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，第 1 页
- 设置日期和时间，第 3 页
- 配置主密码，第 6 页
- 配置 DNS 服务器，第 9 页
- 配置硬件旁路和双重电源（思科 ISA 3000），第 12 页
- 调整 ASP（加速安全路径）性能和行为，第 13 页
- 监控 DNS 缓存，第 15 页
- 基本设置历史记录，第 15 页

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。
- 要从系统更改为情景配置，请在 **Configuration > Device List** 窗格中双击主用设备 IP 地址下的情景名称。

过程

步骤 1 依次选择**配置** > **设备设置** > **设备名称/密码**。

步骤 2 输入主机名。默认主机名为“ciscoasa”。

该主机名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。该主机名同时用于系统日志消息。

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。在情景中选择性设置的主机名将不会显示在命令行中；但可用于标题。

步骤 3 输入域名。默认域名为 default.domain.invalid。

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 4 更改特权模式（启用）密码。默认密码为空，但第一次在 CLI 输入 **enable** 命令时，系统会提示您更改密码。

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。ASDM 不像 CLI 访问那样强制执行启用密码更改。

a) 选中 **Change the privileged mode password** 复选框。
b) 输入、新密码，然后确认新密码。设置一个长度为8到127个字符且区分大小写的密码。它可以任意组合使用 ASCII 可打印字符（字符代码 32-126），但是下列除外。
   - 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**

您无法将密码重置为空值。

步骤 5 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。

a) 选中 **Change the password to access the console of the security appliance** 复选框。
b) 输入旧密码（对于新 ASA 而言，将此字段留空）、新密码，然后确认新密码。密码长度最大为16个字符。它可以任意组合使用ASCII可打印字符（字符代码32-126），但是空格和问号除外。

步骤 6 点击 **Apply** 保存更改。

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。

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。

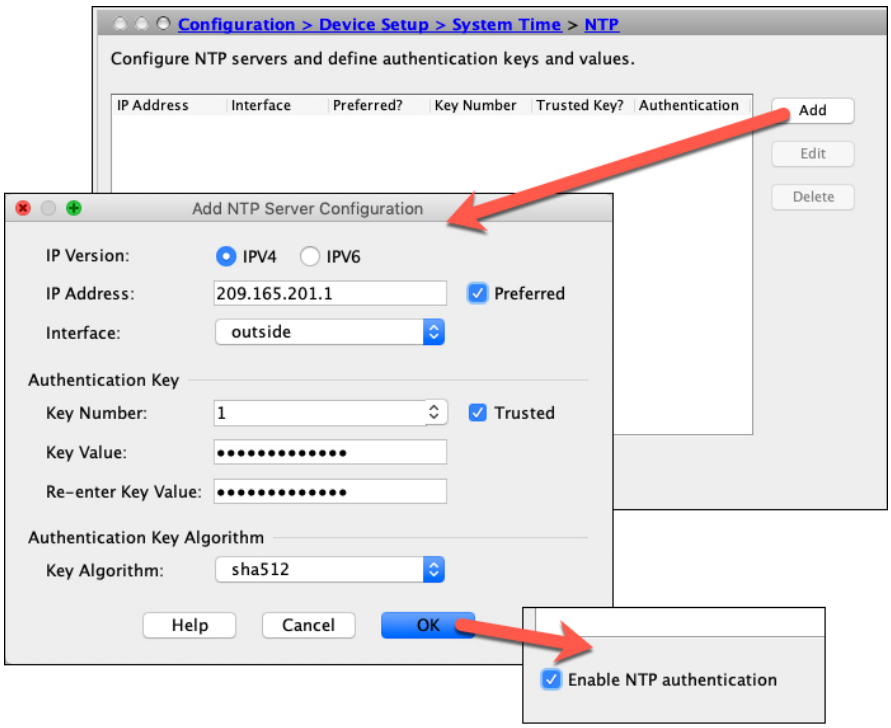
ASA 支持 NTPv4。

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 依次选择**配置** > **设备设置** > **系统时间** > **NTP**。



步骤 2 点击**添加**，可显示**添加 NTP 服务器配置**对话框。

步骤 3 输入 NTP 服务器的 **IPv4** 或 **IPv6 IP 地址**。

不能输入服务器的主机名；ASA 不支持 NTP 服务器的 DNS 查找。

步骤 4 （可选） 选中**首选 (Preferred)** 复选框，将该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。如果多台服务器准确度相似，则使用首选服务器。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。

步骤 5 （可选） 从下拉列表中选择**接口**。

该设置指定 NTP 数据包的传出接口。如果接口为空，则 ASA 根据管理路由表使用默认管理情景接口。

步骤 6 （可选） 配置 NTP 身份验证。

a) 输入介于 1 和 4294967295 之间的**密钥号**，或者如果您之前为要重用的其他 NTP 服务器创建了密钥，请从下拉列表中选择现有密钥号。

该设置指定此身份验证密钥的密钥 ID，可供您使用 身份验证与 NTP 服务器进行通信。NTP 服务器数据包必须也使用此密钥 ID。

b) 选中**已信任**复选框。
c) 输入**密钥值**（密钥长度为 32 个字符），然后重新输入密钥值。
d) 从下拉列表中选择一种**密钥算法**。
e) 点击**确定 (OK)**。

步骤 7 选中**启用 NIP 身份验证 (Enable NTP authentication)** 复选框以启动 NTP 身份验证。

步骤 8 点击 **Apply** 保存更改。

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

步骤 1 依次选择**配置** > **设备设置** > **系统时间** > **时钟**。

步骤 2 从下拉列表中选择时区。该设置将时区指定为 GMT 加上或减去适当的小时数。如果选择东部时间、中部时间、山地时间或太平洋时间时区，则时间将自动调整为夏令时，时间范围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 ASA 上更改时区可能会丢弃到智能 SSM 的连接。

步骤 3 点击 **Date** 下拉列表以显示日历。然后，使用以下方法查找正确的日期：

- 点击月份名称以显示月份列表，然后点击所需的月份。日历将更新至该月。
- 点击年份进行更改。使用向上和向下箭头滚动浏览年份，或在输入字段中输入年份。
- 点击月份和年份右侧和左侧的箭头，向前向后滚动日历，每次一个月。
- 点击日历上的一个日期，设置日期。

步骤 4 以小时、分钟和秒的形式手动输入时间。

步骤 5 点击 **Update Display Time** 可更新 ASDM 窗格右下角显示的时间。当前时间每十秒钟自动更新一次。

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 依次选择 **Configuration** > **Device Management** > **PTP**。

步骤 2 输入 **Domain value**。

这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 3 （可选）选择“**启用端到端透明时钟模式**”，可在所有启用 PTP 的接口上启用端到端透明模式。

透明时钟是通过测量滞留时间并更新 PTP 数据包中的 `correctionField` 来补偿其延迟的时钟。

步骤 4 通过选择一个接口并点击**启用 (Enable)** 或**禁用 (Disable)**，在一个或多个设备接口上启用 PTP。

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。

步骤 5 点击**应用 (Apply)**。

下一步做什么

您可以选择 **Monitoring** > **Properties** > **PTP** 以查看 PTT 时钟和接口/端口信息。

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）
- 故障转移

- 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。
- 如果已启用故障转移，但未设置故障转移共享密钥，则在更改主密码时会显示错误消息，通知您必须输入故障转移共享密钥，以防主密码更改以纯文本形式发送。

  依次选择**配置 > 设备管理 > 高可用性 > 故障转移**，在**共享密钥**字段中输入任意字符，或如果已选择故障转移十六进制密钥，则请输入 32 个十六进制数字 (0-9A-Fa-f)，但退格符号除外。然后点击**应用 (Apply)**。
- 在主用/备用故障转移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/主用故障转移，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 选择以下选项之一：

- 在单一情景模式下，依次选择 **Configuration > Device Management > Advanced > Master Passphrase**。
- 在多情景模式下，依次选择 **Configuration > Device Management > Device Administration > Master Passphrase**。

步骤 2 选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果没有有效主密码，则在点击“应用”(Apply) 时将显示警告消息。可点击“确定”(OK) 或“取消”(Cancel) 继续操作。

如果稍后禁用密码加密，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 选中 **Change the encryption master passphrase** 复选框，以便能够输入并确认新的主密码。其已默认禁用。

新的主密码长度必须介于 8 和 128 个字符之间。

如果更改现有密码，则必须在输入新密码之前输入原密码。

将 **New** 和 **Confirm master passphrase** 字段留空，以删除主密码。

步骤 4 点击**应用**。

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。
- 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 选择以下选项之一：

- 在单一情景模式下，依次选择 **Configuration > Device Management > Advanced > Master Passphrase**。
- 在多情景模式下，依次选择 **Configuration > Device Management > Device Administration > Master Passphrase**。

步骤 2 选中 **Advanced Encryption Standard (AES) password encryption** 复选框。

如果没有有效主密码，则在点击 Apply 时将显示警告语句。可点击 OK 或 Cancel 继续操作。

步骤 3 选中 Change the encryption master passphrase 复选框。

步骤 4 在 **Old master passphrase** 字段中输入原主密码。只有提供原主密码才能禁用该主密码。

步骤 5 将 **New master passphrase** 和 **Confirm master passphrase** 字段留空。

步骤 6 点击**应用**。

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 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 依次选择**配置 (Configuration)** > **设备管理 (Device Management)** > **DNS** > **DNS 客户端 (DNS Client)**。

步骤 2 在 **DNS Setup** 区域中，选择以下选项之一：

- **配置一个 DNS 服务器组 (Configure one DNS server group)** - 此选项定义 DefaultDNS 组中的服务器。
- **配置多个 DNS 服务器组**-使用此选项，您可以配置 DefaultDNS 组以及可与特定域关联的其他组，以及用于远程访问 SSL VPN 组策略的组。即使您仅配置了 DefaultDNS 组，如果要更改超时和此组使用的其他特征，必须选择此选项。

步骤 3 如果选择**配置一个 DNS 服务器组 (Configure one DNS server group)**，则配置 DefaultDNS 组中的服务器。

a) 在**主 DNS 服务器 (Primary DNS Server)** 中，输入可用时应当使用的 DNS 服务器的 IP 地址。对于此服务器以及每个辅助服务器，可以选择性地指定 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。

b) 点击**添加 (Add)**，添加辅助 DNS 服务器。

最多可添加六台 DNS 服务器。ASA 按顺序尝试每台 DNS 服务器，直至收到响应。使用 **Move Up**/**Move Down** 按钮按优先级顺序放置服务器。

c) 输入附加到主机名的 DNS 域名（如果主机名不是完全限定名称）。

步骤 4 如果选择**配置多个 DNS 服务器组 (Configure multiple DNS server groups)**，则定义服务器组属性。

a) 点击 **Add** 创建新组，或者选择组并点击 **Edit**。

始终列出 DefaultDNS 组。

b) 配置组属性。

- **要添加的服务器 IP 地址 (Server IP Address to Add)**，**源接口 (Source Interface)** - 输入 DNS 服务器的 IP 地址，点击**添加>> (Add>>)**。对于每个服务器，可以选择性地指定 ASA 与服务器通信时使用的 *interface_name*。如果不指定接口，ASA 将查看仅管理路由表；如果没有匹配，则会查看数据路由表。

  最多可添加六台 DNS 服务器。ASA 按顺序尝试每台 DNS 服务器，直至收到响应。使用 **Move Up**/**Move Down** 按钮按优先级顺序放置服务器。

- **超时** - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次 ASA 重试服务器列表，此超时将加倍。

- **重试 (Retries)** - 当 ASA 接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。

- 过期条目计时器（仅适用于DefaultDNS或活动组）-DNS条目的最小TTL，以分钟为单位。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。

- **轮询计时器 (Poll Timer)**（仅 DefaultDNS 或活动组）- 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。

- **域名**（仅限默认 DNS 或主用组）- 附加到主机名的域名（如果主机名不是完全限定名称）。

c) 点击**确定 (OK)**。

d) 如果您有多个组，可以通过选中默认组，点击 **设置有效**，更改该组。

如果某个组没有映射任何域，则只能将其用作默认组（请参阅 步骤 8，第 11 页）。

步骤 5 确保至少在一个接口上已启用 DNS 查找。在 **DNS 查找 (DNS Lookup)** 接口列表中，在 DNS 服务器组表下方，点击 **DNS 已启用 (DNS Enabled)** 列，选择 **真 (True)**，在接口上启用查找。

确保在将用于访问 DNS 服务器的所有接口上启用 DNS 查找。

如果不在接口上启用 DNS 查找，则无法使用 DNS 服务器**源接口 (Source Interface)** 或使用路由表找到的接口。

步骤 6 （可选） 在受信任DNS服务器下，配置用于确定在解析网络服务对象中的域名时信任哪些服务器的选项。

a) （可选） 添加或删除显式配置的受信任DNS服务器。

- 点击Add以添加新服务器，然后选择IP类型（IPv4或IPv6），输入服务器的IP地址，然后点击OK。
- 选择服务器并点击编辑以更改地址。
- 选择服务器，然后点击删除将其从受信任服务器列表中删除。

b) 选择或取消选择以下选项：

- Any-信任每个DNS服务器，监听所有DNS服务器。默认情况下该选项处于禁用状态。
- Configured-Servers-DNS服务器组中配置的服务器是否应受信任。默认情况下，此选项已启用。
- DHCP客户端-通过在DHCP客户端和DHCP服务器之间监听消息获知的服务器是否被视为受信任DNS服务器。默认情况下，此选项已启用。
- DHCP池-DHCP池中为通过设备接口上运行的DHCP服务器获取地址的客户端配置的DNS服务器是否值得信任。默认情况下，此选项已启用。
- DHCP中继-通过在DHCP客户端和DHCP服务器之间监听DHCP中继消息获知的服务器是否被视为受信任DNS服务器。默认情况下，此选项已启用。

步骤 7 （可选） 选中**在所有接口上启用 DNS Guard (Enable DNS Guard on all interfaces)** 复选框，以对每个查询执行一次 DNS 响应。

配置 DNS 检查时，还可设置 DNS 防护。对于给定接口，在 DNS 检测中配置的 DNS 防护设置优先于该全局设置。默认情况下，在已启用 DNS 防护的所有接口上都会启用 DNS 检测。

步骤 8 （可选） 将域映射到特定 DNS 服务器组。

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）。

a) 在 **DNS 组映射** 区域中，选中 **启用 DNS 组映射**。
b) 点击**添加 (Add)**。

系统将显示 **将域添加到 DNS 服务器组** 对话框。

c) 在 **DNS 服务器组到域名的映射** 下拉列表中，选择 DNS 服务器组名称。
d) 在 **域名** 字段中，输入要映射到 DNS 组的域名。
e) 点击**确定 (OK)**。
f) 重复这些步骤以添加更多映射。

步骤 9 点击 **Apply** 保存更改。

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准则：

- 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 要配置硬件旁路，请依次选择 **Configuration** > **Device Management** > **Hardware Bypass**。

步骤 2 通过选中“**关机过程中启用旁路**”复选框，将硬件旁路配置为对于每个接口对激活。

步骤 3 （可选） 通过选中 **Stay in Bypass after Power Up** 复选框，将每个接口对配置为在电源恢复及设备启动后仍保持硬件旁路模式。

停用硬件旁路后，当ASA接管数据流时，连接会短暂中断。在这种情况下，您需要在准备就绪后手动关闭硬件旁路；此选项允许您控制何时会短暂中断。

步骤 4 对于接口对，请通过选中 **Bypass Immediately** 复选框手动激活或停用硬件旁路。

步骤 5 （可选） 通过选中 **Stay in Bypass Mode until after the ASA Firepower Module Boots Up** 复选框，将硬件旁路配置为保持活动状态，直到 ASA FirePOWER 模块启动后。

启用硬件旁路时必须不带 **Stay in Bypass after Power Up** 选项，才能运行启动延迟。没有此选项，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 6 点击 **Apply**。

步骤 7 禁用 TCP 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。

a) 依次选择 **Configuration** > **Firewall** > **Service Policy**。
b) 选择 **sfrclass** 规则，然后点击 **Edit**。
c) 点击 **Rule Actions**，然后点击 **Connection Settings**。
d) 取消选中 **Randomize Sequence Number** 复选框。
e) 点击 **OK**，然后点击 **Apply**。

步骤 8 要作为预期配置建立双重电源，请依次选择 **Configuration** > **Device Management** > **Power Supply**，选中 **Enable Redundant Power Supply** 复选框，然后点击 **Apply**。

此屏幕还会显示可用的电源。

步骤 9 点击“保存”。

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

依次选择 **Configuration > Device Management > Advanced > Rule Engine**，并选择所需的选项：

- **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。

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

过程

步骤 1 要启用 ASP 负载均衡的自动打开和关闭，请依次选择 **Configuration** > **Device Management** > **Advanced** > **ASP Load Balancing**，并选中 **Dynamically enable or disable ASP load balancing based on traffic monitoring** 复选框。

步骤 2 要手动启用或禁用 ASP 负载均衡，请选中或取消选中 **Enable ASP load balancing** 复选框。

手动启用 ASP 负载均衡时，它将在您手动将其禁用之前一直保持启用状态，即使您启用了 Dynamic 选项亦是如此仅当您手动启用了 ASP 负载均衡时，才可以手动禁用 ASP 负载均衡。如果您也启用了 Dynamic 选项，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。

基本设置历史记录

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/修改的屏幕： **配置** > **设备管理** > **DNS** > **DNS 客户端**
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/修改的屏幕： **配置** > **设备管理** > **DNS** > **DNS 客户端**

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/修改的屏幕： • **配置** > **设备管理** > **用户/AAA** > **用户账号** • **配置** > **设备设置** > **设备名称/密码**
NTPv4 支持	9.14(1)	ASA 现在支持 NTPv4。 未修改任何菜单项。
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 新建/修改的菜单项： **配置** > **设备设置** > **系统时间** > **NTP** > **添加**按钮 > **添加 NTP 服务器配置**对话框> **密钥算法**下拉列表
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。 新建/修改的菜单项： **配置** > **设备设置** > **系统时间** > **NTP** > **添加**按钮 > **添加 NTP 服务器配置**对话框

功能名称	平台版本	说明
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。 未修改任何菜单项。
在 ASA virtual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 virtual的加速安全路径（ASP）中，ASA virtual 在禁用此功能的情况下表现出更好的性能。
ASA virtual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。 修改了以下菜单项：**配置 > 设备管理 > 高级 > ASP 负载均衡**
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。如需下载准则，请参阅一般操作配置指南中的“软件和配置”一章。 修改了以下菜单项： **配置** > **设备设置** > **设备名称/密码** > **启用密码** **配置** > **设备管理** > **用户/AAA** > **用户账户** > **添加/编辑用户账户** > **身份**
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。 引入了以下屏幕：**Configuration** > **Device Management** > **Power Supply**
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。 修改了以下菜单项： **配置** > **设备设置** > **设备名称/密码** > **启用密码** **配置** > **设备管理** > **用户/AAA** > **用户账户** > **添加/编辑用户账户** > **身份**

功能名称	平台版本	说明
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。 引入了以下菜单项：**配置** > **设备管理** > **硬件旁路** *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 virtual不支持该自动功能；仅支持手动启用和禁用。 修改了以下屏幕：**Configuration > Device Management > Advanced > ASP Load Balancing**
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。 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。 未修改任何 ASDM 屏幕。
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。 引入了以下屏幕： **Configuration > Device Management > Advanced > Master Passphrase** **Configuration > Device Management > Device Administration > Master Passphrase**

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。