

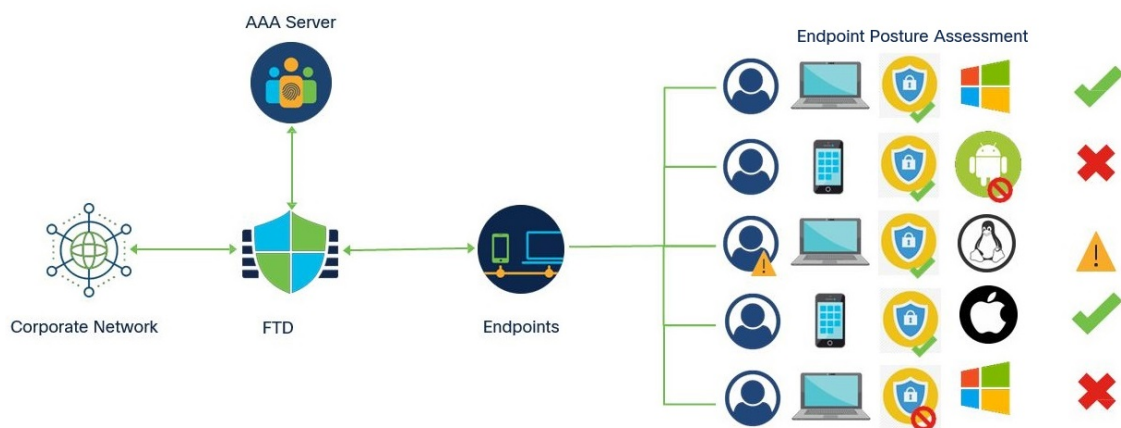
# 思科 Firepower 威胁防御动态访问策略使用案例

## 思科 Firepower 威胁防御动态访问策略

DTD 上的 DAP 允许您配置授权以解决 VPN 环境的动态问题。您可以使用 Firepower 管理中心 (FMC) Web 界面通过配置一系列的访问控制属性来创建 DAP。您可以将属性与特定用户隧道或会话相关联。这些属性可解决多重组成员身份和终端安全的问题。

FTD 会根据您的 DAP 配置向特定用户会话授予 VPN 访问权限。FTD 从一个或多个 DAP 记录中选择并汇聚属性，然后在用户身份验证期间生成 DAP。FTD 会根据远程设备的端点安全信息和 AAA 信息来选择 DAP 记录。然后，FTD 会将 DAP 记录应用至用户隧道或会话。

图 1: 动态访问策略示例



## FTD 远程访问 VPN 如何与 DAP 配合使用

1. 远程用户可尝试从终端设备使用 AnyConnect 安全移动客户端进行 VPN 连接。
2. FTD 对终端执行安全评估。
3. FTD 通过身份验证、授权和记帐服务器对用户进行身份验证。AAA 服务器还会返回用户的授权属性。
4. FTD 将 AAA 授权属性应用至会话并建立 VPN 隧道。
5. FTD 根据用户 AAA 授权信息和终端安全评估信息选择 DAP 记录。
6. FTD 汇聚选定 DAP 记录中的 DAP 属性，并创建 DAP 策略。

7. FTD 将 DAP 策略应用至远程访问 VPN 会话。

## 为什么实施 DAP?

您可以配置 DAP 属性来识别连接终端并授权用户访问各种网络资源。您可以为以下场景创建 DAP，并且可以使用 DAP 属性来执行更多操作，以保护终端和网络资源：

- 确保连接到 VPN 的终端遵守组织的安全策略，无论终端设备或平台如何。
- 识别操作系统、终端上运行的各种安全软件、注册表设置、文件版本以及终端上运行的潜在按键记录器。
- 检测并实施公司托管终端上应用的可用性和更新。例如，防病毒软件
- 确定授权用户可以访问的网络资源。

## DAP 配置的组件

新的 DAP 配置需要创建 DAP 策略、DAP 记录和 DAP 条件属性：

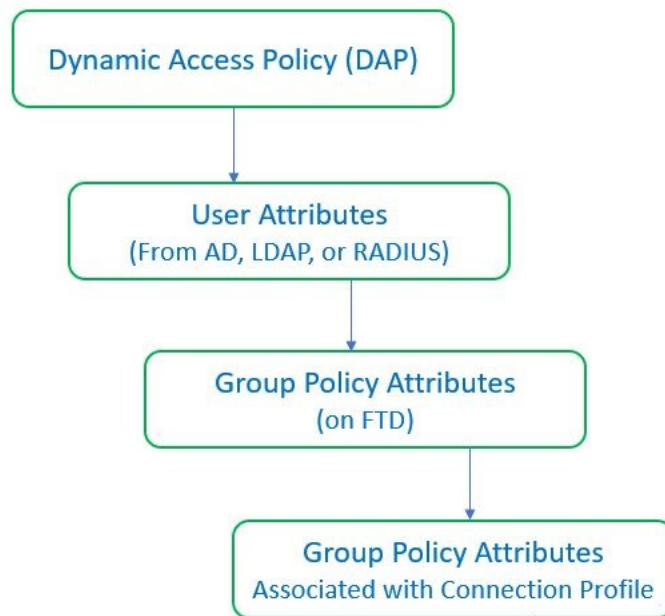
- **动态访问策略 (Dynamic Access Policy)** - DAP 配置由记录组成。
- **DAP 记录 (DAP Record)** - DAP 记录包含标准终端评估和用户授权 (AAA) 属性。如果记录匹配，则 DAP 会定义要在 VPN 会话上应用的操作。
- **DAP 标准和属性 (DAP Criteria and Attributes)** - AAA 条件、终端条件和高级条件包含用于网络访问的精细配置属性。

## FTD 中权限和属性的策略实施

FTD 设备支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接。从 FTD 上的 DAP、外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或从 FTD 设备上的组策略应用属性。

如果 FTD 设备收到来自所有来源的属性，则 FTD 会评估、合并，并将它们应用于用户策略。如果来自 DAP、AAA 服务器或组策略的属性之间发生冲突，从 DAP 获得的属性始终会被优先考虑。

图 2: 策略实施流程



1. **FTD 上的 DAP 属性** - DAP 属性优先于所有其他的属性。
2. **外部 AAA 服务器上的用户属性** - 该服务器在用户身份验证和/或授权成功后返回这些属性。
3. **FTD 上配置的组策略** - 如果 RADIUS 服务器为用户返回 RADIUS 类属性 IETF-Class-25 (OU=group-policy) 值，FTD 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
4. **连接配置文件 (也称为隧道组) 分配的组策略** - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。



**注释** FTD 设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。如果没有被用户属性或 AAA 服务器的组策略覆盖，则从连接配置文件中分配的组策略属性将用于用户会话。

## 动态访问策略许可

FTD 必须具有支持远程访问 VPN 的 AnyConnect 许可证之一：

- AnyConnect Apex
- AnyConnect Plus
- AnyConnect VPN Only

FMC 必须启用导出控制功能。

## 配置动态访问策略

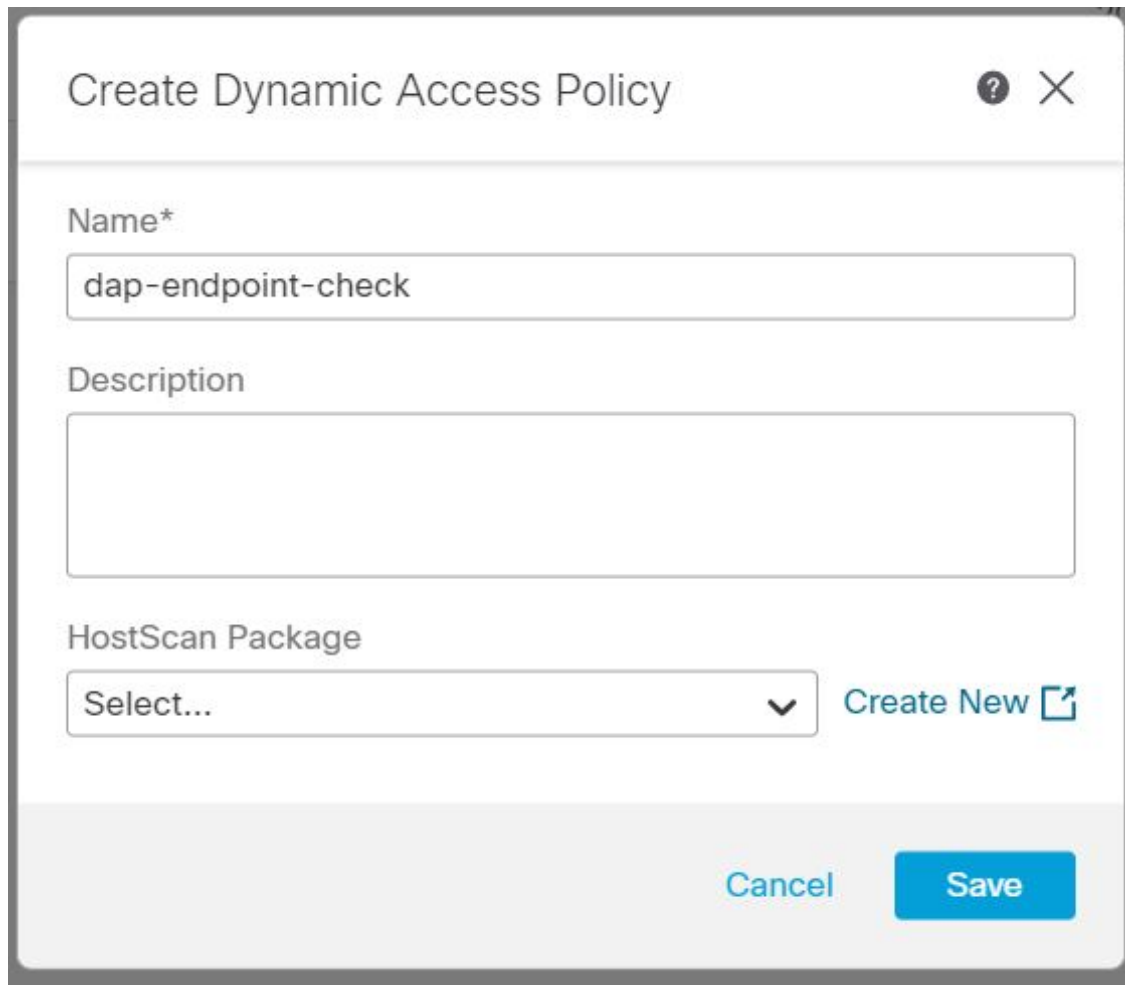
动态访问策略 (DAP) 可以包含多个 DAP 记录，您可以在这些记录中配置用户和终端属性。您可以确定 DAP 记录的优先级，以便在用户尝试 VPN 连接时应用所需的条件。

### 开始之前

确保在创建动态访问策略 (DAP) 之前配置所需的应用程序和设置：

- **HostScan 软件包 (HostScan Package)** - 下载 4.6 或更高版本的 HostScan 软件包。
  - **AAA 服务器 (AAA Server)** - 配置所需的 AAA 服务器，以便在对 VPN 会话进行身份验证或授权时返回正确的属性。
  - **AnyConnect 客户端软件包 (AnyConnect Client Package)** - 下载最新版本的思科 AnyConnect 安全移动客户端并将其添加到您的远程访问 VPN 配置。
  - **远程访问 VPN (Remote Access VPN)** - 使用设备 (**Devices**) > VPN > 远程访问 (**Remote Access**) 下的远程访问 VPN 配置向导来配置远程访问 VPN 的设置。
  - 在对象 (**Objects**) > 对象管理 (**Object Management**) > VPN > AnyConnect 文件 (**AnyConnect File**) 中上传 HostScan 软件包。
1. 配置新的动态策略（如果尚未配置）。
    - a) 依次选择设备 (**Devices**) > 动态访问策略 (**Dynamic Access Policy**) > 创建动态访问策略 (**Create Dynamic Access Policy**)。

图 3: 创建动态访问策略



The screenshot shows a 'Create Dynamic Access Policy' dialog box. The title bar includes a help icon (question mark) and a close icon (X). The form contains the following fields and controls:

- Name\***: A text input field containing the value 'dap-endpoint-check'.
- Description**: A large, empty text area for providing details about the policy.
- HostScan Package**: A dropdown menu currently showing 'Select...' with a downward arrow, and a 'Create New' button with an external link icon.
- Buttons**: 'Cancel' and 'Save' buttons are located at the bottom right of the dialog.

b) 为 DAP 策略指定名称 (**Name**) 和可选的说明 (**Description**)。

c) 从下拉列表中选择 **HostScan** 软件包 (**HostScan Package**)；或单击新建 (**Create New**) 以添加 HostScan 软件包文件。

动态访问策略包含默认的 DAP 记录。您可以使用 Lua 脚本开始在 AAA 条件、终端条件和高级条件下添加包含所需属性的 DAP 记录。

d) 单击保存 (**Save**)。

## 2. 创建 DAP 记录，然后分配优先级编号。

DAP 记录包含用于在 VPN 用户尝试与 FTD VPN 网关建立 VPN 连接时进行匹配的属性。您可以根据所选条件属性使用 DAP 记录来设置授予、拒绝或限制 VPN 访问。

**优先级 (Priority)** 数字表示记录匹配的顺序。FTD 使用 DAP 记录的优先级编号来对记录进行排序和选择。数值越低，优先级越高。



注释 如果没有为 DAP 配置 DAP 记录，则会应用默认 DAP 记录。默认 DAP 记录没有优先级。

- 依次选择设备 (Devices) > 动态访问策略 (Dynamic Access Policy)。
- 编辑现有的 DAP 策略或创建一个新策略。
- 单击创建 DAP 记录 (Create DAP Record)。

The screenshot shows the configuration page for a Dynamic Access Policy (DAP) record. The 'General' tab is active. The 'Name' field is set to 'check-antivirus' and the 'Priority' is set to '2'. Under the 'Action' section, the 'Continue' button is selected. The 'Display User Message on Criterion Match' checkbox is checked, and a text box contains the message: 'Your anti-virus software is out-of-date. Update recommended.' Below this, there are two sections for applying ACLs and custom attributes, both currently unchecked.

- 指定 DAP 记录的名称 (Name)。
- 输入 DAP 记录的优先级 (Priority) 编号。
- 选择在 DAP 记录匹配时要执行的操作 (Action):
  - 继续 (Continue) - 单击以将访问策略属性应用于会话并允许用户。
  - 终止 (Terminate) - 选择以终止会话。
  - 隔离 (Quarantine) - 选择以隔离连接。
- 选择在条件匹配时显示用户消息 (Display User Message on Criterion Match) 并在框中添加消息。



注释 VPN 用户会在 DAP 记录匹配时收到消息。

- h) 选中对流量应用网络 ACL (**Apply a Network ACL on Traffic**) 复选框，然后从列表中选择 ACL。您还可以创建一个新的 ACL，然后选择它。

当此 DAP 记录匹配时，网络 ACL 将应用于 VPN 会话。

- i) 选择应用一个或多个 **AnyConnect** 自定义属性 (**Apply one or more AnyConnect Custom Attributes**)，然后从下拉列表中选择自定义属性对象。
- j) 单击**保存 (Save)**。

有关网络 ACL 和 AnyConnect 自定义属性的信息，请参阅最新的《[Firepower 管理中心配置指南](#)》。

- k) 配置 DAP 属性以检查用户和终端何时连接到 VPN。

- [配置 DAP 的 AAA 标准设置，第 8 页](#)
- [配置 DAP 中的终端属性选择条件，第 9 页](#)
- [配置 DAP 的高级设置，第 11 页](#)

### 3. 将 DAP 与远程访问 VPN 配置关联起来。

您必须将 DAP 与远程访问 VPN 策略相关联，才能在 VPN 会话身份验证或授权期间匹配 DAP 属性。

- a) 在 Firepower 管理中心 Web 界面上，依次选择**设备 (Devices) > VPN > 远程访问 (Remote Access)**。
- b) 选择并编辑要添加 DAP 的远程访问策略。
  - a) 单击动态访问策略关联链接。
  - b) 从列表选择**动态访问策略 (Dynamic Access Policy)**。
  - c) 单击**确定 (OK)**。

将 DAP 关联到远程访问 VPN 后，FTD 会在用户尝试 VPN 连接时检查配置的 DAP 记录和属性。FTD 会根据匹配情况来创建 DAP，并对 VPN 会话采取适当的操作。

### 4. 在 FTD 设备上部署远程访问 VPN。

- a) 在 Firepower 管理中心菜单栏中，单击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

您可以查看 FTD 设备上所有待部署的过期配置列表。
- b) 识别并选择要部署远程访问 VPN 和其他配置更改的设备。
- c) 单击**部署 (Deploy)**。



注释 在部署配置之前纠正任何错误。

## 配置 DAP 的 AAA 标准设置

FTD 使用 AAA 服务器附加到 VPN 会话的 AAA 属性来匹配用户或用户组。

DAP 可提供一组限定的授权属性，这些属性可覆盖 AAA 提供的属性，从而补充 AAA 服务。FTD 会根据 AAA 授权信息和 VPN 会话的终端安全评估信息来选择 DAP 记录。FTD 可根据评估来选择多个 DAP 记录，然后将其汇聚以创建 DAP 授权属性。

### 开始之前

确保已为 VPN 用户身份验证、授权和记帐配置了所需的 AAA 服务器。必须从要部署远程访问 VPN 的 Firepower Threat Defense 设备访问 AAA 服务器。

### 过程

**步骤 1** 依次选择设备 (**Devices**) > 动态访问策略 (**Dynamic Access Policy**)。

**步骤 2** 编辑现有 DAP 策略或创建新的 DAP 策略，然后编辑该策略。

**步骤 3** 选择 DAP 记录或创建新记录，然后编辑 DAP 记录。

**步骤 4** 单击 AAA 条件 (**AAA Criteria**)。

Type	Op.	Value
Group Policy	≠	general-admin-team
	=	finance-user-group

Type	Op.	Value
memberOf	=	finance

**步骤 5** 选择部分之间匹配条件 (**Match criteria between sections**) 之一：

- 任意 (**Any**) - 匹配任何条件。



- **全部 (All)** - 匹配所有设定的条件。
- **无 (None)** - 不匹配任何设定的条件。

**步骤 6** 单击添加 (**Add**) 以添加所需的思科 VPN 条件。

思科 VPN 条件包括组策略的预定义属性、分配的 IPv4 地址、分配的 IPv6 地址、连接配置文件、用户名、用户名 2 和所需的 SCEP。

- a) 选择属性 ID (**Attribute ID**) 和运算符，然后指定要匹配的值 (**Value**)。
- b) 单击添加其他条件 (**Add another criteria**) 以添加更多 AAA 条件。
- c) 单击保存 (**Save**)。

**步骤 7** 选择 **LDAP 条件 (LDAP Criteria)**、**RADIUS 条件 (RADIUS Criteria)** 或 **SAML 条件 (SAML Criteria)**。指定属性 ID (**Attribute ID**) 和值 (**Value**)。

可以将这些属性设置为所输入的 = 或  $\neq$  值。您可以为每个 DAP 记录添加任意数量的 AAA 属性。

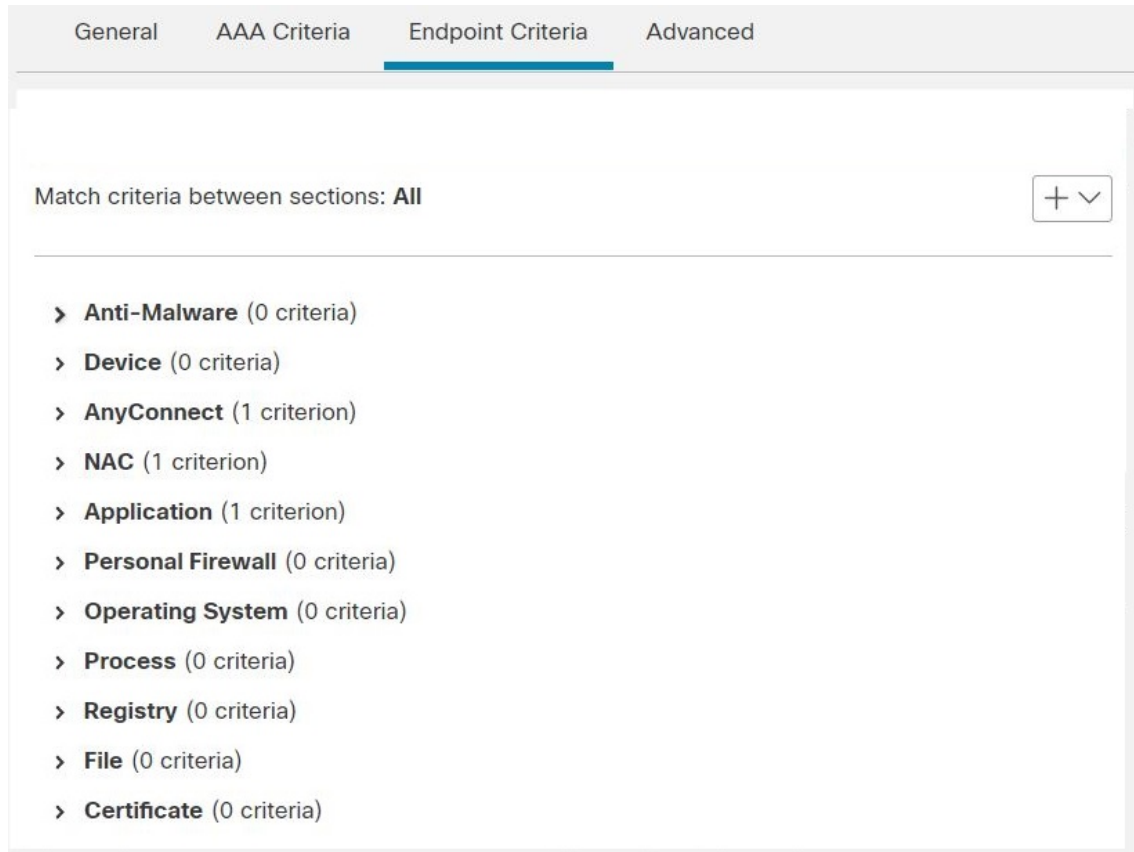
**步骤 8** 单击保存 (**Save**)。

---

## 配置 DAP 中的终端属性选择条件

终端属性包含终端系统环境、终端安全评估结果和应用的相关信息。FTD 会在会话建立期间动态生成终端属性的集合，并将这些属性存储在与此会话关联的数据库中。每个 DAP 记录指定终端选择属性，这些属性必须得到满足，FTD 才能选择将其用于会话。FTD 仅选择满足每个配置的条件 DAP 记录。

图 4. DAP 终端属性



## 过程

**步骤 1** 依次选择设备 (**Devices**) > 动态访问策略 (**Dynamic Access Policy**) > 创建动态访问策略 (**Create Dynamic Access Policy**)。

**步骤 2** 编辑 DAP 策略，然后编辑 DAP 记录。

注释 创建 DAP 策略和 DAP 记录（如果尚未创建）。

**步骤 3** 单击终端条件 (**Endpoint Criteria**) 并从以下属性类型中配置所需的终端条件属性：

- 防恶意软件
- 设备
- AnyConnect
- NAC
- 应用
- 防火墙

- 操作系统
- 过程
- 注册表
- 文件
- 证书

**注释** 您可以创建每个终端属性类型的多个实例。您还可以为每个 DAP 记录添加任意数量的终端属性。

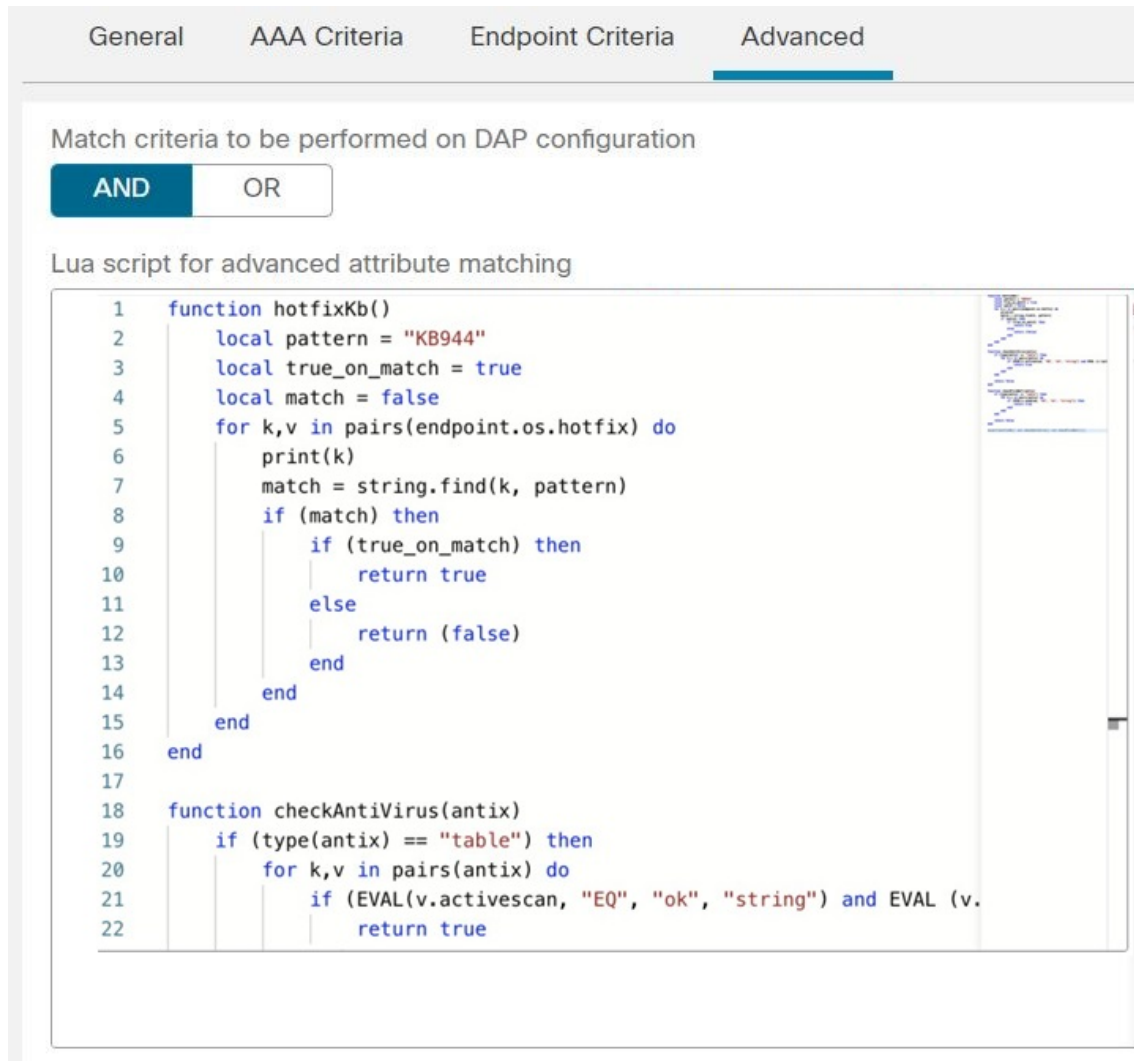
**步骤 4** 单击保存 (Save)。

---

## 配置 DAP 的高级设置

您可以使用“高级”(Advanced)选项卡来添加除 AAA 和端点属性区域中可能存在的选择条件。在 Lua 中创建适当的逻辑表达式并在此处输入。

图 5: 使用 Lua 脚本的高级条件匹配



## 过程

**步骤 1** 依次选择设备 (Devices) > 动态访问策略 (Dynamic Access Policy)。

**步骤 2** 编辑 DAP 策略，然后编辑 DAP 记录。

注释 创建 DAP 策略和 DAP 记录（如果尚未创建）。

**步骤 3** 选择 AND 或 OR 作为要在 DAP 配置上进行匹配的匹配条件。

**步骤 4** 添加用于高级属性匹配的 Lua 脚本 (Lua script for advanced attribute matching)。

**步骤 5** 单击保存 (Save)。

## 动态访问策略故障排除

在排除 DAP 问题之前：

- 在平台设置策略中启用 VPN 系统日志。
- 检查设备 (Devices) > VPN > 故障排除 (Troubleshooting) > 下的 DAP 相关日志。

### 问题 1：无法保存 DAP 配置

#### 解决方案

如果您无法从 FMC Web 界面保存 DAP 配置，请检查相应的日志以查找失败原因：

- /var/opt/CSCOPx/MDC/log/operation/vmssharedsvcs.log.\*
- /var/opt/CSCOPx/MDC/log/operation/usmsharedsvcs.log.\*

您可以使用关键字 `vpn` 或 `sso` 来过滤相关日志。

### 问题 2：DAP 部署失败

#### 解决方案：

如果 DAP 部署失败，请检查部署脚本详细信息，然后检查日志文件  
/var/opt/CSCOPx/MDC/log/operation/vmsbesvcs.log.\*

## 动态访问策略的示例

本节提供允许或阻止 VPN 用户及其终端的 VPN 访问的动态访问策略 (DAP) 配置示例。



#### 注释

本文档中提供的说明是示例配置。您可以根据自己的需要使用各种 DAP 设置来配置单个 DAP 记录或多个 DAP 记录。DAP 设置包括使用 Lua 脚本的 AAA 条件、终端条件和高级设置下的属性。

根据您的安全要求，您可以为多个条件匹配配置单个 DAP 记录，或者创建多个 DAP 记录并根据需要来确定它们的优先级。

## 允许或阻止基于操作系统的 VPN 访问

您可以根据操作系统决定终端的 VPN 访问。使用此处的示例来阻止运行 Windows 操作系统版本 7 且不使用服务包 SP1 便捷汇总的终端。

## 过程

- 步骤 1 创建 DAP 记录或使用终止 (Terminate) 操作编辑现有记录。
- 步骤 2 选择终端条件 (Endpoint Criteria) > 操作系统 (Operating System)。
- 步骤 3 选择匹配条件全部 (All) 以仅在所有配置的属性匹配时选择条件。
- 步骤 4 单击添加 (Add) 以添加操作系统属性。

图 6: DAP 操作系统终端条件

- 步骤 5 选择操作系统 (Operating System) 等于 (=) 运算符，然后选择 Windows 7。
- 步骤 6 选择服务包 (Service Pack) 不等于 (≠) 操作符，然后指定 SP1 便捷汇总 (SP1 Convenience Rollup)。
- 步骤 7 单击保存 (Save)。

## 根据终端上的防恶意软件属性阻止流量

此处列出的步骤允许您配置防恶意软件属性，以便在终端尝试连接到 VPN 时进行检查。您可以使用 DAP 记录属性来检查，

- 终端是否已安装思科面向终端的 AMP 并启用实时扫描。
- 如果面向终端的思科 AMP 的版本高于 1.1，并且防恶意软件会在 15 天内更新。

有关在 FTD 上配置 DAP 的详细说明，请参阅[配置动态访问策略](#)，第 4 页。

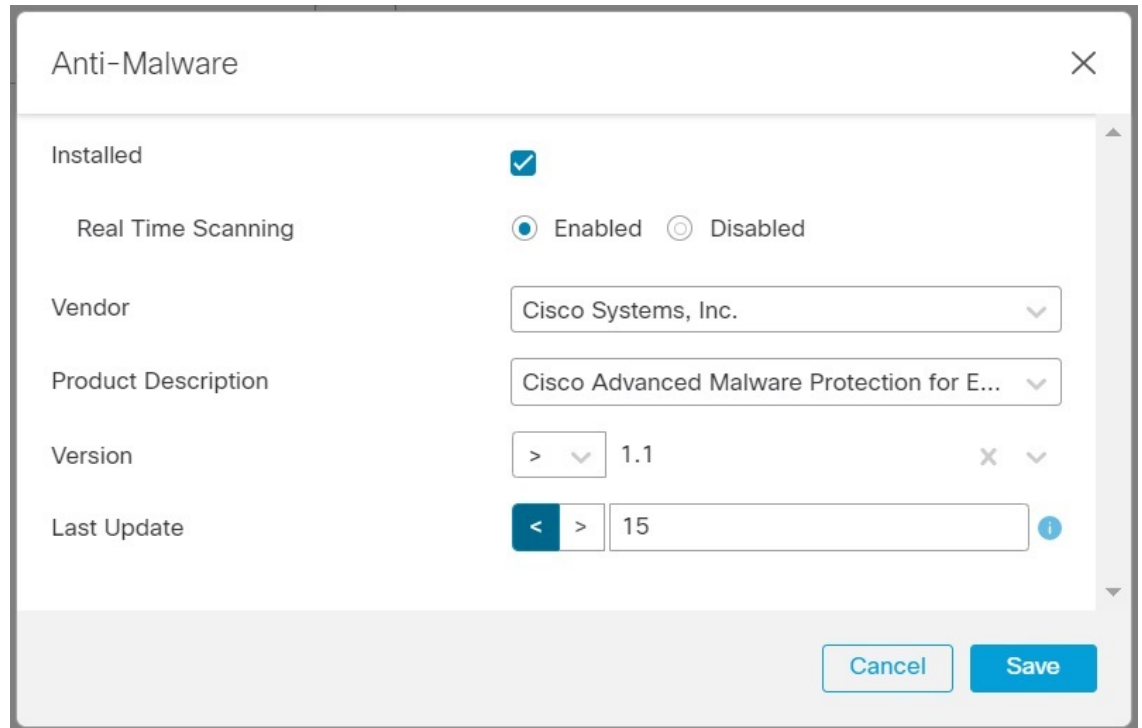
## 过程

- 步骤 1 使用终止 (Terminate) 操作创建 DAP 记录或编辑现有 DAP 记录。
- 步骤 2 在 DAP 记录中选择终端标准 (Endpoint Criteria) > 防恶意软件 (Anti-Malware)。

**步骤 3** 选择匹配条件**全部 (All)** 以仅在所有配置的属性匹配时选择条件，或选择**任意 (Any)** 以在任何属性匹配时选择条件。

**步骤 4** 单击**添加 (Add)** 以添加防恶意软件属性。

图 7: DAP 防恶意软件终端标准



**步骤 5** 单击**已安装 (Installed)** 以指明是否已安装防恶意软件产品。

**步骤 6** 选择**已启用 (Enabled)** 以检查实时恶意软件扫描是否处于活动状态。

**步骤 7** 从列表中选择防恶意软件供应商的名称。

对于本示例，请选择 *Cisco Systems, Inc.* 作为面向终端的思科 AMP 的供应商。选择您所选的供应商。

**步骤 8** 依次选择防恶意软件产品说明 (**Product Description**)、面向终端的思科高级恶意软件防护 (*Cisco Advanced Malware Protection for Endpoints*)。

注释 根据连接到 VPN 的终端上运行的防恶意软件产品来选择其他供应商和产品。

**步骤 9** 选择**版本 (Version)** 高于 1.1 的防恶意软件产品。

**步骤 10** 指定距离上次更新 (**Last Update**) 的天数。

表示防恶意软件更新时间必须小于 (<) 15 天。

**步骤 11** 单击**保存 (Save)**。

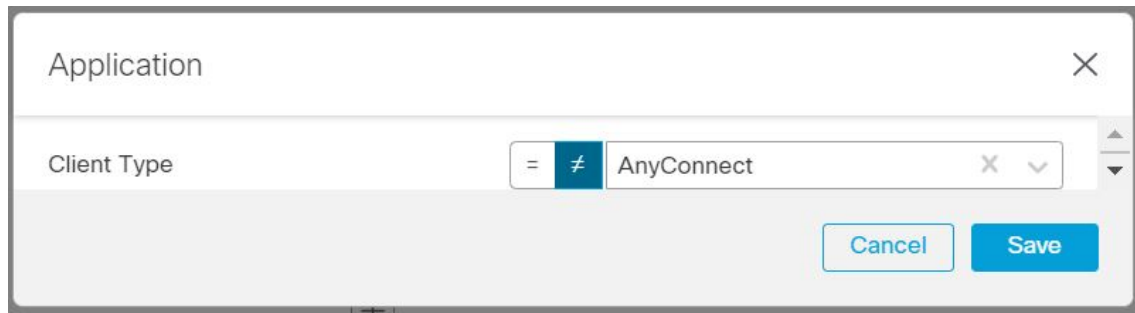
## 允许或阻止远程访问应用程序的 VPN 访问

要检查远程访问连接的类型以允许或拒绝用户的 VPN 访问，请在 DAP 记录中使用应用终端条件。

### 过程

- 步骤 1 根据需要，使用继续 (Continue) 或终止 (Terminate) 操作来创建 DAP 记录或编辑现有记录。
- 步骤 2 选择终端条件 (Endpoint Criteria) > 应用程序 (Application)。
- 步骤 3 选择匹配条件全部 (All) 以仅在所有配置的属性匹配时选择条件，或选择任意 (Any) 以在任何属性匹配时选择条件。
- 步骤 4 单击添加 (Add) 以添加操作系统属性。

图 8. DAP 应用终端条件



注释 您可以使用该示例来允许或阻止使用 AnyConnect 应用连接的 VPN 用户。

您可以仅选择要检查的项目，并输入所需的值。您还可以选择将设备检查与具有多个终端或 AAA 标准的另一个 DAP 记录相结合。

- 步骤 5 选择等于 (=) (=) 或不等于 (≠) 运算符，然后选择远程访问客户端类型 (Client Type)。

列出的客户端类型包括无客户端、直接转发代理、AnyConnect、IPsec、L2TP 和 IPsec-IKEv2-Generic-RA。

- 步骤 6 单击保存 (Save)。

## 选中终端设备以允许或屏蔽 VPN 访问

您可以创建 DAP 条件以允许或阻止特定设备的 VPN 访问。配置设备详细信息，以便在用户尝试 VPN 连接时进行检查。

### 过程

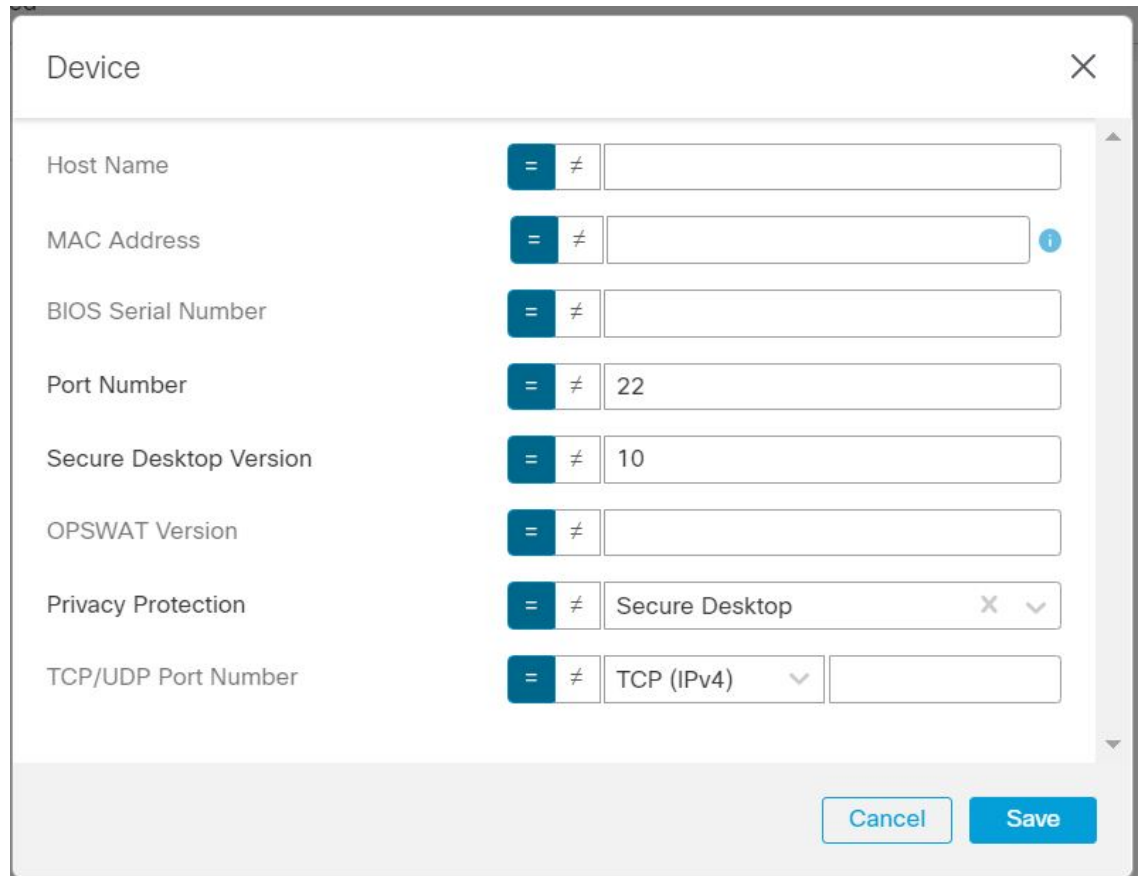
- 步骤 1 根据需要，使用继续 (Continue) 或终止 (Terminate) 操作来创建 DAP 记录或编辑现有记录。
- 步骤 2 选择终端标准 (Endpoint Criteria) > 设备 (Device)。



**步骤 3** 选择匹配条件全部 (**All**) 以仅在所有配置的属性匹配时选择条件，或选择任意 (**Any**) 以在任何属性匹配时选择条件。

**步骤 4** 单击添加 (**Add**) 以添加操作系统属性。

图 9: DAP 设备终端条件示例



**注释** 使用该示例允许或阻止通过端口 22、安全桌面版本 10 和隐私保护安全桌面连接的终端。您可以仅选择要检查的项目，然后输入所需的值。您还可以选择将设备检查与具有多个终端或 AAA 标准的另一个 DAP 记录相结合。

**步骤 5** 选择等于 (=) 或不等于 (≠) 运算符，然后指定设备信息。选择必填字段并输入主机名、MAC 地址、BIOS 序列号、端口号、安全桌面版本和 OPSWAT 版本的值。

**步骤 6** 选择等于 (=) 或不等于 (≠) 运算符，然后选择隐私保护和 TCP/UDP 端口号。

**步骤 7** 单击保存 (**Save**)。

## 使用 Lua 脚本来检查终端上的防恶意软件

本节中显示的配置示例提供了检查终端上是否存在防恶意软件产品所需的 Lua 脚本。

要使用 Lua 脚本构建逻辑表达式，则需要了解 LUA。您可以在 <http://www.lua.org/manual/5.1/manual.html> 找到有关 LUA 编程的详细信息。

有关详细信息，请参阅《Firepower 管理中心配置指南》的《Firepower 威胁防御动态访问策略部分》。

## 过程

---

**步骤 1** 创建 DAP 记录或编辑现有 DAP 记录。

**步骤 2** 单击 DAP 记录中的高级 (Advanced)。

**步骤 3** 选择匹配条件 AND 或 OR。

**步骤 4** 将以下脚本复制到 Lua 脚本区域：

```
assert(function()  
local am_count = 0;  
CheckAndMsg( true, "endpoint.av"..type(endpoint.am), nil)  
for k,v in pairs(endpoint.am) do  
am_count = am_count + 1  
-- CheckAndMsg( true, "v.exists"..v.exists, nil)  
-- CheckAndMsg( true, "v.description"..v.description, nil)  
-- CheckAndMsg( true, "v.version"..v.version, nil)  
-- CheckAndMsg( true, "v.activescan"..v.activescan, nil)  
end  
CheckAndMsg( true, "Your request has "..am_count.." Ams", nil)  
return true  
end)()
```

**步骤 5** 单击保存 (Save)。

---

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. 保留所有权利。