动态访问策略

本章介绍如何配置动态访问策略。

关于动态访问策略

VPN 网关在动态环境下运行。许多可变因素都可能会影响各个 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。

利用 ASA 上的动态访问策略 (DAP)，您可以配置兼顾上述众多可变因素的授权方法。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。换言之，ASA 会根据您定义的策略，为特定用户授予特定会话的访问权限。从一个或多个 DAP 记录选择和/或汇聚属性时，ASA 会生成一个 DAP。它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。然后它会将 DAP 记录应用至用户隧道或会话。

DAP 系统包含的以下组件需要您加以注意：

- DAP 选择配置文件 - 一个文本文件，该文件包含 ASA 在会话建立期间用于选择和应用 DAP 记录的条件。该文件存储在 ASA 上。您可以使用 ASDM 对其进行修改，并以 XML 数据格式上传至 ASA。DAP 选择配置文件包含您配置的所有属性。这些属性包括 AAA 属性、终端属性、在网络和 Web 类型 ACL 过滤器中配置的访问策略、端口转发以及 URL 列表。

- DfltAccess Policy - 始终是 DAP 摘要表中的最后一个条目，而且优先级始终为 0。您可以配置默认访问策略的访问策略属性，但是它不包含 AAA 或终端属性（用户无法配置）。您不能删除 DfltAccessPolicy，它必须是摘要表中的最后一个条目。

有关详细信息，请参阅《动态访问部署指南》(https://supportforums.cisco.com/docs/DOC-1369)。

远程访问协议的 DAP 支持和终端安全评估工具

ASA 使用您配置的终端安全评估工具来获取终端安全属性。这些终端安全评估工具包括 Cisco Secure Firewall 终端安全评估模块、独立的 HostScan/Cisco Secure Firewall 终端安全评估软件包和 NAC。

下表确定了 DAP 支持的每个远程访问协议、可用于该方法的终端安全评估工具，以及该工具提供的信息。

支持远程访问协议	**Cisco Secure Firewall 终端安全评估模块** 主机扫描包 **Cisco Secure Firewall Posture**	**Cisco Secure Firewall 终端安全评估模块** **HostScan 软件包** **Cisco Secure Firewall Posture**	**NAC**	**思科 NAC 设备**
	返回文件信息、注册表项值、运行的进程、操作系统	返回防恶意软件和个人防火墙软件信息	返回 NAC 状态	返回 VLAN 类型和 VLAN ID
IPSec VPN	不兼容	不兼容	兼容	兼容
Cisco AnyConnect VPN	兼容	兼容	兼容	兼容
无客户端（基于浏览器的）SSL VPN	兼容	兼容	不兼容	不兼容
PIX 直通代理（终端安全评估不可用）	不兼容	不兼容	不兼容	不兼容

使用 DAP 的远程访问连接操作程序

以下操作程序概述典型远程访问连接的建立过程。

1. 远程客户端会尝试 VPN 连接。
2. ASA 使用配置的 NAC 和 HostScan/Cisco Secure Firewall Posture 值执行终端安全评估。
3. ASA 通过 AAA 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. ASA 将 AAA 授权属性应用至会话，并建立 VPN 隧道。

5. ASA 根据用户 AAA 授权信息和会话终端安全评估信息选择 DAP 记录。
6. ASA 汇聚选定 DAP 记录中的 DAP 属性，随后它们会成为 DAP 策略。
7. ASA 将 DAP 策略应用至会话。

动态访问策略许可

注释 此功能不适用于无负载加密型号。

动态访问策略 (DAP) 需要以下许可证之一：

- Secure Client Premier- 使用所有 DAP 功能。
- Secure Client Advantage- 仅适用于操作系统和操作系统/Secure Client 版本检查。

相关主题

向 DAP 添加 Secure Client 终端属性，第 12 页

配置动态访问策略

开始之前

- 除非另有说明，否则您必须在配置 DAP 终端属性之前安装 HostScan/Cisco Secure Firewall Posture。
- 如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。
- 由于 Java Web Start 安全问题，如果您在设备上使用基于 webvpn 的配置，您可能会发现无法使用配置的值填充高级终端属性。要解决此问题，请使用 ASDM 桌面应用或将 AEA 相关 URL 添加为 Java Security 中的例外项。
- 在配置文件、进程和注册表终端属性前，先配置文件、进程和注册表基本 HostScan/Cisco Secure Firewall Posture 属性。有关说明，请在 ASDM 中导航至相应的 UI 屏幕，然后点击 **帮助**。
- DAP 仅支持 ASCII 字符。

过程

步骤 1 启动 ASDM 并选择 **配置** > **远程访问 VPN** > **Network**（客户端）访问 **Dynamic Access Policies**。

注释 如果“添加”、“编辑”和“删除”操作下显示**不兼容**操作按钮，则表示您已尝试将 HostScan 升级到某个版本（4.6.x 或更高版本），该版本的内部库更新使其与您现有的 DAP 策略（创建于使用 HostScan 4.3.x 或更低版本时）不兼容。您必须执行一个一次性迁移程序来调整您的配置。

不兼容 操作按钮的出现表示 HostScan 升级已启动，您现在需要迁移配置。有关详细说明，请参阅《AnyConnect Hostscan 4.3.x 到 4.6.x 迁移指南》。

步骤 2 要包括特定防恶意软件或个人防火墙终端属性，请点击靠近窗格顶部的**配置**。如果您之前已启用这两个功能，此链接不会显示。

步骤 3 查看先前配置的 DAP 列表。

以下字段会显示在表格中：

- ACL Priority - 显示 DAP 记录的优先级。

  ASA 在汇聚来自多个 DAP 记录的网络和 Web 类型 ACL 时，会使用此值来对 ACL 进行逻辑排序。ASA 会将记录按优先级数值从大到小排序，数值最小的位于表格底部。较大的数值拥有较高的优先级，即值为 4 的 DAP 记录的优先级高于值为 2 的记录。您不能对其进行手动排序。

- Name - 显示 DAP 记录的名称。
- Network ACL List - 显示对会话应用的防火墙 ACL 的名称。
- Web-Type ACL List - 显示对会话应用的 SSL VPN ACL 的名称。
- Description - 描述 DAP 记录的用途。

步骤 4 点击 **Add** 或 **Edit**，以便添加或编辑动态访问策略，第 4 页。

步骤 5 点击 **Apply** 以便保存 DAP 配置。

步骤 6 使用 **Find** 字段，可以搜索动态访问策略 (DAP)。

在该字段中开始键入字符时，该工具将会搜索DAP表的每个字段的起始字符以获取匹配项。您可以使用通配符扩大搜索。

例如，在 **Find** 字段中键入 **`sal`** 匹配名为 `Sales` 的 DAP，但不会匹配名为 `Wholesalers` 的 DAP。如果您在**查找**字段中键入 **`*sal`**，搜索结果会找到表中的第一个 **`Sales`** 或 **`Wholesalers`** 实例。

步骤 7 测试动态访问策略，第 6 页可验证您的配置。

添加或编辑动态访问策略

过程

步骤 1 启动 ASDM 并依次选择**配置** > **远程访问 VPN** > **网络（客户端）访问**或**无客户端 SSL VPN 访问** > **动态访问策略** > **添加**或**编辑**。

步骤 2 提供此动态访问策略的名称（必选）和说明（可选）。

- **Policy Name** 是一个 4 至 32 个字符的字符串，不允许包含空格。
- 您可在 DAP 的 **Description** 字段中，输入最多 80 个字符。

步骤 3 在 **ACL Priority** 字段中，设置动态访问策略的优先级。

安全设备会以您在此处设置的顺序应用访问策略，最大的数值拥有最高的优先级。有效值范围为 0 至 2147483647。默认值为 0。

步骤 4 为此 DAP 指定您的选择条件：

a) 在 Selection Criteria 窗格中，请使用 ANY/ALL/NONE 下拉列表（未标记）就使用此动态访问策略所需配置的 AAA 属性值进行选择，用户是只需配置任意一个值，还是必须配置所有值，抑或是无需配置这些值，以及是否需要满足每一个终端属性。

不允许重复的条目。如果您配置没有 AAA 或终端属性的 DAP 记录，ASA 会始终选择该记录，因为所有选择条件都已满足。

b) 点击 AAA Attributes 字段中的 **Add** 或 **Edit**，以便配置 DAP 中的 AAA 属性选择条件，第 7 页。

c) 点击 Endpoint Attributes 区域中的 **Add** 或 **Edit**，以便配置 DAP 中的终端属性选择条件，第 10 页。

d) 点击 **Advanced** 字段，以便#unique_178。使用此功能需要 Lua 编程语言方面的知识。

- AND/OR - 点击以便定义基本选择规则和您在此处输入的逻辑表达式之间的关系，即是将新属性添加至已设置的 AAA 和终端属性，还是替代已设置的属性。默认值为 AND。
- Logical Expressions - 您可以配置每个终端属性类型的多个实例。输入用于定义新的 AAA 和/或终端选择属性的任何形式的 LUA 文本。ASDM 不会验证您在此处输入的文本；只是将此文本复制到 DAP XML 文件，然后 ASA 会对其进行处理，丢弃其无法解析的所有表达式。

有关导入/导出 *dap.xml* 文件的信息，请参阅 在两个 ASA 之间导入和导出 DAP XML 文件，第 5 页。

步骤 5 指定此 DAP 的 **Access/Authorization Policy Attributes**。

您在此处配置的属性值会覆盖 AAA 系统中的授权值，包括现有用户、组、隧道组和默认组记录中的授权值。请参阅配置 DAP 访问和授权策略属性，第 27 页。

步骤 6 点击**确定 (OK)**。

在两个 ASA 之间导入和导出 DAP XML 文件

ASA 的动态访问策略 (DAP) 配置存储在 ASA 闪存上名为 *dap.xml* 的文件中。该文件包含 DAP 策略选择属性。

注释 虽然您可以导出 *dap.xml* 文件，对其进行编辑（如果您了解 xml 语法）并将其重新导入，但要非常小心，因为如果配置错误，可能会导致 ASDM 停止处理 DAP 记录。没有用于操作此部分配置的 CLI。

使用以下步骤在两个 ASA 之间导入和导出 *dap.xml* 文件。

该程序使用从 ASA#1 导出 *dap.xml* 文件并在 ASA#2 上导入 的示例。

有关使用 ASDM 处理 ASA 上的文件的信息，请参阅 *Cisco ASA* 系列常规操作 *ASDM* 配置指南的管理文件部分。

过程

步骤 1 清除 ASA#2 上的 *dap.xml* 文件。

a) 将 ASA#2 配置和 *dap.xml* 从 外部保存到 tftp 或 ftp 服务器。
b) 退出 ASA#2 的 ASDM。

注释 您还可以使用 **ASDM** > **工具** > **备份配置** > **DAP 配置** 选项保存 *dap.xml* 文件。

您还可以重命名或删除 ASA#2 闪存上的 *dap.xml* 文件。

步骤 2 在 ASA#2 命令提示符下，输入 **clear configure dynamic-access-policy-record** 命令以删除 DAP 记录配置。

步骤 3 从 ASA#1 闪存中导出 *dap.xml* 文件，并将其导入到 ASA#2 闪存中。

步骤 4 使用 **dynamic-access-policy-record** 命令在 ASA#2 上配置来自 ASA#1 的 DAP 记录条目。

步骤 5 在 ASA#2 上，使用 **dynamic-access-policy-config activate** 命令启用 DAP。

注释 您还可以重新启动 ASA#2 的 ASDM 以激活 DAP 配置。

步骤 6 在 ASA#2 上重新启动 ASDM。
在 ASA#2 中配置新的 DAP 策略。

测试动态访问策略

此窗格允许您指定授权属性值对，从而测试设备上配置的一组 DAP 记录的检索。

过程

步骤 1 可以使用与 AAA 属性和终端属性表关联的 Add/Edit 按钮来指定属性值对。

点击这些 Add/Edit 按钮时显示的对话信息与 Add/Edit AAA Attributes 和 Add/Edit Endpoint Attributes 对话框中的对话信息类似。

步骤 2 点击 **Test** 按钮。

评估每个记录的 AAA 和终端选择属性时，设备上的 DAP 子系统会引用这些值。结果会显示在 **Test Results** 区域中。

配置 DAP 中的 AAA 属性选择条件

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。您可以指定 AAA 属性，这些属性来自思科 AAA 属性层次结构，或者来自 ASA 从 RADIUS 或 LDAP 服务器收到的全部响应属性。ASA 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。ASA 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

要将 AAA 属性配置为 DAP 记录的选择条件，请在 Add/Edit AAA Attributes 对话框中设置要使用的 Cisco、LDAP 或 RADIUS 属性。可以将这些属性设置为所输入的 = 或 != 值。每个 DAP 记录的 AAA 属性数量没有限制。有关 AAA 属性的详细信息，请参阅 AAA 属性定义，第 9 页。

AAA Attributes Type - 使用下拉列表选择 Cisco、LDAP 或 RADIUS 属性：

- Cisco - 指存储在 AAA 层次模型中的用户授权属性。您可以为 DAP 记录中的 AAA 选择属性指定这些属性的一小部分。这些属性包括：
  - Group Policy - 与 VPN 用户会话关联的组策略名称。该名称可以在安全设备上本地设置，也可以作为 IETF-Class (25) 属性通过 RADIUS/LDAP 服务器发送。最多 64 个字符。
  - Assigned IP Address - 输入要为策略指定的 IPv4 地址。
  - Assigned IPv6 Address - 输入要为策略指定的 IPv6 地址。
  - Connection Profile - 连接或隧道组的名称。最多 64 个字符。
  - Username - 经过身份验证的用户的用户名。最多 64 个字符。使用 Local、RADIUS、LDAP 身份验证/授权，或者任何其他身份验证类型（例如 RSA/SDI、NT Domain 等）时适用。
  - =/!= - 等于/不等于。
- LDAP - LDAP 客户端（安全设备）会将所有本机 LDAP 响应属性值对存储在与用户的 AAA 会话关联的数据库中。LDAP 客户端会按收到响应属性的顺序将响应属性写入数据库。它会丢弃使用该名称的所有后续属性。当从LDAP服务器读取用户记录和组记录时，可能会发生此情况。用户记录属性会先被读取，而且其优先级始终高于组记录属性。

  为支持 Active Directory 组成员资格，AAA LDAP 客户端会对 LDAP memberOf 响应属性进行特殊处理。AD memberOf 属性指定 AD 中的组记录的 DN 字符串。组的名称是 DN 字符串中的第一个 CN 值。LDAP 客户端从 DN 字符串中提取组名，将它作为 AAA memberOf 属性存储，并作为 LDAP memberOf 属性存储在响应属性数据库中。如果在 LDAP 响应消息中有其他的

memberOf 属性，则会从这些属性中提取组名称，然后将组名称与之前的 AAA memberOf 属性结合，形成以逗号分隔的组名称字符串，这些字符串也会在响应属性数据库中更新。

在与 LDAP 身份验证/授权服务器进行 VPN 远程访问会话的情况下，会返回以下三个 Active Directory 组（memberOf 枚举）：

cn=Engineering,ou=People,dc=company,dc=com

cn=Employees,ou=People,dc=company,dc=com

cn=EastCoastast,ou=People,dc=company,dc=com

ASA 会处理三个 Active Directory 组：Engineering、Employees 和 EastCoast，可以将其随意组合用作 aaa.ldap 选择条件。

LDAP 属性包含 DAP 记录中的属性名称和属性值对。LDAP 属性名称与语法有关且区分大小写。例如，如果您指定 LDAP 属性 Department，用来代替 AD 服务器作为 department 返回的属性，DAP 记录不会根据此属性设置进行匹配。

注释 要在 Value 字段中输入多个值，请使用分号 (;) 作为分隔符。例如：

eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS - RADIUS 客户端会将所有本机 RADIUS 响应属性值对存储在与用户的 AAA 会话关联的数据库中。RADIUS 客户端会按接收到响应属性的顺序，将响应属性写入数据库。它会丢弃使用该名称的所有后续属性。当从 RADIUS 服务器读取用户记录和组记录时，可能会发生此情况。用户记录属性会先被读取，而且其优先级始终高于组记录属性。

  RADIUS 属性包含 DAP 记录中的属性编号和属性值对。

  注释 对于 RADIUS 属性，DAP 定义 Attribute ID = 4096 + RADIUS ID。

  例如：

  RADIUS 属性“Access Hours”的 Radius ID = 1，因此 DAP 属性值 = 4096 + 1 = 4097。

  RADIUS 属性“Member Of”的 Radius ID = 146，因此 DAP 属性值 = 4096 + 146 = 4242。

- LDAP 和 RADIUS 属性包括：
  - Attribute ID - 属性的名称/编号。最多 64 个字符。
  - Value - 属性名称 (LDAP) 或编号 (RADIUS)。

    要在 Value 字段中输入多个值，请使用分号 (;) 作为分隔符。例如：`eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
  - =/!= - 等于/不等于。

- LDAP 包含 Gep AD Groups 按钮。请参阅检索 Active Directory 组 ，第 9 页。

检索 Active Directory 组

您可以在此窗格中查询 Active Directory 服务器，获取可用 AD 组。此功能仅适用于使用 LDAP 的 Active Directory 服务器。此按钮可以查询 Active Directory LDAP 服务器，获取此用户所属的组的列表（memberOf 枚举）。可以使用组信息来指定动态访问策略 AAA 选择条件。

可以在后台使用 CLI 的**how-ad-groups** 命令从 LDAP 服务器检索 AD 组。ASA 等待服务器响应的默认时间为 10 秒。您可在 aaa-server 主机配置模式下使用 **group-search-timeout** 命令调整此时间。

您可以在 Edit AAA Server 窗格中更改 Group Base DN，从而更改搜索在 Active Directory 层次结构中的起始层次。您也可以在此窗口中更改ASA等待服务器响应的时间。要配置这些功能，请依次选择 **配置 > 远程访问 VPN > AAA/本地用户 > AAA 服务器组 > 编辑 AAA 服务器**。

注释 如果 Active Directory 服务器有大量的组，检索的 AD 组列表（或者 **show ad-groups** 命令的输出）可能会根据服务器可填充至响应数据包的数据量限制进行截断。要避免此问题，请使用过滤器功能来减少服务器报告的组的数量。

AD 服务器组 - 用于检索 AD 组的 AAA 服务器组的名称。

过滤依据 - 指定一个组或组的部分名称，以便减少显示的组。

组名称 - 从服务器检索到的 AD 组的列表。

AAA 属性定义

下表可定义可供 DAP 使用的 AAA 选择属性的名称。“属性名称”字段显示以 LUA 逻辑表达式输入每个属性名称的方式，您可以在“添加/编辑动态访问策略”窗格的“高级”部分中输入表达式。

属性类型	属性名称	来源	值	最大字符串长度	说明
Cisco	aaa.cisco.grouppolicy	AAA	字符串	64	ASA 上的组策略名称，或者作为 IETF-Class (25) 属性通过 Radius/LDAP 服务器发送的组策略名称
	aaa.cisco.ipaddress	AAA	数字	-	为完整的隧道 VPN 客户端（IPsec、L2TP/IPsec、SSL VPN AnyConnect 模型）分配的 IP 地址
	aaa.cisco.tunnelgroup	AAA	字符串	64	连接配置文件（隧道组）名称
	aaa.cisco.username	AAA	字符串	64	经过身份验证的用户的名称（在使用本地身份验证/授权的情况下适用）

属性类型	属性名称	来源	值	最大字符串长度	说明
LDAP	aaa.ldap.<*label*>	LDAP	字符串	128	LDAP 属性值对
RADIUS	aaa.radius.<number>	RADIUS	字符串	128	Radius 属性值对

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。ASA 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记录都指定了终端选择属性，这些属性必须得到满足，ASA才能选择将其用于会话。ASA仅选择满足配置的每个条件的 DAP 记录。

开始之前

- 将终端属性配置为 DAP 记录的选择条件是配置动态访问策略，第 3 页大流程的一个环节。将终端属性配置为 DAP 的选择条件之前，请查阅此程序。
- 有关终端属性的详细信息，请参阅终端属性定义，第 18 页。
-
- 有关 HostScan/Cisco Secure Firewall 终端安全评估如何检查内存驻留的反恶意软件和个人防火墙程序的详细信息，请参阅 DAP 以及防恶意软件和个人防火墙程序，第 17 页。

过程

步骤 1 点击 **Add** 或 **Edit**，将以下任意终端属性添加为选择条件。

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 添加防恶意软件终端属性，第 11 页
- 向 DAP 添加应用属性，第 12 页
- 向 DAP 添加 Secure Client 终端属性，第 12 页
- 向 DAP 添加文件终端属性，第 13 页
- 向 DAP 添加设备终端属性，第 14 页
- 向 DAP 添加 NAC 终端属性，第 14 页
- 向 DAP 添加操作系统终端属性，第 15 页
- 向 DAP 添加个人防火墙终端属性，第 15 页
- 向 DAP 添加策略终端属性，第 16 页

- 向 DAP 添加流程终端属性，第 16 页
- 向 DAP 添加注册表终端属性，第 16 页
- 向 DAP 添加多证书身份验证属性，第 17 页

步骤 2 指定 DAP 策略匹配条件。

对于每个此类终端属性类型，请确定 DAP 策略应要求用户是配置一个类型的所有实例（Match All = AND，默认设置），还是仅配置其中的一个实例 （Match Any = OR)。

a) 点击 **Logical Op**。
b) 为每个终端属性类型选择 **Match Any**（默认）或 **Match All**。
c) 点击 **OK**。

步骤 3 返回至 添加或编辑动态访问策略，第 4 页。

向 DAP 添加防恶意软件终端属性

开始之前

如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

过程

步骤 1 在**终端属性类型**列表框中，选择**防恶意软件**。

步骤 2 点击相应的“**安装**”或“**不安装**”按钮，指示安装还是不安装所选终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

步骤 3 确定要启用还是禁用实时扫描。

步骤 4 从**供应商 ID** 列表框中，选择要测试的防恶意软件的供应商的名称。

步骤 5 选中 **Product Description** 复选框，从列表框中选择您要测试的供应商产品名称。

步骤 6 选中 **Version** 复选框，将运算字段设为等于 (=)、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您从 **Version** 列表框中选择的产品版本号。

如果 Version 列表框中的选项包含 x（例如 3.x），可以将 x 替换为特定版本号（例如 3.5）。

步骤 7 选中 **Last Update** 复选框。指定距离上次更新的天数。您可能想要指明更新时间应小于 (<) 或大于 (>) 您在此处输入的天数。

步骤 8 点击**确定 (OK)**。

向 DAP 添加应用属性

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Application**。

步骤 2 在 Client Type 运算字段中，请选择等于 (=) 或者不等于 (!=)。

步骤 3 在 Client type 列表框中，请指明要测试的远程访问连接类型。

步骤 4 点击**确定 (OK)**。

向 DAP 添加 Secure Client 终端属性

Secure Client 终端属性，也称为移动终端安全评估或 AnyConnect 标识扩展 (ACIDex)，Cisco 安全客户端 AnyConnect VPN 模块会使用这些属性与 ASA 进行终端安全评估信息通信。动态访问策略使用这些终端属性向用户进行授权。

这些移动终端安全评估属性可以包含在动态访问策略中，并且在在终端上没有安装 HostScan/Secure Firewall Posture 的情况下实施。

某些移动终端安全评估属性仅与在移动设备上运行的 Secure Client 相关。某些移动终端安全评估属性与在移动设备上运行的 Secure Client和 Secure Client 桌面客户端都相关。

开始之前

移动终端安全评估需要在 ASA 上安装 Secure Client 移动许可证和 Secure Client 高级许可证。安装这些许可证的企业将能够根据 DAP 属性和其他现有终端属性，在受支持的移动设备上实施 DAP 策略。这包括允许或拒绝来自移动设备的远程访问。

过程

步骤 1 在 **终端属性类型** 列表框中，选择 Secure Client。

步骤 2 选中**客户端版本**复选框，并将操作字段设置为等于（=）、不等于（！=）、小于（<）、大于（>）、小于或等于（<=）或大于或等于（>=）然后在**客户端版本**字段中指定的 Secure Client 版本号。

您可以使用此字段来评估移动设备（例如移动电话和平板电脑）或者台式计算机和笔记本电脑设备上的客户端的版本。

步骤 3 选中 **Platform** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您随后从 **Platform** 列表框中选择的操作系统。

您可以使用此字段来评估移动设备（例如移动电话和平板电脑）以及台式计算机和笔记本电脑设备上的操作系统。选择一个平台将激活 Device Type 和 Device Unique ID 的其他属性字段。

步骤 4 选中 **Platform Version** 复选框，将运算字段设为等于 (=) 、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您随后在 **Platform Version** 字段中指定的操作系统版本号。

如果您想要创建包含此属性的 DAP 记录，请确保也在上一步指定平台。

步骤 5 如果您已选中 Platform 复选框，可以选中 **Device Type** 复选框。将运算字段设为等于 (=) 或不等于 (!=) 您随后在 **Device Type** 字段中选择或输入的设备。

如果您有未在 Device Type 字段中列出的受支持设备，可在 Device Type 字段中输入该设备。获取设备类型信息的最可靠方法是，在终端上安装 Secure Client，连接到 ASA，然后执行 DAP 跟踪。在 DAP 跟踪结果中，请查找 **endpoint.anyconnect.devicetype** 的值。这是您需要在 Device Type 字段中输入的值。

步骤 6 如果您已选择 Platform 复选框，可以选中 **Device Unique ID** 复选框。将运算字段设为等于 (=) 或不等于 (!=) 您随后在 **Device Unique ID** 字段中指定的设备唯一 ID。

设备唯一 ID 可区分允许您为特定移动设备设置策略的个别设备。要获得设备的唯一 ID，您需要将此设备连接至 ASA，并执行 DAP 跟踪，然后查找 **endpoint.anyconnect.deviceuniqueid** 的值。这是您需要在 Device Unique ID 字段中输入的值。

步骤 7 如果您已选择平台，可以将 MAC 地址添加至 **MAC Addresses Pool** 字段。将运算字段设为等于 (=) 或不等于 (!=) 指定的 MAC 地址。每个 MAC 地址必须为 xx-xx-xx-xx-xx-xx 格式，其中“x”是有效的十六进制字符（0-9、A-F 或 a-f）。MAC 地址应至少用一个空格分隔。

MAC 地址可区分允许您为特定设备设置策略的个别系统。要获得系统的 MAC 地址，您需要将此设备连接至 ASA，并执行 DAP 跟踪，然后查找 **endpoint.anyconnect.macaddress** 的值。这是您需要在 MAC Address Pool 字段中输入的值。

步骤 8 点击**确定 (OK)**。

向 DAP 添加文件终端属性

开始之前

在配置文件终端属性之前，请定义要在 HostScan/Cisco Secure Firewall Posture 窗口中扫描的文件。

对于 HostScan 版本 4.x，在 ASDM 中，选择 **配置 > 远程访问 VPN > 安全桌面管理器 > HostScan**。对于 Cisco Secure Firewall Posture 版本 5.x，在 ASDM中，选择 **配置 > 远程访问 VPN > Posture (对于 Cisco Secure Firewall) > Posture 设置**。

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **File**。

步骤 2 选择适当的 **Exists** 或 **Does not exist** 单选按钮，指示选定终端属性及其附带限定词（Exists/Does not exist 按钮下方的字段）是否应存在。

步骤 3 在 **Endpoint ID** 列表框中，从下拉列表中选择等同于要扫描的文件条目的终端 ID。

文件信息显示在 Endpoint ID 列表框的下方。

步骤 4 选中 **Last Update** 复选框，将运算字段设为小于 (<) 或大于 (>) 已经过去的特定天数。在 **days** 字段中输入已经过去的特定天数。

步骤 5 选中 **Checksum** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的文件的校验和值。

步骤 6 点击 **Compute CRC32 Checksum** 可确定您要测试的文件的校验和值。

步骤 7 点击**确定 (OK)**。

向 DAP 添加设备终端属性

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Device**。

步骤 2 选中 **Host Name** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的设备的主机名称。此处仅会使用计算机的主机名，而不是完全限定域名 (FQDN)。

步骤 3 选中 **MAC address** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的网络接口卡的 MAC 地址。每个条目只允许有一个 MAC 地址。地址必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。

步骤 4 选中 **BIOS Serial Number** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的设备的 BIOS 序列号值。此编号格式由制造商指定。没有格式要求。

步骤 5 选中 **TCP/UDP Port Number** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的处于侦听状态的 TCP 或 UDP 端口。

在 TCP/UDP 组合框中，选择您要测试的端口的类型：TCP (IPv4)、UDP (IPv4)、TCP (IPv6) 或 UDP (IPv6)。如果将要测试多个端口，可以在 DAP 中创建多个单独的终端属性规则，并在每个规则中指定一个端口。

步骤 6 选中 **Version of Secure Desktop (CSD)** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 在此终端上运行的 HostScan/Secure Firewall Posture 映像的版本。

步骤 7 选中 **Version of Endpoint Assessment** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您要测试的终端评估 (OPSWAT) 的版本。

步骤 8 点击**确定 (OK)**。

向 DAP 添加 NAC 终端属性

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **NAC**。

步骤 2 选中 **Posture Status** 复选框，将运算字段设为等于 (=) 或不等于 (!=) ACS 收到的终端安全评估标记字符串。在 Postune Status 文本框中输入终端安全评估标记字符串。

步骤 3 点击**确定 (OK)**。

向 DAP 添加操作系统终端属性

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Operating System**。

步骤 2 选中 **OS Version** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您在 **OS Version** 列表框中设置的 Windows、Mac 或 Linux 操作系统。

步骤 3 选中 **OS Update** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 您在 **OS Update** 文本框中输入的操作系统的 Windows、Mac 或 Linux 服务包。

步骤 4 点击**确定 (OK)**。

向 DAP 添加个人防火墙终端属性

开始之前

如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Operating System**。

步骤 2 点击相应的“**安装**”或“**不安装**”按钮，指示安装还是不安装所选终端属性及其附带限定词（“名称”/“操作”/“值”列下面的字段）。

步骤 3 在**供应商**列表框中，点击要测试的个人防火墙的供应商的名称。

步骤 4 选中 **Product Description** 复选框，从列表框中选择您要测试的供应商产品名称。

步骤 5 选中 **Version** 复选框，将运算字段设为等于 (=)、不等于 (!=)、小于 (<)、大于 (>)、小于或等于 (<=)，或者大于或等于 (>=) 您从 **Version** 列表框中选择的产品版本号。

如果 **Version** 列表框中的选项包含 x（例如 3.x），可以将 x 替换为特定版本号（例如 3.5）。

步骤 6 选中 **Last Update** 复选框。指定距离上次更新的天数。您可能想要指明更新时间应小于 (<) 或大于 (>) 您在此处输入的天数。

步骤 7 点击 **OK**。

向 DAP 添加策略终端属性

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Policy**。

步骤 2 选中 **Location** 复选框，将运算字段设为等于 (=) 或不等于 (!=) 思科安全桌面 Microsoft Windows 位置配置文件。在 **Location** 文本框中输入思科安全桌面 Microsoft Windows 位置配置文件字符串。

步骤 3 点击**确定 (OK)**。

向 DAP 添加流程终端属性

开始之前

在配置进程终端属性之前，请为思科安全桌面定义要在 HostScan/Cisco Secure Firewall Posture 窗口中扫描的进程。

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Process**。

步骤 2 点击适当的 **Exists 或 Does not exist** 按钮，指示选定终端属性及其附带限定词（Exists 和 Does not exist 按钮下方的字段）是否应存在。

步骤 3 在 **Endpoint ID** 列表框中，从下拉列表中选择要扫描的终端 ID。

终端 ID 进程信息会显示在列表框的下方。

步骤 4 点击**确定 (OK)**。

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，请定义要在 HostScan/Cisco Secure Firewall Posture 窗口中扫描的注册表密钥。

过程

步骤 1 在 **Endpoint Attribute Type** 列表框中，选择 **Registry**。

步骤 2 点击适当的 **Exists 或 Does not exist** 按钮，指示 **Registry** 终端属性及其附带限定词（Exists 和 Does not exist 按钮下方的字段）是否应存在。

步骤 3 在 **Endpoint ID** 列表框中，从下拉列表中选择等同于要扫描的注册表项的终端 ID。

注册表信息显示在 Endpoint ID 列表框的下方。

步骤 4 选中 **Value** 复选框，将运算字段设为等于 (=) 或不等于 (!=)。

步骤 5 在第一个 **Value** 列表框中，将注册表项确定为 dword 或字符串。

步骤 6 在第二个 Value 运算列表框中，输入您要扫描的注册表项的值。

步骤 7 如果要在扫描时忽略注册表项的大小写，请点击该复选框。如果要搜索区分大小写，请勿选中该复选框。

步骤 8 点击**确定 (OK)**。

向 DAP 添加多证书身份验证属性

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 依次浏览至**配置 > 远程访问 VPN > 网络（客户端）访问 > 动态访问策略 > 添加终端属性**。

步骤 2 在下拉菜单中选择**多证书身份验证**作为“终端属性类型”。

步骤 3 根据您的首选项进行以下一项或多项配置：

- 证书持有者名称
- 颁发机构名称
- 主题备用名称
- 序列号

步骤 4 将“证书存储区”保留默认值“无”以允许来自任一存储区的证书，或者选择允许的存储区 - 仅用户还是仅计算机。如果选择“用户”或“计算机”，必须输入证书来自哪个存储区。客户端将在协议中发送此信息。

DAP 以及防恶意软件和个人防火墙程序

当用户属性与配置的 AAA 和终端属性匹配时，安全设备会使用 DAP 策略。登录前评估和 HostScan/Secure Firewall Posture 模块将向安全设备返回关于配置的终端属性的信息，DAP 子系统则会使用该信息来选择与这些属性的值匹配的 DAP 记录。

大多数（但不是所有）防恶意软件和个人防火墙程序都支持活动扫描，这意味着这些程序会驻留在内存中，因而会始终运行。HostScan/Secure Firewall Posture 按照以下方式检查终端是否安装了程序，以及它是否驻留在内存中：

- 如果安装的程序不支持活动扫描，HostScan/Secure Firewall Posture 将报告系统存在此软件。DAP 系统选择指定程序的 DAP 记录。
- 如果安装的程序确实支持活动扫描，并且为该程序启用了活动扫描，HostScan/Secure Firewall Posture 将报告此软件的存在。同样，安全设备会选择指定程序的 DAP 记录。
- 如果安装的程序确实支持活动扫描，并且为该程序启用了活动扫描，HostScan/Secure Firewall Posture 将忽略此软件的存在。安全设备不会选择指定该程序的 DAP 记录。此外，**debug trace** 命令的输出（包括有关DAP的大量信息）不指示该程序的存在，即使安装了此程序也是如此。

注释 如果从 HostScan 4.3.x 升级到 HostScan 4.6.x 或更高版本，必须在升级前将任何现有的 AV/AS/FW 终端属性迁移到取代其的相应 AM/FW 终端属性。有关完整的升级和迁移程序，请参阅《AnyConnect HostScan 4.3.x 到 4.6.x 迁移指南》。

终端属性定义

以下终端选择属性可供 DAP 使用。“属性名称”字段显示以 LUA 逻辑表达式输入每个属性名称的方式，您可以在“动态访问策略选择条件”窗格的“高级”区域中输入表达式。*label* 变量标识应用、文件名、进程或注册表项。

属性类型	属性名称	来源	值	最大字符串长度	说明
反恶意软件	endpoint.am["*label*"].exists	HostScan/Secure Firewall Posture	true	-	防恶意软件程序存在
	endpoint.am["*label*"].version		字符串	32	版本
	endpoint.am["*label*"].description		字符串	128	防恶意软件说明
	endpoint.am["*label*"].lastupdate		整数	-	防恶意软件定义更新以来经过的秒数
个人防火墙	endpoint.pfw["*label*"].exists	HostScan/Secure Firewall Posture	true	-	此个人防火墙存在
	endpoint.pfw["*label*"].version		字符串	字符串	版本 (Version)
	endpoint.pfw["*label*"].description		字符串	128	个人防火墙说明

属性类型	属性名称	来源	值	最大字符串长度	说明
AnyConnect（不需要 HostScan/Secure Firewall Posture）	endpoint.anyconnect.clientversion	终端	版本	-	Secure Client 版本
	endpoint.anyconnect.platform		字符串	—	Secure Client 上安装了哪个操作系统？
	endpoint.anyconnect.platformversion		版本	64	Secure Client 上安装了哪个版本的操作系统？
	endpoint.anyconnect.devicetype		字符串	64	安装 Secure Client 的移动设备的类型
	endpoint.anyconnect.deviceuniqueid			64	安装 Secure Client 的移动设备的唯一 ID
	endpoint.anyconnect.macaddress		字符串	—	安装 Secure Client 的设备的 MAC 地址。 必须为 xx-xx-xx-xx-xx-xx 格式，其中 'x' 是有效的十六进制字符
应用	endpoint.application.clienttype	应用	字符串	—	客户端类型： CLIENTLESS ANYCONNECT IPSEC L2TP

属性类型	属性名称	来源	值	最大字符串长度	说明
设备	endpoint.device. hostname	终端	字符串	64	仅主机名，而不是 FQDN
	endpoint.device.MAC		字符串	—	网络接口卡的 Mac 地址。每个条目只允许有一个 MAC 地址 必须是 xxxx.xxxx.xxxx 格式，其中 x 是十六进制字符。
	endpoint.device.id		字符串	64	BIOS 序列号。此编号格式由制造商指定。没有格式要求
	endpoint.device.port		字符串	—	TCP 端口处于侦听状态 您可以为一条线路定义一个端口 介于 1 和 65535 之间的整数
	endpoint.device. protection_version		字符串	64	设备运行的 HostScan/Cisco Secure Firewall Posture 映像的版本
	endpoint.device. protection_extension		字符串	64	终端评估版本 (OPSWAT)
文件	endpoint.file["*label*"].exists		true	-	此文件存在
	endpoint.file[“label”]. endpointid				
	endpoint.file["*label*"]. lastmodified		整数	-	文件上次修改之后经过的时间（秒）
	endpoint.file["*label*"]. crc.32		整数	-	此文件的 CRC32 散列值
NAC	endpoint.nac.status	NAC	字符串	—	用户定义的状态字符串

属性类型	属性名称	来源	值	最大字符串长度	说明
操作系统	endpoint.os.version		字符串	32	操作系统
	endpoint.os.servicepack		整数	-	Windows 服务包
策略	endpoint.policy.location		字符串	64	
流程	endpoint. process["*label*"].exists		true	-	此进程存在
	endpoint. process["*label*"].path		字符串	255	此进程的完整路径
注册表	endpoint. registry["*label*"].type		*dword* 字符串	-	dword
	endpoint. registry["*label*"].value		字符串	255	注册表项的值
VLAN	endoint.vlan.type	CNA	字符串	—	VLAN 类型： [illegible]

使用 LUA 在 DAP 中创建其他 DAP 选择条件

本节提供为 AAA 或终端属性构建逻辑表达式的相关信息。请注意，执行此操作需要精通 LUA 知识。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。

在“高级”字段中，您可以输入代表 AAA 和/或终端选择逻辑运算的任何格式的 LUA 文本。ASDM 不会验证您在此处输入的文本；只是将此文本复制到 DAP 策略文件，然后 ASA 会对其进行处理，丢弃其无法解析的所有表达式。

对于添加上文所述的 AAA 和终端属性区域中无法添加的选择条件，该选项十分有用。例如，虽然您可以将 ASA 配置为使用满足任意指定条件、满足所有指定条件或不满足所有指定条件的 AAA 属性，但终端属性是累计的，必须全部满足。要让安全设备使用一个或另一个终端属性，您需要创建适当的 LUA 逻辑表达式，并在此处输入它们。

以下各节将详细介绍创建 LUA EVAL 表达式的相关信息及示例。

- 创建 LUA EVAL 表达式的语法，第 22 页
- DAP EVAL 表达式示例，第 26 页
- 其他 LUA 函数，第 23 页

创建 LUA EVAL 表达式的语法

注释 如果您必须使用 Advanced 模式，为使内容清晰易懂，我们建议您尽可能使用 EVAL 表达式，以便使程序验证简单明了。

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA 属性或思科安全桌面返回的属性，有关属性定义的信息，请参阅终端属性定义，第 18 页。	
<comparison>	以下任一字符串（需要括在双引号中）	
	"EQ"	等于
	"NE"	不等于
	"LT"	小于
	"GT"	大于
	"LE"	小于或等于
	"GE"	大于或等于
<value>	双引号中的字符串包含与该属性比较的值	
<type>	以下任一字符串（需要括在双引号中）	
	“string”	区分大小写的字符串比较
	“”	不区分大小写的字符串比较
	“integer”	数值比较，将字符串值转换为数值
	“hex”	使用十六进制值比较数值，将十六进制字符串转换为十六进制数值
	“version”	比较 X.Y.Z. 形式的版本，其中 X、Y 和 Z 为数字。

HostScan 4.6（及更高版本）和 Secure Firewall Posture 版本 5 的 LUA 程序

用于检查应用了上次更新的“任意”防恶意软件 (endpoint.am) 的 LUA 脚本

使用以下 LUA 脚本检查“任意”防恶意软件产品/供应商 (endpoint.am)。可以进行修改以适应不同的“上次更新”间隔。以下示例显示了如何表示执行“上次更新”的时间必须在30天（记为2592000秒）以内。

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
             return true
        end
  end
  return false
end)()
```

用于检查“任意”个人防火墙的 LUA 脚本

使用以下 LUA 脚本检查“任意”防火墙产品/供应商 (endpoint.pfw)：

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

其他 LUA 函数

在与动态访问策略配合使用时，您可能需要增加匹配条件的灵活性。例如，您可能想要根据以下内容应用一个不同的 DAP：

- CheckAndMsg 是您可以配置 DAP 使其调用的 LUA 函数。它根据条件生成一条用户消息。
- 用户对象层次结构的组织单位 (OU) 或其他层次。
- 遵循命名约定但有许多匹配项的组名称可能需要您能够使用通配符。

您可以在 ASDM 中的 DAP 窗格的“高级”部分中创建 LUA 逻辑表达式，从而实现这种灵活性。

DAP CheckAndMsg 函数

ASA 仅在选择了包括 LUA CheckAndMsg 函数的 DAP 记录并导致连接终止时，才会向用户显示消息。

CheckAndMsg 函数的语法如下：

```
CheckAndMsg(value, “<message string if value is true>”, “<message string if value if false>”)
```

在创建 CheckAndMsg 函数时，请注意以下事项：

- CheckAndMsg 会返回作为其第一个参数传入的值。
- 如果您不想使用字符串比较，请将 EVAL 函数用作第一个参数。例如：

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg 返回 EVAL 函数的结果，并且安全设备会使用它来确定是否选择 DAP 记录。如果选择此记录，并导致终止，安全设备会显示相应的消息。

基于 OU 的匹配示例

DAP 可在逻辑表达式中使用从 LDAP 服务器返回的许多属性。有关此示例的输出，请参阅 DAP 跟踪部分，或运行 debug dap trace。

LDAP 服务器将返回用户的可分辨名称 (DN)。这会明确确定用户对象在目录中所处的位置。例如，如果用户 DN 是 CN=Example User, OU=Admins, dc=cisco, dc=com，则此用户位于 OU=Admins,dc=cisco,dc=com 中。如果所有管理员都在此 OU（或此层次下的任何容器）中，可如下使用逻辑表达式来匹配此条件：

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

在本示例中，string.find 函数允许使用正则表达式。在字符串结尾处使用 $，将此字符串定位至 distinguishedName 字段末尾。

组成员身份示例

您可以为 AD 组成员身份的模式匹配创建基本逻辑表达式。由于用户可以是多个组的成员，DAP 会将 LDAP 服务器响应解析为表格中的不同条目。您需要一个高级函数来完成以下操作：

- 将 memberOf 字段作为字符串进行比较（用户仅属于一个组的情况）。
- 如果返回的数据的类型为“table”，则循环访问每个返回的 memberOf 字段。

我们出于此目的编写并测试过的函数如下所示。在本示例中，如果用户是以“-stu”结尾的任意组的成员，它们会与此 DAP 匹配。

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

拒绝访问示例

您可以使用以下函数，以便在没有防恶意软件程序的情况下拒绝访问。将它与 Action 已设置为 Terminate 的 DAP 配合使用。

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ”, "true", "string")) then

            return false

        end
    end
   return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

如果缺少防恶意软件程序的用户尝试登录，DAP 会显示以下消息：

```
Please install antimalware software before connecting.
```

多证书身份验证示例

您可以在 DAP 规则中使用多证书身份验证来确定通配符颁发者 CN。

如果您已配置由两个不同的证书颁发机构（例如 abc.cisco.com 和 xyz.cisco.com）颁发给两台不同计算机的两个证书，则 DAP 规则必须具有多个证书身份验证的条件，其中颁发者 CN 为*.cisco.com 或 cisco.com。

您可以使用以下函数为用户和计算机证书使用通配符 issuer_cn cisco.com 定义证书的 DAP 规则：

```
assert(
 function()
```

```
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

DAP EVAL 表达式示例

研究这些示例将有助于创建 LUA 逻辑表达式：

说明	示例
终端 LUA 检查：检查 Windows 10	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
终端 LUA 检查：检查 CLIENTLESS 或 CVC 客户端类型的匹配项。	`(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))`
终端 LUA 检查：检查用户 PC 上是否安装有一个防恶意软件程序 Symantec Enterprise Protection，如未安装则显示一条消息。	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
终端 LUA 检查：检查 McAfee Endpoint Protection 版本 10 到 10.5.3 及 10.6 以上的版本。	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
终端 LUA 检查：检查 McAfee 防恶意软件定义在过去 10 天（864000 秒）内是否更新，如需要更新则显示一条消息。	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
debug dap trace 返回 `endpoint.os.windows.hotfix["KB923414"] = "true";` 后，检查特定修补程序	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

检查防恶意软件程序并提供消息

您可以配置消息，以便最终用户了解并能够修复防恶意软件的问题。如果允许访问，ASA 会在门户页面上显示 DAP 评估过程中生成的所有消息。如果访问被拒绝，ASA 会收集导致“终止”情况的 DAP 的所有消息，并于浏览器中在登录页面上显示这些消息。

以下示例显示了如何使用此功能检查 Symantec Endpoint Protection 的状态。

1. 将以下LUA表达式复制并粘贴至“添加/编辑动态访问策略”窗格的“高级”字段中（请点击最右侧的双箭头，以便展开此字段）。

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec
 Endpoint Protection is disabled. You must enable before being granted access", nil))
```

2. 在同一 Advanced 字段中，点击 **OR** 按钮。
3. 在下面的 Access Attributes 部分，在最左侧的选项卡 Action 中，点击 **Terminate**。
4. 从已安装 Symantec Endpoint Protection 但 Symantec Endpoint Protection 已被禁用的 PC 进行连接。预期结果应该是不允许该连接，并且用户将看到消息“Symantec Endpoint Protection 已被禁用。您必须将其启用后才能获得访问权限。”

检查防恶意软件程序和超过 2 天的定义

此示例检查 Symantec 和 McAfee 防恶意软件程序是否存在，以及病毒定义是否超过 2 天（172800 秒）。如果定义超过 2 天，ASA 将终止此会话，并显示一条消息和补救链接。要完成此任务，请执行以下步骤。

1. 将以下 LUA 表达式复制并粘贴至“添加/编辑动态访问策略”窗格的“高级”字段中：

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
"Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
 before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
"McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
 Virus Definitions before being granted access", nil))
```

2. 在同一 Advanced 字段中，点击 **AND**。
3. 在下面的“访问属性”部分，在最左侧的选项卡“操作”中，点击 **终止**。
4. 从安装了 Symantec 和 McAfee 防恶意软件程序并且版本已超过 2 天未更新的 PC 进行连接。

   预期结果应该是不允许该连接，并且用户将看到一条消息，说明病毒定义已过期。

配置 DAP 访问和授权策略属性

点击以下每个选项卡，并配置其中包含的字段。

过程

步骤 1 选择 **Action** 选项卡指定应用至特定连接或会话的特殊处理。

- Continue -（默认值）点击以将访问策略属性应用于会话。
- Quarantine - 通过使用隔离，您可以限制已通过 VPN 建立隧道的特定客户端。ASA 可根据选定的DAP记录，将受限的ACL应用于会话，以形成一个受限组。当终端不符合管理定义策略时，

用户仍然可以访问补救服务，但会对用户施加限制。修复后，用户可以重新连接，调用新的终端安全评估。如果通过此评估，用户可进行连接。此参数需要支持 安全客户端 功能的发行版 Secure Client 。

- Terminate - 点击以终止会话。
- User Message - 输入一条文本消息，当此 DAP 记录选定时，该消息会显示在门户页面上。最多 490 个字符。用户消息显示为黄色球体。当用户登录时，它会闪烁三次以引起注意，然后停止闪烁。如果选择了多条 DAP 记录，并且它们都有用户消息，系统会显示所有用户信息。

  您可以包含 URL 或其他嵌入式文本，这需要您使用正确的 HTML 标记。例如：有关升级防恶意软件的程序，请所有承包商阅读说明。

步骤 2 选择 **Network ACL Filters** 选项卡可配置应用至此 DAP 记录的网络 ACL。

DAP 的 ACL 可以包含允许或拒绝规则，但不能同时包含二者。如果 ACL 同时包含允许和拒绝规则，则 ASA 会拒绝它。

- Network ACL 下拉列表 - 选择已配置的网络 ACL，以便添加至此 DAP 记录。ACL 可以是允许和拒绝规则的任意组合。此字段支持可定义 IPv4 和 IPv6 网络流量访问规则的统一 ACL。
- **Manage** - 点击以便添加、编辑和删除网络 ACL。
- **Network ACL list** - 显示此 DAP 记录的网络 ACL。
- **添加** - 点击以便将下拉列表中选定的网络 ACL 添加至右侧的网络 ACL 列表。
- **Delete** - 点击以便将突出显示的网络 ACL 从 Network ACL 列表中删除。您不能从 ASA 中删除 ACL，除非您先将其从 DAP 记录中删除。

步骤 3 选择 **Web-Type ACL Filters (clientless)** 选项卡以配置应用至此 DAP 记录的 Web 类型 ACL。DAP 的 ACL 仅可以包含允许或拒绝规则。如果 ACL 同时包含允许和拒绝规则，则 ASA 会拒绝它。

- **Web-Type ACL** 下拉列表 - 选择已配置的 Web 类型 ACL，以便添加至此 DAP 记录。ACL 可以是允许和拒绝规则的任意组合。
- **管理** - 点击以便添加、编辑和删除 Web 类型 ACL。
- **Web-Type ACL** 列表 - 显示此 DAP 记录的 Web 类型 ACL。
- **添加** - 点击以便将下拉列表中选定的 Web 类型 ACL 添加至右侧的 Web 类型 ACL 列表。
- **Delete** - 点击以便将 Web 类型 ACL 从 Web 类型 ACL 列表中删除。您不能从 ASA 中删除 ACL，除非您先将其从 DAP 记录中删除。

步骤 4 选择 **Functions** 选项卡为 DAP 记录配置文件服务器条目和浏览、HTTP 代理以及 URL 条目。

- **File Server Browsing** - 启用或禁用文件服务器或共享功能的 CIFS 浏览。

  浏览要求使用NBNS（主浏览器或WINS）。如果该协议发生故障或未配置，则使用DNS。CIFS 浏览功能不支持国际化。

- **File Server Entry** - 允许或阻止用户在门户页面上输入文件服务器路径和名称。启用时，系统会将文件服务器条目部分放在门户页面上。用户可以直接输入 Windows 文件的路径名。可以下载、编辑、删除、重命名和移动文件。还可以添加文件和文件夹。另外还必须在适用的Windows服务器上为用户访问配置共享。用户可能必须通过身份验证才能访问文件，具体取决于网络要求。
- **HTTP Proxy** - 能够影响 HTTP 小应用程序代理向客户端的转发。对于使用适当内容转换进行介入的技术（如 Java、ActiveX 和 Flash），代理十分有用。它会绕过处理，同时确保安全设备的持续使用。转发的代理自动修改浏览器的原有代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新的代理配置。支持几乎所有客户端技术，包括 HTML、CSS、JavaScript、VBScript、ActiveX 和 Java。唯一支持的浏览器是 Microsoft Internet Explorer。
- **URL Entry** - 允许或阻止用户在门户页面上输入 HTTP/HTTPS URL。如果启用此功能，用户可在 URL 输入框中输入 Web 地址。

使用 SSL VPN 不能保证与每个站点的通信是安全的。SSL VPN 可确保远程用户 PC 或工作站与企业网络上的 ASA 之间数据传输的安全性。如果用户届时访问非 HTTPS Web 资源（位于互联网或内部网络上），则从企业 ASA 到目的 Web 服务器之间的通信不安全。

在无客户端 VPN 连接中，ASA 用作最终用户 Web 浏览器和目标 Web 服务器之间的代理。当用户连接到支持 SSL 的 Web 服务器时，ASA 将建立安全连接，并验证服务器的 SSL 证书。最终用户浏览器从不接收提供的证书，因此无法检查并验证证书。SSL VPN 的当前实施不允许与提供已到期证书的站点进行通信。ASA 也不会执行可信 CA 证书验证。因此，用户在与支持 SSL 的 Web 服务器通信前，无法分析其提供的证书。

要限制用户访问互联网，请为 URL Entry 字段选择 Disable。这可以防止 SSL VPN 用户在进行无客户端 VPN 连接的过程中使用 Web。

- **Unchanged** -（默认值）点击以便使用应用至此会话的组策略中的值。
- **Enable/Disable** - 点击以便启用或禁用该功能。
- **Auto-start** - 点击以启用 HTTP 代理，并让 DAP 记录自动启动与这些功能关联的小应用程序。

步骤 5 选择 **Port Forwarding Lists** 选项卡为用户会话配置端口转发列表。

端口转发为此组中的远程用户提供对客户端/服务器应用的访问权限，这些应用经由已知的固定TCP/IP端口进行通信。远程用户可以使用安装在其本地 PC 上的客户端应用，并安全访问支持该应用的远程服务器。思科已经测试了以下应用：Windows Terminal Services、Telnet、Secure FTP (FTP over SSH)、Perforce、Outlook Express 和 Lotus Notes。其他基于 TCP 的应用可能也可以正常使用，但是思科没有对其进行过测试。

注释 端口转发不能与某些 SSL/TLS 版本配合使用。

注意 确保在远程计算机上安装 Sun Microsystems Java Runtime Environment (JRE) 来支持端口转发（应用访问）和数字证书。

- **Port Forwarding** - 为应用于此 DAP 记录的端口转发列表选择一个选项。此字段中的其他属性只在您将 Port Forwarding 设为 Enable 或 Auto-start 时启用。

- **Unchanged** - 点击以将属性从运行配置中删除。
- **Enable/Disable** - 点击以启用或禁用端口转发。
- **Auto-start** - 点击以启用端口转发，并让 DAP 记录自动启动与此端口转发列表关联的端口转发小应用程序。
- **Port Forwarding List** 下拉列表 - 选择已经配置的端口转发列表，以添加至 DAP 记录。
- **New...** - 点击以配置新的端口转发列表。
- **Port Forwarding Lists**（未标记）- 显示 DAP 记录的端口转发列表。
- **Add** - 点击以将下拉列表中的选定端口转发列表添加至右侧的 Network ACL 列表。
- **Delete** - 点击以从 Port Forwarding 列表中删除选定的端口转发列表。不能从 ASA 中删除端口转发列表，除非您先将其从 DAP 记录中删除。

步骤 6 选择 **Bookmarks** 选项卡，为特定用户会话 URL 配置书签。

- **Enable bookmarks** - 点击以便启用。如果取消选中，连接的门户页面中不会显示书签。
- **Bookmark** 下拉列表 - 选择已配置的书签，以便添加至 DAP 记录。
- **管理...** - 点击以添加、导入、导出和删除书签。
- **Bookmarks (unlabeled)** - 显示 DAP 记录的 URL 列表。
- **Add>>** - 点击以将下拉列表中的选定书签添加至右侧的 URL 区域。
- **Delete** - 点击以从 URL 列表区域中删除选定书签。您不能从 ASA 中删除书签，除非您先将其从 DAP 记录中删除。

步骤 7 选择 **Access Method** 选项卡，配置允许的远程访问的类型。

- **Unchanged** - 继续使用当前的远程访问方式。
- **Secure Client**-使用 Cisco Secure 客户端映像的 AnyConnect VPN 模块连接

  。
- **Web-Portal** - 使用无客户端 VPN 进行连接。
- **Both-default-Web-Portal**-通过无客户端或 Secure Client客户端进行连接，默认使用无客户端。
- **Both-default-Secure Client**-通过无客户端或 Secure Client进行连接，默认使用 Secure Client。

步骤 8 选择 **Secure Client** 选项卡，以选择永远在线 VPN 标志状态。

- Secure Client Always-On VPN - 确定是否没有改变、禁用了 Secure Client 服务配置文件中的永久在线 VPN 标志设置，或者是否应使用 Secure Client 服务配置文件设置。

  此参数需要为 Cisco 安全客户端的 AnyConnect VPN 模块提供安全移动解决方案许可支持的思科网络安全设备版本。它还需要支持“安全移动解决方案”功能的 Secure Client 版本。有关其他信息，请参阅《思科 *AnyConnect VPN* 客户端管理员指南》。

步骤 9 选择 Secure Client **自定义属性** 选项卡，查看之前定义的自定义属性并将其与此策略关联。您还可以定义自定义属性，然后将其与此策略关联。

自定义属性会被发送到 Secure Client，并且该客户端用其配置诸如延迟升级的功能。一个自定义属性有一个类型和一个命名值。先定义属性的类型，然后可以定义此类型的一个或多个命名值。有关为某个功能配置特定自定义属性的详细信息，请参阅所用 Secure Client 版本的 *Cisco Secure Client*管理员指南。

自定义属性可以在**配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 >** Secure Client**自定义属性**和**Secure ClientYY 自定义属性名称**中预定义。动态访问策略和组策略都可使用预定义的自定义属性。

使用 DAP 配置 SAML 授权

您可以使用 DAP 配置 SAML 授权和组策略选择，而不必依赖外部服务器（RADIUS 或 LDAP）来检索授权属性。

可以将 SAML 身份提供程序配置为除身份验证断言外还发送授权属性。ASA 中的 SAML 服务提供程序组件解释 SAML 断言，并根据收到的断言进行授权或组策略选择。使用 ASDM 配置的 DAP 规则处理断言属性。

组策略属性必须使用属性名称 **cisco_group_policy**。此属性不依赖于正在配置的 DAP。但是，如果配置了 DAP，则可以将其用作 DAP 策略的一部分。

组策略对象选择

当接收到名为 **cisco_group_policy** 的属性时，相应的值会被用于选择连接组策略。

建立连接后，可以从多个源获取组策略信息，并将其组合以形成应用于连接的有效组策略。

组合收到的组策略信息时，可能出现以下情况：

在 SAML 身份验证中接收的组策略，未配置授权

在这种情况下，有效的组策略按优先级降序确定：

1. SAML 属性中指定的组策略。
2. 在隧道组中指定的组策略。
3. 默认组策略。

在 SAML 身份验证中接收的组策略，已配置授权

在这种情况下，有效的组策略按优先级降序确定：

1. 授权属性中指定的组策略。
2. 用户组策略：使用从授权服务器返回的值（如果有）。
3. 用户组策略：使用 SAML 属性中返回的值。
4. 在隧道组中指定的组策略。

5. 默认组策略。

过程

步骤 1 在 ASDM，选择 **配置** > **远程访问 VPN** > **网络 (客户端) 访问** > **动态访问策略** > **添加/编辑动态访问策略** 。

步骤 2 在 AAA 属性选择区域中，点击 **添加**。

a) 从 **AAA 属性类型** 下拉列表中，选择 SAML。

b) 指定 *memberOf* 作为 **属性 ID**。

c) 输入 *memberOf* 属性 **值** ，如果已配置 AD 服务器组，请点击 **Get AD Group** 。

要配置其他 AD 服务器组，请转至 **配置** > **远程访问 VPN** > **AAA/本地用户** > **AAA 服务器组**。

要配置组策略选择属性，请根据需要在同一 DAP 策略或另一个 DAP 策略中选择以下设置：

- **AAA 属性类型**：SAML
- **属性 ID**：cisco_group_policy
- **值**：组策略的名称

步骤 3 点击**确定 (OK)**。

步骤 4 点击 **确定 (OK)** 保存 DAP 策略。

执行 DAP 跟踪

DAP 跟踪显示所有连接的设备的 DAP 终端属性。

过程

步骤 1 从 SSH 终端登录至 ASA，并进入 Privileged Exec 模式。

在 Privileged Exec 模式中，ASA 会提示：`hostname#`。

步骤 2 请启用 DAP 调试，以便在终端窗口中显示此会话的所有 DAP 属性：

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

步骤 3 （可选） 为搜索 DAP 跟踪的输出，请将此命令的输出结果发送至系统日志。要了解有关登录 ASA 的详细信息，请参阅《思科 *ASA* 系列常规操作 *ASDM* 配置指南》的配置登录。

DAP 示例

使用 DAP 定义网络资源

本示例显示如何将动态访问策略配置为给用户或组配置网络资源的一种方法。名为 Trusted_VPN_Access 的 DAP 策略允许无客户端和 Cisco Secure 客户端的 AnyConnect VPN 访问。名为 Untrusted_VPN_Access 的策略只允许无客户端 VPN 访问。

过程

步骤 1 在 ASDM 中，依次转至**Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Dynamic AccessPolicies** > **Add/Edit Dynamic Access Policy** > **Endpoint**。

步骤 2 为每个策略配置以下属性：

属性	**Trusted_VPN_Access**	**Untrusted_VPN_Access**
Endpoint Attribute Type Policy	Trusted	不受信任
Endpoint Attribute Process	ieexplore.exe	-
Advanced Endpoint Assessment	AntiVirus= McAfee Attribute	
CSD Location	Trusted	不受信任
LDAP memberOf	Engineering, Managers	Vendors
ACL		Web-Type ACL
Access	**Secure Client** 和 **Web** 门户	**Web Portal**

使用 DAP 应用 WebVPN ACL

DAP 可直接实施访问策略属性的子集，包括网络 ACL（用于 IPsec 和 Secure Client）、URL 列表和函数。它不能直接实施，例如欢迎信息或分割隧道列表，这些由组策略实施。Add/Edit Dynamic Access Policy 窗格中的 Access Policy Attributes 选项卡提供了 DAP 可直接实施的属性的完整菜单。

Active Directory/LDAP 将用户组策略成员资格存储为用户条目中的“memberOf”属性。定义一个 DAP，以便 ASA 对 AD 组 (memberOf) = Engineering 中的用户应用配置的 Web 类型 ACL。

过程

步骤 1 在 ASDM 中，转至“添加 AAA 属性”窗格，**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **动态访问策略** > **添加/编辑动态访问策略** > **AAA 属性部分** > **添加 AAA 属性**。

步骤 2 对于 AAA 属性类型，请使用下拉列表选择 **LDAP**。

步骤 3 在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 4 在 Value 字段中，使用下拉列表选择 =，并在相邻字段中输入 Engineering。

步骤 5 在此窗格的 Access Policy Attributes 区域中，点击 Web-Type ACL Filters 选项卡。

步骤 6 使用 Web-Type ACL Filters 下拉列表，以便选择您要应用于 AD group (memberOf) = Engineering 中的用户的 ACL。

执行 CSD 检查，并通过 DAP 应用策略

本示例将创建检查用户是否属于两个特定 AD/LDAP 组（Engineering 和 Employees）和特定 ASA 隧道组的 DAP。然后将一个 ACL 应用至该用户。

DAP 应用的 ACL 将控制资源的访问。它们将覆盖在 ASA 上定义组策略的任意 ACLS。此外，对于 DAP 未定义或控制的那些内容（例如分割隧道列表、横幅和 DNS），ASA 将应用常规 AAA 组策略继承规则和属性。

过程

步骤 1 在 ASDM 中，转至“添加 AAA 属性”窗格，**配置** > **远程访问 VPN** > **无客户端 SSL VPN 访问** > **动态访问策略** > **添加/编辑动态访问策略** > **AAA 属性部分** > **添加 AAA 属性**。

步骤 2 对于 AAA 属性类型，请使用下拉列表选择 LDAP。

步骤 3 在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 4 在 Value 字段中，使用下拉列表选择 =，并在相邻字段中输入 Engineering。

步骤 5 在 Attribuet ID 字段中，输入 memberOf，正如此处所示。大小写非常重要。

步骤 6 在 Value 字段中，请使用下拉列表选择 =，在相邻字段中输入 Employees。

步骤 7 对于 AAA 属性类型，请使用下拉列表选择 Cisco。

步骤 8 选中 Tunnel 组框，使用下拉列表选择 =，并且在相邻下拉列表中选择适当的隧道组（连接策略）。

步骤 9 在 Access Policy Attributes 区域的 Network ACL Filters 选项卡中，选择要应用于符合之前步骤定义的 DAP 条件的用户的 ACL。

使用 DAP 检查会话令牌安全

当 ASA 对来自 Secure Client的 VPN 连接请求进行身份验证时，ASA 会向客户端返回会话令牌。从 AnyConnect 4.9 (MR1) 开始，ASA 和 Secure Client 支持为会话令牌提供增强安全性的机制。您必须配置 DAP 以确保 Secure Client 支持会话令牌安全。

使用此DAP与终端属性设置和LUA脚本拒绝来自不支持令牌安全的Secure Client版本的连接尝试。

过程

步骤 1 在 ASDM，选择 **配置** > **远程访问 VPN** > **网络 (客户端) 访问** > **动态访问策略** > **添加/编辑动态访问策略** 。

步骤 2 在终端属性选择区域中，点击 **添加**。

a) 从 **终端属性类型** 下拉列表中，选择应用。

b) 对于 **客户端类型**，选择等号 (=) 运算符，然后从下拉列表中选择 Secure Client 。

c) 点击**确定 (OK)**。

步骤 3 配置 **高级** 选择条件：

a) 选择 **AND** 运营商。

b) 添加 **逻辑表达式**

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

步骤 4 在 **操作** 区域中，选择 **终止**。

步骤 5 添加可选的用户消息，然后点击 **确定**。

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。