



动态访问策略

动态访问策略(DAP)让您能够配置解决VPN环境动态问题的授权。您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。

- [关于 Cisco Secure Firewall Threat Defense 动态访问策略，第 1 页](#)
- [动态访问策略许可，第 3 页](#)
- [动态访问策略的必备条件，第 3 页](#)
- [动态访问策略的准则与限制，第 3 页](#)
- [配置动态访问策略\(DAP\)，第 4 页](#)
- [将动态访问策略与远程访问 VPN 关联，第 12 页](#)
- [动态访问策略的历史记录，第 12 页](#)

关于 Cisco Secure Firewall Threat Defense 动态访问策略

VPN 网关在动态环境下运行。多个变量可能会影响每个 VPN 连接。例如，频繁更改内联网配置、每个用户在组织中可能有不同的角色，以及使用不同配置和安全级别从远程访问站点尝试登录。相比采用静态配置的网络，授权用户的任务在 VPN 环境中更为复杂。

您可以设置一个与特定用户隧道或会话关联的访问控制属性集合，从而创建动态访问策略。这些属性可解决多重组成员身份和终端安全的问题。威胁防御会根据您定义的策略，为特定的会话向特定用户授予访问权限。威胁防御设备会通过从一个或多个 DAP 记录中选择或汇总属性，从而在用户身份验证期间生成 DAP。然后，设备会根据远程设备的终端安全信息，以及经过身份验证的用户的 AAA 授权信息，选择这些 DAP 记录。然后，设备会将 DAP 记录应用至用户隧道或会话。

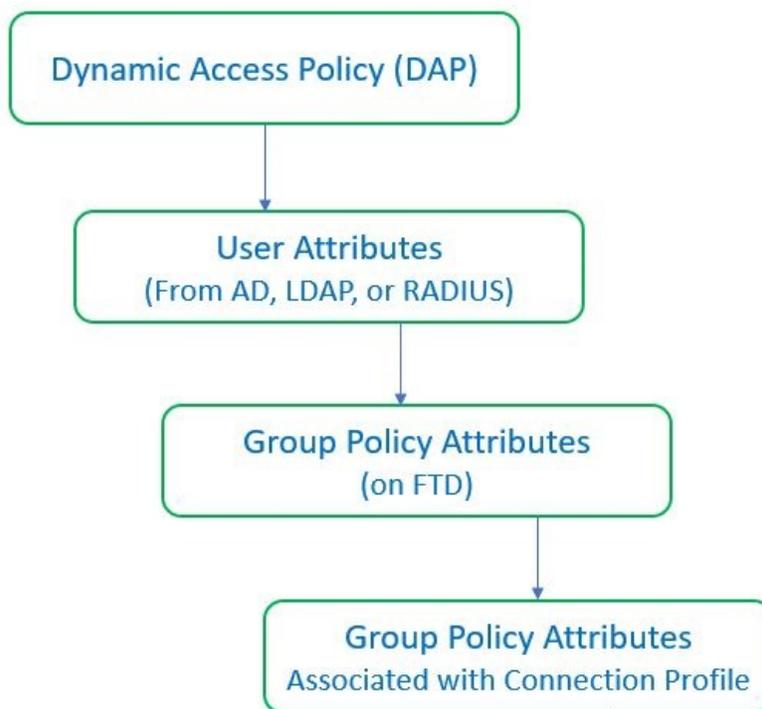
威胁防御 中权限和属性的策略实施层次结构

威胁防御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。从威胁防御上的 DAP、外部身份验证服务器和/或授权 AAA 服务器 (RADIUS) 或从威胁防御设备上的组策略应用属性。

如果威胁防御设备收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果来自 DAP、AAA 服务器或组策略的属性之间存在冲突，从 DAP 获得的属性始终会被优先考虑。

威胁防御设备按照以下顺序应用属性：

图 1: 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，威胁防御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

威胁防御设备不支持从默认组策略 *DfltGrpPolicy* 继承系统默认属性。对于用户会话，设备会使用您分配给连接配置文件的组策略上的属性，除非它们被来自 AAA 服务器的用户属性或组策略覆盖。

动态访问策略许可

威胁防御必须具有以下AnyConnect 客户端许可证之一：

- AnyConnect Apex
- AnyConnect Plus
- 仅限 AnyConnect VPN

基本许可证必须允许出口控制功能。

动态访问策略的必备条件

表 1:

前提条件类型	说明
许可	<ul style="list-style-type: none"> • 威胁防御 必须至少拥有以下 AnyConnect 客户端 许可证之一： <ul style="list-style-type: none"> • AnyConnect Apex • AnyConnect Plus • 仅限 AnyConnect VPN • 威胁防御 基本许可证必须允许出口控制功能。
配置	<p>有关前提条件的详细信息，请参阅《Firepower 管理中心配置指南》中的 <i>Cisco Secure Firewall Threat Defense</i> 动态访问策略部分。</p> <p>有关远程访问 VPN 必备条件和配置的详细信息，请参阅《Firepower 管理中心配置指南》的 <i>Cisco Secure Firewall Threat Defense</i> 远程访问 VPN 部分。</p>

动态访问策略的准则与限制

- 只有当 AAA 服务器被配置为在对远程接入 VPN 会话进行身份验证或授权时返回正确的属性时，才能匹配 DAP 中的 AAA 属性。

- DAP 支持的最低 AnyConnect 和 HostScan 软件包版本为 4.6。但是强烈建议使用最新版本的 AnyConnect。

配置动态访问策略 (DAP)

创建动态访问策略

开始之前

在配置动态访问策略之前，请确保您拥有 HostScan 软件包。您可以通过 **对象 (Objects) > 对象管理 (Object Management) > VPN > AnyConnect 文件 (AnyConnect File)** 来添加 HostScan 文件。

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** 为 DAP 策略指定名称 (**Name**) 和可选的说明 (**Description**)。
 - 步骤 3** 从列表中选择 **HostScan** 软件包 (**HostScan Package**)。
 - 步骤 4** 点击保存。

下一步做什么

要配置 DAP 记录，请参阅[创建动态访问策略记录](#)

创建动态访问策略记录

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 内的 DAP 记录的优先级，以便威胁防御 在用户尝试 VPN 连接时选择和排序所需的条件。

过程

-
- 步骤 1** 依次选择设备 (**Devices**) > 动态访问策略 (**Dynamic Access Policy**)。
 - 步骤 2** 编辑现有动态访问策略或创建新策略，然后编辑该策略。
 - 步骤 3** 指定 DAP 记录的名称 (**Name**)。
 - 步骤 4** 为 DAP 记录输入优先级 (**Priority**)。
数值越低，优先级越高。
 - 步骤 5** 选择当 DAP 记录匹配时要执行的以下操作之一：

- **继续 (Continue)** - 点击以将访问策略属性应用于会话。
- **终止 (Terminate)** - 选择以终止会话。
- **隔离 (Quarantine)** - 选择以隔离连接。

步骤 6 选中在条件匹配时显示用户消息 (**Display User Message on Criterion Match**) 复选框并添加用户消息。

当 DAP 记录匹配，威胁防御 将此消息显示给用户。

步骤 7 选中对流量应用网络 ACL (**Apply a Network ACL on Traffic**) 复选框，然后从下拉列表中选择访问控制列表。

步骤 8 选中应用一个或多个 AnyConnect 自定义属性 (**Apply one or more AnyConnect Custom Attributes**) 复选框，然后从下拉列表中选择自定义属性对象。

步骤 9 点击保存 (**Save**)。

配置 DAP 的 AAA 标准设置

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。威胁防御 会根据用户的 AAA 授权信息和会话的终端安全评估信息选择 DAP 记录。威胁防御 可根据此信息选择多个 DAP 记录，然后将其汇聚以创建 DAP 授权属性。

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 点击 **AAA 条件 (AAA Criteria)**。

步骤 5 选择部分之间匹配条件之一。

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

步骤 6 点击添加 (**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。

- 选择属性并指定 值。
- 点击添加其他条件 (**Add another criteria**) 以添加更多条件。
- 点击保存 (**Save**)。

需要 SCEP

步骤 7 选择 **LDAP 条件**、**RADIUS 条件**或 **SAML 条件** 并指定 **属性 ID** 和 **值**。

步骤 8 点击保存 (Save)。

在 DAP 中配置终端属性选择条件

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。威胁防御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，威胁防御才能选择将其用于会话。威胁防御仅选择满足每个配置的条件 DAP 记录。

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 点击终端条件 (Endpoint Criteria) 并配置以下终端条件属性：

注释 您可以创建每个终端属性类型的多个实例。每个 DAP 记录的终端属性数量没有限制。

- [向 DAP 添加 Anti-Malware 终端属性](#)
- [向 DAP 添加设备终端属性](#)
- [向 DAP 添加 AnyConnect 终端属性，第 8 页](#)
- [向 DAP 添加 NAC 终端属性](#)
- [向 DAP 添加应用属性](#)
- [向 DAP 添加个人防火墙终端属性](#)
- [向 DAP 添加操作系统终端属性](#)
- [向 DAP 添加流程终端属性](#)
- [向 DAP 添加注册表终端属性](#)
- [向 DAP 添加文件终端属性](#)
- [向 DAP 添加证书身份验证属性](#)

步骤 4 点击保存 (Save)。

向 DAP 添加 Anti-Malware 终端属性

过程

- 步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 防恶意软件 (Anti-Malware)。
- 步骤 2 选择匹配条件所有 (All) 或任何 (Any)。
- 步骤 3 点击添加 (Add) 以添加防恶意软件属性。
- 步骤 4 点击已安装 (Installed) 以指示安装还是不安装所选终端属性及其附带限定词。
- 步骤 5 选择已启用 (Enabled) 或已禁用 (Disabled) 以激活或停用实时恶意软件扫描。
- 步骤 6 从列表中选择防恶意软件供应商的名称。
- 步骤 7 选择防恶意软件的产品说明 (Product Description)。
- 步骤 8 选择防恶意软件产品的版本 (Version)。
- 步骤 9 指定距离上次更新 (Last Update) 的天数。
您可以指明防恶意软件更新时间应小于 (<) 或大于 (>) 您指定的天数。
- 步骤 10 点击保存 (Save)。

向 DAP 添加设备终端属性

过程

- 步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 设备 (Device)。
- 步骤 2 选择匹配条件所有 (All) 或任何 (Any)。
- 步骤 3 点击添加 (Add) 并选择 = 或 ≠ 运算符，以检查属性是否等于或不等于你为以下属性输入的值。
 - 主机名 (Host Name) - 要测试的设备的主机名。此处仅会使用计算机的主机名，而不是完全限定域名 (FQDN)。
 - MAC 地址 (MAC Address) - 要测试的网络接口卡的 MAC 地址。地址必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。
 - BIOS 序列号 (BIOS Serial Number) - 要测试的设备的 BIOS 序列号值。此编号格式由制造商指定。
 - 端口号 (Port Number) - 设备的侦听端口号。
 - 安全桌面版本 (Secure Desktop Version) - 在终端上运行的主机扫描映像的版本。
 - OPSWAT 版本 (OPSWAT Version) - OPSWAT 客户端版本。
 - 隐私保护 (Privacy Protection) - 无、缓存清理器、安全桌面。
 - TCP/UDP 端口号 (TCP/UDP Port Number) - 您正在测试的处于侦听状态的 TCP 或 UDP 端口。

步骤 4 点击保存 (Save)。

向 DAP 添加 AnyConnect 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > AnyConnect。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (Add) 并选择 = 或 ≠ 运算符，以检查属性是否等于您输入的值。

步骤 4 选择客户端版本 (Client Version) 和平台 (Platform)。

步骤 5 选择平台版本 (Platform Version)，然后指定设备类型 (Device Type) 和设备唯一 ID (Device Unique ID)。

步骤 6 将 MAC 地址添加到 MAC 地址池中。

注释 MAC 地址必须是 XX-XX-XX-XX-XX-XX 格式，其中每个 X 都是十六进制字符。您可以点击添加另一个 MAC 地址 (Add another MAC Address) 以添加更多地址。

步骤 7 点击保存 (Save)。

向 DAP 添加 NAC 终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > NAC。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (Add) 以添加 NAC 属性。

步骤 4 将运算符设置为等于 = 或不等于 ≠ 安全评估状态字符串。在安全评估状态 (Posture Status) 框中输入安全评估标记字符串。

步骤 5 点击保存 (Save)。

向 DAP 添加应用属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 应用 (Application)。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (**Add**) 以添加应用属性。

步骤 4 选择等于 (=) 或不等于 (≠) 并指定表明远程访问连接类型的客户端类型。

步骤 5 点击保存 (**Save**)。

向 DAP 添加个人防火墙终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (**Endpoint Criteria**) > 个人防火墙 (**Personal Firewall**)。

步骤 2 选择匹配条件所有 (**All**) 或任何 (**Any**)。

步骤 3 点击添加 (**Add**) 以添加个人防火墙属性。

步骤 4 点击已安装 (**Installed**) 以指示安装还是不安装个人防火墙终端属性及其附带限定词 (“名称” / “操作” / “值” 列下面的字段)。

步骤 5 选择启用 (**Enabled**) 或禁用 (**Disabled**) 以激活或停用防火墙保护。

步骤 6 从列表中选择防火墙供应商 (**Vendor**) 的名称。

步骤 7 选择防火墙的产品说明 (**Product Description**)。

步骤 8 选择等于 (=) 或不等于 (≠) 运算符，然后选择防恶意软件产品的版本。

步骤 9 点击保存 (**Save**)。

向 DAP 添加操作系统终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (**Endpoint Criteria**) > 操作系统 (**Operating System**)。

步骤 2 选择匹配条件所有 (**All**) 或任何 (**Any**)。

步骤 3 点击添加 (**Add**) 以添加终端属性。

步骤 4 选择等于 (=) 或不等于 (≠) 运算符，然后选择操作系统 (**Operating System**)。

步骤 5 选择等于 (=) 或不等于 (≠) 运算符，然后制定操作系统版本 (**Version**)。

步骤 6 点击保存 (**Save**)。

向 DAP 添加流程终端属性

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (**Endpoint Criteria**) > 流程 (**Process**)。

- 步骤 2 选择匹配条件所有 (All) 或任何 (Any)。
- 步骤 3 点击添加 (Add) 以添加流程属性。
- 步骤 4 选择存在 (Exists) 或不存在 (Does not exist)。
- 步骤 5 指定进程名称 (Process Name)。
- 步骤 6 点击保存 (Save)。

向 DAP 添加注册表终端属性

扫描注册表终端属性仅适用于 Windows 操作系统。

开始之前

在配置注册表终端属性之前，请为思科安全桌面定义要在 Host Scan 窗口中扫描的注册表项。

过程

-
- 步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 注册表 (Registry)。
 - 步骤 2 选择匹配条件所有 (All) 或任何 (Any)。
 - 步骤 3 点击添加 (Add) 以添加注册表属性。
 - 步骤 4 选择注册表的条目路径 (Entry Path) 并指定路径。
 - 步骤 5 选择注册表是存在 (Exists) 还是不存在 (Does not Exist)。
 - 步骤 6 从列表中选择注册表类型 (Type)。
 - 步骤 7 选择等于 (=) 或不等于 (≠) 运算符，然后输入注册表项的值。
 - 步骤 8 选择不区分大小写 (Case insensitive) 以便在扫描时忽略注册表项的大小写。
 - 步骤 9 点击保存 (Save)。

向 DAP 添加文件终端属性

过程

-
- 步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 文件 (File)。
 - 步骤 2 选择匹配条件所有 (All) 或任何 (Any)。
 - 步骤 3 点击添加 (Add) 以添加文件属性。
 - 步骤 4 指定文件路径。
 - 步骤 5 选择存在 (Exists) 或不存在 (Does not Exist) 以指明文件是否存在。
 - 步骤 6 选择小于 (<) 或大于 (>) 并指定文件的上次修改 (Last Modified) 天数。
 - 步骤 7 选择等于 (=) 或不等于 (≠) 运算符，然后输入校验和 (Checksum)。

步骤 8 点击保存 (Save)。

向 DAP 添加证书身份验证属性

您可以对每个证书编制索引，以便配置的规则可以引用接收到的任何证书。以这些证书字段为基础，您可以配置 DAP 规则来允许或禁止连接尝试。

过程

步骤 1 编辑 DAP 记录，然后选择终端条件 (Endpoint Criteria) > 证书 (Certificate)。

步骤 2 选择匹配条件所有 (All) 或任何 (Any)。

步骤 3 点击添加 (Add) 以添加证书属性。

步骤 4 选择证书 Cert1 或 Cert2。

步骤 5 选择使用者 (Subject) 并指定使用者值。

步骤 6 选择颁发机构 (Issuer) 并指定颁发机构值。

步骤 7 选择使用者替代名称 (Subject Alternate Name) 并指定使用者值。

步骤 8 指定序列号 (Serial Number)。

步骤 9 选择证书存储区 (Certificate Store): 无、计算机或用户。

VPN 客户端发送证书存储区信息。

步骤 10 点击保存 (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。例如，在您将威胁防御配置为使用 AAA 属性（这些属性满足任意、所有指定条件，或者不需要满足指定条件）时，终端属性是累计的，并且必须全部满足。要让安全设备使用一个或另一个终端属性，您必须创建适当的 Lua 逻辑表达式，并在此处输入它们。

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 点击高级 (Advanced) 选项卡。

步骤 4 选择 AND 或 OR 作为要在 DAP 配置上使用的匹配条件。

步骤 5 在用于高级属性匹配的 Lua 脚本 (Lua script for advanced attribute matching) 字段中添加 Lua 脚本。

步骤 6 点击保存 (Save)。

将动态访问策略与远程访问 VPN 关联

您可以将动态访问策略 (DAP) 与远程访问 VPN 策略关联，以便在 VPN 会话身份验证和授权期间匹配动态访问策略属性。您可以在 [威胁防御](#) 上部署远程访问 VPN。

过程

步骤 1 选择设备 (Devices) > 远程访问 (Remote Access)。

步骤 2 点击要与动态访问策略关联的远程访问 VPN 策略旁边的编辑 (Edit)。

步骤 3 点击远程访问 VPN 中的链接以选择动态访问策略。

步骤 4 从动态访问策略 (Dynamic Access Policy) 下拉列表中选择策略，或点击创建新的动态访问策略 (Create a new Dynamic Access Policy) 以配置新的动态访问策略。

步骤 5 点击确定 (OK)。

步骤 6 点击保存 (Save) 以保存远程访问 VPN 策略。

当远程访问 VPN 用户尝试连接时，VPN 会检查配置的动态访问策略记录 and 属性。VPN 会根据匹配的动态访问策略记录来创建动态访问策略，并对 VPN 会话执行适当的操作。

动态访问策略的历史记录

特性	版本	详细信息
动态访问策略	7.0	引入了此功能。

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。