证书和密钥

证书和密钥

TLS 证书和密钥由 多云防御网关 在代理场景中使用。对于入口（反向代理），用户通过 多云防御网关 访问应用，并提供为服务配置的证书。对于出口（转发代理）情况，外部主机的证书由定义的证书模拟和签名。

证书正文导入到 多云防御控制器。可以通过以下方式提供私钥：

- 导入私钥内容。
- 存储在 AWS 密钥管理器中并提供密钥名称。
- 存储在 AWS KMS 中并提供密文内容。
- 存储在 GCP 密钥管理器中并提供密钥名称。
- 存储在 Azure 密钥保管库和密钥中，并提供密钥保管库和密钥名称。

出于测试目的，您还可以在 多云防御控制器生成自签名证书。这类似于从本地文件系统导入私钥内容。

Note 证书一旦创建便**不可**编辑。如果需要替换现有证书，则需要创建新证书，编辑解密配置文件以引用新证书，然后删除旧证书。

导入证书和私钥时， 多云防御控制器 / UI 可以检测是否存在不匹配。但是，当使用私钥存储在云服务提供商中的任何其他导入方法时， 多云防御控制器 / UI 将无法检测是否存在不匹配。这是为了确保私钥在您的云服务提供商内保持私有。当 多云防御网关需要私钥时，会访问并使用私钥，如果不匹配，则会生成错误。

导入证书

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 当系统提示 **方法**时，选择 **导入证书和私钥**。
步骤 4 复制证书 **正文**中证书文件的内容。这可以包括证书和链。
步骤 5 复制 **证书私钥**中私钥的内容。
步骤 6 （可选）如果您的证书和证书链位于不同的文件中，请将证书链导入 **证书链** 。
步骤 7 点击**保存 (Save)**。

AWS - KMS

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在方法中，选择 导入 *AWS - KMS*。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 复制 私钥密文中的 AWK KMS 加密密文。。
步骤 7 点击**保存 (Save)**。

AWS - 密钥管理器

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在方法中，选择 导入 *AWS* - 秘密。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 提供存储私钥的密钥名称。私钥内容必须在 AWS 密钥管理器中存储为 其他类型的 密钥 > 纯文本 。
步骤 7 点击**保存 (Save)**。

Azure Key Vault

步骤 1 导航至 **管理** > **安全策略** > **证书**。
步骤 2 点击**创建 (Create)**。
步骤 3 在 Method 中，选择 导入 *Azure - Key Vault Secret*。
步骤 4 选择云账户和区域。
步骤 5 将证书文件的内容复制到 证书正文中。这可以包括证书和链。
步骤 6 提供密钥保管库名称和存储私钥的密钥名称。
步骤 7 点击**保存**。

GCP - 密钥管理器

步骤 1 导航至 **管理** > **安全策略** > **证书**
步骤 2 点击**创建**
步骤 3 在方法中，选择 导入 *GCP* - 密钥
步骤 4 选择云帐户
步骤 5 提供密钥名称（完整路径）和密钥版本
步骤 6 将证书文件的内容复制到 证书正文中。这可以包括证书和链
步骤 7 点击**保存 (Save)**。

服务器证书验证

当网关充当转发代理时，服务器证书验证会自动包含在流量处理中。处理流量不需要指定服务器证书验证 **操作**，但它可以提高总体安全性。默认情况下，不启用服务器证书验证，并且流向可能具有无效服务器证书的服务器的流量会通过。启用服务器证书验证操作，以优先处理不应允许的流量或应受信任的特定流量的规则，无论其服务器证书验证状态如何。

注释 此验证过程 **仅** 适用于转发代理环境且已启用 **解密** 。

我们建议主要在 TLS 解密配置文件中为一般规则操作启用服务器证书验证操作。如果需要覆盖 TLS 解密选择，可以修改 FQDN 服务对象以启用验证操作。您可以通过两种方法包括和启用服务器证书验证：

- TLS 解密配置文件中的服务器证书验证

- FQDN 服务对象中的服务器证书验证

TLS 解密配置文件中的服务器证书验证

当您在 TLS 解密配置文件中选择服务器证书验证操作时，此操作将用于使用此解密配置文件的所有规则集中。默认情况下，验证操作配置为允许所有流量，无论服务器证书是否有效，并且 多云防御不会在 HTTPS 日志中生成警报。

注释 如果您对 **日志**启用验证检查，请在 **调查** > **流分析** > **HTTPS 日志中找到这些日志**。

使用以下程序在 TLS 解密配置文件中启用服务器证书验证：

步骤 1 从 多云防御控制器，导航至 **管理** > **配置文件** > **解密**。

步骤 2 选择要向其添加服务器证书验证的 TLS 解密配置文件。如果您没有准备好配置文件，请在此处创建一个。有关详细信息，请参阅解密配置文件。

步骤 3 **编辑** 解密配置文件。

步骤 4 在 **配置文件属性** 部分下，展开 **无效服务器证书操作** 下拉列表。

步骤 5 选择以下选项之一：

- **拒绝日志** - 此选项会自动丢弃未提供经过验证的服务器证书的连接并记录事件。
- **拒绝无日志** - 此选项会自动丢弃未提供经过验证的服务器证书 **且不** 记录事件的连接。
- **允许日志** - 此选项允许未提供经过验证的服务器证书的连接通过并记录事件。
- **允许无日志** - 此选项允许未提供经过验证的服务器证书的连接通过， **并且不** 记录事件。这是默认操作选择。

步骤 6 点击**保存**。

下一步做什么

确保 TLS 解密配置文件与转发代理服务对象正确关联。有关详细信息，请参阅转发代理服务对象（出口/东西向）。

将 TLS 解密配置文件包含在服务对象中后，请确认策略中的规则顺序是否符合您希望的流量处理方式。

FQDN 服务对象中的服务器证书验证

FQDN 服务对象中的**无效服务器证书验证** 是可选的。如果指定，它将覆盖 TLS 解密配置文件中指定的行为。如果未在此处指定选择，则不会执行其他操作或覆盖操作。您可以使用 FQDN 服务对象中的无效服务器证书验证来阻止或允许 TLS 解密配置文件可能阻止或允许的特定服务器的流量。

请注意，当您对 **Log**启用验证检查时，这些日志将位于 **Investigate** > **Flow Analytics** > **HTTPS Logs** 中。

使用以下程序在 FQDN 服务对象中包含服务器证书验证操作：

步骤 1 在 多云防御控制器中，导航至 **管理** > **安全配置文件** > **FQDN**。

步骤 2 选择要修改的 FQDN 服务对象。

步骤 3 **编辑** 所选的 FQDN 服务对象。

步骤 4 在规则集中包含的 FQDN 服务对象列表中，展开 **服务器证书操作无效** 下拉菜单，然后选择以下选项之一：

- **拒绝日志** - 自动丢弃未提供经过验证的服务器证书的连接并记录事件。
- **拒绝无日志** - 自动丢弃未提供经过验证的服务器证书 **且不** 记录事件的连接。
- **允许日志** - 允许未提供经过验证的服务器证书的连接通过并记录事件。
- **允许无日志** - 允许未提供经过验证的服务器证书的连接通过 **且不** 记录事件。

步骤 5 点击**保存**。

下一步做什么

确保 FQDN 服务对象与规则或规则集正确关联。有关详细信息，请参阅规则集和规则集组。

成功将 FQDN 服务对象与策略中的规则或规则集相关联后，请确认策略中的规则顺序是否支持您希望的流量处理方式。

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。