FlexConfig 策略

以下主题介绍如何配置和部署 FlexConfig 策略。

FlexConfig 策略概述

FlexConfig 策略是 FlexConfig 对象的有序列表的容器。每个对象都包含一系列 Apache Velocity 脚本语言命令（即 ASA 配置命令）和您定义的变量。每个 FlexConfig 对象的内容实质上是一个程序，它生成一系列 ASA 命令，然后将其部署到指定的设备。然后，此命令序列会在 设备上配置相关功能。

使用 ASA 配置命令实现一些功能，但不是所有功能。没有唯一的一组 配置命令。相反，FlexConfig 的要点是允许您配置尚未通过 防火墙管理中心策略和设置直接支持的功能。

注意 思科强烈建议仅具有较强 ASA 背景且自承风险的高级用户使用 FlexConfig 策略。您可以配置不受禁止的任何命令。通过 FlexConfig 启用功能可能会导致配置的其他功能出现意想不到的结果。

您可以联系思科技术支持中心获取有关您已配置的 FlexConfig 策略的支持。思科技术支持中心不代表任何客户设计或编写自定义配置。思科不保证正确的操作或与其他 Firepower 系统功能的互通性。FlexConfig 功能可能随时被摒弃。为获得充分保证的功能支持，您必须等待 防火墙管理中心 支持。当有疑问时，请勿使用 FlexConfig 策略。

FlexConfig 策略的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 转换为 ，并且存在您正在使用（且需要继续使用）的 防火墙管理中心 不直接支持的兼容功能。在这种情况下，请在 ASA 上使用 **show running-config** 命令来查看功能配置，并创建 FlexConfig 对象以实施此功能。尝试使用对象的部署设置（一次/每次和追加/预置）以获得正确的设置。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 ，但有一个设置或功能需要配置，例如思科技术援助中心告诉您特定的设置应解决您遇到的特定问题。对于复杂功能，请使用实验室设备测试 FlexConfig，并验证您是否将得到预期行为。

系统包含一组预定义的 FlexConfig 对象，它们代表已测试的配置。如果所需的功能没有由这些对象表示，请首先确定是否可以在标准策略中配置等效功能。例如，访问控制策略包括 ASA 使用单独功能实现的入侵检测和预防、HTTP 和其他类型的协议检查、URL 过滤、应用过滤和访问控制。由于许多功能并未使用 CLI 命令予以配置，因此，您不会看到各策略均显示在 **show running-config** 输出内。

注释 在任何时候，请记住 ASA 和 之间不存在一对一重叠关系。请勿尝试在 设备上完全重新创建 ASA 配置。您必须仔细测试使用 FlexConfig 配置的各项功能。

FlexConfig 对象中的 CLI 命令

使用 ASA 配置命令配置某些功能。虽然并非所有 ASA 功能都与 兼容，但有一些功能可以在 上使用，但不能在 防火墙管理中心 策略中进行配置。可以使用 FlexConfig 对象指定配置这些功能所需的 CLI。

如果您决定使用 FlexConfig 手动配置功能，则应根据正确的语法了解和执行这些命令。FlexConfig 策略不验证 CLI 命令语法。有关正确语法和配置 CLI 命令的更多信息，请使用以下 ASA 文档作为参考：

- ASA CLI 配置指南介绍了如何配置功能。指南位于： https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html
- ASA 命令参考提供按命令名称排序的附加信息。参考位于： https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html

以下主题介绍了有关配置命令的更多信息。

确定 ASA 软件版本和当前 CLI 配置

由于系统使用 ASA 软件命令配置某些功能，因此需要确定在 设备上运行的软件中使用的当前 ASA 版本。此版本号指示用于指导配置功能的 ASA CLI 配置指南。此外，您还应检查当前基于 CLI 的配置，并将其与要实施的 ASA 配置进行比较。

注意，任何 ASA 配置都与 配置有着显著的差异。许多 策略都是在 CLI 之外配置的，因此查看这些命令看不到配置。请勿尝试在 ASA 和 配置之间创建一对一的对应关系。

要查看此信息，请与设备的管理界面建立 SSH 连接，并发出以下命令：

- **show version system** 并查找思科自适应安全装置软件版本号。（如果您通过 Cisco Secure Firewall Management Center CLI 工具发出命令，请忽略 **system** 关键字。）
- **show running-config** 查看当前的 CLI 配置。
- **show running-config all** 包括当前 CLI 配置中的所有默认命令。

也可以使用以下过程在 防火墙管理中心中发出这些命令。

过程

步骤 1 选择**系统** (⚙) > **健康** > **监控器**。

步骤 2 点击 FlexConfig 策略适用的设备的名称。

您可能需要点击“状态”表中**计数**列中的打开/关闭箭头来查看任何设备。

步骤 3 点击 **查看系统和故障排除详细信息**。

步骤 4 点击**高级故障排除 (Advanced Troubleshooting)**。

步骤 5 点击**威胁防御 CLI (Threat Defense CLI)**。

步骤 6 选择 **设备**，然后选择 **显示** 作为命令，然后键入 **版本** 或其他命令之一作为参数。

步骤 7 点击**执行 (Execute)**

对于版本，请搜索思科自适应安全设备软件版本号的输出。

您可以选择输出并按 Ctrl+C 组合键，然后将其粘贴到文本文件中以供日后分析之用。

禁止的 CLI 命令

FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 防火墙管理中心在 设备上配置的功能。

因此，您无法配置在 防火墙管理中心中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。

此外，一些 **clear** 命令已被禁止，因为它们与多项托管策略重叠，并且可以删除托管策略的部分配置。

FlexConfig 对象编辑器可防止将被禁止的命令纳入对象中。

禁止的 CLI 命令	说明
AAA	阻止配置。
AAA-Server	阻止配置。
Access-list	阻止高级 ACL、扩展 ACL 和标准 ACL。允许 Ethertype ACL。 可以使用在模板内的对象管理器中定义的标准和扩展ACL对象作为变量。

禁止的 CLI 命令	说明
ARP 检测	阻止配置。
As-path Object	阻止配置。
Banner	阻止配置。
BGP	阻止配置。
Clock	阻止配置。
Community-list Object	阻止配置。
Copy	阻止配置。
Delete	阻止配置。
DHCP	阻止配置。
Enable Password	阻止配置。
Erase	阻止配置。
Fragment Setting	被阻止，**fragment reassembly**除外。
Fsck	阻止配置。
HTTP	阻止配置。
ICMP	阻止配置。
Interface	仅阻止 **nameif**、**mode**、**shutdown**、**ip address** 和 **mac-address** 命令。
组播路由	阻止配置。
NAT	阻止配置。
Network Object/Object-group	将阻止在 FlexConfig 对象中创建网络对象，但可使用在模板内的对象管理器中定义的网络对象和组作为变量。
NTP	阻止配置。
OSPF/OSPFv3	阻止配置。
pager	阻止配置。
Password Encryption	阻止配置。
Policy-list Object	阻止配置。

禁止的 CLI 命令	说明
Prefix-list Object	阻止配置。
重新加载	不能安排重新加载。系统不使用 **reload** 命令重启系统，它使用的是 **reboot** 命令。
RIP	阻止配置。
Route-Map Object	将阻止 FlexConfig 对象中创建路由映射对象，但可使用在模板内的对象管理器中定义的路由映射对象作为变量。
Service Object/Object-group	将阻止 FlexConfig 对象中创建服务对象，但可使用在模板内的对象管理器中定义的端口对象作为变量。
SNMP	阻止配置。
SSH	阻止配置。
Static Route	阻止配置。
Syslog	阻止配置。
Time Synchronization	阻止配置。
Timeout	阻止配置。
VPN	阻止配置。

模板脚本

您可以使用脚本语言来控制 FlexConfig 对象内的处理。脚本语言指令是 Apache Velocity 1.3.1 模板引擎中支持的命令子集，它是一种支持循环、if/else 语句和变量的基于 Java 的脚本语言。

要了解如何使用该脚本语言，请参阅 http://velocity.apache.org/engine/devel/developer-guide.html 的 *Velocity* 开发人员指南。

FlexConfig 变量

在命令或处理指令的一部分依赖于运行时信息而不是静态信息的情况下，可以在 FlexConfig 对象中使用变量。在部署过程中，变量将替换为基于变量类型从设备的其他配置所获得的字符串：

- 策略对象变量被替换为从 防火墙管理中心中定义的对象获取的字符串。
- 系统变量会被替换为从设备本身或为其配置的策略中获取的信息。
- 处理脚本命令时，处理变量随策略对象或系统变量的内容一起加载。例如，在循环中将策略对象或系统变量中的一个值通过迭代方式加载到处理变量中，然后使用处理变量组成命令字符串

或执行其他操作。这些处理变量在 FlexConfig 对象中的变量列表中不显示。此外，也不要使用 FlexConfig 对象编辑器中的**插入**菜单添加这些变量。

- 密钥变量被替换为 FlexConfig 对象中为该变量定义的单个字符串。

以 $ 字符开头的变量，除以 @ 字符开头的密钥变量变量之外。例如，在下面的命令中 $ifname 是一个策略对象变量，而 @keyname 是一个密钥。

```
interface $ifname
key @keyname
```

注释 第一次插入策略对象或系统变量时，必须通过 FlexConfig 对象编辑器中的**插入**菜单执行操作。此操作可将变量添加到 FlexConfig 对象编辑器底部的**变量**列表中。但您必须在随后的使用中键入变量字符串，即使在使用系统变量时也是如此。如果添加的处理变量没有对象或系统变量赋值，请不要使用**插入**菜单。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

变量是否被解析为单个字符串、字符串列表或值表取决于分配给变量的策略对象或系统变量的类型。（密钥始终解析为单个字符串）。您必须了解返回的内容，以便正确处理变量。

以下主题解释各种类型的变量以及如何处理这些变量。

如何处理变量

在运行时，变量可以解析为单个字符串、相同类型的字符串列表、不同类型的字符串列表或命名值表。此外，解析为多个值的变量的长度可以是确定的，也可以是不定的。您必须了解要返回的内容才能正确处理这些值。

以下是可能出现的主要情况：

单值变量

如果变量始终解析为单个字符串，则在 FlexConfig 脚本中直接使用该变量而不进行修改。

例如，预定义的文本变量 tcpMssBytes 始终解析为单个值（必须为数字）。然后，**Sysopt_basic** FlexConfig 使用 if/then/else 结构根据另一个单值文本变量 tcpMssMinimum 的值设置最大段大小：

```
#if($tcpMssMinimum == "true")
  sysopt connection tcpmss minimum $tcpMssBytes
#else
  sysopt connection tcpmss $tcpMssBytes
#end
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $tcpMssBytes 的第一个用例，但您可以直接在 #else 行中键入变量。

密钥变量是一种特殊类型的单值变量。对于密钥，始终使用**插入**菜单添加变量，即使是用于第二次和后续的使用。这些变量在 FlexConfig 对象中的变量列表中不显示。

注释 网络对象的策略对象变量也等同于单个 IP 地址规范，即主机地址、网络地址或地址范围。但在这种情况下，您必须清楚需要什么类型的地址，因为 ASA 命令需要特定的地址类型。例如，如果命令需要主机地址，使用指向包含网络地址的对象的网络对象变量将导致部署过程中出错。

多值变量，所有值都具有相同类型

多个策略对象和系统变量解析为同一类型的多个值。例如，指向网络对象组的对象变量解析为组中 IP 地址的列表。同样，系统变量 $SYS_FW_INTERFACE_NAME_LIST 解析为接口名称的列表。

还可以为同一类型的多个值创建文本对象。例如，预定义的文本对象 enableInspectProtocolList 可以包含多个协议名称。

解析为同一类型项目列表的多值变量通常具有不定长度。例如，您无法预先知道命名了设备上的多少个接口，因为用户可以随时配置或取消配置接口。

因此，您通常使用循环来处理同一类型的多值变量。例如，预定义的 FlexConfig **Default_Inspection_Protocol_Enable** 使用 #foreach 循环来遍历 enableInspectProtocolList 对象并处理每个值。

```
policy-map global_policy
    class inspection_default
    #foreach ( $protocol in $enableInspectProtocolList)
    inspect $protocol
    #end
```

在此示例中，该脚本依次将每个值分配给 $protocol 变量，然后在 ASA **inspect** 命令中使用该变量为该协议启用检测引擎。在这种情况下，您只需键入 $protocol 作为变量名称。您不使用**插入**菜单来添加它，因为您没有将对象或系统值分配给该变量。但是，必须使用**插入**菜单添加 $enableInspectProtocolList。

系统在 #foreach 和 #end 之间循环遍历代码，直到 $enableInspectProtocolList 中没有剩余的值。

多个值变量，值具有不同的类型

可以创建多个值文本对象，但每个值都有不同的用途。例如，预定义的 **netflow_Destination** 文本对象应具有 3 个值，分别表示接口名称、目标 IP 地址和 UDP 端口号。

以这种方式定义的对象应具有确定的值数。否则，它们将很难处理。

使用 get 方法处理这些对象。在对象名称的末尾键入 **.get(*n*)**，并将 *n* 替换为对象中的索引。从 0 开始计数，即使文本对象从 1 开始列出其值亦是如此。

例如，Netflow_Add_Destination 对象使用以下行将 netflow_Destination 中的 3 个值添加到 ASA **flow-export** 命令。

```
flow-export destination $netflow_Destination.get(0) $netflow_Destination.get(1)
$netflow_Destination.get(2)
```

在此示例中，您将使用 FlexConfig 对象编辑器中的**插入**菜单添加 $netflow_Destination 的第一次使用，然后添加 **get(0)**。但您可以直接为 **$netflow_Destination.get(1)** 和 **$netflow_Destination.get(2)** 规范键入该变量。

解析到值表的多个值变量

有些系统变量会返回一个值表。这些变量包括其名称中的 MAP，例如 $SYS_FTD_ROUTED_INTF_MAP_LIST。路由接口映射返回的数据如下所示（为了清楚起见，添加了换行）：

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]
```

在上面的示例中，将为 4 个接口返回信息。每个 接口都包括一个指定值表。例如，intf_hardwarare_id 是 接口硬件名称属性的名称，并将返回诸如 GigabitEthernet0/0 的字符串。

这种类型的变量通常长度不确定，因此您需要 使用环路来处理值。但您还需要将属性 名称添加到变量名称中，以指示要检索哪个值。

例如，IS-IS 配置需要在接口配置模式下将 ASA **isis** 命令添加到某一具有逻辑名称的接口。但您可以使用该接口的 硬件名称进入该模式。因此，您需要确定哪些接口具有 逻辑名称，然后仅配置使用其硬件名称的那些接口。预定义了 ISIS_Interface_Configuration 的 FlexConfig 使用 嵌套在环路中的 if/then 结构来进行此操作。在下面的代码中，可以看到 #foreach 脚本命令会将每个接口映射加载到 $intf 变量中， 然后 #if 语句将切断映射 ($intf.intf_logical_name) 中的 intf_logical_name 值，并且如果该值位于 isisIntfList 预定义文本变量中定义的列表中，则请使用 intf_hardwarare_id 值 ($intf.intf_hardwarare_id) 输入接口命令。您需要编辑 isisIntfList 变量以添加要在其上配置 IS-IS 的接口的 名称。

```
#foreach ($intf in $SYS_FTD_ROUTED_INTF_MAP_LIST)
 #if ($isIsIntfList.contains($intf.intf_logical_name))
  interface $intf.intf_hardwarare_id
   isis
   #if ($isIsAddressFamily.contains("ipv6"))
   ipv6 router isis
   #end
 #end
#end
```

如何查看将为设备返回什么变量

评估将会返回什么变量的一种简单方式是创建一个简单的 FlexConfig 对象，该对象除了处理带有注释的变量列表以外，不进行任何其他操作。随后可将该对象分配给某一 FlexConfig 策略，再将该策略分配给某一设备，保存该策略，然后预览该设备的配置。该预览将显示解析出来的值。可以选择预览文本，按 Ctrl+C 键，然后将输出粘贴到文本文件中用于分析。

注释 但不要将此 FlexConfig 部署到设备，因为它不会包含任何有效的配制命令。您将收到部署错误。在获得预览后，请从 FlexConfig 策略中删除该 FlexConfig 对象，然后保存该策略。

例如，可以构建以下 FlexConfig 对象：

```
Following is a network object group variable for the
IPv4-Private-All-RFC1918 object:

$IPv4_Private_addresses

Following is the system variable SYS_FW_MANAGEMENT_IP:

$SYS_FW_MANAGEMENT_IP

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:

$SYS_FTD_ROUTED_INTF_MAP_LIST

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

$SYS_FW_INTERFACE_NAME_LIST
```

此对象的 预览可能如下所示（为了清楚起见，添加了换行）：

```
###Flex-config Prepended CLI ###

###CLI generated from managed features ###

###Flex-config Appended CLI ###
Following is an network object group variable for the
IPv4-Private-All-RFC1918 object:

[10.0.0.0, 172.16.0.0, 192.168.0.0]

Following is the system variable SYS_FW_MANAGEMENT_IP:

192.168.0.171

Following is the system variable SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST:

[dns, ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc,
xdmcp, sip, netbios, tftp, icmp, icmp error, ip-options]

Following is the system variable SYS_FTD_ROUTED_INTF_MAP_LIST:
```

```
[{intf_hardwarare_id=GigabitEthernet0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.10.1, intf_ipv6_link_local_address=,
intf_logical_name=outside},

{intf_hardwarare_id=GigabitEthernet0/1, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=255.255.255.0,
intf_ip_addr_v4=10.100.11.1, intf_ipv6_link_local_address=,
intf_logical_name=inside},

{intf_hardwarare_id=GigabitEthernet0/2, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=},

{intf_hardwarare_id=Management0/0, intf_ipv6_eui64_addresses=[],
intf_ipv6_prefix_addresses=[], intf_subnet_mask_v4=, intf_ip_addr_v4=,
intf_ipv6_link_local_address=, intf_logical_name=management}]

Following is the system variable SYS_FW_INTERFACE_NAME_LIST:

[outside, inside, management]
```

FlexConfig 策略对象变量

策略对象变量与在对象管理器中配置的特定策略对象关联。在 FlexConfig 对象中插入策略对象变量时，将为该变量提供一个名称，并选择与其关联的对象。

尽管可以为变量提供与关联对象完全相同的名称，但变量本身与关联对象不同。必须使用FlexConfig对象编辑器中的**插入** > **插入策略对象** > **对象类型**菜单首次将该变量添加到 FlexConfig 中的脚本，以建立与该对象的关联。仅键入前面带有 $ 符号的对象的名称不会创建策略对象变量。

您可以创建变量以指向以下类型的对象。确保为每个变量创建正确的对象类型。要创建对象，请转到**对象** > **对象管理**页面。

- **文本对象** - 适用于文本字符串，可以包括 IP 地址、数字和其他自由格式文本，如接口或区域名称。从目录中选择 **FlexConfig** > **文本对象**，然后点击**添加文本对象**。可以将这些对象配置为包含单个值或多个值。这些对象具有高度的灵活性，专用于 FlexConfig 对象。有关详细信息，请参阅配置 FlexConfig 文本对象 ， 第 26 页。
- **网络** - 适用于 IP 地址。可以使用网络对象或组。从目录中选择**网络**，然后选择**添加网络** > **添加对象**或**添加组**。如果使用组对象，该变量将返回组中每个 IP 地址规范的列表。地址可以是主机、网络或地址范围，具体取决于对象内容。请参阅网络。
- **安全区域** - 适用于安全区域或接口组中的接口。从目录中选择**接口**，然后选择**添加** > **安全区域**或**接口组**。安全区域变量将为正配置的设备返回该区域或组内的接口列表。请参阅接口。
- **标准的 ACL 对象** - 适用于标准访问控制列表。标准 ACL 变量返回标准 ACL 对象的名称。从目录中选择**访问列表** > **标准**，然后点击**添加标准访问列表对象**。请参阅访问列表。
- **扩展 ACL 对象** - 适用于扩展访问控制列表。扩展 ACL 变量将返回扩展 ACL 对象的名称。从目录中选择**访问列表** > **扩展**，然后点击**添加扩展访问列表对象**。请参阅访问列表。
- **路由映射** - 适用于路由映射对象。路由映射变量将返回路由映射对象的名称。从目录中选择**路由映射**，然后点击**添加路由映射**。请参阅路由映射。

FlexConfig 系统变量

系统变量会被替换为从设备本身或为其配置的策略中获取的信息。

必须使用 FlexConfig 对象编辑器中的**插入** > **插入系统变量** > **变量名**菜单，第一次就开始将变量添加到 FlexConfig 中的脚本以建立与系统变量的关联。只键入系统变量的名称并前跟 $ 符号不会在 FlexConfig 对象的上下文中创建系统变量。

下表介绍了可用的系统变量。在使用变量之前，检查通常为变量返回的内容；请参阅如何查看将为设备返回什么变量，第 9 页。

名称	说明
SYS_FW_OS_MODE	设备的操作系统模式。可能的值包括 ROUTED 或 TRANSPARENT。
SYS_FW_OS_MULTIPLICITY	设备在单情景模式还是多情景模式下运行。可能的值包括 SINGLE、MULTI 或 NOT_APPLICABLE。
SYS_FW_MANAGEMENT_IP	设备的管理 IP 地址
SYS_FW_HOST_NAME	设备主机名
SYS_FTD_INTF_POLICY_MAP	以接口名称作为键并将策略映射为值的映射。如果设备上没有定义基于接口的服务策略，则此变量将不返回任何值。
SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST	启用了检查的协议的列表。
SYS_FTD_ROUTED_INTF_MAP_LIST	设备上路由接口映射的列表。每个映射都包含一组与路由接口配置相关的命名值。
SYS_FTD_SWITCHED_INTF_MAP_LIST	设备上交换接口映射的列表。每个映射都包含一组与交换接口配置相关的命名值。
SYS_FTD_INLINE_INTF_MAP_LIST	设备上内联接口映射的列表。每个映射都包含一组与内联集接口配置相关的命名值。
SYS_FTD_PASSIVE_INTF_MAP_LIST	设备上被动接口映射的列表。每个映射都包含一组与被动接口配置相关的命名值。
SYS_FTD_INTF_BVI_MAP_LIST	设备上网桥虚拟接口映射的列表。每个映射都包含一组与 BVI 配置相关的命名值。
SYS_FW_INTERFACE_HARDWARE_ID_LIST	设备上接口硬件名称（如 GigabitEthernet0/0）的列表。
SYS_FW_INTERFACE_NAME_LIST	设备上接口逻辑名称（如内部）的列表。
SYS_FW_INLINE_INTERFACE_NAME_LIST	配置为被动或 ERSPAN 被动的接口的逻辑名称列表。
SYS_FW_NON_INLINE_INTERFACE_NAME_LIST	不属于内联集的接口（如所有路由接口）的逻辑名称列表。

预定义的 FlexConfig 对象

预定义的 FlexConfig 对象为选定功能提供经过测试的配置。如果需要配置这些功能，请使用这些对象，否则无法使用 防火墙管理中心配置这些功能。

下表列出了可用的对象。记下关联的文本对象。您必须编辑这些文本对象，才能自定义预定义 FlexConfig 对象的行为。文本对象使您可以使用网络和设备所需的 IP 地址和其他属性来自定义配置。

如果需要修改预定义 FlexConfig 对象，请复制该对象，对副本进行更改，然后使用新名称进行保存。不能直接编辑预定义 FlexConfig 对象。

尽管您可以使用 FlexConfig 配置其他基于 ASA 的功能，但这些功能的配置尚未经过测试。如果某个 ASA 功能与您可以在 防火墙管理中心策略中配置的内容重叠，请勿尝试通过 FlexConfig 对该功能进行配置。

例如，Snort 检查包括 HTTP 协议，因此不可启用 ASA 式 HTTP 检查。（实际上，您无法将 **http** 添加到 enableInspectProtocolList 对象。在这种情况下，您将被阻止以免错误配置您的设备。）相反，应根据需要配置访问控制策略以执行应用或 URL 过滤，以实施 HTTP 检查要求。

表 *1:* 预定义的 ***FlexConfig*** 对象

FlexConfig 对象名称	**Description**	关联的文本对象
Default_Inspection_Protocol_Disable	在 global_policy 默认策略映射中禁用协议。	disableInspectProtocolList
Default_Inspection_Protocol_Enable	在 global_policy 默认策略映射中启用协议。	enableInspectProtocolList
Inspect_IPv6_Configure	在 global_policy 策略映射中配置 IPv6 检查，从而根据 IPv6 报头内容记录和丢弃流量。	IPv6RoutingHeaderDropLogList、IPv6RoutingHeaderLogList、IPv6RoutingHeaderDropList。
Inspect_IPv6_UnConfigure	清除并禁用 IPv6 检查。	—
ISIS_Configure	为 IS-IS 路由配置全局参数。	isIsNet、isIsAddressFamily、isISType
ISIS_Interface_Configuration	接口级别 IS-IS 配置。	isIsAddressFamily、IsIsIntfList 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST
ISIS_Unconfigure	清除设备上的 IS-IS 路由器配置。	—
ISIS_Unconfigure_All	从设备中清除 IS-IS 路由器配置，包括来自设备接口的路由器分配。	—
NGFW_TCP_NORMALIZATION	修改默认 TCP 规范化配置。	—

FlexConfig 对象名称	Description	关联的文本对象
Policy_Based_Routing	要使用此示例配置，请复制它，修改接口名称，然后使用 r-map-object 文本对象标识对象管理器中的路由映射对象。	—
Policy_Based_Routing_Clear	从设备中清除策略型路由配置。	—
Sysopt_AAA_radius	忽略 RADIUS 记帐响应中的身份验证密钥。	—
Sysopt_AAA_radius_negate	使 Sysopt_AAA_radius 配置失效。	—
Sysopt_basic	配置 sysopt 等待时间、TCP 数据包的最大报文段长度以及详细流量统计信息。	tcpMssMinimum、tcpMssBytes
Sysopt_basic_negate	清除 sysopt_basic 详细流量统计信息、等待时间和 TCP 最大报文段长度。	—
Sysopt_clear_all	从设备中清除所有 sysopt 配置。	—
Sysopt_noproxyarp	配置 noproxy-arp CLI。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_noproxyarp_negate	清除 Sysopt_noproxyarp 配置。	使用系统变量 SYS_FW_NON_INLINE_INTF_NAME_LIST
Sysopt_Preserve_Vpn_Flow	配置 syopt 保留 VPN 流。	—
Sysopt_Preserve_Vpn_Flow_negate	清除 Sysopt_Preserve_Vpn_Flow 配置。	—
Sysopt_Reclassify_Vpn	配置 sysopt 重新分类 VPN。	—
Sysopt_Reclassify_Vpn_Negate	否定 sysopt 重新分类 VPN。	—
Threat_Detection_Clear	清除威胁检测 TCP 拦截配置。	—
Threat_Detection_Configure	配置 TCP 拦截所拦截攻击的威胁检测统计信息。	threat_detection_statistics
Wccp_Configure	此模板提供了一个配置 WCCP 的示例。	isServiceIdentifier、serviceIdentifier、wccpPassword
Wccp_Configure_Clear	清除 WCCP 配置。	—

弃用的 FlexConfig 对象

下表列出了用于配置您现在可以在 GUI 中本地配置的功能的对象。尽早停止使用这些对象。

表 2: 弃用的预定义 *FlexConfig* 对象

弃用的版本	FlexConfig 对象	Description	现在配置在
7.3	DHCPv6_Prefix_Delegation_Configure	为 IPv6 前缀委派配置一个外部接口（前缀委派客户端）和一个内部接口（委派前缀的接收者）。要使用此模板，请对其进行复制并修改变量。 关联的文本对象：pdoutside、pdinside 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST	接口 IPv6 设置。
7.3	DHCPv6_Prefix_Delegation_UnConfigure	删除 DHCPv6 前缀委派配置。	接口 IPv6 设置。
6.3	Default_DNS_Configure	配置默认 DNS 组，该组定义在数据接口上解析完全限定域名时可以使用的 DNS 服务器。 关联的文本对象：defaultDNSNameServerList、defaultDNSParameters	平台设置。
6.3	DNS_Configure	在非默认 DNS 服务器组中配置 DNS 服务器。复制对象以更改组的名称。	对象管理器中的**DNS 服务器组** 。
6.3	DNS_UnConfigure	删除由 Default_DNS_Configure 和 DNS_Configure 执行的 DNS 服务器配置。如果您更改了 DNS_Configure，则复制该对象以更改 DNS 服务器组名称。	对象管理器中的**DNS 服务器组** 。
7.2	Eigrp_Configure	配置 EIGRP 路由 next-hop、auto-summary、router-id、eigrp-stub。 关联的文本对象：eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary	有关所有 EIGRP 对象，请参阅 EIGRP。 系统允许您部署升级后，但也会警告您重新执行 EIGRP 配置。为了帮助您完成此过程，我们提供了一个命令行迁移工具。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	Eigrp_Interface_Configure	配置 EIGRP 接口身份验证模式、身份验证密钥、呼叫间隔、保持时间、水平分割。 关联的文本对象：eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon 还使用系统变量 SYS_FTD_ROUTED_INTF_MAP_LIST	
7.2	Eigrp_Unconfigure	从设备中清除自治系统的 EIGRP 配置。	
7.2	Eigrp_Unconfigure_all	清除所有 EIGRP 配置。	
7.4	Netflow_Add_Destination	创建和配置 Netflow 导出目标。 关联的文本对象：Netflow_Destinations、netflow_Event_Types	平台设置。
7.4	Netflow_Clear_Parameters	恢复 Netflow 导出全局默认设置。	平台设置。
7.4	Netflow_Delete_Destination	删除 Netflow 导出目标。 关联的文本对象：Netflow_Destinations、netflow_Event_Types	平台设置。
7.4	Netflow_Set_Parameters	为 Netflow 导出设置全局参数。 关联的文本对象：netflow_Parameters	平台设置。
6.3	TCP_Embryonic_Conn_Limit	配置初始连接限制以防止 SYN 泛洪拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_limit	服务政策。
6.3	TCP_Embryonic_Conn_Timeout	配置初始连接超时以防止 SYN 洪流拒绝服务 (DoS) 攻击。 关联的文本对象：tcp_conn_misc、tcp_conn_timeout	服务政策。

弃用的版本	FlexConfig 对象	Description	现在配置在
7.2	VxLAN_Clear_Nve	从设备中删除使用 VxLAN_Configure_Port_And_Nve 时配置的 NVE 1。	有关所有 VxLAN 对象，请参阅配置 VXLAN 接口。 如果在以前的版本中使用 FlexConfig 配置了 VXLAN 接口，它们将继续工作。实际上，在这种情况下，FlexConfig 优先 - 如果您在 Web 接口中重做 VXLAN 配置，请删除 FlexConfig 设置。
7.2	VxLAN_Clear_Nve_Only	在部署时，清除在接口上配置的 NVE。	
7.2	VxLAN_Configure_Port_And_Nve	配置 VLAN 端口和 NVE 1。 关联的文本对象：vxlan_Port_And_Nve	
7.2	VxLAN_Make_Nve_Only	仅为 NVE 设置接口。 关联的文本对象：vxlan_Nve_Only 还使用系统变量 SYS_FTD_ROUTED_MAP_LIST 和 SYS_FTD_SWITCHED_INTF_MAP_LIST	
7.2	VxLAN_Make_Vni	创建 VNI 接口。部署此项后，您必须先注销设备，然后再重新注册设备，才能正确发现 VNI 接口。 关联的文本对象：vxlan_Vni	

预定义的文本对象

有多种预定义的文本对象。这些对象与预定义的 FlexConfig 对象中使用的变量关联。在大多数情况下，如果您使用关联的 FlexConfig 对象，则必须编辑这些对象才能添加值，否则将在部署过程中出错。尽管其中一些对象包含默认值，但其他一些则为空。

有关编辑文本对象的信息，请参阅配置 FlexConfig 文本对象，第 26 页。

名称	说明	关联的 FlexConfig 对象
defaultDNSNameServerList （已弃用。）	要在默认 DNS 组中配置的 DNS 服务器 IP 地址。 从版本 6.3 开始，在威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
defaultDNSParameters （已弃用。）	用于控制默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、过期条目计时器、轮询计时器、域名条目。 从版本 6.3 开始，在威胁防御平台设置策略中为数据接口配置 DNS。	Default_DNS_Configure
disableInspectProtocolList	在默认策略映射 (global_policy) 中禁用协议。	Disable_Default_Inspection_Protocol
dnsNameServerList	要在用户定义的 DNS 组中配置的 DNS 服务器 IP 地址。	DNS_Configure
dnsParameters	用于控制非默认 DNS 服务器组的 DNS 行为的参数。该对象包含单独的条目，依次为重试、超时、域名、域名服务器条目。	DNS_Configure
enableInspectProtocolList	在默认策略映射 (global_policy) 中启用协议。您将不允许添加其检查与 Snort 检查冲突的协议。	Enable_Default_Inspection_Protocol
IPv6RoutingHeaderDropList	要禁止的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，而不记录此丢弃。	Inspect_IPv6_Configure
IPv6RoutingHeaderDropLogList	要禁止和记录的 IPv6 路由报头类型的列表。IPv6 检查会丢弃包含这些报头的数据包，并发送有关此丢弃的系统日志消息。	Inspect_IPv6_Configure
IPv6RoutingHeaderLogList	要允许但会记录的 IPv6 路由报头类型的列表。IPv6 检查会允许包含这些报头的数据包，并发送有关存在报头的系统日志消息。	Inspect_IPv6_Configure
isIsAddressFamily	IPv4 或 IPv6 地址系列。	ISIS_Configure ISIS_Interface_Configuration
IsIsIntfList	逻辑接口名称的列表。	ISIS_Interface_Configuration

名称	说明	关联的 **FlexConfig** 对象
isIsISType	IS 类型（级别 1、级别 2 或级别 1-2）。	ISIS_Configure
isIsNet	网络实体。	ISIS_Configure
isServiceIdentifier	如果为 false，则使用标准的 **web-cache** 服务标识符。	Wccp_Configure
netflow_Destination	定义单个 NetFlow 导出目标的接口、目标和 UDP 端口号。	Netflow_Add_Destination
netflow_Event_Types	将要为目标导出的事件类型定义为以下任意项的子集：**all**、**flow-create**、**flow-defined**、**flow-teardown**、**flow-update**。	Netflow_Add_Destination
netflow_Parameters	提供 NetFlow 导出全局设置：活动刷新间隔（流更新事件之间的分钟数）、延迟（以秒为单位的流创建延迟；默认值 0 = 命令不会出现）和以分钟为单位的模板超时速率。	Netflow_Set_Parameters
PrefixDelegationInside	为 DHCPv6 前缀委派配置内部接口。该对象包含多个条目，依次为接口名称、包含前缀长度的 IPv6 后缀以及前缀池名称。	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
PrefixDelegationOutside	配置外部 DHCPv6 前缀委派客户端。该对象包括多个条目，依次为接口名称和 IPv6 前缀长度条目	没有，但可以与 DHCPv6_Prefix_Delegation_Configure 副本一起使用。
serviceIdentifier	动态 WCCP 服务标识符编号。	Wccp_Configure
tcp_conn_limit （已弃用。）	用于配置 TCP 初始连接限制的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit
tcp_conn_misc （已弃用。）	用于配置 TCP 初始连接设置的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Limit、TCP_Embryonic_Conn_Timeout

名称	说明	关联的 FlexConfig 对象
tcp_conn_timeout （已弃用。）	用于配置 TCP 初始连接超时的参数。 从版本 6.3 开始，在威胁防御服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”选项卡上找到该策略。	TCP_Embryonic_Conn_Timeout
tcpMssBytes	最大段大小（以字节为单位）。	Sysopt_basic
tcpMssMinimum	检查是否设置最大段大小 (MSS)，只有此标志为 true 时才设置该值。	Sysopt_basic
threat_detection_statistics	用于TCP拦截的威胁检测统计信息的参数。	Threat_Detection_Configure
vxlan_Nve_Only	用于在接口上配置仅 NVE 的参数： • 接口的逻辑名称 • IPv4 地址（对于路由接口而言可选） • Ipv4 网络掩码（对于路由接口而言可选）	VxLAN_Make_Nve_Only
vxlan_Port_And_Nve	用于为 VXLAN 配置端口和 NVE 的参数： • Vxlan 端口 • 源接口（逻辑名称） • 类型（对等体或组播） • 对等体 IP 地址或 default-mcast-grooup	VxLAN_Configure_Port_And_Nve

名称	说明	关联的 FlexConfig 对象
vxlan_Vni	用于创建 VNI 的参数： • 接口编号 (1-10000) • segment-id (1-16777215) • nameif（接口的逻辑名称） • 类型（路由或透明） • IP 地址（如果是路由模式设备时使用）或网桥组编号（如果是透明模式设备时使用） • 网络掩码（如果设备处于路由模式）或未使用	VxLAN_Make_Vni
wccpPassword	WCCP 密码。	Wccp_Configure

FlexConfig 策略的要求和前提条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

FlexConfig 的准则与限制

- 如果您在 FlexConfig 策略中犯错，系统将回滚包含失败的 FlexConfig 的部署尝试中包含的所有更改。由于部署失败导致的回滚包括了清除配置，因此这可能会中断您的网络。考虑将FlexConfig 更改纳入非营业时间的计时部署中。此外，请考虑隔离部署，使其仅包括 FlexConfig 更改而不包括其他策略更新。
- 使用 VxLAN_Make_VNI 对象时，必须在形成集群或高可用性对之前，将相同的 FlexConfig 部署到该集群或高可用性对中的所有设备。在形成集群或高可用性对之前，管理中心要求VXLAN 接口在所有设备上都匹配。

- 如果配置适用于连接的任何服务（例如 SIP 检测），请转至设备 CLI 并输入 **clear conn** 命令以清除连接。重建连接时，新配置将应用于会话。

使用 FlexConfig 策略自定义设备配置

使用 FlexConfig 策略自定义 设备的配置。

在使用 FlexConfig 之前，请尝试使用 防火墙管理中心中的其他功能配置所需的所有策略和设置。FlexConfig 是一种配置基于 ASA 的与 兼容但在 防火墙管理中心中不可配置的功能的必备方法。

以下是配置和部署 FlexConfig 策略的端到端过程。

过程

步骤 1 确定要配置的 CLI 命令序列。

如果在 ASA 设备上具有有效的配置，请使用 **show running-config** 获取所需命令的序列。根据需要对接口名称和 IP 地址等项目进行调整。

如果此步骤是面向新功能，最好尝试在实验室设置中的ASA 设备上实现，以验证您具有正确的命令序列。

有关详细信息，请参阅以下主题：

- FlexConfig 策略的建议用法，第 1 页
- FlexConfig 对象中的 CLI 命令，第 2 页

步骤 2 选择**对象** > **对象管理** > **FlexConfig** > **FlexConfig 对象**。

检查预定义的 FlexConfig 对象，以确定是否能够生成所需的命令。点击 **视图**（） 以查看对象内容。如果现有对象接近您所需的内容，请首先复制该对象，然后编辑副本。请参阅预定义的FlexConfig 对象，第 12 页。

检查这些对象还可以让您了解 FlexConfig 对象的结构、命令语法和预期顺序。

注释
如果找到要使用的任何对象（直接对象或或是副本），请检查对象底部的“变量”列表。记下变量名称，但全部采用以 SYS 开头的大写字母的变量除外，这些是系统变量。这些变量是您编辑和定义覆盖可能需要的文本对象，尤其是在默认值列显示对象没有值的情况下更是如此。

步骤 3 如果需要创建自己的 FlexConfig 对象，请确定需要哪些变量并创建关联对象。

您需要部署的 CLI 可能包含 IP 地址、接口名称、端口号以及以后可能需要调整的其他参数。这些变量已经与指向包含所需值的变量实现了最好的分隔。对于属于配置一部分，但以后可能会更改的字符串，您可能也需要变量。

此外，还要确定是否要为您将为其分配策略的每个设备使用不同的值。例如，您可能希望在三个设备上配置该功能，但可能需要为其中每个设备在给定命令上指定不同的接口名称或 IP 地址。如果需要为每个设备自定义对象，请确保在创建对象时启用覆盖，然后按设备定义覆盖值。

有关各种类型的变量的解释以及如何在需要时配置相关对象，请参阅下列主题。

- FlexConfig 变量， 第 5 页
- FlexConfig 策略对象变量， 第 10 页
- FlexConfig 系统变量， 第 11 页
- 配置 FlexConfig 文本对象， 第 26 页

步骤 4 如果使用预定义的 FlexConfig 对象，请编辑用作变量的文本对象。

请参阅配置 FlexConfig 文本对象， 第 26 页。

步骤 5 （如有必要。）配置 FlexConfig 对象， 第 22 页。

只有在预定义的对象无法创建对象时，您才需要执行此操作。

步骤 6 配置 FlexConfig 策略， 第 28 页。

步骤 7 为 FlexConfig 策略设置目标设备， 第 29 页。

还可以在创建策略时将策略分配给设备。策略必须至少有一个已分配的设备，您才能预览它。

步骤 8 预览 FlexConfig 策略， 第 30 页。

必须先保存更改，才能预览策略。

验证所生成的命令是否是所预期的，以及所有变量是否都在正确解析。

步骤 9 在菜单栏中选择**部署 (Deploy)** > **部署 (Deployment)**。

步骤 10 选择分配给该策略的设备，然后点击**部署 (Deploy)**。

等待部署完成。

步骤 11 验证部署的配置， 第 30 页。

步骤 12 （如有必要。）删除使用 FlexConfig 配置的功能， 第 32 页。

与其他类型的策略不同，仅仅从一台设备取消分配 FlexConfig 可能不会删除相关的配置。如果要删除 FlexConfig 生成的配置，需要遵循上述程序。

如果您要删除某项功能，因为产品目前已支持该功能，另请参阅从 FlexConfig 转换为管理功能， 第 33 页。

配置 FlexConfig 对象

使用 FlexConfig 对象定义要部署到设备的配置。每个 FlexConfig 策略由一个 FlexConfig 对象列表组成，因此这些对象实质上是由 Apache 速度脚本命令、ASA 软件配置命令和变量组成的代码模块。

有几个可以直接使用的预定义 FlexConfig 对象，或者如果需要编辑这些对象，可以制作对象副本。还可以从头创建自定义对象。FlexConfig 对象的内容可以是从一个简单的命令字符串到复杂 CLI 命令结构的任何内容，复杂CLI命令结构使用变量和脚本命令来部署其内容因设备或部署而异的命令。

还可以在定义 FlexConfig 策略时创建 FlexConfig 策略对象。

开始之前

记住以下几点：

- FlexConfig 对象转换为随后部署到设备的命令。这些命令已在全局配置模式下发出。因此，请不要将 **enable** 和 **configure terminal** 命令作为 FlexConfig 对象的一部分。
- 确定所需的变量类型，并创建所需的任何策略对象。编辑 FlexConfig 对象时，不能为变量创建对象。
- 确保您的命令与设备上的 VPN 或访问控制配置没有任何冲突。
- 如果接口有多组命令，只部署最后一组命令。因此，我们建议您不要使用开始和结束命令来配置接口。有关配置接口的示例，请参阅 ISIS_Interface_Configuration 预定义的 FlexConfig 对象。

过程

步骤 1 选择**对象** > **对象管理** > **FlexConfig** > **FlexConfig 对象**。

步骤 2 执行以下操作之一：

- 点击**添加 FlexConfig 对象**以创建新对象。
- 点击 **编辑** (✎) 以编辑现有对象。
- 点击 **视图**（🔍） 可查看预定义对象的内容。
- 如果要编辑预定义对象，请点击 **克隆** （⧉） 以创建具有相同内容的新对象。

步骤 3 为对象输入**名称**和（可选）说明

步骤 4 在对象正文区域中，输入生成所需配置的命令和说明。

对象内容是生成有效的 ASA 软件命令序列的脚本命令和配置命令序列。设备使用 ASA 软件命令来配置某些功能。有关脚本和配置命令的详细信息，请参阅：

- 模板脚本，第 5 页
- FlexConfig 对象中的 CLI 命令，第 2 页

您可以使用变量来提供只有在运行时才知道的信息，或者每个设备都不同的信息。您只需键入处理变量，但必须使用**插入**菜单添加与策略对象或系统变量相关联的变量，或者是密钥的变量。有关变量的完整讨论，请参阅FlexConfig 变量，第 5 页。

- 要插入系统变量，请选择**插入** > **插入系统变量** > **变量名称**。有关这些变量的详细说明，请参阅FlexConfig 系统变量，第 11 页。

- 要插入策略对象变量，请选择**插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。然后，为变量命名（可以与关联的策略对象同名），选择要与该变量关联的对象，然后点击**保存**。有关这些类型的详细说明，请参阅FlexConfig 策略对象变量，第 10 页。有关过程的详细信息，请参阅向 FlexConfig 对象添加策略对象变量，第 25 页。
- 要插入密钥变量，请选择**插入** > **密钥**并定义变量名称和值。有关过程的详细信息，请参阅配置密钥，第 26 页。

注释

必须使用**插入**菜单来创建新的策略对象或系统变量。但是，对于该变量的后续使用，您必须键入该变量，包括 $。系统变量也是如此：第一次使用变量时，请从**插入**菜单中添加这些变量。然后，键入该变量以供后续使用。如果对系统变量多次使用**插入**菜单，系统变量将多次添加到变量列表中，FlexConfig 将无法验证，这意味着您无法保存更改。对于处理变量（与策略对象或系统变量不关联的变量），只需输入变量即可。如果要添加密钥，请始终使用**插入**菜单。密钥变量在变量列表中不显示。

步骤 5 选择部署频率和类型。

- **部署** - 将对象中的命令部署为**一次**还是**每次**。选择正确选项的唯一方法是测试部署结果。

  通过选择**每次**来开始操作。然后，在将对象附加到FlexConfig 策略后，部署配置。成功部署后，返回 FlexConfig 策略并预览其中一个已分配设备的配置，如预览 FlexConfig 策略，第 30 页中所述。如果标记为 `###CLI generated from managed features ###` 的部分包含清除或否定对象中命令的命令，且 `###Flex-config Appended CLI ###` 部分包含重新配置此功能的命令，您便可以知道**每次**是正确的选项。

  即使没有看到否定命令，也需对设备配置进行一些细微更改，然后再运行另一个部署。如果成功完成部署，则可以检查部署脚本（请参阅验证部署的配置，第 30 页）。如果您看到命令再次发出（即使它们已经配置）且没有出错，则可以保留**每次**选项。

  仅当系统在再次发出对象中的命令之前没有首先否定命令，或者部署导致出现特定于命令的错误时，才更改为**一次**。在某些情况下，系统不允许您发出已配置的命令，但这是例外情况。

  一些额外提示：

  - 如果 FlexConfig 对象指向系统托管对象，例如网络或 ACL 对象，请选择**每次**。否则，可能无法部署对象的更新。
  - 如果您在对象中执行的唯一操作是清除配置，请选择**一次**。然后，在下一次部署后从 FlexConfig 策略中删除此对象。

- **类型** - 选择以下一个选项：
  - **追加** -（默认值）。对象中的命令将放在从 防火墙管理中心 策略生成的配置的末尾。如果使用策略对象变量（指向从托管对象生成的对象），则必须使用追加。如果为其他策略生成的命令与对象中指定的指令重叠，则应选择此选项，以使您的命令不会被覆盖。这是最安全的选项。
  - **预置** - 对象中的命令放在从 防火墙管理中心 策略生成的配置的开始处。通常对清除或否定配置的命令使用预置。

步骤 6 （可选。）点击对象正文上方的 **验证** （ ） 以检查脚本的完整性。

点击**保存**时始终验证该对象。无法保存无效对象。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改。

向 FlexConfig 对象添加策略对象变量

可以向与其他类型的策略对象相关联的 FlexConfig 策略对象中插入变量。在将 FlexConfig 部署到某一设备后，这些变量将解析到相关联对象的名称或内容。

对于首次在 FlexConfig 对象中使用策略对象变量，可以使用以下程序。如果需要再次引用该对象，则请键入该变量（包括 $ 符号）。要了解如何使用这些变量，请参阅如何处理变量， 第 6 页。

开始之前

有关编辑 FlexConfig 对象的更多信息，请参阅 配置 FlexConfig 对象， 第 22 页。

过程

步骤 1 在编辑 FlexConfig 策略对象时，依次选择 **插入** > **插入策略对象** > **对象类型**，选择适当类型的对象。

步骤 2 输入变量的名称和说明（后者为可选项）。

该名称在 FlexConfig 对象的上下文中必须是唯一的。其中不能包含空格。允许使用跟与变量相关联的对象完全相同的名称。

步骤 3 选择要与变量相关联的对象，然后点击**添加**，以将其移至**选定对象**列表中。

只能使一个变量与一个对象相关联。

注释
对于文本对象，可以根据需要选择任何预定义对象。不过，很多此类对象没有默认值。必须更新这些对象，以直接或以覆盖方式，为将要向其部署 FlexConfig 对象的设备添加所需的值。尝试在不更新这些对象的情况下部署 FlexConfig，通常会导致部署错误。

步骤 4 点击**保存**。

该变量将显示在位于 FlexConfig 对象编辑器底部的“变量”列表中。

配置密钥

密钥是要屏蔽其内容的任何单字符串变量，如密码。系统为这些变量提供特殊处理，以帮助您防止敏感信息的散播。

密钥变量不会显示在 FlexConfig 对象中的“变量”列表中。

使用以下过程在 FlexConfig 对象中创建、插入以及以其他方式管理密钥变量。与其他类型的变量不同，您可以在每次需要插入给定的密钥变量时使用**插入**命令。在处理方面，这些变量的行为类似于单值文本对象变量；请参阅单值变量，第 6 页。

注释 在密钥变量中定义的任何数据都将对用户屏蔽，预览 FlexConfig 策略时除外。此外，如果导出 FlexConfig 策略，则会删除任何密钥变量的内容。导入策略时，需要手动编辑每个密钥变量以输入数据。

开始之前

有关编辑 FlexConfig 对象的更多信息，请参阅 配置 FlexConfig 对象，第 22 页。

过程

步骤 1 编辑 FlexConfig 策略对象时，请选择**插入** > **密钥**。

步骤 2 在 **插入密钥** 对话框中，执行以下任意操作：

- 要创建新密钥，请点击**添加密钥 (Add Secret Key)**，然后填写以下信息并点击**添加 (Add)**。
  - **密钥名称** - 变量的名称。此名称显示在 FlexConfig 对象中，以 @ 为前缀。
  - **密码**、**确认密码** - 密钥字符串，在键入时用星号进行隐蔽。
- 要在 FlexConfig 对象中插入一个密钥变量，请选中该变量对应的复选框。
- 要编辑密钥变量的值，请点击该变量的 **编辑** () 。进行更改并点击**添加 (Add)**。
- 要删除密钥变量，请点击该变量的 **删除** () 。

步骤 3 点击**保存**。

配置 FlexConfig 文本对象

将 FlexConfig 对象中的文本对象用作策略对象变量的目标。您可以使用变量来提供只有在运行时才知道的信息，或者每个设备都不同的信息。在部署过程中，指向文本对象的变量将替换为文本对象的内容。

文本对象可以包含自由格式的字符串，可以是关键字、接口名称、数字、IP 地址等等。内容取决于您在 FlexConfig 脚本中使用这些信息的方式。

在创建或编辑文本对象之前，请准确确定需要的内容。这包括您打算如何处理对象，这将有助于您在创建单字符串或多字符串对象之间做出决定。阅读以下主题：

- FlexConfig 变量，第 5 页
- 如何处理变量，第 6 页

过程

步骤 1 选择**对象** > **对象管理** > **FlexConfig** > **文本对象**。

步骤 2 执行以下操作之一：

- 点击**添加文本对象**以创建一个新对象。
- 点击 **编辑** (✎) 以编辑现有对象。您可以编辑预定义的文本对象，如果您打算使用预定义的 FlexConfig 对象，则需要这样做。

步骤 3 为对象输入**名称**和（可选）说明。

步骤 4 （仅新对象。）从下拉列表中选择**变量类型**：

- **单个** - 如果对象应包含单个文本字符串。
- **多个** - 如果对象应包含文本字符串列表。

保存对象后，则无法更改变量类型。

步骤 5 如果变量类型为**多个**，则使用向上和向下箭头指定**计数**。

在更改数字时，会在对象中添加或删除行。

步骤 6 向对象添加内容。

您可以在变量号旁边的文本框中点击并键入一个值，也可以为每个将被分配使用此文本对象的 FlexConfig 对象的设备设置设备覆盖。您也可以同时执行这两种方法，在这种情况下，在基本对象中配置的值在给定设备的覆盖不存在的情况下充当默认值。

在编辑预定义对象时，最好使用设备覆盖，这样，对于可能需要在不同 FlexConfig 策略中使用该对象的其他用户来说，系统默认值仍然存在。您所采取的方法取决于组织的要求。

提示
某些预定义对象需要多个值，其中每个值都有特定的用途。仔细阅读说明文本以确定对象中的预期值。在某些情况下，这些说明指定您必须使用覆盖而不是更改基本值。如果是 enableInspectProtocolList，您将无法进入其检测与 Snort 检查不兼容的协议。

如果决定使用覆盖，请执行以下操作。

a) 选中 **允许覆盖** 复选框。
b) 展开“覆盖”区域（如果需要），然后点击**添加 (Add)**。

如果设备已存在覆盖，请点击该覆盖的编辑以更改它。

c) 在“添加对象覆盖”对话框的 **目标** 卡上，选择要为其定义值的设备，然后点击 **添加** 将其移动到“选定设备”列表中。

d) 点击 **覆盖**，根据需要调整 **计数** ，然后在变量字段中点击并键入设备的值。

e) 点击**添加 (Add)**。

步骤 7 点击**保存**。

下一步做什么

- 如果活动策略引用您的对象，请部署配置更改；请参阅 部署配置更改。

配置 FlexConfig 策略

FlexConfig 策略包含 FlexConfig 对象的两个有序列表，一个预置列表和一个附加列表。有关对预置/附加的解释，请参阅配置 FlexConfig 对象 ， 第 22 页。

FlexConfig 策略是可以分配给多个设备的共享策略。

过程

步骤 1 选择**设备** > **FlexConfig**。

步骤 2 执行以下操作之一：

- 点击**新建策略**创建新的 FlexConfig 策略。系统将提示您输入名称。（可选）选择“可用设备”列表中的设备，然后点击**添加到策略**以分配设备。点击**保存**。
- 点击 **编辑** (✎) 以编辑现有策略。可以通过在编辑模式下点击名称或说明来对其进行更改。
- 点击 **复制** (⧉) 以创建具有相同内容的新策略。系统将提示您输入名称。系统不会为副本保留设备分配。
- 点击删除可删除不再需要的策略。

步骤 3 从**可用 FlexConfig** 列表中选择策略所需的 FlexConfig 对象，然后点击 > 将它们添加到策略中。

对象将根据 FlexConfig 对象中指定的部署类型自动添加到预置或附加列表中。

要删除所选对象，请点击对象旁边的 **删除** (🗑) 。

步骤 4 对于每个所选对象，点击该对象旁边 **视图**（🔍） 可以标识该对象中使用的变量。

除了系统变量（从 SYS 开始），您需要确保与变量关联的对象不为空。在它们之间没有任何内容的空白或方括号 [] 表示空对象。在部署策略之前，您需要编辑这些对象。

注释

如果使用对象覆盖，则这些值不会显示在此视图中。因此，空的默认值不一定表示您没有使用所需的值更新对象。预览配置将显示变量是否对给定设备正确解析。请参阅预览 FlexConfig 策略，第 30 页。

步骤 5 点击**保存**。

下一步做什么

- 设置策略的目标设备；请参阅为 FlexConfig 策略设置目标设备，第 29 页。
- 部署配置更改；请参阅 部署配置更改。

为 FlexConfig 策略设置目标设备

创建FlexConfig策略时，可以选择使用该策略的设备。您可以随后更改策略的设备分配，如下所述。

注释 通常，当您从设备取消分配策略时，系统会在下次部署时自动删除关联的配置。但是，由于FlexConfig对象是用于部署自定义命令的脚本，因此只从设备取消分配 FlexConfig 策略不会删除由 FlexConfig 对象配置的命令。如果您打算从设备配置中删除FlexConfig生成的命令，请参阅删除使用 FlexConfig 配置的功能，第 32 页。

过程

步骤 1 选择**设备** > **FlexConfig**并编辑 FlexConfig 策略。

步骤 2 点击**策略分配**。

步骤 3 在 **目标设备** 上，建立目标列表：

- 添加 - 选择一个或多个**可用设备**，然后点击**添加到策略**或拖放到**所选设备**列表。可以将策略分配给设备、高可用性对和集群设备。
- 删除 - 点击单个设备旁边的 **删除** ( )，或选择多个设备，点击右键，然后选择 **删除选择**。

步骤 4 点击**确定**，保存选择。

步骤 5 点击**保存**以保存 FlexConfig 策略。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

预览 FlexConfig 策略

预览 FlexConfig 策略可以查看 FlexConfig 对象如何转换为 CLI 命令。预览将显示从 FlexConfig 对象中使用的脚本和变量为选定设备生成的命令。这些变量基于设备的配置进行解析，因此您可以清楚地了解将部署什么。

使用预览可以查找 FlexConfig 对象中存在的潜在问题。更正对象，直到预览显示预期结果为止。

您必须单独预览每个设备的配置，因为这些变量可以基于设备配置进行不同的解析。

过程

步骤 1 选择**设备** > **FlexConfig**并编辑 FlexConfig 策略。

步骤 2 如果有任何待保存的更改，请点击**保存**。

预览仅显示最近保存的策略版本中的那些 FlexConfig 对象的结果。必须保存策略才能查看新添加对象的预览。

步骤 3 点击**预览配置**。

步骤 4 从**选择设备**下拉列表中选择设备。

系统从设备和配置的策略中检索信息，并确定将在下次部署到设备时生成哪些 CLI 命令。您可以选择输出并使用 Ctrl+C 将其复制到剪贴板，您可以再次将其粘贴到文本文件中以进行进一步分析。

预览包括以下部分：

- Flex-config 预置 CLI - 这些是由 FlexConfigs 生成、的命令，这些命令。
- 从托管功能生成的 CLI - 这些是为在 防火墙管理中心中配置的策略生成的命令。自上次成功部署到设备后，系统将为新的或更改的策略生成命令。这些命令并不代表实现分配的策略所需的所有命令。本部分中的任何命令都不是从 FlexConfig 对象中生成。
- Flex-config 附加 CLI - 这些是由 FlexConfigs 生成、将被附加到配置的命令。

步骤 5 点击**关闭**以关闭预览对话框。

验证部署的配置

在将 FlexConfig 策略部署到设备后，请验证部署是否成功，以及得到的配置是否是您所预期的。此外，请验证设备是否按预期工作。

过程

步骤 1 要验证部署是否成功，请执行以下操作：

a) 点击菜单栏中的 **通知** ，即 **部署** 和 **系统**之间的未命名。

该图标看起来像以下图标中的一个，如果有错误，它可能会包括数字：

- **指示无警告** - 指示系统上不存在任何警告或错误。
- 指示 **一个或多个警告** - 指示系统上存在一个或多个警告而没有错误。
- **指示一个或多个错误** - 指示系统上存在一个或多个错误和任意数量的警告。

b) 在 **部署**上，验证部署是否成功。

c) 要查看更多详细信息，特别是对于失败的部署，请点击**显示历史记录**。

d) 在左侧列的作业列表中选择部署作业。

作业以倒序顺序列出，最近的作业位于列表顶部。

e) 在右侧列中点击设备的 **脚本** 列中的下载。

部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示您通过FlexConfig发送的命令错误的消息。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释
为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示 防火墙管理中心 发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为0。 不会将安全级别用于任何操作。与FlexConfig相关的消息在该脚本的“CLI 应用”部分中。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

步骤 2 验证部署的配置是否包含预期的命令。

您可以通过与设备的管理 IP 地址建立 SSH 连接来完成此项工作。使用 **show running-config** 命令查看配置。

或者，在 Cisco Secure Firewall Management Center中使用 CLI 工具。

a) 选择 **系统** (⚙) > **健康** > **监控器** 并点击设备名称。

您可能需要点击状态表中**计数**列中的打开/关闭箭头来查看任何设备。

b) 点击**高级故障排除 (Advanced Troubleshooting)**。

c) 点击**威胁防御 CLI (Threat Defense CLI)**。

d) 选择 **show** 作为命令，然后键入 **running-config** 作为参数。

e) 点击**执行 (Execute)**

正在运行的配置显示在文本框中。您可以选择配置并按Ctrl+C，然后将其粘贴到文本文件中以供以后分析。

步骤 3 验证设备是否按预期工作。

使用与此功能相关的**show**命令可查看详细信息和统计信息。例如，如果您启用了其他协议检查，则**show service-policy**命令会提供此信息。要使用的确切命令与功能相关，并且应在您用来了解如何配置此功能的 ASA 配置指南和命令参考中提及。

如果显示统计信息的命令指示数字未发生更改（例如，命中次数、连接计数等），则配置可能有效，但没有意义。如果您知道流量正在通过应在统计中显示的设备，则查找配置中缺少的内容。例如，NAT 或访问规则可能需要丢弃或更改流量，才能对其应用此功能。

您可以从 SSH 会话或通过 防火墙管理中心 CLI 工具使用 **show** 命令。

但是，如果您需要使用的 **show** 命令无法直接从 CLI 中获得，则需要与设备建立 SSH 连接才能使用这些命令。在 CLI 中，输入以下命令序列以在诊断 CLI 中进入特权 EXEC 模式。您可以在此处输入这些不受支持的 **show** 命令。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

删除使用 FlexConfig 配置的功能

如果您决定需要删除使用 FlexConfig 配置的一组配置命令，则可能需要手动删除该配置。从设备取消分配 FlexConfig 策略可能不会删除所有配置。

要手动删除该配置，请创建新的 FlexConfig 对象以清除或取消配置命令。

开始之前

要确定是否需要手动删除对象生成的部分或全部配置，请执行以下操作：

1. 检查配置预览，如预览 FlexConfig 策略，第 30 页中所述。如果 `###CLI generated from managed features ###` 部分包含清除或否定命令以删除 FlexConfig 对象中的所有命令，您只需从 FlexConfig 策略中删除此对象，保存并重新部署。
2. 从 FlexConfig 策略中删除对象，保存更改，然后再次预览配置。如果 `###CLI generated from managed features ###` 部分仍不包含所需的清除或否定命令，则必须按照此程序手动删除配置。

过程

步骤 1 选择 **对象** > **对象管理** 并创建用于清除或否定配置命令的 FlexConfig 对象。

如果某个功能具有可以删除所有配置设置的 **clear** 命令，则使用此命令。例如，预定义的 ISIS_Unconfigure_All 对象就包含一个可以删除所有与 ISIS 相关的配置命令的命令：

```
clear configure router isis
```

如果此功能没有 **clear** 命令，则需要使用每个要删除的命令的 **no** 形式。例如，预定义的 Sysopt_basic_negate 对象将删除通过预定义的 Sysopt_basic 对象配置的命令。

```
no sysopt traffic detailed-statistics
no sysopt connection timewait
```

通常，您将配置一个 FlexConfig 对象，以预置的一次性部署对象形式删除配置。

步骤 2 选择 **设备** > **FlexConfig** 并创建新的 FlexConfig 策略或编辑现有策略。

如果要保留部署配置命令的 FlexConfig 策略，请创建一个专门用于取消命令的新策略，并将设备分配给该策略。然后，将新的 FlexConfig 对象添加到该策略。

如果要从所有设备中完全删除 FlexConfig 配置对象，只需从现有 FlexConfig 策略中删除这些命令，并将它们替换为取消该配置的对象。

步骤 3 点击**保存**以保存 FlexConfig 策略。

步骤 4 点击**预览配置**并确认清除和取消命令会正确生成。

步骤 5 选择菜单栏中的 **部署** > **部署** ，选择该设备，然后点击 **部署**。

等待部署完成。

步骤 6 验证是否已删除命令。

查看设备上正在运行的配置，以确认这些命令已被删除。有关详细信息，请参阅验证部署的配置，第 30 页。

步骤 7 编辑 FlexConfig 策略时，点击**策略分配**并删除该设备。（可选）从策略中删除 FlexConfig 对象。

假定 FlexConfig 策略仅删除不需要的配置命令，则在删除完成后无需保留分配给该设备的策略。

但是，如果 FlexConfig 策略保留了您仍希望在设备上配置的选项，请从策略中删除取消对象。不再需要保留它们。

从 FlexConfig 转换为管理功能

每个软件版本都会向产品添加托管功能，也就是您通过在 FlexConfig 外部控制的策略直接配置的功能。这可能会弃用您当前使用的 FlexConfig 命令；您的配置不会自动转换。在升级后，您无法使用新近弃用的命令来分配或创建 FlexConfig 对象。在升级软件后，检查 FlexConfig 策略和对象。

在使用 FlexConfig 配置的功能开始受支持作为托管功能时，您必须从使用 FlexConfig 转换为使用托管功能。在大多数情况下，您现有的 FlexConfig 配置会在升级后继续工作，您仍然可以进行部署。但在某些情况下，使用已弃用的命令可能会导致部署问题。不支持同时在 GUI 和 FlexConfig 中配置功能。

注释 如果迁移工具支持您要迁移的功能配置，请使用迁移工具来代替此程序。

过程

步骤 1 删除 FlexConfig，如删除使用 FlexConfig 配置的功能，第 32 页中所述。

步骤 2 配置最新支持的托管功能中的设置。

版本说明包含了该版本的新功能列表。

FlexConfig 示例

以下是使用 FlexConfig 的一些示例。

如何配置精确时间协议 (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 设备配置为透明时钟。 设备不会将其时钟与 PTP 时钟同步。 设备将使用 PTP 默认配置文件，如 PTP 时钟上所定义。

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，可以配置多个 PTP 域，然后将每个非 PTP 设备配置为特定域使用 PTP 时钟。

开始之前

确定设备应使用的 PTP 时钟上配置的域编号。此示例假定 PTP 域编号为 10。另外，确定系统可通过哪些接口到达域中的 PTP 时钟。

以下是 PTP 配置准则：

- 此功能在思科 ISA 3000 设备上不可用。
- 思科 PTP 仅支持组播 PTP 消息。
- PTP 仅可用于 IPv4 网络，不可用于 IPv6 网络。
- 物理以太网数据接口支持 PTP 配置，无论是独立式还是网桥组成员。管理接口、子接口、Etherchannel 接口、桥接虚拟接口 (BVI) 或任何其他虚拟接口均不支持此版本。

- 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。PTP 流量由 UDP 目标端口 319 和 320 以及目标 IP 地址 224.0.1.129 标识，因此允许此流量的任何访问控制规则均应有效。
- 在路由防火墙模式下，必须为 PTP 组播组启用组播路由：此外，如果启用 PTP 的接口不在网桥组中，则必须将该接口配置为加入 IGMP 组播组 224.0.1.129。如果物理接口是网桥组成员，则不要将其配置为加入 IGMP 组播组。

过程

步骤 1 （仅路由模式。）启用组播路由，并为接口配置 IGMP 组。

在路由模式下，必须启用组播路由。此外，对于独立物理接口（即非网桥组成员），还必须配置接口以加入 224.0.1.129 IGMP 组。您无法将网桥组成员配置为加入 IGMP 组，但网桥组成员上的 PTP 配置将在没有 IGMP 加入的情况下起效。

对要配置 PTP 的每台设备执行此程序。

注释
记下每个设备上每个面向 PTP 时钟的接口的硬件名称，例如，GigabitEthernet1/1。

a) 选择 **设备** > **设备管理**，然后编辑设备。
b) 点击**路由 (Routing)**。
c) 选择 **组播路由** > **IGMP**。
d) 选中**启用组播路由**复选框。
e) 点击**加入组 (Join Group)**。
f) 点击 **添加**，，然后在 **添加 IGMP 加入组参数** 对话框中，配置以下选项，然后点击 **确定**。

- **接口 (Interface)** - 选择面向 PTP 时钟的独立接口。
- **加入组 (Join Group)** - 点击 **+** 以添加新的网络对象。使用地址 224.0.1.129 来创建主机对象。在配置其他接口时，可直接选择此对象。（请参阅创建网络对象。）

对设备上每个面向 PTP 时钟的独立接口重复此步骤。

g) 点击“路由”页面上的**保存**。

步骤 2 创建 FlexConfig 对象，以便全局启用 PTP 以及在接口上启用 PTP。

以下程序假定您正在配置的每台设备上的面向 PTP 时钟的接口均相同。如果在不同的设备上使用了不同的接口，则您需要为每个不同的组合创建单独的对象。例如，如果您在设备 A 和 B 上使用 GigabitEthernet1/1，在设备 C 和 D 上使用 GigabitEthernet1/2，在设备 E 和 F 上同时使用 GigabitEthernet1/1 和 1/2，则您需要 3 个单独的 FlexConfig 对象，随后还需要 3 个单独的 FlexConfig 策略（将在下一步中进行说明）。

a) 选择**对象** > **对象管理** > **FlexConfig** > **FlexConfig 对象**。
b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Enable_PTP。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。
- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。这样可确保在这些命令之前配置对接口配置所做的任何其他更改。
- **对象正文 (Object body)** - 在对象正文中，键入在每个面向 PTP 时钟的接口上全局配置 PTP 所需的命令。例如，PTP 域 10 的全局配置和 GigabitEthernet1/1 上的接口配置所需的命令如下：

```
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

此对象正文应如下所示：

步骤 3 创建 FlexConfig 策略并将其分配给设备。

如果为面向 PTP 时钟的接口的不同组合创建了多个 FlexConfig 对象，则需要为每个对象创建单独的 FlexConfig 策略，并根据需要配置的接口将这些策略分配给正确的设备。对每组设备重复以下程序。

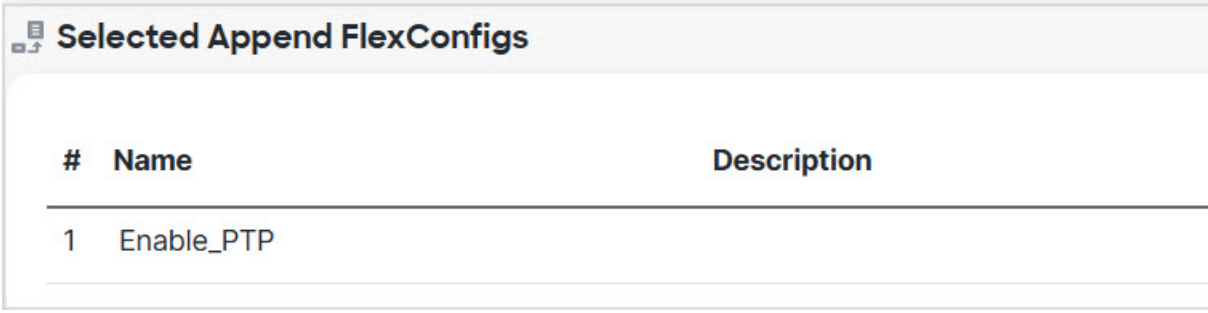
a) 选择**设备** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择 PTP FlexConfig 对象，然后点击 > 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从 PTP FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于 PTP 命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
ptp mode e2etransparent
ptp domain 10
interface gigabitethernet1/1
 ptp enable
```

步骤 4 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 30 页。

步骤 5 在每台设备上验证 PTP 配置。

从 SSH 或控制台会话到每台设备，验证 PTP 设置：

```
> show ptp clock
 PTP CLOCK INFO
  PTP Device Type: End to End Transparent Clock
  Operation mode: One Step
  Clock Identity: 34:62:88:FF:FE:1:73:81
  Clock Domain: 10
  Number of PTP ports: 4
> show ptp port
 PTP PORT DATASET: GigabitEthernet1/1
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 1
  PTP version: 2
  Port state: Enabled

 PTP PORT DATASET: GigabitEthernet1/2
  Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
  Port identity: Port Number: 2
  PTP version: 2
  Port state: Disabled
```

```
PTP PORT DATASET: GigabitEthernet1/3
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 3
 PTP version: 2
 Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
 Port identity: Clock Identity: 34:62:88:FF:FE:1:73:81
 Port identity: Port Number: 4
 PTP version: 2
 Port state: Disabled
```

如何对电源故障配置自动硬件旁路 (ISA 3000)

您可以启用硬件旁路，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接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。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）支持硬件旁路。

启用硬件旁路时，流量将在这些接口对之间的第 1 层传递。 CLI 将显示接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

在 CLI 控制台或 SSH 会话中，使用 **show hardware-bypass** 命令以监控运行状态。

开始之前

要使用硬件旁路：

- 必须将接口对放置在同一网桥组内。
- 必须将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。

我们建议您通过使用附加到分配给设备的访问控制策略的威胁防御服务策略，来全局禁用 TCP 序列号随机化。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。硬件旁路激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，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关闭。

过程

步骤 1 创建 FlexConfig 对象以启用自动旁路。

a) 选择**对象** > **对象管理** > **FlexConfig** > **FlexConfig 对象**。

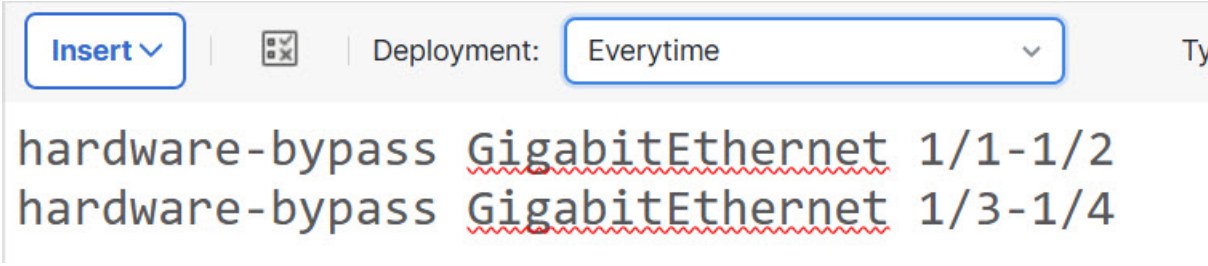
b) 点击**添加 FlexConfig 对象**，配置以下属性，然后点击**保存**。

- **Name** - 对象名称。例如，Enable_HW-Bypass。
- **部署 (Deployment)** - 选择**每次 (Everytime)**。您想在每个部署中发送此配置，以确保其保持配置状态。

- **类型 (Type)** - 保留默认值**附加 (Append)**。这些命令会在直接支持的功能的命令之后被发送到设备。
- **对象正文 (Object body)** - 在对象正文中，键入启用自动硬件旁路所需的命令。例如，两个可能的接口对所需的命令：

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

此对象正文应如下所示：



步骤 2 创建 FlexConfig 策略并将其分配给设备。

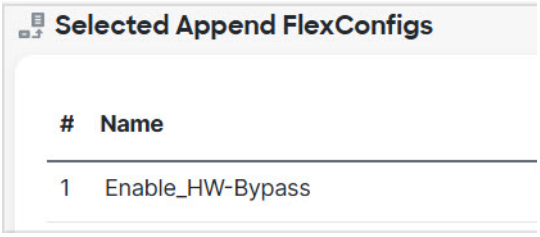
a) 选择**设备** > **FlexConfig**。

b) 点击**新建策略 (New Policy)**，或者如果现有 FlexConfig 策略应分配给（或已分配给）目标设备，则只需编辑该策略。

在创建新的策略时，请在为策略命名的对话框中将目标设备分配给策略。

c) 在目录的 **User Defined** 文件夹中选择硬件旁路 FlexConfig 对象，然后点击 > 将其添加到策略中。

此对象应被添加到**所选附加 Flexconfig (Selected Appended FlexConfigs)** 列表中。



d) 点击**保存**。

e) 如果尚未将所有目标设备分配给策略，请点击“保存”下面的**策略分配**链接并立即进行分配。

f) 点击**预览配置 (Preview Config)**，然后在预览对话框中选择一个已分配的设备。

系统会生成将被发送到设备的配置 CLI 预览。验证从硬件旁路 FlexConfig 对象生成的命令看起来是否正确。这些将在预览结束时显示。请注意，您还会看到通过对托管功能所做的其他更改而生成的命令。对于硬件旁路命令，您应该会看到类似如下的内容：

```
###Flex-config Appended CLI ###
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

步骤 3 部署更改。

由于您已将 FlexConfig 策略分配给设备，因此您始终会收到部署警告，以提醒您有关 FlexConfig 的使用。点击**继续 (Proceed)** 以继续部署。

在部署完成后，您可以检查部署历史记录并查看部署脚本。如果部署失败，这一点尤为重要。请参阅验证部署的配置，第 30 页。

下一步做什么

如果您要手动调用硬件旁路或手动将其关闭，则需要创建两个 FlexConfig 对象：

- 一个是手动启动绕行，其中包含以下一个或两个命令，具体取决于您是否要为两个对调用绕行：

```
hardware-bypass manual GigabitEthernet 1/1-1/2
hardware-bypass manual GigabitEthernet 1/3-1/4
```

- 另一个是手动关闭旁路，其中包含以下一个或两个命令：

```
no hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/3-1/4
```

然后，您需要将一个或另一个对象添加到 FlexConfig 策略中并部署更改，以打开或关闭绕行。您还需要在部署后立即从 FlexConfig 策略中删除该对象。如果您手动调用绕行，则需要重复该过程以再次将其关闭。因此，使用此手动方法需要经常仔细编辑 FlexConfig 策略和其他部署。

迁移 FlexConfig 策略

注意 有关迁移 FlexConfig 策略的本节仅适用于迁移 ECMP、VXLAN 和 EIGRP 策略。

使用 FlexConfig 对象和早期版本 防火墙管理中心中的策略配置了 ECMP、VXLAN 和 EIGRP 策略。您现在可以直接在管理中心UI中配置这些策略。从早期版本升级管理中心时，系统会保留FlexConfig配置。但是，要从 UI 管理策略，您必须在相应的**设备（编辑）(Device [Edit])** > **路由 (Routing)** 页面重新执行配置，并从 FlexConfig 中删除配置。要在 UI 中自动创建策略，防火墙管理中心 提供了将策略从FlexConfig迁移到UI的选项。但是，它不会从FlexConfig中删除已迁移的策略。有关迁移后的程序，请参阅步骤 7，第 41 页。

开始之前

- 确保部署的FlexConfig策略是最新的，而不是过时的。只有当策略在至少1台设备上为最新时，迁移选项才可用。对于具有过期策略的设备不会进行迁移。
- 如果在 FlexConfig 和管理中心中配置了策略：
  - 如果已在**设备（编辑）(Device [Edit])** > **路由 (Routing)** 中配置了策略，则不会发起迁移。

- 在部署期间，管理中心会显示错误消息。示例 EIGRP 迁移错误消息 - *EIGRP 通过 FlexConfig 对象进行配置，也可在设备的“设备列表”(Device Listing) -> “路由 EIGRP”(Routing EIGRP)* 下进行配置。在路由 *EIGRP* 或 *FlexConfig* 中维护 *EIGRP* 配置。

- 如果策略中使用的网络对象存在于管理中心，则在迁移期间，它们会被重用。在迁移过程中，当与 IP 配置匹配的网络对象不可用时，会创建一个新的网络对象，即 *bb* 附加时间戳和整数，例如 ***bb_<timestamp>_<integer>*** 。对于多个此类网络对象，名称中的整数变量将递增一。

过程

步骤 1 选择 **设备** > **FlexConfig**，点击要迁移的 FlexConfig 策略旁边的 **编辑** (✎)。

步骤 2 点击**迁移配置 (Migrate Config)**。

注释
迁移开始后，**迁移配置 (Migrate Config)** 和 FlexConfig **编辑 (Edit)** 选项都将不可用。

在以下情况下，**迁移配置 (Migrate Config)** 选项不可用：

- 没有要迁移的适用 FlexConfig CLI。
- FlexConfig 策略没有与任何 FlexConfig 对象关联。
- 没有设备与 FlexConfig 策略关联。

步骤 3 在**迁移 Flex 配置**对话框中，选择要向其迁移配置的设备，然后点击**确定**。

迁移进度会显示为任务通知。迁移完成后，点击查看详细信息 *(View Details)* 链接并下载迁移报告（PDF 格式）。

步骤 4 要查看策略更改，请选择 **系统** (⚙) > **监控** > **审核** 并点击 *FlexConfig* 迁移消息。

步骤 5 要查看 FlexConfig 迁移报告，请选择 **系统** (⚙) > **监控** > **审核** 并点击 *FlexConfig* 迁移消息。要查看完整的迁移报告，请点击**报告 (Report)** 图标。

步骤 6 在对应的**设备**（**编辑**）**(Device [Edit])** > **路由 (Routing)** 页面中验证已迁移的配置设置。

步骤 7 要从 FlexConfig 中删除设备的特定策略配置，请在管理中心执行以下操作：

a) 确定设备的已迁移 FlexConfig 策略。
b) 使用复制选项并创建 FlexConfig 策略的副本。
c) 从复制的 FlexConfig 策略中删除对应的 CLI 对象。
d) 将设备关联到复制的 FlexConfig 策略。

步骤 8 保存并部署配置。

FlexConfig 的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
Firepower 1000/2100 和 Firepower 4100/9300 的数据平面故障后恢复速度更快。	7.4.1	7.4.1	如果数据平面进程崩溃，系统现在仅重新加载数据平面进程，而不是重新启动设备。随着数据平面进程重新加载，Snort 和其他几个进程也会重新加载。 但是，如果数据平面进程在启动期间崩溃，设备将遵循正常的重新加载/重新启动顺序，这有助于避免发生重新加载过程循环。 默认情况下，新设备和升级设备均启用此功能。 新增/修改的CLI 命令： **data-plane quick-reload**、 **no data-plane quick-reload**、 **show data-plane quick-reload status** 支持的平台：Firepower 1000/2100、Firepower 4100/9300 平台限制：不支持多实例模式。 请参阅： Cisco Secure Firewall Threat Defense 命令参考 和 Cisco Secure Firewall ASA 系列命令参考。
迁移工具支持。	7.3.0	任意	引入了对将 Flex 配置的 ECMP、VXLAN 和 EIGRP 策略迁移到管理中心的支持。 新增/修改的屏幕：**设备 (Devices)** > **FlexConfig** > **迁移 FlexConfig (Migrate FlexConfig)**
删除 FlexConfig 中的 BFD 配置。	7.3.0	任意	引入了对直接在管理中心用户界面中配置 BFD 策略的支持。因此，用于配置 EIGRP 策略的 FlexConfig 支持已被删除。
删除优先级队列。	7.2.5	7.2.5	删除了在威胁防御中配置优先级队列的支持。
删除 FlexConfig 中的 EIGRP 配置。	7.2.0	任意	引入了对直接在管理中心用户界面中配置 EIGRP 的支持。因此，用于配置 EIGRP 策略的 FlexConfig 支持已被删除。
删除 PBR 配置。	7.1.0	7.1.0	支持直接在 FMC 用户界面上配置 PBR。因此，为 FTD 7.1 及更高版本配置 PBR 的 FlexConfig 支持已被删除。 新增/修改的命令：**policy-route route-map***routemap-object-name*。
在 FlexConfig 中删除 ECMP 区域创建支持。	7.1.0	任意	引入了对直接在 FMC 用户界面中配置 ECMP 区域的支持。因此，用于配置 ECMP 区域的 FlexConfig 支持已被删除。

功能	防火墙管理中心最低版本	最低版本	详细信息
适用于 ISA 3000 设备的精确时间协议 (PTP) 配置。	6.5.0	任意	可以使用 FlexConfig 在 ISA 3000设备上配置精确时间协议 (PTP)。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。该协议专为工业、网络测量和控制系统而设计。 现在，我们允许在 FlexConfig 对象中包含 **ptp**（接口模式）命令和全局命令 **ptp mode e2etransparent** 和 **ptp domain** 新增/修改的命令：**show ptp**。
弃用的 FlexConfig 对象。	6.3.0	任意	在以前的版本中使用 FlexConfig 配置的几个功能如今已在 FMC 中直接支持。如果正在使用这些 FlexConfig 对象，您需要将其删除，然后将配置转换为使用新对象。以下是已弃用的 FlexConfig 对象和文本对象。 • **Default_DNS_Configure**，包括 defaultDNSNameServerList 和 defaultDNSParameters 文本对象。现在，请使用平台设置策略为数据接口配置 DNS。 • **TCP_Embryonic_Conn_Limit**，以及 tcp_conn_misc 和 tcp_conn_limit 文本对象。在FTD 服务策略中配置这些功能，您可以在分配给设备的访问控制策略的“高级”(Advanced) 选项卡上找到该策略。 • **TCP_Embryonic_Conn_Timeout**，以及 tcp_conn_misc 和 tcp_conn_timeout 文本对象。在 FTD 服务策略中配置这些功能。
FlexConfig 更新。	6.2.1	任意	根据政府认证要求，密码、系统提供的共享密钥或用户定义的FlexConfig 对象中的所有敏感信息都应使用密钥变量来加以屏蔽。将FTD 更新为版本 6.2.1+ 后，FlexConfig 对象中的所有敏感信息都会被转换为密钥变量格式。 此外，还添加了以下新的 FlexConfig 模板： • **Default_DNS_Configure** 模板让您能够使用默认 DNS 组，以便用于解析通过数据接口解析名称的命令或功能的主机名。 • **TCP 初期连接限制和超时配置**模板让您能够配置初期连接限制/超时 CLI，以防止 SYN 泛洪 DoSA攻击。 • **启用威胁检测配置和清除**模板让您能为 TCP 拦截拦截的攻击配置威胁检测统计信息。 • **IPV6 路由器报头检测**模板让您能配置 IPV6 检测报头，以便选择性地允许/阻止某些不同类型的报头（例如，允许RH类型2、移动）。 • **DHCPv6 前缀授权**模板让您能为 IPv6 前缀授权配置一个外部（PD 客户端）和一个内部接口（被授权前缀的接收者）。

功能	防火墙管理中心最低版本	最低版本	详细信息
FlexConfig。	6.2.0	任意	FlexConfig 功能让您能使用 FMC 将基于 ASA CLI 的功能部署到 FTD 设备。此功能允许您启用 FTD 设备上当前不可用的一些最具价值的 ASA 功能。此功能被结构化为在策略中协同工作的模板和对象。思科 TAC 正式支持默认模板。 新增/修改的屏幕： • **设备** > **FlexConfig** • **对象 (Objects)** > **对象管理 (Object Management)** > **FlexConfig** > **FlexConfig 对象 (FlexConfig Objects)** • **对象 (Objects)** > **对象管理 (Object Management)** > **FlexConfig** > **文本对象 (Text Object)**

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。