高级配置

某些设备功能可使用 ASA 配置命令进行配置。虽然 防火墙设备管理器 可以配置很多基于命令的功能，但它并非支持所有功能。如果需要使用 防火墙设备管理器本不支持的一些 ASA 功能，可以使用 Smart CLI 或 FlexConfig 手动配置这些功能。

以下主题详细说明这种类型的高级配置。

关于 Smart CLI 和 FlexConfig

Firewall Threat Defense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 Firewall Threat Defense 配置命令。

您可以借助以下方法使用 CLI 配置功能：

- **Smart CLI** -（首选方法。）Smart CLI 模板为用于特定功能的预定义模板，提供相应功能所需的所有命令，您只需选择变量值即可。系统会验证您的选择，以促进您正确配置具体功能。如果您所需的功能有对应的 Smart CLI 模板，则必须使用此方法。
- **FlexConfig** - FlexConfig 策略是 FlexConfig 对象的集合。FlexConfig 对象的形式比 Smart CLI 模板更自由，且系统不执行 CLI、变量或数据验证。您必须了解 ASA 配置命令，并按照 ASA 配置指南创建有效的命令序列。

Smart CLI 和 FlexConfig 的意义在于允许您配置不直接通过 防火墙设备管理器 策略和设置支持的功能。

注意 思科强烈声明，只建议具有较强 ASA 背景且自承风险的高级用户使用 Smart CLI 和 FlexConfig。您可以配置不受禁止的任何命令。通过 Smart CLI 和 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 Smart CLI 和 FlexConfig 对象的支持。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 Firewall Threat Defense功能的互通性。Smart CLI 和 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 防火墙设备管理器 支持。如有疑问，请勿使用 Smart CLI 或 FlexConfig。

以下主题更详细地解释这些功能。

Smart CLI 和 FlexConfig 的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 迁移至 Firewall Threat Defense，并且存在您正在使用（且需要继续使用）的 防火墙设备管理器 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，并创建实现功能的 FlexConfig 对象。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 Firewall Threat Defense ，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。

尝试重新创建ASA配置前，请先确定是否可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 Firewall Threat Defense之间不存在一对一重叠关系。请勿尝试在 Firewall Threat Defense 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。

Smart CLI 和 FlexConfig 对象中的 CLI 命令

Firewall Threat Defense 使用 ASA 配置命令配置某些功能。虽然并非所有 ASA 功能都与 Firewall Threat Defense兼容，但有一些功能可以在 Firewall Threat Defense 上使用，但不能在 防火墙设备管理器 策略中进行配置。您可以使用 Smart CLI 和 FlexConfig 对象指定配置这些功能所需的 CLI。

如果决定使用 Smart CLI 或 FlexConfig 手动配置功能，则需负责根据正确语法了解和执行这些命令。FlexConfig 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：http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/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：http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

以下主题介绍了有关配置命令的更多信息。

软件升级如何影响 FlexConfig 策略

每个新版本的 Firewall Threat Defense 软件都添加了对配置 Firewall Threat Defense中功能的支持。有时，这些新功能可能与您先前已使用 FlexConfig 配置的功能重叠。

升级后，您需要检查 FlexConfig 策略和对象。如果任何策略和对象包含因 防火墙设备管理器 或 Smart CLI 中添加的支持而被禁用的命令，则对象列表中的图标和相关消息会指出这一问题。请抽出时间重新进行配置。参考禁用命令列表，以帮助确定现在应在何处配置这些命令。

系统不会阻止您部署更改，尽管连接到 FlexConfig 策略的 FlexConfig 对象包含新禁用的命令。但是，您将无法创建新的 Smart CLI 对象，直到解决 FlexConfig 策略中提及的所有问题。

从 FlexConfig 策略中删除有问题的对象即可，因为限制仅适用于您主动部署到设备配置的对象。因此，您可以删除这些对象，创建相应的 Smart CLI 或集成 防火墙设备管理器 配置时再使用这些对象作参考。新配置达到要求后，删除对象即可。如果删除的对象包含一些未禁用的元素，您可以编辑这些对象以删除不受支持的命令，然后将对象重新连接到 FlexConfig 策略。

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 Firewall Threat Defense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 Firewall Threat Defense 配置有着显著的差异。许多 Firewall Threat Defense 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 Firewall Threat Defense 配置之间创建一对一的对应关系。

要查看此信息，请在 防火墙设备管理器 中打开 CLI 控制台，或与设备管理接口建立 SSH 连接，然后发出以下命令：

- **show version system** 并查找思科自适应安全设备软件版本号。
- **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。

禁止的 CLI 命令

Smart CLI 和 FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 防火墙设备管理器在 Firewall Threat Defense 设备上配置的功能。

因此，您无法配置在 防火墙设备管理器中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。该列表包含许多进入配置模式的父命令。禁止父命令包括禁止子命令。还包括命令的**no**版本及其相关的 **clear** 命令。

FlexConfig 对象编辑器可防止将这些命令纳入对象中。此列表不适用于 Smart CLI 模板，因为这些模板仅包含可有效配置的命令。

禁止的 CLI 命令	备注
aaa	使用**对象** > **身份源**。
aaa-server	使用**对象** > **身份源**。
access-list	部分阻止。 • 可以创建 **ethertype** 访问列表。 • 不能创建 **extended** 和 **standard** 访问列表。使用 Smart CLI 扩展访问列表或标准访问列表对象创建这些 ACL。然后，可以在按对象名称引用 ACL 且支持 FlexConfig 的命令中使用，例如带扩展 ACL 的 **match access-list** 用于服务策略流量类别。 • 无法创建 **advanced** 访问列表，系统将该访问列表与 **access-group** 命令一起使用。请使用**策略** > **访问控制**来配置访问规则。 • 不能创建 **webtype** 访问列表。
anyconnect-custom-data	使用**设备** > **远程访问 VPN**来配置 Secure Client。
asdm	此功能不适用于 Firewall Threat Defense 系统。
as-path	创建 Smart CLI AS 路径对象，并将其用于 Smart CLI BGP 对象，以配置自治系统路径过滤器。
attribute	—
auth-prompt	此功能不适用于 Firewall Threat Defense 系统。
boot	—
call-home	—
captive-portal	使用**策略** > **身份**配置用于主动身份验证的强制网络门户。
clear	—
client-update	—
clock	使用**设备** > **系统设置** > **NTP** 来配置系统时间。
cluster	—

禁止的 **CLI** 命令	备注
command-alias	—
community-list	创建 Smart CLI 扩展社区列表或标准社区列表对象，并将其用于 Smart CLI BGP 对象，以配置社区列表过滤器。
compression	—
configure	—
crypto	在**对象**页面上，使用**证书**、**IKE 策略**和 **IPSec 提议**。
ddns	使用**设备** > **系统设置** > **DDNS 服务**配置动态 DNS。
dhcp-client	—
dhcpd	依次选择**设备** > **系统设置** > **DHCP 服务器**。 但是，允许使用 **dhcpd option** 命令。
dhcprelay	请改用 Threat Defense API 中的 dhcprelayservices 资源。
dns	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
dns-group	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
domain-name	使用**对象** > **DNS 组**配置 DNS 组，并使用**设备** > **系统设置** > **DNS 服务器**分配这些组。
dynamic-access-policy-config **dynamic-access-policy-record**	—
enable	—
event	—
failover	—
fips	—
firewall	防火墙设备管理器 仅支持路由防火墙模式。
hostname	依次选择**设备** > **系统设置** > **主机名**。
hpm	此功能不适用于 Firewall Threat Defense 系统。
http	依次访问**设备** > **系统设置** > **管理访问**，使用**数据接口**选项卡。
inline-set	—

禁止的 CLI 命令	备注
interface 用于 BVI、管理、以太网、千兆以太网和子接口。	部分阻止。 在**设备** > **接口**页面上，配置物理接口、子接口和网桥虚拟接口。然后，可使用 FlexConfig 配置其他选项。 但对于这些接口类型，禁止如下 **interface** 模式命令。 **cts** **ip address** **ip address dhcp** **ipv6 address** **ipv6 enable** **ipv6 nd dad** **ipv6 nd suppress-ra** **mode** **nameif** **security-level** **shutdown** **zone-member**
vni、**redundant**、**tunnel** 的 **interface**	在 **设备** > **接口**页面上配置接口。防火墙设备管理器 不支持这些类型的接口。
ip audit	此功能不适用于 Firewall Threat Defense 系统。而应使用访问控制规则应用入侵策略。
ip-client	要将系统配置为使用数据接口作为管理网关，请使用**设备** > **系统设置** > **管理接口**。
ip local pool	使用**设备** > **远程访问 VPN**，配置地址池。
ipsec	—
ipv6	创建 Smart CLI IPv6 前缀列表对象，并将其用于 Smart CLI BGP 对象，以配置 IPv6 前缀列表过滤。
ipv6-vpn-addr-assign	使用**设备** > **远程访问 VPN**，配置地址池。
isakmp	使用**设备** > **站点间 VPN**。
jumbo-frame	如果将任何接口的 MTU 增至超出默认值 1500，系统将自动启用巨型帧支持。
ldap	—
license-server	使用**设备** > **智能许可证**。

禁止的 **CLI** 命令	备注
logging	使用**对象** > **系统日志服务器**和**设备** > **系统设置** > **日志记录设置**。 但是，您可以在 FlexConfig 中配置 **logging history** 命令。
management-access	—
migrate	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN** 来启用 IKEv2 支持。
mode	防火墙设备管理器 仅支持单情景模式。
mount	—
mtu	在**设备** > **接口**上配置各接口的 MTU。
nat	使用**策略** > **NAT**。
ngips	—
ntp	使用**设备** > **系统设置** > **NTP**
object-group network **object network**	使用**对象** > **网络**。 无法在 FlexConfig 中创建网络对象或组，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。
object service |natorigsvc **object service |natmappedsvc**	通常允许 **object service** 命令，但无法编辑名为 |natorigsvc 或 |natmappedsvc 的内部对象。在这些名称中，竖线是有意使用的，是限制对象名称的首个字符。
passwd **password**	—
password-policy	—
policy-list	创建 Smart CLI 策略列表对象，并将其用于 Smart CLI BGP 对象，以配置策略列表。
policy-map 子命令	不能在策略映射中配置以下命令。 **priority** **police** **match tunnel-group**
prefix-list	创建 Smart CLI IPv4 前缀列表对象，并将其用于 Smart CLI OSPF 或 BGP 对象，以配置 IPv4 前缀列表过滤。
priority-queue	—
privilege	—

禁止的 CLI 命令	备注
reload	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。
rest-api	此功能不适用于 Firewall Threat Defense 系统。始终安装并启用 REST API。
route	使用**设备** > **路由**配置静态路由。
route-map	创建 Smart CLI 路由映射对象，并将其用于 Smart CLI OSPF 或 BGP 对象，以配置路由映射。
router bgp	使用适用于 BGP 的 Smart CLI 模板。
router eigrp	使用适用于 EIGRP 的 Smart CLI 模板。
router ospf	使用适用于 OSPF 的 Smart CLI 模板。
scansafe	此功能不适用于 Firewall Threat Defense 系统。请在访问控制规则中配置 URL 过滤。
setup	此功能不适用于 Firewall Threat Defense 系统。
sla	—
snmp-server	使用 FTP API SNMP 资源配置 SNMP。 但是，您可以配置或禁用无法通过 API 配置的参数，例如 **enable oid mempool**。
ssh	依次访问**设备** > **系统设置** > **管理访问**，使用**数据接口**选项卡。
ssl	使用**设备** > **系统设置** > **SSL 设置**。
telnet	Firewall Threat Defense 不支持 Telnet 连接。使用 SSH 而不是 Telnet 访问设备 CLI。
time-range	—
tunnel-group	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN**。
tunnel-group-map	使用**设备** > **远程访问 VPN** 和**设备** > **站点间 VPN**。
user-identity	使用**策略** > **身份**。
username	要创建 CLI 用户，请打开 SSL 或设备控制台会话并使用 **configure user** 命令。
vpdn	—
vpn	—

禁止的 CLI 命令	备注
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—
zone	—
zonelabs-integrity	此功能不适用于 Firewall Threat Defense 系统。

Smart CLI 模板

下表介绍的是基于该功能的 Smart CLI 模板。

注释 您还可以使用 Smart CLI 模板配置 OSPF 和 BGP。但是，可通过**设备**>**路由**页面而不是“高级配置”页面使用这些模板。

功能	模板	说明
对象：AS 路径	ASPath	创建用于路由协议对象的 ASPath 对象。
对象：访问列表	扩展访问列表 标准访问列表	创建用于路由对象的扩展或标准 ACL。您也可以从 FlexConfig 对象（用于配置使用 ACL 的允许命令）按名称引用这些对象。
对象：社区列表	扩展社区列表 标准社区列表	创建用于路由对象的扩展或标准社区列表。
对象：前缀列表	IPV4 前缀列表 IPV6 前缀列表	创建用于路由对象的 IPv4 或 IPv6 前缀列表。
对象：策略列表	策略列表	创建用于路由对象的策略列表。
对象：路由映射	路由映射	创建用于路由对象的路由映射。

Smart CLI 和 FlexConfig 的准则和限制

通过 Smart CLI 或 FlexConfig 配置功能时，请牢记以下几点。

- FlexConfig 对象中定义的命令应在通过 防火墙设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建和部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。
- 如果要删除通过 FlexConfig 配置的功能或功能的一部分，但 Smart CLI 模板引用该功能，则首先必须删除 Smart CLI 模板中使用该功能的命令。然后，部署配置，以便 Smart-CLI 配置功能不再引用它。然后，您可以从 FlexConfig 中删除该功能，并重新部署配置，最终完全清除该配置。

配置 Smart CLI 对象

Smart CLI 对象定义了无法在 防火墙设备管理器中配置的功能。Smart CLI 对象为功能配置提供了一定程度的指导。对于给定的功能（模板），所有可能的命令均已预先加载且已验证所输入的变量。因此，尽管仍然使用 CLI 命令进行功能配置，但 Smart CLI 对象并不像 FlexConfig 对象一样具有自由的形式。

虽然 Smart CLI 模板确实提供了一定程度的指导，但仍然需要阅读 ASA 配置指南和命令参考，了解命令的用法，从而选择可以在您的网络环境下正确运行的值。最好已有可作为配置基础使用的 ASA 配置，只需在 Smart CLI 对象中构建相同的命令序列。

Smart CLI 对象根据功能区进行分组。

注释 所定义的所有 Smart CLI 对象都将被部署。与 FlexConfig 不同的是，无法创建多个 Smart CLI 对象，然后再从中选择要部署的对象。只需为要配置的功能创建 Smart CLI 对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中点击 **Smart CLI** 下的相应功能区。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 输入对象的名称和说明（后者为可选项）。

步骤 5 为要配置的功能选择 **CLI 模板**。

系统会将命令模板加载到**模板**窗口中。最初，系统只显示模板所需的命令。这些命令表示模板所需的最低配置。

步骤 6 填写变量并根据需要在模板中添加命令。

最好使用 ASA 或 Firewall Threat Defense 设备（由 负责管理）的现有配置。有了相应配置，只需确保模板符合配置要求，即可更改适合网络中该特定设备位置的变量（例如 IP 地址和接口名称）。

以下是填写模板的一些提示：

- 要选择变量值，请点击变量，然后键入适当的值或从列表中选择（在有枚举值的情况下）。将鼠标移动到需要键入的变量上，显示该选项的有效值（例如数字范围）。在某些情况下，系统会提供建议值。

  例如，在 OSPF 模板中，所需的命令 **router ospf** *process-id* 在鼠标悬停于其上时显示“进程 ID (1-65535)”，点击 *process-id* 时，该字段会高亮显示。只需键入所需的数字即可。

- 选择变量选项时，如果有其他可能的命令可以配置该选项，则会自动显示并根据需要禁用或启用。注意这些附加命令。

- 使用模板上方的**显示/隐藏禁用**链接控制视图。系统不会配置禁用的命令，但您必须显示这些命令才能进行配置。要查看完整模板，请点击模板上方的**显示已禁用**链接。如只查看将要配置的命令，请点击表上方的**隐藏禁用**链接。

- 要清除上次保存对象之后的所有编辑内容，请点击模板上方的**重置**链接。

- 要启用可选命令，请点击行号左侧的 +按钮。

- 要禁用可选命令，请点击行号左侧的 - 按钮。如果已编辑该行，则不会删除编辑内容。

- 要复制命令，请点击“选项”**...** 按钮，然后选择**复制**。只有在多次输入命令有效时，才允许复制命令。

- 要删除复制命令，请点击选项 **...** 按钮，然后选择**删除**。无法删除作为基本模板组成部分的命令。

步骤 7 点击**确定**。

配置 FlexConfig 策略

FlexConfig 策略只是希望部署到设备配置中的 FlexConfig 对象列表。系统仅部署该策略中包含的对象，所有其他对象均只进行定义而不使用。

FlexConfig 对象中定义的命令应在通过 防火墙设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建和部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。

注释 如有用于功能的 Smart CLI 模板，则不可使用 FlexConfig 进行配置。必须使用 Smart CLI 对象。

开始之前

创建 FlexConfig 对象。请参阅以下主题：

- 配置 FlexConfig 对象， 第 13 页
- 在 FlexConfig 对象中创建变量， 第 14 页
- 配置密钥对象， 第 21 页

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”(Advanced Configuration) 目录中依次点击 **FlexConfig** > **FlexConfig 策略 (FlexConfig Policy)**。

步骤 3 管理**组列表**中的对象列表。

- 要添加对象，请点击 + 按钮。如果对象尚不存在，请点击**创建新的 FlexConfig 对象 (Create New FlexConfig Object)** 来定义。
- 要删除对象，请点击对象条目右侧的 **X** 按钮。

注释
建议使每个对象都完全独立，而不依赖于任何其他 FlexConfig 对象中定义的配置。这样可以确保在不影响其他对象的情况下添加或删除对象。

步骤 4 在**预览**窗格中评估建议的命令。

可以点击**展开 (Expand)** 按钮（随后点击**折叠 (Collapse)**）加宽显示画面，以便更清晰地查看长命令。

预览将评估变量并生成将要发布的确切命令。请确保这些命令正确且有效。您必须确保这些命令不会导致错误或配置不当，否则会使设备无法使用。

注意
系统不验证命令。可以部署无效甚至可能有破坏性的命令。在部署更改之前，请仔细检查预览。

步骤 5 点击**保存 (Save)**。

下一步做什么

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果出现错误，请更正对象中的 CLI。请参阅 FlexConfig 策略故障排除， 第 22 页。

配置 FlexConfig 对象

对于无法使用 防火墙设备管理器进行配置的特定功能，FlexConfig 对象包含配置这类功能所需的 ASA 命令。您必须确保输入正确的命令序列，且无拼写错误。系统不验证 FlexConfig 对象的内容。

建议为要配置的每个常规功能创建单独的对象。例如，如要定义 banner 并配置 RIP 路由协议，请使用 2 个单独的对象。如果以单独的对象隔离各个功能，则可以更轻松地选择要部署的对象，而且更易于进行故障排除。

注释 请勿包括 **enable** 和 **configure terminal** 命令。系统将自动进入配置命令的正确模式。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 输入对象的名称和说明（后者为可选项）。

步骤 5 在**变量**部分，创建要在对象正文中使用的所有变量。

唯一必须创建的变量是指向 防火墙设备管理器中所定义对象的变量，具体而言即网络、端口和密钥变量类型，或指向指定接口的接口变量。对于其他变量类型，只需将值输入到对象正文中。

有关创建和使用变量的详细信息，请参阅在 FlexConfig 对象中创建变量，第 14 页。

步骤 6 在**模板**部分，键入配置该功能所需的 ASA 命令。

必须按正确的顺序输入命令，以便配置该功能。使用 ASA CLI 配置指南，了解如何输入命令。最好拥有 ASA 或其他 Firewall Threat Defense 设备提供的经过预先测试的配置文件，以便用作参考。

此外，还可以使用 Mustache 表示法来引用和处理变量。有关详细信息，请参阅引用 FlexConfig 变量和检索值，第 16 页。

以下是创建对象正文的一些提示：

- 要添加行，请将光标放在行尾然后按 Enter 键。
- 要使用变量，请在双括号 {{*variable_name*}} 中键入变量名称。对于引用对象的变量，必须包括要检索其值的属性：{{*variable_name.attribute*}}。可用属性因对象类型而异。有关完整信息，请参阅变量引用：{{variable}} 或 {{{variable}}}，第 16 页。

- 要使用 Smart CLI 对象，请键入对象的名称。如果需要引用 Smart CLI 中配置的路由进程，请输入进程标识符。请参阅在 FlexConfig 对象中引用 Smart CLI 对象，第 20 页。
- 点击模板正文上方的**展开/折叠**链接，放大或缩小正文。
- 点击**重置**链接，清除自上次保存对象之后所做的任何更改。

步骤 7 在**取消模板**部分，输入删除或反向对象正文中已配置命令所需的命令

“取消”部分非常重要，有两个用途：

- 它简化了部署。在重新部署正文中的命令之前，系统将使用这些命令先清除或取消配置。这将确保一个干净的部署环境。
- 如果您决定通过从 FlexConfig 策略中删除对象的方式来删除该功能，系统将使用这些命令从设备中删除命令。

如果不提供在对象正文中取消或反向 CLI 所需的命令，则部署操作可能需要清除整个设备配置并重新部署所有策略，而不仅仅是对象中的命令。这将使部署时间更长，并且将造成流量中断。确保拥有撤消对象正文中所定义配置所需的所有命令，而且只有这些命令。虽然在模板中否定命令通常是命令的 **no** 或 **clear** 形式，如果真实关闭已启用的功能，“否定”命令实际上是命令的肯定形式，也即启用功能的形式。

使用ASA配置指南和命令参考确定相应的命令。有时，可以使用单个命令撤消配置。例如，在配置 RIP 的对象中，单个 **no router rip** 命令即可删除整个 **router rip** 配置，包括子命令。

同样，如果输入多个 **banner login** 命令创建多行横幅，则单个 **no banner login** 命令将取消整个登录横幅。

如果模板创建多个嵌套对象，取消模板需要按照反向顺序删除对象，即首先删除对象引用，然后再删除对象。例如，如果您先创建一个ACL，接着在流量类中引用该ACL，随后在策略映射中引用流量类，最后使用服务策略启用策略映射，那么取消模板必须依次删除服务策略、策略映射、流量类以及 ACL 来撤消配置。

步骤 8 点击**确定**。

下一步做什么

仅创建一个FlexConfig对象不足以完成部署。必须将该对象添加到FlexConfig策略中。仅FlexConfig策略中的对象可进行部署。这样可细化 FlexConfig 对象并为特殊用途做一些准备，而不会自动部署这些对象。请参阅配置 FlexConfig 策略，第 11 页。

在 FlexConfig 对象中创建变量

FlexConfig 对象中使用的变量在该对象中进行定义。没有单独的变量列表。因此，无法定义某个变量，然后在单独的 FlexConfig 对象中使用该变量。

变量提供以下主要好处：

- 可以指向使用 防火墙设备管理器定义的对象。这包括网络、端口和密钥对象。
- 可以隔离可能会随对象正文变化的值。因此，如果需要更改值，只需编辑变量，而无需编辑对象正文。如果需要在多个命令行中引用对象，这会特别有用。

此程序说明向 FlexConfig 对象中添加变量的过程。

过程

步骤 1 从**设备** > **高级配置页**中编辑或创建 FlexConfig 对象。

请参阅配置 FlexConfig 对象 ， 第 13 页。

步骤 2 在**变量**部分执行下列操作之一：

- 要添加变量，请点击 + 按钮（如果尚未定义变量，请点击**添加变量 (Add Variable)**）。
- 要编辑变量，请点击该变量的编辑图标 ()。

要删除变量，请点击该变量的垃圾桶 () 图标。确保从模板正文中删除变量的任何引用。

步骤 3 输入变量的名称和说明（后者为可选项）。

步骤 4 选择变量的数据**类型**，然后输入或选择相应值。

可以创建以下类型的变量。选择满足使用变量的命令数据要求的类型。

- **字符串** - 文本字符串。例如，主机名、用户名等。
- **数字** - 整数。不要使用逗号、小数、符号（如负号 -）或十六进制表示法。对于非整数数字，请使用字符串变量。
- **布尔值** - 逻辑真/假。选择真或假。
- **网络** -“对象”(Objects) 页面上定义的网络对象或组。选择网络对象或组。
- **端口** -“对象”(Objects) 页面上定义的 TCP 或 UDP 端口对象。选择端口对象。无法为其他协议选择组或对象。
- **接口** -“设备”(Device) >“接口”(Interfaces) 页面上定义的指定接口。选择接口。无法选择没有名称的接口。
- **IP** - 不带网络掩码或前缀长度的单个 IPv4 或 IPv6 IP 地址。
- **密钥** - 为 FlexConfig 定义的密钥对象。选择对象。有关创建密钥对象的详细信息，请参阅配置密钥对象 ， 第 21 页。

步骤 5 在“变量”对话框中点击**添加**或**保存**。

此时，可以在FlexConfig对象正文中使用该变量。引用变量的方式根据变量类型的不同而有所不同。有关如何使用这些变量的详细信息，请参阅下列主题：

- 变量引用：{{variable}} 或 {{{variable}}}，第 16 页
- 部分 {{#key}} {{/key}} 和反向部分 {{^key}} {{/key}}，第 18 页

步骤 6 在“FlexConfig 对象”对话框中点击**确定**。

引用 FlexConfig 变量和检索值

FlexConfig 将 Mustache 作为模板语言，但支持仅限于以下各节中介绍的功能。使用这些功能引用变量、检索其值并予以处理。

变量引用：{{variable}} 或 {{{variable}}}

要引用在 FlexConfig 对象中定义的变量，请使用以下表示法：

{{*variable_name*}}

或：

{{{*variable_name*}}}

这足以用于为单值的简单变量，其中包括如下类型的变量：**数字**、**字符串**、**布尔值**和 **IP**。如果变量包含特殊字符（如 &），请使用三重大括号 。或者，您可以始终对所有变量使用三重大括号。

但是，对于指向在配置数据库中建模为对象的元素的变量，必须使用点符号并纳入要检索的对象属性的名称。可通过检查相关对象类型的 API Explorer 中的模型查找这些属性名称。必须借助以下表示法使用以下类型的变量：**密钥**、**网络**、**端口**和**接口**。

{{*variable_name.attribute*}}

例如，要从名为 net-object1 的网络变量（指向网络对象，而不是网络组）检索地址，可使用：

{{net-object1.value}}

如果想要从对象内的对象中检索属性值，则需使用一系列带点符号的属性向下钻取所需值。例如，将接口的 IP 地址建模为名为 ipv4 和 ipv6 的接口对象子接口。因此，要检索名为 int-inside（指向内部接口）的接口变量的 IPv4 地址和子网掩码，可以使用：

{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}

注释 要打开 API Explorer，点击更多选项按钮 (⋮) 并选择 **API Explorer**。

下表列出的是变量类型、引用方式、API 模型名称及最可能使用的引用（对于对象）。

变量类型	参考模型	说明

布尔值
（简单变量）
	变量：
	{{*variable_name*}}
	部分：
	`{{#variable_name}}`
	`commands`
	`{{/variable_name}}`
	反向部分：
	`{{^variable_name}}`
	`commands`
	`{{/variable_name}}`
		逻辑 true/false。布尔变量的主要用途是用于部分或反向部分。可以编辑布尔变量值打开或关闭一部分命令，例如，如果需要定期或在特殊情况下启用某项功能。
		一些对象在其模型中也具有布尔属性，可用于提供可选的部分处理。

接口
（对象变量：API 模型是 Interface）
	变量：
	{{*variable_name.attribute*}}
	部分：
	`{{#variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
	反向部分：
	`{{^variable_name.attribute}}`
	`commands`
	`{{/variable_name.attribute}}`
		在“设备”(Device)>“接口”(Interfaces) 页面上定义命名的接口。无法指向未命名接口。
		接口模型中有各种可用属性。此外，接口模型包括子对象，例如 IP 地址子对象。
		以下是您可能觉得有用的一些主要属性：
		• *variable_name*.**name** 返回接口的逻辑名称。
		• *variable_name*。**hardwareName** 返回接口端口名称，如 GigabitEthernet1/8。
		• *variable_name*.**managementOnly** 是一个布尔值。TRUE 表示该接口被定义为仅限于管理。FALSE 表示该接口用于流经设备的流量。可以将此选项用作部分密钥。
		• *variable_name*.**ipv4.ipAddress.ipAddress** 返回接口的 IPv4 地址。
		• *variable_name*.**ipv4.ipAddress.netmask** 返回接口的 IPv4 地址的子网掩码。

IP （简单变量）	**变量：** {{*variable_name*}}	单个 IPv4 或 IPv6 IP 地址，无网络掩码或前缀长度。

变量类型	参考模型	说明
网络 （对象变量：API 模型是 NetworkObject）	**变量（网络对象）：** {{*variable_name*.*attribute*}} **部分（组对象）：** {{#*variable_name*.**networkObjects**}} commands referring to one of {{**value**}} {{**name**}} {{/*variable_name*.**networkObjects**}}	“对象”(Objects) 页面上定义的网络对象或组。可使用部分处理网络组。 以下是可能对您有用的主要属性： • {{*variable_name*.**name**}} 返回网络对象或组名称。 • {{*variable_name*.**value**}} 返回网络对象（而非网络组）的 IP 地址内容。确保将具有正确类型内容的网络对象用于给定命令，例如使用主机地址而不是子网掩码地址。 • {{*variable_name*.**groups**}} 返回网络组中包含的网络对象的列表。仅与指向网络组的变量结合使用，并在部分标记上使用以反复处理组内容。使用 {{**value**}} 或 {{**name**}} 依次检索各网络对象的内容。
数字 （简单变量）	**变量：** {{*variable_name*}}	整数。不要使用逗号、小数、符号（如负号 -）或十六进制表示法。对于非整数数字，请使用字符串变量。
端口 （对象变量：API 模型是 PortObject、tcpports 或 udpports）	**变量：** {{*variable_name.attribute*}}	在“对象”(Objects) 页面定义的 TCP 或 UDP 端口对象。必须为端口对象，而不是端口组。 以下是可能对您有用的主要属性： • {{*variable_name*.**port**}} 返回端口号。协议不包括在内。 • {{*variable_name*.**name**}} 返回端口对象名称。
密钥 （对象变量：API 模型是 Secret）	**变量：** {{*variable_name*.**password**}} 或： {{{*variable_name*.**password**}}}	为 FlexConfig 定义的密钥对象。 应该进行的唯一引用是返回加密字符串的 **password** 属性。 如果密码包含特殊字符（如 &），请使用三重大括号。
字符串 （简单变量）	**变量：** {{*variable_name*}}	文本字符串。例如，主机名、用户名等。

部分 {{#key}}{{/key}} 和反向部分 {{^key}}{{/key}}

部分或反向部分是部分开始和结束标记之间的命令块，将密钥作为处理条件。部分的处理方式取决于它是常规部分还是反向部分：

- 如果密钥为空或具有非空内容，则处理常规部分（或简称为部分）。如果密钥为FALSE或对象无内容，则该部分中的命令不予配置。该部分被绕过了。

  以下是常规部分的语法。

```
{{#key}}
one or more commands
{{/key}}
```

- 反向部分即部分的反面。如果密钥为FALSE或对象无内容，则处理反向部分。如果密钥为TRUE或对象具有内容，则绕过反向部分。

  以下是反向部分的语法。唯一的区别是插入符号替换散列标记。

```
{{^key}}
one or more commands
{{/key}}
```

以下主题介绍部分和反向部分的主要用途。

如何处理多值变量

多值变量处理的一个主要示例是指向网络组的网络变量。由于该组包含多个对象（在 **objects** 属性下），可迭代地遍历网络组中的值以使用不同值多次配置相同命令。

虽然对象组定义了对象属性中包含的网络对象，但这些对象并不包括所包含对象的内容。相反，您可以使用 **networkObjects** 属性获取所包含对象的内容。

例如，如果主机为 192.168.10.0、192.168.20.0 和 192.168.30.0 的网络组名称为 net-group，则可使用以下方法为各 RIP 路由地址配置网络命令。请注意，仅使用网络对象的 **value** 属性，因为在本部分开始时使用 **net-group.networkObjects** 意味着将从成员对象中获取该“value”属性。（对于 FlexConfig 对象中的“value”属性，不需要创建单独的变量。）

```
router rip
{{#net-group.networkObjects}}
 network {{value}}
{{/net-group.networkObjects}}
```

系统将该部分结构转换为：

```
router rip
   network 192.168.10.0
   network 192.168.20.0
   network 192.168.30.0
```

如何基于布尔值或空对象执行可选处理

注释 此主题中的示例仅作说明用途。例如，从版本 6.7 开始，不能使用 FlexConfig 配置 SNMP，而必须改用 Firewall Threat Defense API SNMP 资源。

如果相应部分开始标记中的变量内容为TRUE，或对象不为空，则处理该部分。如果布尔值为FALSE或空（例如空对象），则绕过该部分。

这里主要用于布尔值。例如，您可以创建布尔变量，并将命令置于变量所覆盖的节中。然后，如果需要启用或禁用 FlexConfig 对象中的一部分命令，则只需更改布尔变量的值，无需从代码中删除这些行。这使得启用或禁用功能很容易。

例如，如果使用 FlexConfig 启用 SNMP，则可能希望能够关闭 SNMP 陷阱。您可以创建名为 enable-traps 的布尔变量，且最初将其设为 TRUE。然后，如果需要关闭陷阱，只需编辑变量、将其更改为 FALSE、保存该对象，然后重新部署配置。命令序列可能如下所示：

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

还可根据对象内的布尔值执行此类处理。例如，您可以在接口上配置某些特性之前检查该接口是否仅限于管理。在下例中，int-inside 是指向名为 inside 的接口的接口变量。仅当并未将接口设为仅限于管理时，FlexConfig 才可在该接口上配置 EIGRP 相关接口选项。可使用反向部分，以便仅在布尔值为 FALSE 时才配置命令。

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
{{^int-inside.managementOnly}}
interface {{int-inside.hardwareName}}
 hello interval eigrp 2 60
 delay 200
{{/int-inside.managementOnly}}
```

在 FlexConfig 对象中引用 Smart CLI 对象

创建 FlexConfig 对象时，您可以使用变量指向可以在 防火墙设备管理器中配置的对象。例如，您可以创建指向接口元素或网络对象的变量。

但是，不能以相同的方式指向 Smart CLI 对象。

相反，如果您创建需要在 FlexConfig 策略中使用的 Smart CLI 对象，只需在适当的位置输入 Smart CLI 对象的名称。

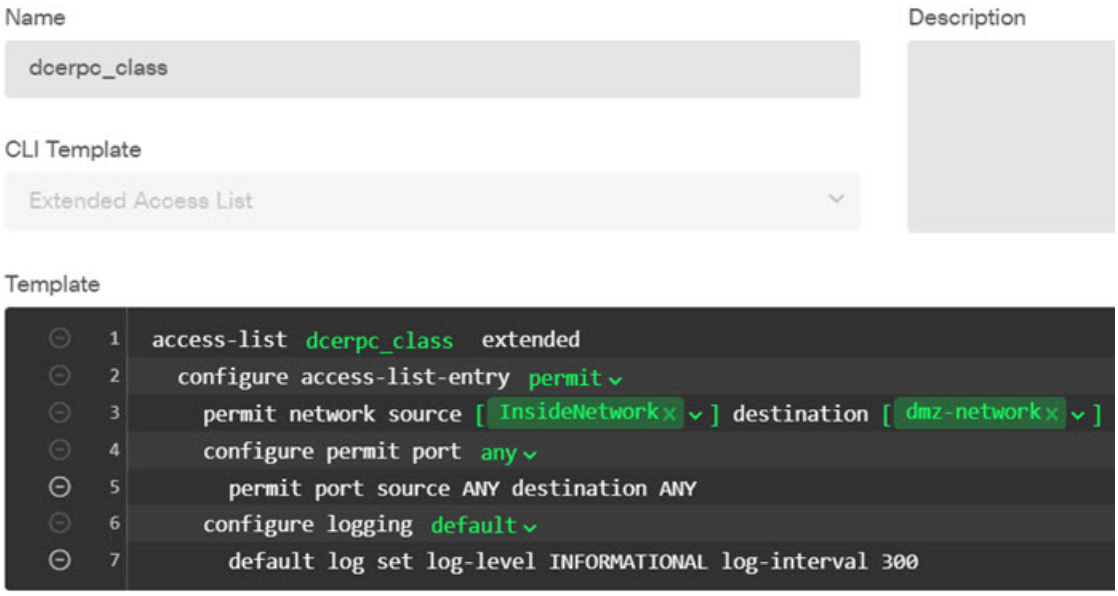
例如，配置协议检测时，您可能想将扩展访问列表用作流量类。由于扩展访问列表具有 Smart CLI 对象，您需要使用 Smart CLI 对象来创建 ACL：不能在 FlexConfig 对象中使用 **access-list** 命令。

例如，如果您要在网络 192.168.1.0/24 和 192.168.2.0/24 之间全局启用 DCERPC 检测，应执行以下操作。

过程

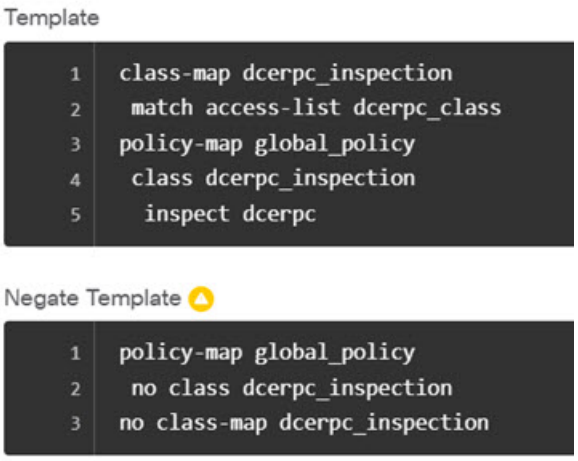
步骤 1 为两个网络创建单独的网络对象。例如，InsideNetwork 和 dmz-network。

步骤 2 在 Smart CLI 扩展访问列表对象中使用这些对象。



步骤 3 创建按名称指向 Smart CLI 对象的 FlexConfig 对象。

例如，如果为对象命名“dcerpc_class”，FlexConfig 对象应如下所示。请注意，在取消模板中，不对通过 Smart CLI 对象创建的访问列表求反，因为该对象实际上并非通过 FlexConfig 创建。



步骤 4 将对象添加到 FlexConfig 策略中。

配置密钥对象

密钥对象的重点在于隐藏密码或敏感字符串。如果不希望冒险让人看到 FlexConfig 对象或 Smart CLI 模板中使用的字符串，请为该字符串创建一个密钥对象。

过程

步骤 1 选择**对象**，然后从目录中选择**密钥**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 输入对象的名称和说明（后者为可选项）。

步骤 4 在**密码**字段和**确认密码**字段中输入密码或其他密钥字符串。

键入时系统会隐藏文本。

步骤 5 点击**确定**。

下一步做什么

- 如果是一个新对象，要在 FlexConfig 中使用该对象，请编辑 FlexConfig 对象，创建一个密钥类型变量，再选择该对象。然后，引用对象正文中的变量。有关详细信息，请参阅在 FlexConfig 对象中创建变量，第 14 页。
- 如要编辑作为 FlexConfig 策略一部分在 FlexConfig 对象中使用的现有对象，则需要部署配置，以使用新字符串更新设备。
- 在 Smart CLI 模板中，如果命令需要密钥，则在编辑相关属性时将会看到这些对象的列表。选择用于此用途的正确密钥。

FlexConfig 策略故障排除

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果您在“待处理更改”对话框中收到“上次部署失败”消息，请点击**查看详细信息**链接。链接将转至审核日志，您可以在其中找到失败的部署作业。打开作业，查找特定错误消息。

如果由于 FlexConfig 问题部署失败，则详细信息将提及带有错误命令的 FlexConfig 对象，并显示失败的命令。使用此信息更正对象并再次尝试部署。对象名称是一个链接，点击打开对象的编辑对话框。

例如，您可能需要配置最大 TCP 段大小 (TCP MSS)。您可以使用 **sysopt connection tcpmss** 命令控制此设置。通过 防火墙设备管理器配置时，此选项的 Firewall Threat Defense 默认值为 0，而 ASA 默认值为 1380。

ASA 默认值是在使用 1500 默认 MTU 的接口上运行 IPv4 VPN 时的最佳处理。系统需要 120 个字节用于 VPN 报头。对于 IPv6，系统需要 140 个字节。 Firewall Threat Defense 默认值为 0，仅允许终端协商 MSS，这是正常流量的理想设置，尤其是在设备接口上使用不同 MTU（包括超过 1500 的 MTU）的情况下。由于 TCP MSS 是一个全局设置而不是根据接口，所以仅当流量中很大一部分通过 VPN，且获得过多分段时，才可对其进行更改。在这种情况下，可将 TCP MSS 设为 MTU - 120（适用于 IPv4）或 MTU - 140（适用于 IPv6），并将同一 MTU 用于所有接口。请注意，即使您明确设置了 MSS，如果 TLS/SSL 解密或服务器发现等组件需要某个特定 MSS，它也会根据接口 MTU 设置该 MSS 并忽略您设置的 MSS。

为了说明这个问题，现在假设需要将 TCP MSS 设为 3 个字节。该命令需要取 48 个字节作为最小值，因此，您会得到类似于以下内容的部署错误：

错误由这些元素组成：

1. 部署错误消息，其中包括导致错误的 FlexConfig 对象的名称。对象名称链接到编辑对话框，以便可快速打开对象更正错误。这是消息的第一句。
2. 以“ERROR：”开头的文本是从设备返回的消息。在键入错误命令但不格式化 SSH 客户端的情况下，ASA 就会做出这种响应。在本例中，错误消息是 “ERROR：[3] 小于 RFC 791 允许的最小 MSS 值 48”。以“Config Error”开头的文本会提及生成错误消息的特定行。
3. 黑色文本是实际导致错误的 FlexConfig 对象行。必须修复此行。在本例中，如果尝试在 MTU 1500 接口上（常见情况）容纳 IPv4 VPN 流量，则应将 3 改为 1380。

   修复本例时，可保持打开 CLI 控制台并使用 **show running-config all sysopt** 查看所有 **sysopt** 命令设置。多数 **sysopt** 命令均具有适用于多数用途的默认设置，因此，不会出现在运行配置中。**all** 关键字包括输出中的这些默认设置。

FlexConfig 示例

以下主题介绍使用 FlexConfig 配置功能的一些示例。

如何启用和禁用默认全局检测

某些协议在用户数据包中嵌入 IP 寻址信息，或在动态分配的端口上打开辅助信道。这些协议需要系统执行深度数据包检测，以便应用 NAT，并允许辅助信道。默认情况下，系统上启用了几个常见检测引擎，但您可能需要根据您的网络启用其他检测引擎或禁用默认检测。

要查看当前已启用的检测列表，请在 CLI 控制台或 SSH 会话中使用 **show running-config policy-map** 命令。以下是此命令在尚未更改检测配置的系统上运行的情况。在此输出中，输出末尾的 **inspect** 命令列表显示启用了哪些协议检测。上述命令在 inspection_default 流量类上启用这些检测（这是常规协议以及被检查协议的端口号，如果适用）。此类是 global_policy 策略映射的一部分，该映射使用

高级配置

未在输出中显示的服务策略命令将这些检测应用到所有接口。例如，在通过设备的所有 ICMP 流量上执行 ICMP 检查。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
!
```

注释 有关每个检测的详细讨论，请参阅《思科 *ASA* 系列防火墙配置指南》，网址为 https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

以下过程介绍如何启用或禁用此全局应用默认检测类中的检测。为便于解释，在本例中：

- 启用 PPTP（点对点隧道协议）。此协议用于在终端之间创建点对点连接。
- 禁用 SIP（会话发起协议）。通常仅当检测引发网络问题时，才会禁用 SIP。但是，如果禁用 SIP，必须确保访问控制策略允许 SIP 流量 (UDP/TCP 5060) 和任何动态分配的端口，而且，您无需为 SIP 连接提供 NAT 支持。通过标准页面而不是 FlexConfig 相应地调整访问控制和 NAT 策略。

开始之前

良好的规划可帮助您有效地使用 FlexConfig。在本示例中，我们要更改两个不同的不相关检测，尽管我们在同一流量类中进行更改。如果您需要更改这些策略，很可能需要单独执行此操作。

因此，我们建议在本示例中为每项检测创建单独的 FlexConfig 对象。通过这种方式，您可以轻松更改一项检测的设置，无需更改另一项检测的设置，也无需编辑 FlexConfig 对象。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 创建要启用 PPTP 检测的对象。

a) 点击 **+** 按钮以创建新的对象。

b) 为对象输入名称。例如，**Enable_PPTP_Global_Inspection**。

c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
policy-map global_policy
 class inspection_default
  inspect pptp
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从FlexConfig策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
policy-map global_policy
 class inspection_default
  no inspect pptp
```

该对象应如下所示：

高级配置

注释
由于 inspection_default 类启用了其他检测命令，您不想取消整个类。同样，global_policy 策略映射包括这些其他检测，而您也不想否定策略映射。

e) 点击**确定**保存对象。

步骤 4 创建要禁用 SIP 检查的对象。

a) 点击 **+** 按钮以创建新的对象。
b) 为对象输入名称。例如，**Disable_SIP_Global_Inspection**。
c) 在**模板**编辑器中，输入以下命令，包括缩进。

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

d) 在**取消模板**编辑器中，输入撤消此配置所需的命令。

禁用“no”命令的“否定”命令是启用功能的命令。因此，“取消”模板不仅仅是禁用某项功能的命令，它是“肯定”模板中所执行任何命令的反向命令。取消模板的实质是撤消所做的更改。

因此，在本示例中，取消模板为：

```
policy-map global_policy
```

```
class inspection_default
 inspect sip
```

该对象应如下所示：

e) 点击**确定**保存对象。

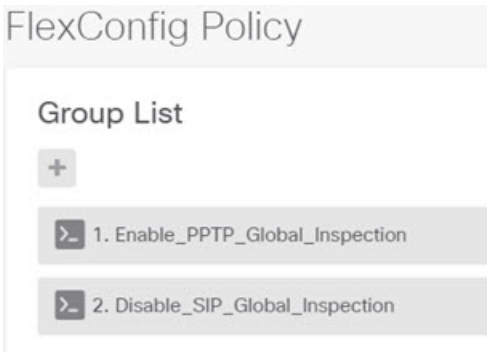
步骤 5 将对象添加到 FlexConfig 策略中。

仅创建对象远远不够。仅当您将对象添加到FlexConfig策略（并保存所做的更改）时，才部署对象。这样，您可以在对象上试验（可部分完成），不必担心会在未完成的作业上失败。您可以通过添加和删除对象轻松打开或关闭功能：无需每次都重新创建对象。

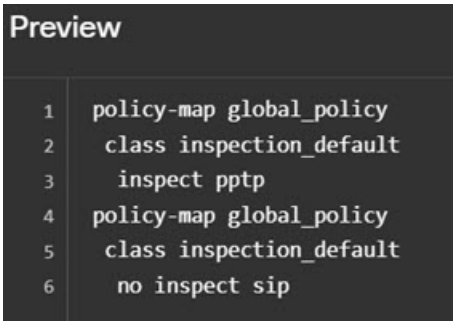
a) 点击目录中的 **FlexConfig 策略**。
b) 在组列表中点击 **+**。
c) 选择 Enable_PPTP_Global_Inspection 和 Disable_SIP_Global_Inspection 对象，然后点击**确定**。

组列表应如下所示：

高级配置



系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。



d) 点击**保存**。

您现在可以部署策略。

步骤 6 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 7 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect pptp** 已添加到 inspection_default 类的底部，而 **inspect sip** 在类中不再存在。这表示已成功部署 FlexConfig 对象中定义的更改。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
```

```
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
!
```

如何撤消 FlexConfig 更改

如果您在 FlexConfig 对象中输入正确的取消模板，删除使用该对象所做的更改非常简单。只需从 FlexConfig 策略中删除该对象，下一个部署时，系统即可使用取消模板撤消所做的更改。

您不需要创建新对象来撤消所做的更改。

以下示例展示如何重新启用全局 SIP 检测。该示例将恢复如何启用和禁用默认全局检测，第 23 页中所述的更改，此部分已禁用 SIP 检测。

开始之前

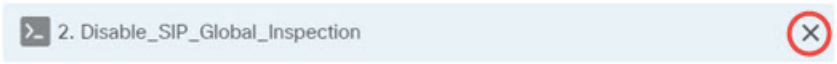
验证 FlexConfig 对象是否具有正确的取消模板。如果没有，请编辑对象更正取消模板。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”(Advanced Configuration) 目录中依次点击 **FlexConfig** > **FlexConfig 策略 (FlexConfig Policy)**。

步骤 3 点击 FlexConfig 策略中 **Disable_SIP_Global_Inspection** 对象条目右侧的 **X**，将其从策略中删除。



预览中将删除该对象中的命令。取消命令不会添加到预览，而是在后台执行。

步骤 4 点击**保存 (Save)**。

步骤 5 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 6 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect sip** 已添加到 inspection_default 类的底部。这表示已成功部署 FlexConfig 对象中定义的更改。（顺序在此类中不重要，因此， **inspect sip** 在末尾，而不在其原始位置并不重要。)

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect pptp
  inspect sip
!
```

如何启用唯一流量类检测

在本示例中，我们将对特定接口上两个终端之间的流量启用 PPTP 检测。此检测仅面向两者之间配置点到点隧道的终端。

启用 2 个终端之间 PPTP 检测所需的 CLI 涉及以下要素：

1. 源和目标设置为终端主机 IP 地址的 ACL。
2. 引用此 ACL 的流量类。
3. 包含流量类，并在该流量类上启用 PPTP 检测的策略映射。

4. 将策略映射应用到所需接口的服务策略。此步骤实际上是激活策略并启用检测的操作。

注释 有关与检测相关的服务策略的详细讨论，请参阅《思科 *ASA* 系列防火墙配置指南》，网址为：https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html。

过程

步骤 1 在**设备** > **高级配置**中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 对象**。

步骤 3 点击 + 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_PPTP_Inspection_on_Interface**。

步骤 5 为内部接口添加一个变量。

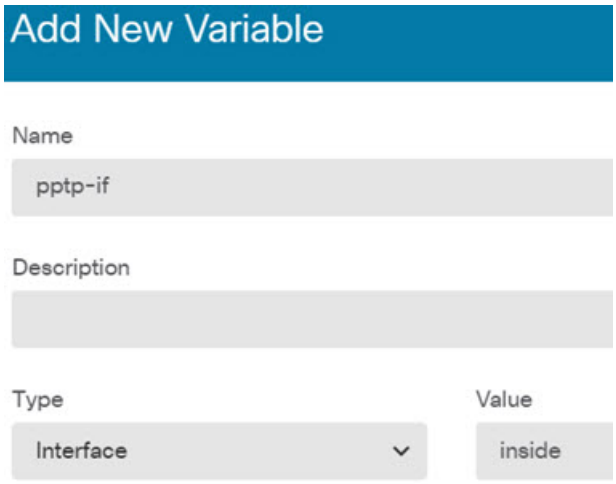
a) 点击变量列表上方的 +。

b) 输入变量的名称，例如 **pptp-if**。

c) 对于**类型**，请选择**接口**。

d) 对于**值**，请选择**内部**接口。

对话框应如下所示：



e) 点击**添加**。

步骤 6 在**模板**编辑器中，输入以下命令，包括缩进。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
 match access-list MATCH_ACL
policy-map PPTP_POLICY
 class MATCH_CMAP
```

```
  inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

请注意，要使用 变量，请在双括号中键入变量名称。此外，您还需要使用圆点表示法来选择您想要检索的属性，因为定义接口的对象具有许多属性。由于接口名称保存在“name”属性中，输入 **{{pptp-if.name}}** 将为接口检索分配给变量的名称属性的值。如果您需要更改执行 PPTP 检测的接口，只需选择变量定义中的其他接口。

步骤 7 在**取消模板**编辑器中，输入撤消此配置所需的命令。

对于本示例中，我们将假设类映射、策略映射和服务策略仅用于应用 PPTP 检测目的。因此，在取消模板中，我们想要删除所有这些要素。

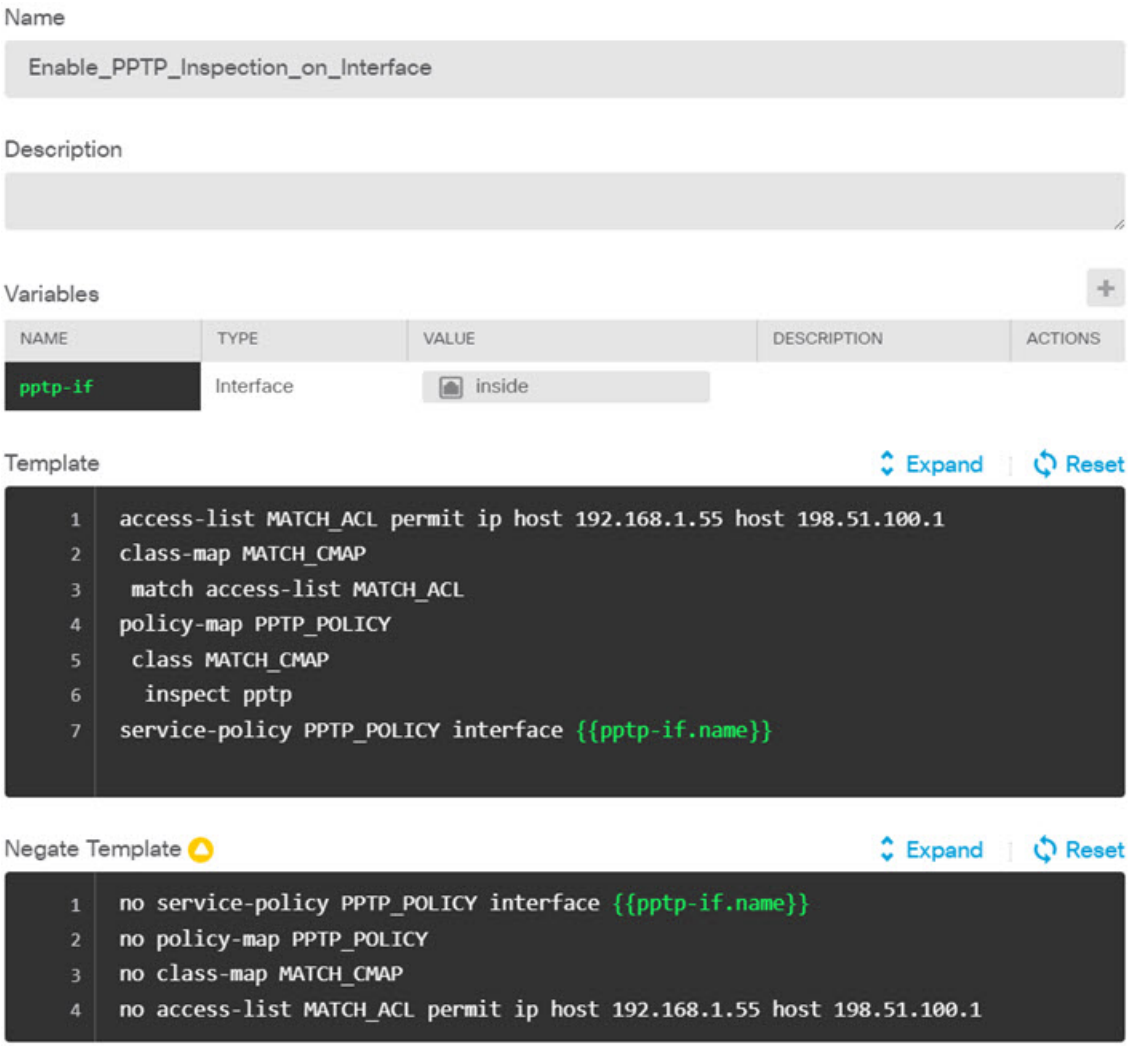
但是，如果您将 PPTP 检测实际添加到接口上的现有服务策略，不需要对策略映射或服务策略求反。您可以从策略映射对类求反，或仅在策略映射的类中关闭检测。您需要清楚了解您在其他 FlexConfig 对象中实施的策略，确保取消模板不会产生意外的后果。

删除嵌套项目时，您需要按照与项目创建顺序相反的顺序执行删除。因此，您需要先删除服务策略，最后再删除访问列表。否则，您将尝试删除正在使用的对象，而系统将返回错误，不允许您执行此操作。

```
no service-policy PPTP_POLICY interface {{pptp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

该对象应如下所示：

高级配置



步骤 8 点击**确定**保存对象。

步骤 9 将对象添加到 FlexConfig 策略中。

a) 点击目录中的 **FlexConfig 策略**。

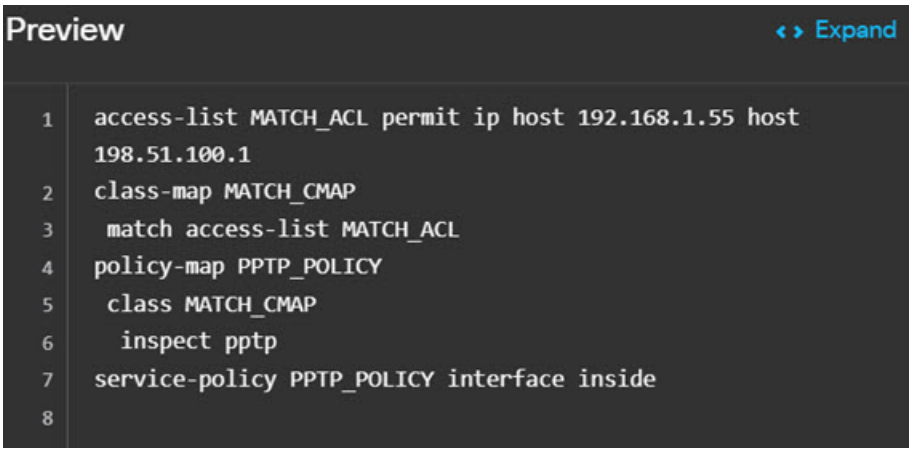
b) 在组列表中点击 **+**。

c) 选择 **Enable_PPTP_Inspection_on_Interface** 对象，然后点击**确定**。

组列表应如下所示：

高级配置

系统应随即使用模板中的命令更新预览。验证您是否看到下图所示的预期命令。请注意，接口变量在预览中解析为名称“inside”。需要特别注意变量：如果在预览中解析不正确，它们将不能正确部署。编辑 FlexConfig 对象，直到可以在预览中获得正确的变量转换。



d) 点击**保存**。

您现在可以部署策略。

步骤 10 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 11 在 CLI 控制台或 SSH 会话中，使用 **show running-config** 命令的变体并验证运行配置是否具有正确的更改。

您可以输入 **show running-config** 检查整个 CLI 配置，也可以使用以下命令验证此配置的每个部分：

- **show running-config access-list MATCH_ACL** 验证 ACL。
- **show running-config class** 验证类映射。此命令将显示所有类映射。
- **show running-config policy-map PPTP_POLICY** 验证类和策略映射配置。
- **show running-config service-policy** 验证应用于接口的策略映射。这将显示所有服务策略。

以下输出显示该序列命令，您可以看到配置已正确应用。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
```

```
 match access-list MATCH_ACL
class-map inspection_default
 match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
 class MATCH_CMAP
  inspect pptp
!
> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

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。

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。

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。

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。