安全配置文件

解密配置文件

多云防御网关 在反向代理 **或** 正向代理场景中使用解密配置文件。代理连接时，会在网关上终止前端会话，并与服务器建立新的后端会话。此终止的目的是解密和检查流量，以防止恶意活动。要解密加密流量，需要解密配置文件。

创建解密配置文件

使用以下程序来创建应用配置文件。

步骤 1 导航至 **管理** > **配置文件** > **解密**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定 **配置文件名称** 和 **说明**。

步骤 4 对于 **证书方法**，选择 **选择现有**。

步骤 5 对于 **证书**，选择想要的证书。

步骤 6 对于 **最小 TLS 版本**，请选择解密配置文件接受的最低 TLS 版本。默认值为 TLS 1.0。

步骤 7 如果使用非默认（非 PFS）密码套件，请从 Diffie-Hellman 或 PKCS (RSA) 菜单中选择所需的密码套件集。

步骤 8 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

解密配置文件中的 TLS 版本

多云防御网关 支持所有 TLS 版本（TLS 1.3、TLS 1.2、TLS 1.1、TLS 1.0）。用户可以指定要使用的最低 TLS 版本， 多云防御网关 将协商等于或高于指定的最低 TLS 版本的 TLS 版本。在 TLS 协商期间， 多云防御网关 将始终使用最高的 TLS 版本。如果 多云防御网关 无法协商满足指定的最低 TLS 版本的版本， 多云防御网关 将丢弃会话并记录 `TLS_ERROR` 事件。

Note 只能将一个最低 TLS 版本应用于网关。策略规则集或策略规则集组中使用的所有服务对象引用的所有解密配置文件必须使用一致的最低 TLS 版本。如果指定了不同的最低 TLS 版本，则无法预先确定将应用的最低 TLS 版本。

Cipher Suites

多云防御网关 支持一组默认和用户可选的密码套件。默认设置为始终处于选中状态的 PFS 密码套件。用户可选择的密码套件包括可由用户选择的 Diffie-Hellman 和 PKCS (RSA) 密码套件。网关使用组合的密码套件集（默认和用户选择）来建立安全的前端加密会话。客户端将发送首选密码套件的有序列表。网关将使用从客户端提交的有序集合和网关可用的集合中选择的密码套件进行响应。如果客户端允许服务器定义顺序，则选择的cpher套件来自网关可用的有序集合和客户端提交的集合。

以下是网关支持且在解密配置文件中可用的密码套件的有序列表：

类别	密码套件	密钥交换	密码	哈希	默认值
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	

类别	密码套件	密钥交换	密码	哈希	默认值
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS (RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS (RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS (RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS (RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS (RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS (RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	
PKCS (RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS (RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

反恶意软件配置文件

防恶意软件配置文件使用 Talos ClamAV 病毒检测引擎启用防恶意软件保护。ClamAV® 是用于检测木马、病毒、恶意软件和其他恶意威胁的防病毒引擎。

以下步骤将指导您创建防恶意软件配置文件并将其与策略规则相关联。

创建防恶意软件配置文件

步骤 1 导航至 **管理** > **配置文件** > **网络威胁**。

步骤 2 选择 **防恶意软件**。

步骤 3 提供 **名称** 和输入说明。

步骤 4 为 Talos 规则集选择以下模式之一：

- **手动模式** - 从下拉列表中选择 Talos 规则集版本。所选规则集版本由使用此配置文件的所有网关上的 多云防御 数据路径引擎使用，并且不会自动更新到较新的规则集版本。
- 自动模式 - 选择在 多云防御 发布规则集版本后将部署延迟多少天。 多云防御 每天发布新规则集，使用此配置文件的网关会自动更新为 **N** 天或更早的最新规则集版本，其中 **N** 是从下拉列表中选择的“延迟天数”参数。例如，如果您选择在 2024 年 1 月 10 日将部署延迟 5 天，则 多云防御控制器 将选择在 1 月 5 日或更早发布的规则集版本。请注意，如果我们对该规则集版本的内部测试由于某种原因失败，则 多云防御 可能不会在某些天发布。

步骤 5 选择找到病毒签名匹配项时要执行的 **操作** 。

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

防数据丢失 (DLP) 配置文件

在转发代理（出口）模式下部署解决方案时，DLP（数据丢失防护）配置文件使 多云防御多云防御 客户能够指定策略规则，以在发现数据泄露模式时进行检测并采取措施。

多云防御 除了基于自定义 PCRE 的正则表达式模式外，还允许客户指定常见的预打包数据模式，例如社会保险号 (SSN)、AWS 密钥、信用卡号等。这样可以轻松地对 PCI、PII 和 PHI 数据实施保护，以满足合规性要求。此功能与现有的 多云防御 功能集集成，无需单独的 DLP 服务。

创建防数据丢失配置文件

步骤 1 导航至 **管理** > **配置文件** > **网络威胁**。

步骤 2 点击 **创建入侵配置文件**。

步骤 3 选择 **数据防泄漏**。

步骤 4 提供 **名称** 和输入说明。

步骤 5 在表中输入 **DLP 过滤器列表** 。

步骤 6 点击 **添加** 以根据需要插入更多行。

步骤 7 提供过滤器的 **说明** 。

步骤 8 从下拉列表中选择预定义的静态模式（例如 CVE 编号）或提供自定义正则表达式。

步骤 9 提供 **计数** 以定义必须在流量中看到该模式的次数。

步骤 10 选择模式与计数次数匹配时要执行的 **操作** 。

注释 在某些情况下，由于模式更严格，AWS 访问密钥和 AWS 密钥的预定义模式在 DLP 检测中不匹配。在 DLP 配置文件中使用以下宽松的自定义模式检测 AWS 访问密钥和 AWS 密钥。请注意，这可能会生成误报日志事件。

```
AWS 访问密钥：(?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])
```

```
AWS 密钥：(?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

网络入侵 (IDS/IPS) 配置文件

网络入侵配置文件是一组入侵检测和保护 (IDS/IPS) 规则，可用于评估事务以确保流量不是恶意的。

多云防御 支持以下 IDS/IPS 规则集：

Table 1: 多云防御 支持以下 ***IDS/IPS*** 规则集

规则集	说明
Talos 规则	Talos 规则是基于从实际调查、渗透测试和研究中收集的情报而制定的一组高级规则，可为应用和框架提供高级保护。
自定义规则	自定义规则是由客户编写的一组特定规则，可为自定义应用提供特定级别的保护。

上传自定义 IDS/IPS 规则

包含一个或多个规则的自定义规则集可以由思科安全 IDS/IPS 安全引擎上传和使用。规则集中包含的规则提供客户对其特定应用和框架所需的专用应用评估。在评估 IDS/IPS 配置文件中配置的任何其他规则集之前，将首先评估 IDS/IPS 配置文件中包含的自定义规则。

上传自定义规则集时，文件应为扩展名为 `tar.gz`的 Gzip 压缩 TAR 文件。压缩的 TAR 文件将包含以下文件：

- 自述文件 - 提供规则集说明的文件。
- 更改日志文件 - 表示更改历史记录的文件。
- Rules 文件夹 - 包含一个或多个 ModSecurity 格式的规则文件的文件夹。每个文件的扩展名必须为 `.conf`。文件夹必须包含至少一个规则文件（不能为空）。每个文件都必须遵循 ModSecurity 规则格式准则。

步骤 1 导航至 **管理** > **威胁研究** > **网络入侵**。

步骤 2 点击 **自定义** 选项卡。

步骤 3 点击 **导入** 按钮并上传自定义规则集文件。

创建 IPS/IDS 配置文件

使用以下程序创建 IPS/IDS 配置文件并将其添加到规则集：

步骤 1 导航至 **管理** > **配置文件** > **IPS/IDS**。

步骤 2 点击 **创建入侵配置文件**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 使用以下选项之一指定 **操作**：

- **规则默认值** - 根据每个触发的规则中指定的操作允许或拒绝请求，并记录事件。
- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 6 如果 IDS/IPS 配置文件检测到恶意活动，请检查是否生成威胁 PCAP 文件。

步骤 7 指定 **规则集**。请注意，需要在 IDS/IPS 配置文件中指定规则库中的至少一个规则集（Talos、自定义）。如果使用 Talos 规则和自定义规则集，则必须至少启用这两个规则之一。如果希望禁用整个 IDS/IPS 配置文件，请从任何策略规则集中删除 IDS/IPS 配置文件，以便不评估 IDS/IPS 配置文件。

指定以下其中一项 **Talos 规则**：

- **已禁用** - 指定是否禁用 Talos 规则。
- **手动** - 指定 Talos 规则的版本。
- **自动** - 指定从发布日期到延迟自动更新到最新 Talos 规则版本的天数。

步骤 8 将特定 **自定义规则集** 添加到 IPS/IDS 配置文件。

步骤 9 为可针对特定 IP 或 CIDR 列表抑制的规则指定 **规则抑制**，然后点击 **添加**。

步骤 10 找到并选择 **高级设置** 选项卡，然后在“规则抑制”下点击 **添加**。

a) 对于 **规则 ID 列表**，提供以逗号分隔的规则 ID 列表。对于 **源 IP/CIDR 列表**，请提供以逗号分隔的 IP 或 CIDR 列表。

b) 对于 **操作**，请提供一个选项，但此选项不适用，因为系统不会评估被抑制的规则。

步骤 11 选择 **事件过滤类型**；这会减少触发 IPS/IDS 配置文件时生成的安全事件的数量，并且可以将事件过滤配置为以下选项之一：

- **速率** - 根据在时间评估间隔内触发的指定 **事件数** （以秒为单位）对生成的事件进行速率限制。
- **类型** - 根据指定 **的事件数对**生成的事件进行采样。

步骤 12 在 **规则事件过滤**下，点击 **添加**。

步骤 13 对于 **规则 ID 列表**，请指定以逗号分隔的规则 ID 列表。

步骤 14 使用以下选项之一指定规则事件过滤 **类型** ：

- **速率** - 指定 **事件数量** 和 **时间** 评估间隔（以秒为单位）。
- **样本** - 指定 **事件数**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

恶意 IP 配置文件

可以启用其他安全保护，以防止与已知恶意 IP 之间的通信。这些恶意 IP 由 Trustwave 定义，并作为安全配置文件规则集集成到 多云防御 中。随着 Trustwave 提供更新，规则集会经常更新。可以使用恶意 IP 配置文件的自动更新配置将更新动态应用到策略规则集。

Note Trustwave 根据已获知的各种行为识别恶意 IP：

- 从网络蜜罐中识别的恶意攻击者
- 僵尸网络 C&C 主机
- Tor 出口节点
- 其他学习行为

创建恶意 IP 配置文件

使用以下程序创建恶意 IP 配置文件：

步骤 1 导航至 **管理** > **配置文件** > **恶意 IP**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这有助于区分具有相似名称的其他配置文件。

步骤 5 选中此复选框可启用 **IP 信誉**。

步骤 6 选择 **Trustwave 规则集版本** 下拉菜单的两个选项之一：

- **手动** - 所选规则集版本由使用此配置文件的所有网关上的 多云防御 数据路径引擎使用。配置文件不会自动更新到较新的规则集版本。
- **自动** - 选择在 多云防御发布规则集版本后延迟更新的天数。新规则集由 多云防御 频繁发布，使用此配置文件的网关会自动更新为 **N** 天或更早的最新规则集版本，其中 **N** 是从下拉列表中选择的“延迟天数”参数。例如，如果您选择在 2021 年 1 月 10 日将部署延迟 5 天，则 多云防御 控制器将选择在 1 月 5 日或更早发布的规则集版本。请注意，如果我们对该规则集版本的内部测试由于某种原因失败，则 多云防御 可能不会在某些天发布。

步骤 7 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

IP 信誉

IP 信誉复选框用于 **启用** 或 **禁用** 配置文件。选中并将配置文件附加到策略规则集时，将实施恶意 IP 保护。取消选中且配置文件附加到策略规则时，不会实施恶意 IP 保护。我们建议始终选中配置文件的 IP 信誉复选框，以便启用该配置文件。如果要禁用恶意 IP 配置文件，请从策略规则中删除其关联，而不是取消选中该复选框。

Web 应用防火墙 (WAF) 配置文件

Web 保护配置文件是 Web 应用防火墙 (WAF) 规则的集合，可用于评估基于 Web 的事务，以确保流量不是恶意的。

上传自定义 WAF 规则

多云防御 支持以下 WAF 规则集：

Table 2: 多云防御 支持以下 *WAF* 规则集

规则集	说明
核心规则	核心规则是来自 ModSecurity CRS（核心规则集）的一组标准规则，可为任何 Web 应用提供基本保护。
Trustwave 规则	TheTrustwave 规则是来自 ModSecurity 的一组高级规则，基于从实际调查、渗透测试和研究中收集的情报，为特定 Web 应用和框架提供高级保护。
自定义规则	自定义规则是由客户编写的一组特定规则，可为自定义 Web 应用提供特定级别的保护。

多云防御 WAF 安全引擎可以上传和使用包含一个或多个规则的自定义规则集。规则集中包含的规则提供客户对其特定 Web 应用和框架所需的专用 Web 应用评估。在评估 WAF 配置文件中配置的任何其他规则集之前，将首先评估 WAF 配置文件中包含的自定义规则。

上传自定义规则集时，文件应为扩展名为 `tar.gz`的 Gzip 压缩 TAR 文件。压缩的 TAR 文件将包含以下文件：

- **自述文件** - 提供规则集说明的文件。
- **更改日志文件** - 表示更改历史记录的文件。
- **规则文件夹** - 包含一个或多个 ModSecurity 格式的规则文件的文件夹。每个文件的扩展名必须为`.conf`。文件夹必须包含至少一个规则文件（不能为空）。每个文件都必须遵循 ModSecurity 规则格式准则。

步骤 1 导航至 **管理** > **威胁研究** > **Web 防护**。

步骤 2 点击 **自定义** 选项卡。

步骤 3 点击 **导入** 按钮并上传自定义规则集文件。

创建 WAF 配置文件

使用以下程序创建 WAF 配置文件。

Note 如果指定了核心规则集，则无法禁用核心规则。要禁用核心规则，请从 WAF 配置文件中删除所有核心规则集，以便不对它们进行评估。

步骤 1 导航至 **管理** > **配置文件** > **WAF**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定以下常规设置：

a) 在**名称 (Name)** 中输入唯一的名称。

b) （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

c) 指定操作：

- **规则默认值** - 根据每个触发规则中指定的操作 **允许** 或 **拒绝** 请求，并记录事件。
- **允许日志** - 允许请求并记录事件。
- **拒绝日志** - 拒绝请求并记录事件。

d) 指定在 WAF 配置文件检测到恶意活动时是否生成威胁 HAR 文件。

e) 指定在 WAF 配置文件检测到恶意活动时是否生成 HTTP 请求 HAR 文件。

f) 在左侧的垂直选项卡中，点击 **核心规则**。您必须从规则库（核心、Trustwave、自定义）中指定至少一个规则集：

- 指定 **手动** 或 **自动**。**手动**- 指定要使用的核心规则版本； **自动** - 指定从发布日期到延迟自动更新到最新核心规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

g) 在左侧的垂直选项卡中，点击 **Trustwave 规则**。

- 指定 **已禁用**、**手动** 或 **自动**。**已禁用** - 指定是否禁用 Trustwave 规则； **手动** - 指定要使用的 Trustwave 规则版本； **自动** - 指定从发布日期到延迟自动更新到最新 Trustwave 规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

h) 在左侧的垂直选项卡中，点击 **自定义规则**。

- 指定以下选项之一：
  - **已禁用** - 指定是否禁用自定义规则。
  - **手动** - 指定要使用的自定义规则版本。
  - **自动** - 指定从发布日期到延迟自动更新到最新自定义规则版本的天数。
- 确定要添加到配置文件的规则，然后点击 **添加到配置文件**。选项显示在右侧的表中。

步骤 4 滚动到窗口顶部，然后点击 **高级设置** 选项卡：

a) 在“规则抑制”下，点击 **添加** 为规则添加一行或多行。可以为特定 IP 或 CIDR 列表抑制规则：

- 对于 **源 IP/CIDR 列表**，请提供以逗号分隔的 IP 或 CIDR 列表。
- 对于 **规则 ID 列表**，提供以逗号分隔的规则 ID 列表。

b) 在“事件过滤”下，提供以下信息：

- **类型** - **速率** 或 **样本**。

- 事件数。
- 时间 **(Time)**。

c) 在“规则事件过滤”下，点击 **添加** 为规则添加一行或多行。对于您创建的每个新行，请输入有效的 **规则 ID 列表**、 **事件数量**、 **时间**（秒），然后选择类型或样本作为 **类型**。

d) 在“核心规则集”下，输入 **请求异常** 和 **响应异常**的值。请注意，对“请求异常”使用小于 3 的值会导致大量警报。

e) 选择 **偏好水平**。选项范围为 1-4。

步骤 5 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

规则事件过滤

要减少触发 WAF 配置文件时生成的安全事件的数量，可以配置事件过滤来对事件进行速率限制或采样。配置不会改变检测或保护行为。

规则事件过滤适用于 WAF 配置文件中配置的特定规则。

步骤 1 点击规则事件过滤下的 **添加** 。

步骤 2 对于 **规则 ID 列表**，请指定规则 **ID**的逗号分隔列表。

步骤 3 将“类型”指定为 **速率** 或 **示例**。

- **速率**- 指定 **事件数量** 和 **时间** 评估间隔（以秒为单位）。
- **样本**- 指定 **事件数**。

下一步做什么

将 WAF 配置文件与策略规则关联

创建 L7 DoS 配置文件

第 7 层 DoS 攻击的目标是耗尽 Web 服务器资源，通过发送许多 HTTP 请求来影响服务可用性。 多云防御网关提供的功能通过持续监控发送到后端 Web 服务器的客户端请求来实现对应用层攻击的监控、检测和补救。启用网关以代理与后端 Web 服务的入站连接时，将启用此功能。启用此功能还允许网关在前端负载均衡器可能不支持或可能未经过优化以检测和补救应用 DoS 攻击的情况下增加安全深度。

此功能可应用于后端 Web 服务，以保持基于 Web 的应用的可用性，也可用于针对托管 API 服务的后端 Web 服务器提供 DoS 保护。

步骤 1 导航至 **管理** > **配置文件** > **Web 保护**。

步骤 2 选择 **第 7 层 DOS**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的其他配置文件。

步骤 5 添加 **请求速率限制**。

限制对资源的过多请求基于以下参数。这些参数的值应基于测量和了解要受第 7 层 DOS 选项保护的 Web 服务的流量模式。

***Table 3:* 参数**

参数	说明
URI	用于指示限制资源请求的路径的相对 URI。例如，如果您打算监控和保护位于 https://www.example.com/login.html 的服务资源，则应在“**请求速率限制**” 表中输入 /login.html 作为 URI 参数。
HTTP 方法 (HTTP Methods)	可以按资源 URI 指定 HTTP 方法，以控制客户端请求中的哪些 HTTP 方法受速率限制，哪些不受速率限制。您可以从表中每一行的下拉列表中选择多个方法。空 HTTP 方法列表意味着该方法将被忽略，并且该速率适用于对该资源的所有调用。 **Note** 速率适用于每个资源；因此，多个方法共享该行中“请求速率”中指定的速率限制。例如，如果速率为每秒 3 个请求，并且在 HTTP 方法中指定了 GET、POST 和 PUT，并且在同一秒内从单个客户端 IP 对该 URI 执行了 2 个 GET 和 1 个 POST，则 PUT 不会在同一秒内允许。
请求速率	每秒的请求数。它确定单个客户端可以向规则的 URI 部分中提到的 URI 资源发送请求的速率。
BurstSize	指定客户端可以发送到规则的 URI 部分中提到的 URI 资源的最大并发请求数。超过此阈值的任何请求同时到达代理，将不会发送到后端服务器。

步骤 6 完成后，请点击 **保存** 。根据 URI，规则的顺序很重要，因为规则是从上到下检查的，并在第一个匹配项时应用。如果在列表中较高位置添加的 URI 包含的资源路径包含其下方规则中的资源，则将应用匹配的第一个规则。

What to do next

- 查看配置文件详细信息

- 将网关关联添加到配置文件

网关指标转发配置文件

此配置文件旨在转发 多云防御网关 生成的网关指标，以进行数据监控和分析。虽然指标由网关生成，但 多云防御控制器 会将指标转发到第三方分析应用。使用此转发配置文件，您无需登录 多云防御即可监控、分析和组织网关指标。使用此信息来衡量网关环境的性能和行为；您还可以利用此信息进行环境故障排除。

注释 从 多云防御控制器 版本 23.09 开始，仅支持 Datadog 作为第三方分析应用。

对于大多数可用的分析应用（例如 Datadog），您必须已经是授权用户才能访问该工具的 API 和呈现的数据。

创建独立指标转发配置文件

使用以下程序为指标转发创建独立配置文件：

开始之前

在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。

步骤 1 导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于与具有相似名称的其他配置文件区分开来。

步骤 5 展开 **类型** 下拉菜单，然后选择 **独立**。

步骤 6 拓展 **目标** 下拉菜单，然后选择第三方应用来处理和分析指标。

步骤 7 输入要用作指标的 **终端** 位置的终端。

步骤 8 点击**保存**。

如果选择 Datadog 作为分析应用，则默认情况下会使用 HTTPS Webhook 填充 **终端** 。如果默认设置，可以在保存配置文件之前修改此条目。

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

创建组指标转发配置文件

在此过程中，您需要创建一个配置文件，然后将其分配给特定网关。组配置文件最多组合五个独立的指标转发配置文件，然后可以将其分配给单个网关。使用以下程序创建分组指标转发配置文件：

开始之前

- 在创建此配置文件之前，您必须至少有一个第三方应用来转发指标。
- 您必须至少创建两个独立的指标转发配置文件。有关详细信息，请参阅创建独立指标转发配置文件，第 13 页。

步骤 1 在 多云防御控制器 界面中，导航到 **管理器** > **配置文件** > **指标转发**。

步骤 2 点击**创建 (Create)**。

步骤 3 输入唯一的 **配置文件名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 展开 **类型** 下拉菜单，然后选择 **组**。

-
- **说明** - 输入说明以帮助将此配置文件与其他独立配置文件区分开来。
- **类型** - 选择 **组**。

步骤 6 在组详细信息下，为需要添加到配置文件的每个新行点击 **添加** 。

步骤 7 展开每行的下拉菜单，选择要添加到组的配置文件。如果要在保存之前删除配置文件，请选中配置文件的复选框，使其突出显示，然后选择 **删除**。

步骤 8 点击**保存 (Save)**。

下一步做什么

- 查看配置文件详细信息
- 将网关关联添加到配置文件

FQDN（完全限定域名）过滤器配置文件

FQDN 过滤器配置文件评估与流量关联的 FQDN，并应用操作来允许或拒绝流量。要评估 FQDN，流量必须经过 TLS 加密，并在 TLS hello 报头的 SNI 中包含 FQDN。可以为 **转发** 或 **转发代理** 规则处理的流量评估 FQDN。配置文件中的 FQDN 集可以指定为表示完整域的字符串，也可以指定为 Perl 兼容正则表达式 (PCRE) 表示的字符串。如果只需要域过滤，最好使用 FQDN 过滤配置文件。FQDN过滤配置文件也可以与 URL 过滤配置文件结合使用，其中使用 FQDN 过滤配置文件评估域，使用 URL 过滤配置文件评估 URL。

FQDN 过滤配置文件可以使用一组预定义的类别。要查看有关类别的更多信息，请参阅 FQDN/URL 过滤类别。

Note FQDN 过滤配置文件组织为一个表，其中包含用户指定的行（FQDN 和类别）以及两个默认行（未分类和任意）。如果需要，可以在每行中组合类别和 FQDN。

每个 FQDN 过滤器配置文件的限制如下：

- 用户指定的最大行数：254（独立行或独立组）
- 每行的最大类别和 FQDN：60
- 最大 FQDN 字符长度：255

指定多级域（例如，“www.example.com”）时，必须转义 `.` 字符（例如，`www\.example\.com`），否则将被视为通配符任何单个字符。

独立与组

可以将 FQDN 过滤器配置文件指定为独立或组。

独立的 FQDN 过滤器配置文件包含 FQDN 和类别。配置文件将直接应用于一组一个或多个策略规则集或与 FQDN 组配置文件关联。

FQDN 过滤器组配置文件包含独立配置文件的有序列表，这些配置文件可针对不同目的进行定义，并可组合在一起形成组配置文件。组配置文件可以直接应用于一组一个或多个策略规则集。每个团队都可以创建和管理特定的独立配置文件。这些独立配置文件可以组合到一个组配置文件中，以根据使用案例创建层次结构或不同的组合。一个示例组合可以是适用于所有内容的全局 FQDN 列表、适用于每个不同 CSP 的 CSP 特定列表以及适用于每个不同应用的应用特定列表。

未分类

- FQDN 过滤器配置文件中的倒数第二行，表示为 **未分类**。
- 指定要对与用户指定的 FQDN 不匹配或没有类别的 FQDN 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且组配置文件应用于策略规则集，则 **未分类** 行将从组配置文件中获取。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **未分类** 行才适用。

默认 (ANY)

- FQDN 过滤器配置文件中的最后一行，表示为 **ANY**。
- 指定要对与用户指定的 FQDN 或类别不匹配或未分类的 FQDN 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且该组配置文件应用于策略规则集，则将从组配置文件中获取 **ANY** 行。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **ANY** 行才适用。

创建独立 FQDN 过滤器配置文件

使用以下程序创建独立的 FQDN 过滤器配置文件：

步骤 1 导航至 **管理** > **配置文件** > **FQDN 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的配置文件。

步骤 5 将类型指定为 **独立**。

步骤 6 点击 **添加** 以创建新行。

步骤 7 指定单个 FQDN（例如 google.com）。

a) 每个 FQDN 都指定为 PCRE（Perl 兼容正则表达式）。

b) 考虑转义“.”字符，否则将被视为单个字符通配符。

步骤 8 指定 **类别** （例如，赌博、体育、社交网络）。

步骤 9 为用户指定的 FQDN/Categories、Uncategorized 和 ANY 行指定策略 **Action** 。

- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 10 （可选）为不需要或不可能解密的任何 FQDN 指定 **解密例外** 。考虑解密异常的可能原因包括：

- 希望不检查加密流量（金融服务、国防、医疗等）。
- 无法解密的 SSO 身份验证流量。
- 无法代理的 NTLM 流量。

步骤 11 完成后，请点击 **保存** 。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

创建组 FQDN 过滤器配置文件

使用以下程序创建至少包含两个独立配置文件的组 FQDN 过滤器配置文件：

步骤 1 导航至 **管理** > **配置文件** > **FQDN 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分可能具有相似名称的配置文件。

步骤 5 将类型指定为 **组**。

步骤 6 选择初始独立配置文件（至少需要一个独立配置文件）。

步骤 7 点击 **添加 FQDN 配置文件** ，为其他配置文件创建一个新行。

步骤 8 选择独立配置文件。

步骤 9 为未分类的 FQDN 指定策略 **操作** 。

步骤 10 为 **ANY** FQDN 指定策略 **操作** （默认）。

步骤 11 （可选）如果不需要或不可能解密，请为未分类或 ANY 指定 **解密例外** 。考虑解密异常的可能原因包括：

- 希望不检查加密流量（金融服务、国防、医疗等）。
- 无法解密的 SSO 身份验证流量。
- 无法代理的 NTLM 流量。

步骤 12 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

URL（统一资源定位符）过滤器配置文件

URL 过滤配置文件评估 HTTP 请求的 URL 并应用操作来允许或拒绝流量。要评估 URL，必须通过 **转发代理** 规则处理流量。配置文件中的 URL 集可以指定为表示完整路径的字符串，也可以指定为表示 Perl 兼容正则表达式 (PCRE) 的字符串。如果只需要域过滤，最好使用 FQDN 过滤配置文件。FQDN 过滤配置文件也可以与 URL 过滤结合使用，其中使用 FQDN 过滤配置文件评估域，使用 URL 过滤配置文件评估 URL。

URL 过滤配置文件可以使用一组预定义的类别。要查看有关类别的更多信息，请参阅 FQDN/URL 过滤类别。

Note URL 过滤组织为一个表，其中包含用户指定的行（URL 和类别）以及两个默认行（**未分类** 和 **任意**）。如果需要，可以在每行中组合类别和 URL。

每个 URL 过滤配置文件的限制如下：

- 用户指定的最大行数：254（独立行或一组独立行）
- 每行的最大类别和 URL 数：60
- 最大 URL 字符长度：2048

指定多级域（例如，`www.example.com`）时，必须对`.` 字符进行转义（例如，`www\.example\.com`），否则将被视为通配符任何单个字符

未分类

- URL 过滤配置文件中的倒数第二行，表示为 **未分类**。
- 指定对与用户指定的 URL 不匹配或没有类别的 URL 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且组配置文件应用于策略规则集，则**未分类**行将从组配置文件中获取。仅当独立配置文件直接应用于策略规则集时，独立配置文件的**未分类**行才适用。

默认 (ANY)

- URL 过滤配置文件中的最后一行，表示为 **ANY**。
- 指定对与用户指定的 URL 或类别不匹配或未分类的 URL 采取的策略操作。
- 如果在组配置文件中使用独立配置文件，并且该组配置文件应用于策略规则集，则将从组配置文件中获取 **ANY** 行。仅当独立配置文件直接应用于策略规则集时，独立配置文件的 **ANY** 行才适用。

创建 URL 过滤配置文件

使用以下程序创建独立的 URL 过滤配置文件：

步骤 1 导航至 **管理** > **配置文件** > **URL 过滤**。

步骤 2 点击**创建 (Create)**。

步骤 3 请提供唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 点击 **添加** 以创建新行。

步骤 6 指定单个 URL（例如 https://www.google.com）：

- 每个 URL 都指定为 PCRE（Perl 兼容正则表达式）。
- 每个 URL 必须指定为完整路径。
- 考虑转义十进制“”。字符，否则将被视为单个字符通配符。

步骤 7 指定 **类别** （例如，赌博、体育、社交网络）。

步骤 8 指定应用策略的 HTTP 方法。

步骤 9 选择以下方法之一作为方法的子集：

- 删除
- 获取
- 标题
- 选项
- 修补 (Patch)
- Post
- Put

步骤 10 为所有方法指定 **所有** 。

步骤 11 为用户指定的 URL/类别、未分类和任何行指定策略 **操作** ：

- **允许日志** - 允许请求并记录事件。
- **允许无日志** - 允许请求但不记录事件。
- **拒绝日志** - 拒绝请求并记录事件。
- **拒绝无日志** - 拒绝请求且不记录事件。

步骤 12 指定 **退货状态代码**。

步骤 13 指定一个 **大于或等于 100 且小于 600**的整数值。该值表示将返回到发出请求的客户端的 HTTP 状态。常见的返回代码是 **503**。

步骤 14 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

NTP

多云防御网关 使用 NTP 来确保其时间同步。NTP 通过管理接口运行，并配置为用于管理目的的 Linux shell 的一部分。每个 CSP 的 NTP 默认配置略有不同，如下所示：

- **AWS**：`2.centos.pool.ntp.org`， `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP**： `metadata.google.internal`
- **OCI:**`0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`,`3.centos.pool.ntp.org`, `169.254.169.254`

要覆盖默认配置，可以创建NTP配置文件并将其应用于每个网关。将NTP配置文件应用于网关后，将使用新配置。此操作会立即应用。

创建配置文件

使用以下程序创建 NTP 配置文件：

步骤 1 导航至 **管理** > **配置文件** > **NTP**。
步骤 2 点击**创建 (Create)**。
步骤 3 指定唯一的 **名称**。
步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。
步骤 5 指定 NTP 服务器 **列表** 。
步骤 6 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

数据包捕获配置文件

数据包捕获配置文件已配置并与 多云防御网关 关联，并在策略规则、网络威胁配置文件和 Web 保护配置文件中启用。数据包捕获可以捕获流量（PCAP 文件）以及应用和网络威胁（HAR 文件）。

数据包捕获格式

请考虑以下格式规则：

Policy Rule Capture - <bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz

IPS Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz

WAF Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

API Logging - <bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

创建数据包捕获配置文件

使用以下程序创建数据包捕获配置文件：

步骤 1 导航至 **管理** > **配置文件** > **数据包捕获**。

步骤 2 点击**创建 (Create)**。

步骤 3 指定唯一的 **名称**。

步骤 4 （可选）输入**说明 (Description)**。这可能有助于区分具有相似名称的其他配置文件。

步骤 5 指定 **CSP 账户**。

步骤 6 云服务提供商的类型可以确定存储桶的参数。请注意每个云服务提供商的以下要求：

- **AWS** - S3 存储桶。
- **Azure** - 存储帐户名称、博客容器和存储访问密钥。
- **GCP** - 存储桶。

步骤 7 点击**保存 (Save)**。

What to do next

- 查看配置文件详细信息
- 将网关关联添加到配置文件

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。