添加到静态数据库时，ASA 会等待 1 分钟，然后发送该域名的 DNS 请求，并将域名/IP 地址对添加到 *DNS* 主机缓存 。（此操作是一个后台进程，不会影响您继续配置 ASA）。

如果没有为ASA配置域名服务器，或域名服务器不可用，则可以启用包含僵尸网络流量过滤器侦听的 DNS 数据包检测（请参阅**inspectdnsdynamic-filter-snooping** 命令）。利用 DNS 监听，当受感染主机发送对静态数据库中的名称的 DNS 请求时，ASA 将在 DNS 数据包内查找域名和关联的 IP 地址，并将名称和 IP 地址添加到 DNS 反向查找缓存。有关 DNS 反向查找缓存的信息，请参阅 **inspectdnsdynamic-filter-snooping** 命令。

DNS 主机缓存中的条目有一个由 DNS 服务器提供的生存时间 (TTL) 值。允许的最大 TTL 值为 1 天（24 小时）；如果 DNS 服务器提供更大的 TTL，则会截断为最大值 1 天。

对于 DNS 主机缓存，在条目超时后，ASA 会定期请求刷新该条目。

## CR_Examples

以下示例为黑名单和白名单创建条目：

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2255.255.255.255
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address** | 将 IP 地址添加到黑名单或白名单。 |
| clear configure dynamic-filter | 清除正在运行的僵尸网络流量过滤器配置。 |
| **cleardynamic-filterdns-snoop** | 清除僵尸网络流量过滤器 DNS 监听数据。 |
| **cleardynamic-filterreports** | 清除僵尸网络流量过滤器报告数据。 |
| **cleardynamic-filterstatistics** | 清除僵尸网络流量过滤器统计信息。 |
| dns domain-lookup | 使 ASA 能够向 DNS 服务器发送 DNS 请求以执行支持的命令的名称查找。 |
| dns server-group | 标识 ASA 的 DNS 服务器。 |
| **dynamic-filterblacklist** | 编辑僵尸网络流量过滤器黑名单。 |
| 动态过滤器数据库获取 | 手动检索僵尸网络流量过滤器动态数据库。 |
| **dynamic-filterdatabasefind** | 搜索域名或 IP 地址的动态数据库。 |
| 动态过滤器数据库清除 | 手动删除僵尸网络流量过滤器动态数据库。 |
| **dynamic-filterenable** | 为一个流量类或为所有流量（如果不指定访问列表）启用僵尸网络流量过滤器。 |
| **dynamic-filterupdater-clientenable** | 启用下载动态数据库。 |
| **dynamic-filteruse-database** | 允许使用动态数据库。 |
| **dynamic-filterwhitelist** | 编辑僵尸网络流量过滤器白名单。 |
| **inspectdnsdynamic-filter-snoop** | 启用包含僵尸网络流量过滤器侦听的 DNS 检查。 |
| **name** | 将名称添加到黑名单或白名单。 |

| 命令 | 说明 |
| --- | --- |
| **showasptabledynamic-filter** | 显示加速安全路径中安装的僵尸网络流量过滤器规则。 |
| **showdynamic-filterdata** | 显示有关动态数据库的信息，包括上次下载动态数据库的时间、数据库的版本、数据库包含的条目数和 10 个示例条目。 |
| **showdynamic-filterdns-snoop** | 显示僵尸网络流量过滤器 DNS 监听摘要，或与 **detail** 关键字一起显示实际 IP 地址和名称。 |
| **showdynamic-filterreports** | 生成有关前 10 个僵尸网络站点、端口和受感染主机的报告。 |
| **showdynamic-filterstatistics** | 显示受僵尸网络流量过滤器监控的连接数，以及其中与白名单、黑名单和灰名单匹配的连接数。 |
| **showdynamic-filterupdater-client** | 显示更新程序服务器的相关信息，包括服务器 IP 地址、ASA 下次与服务器连接的时间和上次安装的数据库版本。 |
| show running-config dynamic-filter | 显示僵尸网络流量过滤器运行配置。 |

# name（全局）

要将名称与 IP 地址相关联，请在全局配置模式下使用 **name** 命令。要禁用文本名称但不将其从配置中删除，请使用此命令的 **no** 形式。

**name***IP* 地址 [ 名称 [ **description** 文本 ] ]
**no name***IP* 地址 [ 名称 [ **description** 文本 ] ]

## Syntax Description

| | |
|---|---|
| **description** | （可选）指定 IP 地址名称说明。 |
| *ip_address* | 指定所命名的主机的 IP 地址。 |
| *name* | 指定分配给 IP 地址的名称。使用字符 a 到 z、A 到 Z、0 到 9、破折号和下划线。 名称不得超过 63 个字符。此外， 名称不能以数字开头。 |
| 文本 | 指定说明的文本。 |

## Command Default

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 |
| 全局配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 7.0(4) | 此命令已增强，包括可选说明。 |
| 8.3(1) | 不能再在 **nat** 命令或 **access-list** 命令中使用命名的 IP 地址；必须改用 **objectnetwork** 名称。虽然对象组中的 **network-object** 命令接受 **objectnetwork** 名称，但您仍然可以使用由 **name** 命令标识的命名 IP 地址。 |

## 使用指南

要启用名称与 IP 地址的关联，请使用 **names** 命令。一个 IP 地址只能关联一个名称。

在使用 **names** 命令之前，必须先使用 **name** 命令。紧随使用 name 命令之后、使用 **writememory** 命令之前，使用 name 命令。

通过 **name** 命令，您可以通过文本名称标识主机并将文本字符串映射到 IP 地址。 **noname** 命令允许您禁用文本名称，但不会将其从配置中删除。使用 **clearconfigurename** 命令清除配置中的名称列表。

要禁用显示 **name** 值，请使用 **nonames** 命令。

name 和 name 命令都会保存在配置中。

name 命令不支持为网络掩码分配名称。例如，以下命令会被拒绝：

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```

注释 需要掩码的所有 命令都无法将名称作为接受的网络掩码来处理。

## CR_Examples

此示例显示 **names** 命令允许您使用 **name** 命令。 **name** 命令用 **sa_inside** 替代对 192.168.42.3 的引用，用 **sa_outside** 替代对 209.165.201.3 的引用。为网络接口分配 IP 地址时，您可以将这些名称与 **ipaddress** 命令配合使用。 **nonames** 命令禁用 **name** 命令值的显示。随后再次使用 **names** 命令可恢复**name** 命令值显示。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearconfigurename** | 从配置中清除名称列表。 |
| **names** | 启用名称与IP地址的关联。 |
| **showrunning-configname** | 显示与IP地址关联的名称。 |

# nameif

要为接口提供名称，请在 **nameif**接口配置模式下使用该命令。要删除名称，请使用**no**此命令的形式。ASA 上的所有配置命令中都会使用接口名称来代替接口类型和 ID（例如，gigabitethernet0/1），因此必须具备接口名称，流量才能通过接口。

**nameif***name*
**no nameif**

## Syntax Description

*name* 设置长度最多为 48 个字符的名称。该名称不区分大小写。

请勿使用“Metrics_History”或“MH”名称；其原因是，ASDM 将接口显示为关闭状态。

请勿使用名称“internal”，因为它会阻止配置其他功能，例如静态 ARP。

## 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 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 此命令已从全局配置命令更改为接口配置模式命令。 |

## 使用指南

对于子接口，在输入 **nameif** 命令之前，必须使用 **vlan** 命令分配 VLAN。

使用一个新值重新输入此命令可更改名称。不要输入该**no**表单，因为该命令会导致所有引用该名称的命令被删除。

## CR_Examples

以下示例将两个接口的名称配置为“inside”和“outside”：

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **clearxlate** | 重置现有连接的所有转换，导致连接重置。 |
| **interface** | 配置接口并进入接口配置模式。 |
| **security-level** | 设置接口的安全级别。 |
| **vlan** | 将 VLAN ID 分配给子接口。 |

# names

要启用名称与 IP 地址的关联，请在全局配置模式下使用 **names** 命令。一个 IP 地址只能关联一个名称。要禁用显示 **name** 值，请使用 **nonames** 命令。

**names**
**no names**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

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 |
| 全局配置 | • 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

要启用名称与 IP 地址的关联，请使用 **names** 命令。一个 IP 地址只能关联一个名称。

在使用 **names** 命令之前，必须先使用 **name** 命令。紧随使用 name 命令之后、使用 **writememory** 命令之前，使用 name 命令。

要禁用显示 **name** 值，请使用 **nonames** 命令。

name 和 name 命令都会保存在配置中。

## CR_Examples

此示例显示 **names** 命令允许您使用 **name** 命令。 **name** 命令用 **sa_inside** 替代对 192.168.42.3 的引用，用 **sa_outside** 替代对 209.165.201.3 的引用。为网络接口分配 IP 地址时，您可以将这些名称与 **ipaddress** 命令配合使用。 **nonames** 命令禁用 **name** 命令值的显示。随后再次使用 **names** 命令可恢复**name** 命令值显示。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
```

```
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearconfigurename** | 从配置中清除名称列表。 |
| **name** | 将名称与 IP 地址相关联。 |
| **showrunning-configname** | 显示与IP地址关联的名称列表。 |
| **showrunning-confignames** | 显示 IP 地址到名称的转换。 |

# name-separator (pop3s, imap4s, smtps) (已弃用)

注释 支持此命令的最后一个版本是版本 9.5(1)。

要指定一个字符作为邮件与 VPN 用户名和密码之间的分隔符，请在相应的邮件代理模式下使用 **name-separator** 命令。要恢复默认的“：”，请使用此命令的 **no**版本。

**name-separator** [*symbol*]
**no name-separator**

## Syntax Description

| | |
|---|---|
| symbol | （可选）分隔邮件和VPN用户名和密码的字符。选项包括“@”、（在）“\|”（竖线）、“:”（冒号）、“#”（散列）、“,”（逗号）和“;”（分号）查找。 |

## Command Default

默认值为“:”（冒号）。

## 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 |
| Pop3s | • 是 | • — | • 是 | • — | — |
| Imap4s | 是 | — | 是 | — | — |
| Smtps | 是 | — | 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.5(2) | 此命令已弃用。 |

## 使用指南

名称分隔符必须与服务器分隔符不同。

## CR_Examples

以下示例显示如何将散列字符 (#) 设置为 POP3S 的名称分隔符：

```
ciscoasa
(config)#
```

```
 pop3s
ciscoasa(config-pop3s)# name-separator #
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **server-separator** | 分隔邮件名称和服务器名称。 |

# name-server

要标识一个或多个 DNS 服务器以便 ASA 可将主机名解析为 IP 地址，请在 dns 服务器组配置模式下使用 **name-server**命令。要删除服务器，请使用此命令的 **no** 形式。

注释 ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，大多数命令都要求您输入 IP 地址，并且只有当您手动配**name**置命令以将名称与IP地址关联并使用该命令启用名称时才能使用名**names**称。

**name-server***ip_address*[*ip_address2*][...][*ip_address6*][*interface_name*]
**no name-server***ip_address*[*ip_address2*][...][*ip_address6*][*interface_name*]

## Syntax Description

| | |
|---|---|
| *interface_name* | （可选）指定ASA与服务器通信的接口名称。如果未指定接口，ASA将检查数据路由表；如果没有匹配项，则会检查仅管理路由表。 |
| *ip_address* | 指定 DNS 服务器 IP 地址。您最多可以指定六个地址，将其作为单独的命令；或者为方便起见，在一个命令中最多指定六个地址，以空格分隔。如果在一个 命令中输入多个服务器，ASA 会将每个服务器保存在配置中的单独命令中。ASA 按顺序尝试每台 DNS 服务器，直至收到响应。 |

## 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 |
| dns server-group 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.1(1) | 添加了此命令。 |
| 9.5(1) | 添加了 *interface_name* 参数。 |

## 使用指南

要在接口上启用 DNS 查找，请配置 **dnsdomain-lookup** 命令。如果不启用 DNS 查找，则不能使用 DNS 服务器。

默认情况下，ASA 使用服务 **dnsserver-groupDefaultDNS**器组来处理传出请求。您可以使用 **dns-group** 命令。其他服务器组可与特定域相关联。与 DNS 服务器组关联的域匹配的 DNS 请求将使用该组。例如，如果您希望发往内部eng.cisco.com服务器的流量使用内部DNS服务器，则可以将eng.cisco.com

映射到内部 DNS 组。与域映射不匹配的所有 DNS 请求都将使用没有关联域的默认 DNS 服务器组。例如，DefaultDNS 组可以包括外部接口上可用的公共 DNS 服务器。可为 VPN 隧道组配置其他 DNS 服务器组。有关详细信息，请参阅 **tunnel-group** 命令。

某些 ASA 功能需要使用 DNS 服务器通过域名访问外部服务器；例如，僵尸网络流量过滤器功能需要 DNS 服务器访问动态数据库服务器并解析静态数据库中的条目；思科智能软件许可需要 DNS 来解析许可证颁发机构地址。通过其他功能，例如 **ping** 或 **traceroute** 命令，可输入要 ping 或 traceroute 的名称，而且 ASA 能够通过与 DNS 服务器进行通信来解析名称。许多 SSL VPN 和证书命令也支持名称。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

如果没有指定接口 **name-server**，ASA 将检查数据路由表；如果没有匹配项，它将检查仅管理路由表。请注意，如果有通过数据接口的默认路由，则所有DNS流量都将与该路由匹配，从不检查管理专用路由表。在此场景中，如果您需要通过管理接口访问服务器，请始终指定 接口。

## CR_Examples

以下示例将三个 DNS 服务器添加到“DefaultDNS”组：

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA 会将配置保存为单独的命令，如下所示：

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

要添加两台其他服务器，可以将它们作为一个 命令输入：

```
ciscoasa(config)# dns server-groupDefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

要删除多个服务器，可以将其作为多个命令或作为一个命令输入，如下所示：

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# noname-server 10.5.1.1 10.8.3.8
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **domain-name** | 设置默认域名。 |
| **retries** | 指定当 ASA 未收到响应时重试 DNS 服务器列表的次数。 |
| **timeout** | 指定尝试下一个 DNS 服务器之前等待的时间量。 |
| **showrunning-configdnsserver-group** | 显示一个或所有现有 dns-server-group 配置。 |

# nat (global)

要为 IPv4、IPv6 或 IPv4 与 IPv6 之间的 NAT (NAT64) 配置两次 NAT，请在全局配置模式下使用 **nat** 命令。要删除两次 NAT 配置，请使用此命 **no**令的形式。

对于静态 NAT：

**nat** [ (*real_ifc* ,*mapped_ifc*) ] [*line* | { **after-auto** [*line*] } ] **source**
**static** { *real_obj* | **any** } { *mapped_obj* | **interface** [ **ipv6** ] | **any** } [ **destination**
**stat**{*mapped_obj*|**inte**[**ipv6**]}{*real_obj*|**any**}] [**servi**{*real_mapped_dest_svc_obj* *real_real_dest_svc_obj*|**any**}*mapped_src_real_dest_svc_obj*] [**rotat**] [**dns**] [**unidirectional**] [**noproxy-arp**] [**route-lookup**] ] [**inac**] [**descriptio***desc*

**no nat** [ (*real_ifc* ,*mapped_ifc*) ] [*line* | { **after-auto** [*line*] } ] **source**
**static** { *real_obj* | **any** } { *mapped_obj* | **interface** [ **ipv6** ] | **any** } ] [ **destination**
**stat**{*mapped_obj*|**inte**[**ipv6**]}{*real_obj*|**any**}] [**servi**{*real_mapped_dest_svc_obj* *real_real_dest_svc_obj*|**any**}*mapped_src_real_dest_svc_obj*] [**rotat**] [**dns**] [**unidirectional**] [**noproxy-arp**] [**route-lookup**] ] [**inac**] [**descriptio***desc*

对于动态 NAT：

**nat** [ (*real_ifc* ,*mapped_ifc*) ] [*line* | { **after-auto** [*line*] } ] **source**
**dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [ **ipv6** ] | **pat-pool***mapped_obj* [ **round-robin** ] [ **extended** ] [ **flat** [ **include-reserve** ] ] [ **block-allocation** ] [ **interface** [ **ipv6** ] ] | **interface** [ **ipv6** ] } [ **destination**
**static** { *mapped_obj* | **interface** [ **ipv6** ] } { *real_obj* | **any** } ] [ **service** { *mapped_dest_svc_obj real_dest_svc_obj* ]
[ **dns** ] [ **unidirectional** ] [ **inactive** ] [ **description***desc*

**no nat** [ (*real_ifc* ,*mapped_ifc*) ] [*line* | { **after-auto** [*line*] } ] **source**
**dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [ **ipv6** ] | **pat-pool***mapped_obj* [ **round-robin** ] [ **extended** ] [ **flat** [ **include-reserve** ] ] [ **block-allocation** ] [ **interface** [ **ipv6** ] ] | **interface** [ **ipv6** ] } [ **destination**
**static** { *mapped_obj* | **interface** [ **ipv6** ] } { *real_obj* | **any** } ] [ **service** { *mapped_dest_svc_obj real_dest_svc_obj* ]
[ **dns** ] [ **unidirectional** ] [ **inactive** ] [ **description***desc*

或

**nonat** { *line***after-auto***line* }

## Syntax Description

| | |
|---|---|
| **(***real_ifc***,***mapped_ifc***)** | （可选）指定真实接口和映射接口。如果您未指定真实接口和映射接口，则使用所有接口。您还可以 **any**为一个或两个接口指定关键字。对于桥接组成员接口（在透明或路由模式下），必须指定实际接口和映射接口；则不能使用 **any**。<br><br>由于两次 NAT 可以转换源地址和目标地址，因此最好将这些接口理解为源接口和目标接口。 |
| **after-auto** | 在 NAT 表第 3 部分的末尾、网络对象 NAT 规则之后插入规则。默认情况下，两次 NAT 规则会添加到第 1 部分。您可以使用行参数在第 3 部分的 任何位置插入规则。 |

| | |
|---|---|
| **any** | （可选）指定通配符值。 **any** 的主要用途包括：<br>• 接口 - 您可以使用 **any** 表示一个或两个接口（例如 **(any,outside)**）。如果您没有指定接口，那么就 **any**是默认的。但是， **any** 不适用于桥接组成员接口，并且 **any** 在透明模式下不可用。<br>• 静态 NAT 源实际和映射 IP 地址 - 您可以指定 **sourcestaticanyany** ，以启用所有地址的身份 NAT。<br>• 动态 NAT 或 PAT 源实际地址 - 通过指定 **sourcedynamicany***mapped_obj*，可以转换源接口上的所有地址。<br>对于静态 NAT，虽然 **any** 也可用于实际源端口/映射目标端口，或可用于源或目标实际地址（不带 **any** 作为映射地址），但使用这些命令可能会导致不可预测的行为。<br>**注释**<br>“任何”流量（IPv4 与 IPv6）的定义取决于规则。在 ASA 对数据包执行 NAT 之前，数据包必须是 IPv6 到 IPv6 或 IPv4 到 IPv4；有了这个先决条件，ASA 才能确定 NAT 规则中的值。 **any** 例如，如果您配置一条从“任何”到 IPv6 服务器的规则，并且该服务器是从 IPv4 地址映射的， **any**则表示“任何 IPv6 流量”。如果您配置从“任何”到“任何”的规则，并且将源映射到接口 IPv4 地址，则意味 **any**着“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。 |
| **block-allocation** | 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由NAT每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与兼容 **round-robin**，但不能使用 **extended**或 **flat**[**include-reserve**] 选项。也无法使用接口 PAT 回退。 |
| **description***desc* | （可选）提供最多 200 个字符的描述。 |
| 目的 | （可选）配置目标地址的转换。尽管两次 NAT 的主要功能是纳入目标IP地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅《CLI 配置指南》。 |
| **dns** | （可选）转换 DNS 应答。确保 DNS 检查已启用（**inspectdns**）（默认启用）。如果配置了 **dns**地址，则不能配置关键 **destination**字。请勿将此选项与 PAT 规则一起使用。有关详细信息，请参阅 CLI 配置指南。 |

| | |
|---|---|
| **dynamic** | 为源地址配置动态 NAT 或 PAT。目标转换始终为静态。 |
| **extended** | （可选）为 PAT 池启用扩展 PAT。扩展 PAT 通过在转换信息中包含目标地址和端 口 ，为每个服务（而不是每个 IP 地址）使用 65535 个端口。通常，创建PAT转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。 |
| **flat** [**include-reserve**]<br>**include-reserve** | （可选，9.15 之前版本）分配端口时允许使用整个 1024 到 65535 端口范围。当选择要转换的映射端口号时，ASA 将使用实际源端口号（如果可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，另请指定 **include-reserve** 关键字。<br><br>(9.15+) 从 9.15 开始，平面是 PAT 池的默认且不可配置的行为。**include-reserve** 关键字独立于平面关键字，因此您仍然可以选择在 PAT 池中包含保留端口 1-1023。 |
| **inactive** | （可选）要使此规则不活动而不必删除命令，请使用关**inactive**键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。 |
| **interface**[**ipv6**] | （可选）使用接口 IP 地址作为映射地址。如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。<br><br>对于动态NAT源映射地址，如果您指定映射对象或组，后跟**interface**关键字，则仅在所有其他映射地址已分配时，才会使用映射接口的IP地址。<br><br>对于动态 PAT，可以为源映射地址单独指定 **interface** 。<br><br>对于支持端口转换（源或目标）的静态NAT，请务必同时配置**service**关键字。<br><br>对于此选项，您必须为 *mapped_ifc* 配置一个特定的接口。<br><br>此选项在透明模式下不可用。在路由模式下，如果目标接口为桥接组成员，则不能使用此选项。 |
| 折线图 | （可选）在NAT表第1部分的任意位置插入规则。默认情况下，NAT规则将添加到第 1 部分的末尾（有关详细信息，请参阅 CLI 配置指南）。如果您想将规则添加到第3部分（网络对象NAT规则之后），请使用 **after-auto**线 路选项。 |
| *mapped_dest_svc_obj* | （可选）对于动态 NAT/PAT，指定映射目标端口（目标转换始终为静态）。有关详细信息，请参阅 **service** 关键字。 |

| | |
|---|---|
| *mapped_object* | 标识映射的网络对象或对象组（**objectnetwork**或**object-groupnetwork**）。<br><br>对于动态NAT，您通常会配置一组较大的地址来映射到一组较小的地址。<br><br>注释<br>映射对象或组不能包含子网。如果需要，可以在不同的动态 NAT 规则之间共享此映射 IP 地址。不能使用同时包含 IPv4 和 IPv6 地址的对象组；只有在对象组中才可以使用。对象组只能包含一种类型的地址。<br><br>对于动态 PAT，请将一组地址配置为映射到一个地址。您可以将实际地址转换为您选择的单个映射地址，也可以将其转换为映射接口地址。如果要使用接口地址，请勿为映射地址配置网络对象；请注意而是使用 **interface** 关键字。<br><br>对于静态NAT，映射通常是一对一的，因此实际地址与映射地址的数量相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅《CLI 配置指南》。 |
| *mapped_src_real_dest_svc_obj* | （可选）对于静态 NAT，指定映射源端口和/或实际目的端口。有关详细信息，请参阅 **service** 关键字。 |
| **net-to-net** | （可选）对于静态NAT 46，指 **net-to-net**定将第一个 IPv4 地址转换为第一个IPv6地址，将第二个转换为第二个，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。 |
| **no-proxy-arp** | （可选）对于静态 NAT，禁用发往映射 IP 地址的传入数据包的代理 ARP。 |
| **pat-pool***mapped_obj* | （可选）启用地址 PAT 池；对象中的所有地址均用作 PAT 地址。对于动态NAT，可以将PAT池配置为回退方法。不能使用同时包含IPv4和 IPv6 地址的对象组，对象组只能包括一种类型的地址。 |
| *real_dest_svc_obj* | （可选）对于动态 NAT/PAT，指定实际目标端口（目标转换始终为静态）。有关详细信息，请参阅 **service** 关键字。 |
| *real_ifc* | （可选）指定数据包可能源自的接口的名称。对于源选项。对于source选项， origin_ifc 是实际接口。对于目标选项，real_ifc 是映射接口。 |
| *real_object* | 标识实际网络对象或对象组（**objectnetwork**或**object-groupnetwork**）。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。 |
| *real_src_mapped_dest_svc_obj* | （可选）对于静态 NAT，指定实际源端口和/或映射目标端口。有关详细信息，请参阅 **service** 关键字。 |

| | |
|---|---|
| **round-robin** | （可选）为 PAT 池启用循环地址分配。默认情况下，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。 |
| **route-lookup** | （可选）对于路由模式下的身份NAT，使用路由查找而不是使用NAT命令中指定的接口来确定出口接口。如果不在NAT命令中指定接口，默认情况下将使用路由查找。 |
| **service** | （可选）指定端口转换。<br>• 动态 NAT 和 PAT - 动态 NAT 和 PAT 不支持（其他）端口转换。但是，由于目标转换 始 终是静态的，因此您可以对目标端口执行端口转换。服务对象（**objectservice**）可以同时包含源端口和目标端口，但在这种情况下只使用目标端口。系统将忽略您指定的源端口。<br>• 带端口转换的静态 NAT — 您应该 为两个服务对象指 定源端口或 目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。<br><br>对于源端口转换，对象必须指定源服务。在本例中，命令中服务对象的顺序为 **service** *real_port mapped_port* 。对于目标端口转换，对象必须指定目标服务。在这种情况下，服务对象的顺序为 **service***mapped_port real_port* 。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。有关“源”和“目标”术语的详细信息，请参阅“使用指南”部分。<br><br>对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。不支持“不等于” (**neq**) 运算符。<br><br>NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。 |
| **source** | 配置源地址的转换。 |
| **static** | 配置静态 NAT 或带端口转换的静态 NAT。 |
| **unidirectional** | （可选）对于静态 NAT， 使从源到目标的单向转换；目标地址无法发起流向源地址的流量。此选项可用于测试目的。 |

## Command Default

- 默认情况下，该规则被添加到 NAT 表第 1 部分的末尾。
- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**，表示将规则应用于所有接口。

- （8.3(1)、8.3(2) 和 8.4(1)）用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。（8.4(2) 及更高版本）用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。
- 如果指定可选接口，则 ASA 使用 NAT 配置来确定出口接口。（8.3(1) 到 8.4(1)）唯一的例外是面向身份 NAT，其中该身份 NAT 始终使用路由查询，无论 NAT 配置如何。（8.4(2) 及更高版本）对于身份 NAT，默认行为是使用 NAT 配置，但可以选择始终使用路由查找。

## 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 |
|---|---|
| 8.3(1) | 添加了此命令。 |
| 8.3(2) | 当从 8.3 之前版本的 NAT 豁免配置进行迁移时，系统会为生成的静态身份 NAT 规则添加关键字 **unidirectional** 。 |
| 8.4(2)/8.5(1) | 添加 **no-proxy-arp**了、 **route-lookuppat-pool**和关**round-robin** 键字。<br>身份 NAT 的默认行为已更改为启用代理 ARP，以匹配其他静态 NAT 规则。<br>对于 8.3 之前的配置，NAT 豁免规则（命 **nat0access-list**令）迁移到 8.4(2) 及更高版本现在包括以下关键字，以禁用代理 ARP 并使用路由查找： **no-proxy-arp**和。**route-lookup** 用于迁移到 8.3(2) 和 8.4(1) 的 **unidirectional**关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置此时都将包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字将被删除。 |
| 8.4(3) | 添加 **extended**了 **flat**、和关 **include-reserve**键字。<br>组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。<br>此功能在 *8.5(1)* 中不可用。 |
| 9.0(1) | NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。添加了 **interfaceipv6** 选项和**net-to-net**选项。 |
| 9.5(1) | 添加了 **block-allocation** 关键字。 |
| 9.15(1) | 已删除 **flat** 关键字，并且 **include-reserve** 关键字不再是平面的子参数。现在，所有 PAT 池都使用平面端口范围 1024-65535，并且您可以选择包含保留的端口 1-1023。 |

| 版本 | 修改 |
| --- | --- |
| 9.17(1) | 可以将 FQDN 网络对象指定为转换（映射）目的。 |

使用指南

## 使用指南

两次NAT可供您在单一规则中同时标识源和目标地址。例如，同时指定源和目标地址可以指定：源地址在前往目标 X 时转换为 A，而在前往目标 Y 时转换为 B。

注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果您配置带有端口转换的静态NAT，并将源地址指定为 Telnet 服务器，并且您希望所有到该 Telnet 服务器的流量的端口从 2323 转换为 23，那么在命令中，您必须指定要转换的源端口（实际：23，映射：2323）。您指定源端口是因为您指定了 Telnet 服务器地址作为地 **source**址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

两次 NAT 还可以让您将服务对象用于支持端口转换的静态 NAT；网络对象 NAT 仅接受内联定义。

有关两次 NAT 和网络对象 NAT 之间差异的详细信息，请参阅《CLI 配置指南》。

两次 NAT 规则将添加到 NAT 规则表的第 1 部分或第 3 部分（如果已指定）。有关 NAT 排序的更多信息，请参阅 CLI 配置指南。

### 映射地址指南

映射 IP 地址池不能包括：

- 映射接口的IP地址。如 **any** 果为规则指定接口，则所有接口 IP 地址都将被禁止。对于接口 PAT（仅限路由模式），使用关 **interface**键字而不是 IP 地址。
- （透明模式）管理 IP 地址。
- （动态 NAT）启用 VPN 时的备用接口 IP 地址。
- 现有的 VPN 池地址。

### 必备条件

- 对于实际地址和映射地址，请使用 **objectnetwork** 或 **object-groupnetwork** 命令）配置网络对象或网络对象组。在使用不连续的IP地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- 对于支持端口转换的静态 NAT，请配置 TCP 或 UDP 服务对象（使用 **objectservice**命令）。

NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。

### 清除会话转换

如果您更改 NAT 配置，并且不想等待现有转换超时后再使用新的 NAT 信息，则可以使用 clear xlate 命令清除转换表。但是，清除转换表会断开所有当前连接。

**PAT 池指南**

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 记录，而且要使用的 PAT 规则不确定。
- （9.15 之前）如果可用，则使用真实源端口号作为映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。（8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果有大量流量使用较低的端口范围，您现在可以指定要使用的固定端口范围，而不是三个大小不等的层级：1024 到 65535，或 1 到 65535。
- （9.15+）端口映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

在集群中运行时，每个地址的 512 个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。
- 如果将包含主机地址的对象组用于动态 NAT 映射 IP 地址，启用 PAT 池则可以将这些主机地址的使用从 PAT 回退更改为动态 NAT。
- （8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果在两个单独的规则中使用相同的 PAT 池对象，请确保为每个规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和不分段范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

**PAT 池指南的扩展 PAT**

- 许多应用检测不支持扩展 PAT。请参阅配置指南以获取不受支持的检查的完整列表。
- 如果为动态 PAT 规则启用扩展 PAT，则您不能将 PAT 池中的地址用作单独的静态 NAT 带端口转换规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。

**PAT 池的轮询准则**

- （8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果主机已存在连接，则如果有可用端口，来自该主机的后续连接将使用相同的 PAT IP 地址。：**Note**这种“粘性”在故障转移后无法继续存在。如果 ASA 发生故障转移，则来自主机的后续连接可能不会使用初始 IP 地址。

- （8.4(2)、8.5(1) 和 8.6(1)）如果主机具有现有连接，则由于轮询分配，来自该主机的后续连接可能对每个连接使用 不同的 PAT 地址。在这种情况下，当您访问交换主机信息的两个网站（例如电子商务网站和支付网站）时可能会遇到问题。当这些站点发现本应是单个主机的两个不同 IP 地址时，事务可能会失败。

**NAT 和 IPv6**

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践。请注意，当接口是同一网桥组的成员时，不能执行 NAT64/46。

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）当转换为 IPv6 子网（/96 或更低）时，生成的映射地址是 IPv4 嵌入的 IPv6 地址，其中 IPv4 地址的 32 位嵌入在 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

## CR_Examples

以下示例包括 10.1.2.0/24 网络上访问两个不同服务器的主机。当主机访问 209.165.201.11 的服务器时，真实地址被转换为 209.165.202.129:*port* 。当主机访问 209.165.200.225 的服务器时，真实地址被转换为 209.165.202.130:*port* 。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

以下示例显示了源端口和目标端口的使用。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机访问服务器进行Telnet服务时，真实地址被转换为 209.165.202.129:*port* 。当主机访问同一台服务器进行Web服务时，真实地址被转换为 209.165.202.130:*port* 。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

```
ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# servicetcpdestination eq telnet
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1 destination
 static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# servicetcpdestination eq http
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2 destination
 static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

以下示例展示支持端口转换的静态接口NAT的用途。外部主机通过目标端口65000至65004连接至外部接口IP地址，从而访问内部FTP服务器。流量未经转换就通过192.168.10.100:6500到 :65004 到达内部 FTP 服务器。请注意，应在服务对象中指定源端口范围（而不是指定目标端口），因为要在命令中将源地址和端口转换为已标识状态；目标端口为“any”。由于静态 NAT 是双向的，“源”和“目标”主要指命令关键字；数据包中的实际源和目标地址与端口取决于发送数据包的主机。在此示例中，连接源自外部，通向内部，因此，FTP服务器的“源”地址和端口实际是源数据包中的目标地址和端口。

```
ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-obvject)# service tcp source range 65000 65004
ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-obvject)# host 192.168.10.100
ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

以下示例在访问 IPv4 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为 IPv6 内部网络 2001:DB8:AAAA::/96 配置动态 NAT：

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254
ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158
ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination static
 SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination static
 SERVERS_2 SERVERS_2
```

以下示例为内部网络 192.168.1.0/24 配置访问外部 IPv6 Telnet 服务器 2001:DB8::23 时的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任何服务器时使用 PAT 池的动态 PAT。

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200
ciscoasa(config)# object network TELNET_SVR
ciscoasa(config-network-object)# host 2001:DB8::23
```

```
ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23
ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
 static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL destination
 static SERVERS SERVERS
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **clearconfigurenat** | 删除 NAT 配置（两次 NAT 和网络对象 NAT）。 |
| show nat | 显示 NAT 策略统计信息。 |
| show nat pool | 显示有关 NAT 池的信息。 |
| **showrunning-configgnat** | 显示 NAT 配置。 |
| show xlate | 显示 NAT 会话（转换）信息。 |
| **xlateblock-allocation** | 配置 PAT 端口块分配特征。 |

# nat (object)

要为网络对象配置 NAT，请在对象网络配置模式下使用 **nat** 命令。要删除 NAT 配置，请使用此命令的形式。**no**

对于动态 NAT 和 PAT：

**nat** [ (*real_ifc* ,*mapped_ifc*) ] **dynamic** { *mapped_inline_host_ip* [ **interface** [ **ipv6** ] ] | [ *mapped_obj* ] [ **pat-pool** *mapped_obj* [ **round-robin** ] [ **extended** ] [ **flat** [ **include-reserve** ] ] [ **block-allocation** ] ] [ **interface** [ **ipv6** ] ] } [ **dns** ]

**no nat** [ (*real_ifc* ,*mapped_ifc*) ] **dynamic** { *mapped_inline_host_ip* [ **interface** [ **ipv6** ] ] | [ *mapped_obj* ] [ **pat-pool** *mapped_obj* [ **round-robin** ] [ **extended** ] [ **flat** [ **include-reserve** ] ] [ **block-allocation** ] ] [ **interface** [ **ipv6** ] ] } [ **dns** ]

对于静态 NAT 和带端口转换的静态 NAT：

**nat** [ (*real_ifc* ,*mapped_ifc*) ] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [ **ipv6** ] } [ **net-to-net** ] [ **dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port* ] [ **no-proxy-arp** ] [ **route-lookup** ]

**no nat** [ (*real_ifc* ,*mapped_ifc*) ] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [ **ipv6** ] } [ **net-to-net** ] [ **dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port* ] [ **no-proxy-arp** ] [ **route-lookup** ]

## Syntax Description

| | |
|---|---|
| **(***real_ifc***,***mapped_ifc***)** | （可选）对于静态 NAT，指定实际接口和映射接口。如果您未指定真实接口和映射接口，则使用所有接口。您还可以 **any** 为一个或两个接口指定关键字。确保在命令中包含括号。对于桥接组成员接口（在透明或路由模式下），必须指定实际接口和映射接口；则不能使用 **any**。 |
| **block-allocation** | 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与兼容 **round-robin**，但不能使用 **extended** 或 **flat**[**include-reserve**] 选项。也无法使用接口 PAT 回退。 |
| **dns** | （可选）转换 DNS 应答。确保 DNS 检查 (**inspectdns**) 已启用（默认启用）。如果指定了 **service** 关键字（用于静态 NAT），则此选项不可用。请勿将此选项与 PAT 规则一起使用。有关详细信息，请参阅《CLI 配置指南》。 |
| **dynamic** | 配置动态 NAT 或 PAT。 |
| **extended** | （可选）为 PAT 池启用扩展 PAT。扩展 PAT 通过在转换信息中包含目标地址和端 口 ，为每个服务（而不是每个 IP 地址）使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。 |

| | |
|---|---|
| **flat** [**include-reserve**]<br>**include-reserve** | （可选，9.15 之前版本）分配端口时允许使用整个 1024 到 65535 端口范围。当选择要转换的映射端口号时，ASA 将使用实际源端口号（如果可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 到 65535 的完整范围，另请指定 **include-reserve** 关键字。<br><br>(9.15+) 从 9.15 开始，平面是 PAT 池的默认且不可配置的行为。 **include-reserve** 关键字独立于平面关键字，因此您仍然可以选择在 PAT 池中包含保留端口 1-1023。 |
| **interface**[**ipv6**] | （可选）对于动态 NAT，如果您在 **interface** 关键字后指定映射 IP 地址、对象或组，则仅在所有其他映射地址均已分配时才会使用映射接口的 IP 地址。<br><br>对于动态 PAT，如果您指定 **interface** 关键字而不是映射 IP 地址、对象或组，则要将接口 IP 地址用于映射 IP 地址。要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。<br><br>如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。<br><br>对于支持端口转换的静态 NAT，如果另外配置了 **service** ] 关键字，则可以指定 **interface** 关键字。<br><br>对于此选项，您必须为 *mapped_ifc* 配置一个特定的接口。<br><br>不能在透明模式下指定 **interface** 。在路由模式下，如果目标接口为桥接组成员，则不能使用此选项。 |
| *mapped_inline_host_ip* | 如果指定 **dynamic**，则使用主机 IP 地址来配置动态 PAT。如果指定 **static**，则映射网络的网络掩码或范围与真实网络的网络掩码或范围相同。比如真实网络里有一个主机，那么这个地址就会被当做主机地址。对于范围或子网，映射地址包含的地址数量与实际范围或子网相同。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 172.20.1.1 指定为映射地址，则映射范围将包括 172.20.1.1 到 172.20.1.6。如果需要多对一映射（我们不建议使用此映射），请使用主机网络对象而非内联地址。 |
| *mapped_obj* | 将映射 IP 地址指定为网络对象 (**objectnetwork**) 或对象组 (**object-groupnetwork**)。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。<br><br>对于动态 NAT，对象或组不能包含子网。如果需要，可以在不同的动态 NAT 规则之间共享此映射对象。有关不允许的映射 IP 地址的信息，请参阅“映射地址指南”。<br><br>对于静态 NAT，通常配置与真实地址相同数量的映射地址，以实现一对一映射。然而，地址数量可以不匹配。有关详细信息，请参阅《CLI 配置指南》。 |
| *mapped_port* | （可选）指定映射的 TCP/UDP/SCTP 端口。可以通过文字名称或 0 至 65535 范围内的数字指定端口。 |

| | |
|---|---|
| **net-to-net** | （可选）对于 NAT 46，指 **net-to-net**定将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个转换为第二个，依此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。 |
| **no-proxy-arp** | （可选）对于静态 NAT，禁用发往映射 IP 地址的传入数据包的代理 ARP。 |
| **pat-pool***mapped_obj* | （可选）启用地址 PAT 池；对象中的所有地址均用作 PAT 地址。对于动态 NAT，可以将 PAT 池配置为回退方法。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。 |
| *real_port* | （可选）对于静态 NAT，指定实际 TCP/UDP/SCTP 端口。可以通过文字名称或 0 至 65535 范围内的数字指定端口。 |
| **round-robin** | （可选）为 PAT 池启用循环地址分配。默认情况下，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。 |
| **route-lookup** | （可选）对于路由模式下的身份 NAT，使用路由查找而不是使用 NAT 命令中指定的接口来确定出口接口。如果不在NAT 命令中指定接口，默认情况下将使用路由查找。 |
| **service**{**tcp**\|**udp** \| **sctp**} | （可选）对于支持端口转换的静态 NAT，指定用于端口转换的协议：TCP、UDP、SCTP。 |
| **static** | 配置静态 NAT 或带端口转换的静态 NAT。 |

## Command Default

- *real_ifc* 和 *mapped_ifc* 的默认值为 **any**，表示将规则应用于所有接口。
- （8.3(1)、8.3(2) 和 8.4(1)）用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。（8.4(2) 及更高版本）用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。
- 如果指定可选接口，则 ASA 使用 NAT 配置来确定出口接口。（8.3(1) 到 8.4(1)）唯一的例外是面向身份 NAT，其中该身份 NAT 始终使用路由查询，无论 NAT 配置如何。（8.4(2) 及更高版本）对于身份 NAT，默认行为是使用 NAT 配置，但可以选择始终使用路由查找。

## 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 |
| 对象网络配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.3(1) | 添加了此命令。 |
| 8.4(2)/8.5(1) | 添加 **no-proxy-arp**了、、、 **route-lookuppat-pool**和关**round-robin** 键字。<br>身份 NAT 的默认行为已更改为启用代理 ARP，以匹配其他静态 NAT 规则。<br>从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置此时都将包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。 |
| 8.4(3) | 添加 **extended**了 **flat**、和关 **include-reserve**键字。<br>组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。<br>此功能在 *8.5(1)* 中不可用。 |
| 9.0(1) | NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。添加了 **interfaceipv6** 选项和 **net-to-net** 选项。 |
| 9.5(1) | 添加了 **block-allocation** 关键字。 |
| 9.5(2) | 已添加关 **servicesctp**键字。 |
| 9.15(1) | 已删除 **flat** 关键字，并且 **include-reserve** 关键字不再是平面的子参数。现在，所有 PAT 池都使用平面端口范围 1024-65535，并且您可以选择包含保留的端口 1-1023。 |

## 使用指南

当数据包进入 ASA 时，将根据网络对象 NAT 规则检查源 IP 地址和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为 规则从未配对，所以不能指定源地址在前往目标 X 时应转换为 A，但在前往目标 Y 时应转换为 B。对此类功能使用两次 NAT（两次 NAT 可让您识别将源和目标地址放在一起）。

有关两次 NAT 和网络对象 NAT 之间差异的详细信息，请参阅《CLI 配置指南》。

网络对象 NAT 规则将添加到 NAT 规则表的第 2 部分。有关 NAT 排序的更多信息，请参阅 CLI 配置指南。

根据配置，可以根据需要内联配置映射地址，也可以为映射地址创建网络对象或网络对象组（使用 **objectnetwork** 或 **object-groupnetwork** 命令）。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。

NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。

您只能为给定对象定义一条 NAT 规则；如果要配置多条 NAT 规则，则需要创建多个指定相同 IP 地址的对象 **objectnetworkobj-10.10.10.1-01**， **objectnetworkobj-10.10.10.1-02**例如，等等。

### 映射地址指南

映射 IP 地址池不能包括：

- 映射接口的 IP 地址。如 **any** 果为规则指定接口，则所有接口 IP 地址都将被禁止。对于接口 PAT（仅限路由模式），使用关 **interface**键字而不是 IP 地址。
- （透明模式）管理 IP 地址。
- （动态 NAT）启用 VPN 时的备用接口 IP 地址。
- 现有的 VPN 池地址。

### 清除会话转换

如果您更改 NAT 配置，并且不想等待现有转换超时后再使用新的 NAT 信息，则可以使用 clear xlate 命令清除转换表。但是，清除转换表会断开所有当前连接。

### PAT 池指南

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 记录，而且要使用的 PAT 规则不确定。
- （9.15 之前）如果可用，则使用真实源端口号作为映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。（8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果有大量流量使用较低的端口范围，您现在可以指定要使用的固定端口范围，而不是三个大小不等的层级：1024 到 65535，或 1 到 65535。
- （9.15+）端口映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

在集群中运行时，每个地址的 512 个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。

如果将包含主机地址的对象组用于动态 NAT 映射 IP 地址，启用 PAT 池则可以将这些主机地址的使用从 PAT 回退更改为动态 NAT。

- （8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果在两个单独的规则中使用相同的 PAT 池对象，请确保为每个规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和不分段范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

### PAT 池指南的扩展 PAT

- 许多应用检测不支持扩展 PAT。请参阅配置指南以获取不受支持的检查的完整列表。
- 如果为动态 PAT 规则启用扩展 PAT，则您不能将 PAT 池中的地址用作单独的静态 NAT 带端口转换规则中的 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。

- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。

### PAT 池的轮询准则

- （8.4(3) 及更高版本，不包括 8.5(1) 或 8.6(1)）如果主机已存在连接，则如果有可用端口，来自该主机的后续连接将使用相同的 PAT IP 地址。：**Note**这种“粘性”在故障转移后无法继续存在。如果 ASA 发生故障转移，则来自主机的后续连接可能不会使用初始 IP 地址。
- （8.4(2)、8.5(1) 和 8.6(1)）如果主机具有现有连接，则由于轮询分配，来自该主机的后续连接可能对每个连接使用 不同的 PAT 地址。在这种情况下，当您访问交换主机信息的两个网站（例如电子商务网站和支付网站）时可能会遇到问题。当这些站点发现本应是单个主机的两个不同 IP 地址时，事务可能会失败。
- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。

### NAT 和 IPv6

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践。请注意，当接口是同一网桥组的成员时，不能执行 NAT64/46。

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，可以使静态 NAT 规则成为单向的（仅两次 NAT）当转换为 IPv6 子网（/96 或更低）时，生成的映射地址是 IPv4 嵌入的 IPv6 地址，其中 IPv4 地址的 32 位嵌入在 IPv6 前缀之后。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

## CR_Examples

### 动态 NAT 示例

以下示例配置动态 NAT，将 192.168.2.0 网络隐藏在外部地址范围 2.2.2.1-2.2.2.10 之后：

```
ciscoasa(config)# object network my-range-obj
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

以下示例使用动态 PAT 备份配置 动态 NAT。内部网络 10.76.11.0 中的主机首先映射到 nat-range 1 池 (10.10.10.10-10.10.10.20)。分配 nat-range1 池中的所有地址之后，使用 pat-ip1

地址 (10.10.10.21) 执行动态 PAT。在不太可能发生 PAT 转换也用完的情况下，使用外部接口地址执行动态 PAT。

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20
ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21
ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

以下示例使用动态 PAT 备份配置动态 NAT，将 IPv6 主机转换为 IPv4 主机。内部网络 2001:DB8::/96 上的主机首先映射到 IPv4_NAT_RANGE 池（209.165.201.1 到 209.165.201.30）。分配 IPv4_NAT_RANGE 池中的所有地址之后，使用 IPv4_PAT 地址 (209.165.201.31) 执行动态 PAT。在 PAT 转换也被用完的情况下， 使用外部接口地址执行动态 PAT。

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30
ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31
ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

### 动态 PAT 示例

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在地址 2.2.2.2 后面：

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口地址后面：

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

以下示例配置动态 PAT，使用 PAT 池将内部 IPv6 网络转换为外部 IPv4 网络：

```
ciscoasa(config)# object network IPv4_POOL
ciscoasa(config-network-object)# range 203.0.113.1 203.0.113.254
ciscoasa(config)# object network IPv6_INSIDE
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

### 静态 NAT 示例

以下示例配置静态 NAT，将内部的真实主机 1.1.1.1 配置为外部的 2.2.2.2，并启用 DNS 重写。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

以下示例使用映射对象为内部的真实主机 1.1.1.1 配置到外部的 2.2.2.2 的静态 NAT。

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

以下示例配置静态 NAT，将 TCP 端口 21 处的 1.1.1.1 转换为端口 2121 处的外部接口。

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

以下示例将内部 IPv4 网络映射到外部 IPv6 网络。

```
ciscoasa(config)# object network inside_v4_v6
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

以下示例将内部 IPv6 网络映射到外部 IPv6 网络。

```
ciscoasa(config)# object network inside_v6
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

### 身份 NAT 示例

以下示例使用内联映射地址将主机地址映射到它本身：

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 10.1.1.1
```

以下示例使用网络对象 将主机地址映射到它本身：

```
ciscoasa(config)# object network my-host-obj1-identity
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **clearconfigurenat** | 删除 NAT 配置（两次 NAT 和网络对象 NAT）。 |
| show nat | 显示 NAT 策略统计信息。 |
| show nat pool | 显示有关 NAT 池的信息。 |
| **showrunning-confignat** | 显示 NAT 配置。 |
| show xlate | 显示转换信息。 |
| **xlateblock-allocation** | 配置 PAT 端口块分配特征。 |

# nat (vpn load-balancing)

要设置 NAT 将此设备的 IP 地址转换为的 IP 地址，请在 VPN 负载均衡配置模式下使用 **nat**命令。要禁用此 NAT 转换，请使用此命 **no**令的形式。

**nat***ip-address*
**no nat**[ *ip-adddress*]

## Syntax Description

| | |
|---|---|
| *ip-address* | 您希望此 NAT 将此设备的 IP 地址转换为的 IP 地址。 |

## 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 |
| VPN 负载平衡配置 | • 是 | • — | • 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。

在命令的 **nonat** 形式中，如果指定可选的 *ip-address* 值，则该 IP 地址必须与运行配置中的现有 NAT IP 地址相匹配。

## CR_Examples

以下 VPN 负载均衡命令序列示例包含一条 **nat**命令，该命令将 NAT 转换地址设置为 192.168.10.10：

```
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)# nat 192.168.10.10
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)# cluster port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

## Related Commands

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

# nat-assigned-to-public-ip

要自动将 VPN 对等体的本地 IP 地址转换回对等体的实际 IP 地址，请在 tunnel-group general-attributes 配置模式下使用 **nat-assigned-to-public-ip** 命令。要禁用 NAT 规则，请使用此命 **no**令的形式。

**nat-assigned-to-public-ip***interface*
**no nat-assigned-to-public-ip***interface*

## Syntax Description

| | |
|---|---|
| *interface* | 指定要应用NAT的接口。 |

## Command Default

此命令默认禁用。

## 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 |
| 隧道组常规属性配置 | • 是 | • 支持 | • 支持 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.4(3) | 添加了此命令。 |

## 使用指南

在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 IP 地址。

可以在每个隧道组一个接口的基础上启用此功能。当VPN会话已建立或断开连接时，动态添加或删除对象 NAT 规则。您可以使用命令查看规则。 **shownat**

### 数据流

以下步骤介绍启用此功能时通过 ASA 的数据包流：

**1.** VPN 对等体向 ASA 发送数据包。

外部源/目的包含对等体公共 IP 地址/ASA IP 地址。加密的内部源/目的地包含 VPN 分配的 IP 地址/内部服务器地址。

**2.** ASA 将解密数据包（删除外部源/目标）。

**3.** ASA 为内部服务器执行路由查找，并将数据包发送到内部接口。

**4.** 自动创建的 VPN NAT 策略会将 VPN 分配的源 IP 地址转换为对等体公用 IP 地址。

**5.** ASA 将转换后的数据包发送到服务器。

**6.** 服务器响应数据包，并将其发送到对等体的公共 IP 地址。

**7.** ASA 接收响应，将目标 IP 地址逆向转换为 VPN 分配的 IP 地址。

**8.** ASA 将未转换的数据包转发到外部接口并在其中对其进行加密，并添加由 ASA IP 地址/对等体公共 IP 地址组成的外部源/目的地。

**9.** ASA 将数据包发回对等体。

**10.** 对等体解密并处理数据。

限制

由于路由问题，除非您确定自己需要此功能，否则我们不建议使用此功能。请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制：

- 仅支持 Cisco IPsec 和 Secure Client。
- 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。
- 如果启用反向路由注入（请参阅**setreverse-route** 命令），则仅通告 VPN 分配的 IP 地址。
- 不支持负载均衡（由于路由问题）。
- 不支持漫游（公共 IP 更改）。

## CR_Examples

以下示例对“vpnclient”隧道组启用到公共 IP 的 NAT：

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

以下是**shownatdetail** 命令的输出示例，其中显示一条自动 NAT 规则，来自网段为 209.165.201.10（已分配 IP 为 10.1.226.174）的设备：

```
ciscoasa# show nat detail
 Auto NAT Policies (Section 2)
 1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
     translate_hits = 0, untranslate_hits = 0
     Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **shownat** | 显示当前网络地址转换。 |
| **tunnel-groupgeneral-attributes** | 设置隧道组的常规属性。 |
| **debugmenuwebvpn99** | 对于 AnyConnect SSL 会话，VPN NAT 接口存储在会话中。 |

| 命令 | 说明 |
| --- | --- |
| **debugmenuike2***peer_ip* | 对于思科 IPsec 客户端会话，VPN NAT 接口存储在 SA 中。 |
| 调试 nat 3 | 显示 NAT 的调试消息。 |

# nat-rewrite

要为 DNS 响应的 A 记录中嵌入的 IP 地址启用 NAT 重写，请在参数配置模式下使用 **nat-rewrite**命令。要禁用此功能，请使用此**no** 命令的形式。

**nat-rewrite**
**no nat-rewrite**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下，NAT 重写已启用。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 **nonat-rewrite** 。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

此功能对 DNS 响应中的 A 类型资源记录 (RR) 执行 NAT 转换。

## CR_Examples

以下示例显示如何在 DNS 检查策略映射中启用 NAT 重写：

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

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

# nbns-server

要配置 NBNS 服务器，请在 tunnel-group webvpn-attributes 配置模式下使用 **nbns-server**命令。要从配置中删除 NBNS 服务器，请使用此命令的 **no**形式。

ASA 查询 NBNS 服务器以将 NetBIOS 名称映射到 IP 地址。WebVPN 需要 NetBIOS 来访问或共享远程系统上的文件。

**nbns-server**{*ipaddr*|主机名}[**master** ][**timeout***timeout*][**retry***retries*]
**no nbns-server**

## Syntax Description

| | |
|---|---|
| *hostname* | 指定 NBNS 服务器的主机名。 |
| *ipaddr* | 指定 NBNS 服务器的 IP 地址。 |
| **master** | 表示这是主浏览器而不是 WINS 服务器。 |
| **retry** | 表示后面是一个重试值。 |
| *retries* | 指定重试 NBNS 服务器查询的次数。在发送错误消息之前，ASA 会按照您在此处指定的次数循环遍历服务器列表。默认值为 2；范围为 1 至 10。 |
| **timeout** | 表示后面是超时值。 |
| *timeout* | 指定 ASA 再次发送查询之前等待的时间（如果只有一个服务器，则向同一服务器发送查询；如果有多个 NBNS 服务器，则向另一个服务器发送查询）。默认超时是 2 秒，范围是 1 至 30 秒。 |

## Command Default

默认没有配置NBNS服务器。

## 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 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 7.1(1) | 已从 webvpn 模式进入隧道组 webvpn 配置模式。 |

## 使用指南

在版本 7.1(1) 中，如果您在 webvpn 配置模式下输入此命令，它将转换为 tunnel-group webvpn-attributes 配置模式下的相同命令。

最多 3 个服务器条目。您配置的第一台服务器为主服务器，其他为备用服务器（用于实现冗余）。

使用 **no** 选项从配置中删除匹配的条目。

## CR_Examples

以下示例显示如何配置具有 NBNS 服务器（作为主浏览器）的隧道组“test”，IP 地址为 10.10.10.19，超时值为 10 秒，重试次数为 8。它还显示如何使用 IP 地址 10.10.10.24、15 秒的超时值和 8 次重试来配置 NBNS WINS 服务器。

```
ciscoasa
(config)#
 tunnel-group test type webvpn
ciscoasa
(config)#
 tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| clear configure group-policy | 删除特定组策略或所有组策略的配置。 |
| show running-config group-policy | 显示特定组策略或所有组策略正在运行的配置。 |
| tunnel-group webvpn-attributes | 指定命名隧道组的 WebVPN 属性。 |

# neighbor (router eigrp)

要定义与其交换路由信息的 EIGRP 邻居路由器，请在路由器 eigrp 配置模式下使用 **neighbor** 命令。要删除邻居条目，请使用此命 **no**令的形式。

**neighbor***IP* 地址**interface**名称
**no neighbor***IP* 地址**interface**名称

## Syntax Description

| | |
|---|---|
| **interface***name* | **nameif** 命令所指定的接口名称，通过该接口可访问邻居。 |
| *ip_address* | 与其交换路由信息的邻居路由器的 IPv4 或 IPv6 地址。 |

## 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 |
| 路由器 eigrp 配置 | — | • | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.0(2) | 添加了此命令。 |
| 9.20(1) | 增加了对 IPv6 的支持。 |

## 使用指南

可以使用多个 neighbor 语句来与特定 EIGRP 邻居建立对等会话。必须在 neighbor 语句中指定 EIGRP 交换路由更新所使用的接口。两个 EIGRP 邻居交换路由更新所使用的接口必须使用来自同一网络的 IP 地址进行配置。

注释 为接口配置该命令将抑制该接口上的**passive-interface**所有传入和传出的路由更新和 hello 消息。无法在配置为被动的接口上建立或维护 EIGRP 邻居邻接关系。

EIGRP 问候消息作为单播消息发送到使用 **neighbor** 命令定义的邻居。

## CR_Examples

以下示例配置与 192.168.1.1 和 192.168.2.2 邻居的 EIGRP 对等会话：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

## CR_Examples

以下示例配置与 fe80::250:56ff:feb9:b41b 和 fe80::250:56ff:fe9f:13f4 邻居的 EIGRP 对等会话：

```
ciscoasa(config)# rtr eigrp 100
ciscoasa(config-rtr)# neighbor fe80::250:56ff:feb9:b41b interface gig1
ciscoasa(config-rtr)# neighbor fe80::250:56ff:fe9f:13f4 interface branch_office
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **debugeigrpneighbors** | 显示 EIGRP 邻居消息的调试信息。 |
| **showeigrpneighbors** | 显示 EIGRP 邻居表。 |

# neighbor (router ospf)

要在点对点非广播网络上定义静态邻居，请在路由器 ospf 配置模式下使用 **neighbor** 命令。要从配置中删除静态定义的邻居，请使用此命令的 **no** 形式。

**neighbor***IP* 地址 [**interface** 名称]
**no neighbor***IP* 地址 [**interface** 名称]

## Syntax Description

| | |
|---|---|
| **interface***name* | （可选）指定 **nameif** 命令所指定的可以通过其访问邻居的接口名称。 |
| *ip_address* | 指定邻居路由器的 IP 地址。 |

## 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 |
| 路由器 ospf 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。 |

## 使用指南

**neighbor** 命令用于通过 VPN 隧道通告 OSPF 路由。必须为每个已知的非广播网络邻居包含一个邻居条目。邻居地址必须在接口的主地址上。

当邻居与系统的任何直接连接的接口不在同一网络上时，需要指定 **interface** 选项。此外，必须创建静态路由才能到达邻居。

## CR_Examples

以下示例使用地址 192.168.1.1 定义了邻居路由器：

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **routerospf** | 进入路由器配置模式。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configrouter** | 显示全局路由器配置中的 命令。 |

# neighbor activate

要启用与边界网关协议 (BGP) 邻居的信息交换，请在 address-family 配置模式下使用 neighbor activate 命令。要禁用与 BGP 邻居交换地址，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **activate**
**no neighbor** { *ip_address* | *ipv6-address* } **activate**

## Syntax Description

| | |
|---|---|
| *ip_address* | BGP 路由器的 IP 地址。 |
| ipv6-address | BGP 路由器的 IPv6 地址 |

## Command Default

对于 IPv4 地址系列，默认情况下与 BGP 邻居启用地址交换。无法为任何其他地址系列启用地址交换。

注释 默认情况下，对于通过 neighbor remote-as 命令定义的每个 BGP 路由会话，启用 IPv4 地址系列的地址交换；否则，除非在配置 neighbor remote-as 命令之前配置了 no bgp default ipv4-activate 命令，或者使用了 no neighbor activate 命令禁用了与特定邻居的地址交换。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 增加了 ipv6-address 参数以及对 IPv6 地址系列的支持。 |

## 使用指南

您可以使用此命令以 IP 前缀的形式通告地址信息。地址前缀信息在 BGP 中称为网络层可达性信息 (NLRI)。

## CR_Examples

以下示例为 BGP 邻居 172.16.1.1 启用 IPv4 地址系列单播的地址交换：

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

以下示例显示如何为名为 group2 的 BGP 对等体组中的所有邻居以及 BGP 邻居 7000::2 启用地址系列 IPv6 的地址交换：

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **neighborremote-as** | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |

# neighbor advertise-map

要通告 BGP 表中与已配置的路由映射匹配的路由，请在路由器配置模式下使用 neighbor advertise-map 命令。要禁用路由通告，请使用此命令的no形式。

**neighbor** { *ip_address* | *ipv6-address* } **advertise-map***map-name* { **exist-map***map-name*| **non-exist-map***map-name* } [ **check-all-paths** ]
**no neighbor** { *ip_address* | *ipv6-address* } **advertise-map***map-name* { **exist-map***map-name*| **non-exist-map***map-name* } [ **check-all-paths** ]

## Syntax Description

| | |
|---|---|
| *ipv4_address* | 指定应接收条件通告的路由器的 IPv4 地址。 |
| ipv6_address | 指定应接收条件通告的路由器的 IPv6 地址。 |
| advertise-map map-name | 指定在满足存在映射或不存在映射的条件时将被通告的路由映射的名称。 |
| exist-map map-name | 指定exist-map的名称，与BGP表中的路由进行比较，以确定是否通告advertise-map路由。 |
| **non-exist-mapmap-name** | 指定不存在的映射表名称，与 BGP 表中的路由进行比较，以确定是否发布 advertise-map 路由。 |
| check-all-paths | （可选）启用 BGP 表中带有前缀的现有映射检查所有路径。 |

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

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

## 使用指南

使用 neighbor advertise-map 命令有条件地通告选定路由。有条件通告的路由（前缀）在两个路由映射中定义：通告映射以及存在映射或非存在映射。

与存在映射或非存在映射关联的路由映射指定 BGP 发言者将跟踪的前缀。

与通告映射关联的路由映射指定条件满足时将通告到指定邻居的前缀。

如果配置了存在映射，则当前缀同时存在于广告映射和存在映射中时，满足条件。

如果配置了不存在的映射，则当前缀在广告映射中存在，但在不存在的映射中不存在时，满足条件。

如果条件未满足，则路由将撤消并且不会进行条件通告。可能已动态通告或未通告的所有路由都需要在 BGP 路由表中存在才能进行条件通告。

## CR_Examples

以下路由器配置示例将 BGP 配置为检查所有：

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

以下地址系列配置示例将 BGP 配置为使用非存在映射有条件地向 10.1.1.1 邻居通告前缀。如果前缀存在于 MAP3 中而不是 MAP4 中，则满足条件并通告前缀。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

以下对等组配置示例将 BGP 配置为针对 BGP 邻居的前缀检查所有路径：

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor route1 send-community both
ciscoasa(config-router-af)# neighbor route1 advertise-map MAP1 exist-map MAP2 check-all-paths
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址系列配置模式。 |

# neighbor advertisement-interval

要设置发送 BGP 路由更新之间的最小路由通告间隔 (MRAI)，请在 address-family 配置模式下使用 neighbor advertise-interval 命令。要恢复默认值，请使用此命令的no形式

**neighbor** { *ip_address* | *ipv6-address* } **advertisement-interval***seconds*
**no neighbor** { *ip_address* | *ipv6-address* } **advertisement-interval***seconds*

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址 |
| seconds | 发送BGP路由更新的最小时间间隔。<br>有效值介于 0 到 600 之间。 |

## Command Default

不在 VRF 中的 eBGP 会话：30 秒

VRF 中的 eBGP 会话：0 秒

iBGP 会话：0 秒。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

当 MRAI 等于 0 秒时，一旦 BGP 路由表发生更改，就会发送 BGP 路由更新。

## CR_Examples

以下示例将发送 BGP 路由更新的最小间隔时间设置为 10 秒：

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

以下示例将发送 BGPv6 路由更新的最小间隔时间设置为 100 秒：

```
asa(config-router-af)# neighbor 2001::1 advertisement-interval 100
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **neighborremote-as** | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |

# neighbor default-originate

要允许BGP发言者（本地路由器）将默认路由0.0.0.0发送至邻居以用作默认路由，请在address-family配置模式下使用 neighbor default- originate 命令。要不发送任何路由作为默认值，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **default-originate** [ **route-map***route-map name* ]
**no neighbor** { *ip_address* | *ipv6-address* } **default-originate** [ **route-map***route-map name* ]

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| route-map路由映射名称 | （可选）路线图的名称。路由映射允许有条件地注入路由0.0.0.0。 |

## Command Default

不会向邻居发送默认路由。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此命令不要求本地路由器中存在0.0.0.0。与路由图一起使用时，如果路由图包含匹配IP地址子句并且存在与 IP 访问列表完全匹配的路由，则会注入默认路由 0.0.0.0。路由映射还可以包含其他 match 子句。

可以将标准或扩展访问列表与 neighbor default-Originate 命令配合使用。

## CR_Examples

在以下示例中，本地路由器无条件地将路由 0.0.0.0 注入邻居 72.16.2.3：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
In the following example, the local router injects route 0.0.0.0 to the neighbor 2001::1:
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **neighborremote-as** | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |

# 邻居描述

要将描述与邻居关联，请在地址系列配置模式下使用 neighbor description 命令。要删除描述，请使用此命令的no形式。

**neighbor** { *ip_address* | *ipv6-address* } **description** 文本
**no neighbor** { *ip_address* | *ipv6-address* } **description** 文本

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 文本 | 用于描述邻居的文本（长度最多为 80 个字符）。 |

## Command Default

没有该邻居的说明信息。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## CR_Examples

在以下示例中，邻居的说明是“peer with example.com”：

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

在以下示例中，IPv6 邻居的描述为“peer with example.com”：

```
ciscoasa(config-router-af)#neighbor 2001::1 description peer with example.com
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **neighborremote-as** | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |

| 命令 | 说明 |
| --- | --- |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |

# neighbor disable-connected-check

要禁用连接验证以与使用环回接口的单跳对等体建立 eBGP 对等会话，请在地址系列配置模式下使用邻居 disable-connected-check 命令。要启用 eBGP 对等会话的连接验证，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **disable-connected-check**
**no neighbor** { *ip_address* | *ipv6-address* } **disable-connected-check**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |

## Command Default

BGP路由进程会默认验证单跳eBGP对等会话（TTL=254）的连接性，判断eBGP对等体是否直连到同一个网段。如果对等体没有直连到同一网段，连接验证将阻止建立对等会话。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

neighbour disable-connected-check 命令用于禁用可通过单跳到达但在环回接口上配置或使用非直接连接 IP 地址配置的 eBGP 对等会话的连接验证过程。

仅当邻居 ebgp-multihop 命令配置的 TTL 值为 1 时，才需要此命令。单跳 eBGP 对等体的地址必须可访问。必须配置 neighbor update-source 命令，以允许 BGP 路由进程将环回接口用于对等会话。

## CR_Examples

在以下示例中，配置了可在同一网段上通过每台路由器上的本地环回接口访问的两个 BGP 对等体之间的单跳 eBGP 对等会话：

BGP Peer 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
```

```
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
BGP Peer 2
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
BGPv6 Peer
ciscoasa(config-router)# neighbor 2001::1 disable-connected-check
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **neighborremote-as** | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |
| neighbor ebgp-multihop | 接受或启动与位于非直接连接网络上的外部对等体的BGP连接。 |

# neighbor distribute-list

要分发访问列表中指定的 BGP 邻居信息，请在地址系列配置模式下使用 neighbor Distribution-list 命令。要删除条目，请使用此命令的 no 形式。

**neighbor***ip_address***distribute-list** {**access-list-name**} {**in** | **out**}
**no neighbor***ip_address***distribute-list** {**access-list-name**} {**in** | **out**}

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| access-list-name | 标准访问列表的名称。 |
| 范围 | 访问列表适用于该邻居的传入广告 |
| out | 访问列表适用于向该邻居发出的通告 |

## Command Default

未指定 BGP 邻居。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |

## 使用指南

使用分发列表是过滤通告的多种方法的一种。也可以使用以下方法过滤通告：

- 自治系统路径过滤器可以使用 ip as-path access-list 和 neighbor filter-list 命令进行配置。
- 可以使用 access-list（IP standard）命令配置标准访问列表，用于过滤通告。
- 可以使用 route-map (IP) 命令过滤通告。可以使用自治系统过滤器、前缀过滤器、访问列表和分发列表来配置路由映射。

标准访问列表可用于过滤路由更新。但是，对于使用无类域间路由 (CIDR) 的路由过滤，标准访问列表不提供配置网络地址和掩码高级过滤所需的精细级别。

## CR_Examples

在以下示例中，标准访问列表分发列表acl中的BGP邻居信息被应用于传入到邻居172.16.4.1的通告。

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与BGP邻居的信息交换。 |
| 网络 | 指定要由 BGP 通告的网络。 |
| access-list permit | 指定要转发的数据包。 |
| access-list deny | 指定要拒绝的数据包。 |

# neighbor ebgp-multihop

要接受并尝试与未直接连接的网络上的外部对等体建立 BGP 连接，请在 address-family 配置模式下使用 neighbor ebgp-multihop 命令。要恢复默认值，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **ebgp-multihop** [ **ttl** ]
**no neighbor** { *ip_address* | *ipv6-address* } **ebgp-multihop**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| ttl | （可选）生存时间。<br>有效值介于 1 至 255 跳之间。 |

## Command Default

仅允许直接连接的邻居。

## 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 |
| 地址族配置模式 | • 是 | • — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此功能只能在思科技术支持人员的指导下使用。为了防止通过振荡路由创建环路，如果通往多跳对等体的唯一路由是默认路由 (0.0.0.0)，则将不会建立多跳。

## CR_Examples

以下示例允许进出邻居 10.108.1.1 的连接，该邻居位于未直连的网络上：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

以下示例允许进出邻居 2001::1 的连接，该邻居位于未直连的网络上：

```
ciscoasa(config)# router bgp 3
```

```
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af) neighbor 12001::1 ebgp-multihop
```

## Related Commands

| 命令 | 说明 |
| --- | --- |
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与BGP邻居的信息交换。 |

# neighbor fall-over bfd (router bgp)

要配置对 BGP 的 BFD 支持，以便注册 BGP 以接收来自 BFD 的转发路径检测失败消息，请在配置邻居时使用 **fall-over** 选项。

**neighbor***ip_address* | *ipv6_address***fall-over bfd**

## Syntax Description

| | |
|---|---|
| *ip_address/ipv6_address* | 邻居路由器的 IP/IPv6 地址 ABCD/ X:X:X:X::X 格式。 |

## 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 |
| 路由器 BFD 配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 添加了此命令。 |

## 使用指南

为多跳配置 BGP 的 BFD 支持时，请确保已为源目标对创建 BFD 映射。

## CR_Examples

以下示例为 172.16.10.2 和 1001::2 邻居配置 BFD 支持：

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.10.2 fall-over bfd
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 1001::2 fall-over bfd
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **authentication** | 在 BFD 模板中为单跳和多跳会话配置身份验证。 |
| bfd echo | 在接口上启用 BFD 回声模式， |
| **bfdinterval** | 在接口上配置基准 BFD 参数。 |
| bfd 映射 | 配置将地址与多跳模板关联的 BFD 映射。 |

| 命令 | 说明 |
| --- | --- |
| bfd 慢计时器 | 配置 BFD 慢速计时器值。 |
| BFD模板 | 将单跳 BFD 模板绑定到接口。 |
| bfd-template单跳\|多跳 | 配置 BFD 模板并进入 BFD 配置模式。 |
| 清除 BFD 计数器 | 清除 BFD 计数器。 |
| echo | 在 BFD 单跳模板中配置回应。 |
| show bfd drops | 显示 BFD 中已丢弃的数据包数。 |
| show bfd map | 显示配置的 BFD 映射。 |
| show bfd neighbors | 显示现有 BFD 邻接关系逐行列表。 |
| show bfd summary | 显示 BFD 的概要信息。 |

# neighbor filter-list

要设置 BGP 过滤器，请在地址系列配置模式下使用 neighbor filter-list 命令。要禁用该功能，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **filter-list***access-list-name* { **in** | **out** }
**no neighbor** { *ip_address* | *ipv6-address* } **filter-list***access-list-name* { **in** | **out** }

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| access-list-name | 自主系统路径访问列表的名称。您可以使用 as-path access-list 命令定义此访问列表。 |
| 范围 | 访问列表应用于传入路由。 |
| out | 访问列表将应用于传出路由。 |

## Command Default

不使用 BGP 过滤器。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此命令将在入站和出站 BGP 路由上建立过滤器。

**注释** 请勿在任何给定方向（入站或出站）上同时将邻居分发列表和邻居前缀列表命令应用于邻居。这两个命令是互斥的，并且每个入站或出站方向只能应用一个命令（邻居分发列表或邻居前缀列表）。

## CR_Examples

在以下地址系列配置模式示例中，不会向使用 IP 地址 172.16.1.1 的 BGP 邻居发送通过或从相邻自治系统 123 发送的有关任何路径的通告：

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_
ciscoasa(config)# as-path access-list as-path-acl deny ^123$
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

在以下地址系列配置模式示例中，系统不会向 IP 地址为 2001::1 的 BGPv6 邻居发送关于任何通过或从相邻自治系统传递的路径的通告：

```
ciscoasa(config-router-af)# neighbor 2001::1 filter-list as-path-acl out
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| neighbor remote-as | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |
| 网络 | 指定 BGP 路由进程要通告的网络。 |

# neighbor ha-mode graceful-restart

要为 BGP 邻居启用或禁用边界网关协议 (BGP) 平稳重启功能，请在 address-family 配置模式下使用 neighbor ha-mode graceful-restart 命令。要从配置中删除邻居的 BGP 平稳重启功能，请使用此命令的 no 形式。

**neighbor***ip_address***ha-mode graceful-restart** [**disable**]
**no neighbor***ip_address***ha-mode graceful-restart**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居的 IP 地址。 |
| disable | （可选）禁用邻居的BGP平滑重启功能。 |

## Command Default

BGP平滑重启功能处于关闭状态。

## 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 |
| Address-family 配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

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

## 使用指南

neighbor ha-mode graceful-restart 命令用于为单个 BGP 邻居启用或禁用平稳重启功能。如果以前为 BGP 对等体启用了平稳重启，则使用 disable 关键字可禁用平稳重启功能。

会话建立过程中，在 OPEN 消息中支持无间断转发 (NSF) 和 NSF 感知的对等体之间协商平稳重启功能。如果在建立 BGP 会话后启用了平滑重启功能，则需要通过软重置或硬重置重新启动会话。

具备 NSF 功能和 NSF 感知的 ASA 支持平稳重启功能。支持 NSF 功能的 ASA 可以执行状态切换 (SSO) 操作（平稳重启），并且可以通过在 SSO 操作期间保留路由表信息来协助对等体重启。支持 NSF 感知的 ASA 与支持 NSF 功能但无法执行 SSO 操作的路由器类似。

注释 要对所有 BGP 邻居全局启用 BGP 平稳重启功能，请使用 bgp graceful-restart 命令。为单个邻居配置 BGP平稳重启功能时，每种配置重启的方法具有相同的优先级，并且最后的配置实例将应用于邻居。

使用 show bgp neighbors 命令验证 BGP 邻居的 BGP 平稳重启配置。

## CR_Examples

以下示例为 BGP 邻居 172.21.1.2 启用 BGP 平稳重启功能：

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

## Related Commands

| 命令 | 说明 |
| --- | --- |
| **bgpgraceful-restart** | 为所有 BGP 邻居全局启用或禁用 BGP 平稳重启功能。 |
| show bgp neighbors | 显示有关与邻居的 TCP 和 BGP 连接的信息。 |

# neighbor local-as

要自定义从外部边界网关协议 (eBGP) 邻居接收的路由的 AS_PATH 属性，请在地址系列配置模式下使用邻居 local-as 命令。要禁用 AS_PATH 属性定制，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **local-as** [ *autonomous-system-number* [ **no-prepend** [ **replace-as** [ **dual-as** ] ] ] ]
**no neighbor** { *ip_address* | *ipv6-address* } **local-as**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 自治系统编号 | （可选）要添加到 AS_PATH 属性的自治系统编号。此参数的值范围是从 1 到 65535 的任意有效的自治系统编号。<br>注释<br>使用此参数，您无法从本地 BGP 路由进程或远程对等方的网络指定自治系统编号。<br>有关自治系统编号格式的详细信息，请参阅 router bgp 命令。 |
| 无预置 | （可选）不要将本地自治系统编号添加到从 eBGP 邻居接收的任何路由之前。 |
| 替换为 | （可选）在 eBGP 更新中将实际自治系统编号替换为本地自治系统编号。来自本地 BGP 路由过程的自主系统编号不会预置到前面。 |
| 双重 AS | （可选）配置 eBGP 邻居使用真实自治系统编号（来自本地 BGP 路由进程）或使用通过 autonomous-system-number 参数配置的自治系统编号 (local-as) 建立对等会话。 |

## Command Default

默认情况下，本地 BGP 路由进程的自治系统编号会被添加到所有外部路由的前面。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

neighbour local-as 命令用于通过添加和删除从 eBGP 邻居接收的路由的自治系统编号来定制 AS_PATH 属性。为了支持自治系统编号迁移，此命令的配置允许路由器作为其他自治系统的成员显示为外部对等体。此功能允许网络运营商在正常服务时段将客户迁移到新配置而无需中断现有的对等布置，简化了在 BGP 网络中更改自治系统编号的过程。

⚠

注意 BGP 预置路由穿越的每个 BGP 网络的自治系统号，以维护网络可达性信息和防止路由环路。此命令应仅针对自主系统迁移进行配置，并且应在转换完成后取消配置。此程序应仅由经验丰富的网络操作员尝试执行。配置不当可能会造成路由环路

此命令仅可用于真正的 eBGP 对等会话。此命令不适用于联盟的不同子自治系统中的两个对等体。

为确保顺利过渡，我们建议将使用 4 字节自主系统编号标识的自主系统中的所有 BGP 发言者升级为支持 4 字节自主系统编号。

## CR_Examples

### 本地 AS 示例

以下示例使用 local-as 功能通过自治系统 300 在 Router 1 和 Router 2 之间建立对等关系：

**Router1(Localrouter)**

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300Router 2 (Remote router)
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

### 无预置关键字配置示例

以下示例将 BGP 配置为不将自治系统 500 预置到从 192.168.1.1 邻居接收的路由：

```
ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend
```

### 替换为关键字配置示例

以下示例从 172.20.1.1 邻居的出站路由更新中删除专用自治系统 64512，并将其替换为自治系统 600：

```
ciscoasa(config)# router bgp 64512

ciscoasa(config-router)# address-family ipv4

ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as
```

```
ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as
```

### 双重 as 关键字配置示例

以下示例显示了两个运营商网络和一个客户网络的配置。路由器 1 属于自治系统 100，路由器 2 属于自治系统 200。自治系统 200 正在合并到自治系统 100 中。发生这种转换需要在不中断自治系统 300（客户网络）中路由器 3 的服务的情况下进行。在路由器 1 上配置 neighbor local-as 命令，以允许路由器 3 在过渡期间保持与自治系统 200 的对等关系。在过渡完成后，可以在正常维护窗口或其他计划停机期间，将路由器 3 上的配置更新为自治系统 100 的对等体。

**Router1Configuration(LocalProviderNetwork)**

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

**Router2Configuration(RemoteProviderNetwork)**

```
ciscoasa(config)# router bgp 200

ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
 ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

**Router3Configuration(RemoteCustomerNetwork)**

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

为了在两个自治系统合并后完成迁移，需要在路由器 3 上更新对等会话：

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

BGPv6 配置

```
ciscoasa(config-router-af)# neighbor 2001::1 local-as 500 no-prepend
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| bgp router-id | 为本地边界网关协议 (BGP) 路由进程配置固定的路由器 ID。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| neighbor remote-as | 向 BGP 或多协议 BGP 邻居表添加一个条目。 |

| 命令 | 说明 |
| --- | --- |
| 网络 | 指定 BGP 路由进程要通告的网络。 |
| synchronization | 实现 BGP 与内部网关协议 (IGP) 系统之间的同步 |

# neighbor maximum-prefix

要控制可从邻居接收的前缀的数量，请在地址系列配置模式下使用 neighbor maximum-prefix 命令。要禁用该功能，请使用此命令的 no 形式。

**neighbor** {*ip_address* | *ipv6-address*} **maximum-prefix***maximum* [*threshold* ] [**restart** *restart-interval*] [**warning-only**]
**no neighbor** {*ip_address* | *ipv6-address*} **maximum-prefix***maximum*

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 最大值 | 此邻居允许的最大前缀数。 |
| 阈值 | （可选）整数，指定路由器在达到最大值的百分比时开始生成警告消息。范围为 1 至 100，默认值为 75（百分比）。 |
| restart | （可选）配置运行 BGP 的路由器，以自动重新建立因超过最大前缀限制而被禁用的对等会话。重启计时器使用 restart-interval 参数配置。 |
| restart-interval | （可选）重新建立对等会话的时间间隔（以分钟为单位）。范围是 1 至 65535 分钟。 |
| 仅警告 | （可选）允许路由器在超过最大值时生成日志消息，而不是终止对等连接。 |

## Command Default

此命令默认禁用。前缀的数量没有限制。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

使用此命令可以配置允许 BGP 路由器从对等体接收的前缀的最大数量。它添加了另一种机制（除了分发列表、过滤列表和路由映射之外）来控制从对等体接收的前缀。

当收到的前缀数量超过配置的最大数量时，路由器将终止对等（默认情况下）。但是，如果配置了 warning-only 关键字，则路由器只发送日志消息，但会继续与发送方建立对等关系。如果对等体终止，对等体将保持关闭，直到发出 clear bgp 命令为止。

## CR_Examples

以下示例将允许从 192.168.6.6 的邻居发送的前缀的最大数量设置为 1000：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

以下示例将所允许的来自 2001::1 的邻居的前缀的最大数量设置为 1000：

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| 网络 | 指定 BGP 路由进程要通告的网络。 |

# neighbor next-hop-self

要将路由器配置为 BGP 发言邻居的下一跳，请在地址系列配置模式下使用 neighbor next-hop-self 命令。要禁用此功能，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **next-hop-self**
**no neighbor** { *ip_address* | *ipv6-address* } **next-hop-self**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 仅警告 | （可选）允许路由器在超过最大值时生成日志消息，而不是终止对等连接。 |

## Command Default

此命令默认禁用。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此命令在无网状结构的网络（例如帧中继或 X.25）中非常有用，在该类网络中，BGP 邻居可能没有对同一 IP 子网上所有其他邻居的直接访问权限。

## CR_Examples

以下示例强制以 10.108.1.1 为目标的所有更新将此路由器通告为下一跳：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

以下示例强制以 2001::1 为目标的所有更新将此路由器通告为下一跳：

```
ciscoasa(config-router-af)#neighbor 2001::1 next-hop-selfs
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与BGP邻居的信息交换。 |

# neighbor password

要在两个 BGP 对等体之间的 TCP 连接上启用消息摘要 5 (MD5) 身份验证，请在地址系列配置模式下使用 neighbor password 命令。要禁用该功能，请使用此命令的no形式

**neighbor** { *ip_address* | *ipv6-address* } **password** [ **0-7** ] *string*
**no neighbor** { *ip_address* | *ipv6-address* } **password**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 字符串 | 区分大小写的密码，长度最多为 25 个字符。<br>第一个字符不能为数字。此字符串包含任意字母数字字符，包括空格。不能指定 number-space-anything 格式的密码。数字后的空格会导致身份验证失败。 |
| 0-7 | （可选）加密类型。0-6 表示未加密。7 用于加密。 |

## Command Default

未对两个 BGP 对等体之间的 TCP 连接进行 MD5 身份验证。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

您可以在两个 BGP 对等体之间配置 MD5 身份验证，这意味着在对等体之间的 TCP 连接上发送的每个数据段都需要验证。必须在两个 BGP 对等体上使用相同的密码配置 MD5 身份验证；否则，将无法在它们之间建立连接。配置 MD5 身份验证会使 ASA 软件生成和检查 TCP 连接上发送的每个分段的 MD5 摘要。

配置时，无论是否启用 service password-encryption 命令，都可以提供区分大小写的密码（最多 25 个字符）。如果密码的长度超过25个字符，将显示错误消息，并且不接受密码。此字符串包含任意字母数字字符，包括空格。密码不能配置为 number-space-anything 格式。数字后的空格会导致身份验证失败。您还可以使用以下符号字符与字母数字字符的任意组合：

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < . , ?

注意 如果身份验证字符串配置不正确，则不会建立BGP对等会话。我们建议您在配置身份验证后仔细输入身份验证字符串，并验证对等会话是否建立。

如果一个路由器为邻居配置了密码，但邻居路由器没有配置密码，那么当路由器尝试在它们之间建立 BGP 会话时，控制台上会显示如下消息：

%TCP-6-BADAUTH：从 [对等体的 IP 地址]：11003 到 [本地路由器的 IP 地址]：179 没有 MD5 摘要

同样，如果两个路由器配置了不同的密码，屏幕上会显示如下消息：

%TCP-6-BADAUTH：从 [对等体的 IP 地址]：11004 到 [本地路由器的 IP 地址]：179 的 MD5 摘要无效

### 在已建立的 BGP 会话中配置 MD5 密码

如果配置或更改用于两个 BGP 对等体之间 MD5 身份验证的密码或密钥，则在您配置密码后，本地路由器不会终止现有会话。本地路由器将尝试使用新密码保持对等会话，直到 BGP 抑制计时器到期。默认时间段为 180 秒。如果在抑制计时器到期之前未在远程路由器上输入或更改密码，则会话将超时。

注释 为抑制计时器配置新的计时器值只有在会话重置后才会生效。因此，无法更改抑制计时器的配置，以避免重置 BGP 会话。

## CR_Examples

以下示例为 10.108.1.1 邻居的对等会话配置 MD5 身份验证。在抑制计时器到期之前，必须在远程对等体上配置相同的密码：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

以下示例在禁用 service password-encryption 命令时为超过 25 个字符的密码配置。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
 ciscoasa(config-router-af)# neighbor 209.165.200.225 password 12345678912345678912345678901

    % BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
 no service password-encryption
  neighbor 209.165.200.225 password 123456789123456789123456
```

在以下示例中，如果在启用 service password-encryption 命令的情况下配置超过 25 个字符的密码，则会出现错误消息。

```
 Router(config)# service password-encryption
```

```
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901

% BGP: Password length must be less than or equal to 25.
 Router(config-router)# do show run | i password  service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| bgp router-id | 为本地边界网关协议(BGP)路由进程配置固定的路由器ID。 |
| neighbor remote-as | 向 BGP 或多协议 BGP 邻居表中添加一个条目。 |

# neighbor prefix-list

要阻止分发前缀列表中指定的边界网关协议 (BGP) 邻居信息，请在地址系列配置模式下使用 neighbor prefix-list 命令。要删除过滤器列表，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **prefix-list***prefix-list-name* { **in** | **out** }
**no neighbor** { *ip_address* | *ipv6-address* } **prefix-list***prefix-list-name* { **in** | **out** }

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| IPv6 地址 | 邻居路由器的 IPv6 地址。 |
| prefix-list-name | 前缀列表的名称。 |
| 范围 | 过滤列表适用于来自该邻居的传入广告。 |
| out | 过滤列表适用于向该邻居发出的通告。 |

## Command Default

所有外部地址和通告的地址前缀都会分发给 BGP 邻居。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

使用前缀列表是过滤 BGP 通告的三种方法的一种。您还可以使用 AS 路径过滤器来过滤 BGP 通告。AS 路径过滤器通过 ip as-path access-list 全局配置命令进行定义，并在 neighbor filter-list 命令中使用。过滤 BGP 通告的第三种方法是将访问列表或前缀列表与 neighbor deploy-list 命令配合使用。

**注释** 请勿在任何给定方向（入站或出站）上同时将邻居分发列表和邻居前缀列表命令应用于邻居。这两个命令是互斥的，并且每个入站或出站方向只能应用一个命令（邻居分发列表或邻居前缀列表）。

## CR_Examples

以下地址系列配置模式示例将名为 abc 的前缀列表应用于从邻居 10.23.4.1 传入的通告：

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

以下地址系列路由器配置模式示例将名为CustomerA的前缀列表应用于传出到邻居10.23.4.3的传出通告：

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
The following address family router configuration mode example applies the prefix list named
 CustomerA to outgoing advertisements to neighbor 2001::1:
ciscoasa(config-router-af)#neighbor 2001::1 prefix-list CustomerA out
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| 网络 | 指定BGP路由进程要通告的网络。 |

# neighbor remote-as

要将条目添加到 BGP 或多协议 BGP 邻居表，请在 address-family 配置模式下使用 neighbor remote-as 命令。要从表中删除条目，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*
**no neighbor** { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 自治系统编号 | 邻居所属的自治系统的编号，范围为 1 到 65535。<br>有关自治系统编号格式的详细信息，请参阅 router bgp 命令。<br>与关键字 Alternative-as 一起使用时，最多可输入五个自治系统编号。 |

## Command Default

没有 BGP 或多协议 BGP 邻居对等体。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

如果为邻居指定的邻居的自治系统编号与在路由器 bgp 全局配置命令中指定的自治系统编号相匹配，则该邻居标识为本地自治系统的内部邻居。否则，邻居将被视为外部邻居。

默认情况下，在路由器配置模式下使用 neighbor remote-as 命令定义的邻居仅交换单播地址前缀。

使用alternate-as 关键字用于指定最多五个备用自治系统，可以在这些系统中标识动态 BGP 邻居。BGP 动态邻居支持允许 BGP 与由一系列 IP 地址定义的一组远程邻居。使用一系列 IP 地址和 BGP 对等体组配置 BGP 动态邻居。在使用 bgplisten 命令配置子网范围并将其与 BGP 对等组关联后，如果为该子网范围内的 IP 地址启动 TCP 会话，则会动态创建新的 BGP 邻居作为该组的成员。新 BGP 邻居将继承该组的所有配置或模板。

思科 4 字节自治系统编号的实施使用 asplain（例如 65538）作为自治系统编号的默认正则表达式匹配和输出显示格式，但您可以使用 asplain 格式和 asdot 格式配置 4 字节自治系统编号。 RFC 5396 中所述。要更改默认的正则表达式匹配并将 4 字节自治系统编号的输出显示为 asdot 格式，请使用 bgp asnotation dot 命令，后跟 clear bgp * 命令以硬重置所有当前 BGP 会话。

## CR_Examples

以下示例指定位于地址 10.108.1.2 的路由器是编号为 65200 的自治系统中的内部 BGP (iBGP) 邻居：

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

以下示例将一台 BGP 路由器分配给自治系统 65400，并且两个网络被列为源自自治系统。然后列出三个远程路由器（及其自治系统）的地址。正在配置的路由器将与邻居路由器共享有关网络 10.108.0.0 和 192.168.7.0 的信息。第一个路由器是与输入此配置的路由器（eBGP 邻居）位于不同自治系统中的远程路由器；第二个 neighbor remote-as 命令显示地址为 10.108.234.2 的内部 BGP 邻居（具有相同的自治系统编号）； last neighbor remote-as 命令指定的邻居与输入此配置的路由器位于不同的网络上（也是 eBGP 邻居）。

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

以下示例将自治系统 65001 中的邻居 10.108.1.1 配置为仅交换单播路由：

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31 1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| 网络 | 指定 BGP 路由进程要通告的网络。 |
| 邻居删除专用 AS | 从eBGP出站路由更新中删除私有自治系统编号。 |

# neighbor remove-private-as

要从 eBGP 出站路由更新中删除专用自治系统编号，请在 address-family 配置模式下使用 neighbor remove-private-as 命令。要禁用该功能，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **remove-private-as** [ **all** [ **replace-as** ] ]
**no neighbor** { *ip_address* | *ipv6-address* } **remove-private-as** [ **all** [ **replace-as** ] ]

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| all | （可选）从传出更新的 AS 路径中删除所有专用 AS 编号。 |
| replace-as | （可选）只要指定了 all 关键字，replace-as 关键字就会导致 AS 路径中的所有专用 AS 编号替换为路由器的本地 AS 编号。 |

## Command Default

不会从 AS 路径中删除专用 AS 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此命令仅适用于外部 BGP (eBGP) 邻居。专用 AS 值范围为从 64512 到 65535。当更新传递到外部邻居时，如果 AS 路径包含专用 AS 编号，软件将丢弃专用 AS 编号

- neighbor remove-private-as 命令从 AS 路径中删除专用 AS 编号，即使路径同时包含公共和专用 ASN
- 即使 AS 路径仅包含专用 AS 编号，neighbor remove-private-as 命令也会删除专用 AS 编号。不可能出现 0 长度的 AS 路径，因为此命令只能应用于 eBGP 对等体，在这种情况下，本地路由器的 AS 编号会附加到 AS 路径。neighbor remove-private-as 命令会删除专用 AS 号，即使专用 ASN 在 AS 路径中出现在联盟网段之前也是如此。

- 从 AS 路径中删除专用 AS 编号后，发送的前缀的路径长度将减少。由于 AS 路径长度是 BGP 最佳路径选择的关键元素，因此可能有必要保留路径长度。通过将所有删除的 AS 编号替换为本地路由器的 AS 编号，replace-as 关键字可确保保留路径长度。
- 该功能可应用于每个地址系列的邻居。因此，您可以将该功能应用于一个地址系列中的邻居，而不应用于另一个地址系列中的邻居，从而影响仅针对配置了该功能的地址系列的出站端上的更新消息。

## CR_Examples

以下示例显示从发送到 172.16.2.33 的更新中删除专用 AS 编号的配置。结果是，10.108.1.1 通过 AS 100 通告的路径的 AS 路径将仅包含“100”（如自治系统 2051 所示）。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer

ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as


Router-in-AS100# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
 Advertised to non peer-group peers:
   172.16.2.33
 65001
    10.108.1.1 from 10.108.1.1
     Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
    172.16.2.32 from 172.16.2.32
     Origin IGP, metric 0, localpref 100, valid, external, best
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| 邻居描述 | 将说明与邻居相关联 |
| neighbor remote-as | 将 BGP 或多协议 BGP 路由条目添加到路由表。 |

# neighbor route-map

要将路由映射应用于传入或传出路由，请在地址系列配置模式下使用 neighbor route-map 命令。要删除路由图，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **route-map***map-name* { **in** | **out** }
**no neighbor** { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| map-name | 路由映射的名称。 |
| 范围 | 将路线图应用于传入路线。 |
| out | 将路由图应用于传出的路由。 |

## Command Default

没有路由映射应用于对等体。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

在地址系列配置模式下指定时，此命令仅将路由映射应用于该特定地址系列。在路由器配置模式下指定此命令时，此命令将仅将路由映射应用于 IPv4 单播路由。

如果指定了出站路由映射，则适当的行为是仅通告至少与路由映射的一个部分匹配的路由。

## CR_Examples

以下示例将名为 internal-map 的路由映射应用于来自 172.16.70.24 的 BGP 传入路由：

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
```

```
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

以下示例将名为 internal-map 的路由映射应用于来自 2001::1 的 BGP 传入路由：

```
ciscoasa(config-router-af)# neighbor 2001::1 route-map internal-map in
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| match as-path | 匹配访问列表指定的 BGP 自治系统路径 |
| route-map | 定义将路由从一个路由协议重新分发到另一个路由协议的条件。 |
| match as-path | 匹配访问列表指定的 BGP 自治系统路径。 |
| set local-preference | 指定自治系统路径的首选值。 |

# neighbor send-community

要指定应将社区属性发送到BGP邻居，请在address-family配置模式下使用neighbor send-community命令。要删除该条目，请使用此命令的no形式。

**neighbor** { *ip_address* | *ipv6-address* } **send-community**
**no neighbor** { *ip_address* | *ipv6-address* } **send-community**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的IP地址。 |
| ipv6-address | 邻居路由器的IPv6地址。 |

## Command Default

没有向任何邻居发送社区属性。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了ipv6-address参数，并添加了对IPv6地址系列的支持。 |

## CR_Examples

在以下地址系列配置模式示例中，路由器属于自治系统109，并被配置为将社区属性发送到IP地址为172.16.70.23的其邻居：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

在以下示例中，路由器被配置为将社区属性发送到IP地址为2001::1的邻居：

```
ciscoasa(config-router-af)# neighbor 2001::1 send-community
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |

# neighbor shutdown

要禁用邻居，请在地址系列配置模式下使用 neighbor shutdown 命令。要重新启用该邻居，请使用此命令的 no 形式。

**neighbor***ip_address***shutdown**
**no neighbor***ip_address***shutdown**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |

## Command Default

不会更改任何 BGP 邻居的状态。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |

## 使用指南

neighbor shutdown 命令用于终止指定邻居的任何活动会话，并删除所有关联的路由信息。

要显示 BGP 邻居摘要，请使用 show bgp summary 命令。具有空闲状态和管理条目的邻居已被 neighbor shutdown 命令禁用。

“State/PfxRcd”显示 BGP 会话的当前状态或路由器从邻居接收的前缀数量。当达到最大数量（由邻居最大前缀命令设置）时，条目中会出现字符串“PfxRcd”，邻居被关闭，连接处于空闲状态。

## CR_Examples

以下示例为邻居 172.16.70.23 禁用所有活动会话：

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |

| 命令 | 说明 |
| --- | --- |
| show bgp summary | 显示 BGP 邻居状态的摘要。 |

# neighbor timers

要为特定 BGP 对等体设置计时器，请在地址系列配置模式下使用 neighbor timers 命令。要清除特定 BGP 对等体的计时器，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **timers** *keepalive holdtime* [ *min-holdtime* ]

**noneighbor** { *ip_address* | *ipv6-address* } **timers**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| keepalive | ASA 软件向其对等方发送保持连接消息的频率（以秒为单位）。默认值为 60 秒。范围是 0 至 65535。 |
| holdtime | 未收到保持连接消息后软件宣布对等体死亡的时间间隔（以秒为单位）。默认值为 180 秒。范围是从 0 到 65535。 |
| min-holdtime | （可选）指定来自 BGP 邻居的最短可接受保持时间的时间间隔（以秒为单位）。可接受的最小保持时间必须小于或等于保持时间参数中指定的间隔。范围是从 0 到 65535。 |

## Command Default

保活时间：60秒

保持时间：180秒

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

- 为特定邻居配置的计时器将覆盖为所有 BGP 邻居使用 timers bgp 命令配置的计时器。

- 当将保持时间参数配置为小于 20 秒的值时，将显示以下警告：保持时间小于 20 秒会增加对等端抖动的可能性。
- 如果可接受的最小保持时间间隔大于指定的保持时间，则会显示一条通知：可接受的最小保持时间应小于或等于配置的保持时间。

注释 如果在BGP路由器上配置最短可接受保持时间，则仅当远程对等设备通告的保持时间等于或大于最短可接受保持时间的时间间隔时，才建立远程BGP对等会话。如果最短可接受保持时间的时间间隔大于配置的保持时间，则下次尝试建立远程会话将失败，并且本地路由器将发送通知表明“不可接受的保持时间”。

## CR_Examples

以下示例将 BGP 对等体 192.168.47.0 的保持连接计时器更改为 70 秒，将保持时间计时器更改为 210 秒：

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

以下示例将 BGP 对等体 192.168.1.2 的保持连接计时器更改为 70 秒，保持时间计时器更改为 130 秒，最小保持时间间隔更改为 100 秒：

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

以下示例将 BGP 对等体 2001::1 的保持连接计时器更改为 70 秒，将保持时间计时器更改为 210 秒：

```
ciscoasa(config-router-af)# neighbor 2001::1 timers 70 210
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与BGP邻居的信息交换。 |

# neighbor transport

要为边界网关协议 (BGP) 会话启用 TCP 传输会话选项，请在路由器或地址系列配置模式下使用 neighbor transport 命令。要禁用 BGP 会话的 TCP 传输会话选项，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [ **disable** ] }
**no neighbor** { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [ **disable** ] }

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 连接模式 | 指定连接类型 - 主动或被动。 |
| active | 指定活动连接。 |
| 被动 | 指定被动连接。 |
| path-mtu-discovery | 启用 TCP 传输路径最大传输单元 (MTU) 发现。默认情况下会启用 TCP 路径 MTU 发现。 |
| disable | 禁用 TCP 路径 MTU 发现。 |

## Command Default

如果未配置此命令，则默认情况下会启用 TCP 路径 MTU 发现，但不会启用其他 TCP 传输会话选项。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

此命令用于指定各种传输选项。可以为 BGP 会话指定主动或被动传输连接。可以启用 TCP 传输路径 MTU 发现，以允许 BGP 会话利用更大的 MTU 链路。使用 show bgp neighbors 命令可确定是否启

用了 TCP 路径 MTU 发现。如果您使用 disable 关键字禁用发现，则在继承禁用了发现的模板的任何对等体上也会禁用发现。

## CR_Examples

以下示例显示如何将 TCP 传输连接配置为单个内部 BGP (iBGP) 邻居的活动连接：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

以下示例显示如何将单个外部 BGP (eBGP) 邻居的 TCP 传输连接配置为被动：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

以下示例显示如何对单个 BGP 邻居禁用 TCP 路径 MTU 发现：

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

以下示例显示如何将单个 BGPv6 邻居的 TCP 传输连接配置为活动连接：

```
ciscoasa(config-router-af)#neighbor 2001::1 transport connection-mode active
```

以下示例显示如何为单个 BGPv6 邻居启用 TCP 路径 MTU 发现：

```
ciscoasa(config-router-af)#neighbor 2001::1 transport path-mtu-discovery
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| neighbor remote-as | 向 BGP 或多协议 BGP 路由表添加条目。 |
| show bgp neighbor | 显示有关 BGP 邻居的信息 |

# neighbor ttl-security

要保护边界网关协议(BGP)对等会话会话并配置用于分隔两个外部BGP(eBGP)对等体的最大跳数，请在 address-family 配置模式下使用 neighbor ttl-security 命令。要禁用此功能，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*
**no neighbor** { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| hop-count | 分隔 eBGP 对等体的跳数。TTL 值由路由器根据已配置的 hop-count 参数计算得出。<br>有效值为 1 至 254 之间的数字。 |

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

neighbour ttl-security 命令提供了一种轻量级的安全机制来保护 BGP 对等会话免受基于 CPU 利用率的攻击。这些类型的攻击通常是暴力拒绝服务 (DoS) 攻击，即通过使数据包报头中包含伪造的源和目标 IP 地址的 IP 数据包充斥网络来尝试禁用网络。

此功能通过仅接受 TTL 计数等于或大于本地配置值的 IP 数据包来利用 IP 数据包的设计行为。准确伪造 IP 数据包中的 TTL 计数通常被视为不可能。如果没有源或目标网络的内部访问权限，则准确伪造数据包以匹配来自信任对等体的 TTL 计数是不可能的。

应在每个参与的路由器上配置此功能。它仅在传入方向保护 BGP 会话，对传出 IP 数据包或远程路由器没有影响。启用此功能后，仅当 IP 数据包报头中的 TTL 值等于或大于为对等会话配置的 TTL 值时，BGP才会建立或维护会话。此功能对BGP对等会话没有影响，如果未收到保持连接数据包，

对等会话仍可能过期。如果接收的数据包中的 TTL 值小于本地配置的值，则系统会以静默方式丢弃该数据包，并且不会生成互联网控制消息协议 (ICMP) 消息。这是有意设计的行为；对伪造的数据包没有必要作出响应。

要最大限度地提高此功能的有效性，“hop-count”值应严格配置为匹配本地与外部网络之间的跃点数。但是，为多跃点对等会话配置此功能时，您还应该考虑路径变化。

以下限制适用于此命令的配置：

- 内部 BGP (iBGP) 对等体不支持此功能。
- 无法为已配置邻居 ebgp-multihop 命令的对等体配置邻居 ttl-security 命令。这些命令的配置互相排斥，只需要使用其中一个命令即可启用多跳 eBGP 对等会话。如果尝试为同一对等会话配置这两个命令，控制台中将会显示错误消息。
- 在大直径多跳对等互连中，此功能的有效性会降低。针对配置为大直径对等关系的 BGP 路由器发起基于 CPU 利用率的攻击，您可能仍需要关闭受影响的对等会话来处理攻击。
- 此功能不能有效抵御来自已在网络内部受到危害的对等体的攻击。此限制还包括位于源网络和目标网络之间的网段上的对等体。

## CR_Examples

以下示例将直接连接的邻居的跳数计数设置为 2。由于 hop-count 参数设置为 2，因此 BGP 仅接受报头中 TTL 计数等于或大于 253 的 IP 数据包。如果收到的数据包在 IP 数据包报头中包含任何其他 TTL 值，数据包将被静默丢弃。

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

以下示例将一个直接连接的 BGPv6 邻居的跳数设置为 2。

```
ciscoasa(config-router-af)#neighbor 2001::1 ttl-security hops 2
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| neighbor ebgp-multihop | 接受并尝试与非直接连接网络上的外部对等体建立 BGP 连接 |

# neighbor update-source

要将接口配置为 BGP 发言邻居的源，请在地址系列配置模式下使用 **neighbor update-source** 命令。要禁用此功能，请使用此命令的 no 形式。

**neighbor** {*ipv_address* | *ipv6-address*} **update-source** {*interface name*}

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| interface name | 指定 `nameif` 命令所指定的 ASA 用作 BGP 路由源的接口的名称。 |

## Command Default

此命令默认禁用。

## 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 |
| 地址族配置模式。 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.18(2) | 添加了此命令。 |

## 使用指南

此命令适用于在环回接口上运行 BGP 协议，并允许环回接口参与重新分发和前缀通告。

## CR_Examples

以下示例将环回接口 loop1 更新为 BGP 邻居 10.108.1.1 的源：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 109
ciscoasa(config-router-af)# neighbor 10.108.1.1 update-source loop1
```

以下示例将环回接口 loop1 更新为 BGP 邻居 2001::1 的源：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 2001::1 remote-as 109
ciscoasa(config-router-af)# neighbor 2001::1 update-source loop1
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |
| neighbor remote-as | 将 BGP 或多协议 BGP 路由条目添加到路由表。 |

# neighbor version

要将 ASA 软件配置为仅接受特定 BGP 版本，请在地址系列配置模式下使用 neighbor version 命令。要使用邻居的默认版本级别，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **version***number*
**no neighbor** { *ip_address* | *ipv6-address* } **version***number*

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 数字 | BGP 版本号。版本可以设置为 2，以强制软件仅对指定邻居使用版本 2。默认使用版本 4，如有要求，可以动态地协商降至版本 2。 |

## Command Default

BGP 版本 4。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

输入此命令会禁用动态版本协商。

## CR_Examples

以下示例锁定到 BGP 协议版本 4：

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
ciscoasa(config-router-af)# neighbor 2001::1 version 4
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **address-familyipv4** | 进入地址族配置模式。 |

| 命令 | 说明 |
| --- | --- |
| neighbor activate | 启用与 BGP 邻居的信息交换。 |

# neighbor weight

要为邻居连接分配权重，请在地址系列配置模式下使用 neighbor weight 命令。要删除权重分配，请使用此命令的 no 形式。

**neighbor** { *ip_address* | *ipv6-address* } **weightnumber**
**no neighbor** { *ip_address* | *ipv6-address* } **weightnumber**

## Syntax Description

| | |
|---|---|
| *ip_address* | 邻居路由器的 IP 地址。 |
| ipv6-address | 邻居路由器的 IPv6 地址。 |
| 数字 | 要分配的权重。<br>有效值介于 0 与 65535 之间。 |

## Command Default

通过另一个 BGP 对等体获知的路由的默认权重为 0，而来自本地路由器的路由的默认权重为 32768。

## 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 |
| 地址族配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

从此邻居获知的所有路由最初都将具有已分配的权重。当特定网络有多个路由可用时，具有最高权重的路由将被选择作为首选路由。

使用 set weight route-map 命令分配的权重会覆盖使用 neighbor weight 命令分配的权重。

## CR_Examples

以下地址系列配置模式示例将通过 172.16.12.1 获知的所有路由的权重设为 50：

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

以下地址系列配置模式示例设置通过 2001::1 获知的所有路由的权重：

```
ciscoasa(config-router-af)# neighbor 2001::1 weight 50
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **address-familyipv4** | 进入地址族配置模式。 |
| neighbor activate | 启用与BGP邻居的信息交换。 |

# nem

要为硬件客户端启用网络扩展模式，请在**nemenable**策略组配置模式下使用该命令。要禁用NEM，请使用该 **nemdisable** 命令。要从运行配置中删除 NEM 属性，请使用此**no**命令的形式。此选项允许从其他组策略继承值。

**nem** {**enable**|**disable**}
**no nem**

## Syntax Description

| | |
|---|---|
| **disable** | 禁用网络扩展模式。 |
| **enable** | 启用网络扩展模式。 |

## Command Default

网络扩展模式已禁用。

## 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 |
| 组策略配置 | • 是 | — | • 是 | — | — |

## 使用指南

网络扩展模式允许硬件客户端通过 VPN 隧道向远程专用网络呈现单个可路由的网络。IPsec 封装从硬件客户端后面的专用网络到 ASA 后面的网络的所有流量。PAT 不适用。因此，ASA 后面的设备可以通过隧道直接访问硬件客户端后面的专用网络上的设备，并且只能通过隧道访问，反之亦然。硬件客户端必须启动隧道，但是在建立隧道之后，任一端都可发起数据交换。

## Command History

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

## CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略设置 NEM：

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
```

# netmod

要禁用网络模块，请在全局配置模式下使用 **netmod** 命令。要启用网络模块，请使用此命令的 **no** 形式。

注释 仅在 Secure Firewall 3100 上支持此命令。

**netmod 2 disable**
**no netmod 2 disable**

## Syntax Description

| | |
|---|---|
| **2** | 指定插槽 2 中的模块。 |
| **disable** | 禁用网络模块。 |

## Command Default

如果该模块在首次启动时安装，则会将其启用。

## 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 |
| 全局配置 | • 是 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 9.17(1) | 此命令是为安全防火墙 3100 引入的。 |

## 使用指南

如果在首次打开防火墙之前安装网络模块，则无需执行任何操作；网络模块已启用并可供使用。如果您需要在初始启动后更改网络模块安装，请使用此命令。

添加新模块或永久删除模块需要重新加载。您可以将网络模块热插拔为相同类型的新模块，而无需重新加载。但是，您必须关闭当前模块才能安全地将其删除。如果您更换了其他类型的网络模块，则需要重新加载。如果新模块的接口少于旧模块，则必须手动删除与不再存在的接口相关的任何配置。

### 示例

以下示例禁用网络模块。

```
ciscoasa(config)# netmod 2 disable
```

以下示例启用 网络模块。

```
ciscoasa(config)# no netmod 2 disable
```

# network (address-family)

要指定将由边界网关协议 (BGP) 路由进程通告的网络，请在 address-family 配置模式下使用 network 命令。要从路由表中删除条目，请使用此命令的 no 形式。

**network** { *ipv4_address* [ **mask***network_mask* ] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [ *subnet_prefix* | *prefix_length* ] } [ **route-map** *route_map_name* ]
**no network** { *ipv4_address* [ **mask***network_mask* ] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [ *subnet_prefix* | *prefix_length* ] } [ **route-map***route_map_name* ]

## Syntax Description

| | |
|---|---|
| *ipv4_address* | BGP 或多协议 BGP 将通告的 IPv4 网络。 |
| *ipv6_prefix/prefix_length* | BGP 或多协议 BGP 将通告的 IPv6 网络。 |
| mask network_mask | （可选）带有掩码地址的网络或子网掩码。 |
| *prefix_delegation_name* | 如果您启用 DHCPv6 前缀委派客户端（**ipv6dhcpclientpd**），那么您可以通告前缀。 |
| *subnet_prefix/prefix_length* | （可选）要为前缀划分子网，请指定 subnet_prefix/prefix 长度。 |
| route-map route_map_name | （可选）已配置路由图的标识符。应检查路由映射，以过滤要通告的网络。如果未指定，则通告所有网络。如果指定了关键字，但没有列出路由图标签，则不会通告任何网络。 |

## Command Default

未指定任何网络。

## 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 |
| Address-family 配置 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.2(1) | 添加了此命令。 |
| 9.6(2) | 添加了 *prefix_delegation_name* [*subnet_prefix/prefix_length*] 参数。 |

## 使用指南

可以从连接的路由、动态路由和静态路由源获知 BGP 和多协议 BGP 网络。

可以使用的网络命令的最大数量取决于路由器的资源（例如，配置的 NVRAM 或 RAM）。

## CR_Examples

以下示例将网络 10.108.0.0 设置为包含在 BGP 更新中：

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

## Related Commands

| 命令 | 说明 |
| --- | --- |
| **showbgpinterfaces** | 显示BGP路由表中的条目。 |

# network (router eigrp)

要为 EIGRP 路由进程指定网络列表，请在路由器配置模式下使用 **network**命令。要删除网络定义，请使用此命令的 **no** 形式。

**network***ip_addr*[*mask*]
**no network***ip_addr*[*mask*]

## Syntax Description

| | |
|---|---|
| *ip_addr* | 直接连接网络的 IP 地址。连接到指定网络的接口将参与 EIGRP 路由进程。 |
| *mask* | （可选）IP 地址的网络掩码。 |

## Command Default

未指定任何网络。

## 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 |
| 路由器配置 | • 是 | — | • 是 | — | — |

## Command History

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

## 使用指南

**network** 命令在指定网络中具有至少一个 IP 地址的所有接口上启动 EIGRP。它将插入 EIGRP 拓扑表中指定网络的连接子网。

然后，ASA 通过匹配的接口建立邻居。对可在 ASA 上配置的 **network** 命令数量没有限制。

## CR_Examples

以下示例将 EIGRP 定义为用于连接到网络 10.0.0.0 和 192.168.7.0 的所有接口上的路由协议：

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **showeigrpinterfaces** | 显示为 EIGRP 配置的接口信息。 |
| **showeigrptopology** | 显示 EIGRP 拓扑表。 |

# network (router rip)

要为 RIP 路由进程指定网络列表，请在路由器配置模式下使用该 **network** 命令。要删除网络定义，请使用此命令的 **no** 形式。

**network** {*ip_addr* | *ipv6-address*} | <*prefix-length*>
**no network** {*ip_addr* | *ipv6-address*} | <*prefix-length*> [**route-map** *route-map-name*]

## Syntax Description

| | |
|---|---|
| *ip_addr* | 直接连接网络的 IP 地址。连接到指定网络的接口将参与 RIP 路由过程。 |
| ipv6-address | 要使用的 IPv6 地址。IPv6 地址必须以 X:X:X:X::X 格式输入。 |
| prefix-length | IPv6 前缀的长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值前面必须有斜线标记。<br>有效值介于 0 到 128 之间。 |
| route-map-name | 将修改其属性的路由映射。 |

## Command Default

未指定任何网络。

## 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 |
| 路由器配置，地址系列配置模式 | • 是 | — | • 是 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 7.2(1) | 添加了此命令。 |
| 9.0(1) | 增加了多情景模式支持。 |
| 9.3(2) | 添加了 ipv6-address 参数，并添加了对 IPv6 地址系列的支持。 |

## 使用指南

指定的网络号不得包含任何子网信息。可在路由器上使用的网络命令的数量没有限制。RIP 路由更新将仅通过指定网络上的接口发送和接收。此外，如果未指定接口的网络，则该接口将不会在任何 RIP 更新中被通告。

## CR_Examples

以下示例将 RIP 定义为用于连接到网络 10.0.0.0 和 192.168.7.0 的所有接口的路由协议：

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
In the following example the attributes of the test-route-map route map connected to the
2001::1 network will be modified.
ciscoasa(config-router)# network 2001:0:0:0::1 route-map test-route-map
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **routerrip** | 进入路由器配置模式。 |
| **showrunning-configrouter** | 显示全局路由器配置中的 命令。 |

# network-acl

如要指定之前使用 **access-list** 命令配置的防火墙 ACL 名称，请在 dynamic-access-policy-record 配置模式下使用 **network-acl**命令。要删除现有网络 ACL，请使用此命令的 **no** 形式。要删除所有网络 ACL，请使用不带参数的 命令。

**network-acl***name*
**no network-acl** [名称]

## Syntax Description

*name* 指定网络 ACL 的名称。名称的最大长度为 240 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 |
| 动态访问策略记录配置 | • 是 | • 支持 | • 支持 | — | — |

## Command History

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

## 使用指南

多次使用此命令，以便将多个防火墙 ACL 分配给 DAP 记录。

ASA会验证您指定的每个ACL，以确保它们仅包含允许规则或仅包含访问列表条目的拒绝规则。如果任何指定的 ACL 包含混合的允许和拒绝规则，ASA 将拒绝该命令。

以下示例显示如何将名为财务限制 (Finance Restrictions) 的网络 ACL 应用于名为财务 (Finance) 的 DAP 记录。

```
ciscoasa
(config)#
dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
 network-acl Finance Restrictions
ciscoasa
(config-dynamic-access-policy-record)#
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| access-policy | 配置防火墙访问策略。 |
| dynamic-access-policy-record | 创建 DAP 记录。 |
| **showrunning-configdynamic-access-policy-record**[名称 ] | 显示所有 DAP 记录或指定 DAP 记录正在使用的配置。 |

# network area

要定义运行 OSPF 的接口并定义这些接口的区域 ID，请在 **networkarea** 路由器配置模式下使用该命令。要禁用使用地址/网络掩码对定义的接口的 OSPF 路由，请使用此命令的 **no**形式。

**network***addr mask***area***area_id*
**no network***addr mask***area***area_id*

## Syntax Description

| | |
|---|---|
| *addr* | IP 地址。 |
| **area***area_id* | 指定与 OSPF 地址范围关联的区域。可以 IP 地址格式或十进制格式指定 *area_id* 。以十进制格式指定时，有效值范围为 0 至 4294967295。 |
| *mask* | 网络掩码。 |

## 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 |
| 路由器配置 | • 是 | • — | • 是 | • — | — |

## Command History

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

## 使用指南

要在接口上运行 OSPF，接口的地址必须被 **networkarea** 命令覆盖。如果 **networkarea** 命令未涵盖接口的 IP 地址，则不会通过该接口启用 OSPF。

您可在 ASA 上使用的 **networkarea** 命令没有数量限制。

## CR_Examples

以下示例在 192.168.1.1 接口上启用 OSPF，并将其分配到 area 2：

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **routerospf** | 进入路由器配置模式。 |

| 命令 | 说明 |
| --- | --- |
| **showrunning-configrouter** | 显示全局路由器配置中的 命令。 |

# network-object

要将主机对象、网络对象或子网对象添加到网络对象组，请在 object-group 网络配置模式下使用 network-object 命令。要删除网络对象，请使用此命 **no**令的形式。

**network-object** { **host***address* | *IPv4_address mask* | *IPv6_address* | *IPv6_prefix* | **object***name* }
**no network-object** { **host***ip_address* | *ip_address mask* | **object***name* }

## Syntax Description

| | |
|---|---|
| **host***ip_address* | 指定主机 IPv4 或 IPv6 地址。 |
| *IPv4_addressmask* | 指定 IPv4 网络地址和子网掩码。 |
| *IPv6* 地址/*IPv6* 前缀 | 指定 IPv6 网络地址和前缀长度。 |
| **object***name* | 指定网络对象（通过 **objectnetwork**命令创建）。 |

## 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 |
| Object-group 网络 配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.3(1) | 添加 **object** 参数是为了支持网络对象（**objectnetwork** 命令）。 |
| 9.0(1) | 以前，网络对象组只能包含所有 IPv4 地址或所有 IPv6 地址。现在网络对象组可以支持 IPv4 和 IPv6 地址的混合，尽管您不能在 NAT 中使用混合组。 |

## 使用指南

**network-object** 命令与 **object-group** 命令一起使用来定义主机对象、网络对象或子网对象。

## CR_Examples

以下示例显示如何使用**network-object** 命令在网络对象组中创建新主机对象：

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **clearconfigureobject-group** | 从配置中 **object-group**删除所有命令。 |
| **group-object** | 添加网络对象组。 |
| object network | 添加网络对象。 |
| **object-groupnetwork** | 定义网络对象组。 |
| **showrunning-configobject-group** | 显示当前对象组。 |

# network-service-member

要将网络服务对象添加到网络服务组，请在对象组配置模式下使用 **network-service-member** 命令。使用命令形 **no**式从组中删除对象

**network-service-member** *object_name*
**no network-service-member** *object_name*

## Syntax Description

| | |
|---|---|
| *object_name* | 网络服务对象的名称。如果名称中有空格，请用双引号括起来。 |

## Command Default

没有默认值。

## 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 |
| 网络服务对象组配置模式 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

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

### 示例

以下示例将三个现有网络服务对象添加到网络服务对象组。

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

## Related Commands

| 命令 | 说明 |
|---|---|
| **clear object-group** | 清除对象组的命中计数。 |
| **object-group network-service** | 定义网络服务对象组。 |
| **show object-group network-service** | 显示网络服务对象及其命中次数。 |

# nis address

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供网络信息服务 (NIS) 地址，请在 ipv6 dhcp 池配置模式下使用 **nisaddress**命令。要删除 NIS 服务器，请使用此命 **no**令的形式。

**nis address***nis_ipv6_address*
**no nis address***nis_ipv6_address*

## Syntax Description

| | |
|---|---|
| *nis_ipv6_address* | 指定 NIS IPv6 地址。 |

## 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 |
| Ipv6 dhcp 池配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 我们引入了此命令。 |

## 使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA **ipv6dhcppool**，使其在向 ASA 发送信息请求 (IR) 数据包时以提供信息（包括 NIS 地址）。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

## CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **clearipv6dhcpstatistics** | 清除 DHCPv6 统计信息。 |
| **domain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的域名。 |
| **dns-server** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。 |
| **import** | 使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。 |
| **ipv6address** | 启用 IPv6 并在接口上配置 IPv6 地址。 |
| **ipv6addressdhcp** | 使用 DHCPv6 获取接口的地址。 |
| **ipv6dhcpclientpd** | 使用授权前缀设置接口的地址。 |
| ipv6 dhcp client pd hint | 提供关于您想要接收的委托前缀的一个或多个提示。 |
| **ipv6dhcppool** | 创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。 |
| **ipv6dhcpserver** | 启用 DHCPv6 无状态服务器。 |
| **network** | 将 BGP 配置为通告从服务器接收的授权前缀。 |
| **nisaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。 |
| **nisdomain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。 |
| **nispaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。 |
| **nispdomain-name** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。 |
| **showbgpipv6unicast** | 显示 IPv6 BGP 路由表中的条目。 |
| **showipv6dhcp** | 显示 DHCPv6 信息。 |
| **showipv6general-prefix** | 显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。 |

| 命令 | 说明 |
| --- | --- |
| **sipaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。 |
| **sipdomain-name** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。 |
| **sntpaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。 |

# nis domain-name

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供网络信息服务 (NIS) 域名，请在 ipv6 dhcp 池配置模式下使用 **nisdomain-name**命令。要删除 NIS 域名，请使用此命 **no**令的形式。

**nis domain-name***nis_domain_name*
**no nis domain-name***nis_domain_name*

## Syntax Description

| | |
|---|---|
| *nis_domain_name* | 指定 NIS 域名。 |

## 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 |
| Ipv6 dhcp 池配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 我们引入了此命令。 |

## 使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以将 ASA 配置为在向 **ipv6dhcppool**ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 域名。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

## CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
```

```
nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **clearipv6dhcpstatistics** | 清除 DHCPv6 统计信息。 |
| **domain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的域名。 |
| **dns-server** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。 |
| **import** | 使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。 |
| **ipv6address** | 启用 IPv6 并在接口上配置 IPv6 地址。 |
| **ipv6addressdhcp** | 使用 DHCPv6 获取接口的地址。 |
| **ipv6dhcpclientpd** | 使用授权前缀设置接口的地址。 |
| ipv6 dhcp client pd hint | 提供关于您想要接收的委托前缀的一个或多个提示。 |
| **ipv6dhcppool** | 创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。 |
| **ipv6dhcpserver** | 启用 DHCPv6 无状态服务器。 |
| **network** | 将 BGP 配置为通告从服务器接收的授权前缀。 |
| **nisaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。 |
| **nisdomain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。 |
| **nispaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。 |
| **nispdomain-name** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。 |
| **showbgpipv6unicast** | 显示 IPv6 BGP 路由表中的条目。 |
| **showipv6dhcp** | 显示 DHCPv6 信息。 |
| **showipv6general-prefix** | 显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。 |

| 命令 | 说明 |
| --- | --- |
| **sipaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。 |
| **sipdomain-name** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。 |
| **sntpaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。 |

# nisp address

要在配置 DHCPv6 服务器时向无状态地址自动配置 (SLAAC) 客户端提供 Network Information Service Plus (NIS+) 服务器 IP 地址，请在 ipv6 dhcp 池配置模式下使用 **nispaddress**命令。要删除 NIS+ 服务器，请使用此命 **no**令的形式。

**nisp address***nisp_ipv6_address*
**no nisp address***nisp_ipv6_address*

## Syntax Description

| | |
|---|---|
| *nisp_ipv6_address* | 指定 NIS+ 服务器 IPv6 地址。 |

## 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 |
| Ipv6 dhcp 池配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 我们引入了此命令。 |

## 使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以配置 ASA **ipv6dhcppool**，使其在向 ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 服务器。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

## CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **clearipv6dhcpstatistics** | 清除 DHCPv6 统计信息。 |
| **domain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的域名。 |
| **dns-server** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。 |
| **import** | 使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。 |
| **ipv6address** | 启用 IPv6 并在接口上配置 IPv6 地址。 |
| **ipv6addressdhcp** | 使用 DHCPv6 获取接口的地址。 |
| **ipv6dhcpclientpd** | 使用授权前缀设置接口的地址。 |
| ipv6 dhcp client pd hint | 提供关于您想要接收的委托前缀的一个或多个提示。 |
| **ipv6dhcppool** | 创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。 |
| **ipv6dhcpserver** | 启用 DHCPv6 无状态服务器。 |
| **network** | 将 BGP 配置为通告从服务器接收的授权前缀。 |
| **nisaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。 |
| **nisdomain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。 |
| **nispaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。 |
| **nispdomain-name** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。 |
| **showbgpipv6unicast** | 显示 IPv6 BGP 路由表中的条目。 |
| **showipv6dhcp** | 显示 DHCPv6 信息。 |
| **showipv6general-prefix** | 显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。 |

| 命令 | 说明 |
| --- | --- |
| **sipaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。 |
| **sipdomain-name** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。 |
| **sntpaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。 |

# nisp domain-name

要在配置DHCPv6服务器时向无状态地址自动配置(SLAAC)客户端提供网络信息服务(NIS+)域名，请在 ipv6 dhcp 池配置模式下使用 **nispdomain-name**命令。要删除 NIS+ 域名，请使用此命 **no**令的形式。

**nisp domain-name***nisp_domain_name*
**no nisp domain-name***nisp_domain_name*

## Syntax Description

| | |
|---|---|
| *nisp_domain_name* | 指定NIS+域名。 |

## 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 |
| Ipv6 dhcp 池配置 | • 是 | — | • 是 | — | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.6(2) | 我们引入了此命令。 |

## 使用指南

对于将 SLAAC 与前缀委派功能结合使用的客户端，您可以将 ASA 配置为在向 **ipv6dhcppool**ASA 发送信息请求 (IR) 数据包时提供信息，包括 NIS+ 域名。ASA 仅接受 IR 数据包，不向客户端分配地址。使用**ipv6dhcpserver** 命令配置 DHCPv6 无状态服务器；启用服务器时指定 **ipv6dhcppool**名称。

使用 **ipv6dhcpclientpd** 命令配置前缀代理。

此功能不支持集群。

## CR_Examples

以下示例创建两个 IPv6 DHCP 池，并在两个接口上启用 DHCPv6 服务器：

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **clearipv6dhcpstatistics** | 清除 DHCPv6 统计信息。 |
| **domain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的域名。 |
| **dns-server** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 DNS 服务器。 |
| **import** | 使用 ASA 从前缀委派客户端接口上的 DHCPv6 服务器获取的一个或多个参数，并在响应 IR 消息时将它们提供给 SLAAC 客户端。 |
| **ipv6address** | 启用 IPv6 并在接口上配置 IPv6 地址。 |
| **ipv6addressdhcp** | 使用 DHCPv6 获取接口的地址。 |
| **ipv6dhcpclientpd** | 使用授权前缀设置接口的地址。 |
| ipv6 dhcp client pd hint | 提供关于您想要接收的委托前缀的一个或多个提示。 |
| **ipv6dhcppool** | 创建一个池，其中包含您要使用 DHCPv6 无状态服务器提供给给定接口上的 SLAAC 客户端的信息。 |
| **ipv6dhcpserver** | 启用 DHCPv6 无状态服务器。 |
| **network** | 将 BGP 配置为通告从服务器接收的授权前缀。 |
| **nisaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NIS 地址。 |
| **nisdomain-name** | 配置在响应 IR 消息时向 SLAAC 客户端提供的 NIS 域名。 |
| **nispaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 NISP 地址。 |
| **nispdomain-name** | 配置在响应 IR 消息中向 SLAAC 客户端提供的 NISP 域名。 |
| **showbgpipv6unicast** | 显示 IPv6 BGP 路由表中的条目。 |
| **showipv6dhcp** | 显示 DHCPv6 信息。 |
| **showipv6general-prefix** | 显示DHCPv6前缀委派客户端获取的所有前缀以及该前缀到其他进程的ASA分发。 |

| 命令 | 说明 |
| --- | --- |
| **sipaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 地址。 |
| **sipdomain-name** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SIP 域名。 |
| **sntpaddress** | 配置在响应 IR 消息中提供给 SLAAC 客户端的 SNTP 地址。 |

# nop

要定义在具有 IP 选项检查的数据包头中出现无操作 IP 选项时的操作，请在 **nop** 参数配置模式下使用该命令。要禁用此功能，请使用此**no** 命令的形式。

**nop action** {**allow | clear**}
**no nop action** {**allow | clear**}

## Syntax Description

| | |
|---|---|
| *allow* | 允许包含无操作 IP 选项的数据包。 |
| *clear* | 从数据包头中删除无操作选项，然后允许数据包。 |

## Command Default

默认情况下，IP 选项检查会丢弃包含无操作 IP 选项的数据包。

您可以使用 IP **default**选项检查策略映射中的命令更改默认值。

## 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 |
| 参数配置 | • 是 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 8.2(2) | 添加了此命令。 |

## 使用指南

此命令可配置的 IP 选项检查策略映射中。

您可以配置 IP 选项检查来控制哪些具有特定 IP 选项的 IP 数据包可以通过 ASA。您可以允许数据包通过，而无需更改或清除指定的 IP 选项，然后允许数据包通过。

IP 报头中的选项字段可以包含零个、一个或多个选项，这使得该字段的总长度可变。但是，IP 报头必须是 32 位的倍数。如果所有选项的位数不是 32 位的倍数，则使用无操作 (NOP) 或 IP 选项 1 作为“内部填充”，以使选项与 32 位边界对齐。

## CR_Examples

以下示例展示如何在策略映射中设置 IP 选项检查的操作：

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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

# nsf cisco

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科不间断转发 (NSF) 操作，请在路由器配置模式下使用 nsf cisco 命令。要恢复默认值，请使用此命令的 no 形式。

**nsf cisco** [**enforce global**]
**no nsf cisco** [**enforce global**]

## Syntax Description

| | |
|---|---|
| *enforceglobal* | （可选）如果在重启过程中在任何接口上检测到不具有 NSF 感知能力的相邻网络设备，则取消所有接口上的 NSF 重启。 |

## Command Default

默认情况下，思科 NSF 平稳重启处于禁用状态。

## 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 |
| 路由器配置模式 | • 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 OSPF 路由器上启用思科 NSF。当在路由器上启用 NSF 时，该路由器也支持 NSF，并将在重启模式下运行。

如果路由器预计与仅执行 NSF 平稳重启的邻居协作，则邻居路由器必须运行支持 NSF 的思科软件版本，但无需在路由器上配置 NSF。当路由器运行支持 NSF 的思科软件版本时，路由器可感知 NSF。

默认情况下，可识别 NSF 的相邻路由器在平滑重启期间将运行在 NSF 助手模式下。

在 NSF 平稳重启期间，如果在网络接口上检测到无法识别 NSF 的邻居，则仅在该接口上中止重启，而在其他接口上继续平稳重启。要在重启期间检测到无法识别 NSF 的邻居时取消整个 OSPF 进程的重启，请将此命令配置为带有 enforce global 关键字。

**注释** 当在任何接口上检测到邻居邻接重置或 OSPF 接口关闭时，整个过程的 NSF 平稳重启也会被取消。

## CR_Examples

以下示例使用 enforce global 选项启用思科 NSF 平稳重启：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# cisco nsf enforce global
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| nsf cisco helper | 在 ASA 上启用思科 NSF 助手模式。 |
| **nsfietf** | 启用 IETF NSF |

# nsf cisco helper

要在运行开放最短路径优先 (OSPF) 的 ASA 上启用思科无间断转发 (NSF) 助手模式，请在路由器配置模式下使用 nsf cisco helper 命令。默认情况下会启用思科 NSF 助手模式，可以通过在路由器配置模式下发出 no nsf cisco helper 来禁用此模式。

**nsf ciscohelper**
**no nsf ciscohelper**

## Syntax Description

此命令没有任何参数或关键字。

## Command Default

默认情况下启用 Cisco NSF 帮助程序模式。

## 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 |
| 路由器配置模式 | • 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

当 ASA 启用了 NSF 时，ASA 称为支持 NSF 并将在平稳重启模式下运行 - OSPF 路由器进程由于路由处理器 (RP) 切换而执行不间断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 可感知 NSF，并将在 NSF 助手模式下运行。当具有 NSF 功能的 ASA 执行平滑重启时，辅助 ASA 会协助不间断转发恢复过程。如果您不希望 ASA 通过不间断转发恢复来帮助重新启动的邻居，请输入 no nsf cisco helper 命令。

## CR_Examples

以下示例禁用 NSF 助手模式：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# no nsf cisco helper
```

## Related Commands

| 命令 | 说明 |
|---|---|
| nsf cisco | 在 ASA 上启用思科 NSF。 |

| 命令 | 说明 |
| --- | --- |
| **nsfietf** | 启用 IETF NSF |

# nsf ietf

要在运行 OSPF 的 ASA 上配置互联网工程任务组 (IETF) NSF 操作，请在路由器配置模式下使用 nsf ietf 命令。要恢复默认值，请使用此命令的 no 形式。

**nsf ietf** [**restart-interval** 秒]
**no nsf ietf**

## Syntax Description

*restart-intervalseconds* （可选）指定平滑重启间隔的长度（以秒为单位）。范围是从 1 到 1800。默认值为 120。

**注释**
对于低于 30 秒的重启间隔，将终止平稳重启。

## Command Default

IETF NSF 平稳重启模式已禁用。

## 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 |
| 路由器配置模式 | • 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 ASA 上启用 IETF NSF。在 ASA 上启用 NSF 时，ASA 将支持 NSF 功能并将在重新启动模式下运行。

如果 ASA 应与仅执行 NSF 平稳重启的邻居协作，则邻居 ASA 必须支持 NSF，但路由器上不需要配置 NSF。当 ASA 运行支持 NSF 的应用时，ASA 可感知 NSF。

## CR_Examples

以下示例禁用 NSF 助手模式：

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# nsf ietf restart-interval 240
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| nsf cisco | 在 ASA 上启用思科 NSF。 |
| **nsfciscohelper** | 在 ASA 上启用思科 NSF 助手模式。 |
| nsf ietf helper | 在 ASA 上启用 IETF NSF 助手模式。 |

# nsf ietf helper

默认情况下启用 IETF NSF 帮助模式。要明确启用 IETF NSF 助手模式，请在路由器配置模式下使用 nsf ietf helper 命令。可以使用该命令的no形式来禁用它。

或者，可以使用 nsf ietf helper strict-lsa-checking 命令启用严格链路状态通告 (LSA) 检查。

**nsf ietf helper**［ **strict-lsa-checking**］
**no nsf ietf helper**

## Syntax Description

| | |
|---|---|
| 严格 *LSA* 检查 | （可选）为助手模式启用严格链路状态通告 (LSA) 检查。 |

## Command Default

默认情况下启用 IETF NSF 帮助模式。

## 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 |
| 路由器配置模式 | • 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

当 ASA 启用了 NSF 时，这意味着 ASA 也支持 NSF 功能，并将在平稳重启模式下运行 - OSPF 进程会由于路由处理器 (RP) 切换而执行不间断转发恢复。默认情况下，支持 NSF 的 ASA 的相邻 ASA 可感知 NSF，并将在 NSF 助手模式下运行。当具有 NSF 功能的 ASA 执行平滑重启时，辅助 ASA 会协助不间断转发恢复过程。如果您不希望 ASA 帮助重启的邻居进行无间断转发恢复，请输入 no nsf ietf helper 命令。

要在支持 NSF 和支持 NSF 的 ASA 上启用严格 LSA 检查，请输入 nsf ietf helper strict-lsa-checking 命令。但是，直到 ASA 在 IETF 平稳重启过程中成为助手 ASA 后，严格 LSA 检查才会生效。启用严格 LSA 检查后，如果辅助 ASA 检测到要泛洪到重启 ASA 的 LSA 发生更改，或者在启动平滑重启过程时重启 ASA 的重传列表中存在已更改的 LSA，则辅助 ASA 将终止重启 ASA 的帮助过程。

## CR_Examples

以下示例启用具有严格 LSA 检查的 IETF NSF 助手：

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa
(config-router)# nsf ietf helper strict-lsa-checking
```

## Related Commands

| 命令 | 说明 |
|---|---|
| nsf cisco | 在 ASA 上启用思科 NSF。 |
| **nsfciscohelper** | 在 ASA 上启用思科 NSF 助手模式。 |
| nsf ietf | 在 ASA 上启用 IETF NSF。 |

# nt-auth-domain-controller

要指定该服务器的NT主域控制器名称，请在aaa-server主机配置模式下使用**nt-auth-domain-controller**命令。要删除此规范，请使用此 **no**命令的形式。

**nt-auth-domain-controller**字符串
**no nt-auth-domain-controller**

## Syntax Description

| | |
|---|---|
| *string* | 为主域控制器指定此服务器的名称，长度最大为16个字符。 |

## Command Default

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 |
| AAA服务器主机配置 | • 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

此命令仅适用于 NT 身份验证 AAA 服务器。首先，必须已使用 **aaa-serverhost**命令进入主机配置模式。 字符串 变量中的名称必须与服务器本身上的 NT 条目匹配。

## CR_Examples

以下示例将此服务器的 NT 主域控制器的名称配置为“primary1”：

```
ciscoasa
(config)# aaa-server svrgrp1 protocol nt
ciscoasa
(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa
(config-aaa-server-host)#
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **aaaserverhost** | 进入 aaa 服务器主机配置模式，以便您可以配置特定于主机的 AAA 服务器参数。 |

| 命令 | 说明 |
| --- | --- |
| **clearconfigureaaa-server** | 从配置中删除所有 AAA 命令语句。 |
| **showrunning-configaaa-server** | 显示所有 AAA 服务器、特定服务器组、特定组中的特定服务器或特定协议的 AAA 服务器统计信息。 |

# ntp authenticate

要启用 NTP 服务器的身份验证，请在 **ntpauthenticate**全局配置模式下使用该命令。要禁用 NTP 身份验证，请使用此命 **no**令的形式。

**ntp authenticate**
**no ntp authenticate**

## 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 |
| 全局配置 | • 是 | • 支持 | • 支持 | • — | 是 |

## Command History

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

## 使用指南

如果启用身份验证，ASA仅当在数据包中使用正确的受信任密钥时，才会与NTP服务器通信（请参阅 **ntptrusted-key** 命令）。您还必须指定服务器密钥（请参阅 **ntpserverkey** 命令），否则即使您配置了 **ntpauthenticate** 命令，ASA 也将在不进行身份验证的情况下与服务器通信。ASA 还使用身份验证密钥与 NTP 服务器同步（请参阅 **ntpauthentication-key** 命令）。

## CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **ntpauthentication-key** | 设置加密的身份验证密钥以与 NTP 服务器同步。 |

| 命令 | 说明 |
| --- | --- |
| **ntpserver** | 标识 NTP 服务器。 |
| **ntptrusted-key** | 为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。 |
| **showntpassociations** | 显示与 ASA 关联的 NTP 服务器。 |
| **showntpstatus** | 显示 NTP 关联的状态。 |

# ntp authentication-key

要设置密钥以使用 NTP 服务器进行身份验证，请在全局配置模式下使用 **ntpauthentication-key** 命令。要删除密钥，请使用此 **no**命令的形式。

**ntp authentication-key***key_id*{**md5 | sha1 | sha256 | sha512 | cmac**}*key*
**no ntp authentication-key***key_id*[{**md5 | sha1 | sha256 | sha512 | cmac**} [**0|8**]*key*]

## Syntax Description

| | |
|---|---|
| 0 | （可选）表示<key_value>为纯文本。如果 0 或 8 不存在，则格式为纯文本。 |
| 8 | （可选）表示<key_value>为加密文本。如果 0 或 8 不存在，则格式为纯文本。 |
| *key* | 将密钥值设置为长度最大为 32 个字符的字符串。 |
| *key_id* | 确定介于 1 和 4294967295 之间的密钥 ID。您必须使用 **ntptrusted-key** 命令将此 ID 指定为受信任密钥。 |
| **md5** | 指定认证算法为 MD5。 |
| **sha1** | 指定身份验证算法为 SHA-1。 |
| **sha256** | 指定身份验证算法为 SHA-256。 |
| **sha512** | 指定身份验证算法为 SHA-512。 |
| **cmac** | 指定身份验证算法为 AES-CMAC。 |

## 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 | • 支持 | • 支持 | • — | 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 添加了此命令。 |
| 9.13(1) | 添加了 **sha1sha512**、、、**sha256**和关 **cmac**键字。 |

## 使用指南

要使用 NTP 身份验证，还需配置 **ntpauthenticate** 命令和 **ntpserverkey** 命令。

## CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **ntpauthenticate** | 启用NTP身份验证。 |
| **ntpserver** | 标识 NTP 服务器。 |
| **ntptrusted-key** | 为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。 |
| **showntpassociations** | 显示与 ASA 关联的 NTP 服务器。 |
| **showntpstatus** | 显示 NTP 关联的状态。 |

# ntp server

要标识要在 ASA 上设置时间的 NTP 服务器，请在全局配置模式下使用 **ntpserver** 命令。要删除服务器，请使用此命 **no**令的形式。

**ntp server***ip_address*[ **key***key_id*][ **source***interface_name*][**prefer**]
**no ntp server***ip_address*[ **key***key_id*][ **source***interface_name*][**prefer**]

## Syntax Description

| | |
|---|---|
| *ip_address* | 设置 NTP 服务器的 IPv4 或 IPv6 IP 地址。 |
| **key***key_id* | 如果使用 **ntpauthenticate** 命令启用身份验证，则设置此服务器的受信任密钥 ID。另请参阅 **ntptrusted-key**命令。 |
| **source***interface_name* | 如果您不想使用路由表中的默认接口，则标识 NTP 数据包的传出接口。由于在多情景模式下系统不包含任何接口，请指定在管理情景中定义的接口名称。 |
| **prefer** | 如果多个服务器具有相似的精度，则将此NTP服务器设置为首选服务器。NTP使用一种算法确定最准确的服务器，然后与该服务器同步。如果多台服务器的准确度相似，**prefer**关键字将指定使用这些服务器中的哪台服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。例如，ASA 使用层数为 2 的服务器，而不是优先使用层数为 3 的服务器。 |

## 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 | • 支持 | • 支持 | — | • 是 |

## Command History

| 版本 | 修改 |
|---|---|
| 7.0(1) | 此命令已修改，以使源接口可选。 |
| 9.12(1) | 我们添加了 IPv6 支持。 |
| 9.14(1) | 添加了 NTPv4 支持。 |

## 使用指南

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证CRL，其包括精确时间戳。可配置多个NTP服务器。ASA选择层级最低的服务器，作为衡量数据可靠性的方式。在多情景模式下，仅在系统配置中设置 NTP 服务器。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

ASA 支持 NTPv4。

## CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **ntpauthenticate** | 启用NTP身份验证。 |
| **ntpauthentication-key** | 设置加密的身份验证密钥以与 NTP 服务器同步。 |
| **ntptrusted-key** | 为 ASA 提供密钥 ID，以在数据包中使用此 ID，以便通过 NTP 服务器进行身份验证。 |
| **showntpassociations** | 显示与 ASA 关联的 NTP 服务器。 |
| **showntpstatus** | 显示 NTP 关联的状态。 |

# ntp trusted-key

要将身份验证密钥 ID 指定为可信密钥（这是使用 NTP 服务器进行身份验证所必需的），请在 **ntptrusted-key**全局配置模式下使用该命令。要删除可信密钥，请使用此命 **no**令的形式。可输入多个受信任密钥，供多台服务器使用。

**ntp trusted-key***key_id*
**no ntp trusted-key***key_id*

## Syntax Description

| | |
|---|---|
| *key_id* | 设置介于 1 和 4294967295 之间的密钥 ID。 |

## 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 | • 支持 | • 支持 | • — | 是 |

## Command History

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

## 使用指南

要使用 NTP 身份验证，还需配置 **ntpauthenticate** 命令和 **ntpserverkey** 命令。要与服务器同步，请使用 **ntpauthentication-key** 命令为密钥 ID 设置身份验证密钥。

## CR_Examples

以下示例标识两个 NTP 服务器并对密钥 ID 1 和 2 启用身份验证：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **ntpauthenticate** | 启用NTP身份验证。 |

| 命令 | 说明 |
| --- | --- |
| **ntpauthentication-key** | 设置加密的身份验证密钥以与NTP服务器同步。 |
| **ntpserver** | 标识 NTP 服务器。 |
| **showntpassociations** | 显示与 ASA 关联的 NTP 服务器。 |
| **showntpstatus** | 显示 NTP 关联的状态。 |

# num-packets

如要指定 SLA 操作期间发送的请求数据包数，请在 SLA 监控协议配置模式下使用 **num-packets** 命令。要恢复默认值，请使用此命 **no**令的形式。

**num-packets**编号
**no num-packets***number*

## Syntax Description

*number* SLA 操作期间发送的数据包数量。有效值为 1 至 100。

注释
当指定为 number 参数（在此命令中）的所有数据包都丢失时，表明被跟踪的路由发生故障。

## Command Default

为回应类型发送的默认数据包数为 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 |
| SLA 监控协议配置 | • 是 | • — | • 是 | • — | — |

## Command History

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

## 使用指南

增加发送的数据包的默认数量，以防止由于丢包而导致错误的可达性信息。

## CR_Examples

以下示例配置一个 ID 为 123 的 SLA 操作，该操作使用 ICMP 回应请求/响应时间探测操作。它将回显请求数据包的有效载荷大小设置为 48 字节，并将 SLA 操作期间发送的回显请求数量设置为 5。被跟踪的路由必须丢失所有 5 个数据包

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
```

```
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

## Related Commands

| 命令 | 说明 |
|---|---|
| **request-data-size** | 指定请求数据包负载的大小。 |
| **slamonitor** | 定义 SLA 监控操作。 |
| **typeecho** | 将SLA操作配置为回应响应时间探测操作。 |

# nve

要为 VXLAN 封装创建网络虚拟化终端 (NVE) 实例，请在全局配置模式下使用 **nve**命令。要删除 NVE 实例，请使用此命 **no**令的形式。

**nve 1**
**no nve 1**

## Syntax Description

| | |
|---|---|
| **1** | 指定 NVE 实例，它始终为 1。 |

## 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 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.4(1) | 添加了此命令。 |

## 使用指南

每个 ASA 或安全情景可以配置一个 VTEP 源接口。您可以配置一个用于指定此 VTEP 源接口的 NVE 实例。所有 VNI 接口都必须与此 NVE 实例关联。

## CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并将 VNI 1 接口与其关联：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
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
ciscoasa(config-if)# mcast-group 236.0.0.100
```

**Related Commands**

| 命令 | 说明 |
| --- | --- |
| **debugvxlan** | 调试 VXLAN 流量。 |
| **default-mcast-group** | 为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。 |
| **encapsulationvxlan** | 将 NVE 实例设置为 VXLAN 封装。 |
| **inspectvxlan** | 强制遵守标准 VXLAN 报头格式。 |
| **interfacevni** | 创建用于 VXLAN 标记的 VNI 接口。 |
| **mcast-group** | 为 VNI 接口设置组播组地址。 |
| **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。 |
| **peerip** | 手动指定对等 VTEP IP 地址。 |
| **segment-id** | 指定 VNI 接口的 VXLAN 网段 ID。 |
| **showarpvtep-mapping** | 显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。 |
| **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。 |
| **showmac-address-tablevtep-mapping** | 使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。 |
| **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。 |
| **showvnivlan-mapping** | 显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。 |
| **source-interface** | 指定 VTEP 源接口。 |
| **vtep-nve** | 将 VNI 接口与 VTEP 源接口相关联。 |
| **vxlanport** | 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。 |

# nve-only

要指定 VXLAN 源接口为仅 NVE，请在接口配置模式下使用 **nve-only** 命令。要删除仅限 NVE 的限制，请使用此命 **no**令的形式。

**nve-only**
[**cluster**]
**no nve-only**

## Syntax Description

## Syntax Description

| | |
|---|---|
| **cluster** | 在配置 ASA virtual 集群时，必须为集群控制链路指定 **nev-only cluster**。 |

## 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 | • 支持 | • 支持 | • 支持 | — |

## Command History

| 版本 | 修改 |
|---|---|
| 9.4(1) | 添加了此命令。 |
| 9.17(1) | 我们添加了 **cluster** 关键字来支持 ASA virtual 集群。 |

## 使用指南

每个 ASA 或安全情景可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)；此时，VXLAN VTEP 是唯一受支持的 NVE。

在透明模式下，VTEP 接口需要**nve-only** 设置，它允许您为接口配置 IP 地址。在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此命令是可选的。

对于 ASA virtual 集群，必须对集群控制链路使用 VXLAN 接口；在这种情况下，请指定 **nev-only cluster**。

## CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并指定它是仅限 NVE 的：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
```

**Related Commands**

| 命令 | 说明 |
|---|---|
| **debugvxlan** | 调试 VXLAN 流量。 |
| **default-mcast-group** | 为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。 |
| **encapsulationvxlan** | 将 NVE 实例设置为 VXLAN 封装。 |
| **inspectvxlan** | 强制遵守标准 VXLAN 报头格式。 |
| **interfacevni** | 创建用于 VXLAN 标记的 VNI 接口。 |
| **mcast-group** | 为 VNI 接口设置组播组地址。 |
| **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。 |
| **peerip** | 手动指定对等 VTEP IP 地址。 |
| **segment-id** | 指定 VNI 接口的 VXLAN 网段 ID。 |
| **showarpvtep-mapping** | 显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。 |
| **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。 |
| **showmac-address-tablevtep-mapping** | 使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。 |
| **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。 |
| **showvnivlan-mapping** | 显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。 |
| **source-interface** | 指定 VTEP 源接口。 |
| **vtep-nve** | 将 VNI 接口与 VTEP 源接口相关联。 |
| **vxlanport** | 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。 |

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。