基本设置

本章介绍如何在 ASA 上配置有效配置通常所需的基本设置。

设置主机名、域名及启用密码和 Telnet 密码

要设置主机名、域名及启用密码和 Telnet 密码，请执行以下步骤。

开始之前

在设置主机名、域名及启用密码和 Telnet 密码之前，请检查以下需求：

- 在多情景模式下，可在系统和情景执行空间中配置主机名和域名。
- 启用密码和 Telnet 密码可在每个情景中设置；此类密码在系统中不可用。
- 要从系统切换至情景配置，请输入 **changeto context** *name* 命令。

过程

步骤 1 为 ASA 或情景指定主机名。默认主机名为“asa”。

hostname *name*

示例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

此名称最多可包含63个字符。主机名必须以字母或数字开头和结尾，并且只能包含字母、数字或连字符。

为ASA设置主机名时，该名称将显示在命令行提示符中。如果建立与多台设备的会话，则该主机名有助于跟踪命令输入位置。

对于多情景模式，在系统执行空间中设置的主机名显示在所有情景的命令行提示符中。在情景内选择性设置的主机名不会显示在命令行中，但可供 **banner** 命令 **$(hostname)** 令牌使用。

步骤 2 为 ASA 指定域名。默认域名为 default.domain.invalid。

domain-name *name*

示例：

```
ciscoasa(config)# domain-name example.com
```

ASA会将域名作为后缀追加到不受限定的名称。例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则ASA会将名称限定为“jupiter.example.com”。

步骤 3 更改启用密码。默认情况下，启用密码为空，但第一次输入 **enable** 命令时，系统会提示您更改密码。

enable password *password*

示例：

```
ciscoasa(config)# enable password Pa$$w0rd
```

如果没有配置启用身份验证，则可使用启用密码进入特权 EXEC 模式。如果没有配置 HTTP 身份验证，还可使用启用密码以空白用户名登录 ASDM。

密码 参数是一个区分大小写的密码，长度为 8 到 127 个字符，可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是以下除外。

- 无空格
- 没有问号
- 不能使用三个或三个以上连续或重复的 ASCII 字符。例如，以下密码将被拒绝：
  - **abc**user1
  - 用户**543**
  - 用户**aaaa**
  - 用户2**666**

该命令可更改最高权限级别 (15) 的密码。如果配置本地命令授权，则可使用以下语法，为从 0 到 15 的每个权限级别设置启用密码：

enable password *password* **level** *number*

encrypted 关键字（在 9.6 和早期版本中，用于 32 个字符或以下的密码）或 **pbkdf2** 关键字（在 9.6 和更高版本中，用于长度超过 32 个字符的密码；在 9.7 和更高版本中，用于所有长度的密码）表示密码已被加密（使用基于 MD5 的散列或 PBKDF2（基于密码的密钥派生功能 2）使用 SHA-512 散列）。请注意，现有密码将继续使用基于 MD5 的散列方法，除非您输入新的密码。当您在 **enable password** 命令中定义密码后，出于安全目的，ASA 会在将其保存到配置时进行加密。输入 **show running-config** 命令后，**enable password**命令不会显示实际密码；它将显示加密的密码，后跟 **encrypted** 或 **pbkdf2** 关键字。例如，如果输入密码“test”，则 **show running-config** 命令输出内容将与以下内容类似：

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

只有在您剪切和粘贴配置文件，以便 在另一 ASA 中使用，而且您使用相同的密码时， 才会真的在 CLI 上输入 **encrypted** 或 **pbkdf2** 关键字。

您无法将密码重置为空值。

步骤 4 为 Telnet 访问设置登录密码。没有默认密码。

未配置 Telnet 身份验证时，登录密码可用于 Telnet 访问。

passwd *password* [**encrypted**]

示例：

```
ciscoasa(config)# passwd cisco12345
```

password 是一个区分大小写的密码，最多由 16 个字母数字和特殊字符组成。可以在密码中使用除问号和空格以外的任意字符。

密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。如果出于某种原因需要将密码复制到另一个 ASA，但不知道原始密码，则可随加密密码和 **encrypted** 关键字一起输入 **passwd** 命令。通常，只能在输入 **showing running-config passwd** 命令时查看该密码。

设置日期和时间

注释 请勿为 Firepower 2100、4100 或 9300 设置日期和时间；ASA 会从机箱接收这些设置。

设置时区和夏令时日期

要设置时区和夏令时日期范围，请执行以下步骤：

过程

步骤 1 设置时区。默认时区为 UTC。

- Firepower 1000、 设备模式下的 Firepower 2100、 Cisco Secure Firewall 3100:

  clock timezone *zone*

  - *zone* - 输入 **clock timezone ?** 命令以查看可接受的时区名称列表。

  示例：

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
Japan
[...]

ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific

ciscoasa(config)# clock timezone US/Mountain
```

- 所有其他型号：

  clock timezone *zone* [-]*hours* [*minutes*]

  - *zone* - 以字符串形式指定时区，例如 PST 表示太平洋标准时间。
  - [-]*hours* - 设置与 UTC 偏离的小时数。例如，PST 为 -8 小时。
  - *minutes* - 设置与 UTC 偏离的分钟数。

  示例：

```
ciscoasa(config)# clock timezone PST -8
```

步骤 2 输入以下命令之一，以更改夏令时日期范围的默认值。默认的循环日期范围是从三月第二个星期日的凌晨 2:00 到十一月第一个星期日的凌晨 2:00。

注释 在设备模式下， Firepower 1000、 设备模式下的 Firepower 2100、 Cisco Secure Firewall 3100不支持此命令。

- 设置夏令时开始和结束日期，作为特定年份中的特定日期。如果使用此命令，则需要每年重置日期。

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

  - *zone* - 以字符串形式指定时区， 例如 PDT 表示太平洋夏令时。
  - *day* - 设置一月中的第几天，从 1 到 31。例如，日期和月份也可输入为“**A**pril 1 或 1 April，具体取决于标准日期格式。
  - *month* - 以字符串形式设置月份。例如，日期和月份也可输入为“April 1 或 1 April，具体取决于标准日期格式。
  - *year* - 以四位数字格式设置年份，例如，2004。年份范围为 1993 至 2035。
  - *hh:mm* - 以 24 小时制设置小时和分钟。
  - *offset* - 设置要为夏令时更改的分钟数。默认情况下，该值为 60 分钟。

  示例：

  ```
  ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
  ```

- 以某月某日某一时间，而非某年中的特定日期这种形式，指定夏令时的开始和结束日期。此命令可供您设置循环日期范围，无需每年更改。

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone* - 以字符串形式指定时区， 例如 PDT 表示太平洋夏令时。
  - *week* - 用 1 到 4 之间的整数或“first”或“last”这样的词指定某月中的第几周。例如，如果某天刚好跨在第五周，则用“last”来指定。
  - *weekday* - 指定星期几：星期一、星期二、星期三等等。
  - *month* - 以字符串形式设置月份。
  - *hh:mm* - 以 24 小时制设置小时和分钟。
  - *offset* - 设置要为夏令时更改的分钟数。默认情况下，该值为 60 分钟。

  示例：

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

使用 NTP 服务器设置日期和时间

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。

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。

开始之前

在多情景模式下，只能在系统配置中设置时间。

过程

步骤 1 （可选） 启用 服务器身份验证。

a) 启用身份验证。

ntp authenticate

示例：

```
ciscoasa(config)# ntp authenticate
```

在启用 NTP 身份验证时，还必须在 **ntp trusted-key** 命令中指定一个密钥 ID，并使用 **ntp server key** 命令将该密钥与服务器关联起来。使用 **ntp authentication-key** 命令为该 ID 配置实际密钥。如果您有多台服务器，请为每台服务器配置一个单独的 ID。

b) 指定要作为受信任密钥的身份验证密钥 ID，通过 NTP 服务器进行身份验证必须执行此操作。

ntp trusted-key *key_id*

示例：

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

key_id 参数为介于 1 和 4294967295 之间的值。可输入多个受信任密钥，供多台服务器使用。

c) 设置 NTP 服务器身份验证密钥。

ntp authentication-key *key_id* {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} *key*

示例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id* - 使用 **ntp trusted-key** 命令设置您设置的 ID。
- {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} - 设置算法。
- *key* - 将 密钥设置为最长 32 个字符的字符串。

步骤 2 标识 NTP 服务器。

ntp server {*ipv4_address* | *ipv6_address* }[**key** *key_id*] [**source** *interface_name*] [**prefer**]

示例：

```
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
```

如果您启用了 NTP 身份验证 (**ntp authenticate**)，则必须使用通过 **ntp trusted-key** 命令设定的 ID 指定 **key***key_id* 参数。

source *interface_name* 关键字参数对标识 NTP 数据包的传出接口（如果不想使用路由表中的默认接口）。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。

如果多台服务器的准确度相似，**prefer** 关键字将此 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 2 层服务器，而不使用作为首选服务器的 3 层服务器。

可确定多台服务器；ASA 会使用最准确的服务器。

手动设置日期和时间

要手动设置日期和时间，请执行以下步骤：

开始之前

在多情景模式下，只能在系统配置中设置时间。

过程

手动设置日期时间。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

示例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:::参数以 24 小时制设置小时、分钟和秒。例如，输入 20:54:00 表示下午 8:54。

day 值设置月中的日期，范围为 1 到 31。例如，可用 april 1 或 1 april 形式输入月份和日期，具体取决于标准日期格式。

month 值设置月份。根据标准日期格式，可用 april 1 或 1 april 形式输入月份和日期。

year 值使用四位数字设置年份，例如 2004。有效范围为 1993 到 2035。

默认时区为 UTC。如果在输入 **clock set** 命令后使用 **clock timezone** 命令更改时区，时间将自动调整为新的时区。

此命令将时间设置在硬件芯片中，不在配置文件中保存时间。该时间保持至重新启动为止。与其他 **clock** 命令不同，此命令为特权 EXEC 命令。要重置时钟，您需要使用 clock set 命令设置新的时间。

配置精确时间协议 (ISA 3000)

精确时间协议 (PTP) 是一种时间同步协议，用于在基于数据包的网络中同步各种设备的时钟。这些设备时钟通常具有不同的精度和稳定性。该协议专为工业联网测量和控制系统设计，而且最适合用于分布式系统，因为其需要极少的带宽和处理开销。

PTP 系统是一个分布式联网系统，包含 PTP 设备和非 PTP 设备的组合。PTP 设备包含常见的时钟、边界时钟和透明时钟。非 PTP 设备包含网络交换机、路由器和其他基础设施设备。

可以将 ASA 设备配置为透明时钟。ASA 设备不会将其时钟与 PTP 时钟同步。ASA 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

当您配置 PTP 设备时，需要为要一起运行的设备定义一个域编号。因此，您可以配置多个 PTP 域，然后将每个非 PTP 设备配置为使用一个特定域的 PTP 时钟。

开始之前

- 此功能在 ISA 3000 上不可用。
- 仅在单情景模式下支持使用 PTP。
- 思科 PTP 仅支持组播 PTP 消息。
- 默认情况下，在透明模式下对所有 ISA 3000 接口启用 PTP。在路由模式下，必须添加必要的配置以确保允许 PTP 数据包通过设备。

- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网接口支持 PTP 配置，无论是独立式还是网桥组成员。它在以下对象上不受支持：
  - 管理接口。
  - 子接口、EtherChannel、BVI 或任何其他虚拟接口。
- 假如父接口上具有适当的 PTP 配置，则支持 VLAN 子接口上的 PTP 流。
- 必须确保允许 PTP 数据包通过设备。在透明防火墙模式下，默认会配置访问列表以允许 PTP 流量。PTP 流量由 UDP 端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此在路由防火墙模式下，允许此流量的任何 ACL 都可接受。
- 在路由防火墙模式下，您还必须为 PTP 组播组启用组播路由：
  - 进入全局配置模式命令 **multicast-routing**。
  - 对于在其上启用了 PTP，且不是网桥组成员的每个接口，请输入接口配置命令 **igmp join-group 224.0.1.129** 以静态启用 PTP 组播组成员身份。桥接组成员不支持或不需要使用此命令。

过程

步骤 1 指定 设备的所有端口的域编号：

ptp domain *domain_num*

示例：

```
ciscoasa(config)# ptp domain 54
```

domain_num 参数是设备上所有端口的域编号。在其他域中接收的数据包将像正常组播数据包一样处理，不会进行任何 PTP 处理。该值可以从 0 到 255；默认值为 0。输入在网络中的 PTP 设备上配置的域编号。

步骤 2 （可选）在设备上配置 PTP 时钟模式：

ptp mode e2etransparent

示例：

```
ciscoasa(config)# ptp mode e2etransparent
```

此命令可在所有启用 PTP 的接口上启用端到端透明模式。

步骤 3 在接口上启用 PTP：

ptp enable

在系统可用于联系至配置的域中 PTP 时钟的每个接口上启用 PTP。

示例：

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

配置主密码

主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，而无需更改任何功能。使用主密码的功能包括：

- OSPF
- EIGRP
- VPN 负载均衡
- VPN（远程访问和站点间）
- 故障切换
- AAA 服务器
- 日志记录
- 共享许可证

添加或更改主密码

如要添加或更改主密码，请执行以下步骤。

开始之前

- 该程序只能在安全会话中进行，例如通过控制台、SSH 或通过 HTTPS 连接 ASDM。
- 如果已启用故障切换，但未设置故障切换共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障切换共享密钥，以防主密码更改以纯文本形式发送。
- 在主用/备用故障切换中启用或更改密码加密会导致 **write standby**，这会将主用配置复制到备用设备。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主用/主用故障切换，您必须手动输入 **write standby**。**write standby** 可能导致主用/主用模式下出现流量中断，因为辅助设备上的配置在同步新配置之前已被清除。您应该使用 **failover active group 1** 和 **failover active group 2** 命令激活主 ASA 上的所有情景，输入 **write standby**，然后使用 **no failover active group 2** 命令将第 2 组情景还原到辅助设备。

过程

步骤 1 设置用于生成加密密钥的密码。密码的长度必须介于 8 和 128 个字符之间。除退格符号和双引号之外的所有字符都可用于密码。如果未在命令中输入新密码，则系统会提示您输入。要更改密码，必须输入原密码。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

示例：

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

注释　　使用交互式提示用户输入密码，以避免密码被记录在命令历史缓冲区。

请谨慎使用 **no key config-key password-encrypt** 命令，因为该命令会将加密密码更改为纯文本密码。降级至不支持密码加密的软件版本时，可使用该命令的 **no** 形式。

步骤 2 启用密码加密。

password encryption aes

示例：

```
ciscoasa(config)# password encryption aes
```

只要启用密码加密且有可用的主密码，所有用户密码均将被加密。运行的配置将以加密格式显示密码。

如果启用密码加密时未配置密码，则该命令将预期该密码在未来可用。

如果稍后使用 **no password encryption aes** 命令禁用密码加密，所有现有加密密码将保持不变，并且只要主密码存在，加密密码就会根据应用要求被解密。

步骤 3 保存主密码的运行时值和生成的配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

如果未输入此命令，启动配置中的密码可能仍然可见（如果此前未加密保存）。此外，在多情景模式下，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果未在系统情景模式中输入 write memory 命令，但也未在所有用户情景中输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 write memory all 命令以保存所有配置。

示例

以下示例显示不存在上一个密钥：

```
ciscoasa(config)# key config-key password-encryption 12345678
```

以下示例显示已存在密钥：

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

在以下示例中，输入不包含参数的命令，以便系统提示您输入密钥。由于密钥已经存在，系统将提示您输入。

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

在以下示例中，因为不存在密钥，所以系统不会提示您提供密钥。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

禁用主密码

禁用主密码可将加密密码恢复为纯文本密码。如果降级为不支持加密密码的以前软件版本，移除密码可能十分有用。

开始之前

- 只有知道当前主密码才能禁用该主密码。请查看删除主口令，第 13 页，看看是否不知道密码。
- 此程序只能在安全会话中进行；即可通过 Telnet、SSH，或通过 HTTPS 连接 ASDM。

要禁用主密码，请执行以下步骤：

过程

步骤 1 删除主密码。如果未在命令中输入密码，则系统将提示您输入。

no key config-key password-encryption [*old_passphrase*]]

示例：

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

步骤 2 保存主密码的运行时值和生成的配置。

write memory

示例：

```
ciscoasa(config)# write memory
```

包含密码的非易失存储器将被 0xFF 模式擦除并覆盖。

在多情景模式下，主密码在系统情景配置中将被更改。因此，所有情景中的密码都将受到影响。如果未在系统情景模式下输入 write memory 命令，但也未在所有用户情景中输入该命令，则用户情景中的加密密码可能会过期。或者，在系统情景中使用 write memory all 命令以保存所有配置。

删除主口令

无法恢复主密码。如果主密码丢失或未知，则可删除该主密码。

要删除主密码，请执行以下步骤：

过程

步骤 1 删除主密钥和包括加密密码的配置。

write erase

示例：

```
ciscoasa(config)# write erase
```

步骤 2 使用启动配置重新加载 ASA，而不使用任何主密钥或加密密码。

reload

示例：

```
ciscoasa(config)# reload
```

配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。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。

某些ASA功能需要使用DNS服务器按域名访问外部服务器。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。

默认情况下，有一个名为 DefaultDNS 的默认 DNS 服务器组。您可以创建多个 DNS 服务器组： 一个组是默认组，而其他组可以与特定域相关联。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，请参阅命令参考中的 **tunnel-group** 命令。

注释 ASA 有限支持使用 DNS 服务器，具体取决于功能。例如，大多数命令要求您输入 IP 地址，只有当手动配置 **name** 命令以将名称与 IP 地址相关联，并使用 names 命令启用名称后，才能够使用名称。

开始之前

确保为启用DNS域名查找所在的任何接口配置合适的路由和访问规则，以便能够到达DNS服务器。

过程

步骤 1 启用 ASA 能够发送 DNS 请求至 DNS 服务器，以对受支持的命令执行名称查找。

dns domain-lookup *interface_name*

如果不在接口上启用 DNS 查找，则 ASA 将不会与该接口上的 DNS 服务器通信。确保在将用于访问 DNS 服务器的所有接口上启用 DNS 查找。

示例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup outside
```

步骤 2 创建一个或多个 DNS 服务器组并将服务器添加到组。

a) DNS 服务器组的名称。

dns server-group *name*

要配置默认的 DefaultDNS 服务器组，请指定 DefaultDNS 作为名称。

示例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

b) 为组指定一个或多个 DNS 服务器。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] *[interface_name]*

可将六个 IP 地址全部输入同一命令中，用空格分隔，或者也可单独输入每个命令。

（可选）指定 ASA 与服务器通信时使用的 *interface_name*。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。

ASA 按顺序尝试每台 DNS 服务器，直至收到响应。

示例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 outside
```

c) （仅对于默认组） 配置附加到主机名的域名（如果主机名不是完全限定名称）。

domain-name *name*

示例：

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

d) （可选） 配置 DNS 服务器组的其他属性。

如果默认设置不适合您的网络，请使用以下命令更改组特征。

- **timeout***seconds* - 尝试下一个 DNS 服务器之前等待的秒数，从 1 到 30 秒。默认值为 2 秒。每次 ASA 重试服务器列表，此超时将加倍。
- **retries***number* - 当 ASA 收不到响应时，重试 DNS 服务器列表的次数，从 0 到 10 次。
- number-DNS条目的最小TTL，以分钟为单位。**expire-entry-timer minutes** 如果到期计时器长于条目的TTL，则TTL增加到到期条目时间值。如果TTL比到期计时器长，则将忽略到期条目时间值：在这种情况下，不会向TTL添加额外时间。到期后，该条目将从DNS查找表中删除。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些 DNS 条目可以有非常短的 TTL（短至 3 秒），所以您能够使用此设置实际上延长 TTL。默认值为1分钟（即，所有分辨率的最小TTL为1分钟）。范围为 1 至 65535 分钟。仅解析 FQDN 网络对象时使用此选项。
- **poll-timer minutes***number* - 将 FQDN 网络/主机对象解析为 IP 地址时使用的轮询周期时间（按分钟计）。仅在防火墙策略中使用 FQDN 对象时才解析这些对象。定时器确定解析的最长时间间隔；DNS 条目的生存时间 (TTL) 值也用于确定更新 IP 地址解析的时间，使各个 FQDN 可以比轮询周期更加频繁地解析。默认设置为 240（4 个小时）。范围为 1 至 65535 分钟。

e) 重复上述步骤添加其他 DNS 服务器组。

步骤 3 （可选） 将域映射到特定 DNS 服务器组。

dns-group-map

dns-to-domain *dns_group_name domain*

您最多可以映射 30 个域。不能将同一域映射到多个 DNS 服务器组，但可以将多个域映射到同一服务器组。请勿将任何域映射到要用于默认值的组（例如，DefaultDNS）。

示例：

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

步骤 4 指定默认 DNS 组。

dns-group *name*

默认情况下，已指定 DefaultDNS。如果配置了其他组，则可以使用此命令指定其他默认组。默认组的 DNS 组映射中不能有任何关联的域。

示例：

```
ciscoasa(config)# dns-group new_default_group
```

配置硬件旁路和双重电源（思科 ISA 3000）

您可以启用硬件旁路，以使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。当硬件旁路处于活动状态时，不会实施防火墙功能，因此请确保您了解允许流量通过的风险。请参阅以下硬件旁路指南：

- 此功能仅可用于思科 ISA 3000 设备。
- 如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件绕行。
- 当 ISA 3000 断电并进入硬件旁路模式时，只有支持的接口对可以通信；当使用默认配置时，inside1 <---> inside2 和 outside1 <---> outside2 无法再进行通信。这些接口之间的所有现有连接将会丢失。
- 我们建议您禁用 TCP 序列随机化（如本程序中所述）。如果启用随机化（默认设置），则在激活硬件旁路时需要重新建立 TCP 会话。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。激活硬件旁路时，ISA 3000 不再位于数据路径中，也不会转换序列号；接收客户端会收到意外的序列号并丢弃该连接。即便禁用 TCP 序列随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时终止。
- 激活硬件旁路时，硬件旁路接口上的思科 TrustSec 连接会被丢弃。当 ISA 3000 开启及停用硬件旁路时，会重新协商这些连接。

- 当停用硬件旁路及流量恢复通过ISA 3000数据路径时，需要重新建立某些现有的TCP会话，因为链路在切换期间会临时终止。
- 当硬件旁路处于活动状态时，以太网 PHY 会断开连接，因此 ASA 无法确定接口状态。接口可能显示为关闭状态。

对于 ISA 3000 中的双电源，可在 ASA OS 中将双电源建立为预期配置。如果其中一个电源发生故障，ASA会发出报警。默认情况下，ASA需要单一电源，只要其中有一个电源正常工作，它就不会发出报警。

开始之前

- 必须将硬件旁路接口连接到交换机的接入端口。不能将它们连接到中继端口。

过程

步骤 1 配置在断电期间要激活的硬件旁路：

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

示例：

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

sticky 关键字会在电源恢复和设备启动后使设备保持处于硬件旁路模式。在这种情况下，您需要在准备就绪后手动关闭硬件旁路；此选项允许您控制流量何时短暂中断。

步骤 2 手动激活或停用硬件旁路：

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** | **1/3-1/4**}

示例：

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

步骤 3 （可选） 将硬件旁路配置为保持活动状态，直到 ASA FirePOWER 模块启动后：

hardware-bypass boot-delay module-up sfr

启用硬件旁路时必须不带 **sticky** 选项，才能运行启动延迟。没有 **hardware-bypass boot-delay** 命令，硬件旁路可能会在 ASA FirePOWER 模块完成启动前处于不活动状态。例如，如果将该模块配置为故障关闭，此情景可能会导致流量被丢弃。

步骤 4 禁用 TCP 序列随机化。此示例显示如何通过向默认配置中添加设置来对所有流量禁用随机化。

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

如果稍后决定将其打开，请将“disable”替换为 **enable**。

步骤 5 作为预期配置建立双重电源：

power-supply dual

步骤 6 保存配置。

write memory

系统启动后硬件旁路的行为由启动配置中的配置设置决定，因此您必须保存运行配置。

调整 ASP（加速安全路径）性能和行为

ASP 是实现层，在此使策略和配置付诸实施。除了在通过思科技术支持中心进行故障排除期间，其他操作均与该层无直接关系。但是，可以调整几项与性能和可靠性相关的行为。

选择规则引擎交易提交模式

默认情况下，当更改基于规则的策略（例如访问规则）时，更改会立即生效。但是，这种即时性将稍微降低性能。在每秒有大量连接的环境下，大型规则列表的性能成本更加明显，例如当ASA每秒处理 18,000 个连接时更改包含 25,000 个规则的策略。

由于规则引擎要编译规则以实现更快的规则查找，所以性能会受到影响。默认情况下，系统在评估连接尝试时也搜索未编译规则，以便能够应用新规则；由于规则未编译，因此搜索需要更长时间。

您可以更改此行为，以便规则引擎在实施规则更改时使用交易模式，并在新规则编译并可用之前继续使用旧规则。通过交易模式，在规则编译期间性能应不会下降。下表解释了行为差异。

模型	编译前	编译中	编译后
默认	匹配原规则。	匹配新规则。 （每秒连接速率降低。）	匹配新规则。
事务性	匹配原规则。	匹配原规则。 （每秒连接速率不受影响。）	匹配新规则。

交易模式的另一个优势是，当替换接口上的 ACL 时，在删除旧的 ACL 和应用新的 ACL 之间没有间隙。该功能减少了可接受连接在操作期间被断开的可能性。

提示 如果为某种规则类型启用交易模式，则将生成系统日志以标记编译的开始和结束。这些系统日志的编号从 780001 到 780004。

请按照以下操作步骤为规则引擎启用交易提交模式。

过程

为规则引擎启用交易提交模式：

asp rule-engine transactional-commit *option*

其中，选项包括：

- **access-group** - 全局应用或应用于接口的访问规则。
- **nat** - 网络地址转换规则。

示例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

启用 ASP 负载均衡

ASP 负载均衡机制有助于避免以下问题：

- 因偶发的流量高峰而造成溢出
- 因大量流量过度订用特定接口接收环而造成溢出
- 单核无法承受负载的相对严重过载接口接收环造成溢出。

ASP 负载均衡允许多个核心在从单个接口接收环接收的数据包上同步工作。如果系统丢弃数据包，并且 **show cpu** 命令输出远小于 100%，此功能可能在数据包属于许多不相关的连接时有助于提高您的吞吐量。

注释 在 ASA 虚拟上禁用 ASP 负载均衡。将 DPDK（数据平面开发套件）集成到 ASA 虚拟的加速安全路径（ASP）中， ASA 虚拟 在禁用此功能的情况下表现出更好的性能。

过程

步骤 1 启用 ASP 负载均衡的自动打开和关闭：

asp load-balance per-packet auto

步骤 2 手动启用 ASP 负载均衡：

asp load-balance per-packet

ASP 负载均衡在您手动将其禁用之前一直保持启用状态，即使您启用了 **auto** 命令亦是如此。

步骤 3 手动禁用 ASP 负载均衡：

no asp load-balance per-packet

仅当您手动启用了 ASA 负载均衡时，才可以使用此命令。如果您也启用了 **auto** 命令，则系统将恢复为自动启用或禁用 ASP 负载均衡。

监控 DNS 缓存

ASA 提供 DNS 信息的本地缓存，这些信息来自于为某些无客户端 SSL VPN 和证书命令而发送的外部 DNS 查询。首先在本地缓存中查找每个 DNS 转换请求。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至已配置的各个 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

如需监控 DNS 缓存，请参阅以下命令：

- **show dns-hosts**

  此命令显示 DNS 缓存，其中包括从 DNS 服务器动态获悉的条目以及使用 name 命令手动输入的名称和 IP 地址。

基本设置历史

功能名称	平台版本	说明
多个 DNS 服务器组	9.18(1)	您现在可以使用多个 DNS 服务器组：一个组是默认值，而其他组可以与特定域相关联。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。 新增/修改的命令： **dns-group-map**、**dns-to-domain**
用于网络服务对象域解析的受信任 DNS 服务器。	9.17(1)	您可以指定在解析网络服务对象中的域名时系统应信任的 DNS 服务器。此功能可确保任何 DNS 域名解析都从受信任的来源获取 IP 地址。 新增/修改的命令： **dns trusted-source**、**show dns trusted-source**

功能名称	平台版本	说明
更强的本地用户和启用密码要求	9.17(1)	对于本地用户和启用密码，添加了以下密码要求： • 密码长度 - 至少为 8 个字符。以前，最小值为 3 个字符。 • 重复和连续字符 - 不允许使用三个或三个以上连续的连续或重复 ASCII 字符。例如，以下密码将被拒绝： • **abc**user1 • 用户**543** • 用户**aaaa** • 用户2**666** 新增/修改的命令： **enable password**、**username**
NTPv4 支持	9.14(1)	ASA 现在支持 NTPv4。 未修改任何命令。
额外 NTP 身份验证算法：	9.13(1)	以前，NTP 身份验证仅支持 MD5。现在 ASA 支持以下加密算法： • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新增/修改的命令：**ntp authentication-key**
NTP 支持使用 IPv6	9.12(1)	现在，您在设置 NTP 服务器时可以使用 IPv6 地址。 新增/修改的命令：**ntp server**
现在登录时需要更改 **enable** 密码	9.12(1)	**enable** 默认密码为空。现在，如果您尝试在 ASA 上进入特权 EXEC 模式，系统会要求您将密码改为一个至少包含 3 到 127 个字符的值。而不能将密码留空。**no enable password** 命令今后将不受支持。 在 CLI 中，您可以使用 **enable** 命令、**login** 命令（用户权限级别应在 2 级以上）或者 SSH 或 Telnet 会话（如果启用 **aaa authorization exec auto-enable**）来进入特权 EXEC 模式。无论使用哪种方法，您都必须设置密码。 但是在登录 ASDM 时，则没有这项更改密码的要求。默认情况下，在 ASDM 中，您无需使用用户名和 **enable** 密码即可登录。 新增/修改的命令：**enable password**

功能名称	平台版本	说明
在 ASA 虚拟上禁用 ASP 负载均衡	9.10(1)	将 DPDK（数据平面开发套件）最近集成到 ASA 虚拟的加速安全路径（ASP）中， ASA 虚拟 在禁用此功能的情况下表现出更好的性能。
ASA 虚拟现在支持自动 ASP 负载均衡	9.8(1)	过去只能手动启用和禁用 ASP 负载均衡。 修改了以下命令：**asp load-balance per-packet auto**
对所有本地 **username** 和 **enable** 密码使用 PBKDF2 散列算法	9.7(1)	配置中存储的所有长度的本地 **username** 和 **enable** 密码都将使用 PBKDF2 (基于密码的密钥派生函数 2)使用 SHA-512 的散列算法。以前，32 个字符或以下的密码使用基于 MD5 的哈希处理方法。已经存在的密码仍将继续使用基于 MD5 的哈希值，但您输入的新密码除外。如需下载指南，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下命令：**enable**、**username**
ISA 3000 支持双电源	9.6(1)	对于 ISA 3000 中的双电源，可在 ASA OS 中将双电源建立为预期配置。如果其中一个电源发生故障，ASA 会发出报警。默认情况下，ASA 需要单一电源，只要其中有一个电源正常工作，它就不会发出报警。 引入了以下命令：**power-supply dual**
本地 **username** 和 **enable** 密码支持更长的密码（最多 127 个字符）	9.6(1)	您现在可以创建最多 127 个字符的本地 **username** 和 **enable** 密码（过去的限制为 32 个字符）。在创建长度超过 32 个字符的密码时，它将使用 PBKDF2（基于密码的密钥派生功能 2）散列存储在配置中。较短的密码将继续使用基于 MD5 的散列处理方法。 修改了以下命令：**enable**、**username**
ISA 3000 硬件旁路	9.4(1.225)	ISA 3000 支持硬件旁路功能，以便在发生断电时允许流量继续通过设备流动。 引入了以下命令：**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** *9.5(1)* 版本不提供此功能。
自动 ASP 负载均衡	9.3(2)	现在可以启用自动开启和关闭 ASP 负载均衡功能。 **注释** ASA 虚拟不支持该自动功能；仅支持手动启用和禁用。 引入了以下命令：**asp load-balance per-packet auto**。

功能名称	平台版本	说明
删除默认 Telnet 密码	9.0(2)9.1(2)	为了提高 ASA 管理访问的安全性，已删除 Telnet 的默认登录密码；使用 Telnet 登录之前必须手动设置密码。 注释 如果不配置 Telnet 用户身份验证，登录密码仅用于 Telent（**aaa authentication telnet console** 命令）。 过去，当清除了密码时，ASA 恢复默认设置“cisco”。现在，当清除密码时，密码也被删除。 登录密码还用于从交换机到 ASASM 的 Telnet 会话（请参阅 **session** 命令）。对于初始 ASASM 访问，必须使用 **service-module session** 命令，直到设置登录密码。 修改了以下命令：**password**
密码加密可见性	8.4(1)	已修改了 **show password encryption** 命令。
主密码	8.3(1)	引入了此功能。主密码可供您用加密格式安全地存储纯文本密码，并提供一个对所有密码进行加密或掩蔽的通用密钥，而无需更改任何功能。 引入了以下命令：**key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption**

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。