部署ASA 9.X动态访问策略(DAP)

目录

简介

本文档介绍ASA 9.x动态访问策略(DAP)的部署、功能和用法。

先决条件

要求

思科建议您了解以下主题：

- 虚拟专用网络(VPN)网关
- 动态访问策略(DAP)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

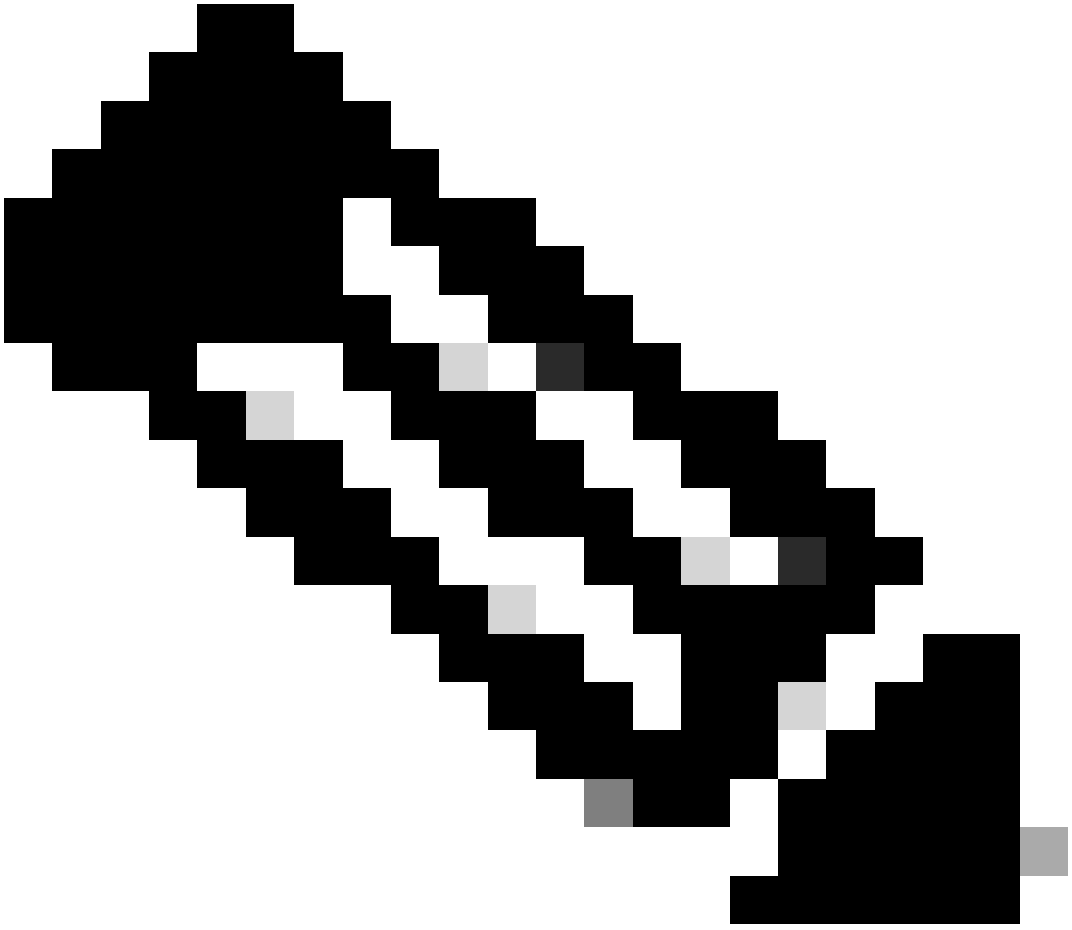
背景信息

虚拟专用网络(VPN)网关在动态环境中运行。多个变量可能会影响每个VPN连接；例如，频繁更改的内联网配置、每个用户可在组织内担任的各种角色，以及从具有不同配置和安全级别的远程访问站点登录。就用户授权任务而言，动态 VPN 环境中的该项任务要远远复杂于拥有静态配置的网络

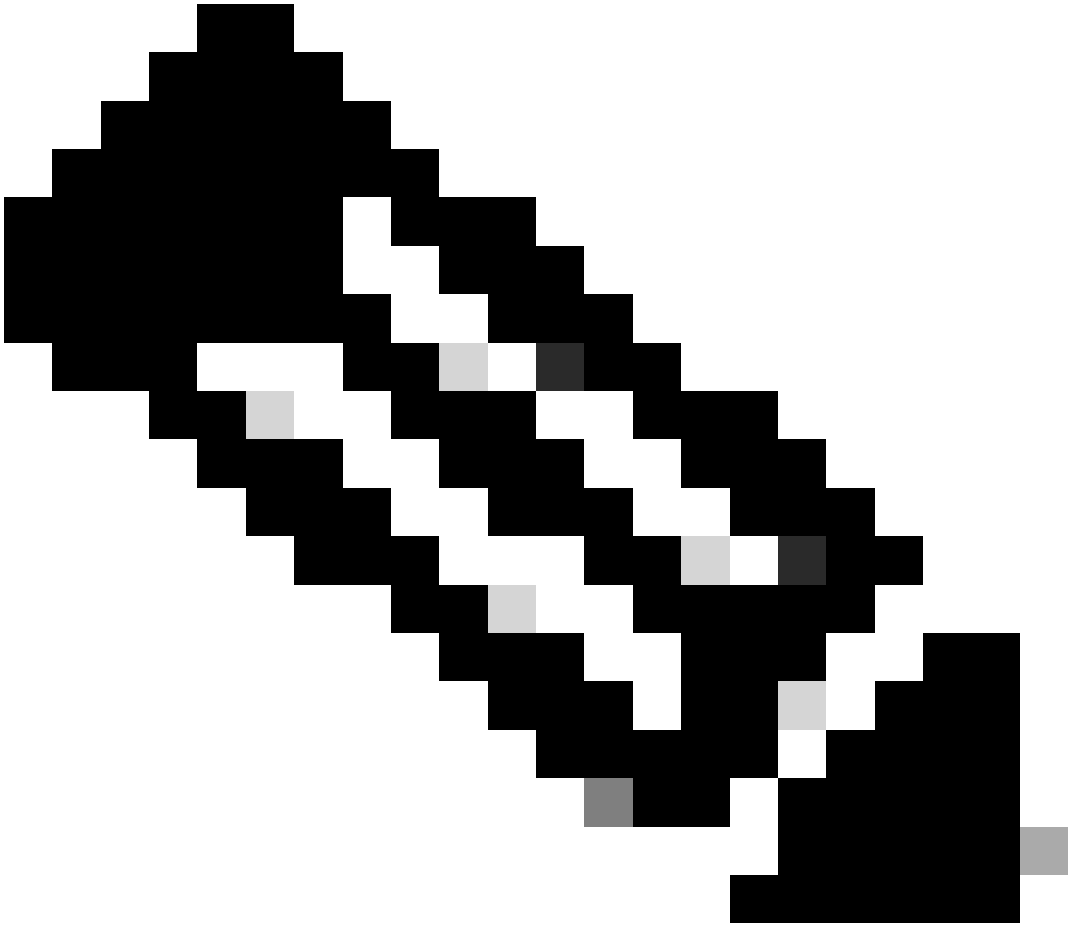
。

动态访问策略(DAP)是一项功能，可用于配置可解决VPN环境动态变化的授权。通过设置一组访问控制属性并将其与特定的用户隧道或会话相关联，您就可以创建动态访问策略。这些属性可解决有关多种组成员资格和终点安全的问题。

例如，安全设备根据您定义的策略向特定用户授予对特定会话的访问权限。它通过从一个或多个DAP记录中选择和/或聚合属性来生成整个用户身份验证的DAP。它根据远程设备的终点安全信息和/或身份验证用户的 AAA 授权信息来选择这些 DAP 记录。然后，安全设备就会将这些 DAP 记录应用于用户隧道或会话。



注意：包含DAP策略选择属性的dap.xml文件存储在ASA闪存中。虽然您可以将dap.xml文件导出到机外，对其进行编辑（如果您知道XML语法），然后重新导入，但请非常小心，因为如果配置有误，可能会导致ASDM停止处理DAP记录。没有CLI来处理此部分的配置。



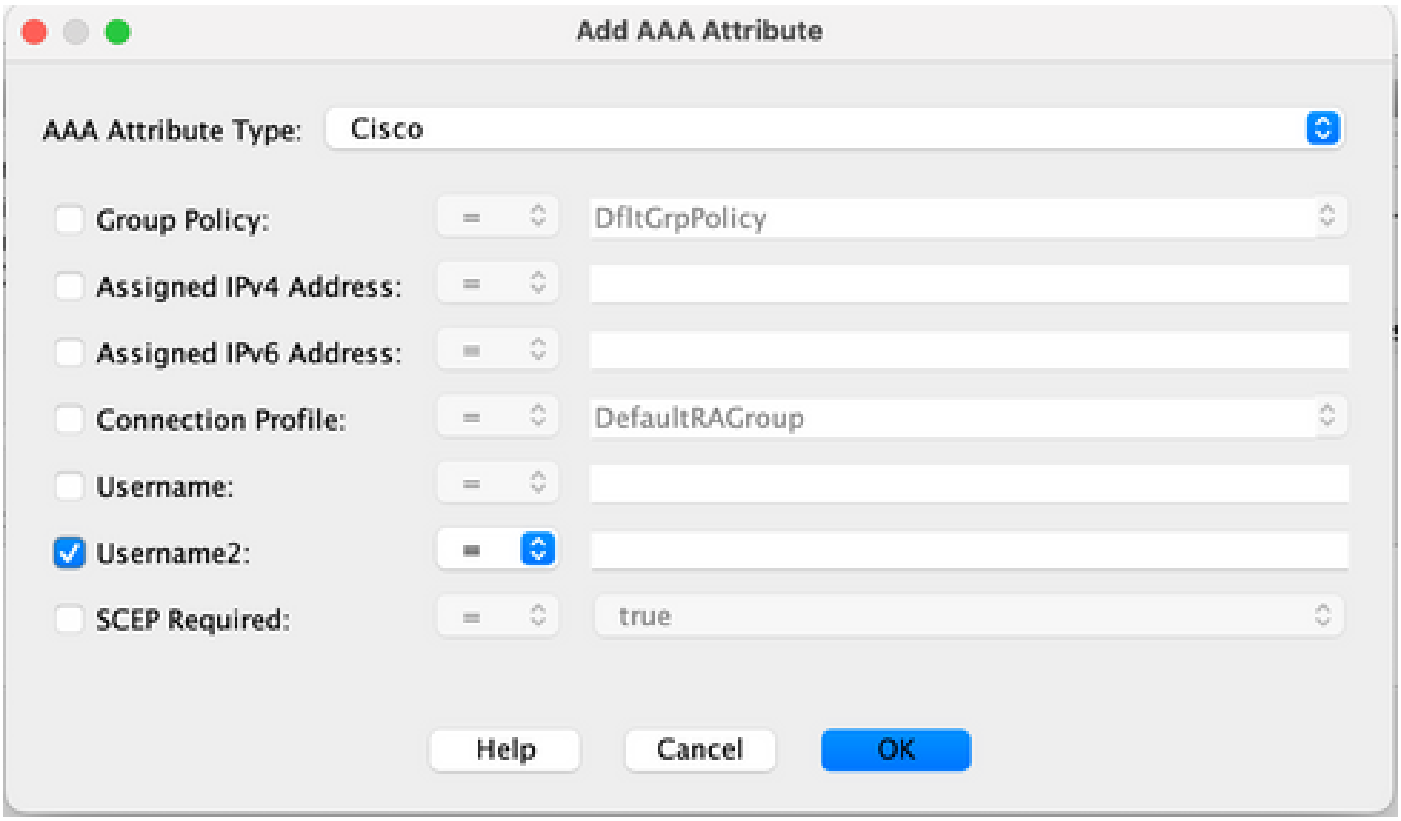
注意：尝试通过CLI配置dynamic-access-policy-record访问参数会导致DAP停止工作，但ASDM会正确管理这些参数。避免CLI，并始终使用ASDM管理DAP策略。

DAP 和 AAA 属性

DAP 是对 AAA 服务所做的补充，它提供了一组有限的授权属性，这些属性可以覆盖 AAA 提供的属性。安全设备可以根据用户的 AAA 授权信息选择 DAP 记录。安全设备可以根据此信息选择多个 DAP 记录，然后聚合这些记录以分配 DAP 授权属性。

您可以从 Cisco AAA 属性层次结构中指定 AAA 属性，也可以在安全设备从 RADIUS 或 LDAP 服务器接收到的全套响应属性中进行指定，如图 1 所示。

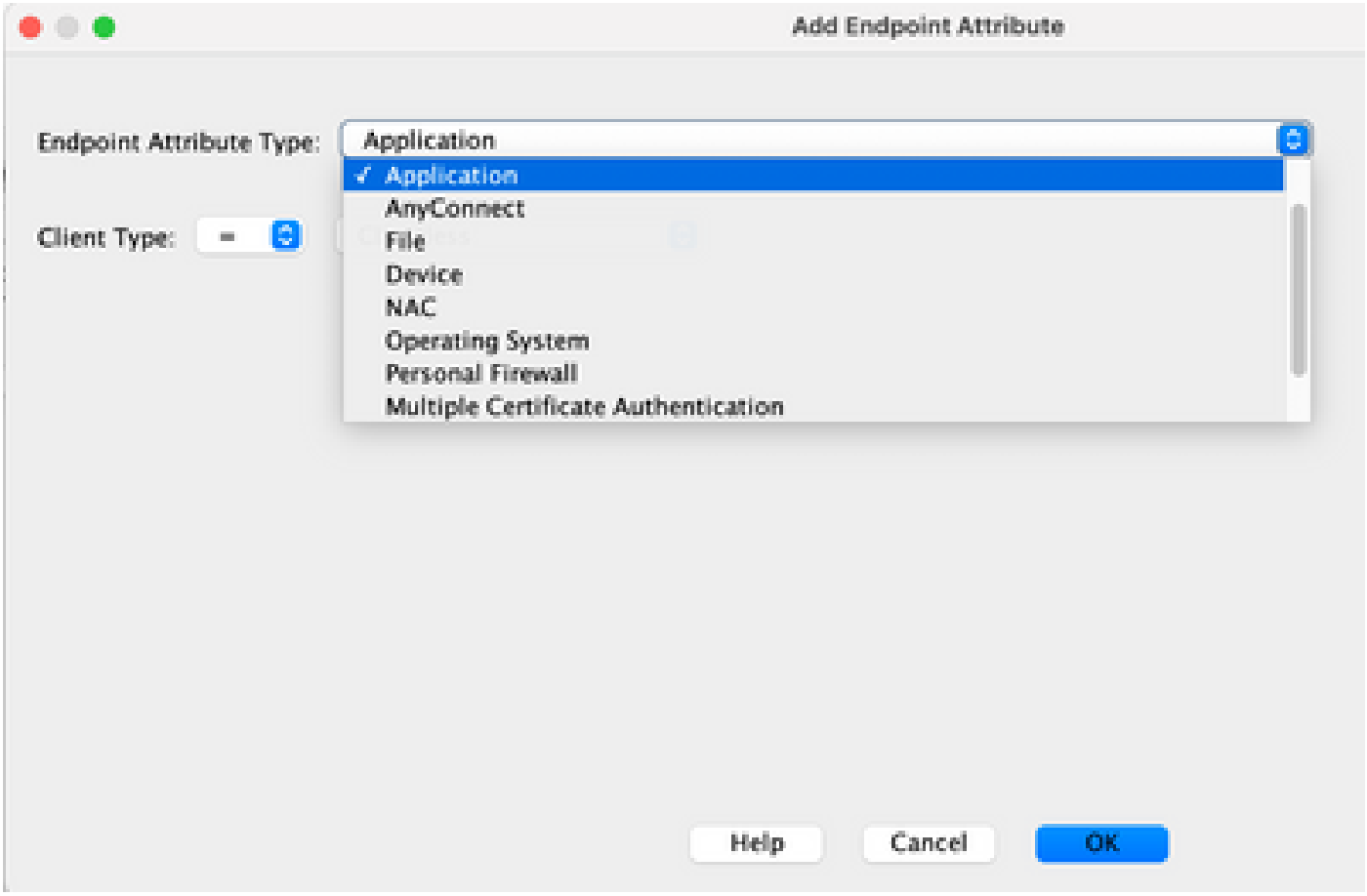
图 1.DAP AAA属性GUI



DAP 和终点安全属性

除AAA属性外，安全设备还可以使用您配置的状态评估方法获取终端安全属性。如图2所示，其中包括基本主机扫描、安全桌面、标准/高级终端评估和NAC。获取终端评估属性并在用户身份验证之前发送到安全设备。但是，AAA 属性（包括整体 DAP 记录）将在用户身份验证过程中检验。

图 2.终端属性GUI

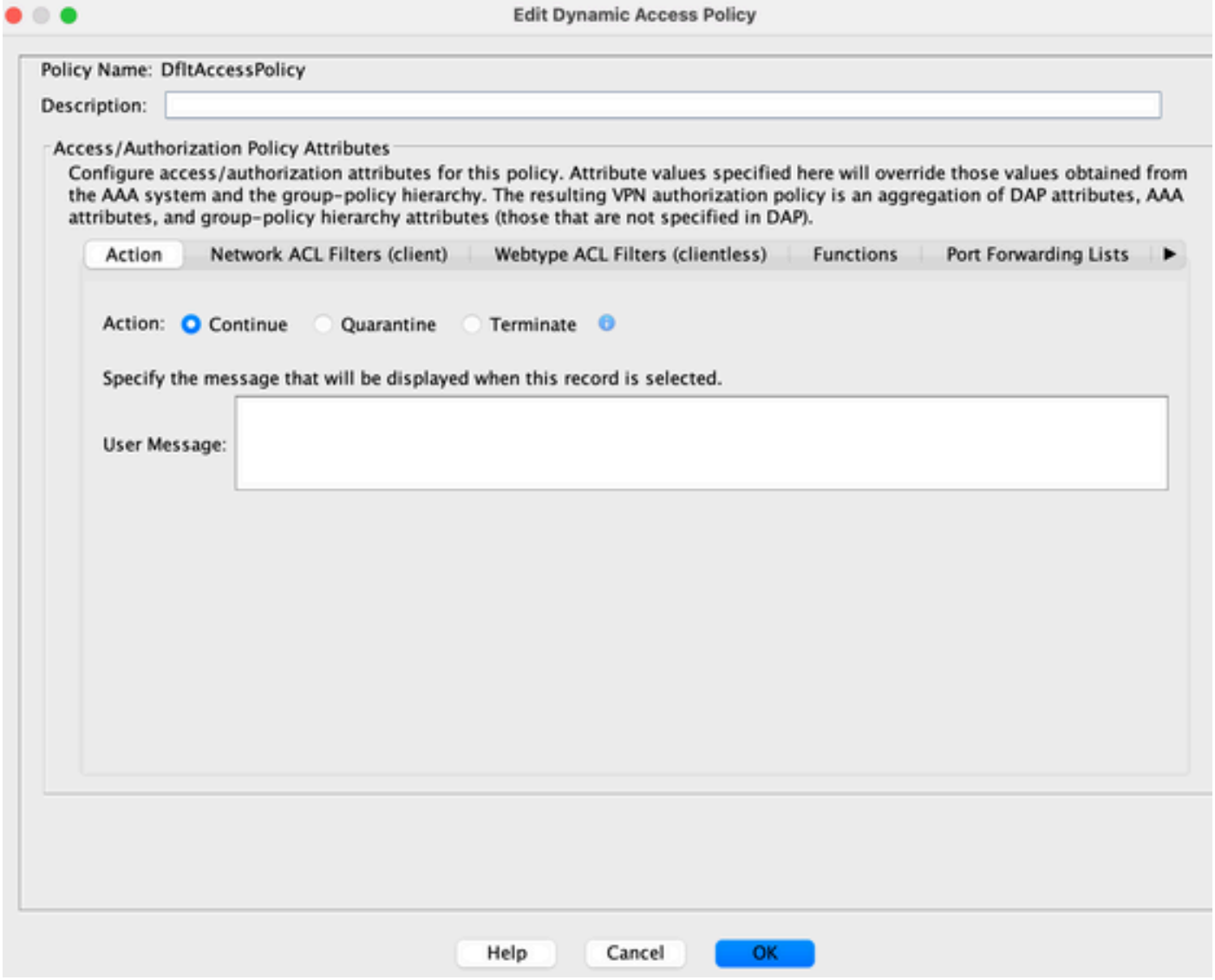


默认动态访问策略

在引入和实施DAP之前，与特定用户隧道或会话关联的访问策略属性/值对是在ASA上本地定义的（即，隧道组和组策略）或通过外部AAA服务器映射。

默认情况下总是强制执行 DAP。例如，通过隧道组、组策略和AAA实施访问控制而不显式实施DAP仍可以获得此行为。对于传统行为，无需对 DAP 功能的配置（包括默认 DAP 记录和 DfltAccessPolicy）进行任何更改，如图 3 所示。

图 3.默认动态访问策略



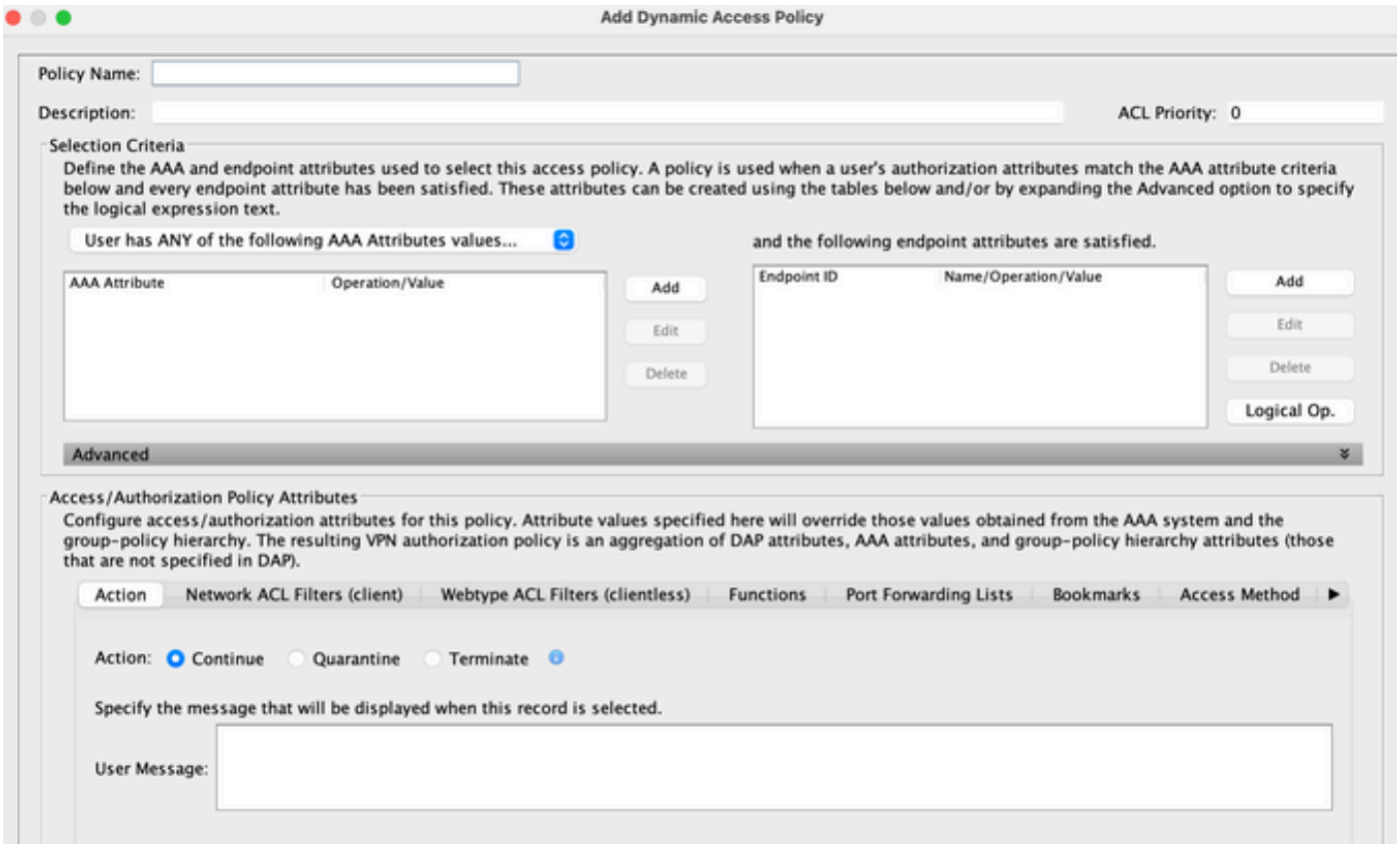
然而，如果DAP记录中的任何默认值已更改(例如，DfltAccessPolicy中的Action：参数已从默认值更改为Terminate，并且未配置其他DAP记录)，则默认情况下，通过身份验证的用户可以匹配DfltAccessPolicy DAP记录，并且可以拒绝VPN访问。

因此，需要创建并配置一个或多个DAP记录，以授权VPN连接并定义通过身份验证的用户有权访问哪些网络资源。因此，DAP（如果已配置）可以优先于传统策略实施。

配置动态访问策略

使用DAP定义用户可以访问的网络资源时，需要考虑许多参数。例如，如果您确定连接终端是否来自托管、非托管或不受信任的环境，请确定识别连接终端所需的选择标准，并根据终端评估和/或AAA凭证（连接用户有权访问哪些网络资源）。为此，您必须首先熟悉DAP特性和功能，如图4所示。

图 4.动态访问策略



在配置 DAP 记录时，需要考虑两个主要组成部分：

- Selection Criteria（包括 Advanced 选项）
- Access Policy Attributes

Selection Criteria 部分由管理员用于配置 AAA 和终点属性，这些属性将用于选择特定的 DAP 记录。当用户的授权属性与 AAA 属性标准相匹配、并且已满足每个终点属性时，将使用 DAP 记录。

例如，如果选择了AAA Attribute Type LDAP (Active Directory)，则Attribute Name字符串是memberOf，Value字符串是Contractors，如图5a所示，验证用户必须是Active Directory组Contractors的成员才能匹配AAA属性条件。

除了满足AAA属性条件外，身份验证用户还需要满足终端属性条件。例如，如果管理员配置为确定连接终端的安全状态并基于该安全状态评估，则管理员可以使用此评估信息作为图5b所示的终端属性的选择条件。

图 5a.AAA 属性标准

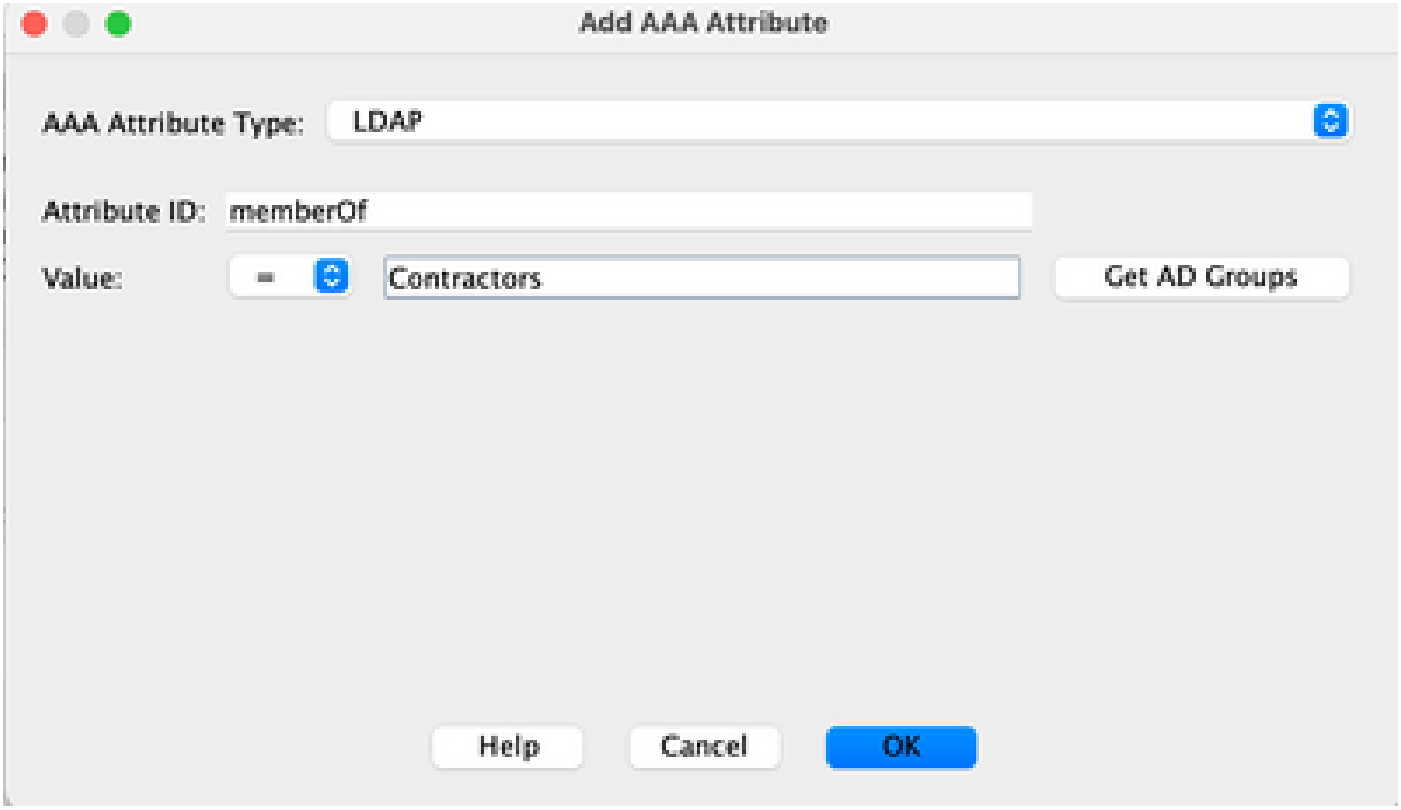


图 5b.终点属性标准

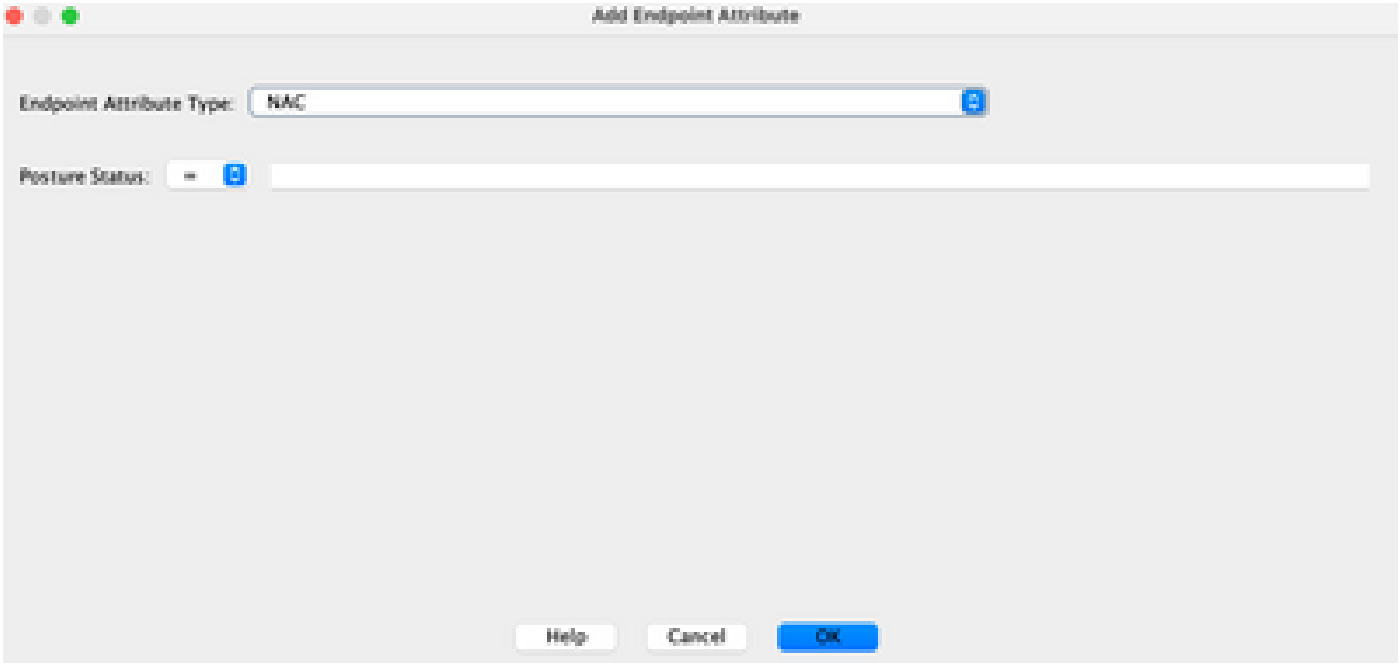
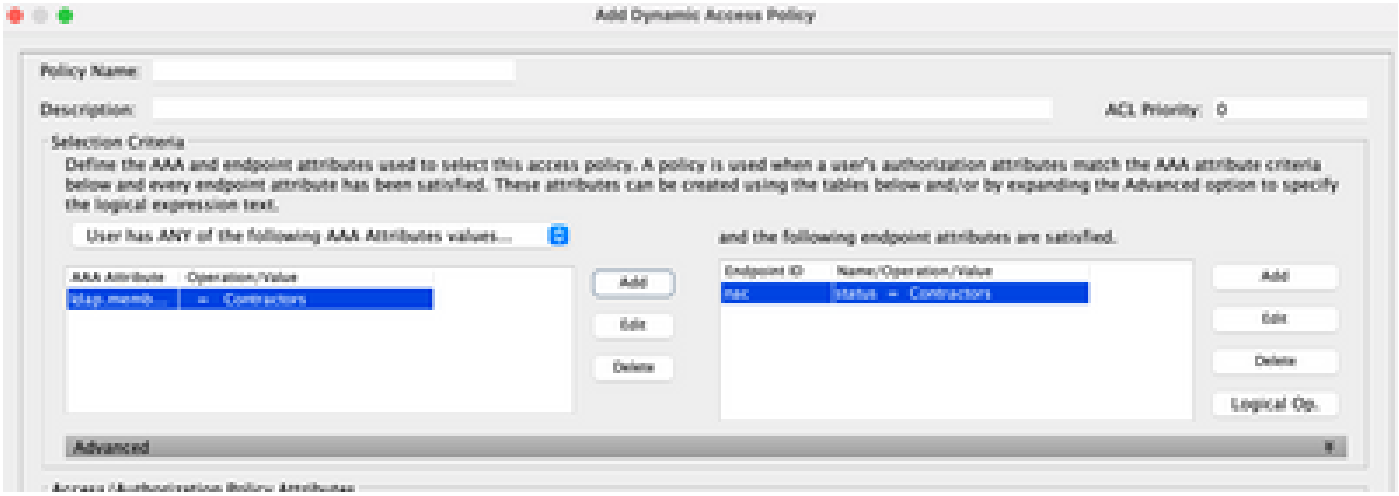


图 6.AAA和终端属性条件匹配



如图 6 所示使用表格和/或如图 7 所示展开 Advanced 选项以指定逻辑表达式，可创建 AAA 和终点属性。目前，逻辑表达式是使用EVAL函数构建的，例如EVAL (endpoint.av.McAfeeAV.exists，"EQ"，"true"，"string")和EVAL (endpoint.av.McAfeeAV.description，"EQ"，"McAfee VirusScan Enterprise"，"string")，这些函数表示AAA和/或终端选择逻辑操作。

如果您需要添加选择标准（AAA和终端属性区域中无法添加的条件除外），则逻辑表达式非常有用，如前所示。例如，虽然可以将安全设备配置为使用满足任意、所有或不满足任何指定条件的AAA属性，但终端属性是累积的，必须全部满足。要让安全设备使用一个或另一个终点属性，需要在 DAP 记录的 Advanced 部分下创建适当的逻辑表达式。

图 7.用于创建高级属性的逻辑表达式GUI

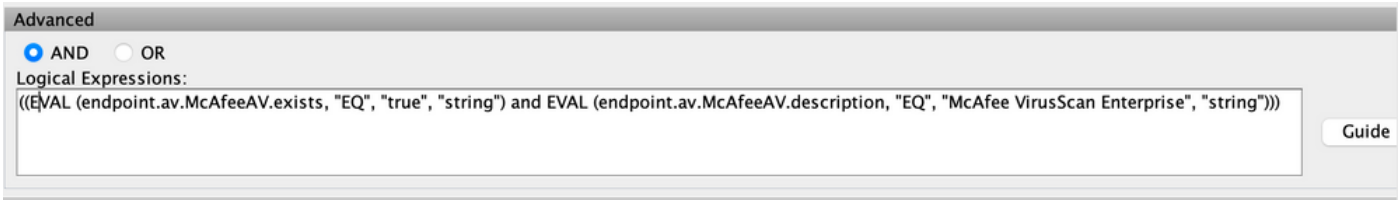
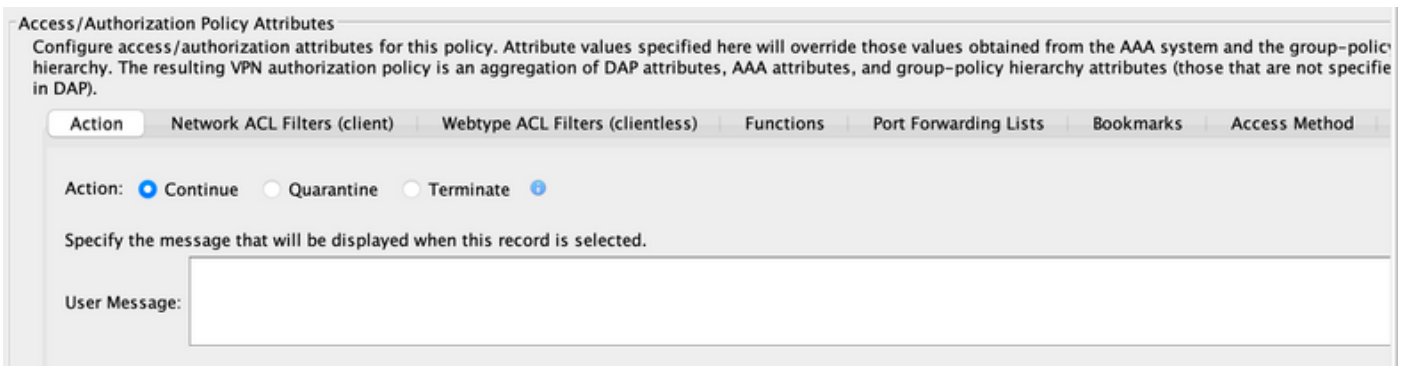


图 8 所示的 Access Policy Attributes 部分由管理员用于针对特定的 DAP 记录配置 VPN 访问属性。当用户授权属性与AAA、终端和/或逻辑表达式条件匹配时，可以实施此部分中配置的访问策略属性值。此处指定的属性值可以覆盖从AAA系统获取的那些值，包括现有用户、组、隧道组和默认组记录中的值。

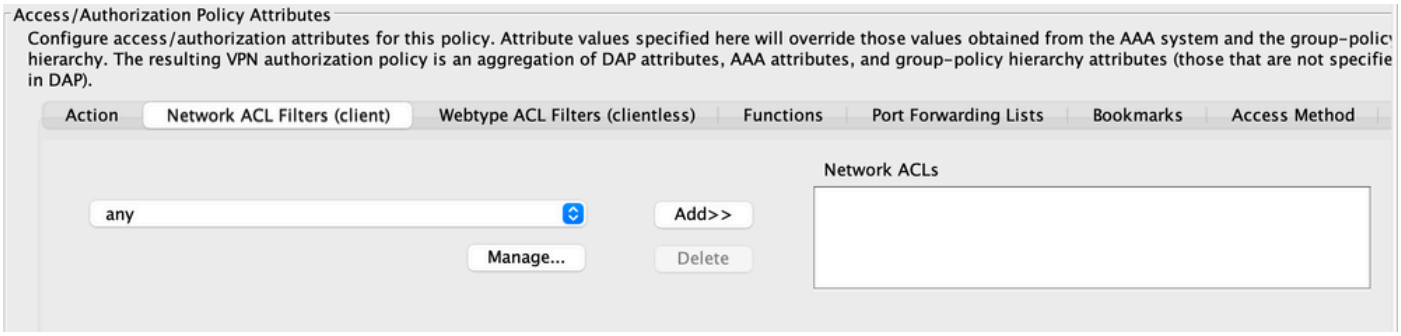
DAP 记录具有一组有限的、可配置的属性值。这些值位于图8至图14所示的选项卡下：

图 8.操作—指定要应用于特定连接或会话的特殊处理。



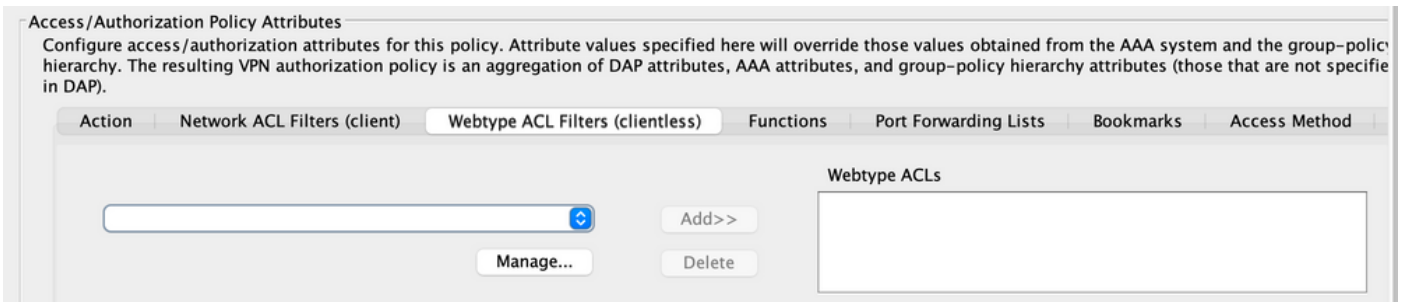
- Continue -（默认值）单击此值可将访问策略属性应用于会话。
- Terminate - 单击此值可终止会话。
- User Message - 输入一段文本消息，选择此 DAP 记录时，将在门户页上显示该消息。最多可输入 128 个字符。用户消息显示为黄色球体。当用户登录时，该球体将闪烁三次以引起注意，然后就会静止。如果选择了多个 DAP 记录，并且每个记录都具有用户消息，则将显示所有用户消息。另外，可以在此类消息中加入 URL 或其他嵌入式文本，但要求使用正确的 HTML 标记。

图 9网络ACL过滤器选项卡—用于选择和配置网络ACL以应用于此DAP记录。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，安全设备将拒绝该 ACL 配置。



- 网络ACL下拉框中已配置网络ACL以添加到此DAP记录中。只有具有所有允许或拒绝规则的ACL才符合条件，而且只有这些ACL会显示在此处。
- Manage - 单击此按钮可添加、编辑和删除网络 ACL。
- 网络ACL列出此DAP记录的网络ACL。
- Add - 单击此按钮可将下拉框中所选的网络 ACL 添加到右边的 Network ACLs 列表。
- Delete - 单击此按钮可从 Network ACLs 列表中删除突出显示的网络 ACL。如果某个 ACL 已分配到 DAP 或其他记录，则不能删除。

图 10.Web-Type ACL Filters选项卡-通过此选项卡，可以选择并配置应用于此DAP记录的Web型ACL。DAP 的 ACL 可以仅包含允许规则或仅包含拒绝规则。如果 ACL 同时包含允许和拒绝规则，安全设备将拒绝该 ACL 配置。

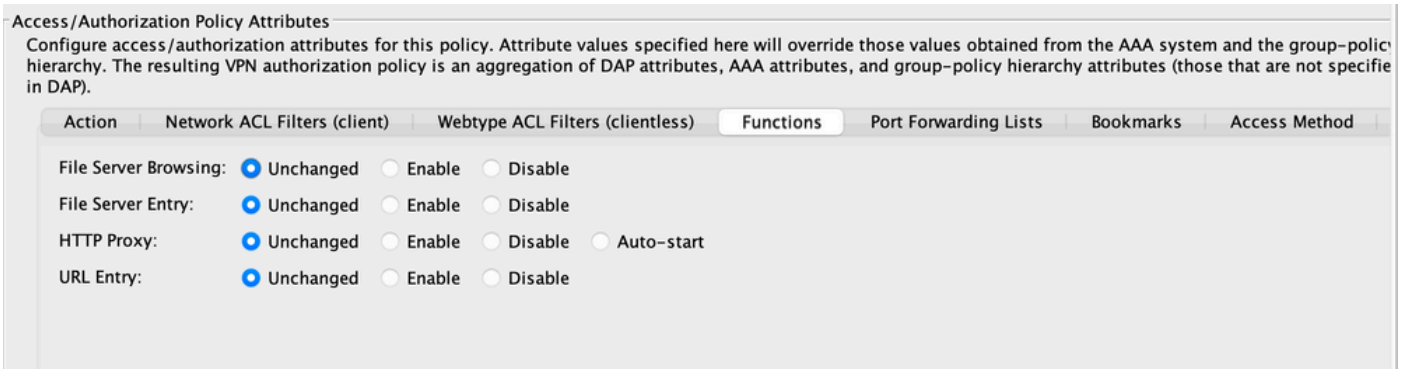


- Web-Type ACL 下拉框 - 选择已配置的 Web 型 ACL 以便添加到此 DAP 记录中。只有包含的规则全部都是允许规则或全部都是拒绝规则的 ACL 才符合规定，并且此处也只会显示这一类

ACL。

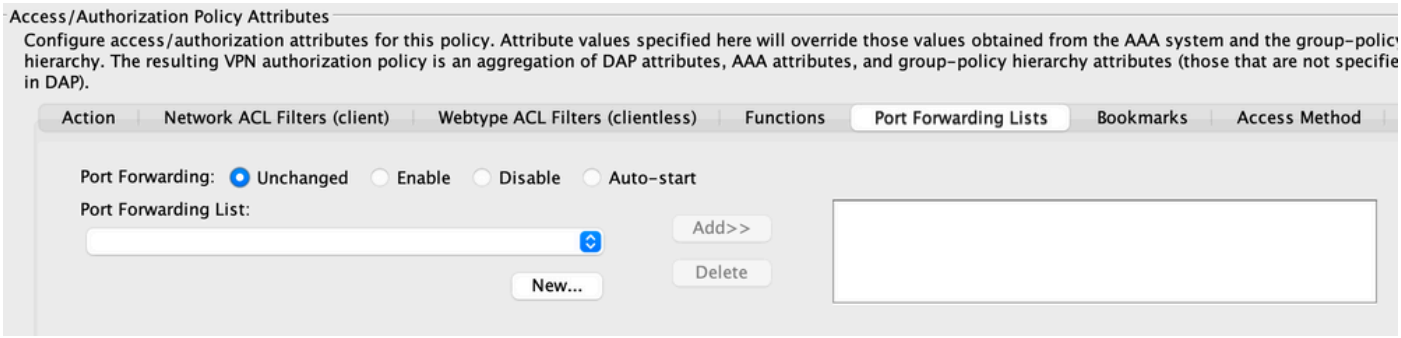
- Manage... —单击以添加、编辑和删除Web类型ACL。
- Web-Type ACLs 列表 - 显示此 DAP 记录的 Web 型 ACL。
- Add - 单击此按钮可将下拉框中所选的 Web 型 ACL 添加到右边的 Web-Type ACLs 列表。
- Delete - 单击此按钮可从 Web-Type ACLs 列表中删除 Web 型 ACL。如果某个 ACL 已分配到 DAP 或其他记录，则不能删除。

图 11.功能选项卡—可使用此选项卡为DAP记录配置文件服务器条目和浏览、HTTP代理和URL条目。



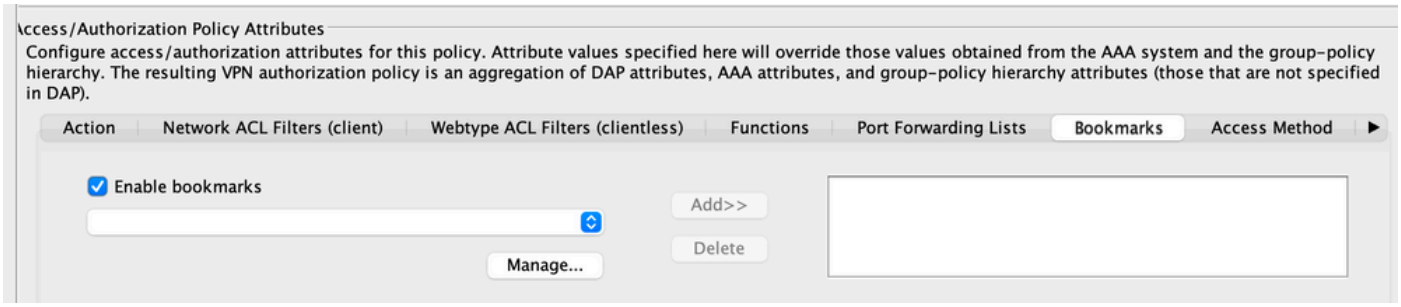
- File Server Browsing - 启用或禁用文件服务器的 CIFS 浏览或者共享功能。
- File Server Entry - 允许或拒绝用户在门户页上输入文件服务器路径和名称。启用时，会将文件服务器输入抽屉置于门户页上。用户可以直接输入 Windows 文件的路径名称，也可以下载、编辑、删除、重命名和移动文件，同时还可以添加文件和文件夹。还必须配置共享，以便用户在适用的 Microsoft Windows 服务器上进行访问。根据网络要求，用户可能需要在访问文件之前进行身份验证。
- HTTP Proxy - 影响 HTTP 小程序代理到客户端的转发。代理对于会干扰正确内容转换的技术（如 Java、ActiveX 和 Flash）非常有用。它可绕过解析/重写流程，同时确保安全设备继续使用。转发的代理会自动地修改浏览器的旧代理配置，并将所有 HTTP 和 HTTPS 请求重定向到新代理配置。它支持几乎所有客户端技术，包括HTML、CSS、JavaScript、VBScript、ActiveX和Java。它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上输入 HTTP/HTTPS URL。如果启用此功能，则用户可在 URL 输入框中输入 Web 地址，并且可使用无客户端 SSL VPN 访问这些网站。
- Unchanged -（默认值）单击以使用应用于此会话的组策略中的值。
- Enable/Disable - 单击以启用或禁用该功能。
- Auto-start - 单击以启用 HTTP 代理，并使 DAP 记录自动启动与这些功能关联的小程序。

图 12.Port Forwarding Lists选项卡—用于为用户会话选择和配置端口转发列表。



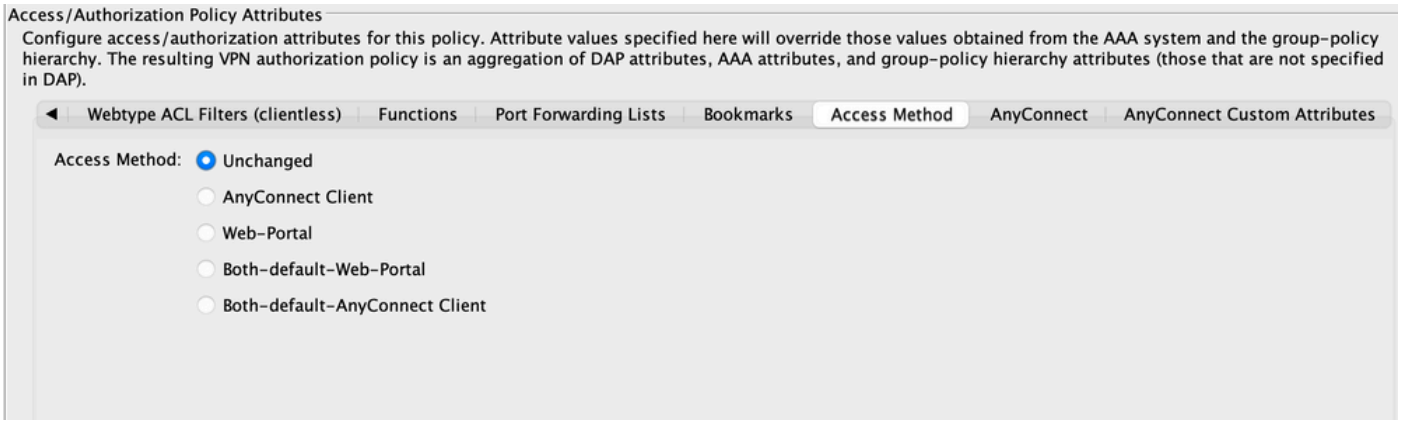
- Port Forwarding - 为应用于此 DAP 记录的端口转发列表选择一个选项。只有将 Port Forwarding 设置为 Enable 或 Auto-start 时，此字段中的其他属性才会启用。
- Unchanged - 单击以使用应用于此会话的组策略中的值。
- Enable/Disable - 单击以启用或禁用端口转发。
- Auto-start - 单击以启用端口转发，并使 DAP 记录自动启动与其端口转发列表关联的端口转发小程序。
- Port Forwarding List 下拉框 - 选择已配置的端口转发列表以便添加到 DAP 记录中。
- New - 单击以配置新的端口转发列表。
- Port Forwarding Lists - 显示 DAP 记录的端口转发列表。
- Add - 单击此按钮将下拉框中所选的端口转发列表添加到右边的 Port Forwarding Lists。
- Delete -点击以便从Port Forwarding列表中删除选定的端口转发列表。如果某个 ACL 已分配到 DAP 或其他记录，则不能删除。

图 13.Bookmarks选项卡—用于为用户会话选择和配置书签/URL列表。



- Enable bookmarks -单击以启用。如果未选中此框，则连接的门户页上不会显示书签列表
- Manage - 单击以添加、导入、导出和删除书签列表。
- Bookmarks Lists（下拉式）- 显示 DAP 记录的书签列表。
- Add - 单击此按钮将下拉框中所选的书签列表添加到右边的书签列表框中。
- 删除 - 单击此按钮可从书签列表框中删除所选的书签列表。除非首先从 DAP 记录中删除，否则无法从安全设备上删除书签列表。

图 14.Method选项卡—用于配置允许的远程访问类型。



- Unchanged -继续使用在会话组策略中设置的当前远程访问方法。
- AnyConnect Client - 使用 Cisco AnyConnect VPN 客户端进行连接。
- Web Portal -使用无客户端VPN连接。
- Both-default-Web-Portal - 通过无客户端或 AnyConnect 客户端进行连接，其中无客户端为默认值。
- Both-default-AnyConnect Client - 通过无客户端或 AnyConnect 客户端进行连接，其中 AnyConnect 为默认值。

如前所述，DAP记录具有一组有限的默认属性值，只有经过修改后，它们才优先于当前AAA、用户、组、隧道组和默认组记录。如果需要在DAP范围之外的其他属性值，例如，拆分隧道列表、横幅、智能隧道、门户自定义等，则需要通过AAA、用户、组、隧道组和默认组记录来实施它们。在这种情况下，这些特定属性值可以补充DAP，并且不能被覆盖。因此，用户将获得所有记录的属性值的累积集合。

聚合多个动态访问策略

管理员可以配置多个 DAP 记录，以应对各种各样的可变因素。因此，身份验证用户可以满足多个DAP记录的AAA和终端属性条件。因此，访问策略属性在这些策略中可能一致或冲突。在这种情况下，授权用户可以获取所有匹配DAP记录的累积结果。

这还包括通过身份验证、授权、用户、组、隧道组和默认组记录强制执行的唯一属性值。访问策略属性的累加结果将形成动态访问策略。下表列出了组合访问策略属性的示例。这些示例描述了 3 个组合 DAP 记录的结果。

表 1 中显示的 Action 属性的值可为 Terminate 或 Continue。如果在任何选定的DAP记录中配置了Terminate值，则聚合属性值为Terminate；如果在所有选定的DAP记录中配置了Continue值，则聚合属性值为Continue。

表 1.操作属性

属性名称	DAP#1	DAP#2	DAP#3	DAP
Action（示例 1）	继续	继续	继续	继续

Action（示例 2）	Terminate（终止）	继续	继续	terminate（终止）

表 2 中显示的 user-message 属性包含一个字符串值。聚合属性值可以是通过将所选DAP记录的属性值链接在一起而创建的行馈送（十六进制值0x0A）分隔的字符串。组合字符串中属性值的顺序无关紧要。

表 2.用户消息属性

属性名称	DAP#1	DAP#2	DAP#3	DAP
user-message	the quick	brown fox	Jumps over	the quick<LF>brown fox<LF>jumps over

表3中显示的无客户端功能启用属性（功能）包含Auto-start、Enable或Disable值。如果在任何所选DAP记录中配置了Auto-Start值，则聚合属性值可以是Auto-start。

如果任何所选DAP记录中没有配置自动启动值，并且至少在一个所选DAP记录中配置了Enable值，则可以启用聚合属性值。

如果在任何所选DAP记录中没有配置任何Auto-start或Enable值，并且至少在一个所选DAP记录中配置了“disable”值，则可以禁用聚合属性值。

表 3.无客户端功能启用属性（功能）

属性名称	DAP#1	DAP#2	DAP#3	DAP
port-forward	enable	disable		enable
file-browsing	disable	enable	disable	enable
file-entry			disable	disable
http-proxy	disable	auto-start	disable	auto-start
url-entry	disable		enable	enable

表4中显示的URL list和port-forward属性包含的值为字符串或逗号分隔字符串。聚合属性值可以是逗号分隔的字符串，该字符串由您从所选DAP记录中将属性值链接起来创建。可以删除组合字符串中的任何重复属性值。属性值在组合字符串中的排序方式无关紧要。

表 4.URL列表和端口转发列表属性

属性名称	DAP#1	DAP#3	DAP#3	DAP
url-list	a	b、c	a	a、b、c
port-forward		d、e	e,f	d、e、f

Access Method属性指定SSL VPN连接允许的客户端访问方法。客户端访问方法可以是仅AnyConnect客户端访问、仅Web门户访问、将Web门户访问作为默认的AnyConnect客户端或Web门户访问，或将AnyConnect客户端访问作为AnyConnect客户端访问作为默认的AnyConnect客户端或Web门户访问。表 5 中汇总了聚合属性值。

表 5.访问方法属性

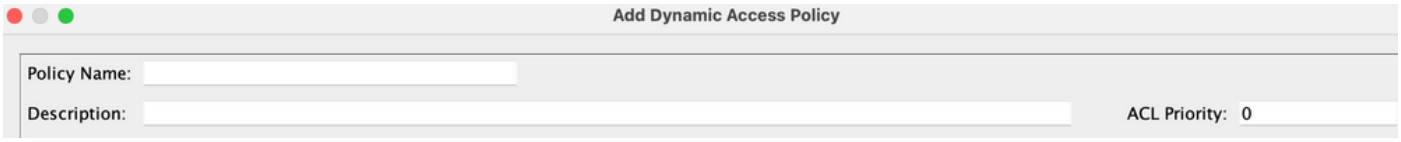
所选的属性值	聚合结果

AnyConnect Client	Web门户	Both-default-Web-门户	Both-default-AnyConnect Client	
			X	Both-default-AnyConnect Client
		X		Both-default-Web-Portal
		X	X	Both-default-Web-Portal
	X			Web-Portal
	X		X	Both-default-AnyConnect Client
	X	X		Both-default-Web-Portal
	X	X	X	Both-default-Web-Portal
X				AnyConnect Client
X			X	Both-default-AnyConnect Client
X		X		Both-default-Web-Portal
X		X	X	Both-default-Web-Portal
X	X			Both-default-Web-Portal
X	X		X	Both-default-AnyConnect Client
X	X	X		Both-default-Web-Portal
X	X	X	X	Both-default-Web-Portal

如果将网络（防火墙）和Web类型（无客户端）ACL过滤器属性相结合，DAP优先级和DAP ACL是需要考虑的两个主要组件。

图15所示的Priority属性并未聚合。聚合多个 DAP 记录中的网络和 Web 型 ACL 时，安全设备将使用此值对访问列表进行逻辑排序。安全设备按优先级从高到低的顺序对记录进行排序，优先级最低的在表底部。例如，值为 4 的 DAP 记录优先级高于值为 2 的记录。不能手动进行排序。

图 15.Priority - 显示 DAP 记录的优先级。

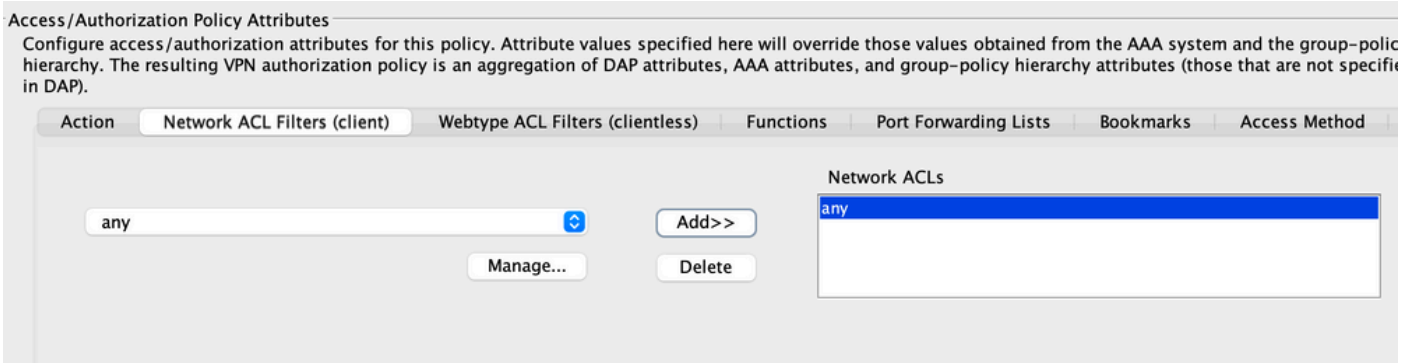


- Policy Name - 显示 DAP 记录的名称。
- Description - 描述 DAP 记录的用途。

DAP ACL属性仅支持符合严格Allow-List或严格Block-List ACL模型的访问列表。在允许列表 ACL模型中，访问列表条目指定规则“允许”对指定网络或主机的访问。在阻止列表 ACL模式下，访问列表条目指定拒绝访问指定网络或主机的规则。不一致的访问列表包含同时具有permit和deny规则的访问列表条目。如果为DAP记录配置了不符合规定的访问列表，则当管理员尝试添加该记录时，该访问列表可能会因配置错误而被拒绝。如果遵循的访问列表已分配给DAP记录，则对访问列表进行的

任何更改符合性特征的修改都可能会因配置错误而被拒绝。

图 16.DAP ACL -用于选择和配置网络ACL以应用于此DAP记录。



选择多个DAP记录时，将聚合网络（防火墙）ACL中指定的访问列表属性，以创建DAP防火墙ACL的动态访问列表。同样，将聚合Web类型（无客户端）ACL中指定的访问列表属性，以创建DAP无客户端ACL的动态访问列表。下一个示例重点介绍如何专门创建动态DAP防火墙访问列表。但是，动态DAP无客户端访问列表也可以执行相同的过程。

首先，ASA会为DAP Network-ACL 动态创建唯一名称，如表6所示。

表 6.动态DAP网络ACL名称

DAP 网络 ACL 名称
DAP-Network-ACL-X（其中X是可以增加以确保唯一性的整数）

第二，ASA从所选的DAP记录中检索Network-ACL属性，如表7所示。

表 7.网络ACL

所选的 DAP 记录	优先级	网络 ACL	网络 ACL 条目
DAP 1	1	101 和 102	ACL 101 具有 4 个拒绝规则，而 ACL 102 具有 4 个允许规则
DAP 2	2	201 和 202	ACL 201 具有 3 个允许规则，而 ACL 202 具有 3 个拒绝规则
DAP 3	2	101 和 102	ACL 101 具有 4 个拒绝规则，而 ACL 102 具有 4 个允许规则

第三，如果所选的2个或更多的DAP记录的优先级值相同，ASA将首先按DAP记录优先级编号对Network-ACL重新排序，然后按块列表重新排序。之后，ASA可以从每个网络ACL检索网络ACL条目，如表8所示。

表 8.DAP记录优先级

网络 ACL	优先级	白名单/黑名单访问列表模式	网络 ACL 条目
101	2	黑名单	4 个拒绝规则 (DDDD)

202	2	黑名单	3 个拒绝规则 (DDD)
102	2	白名单	4 个允许规则 (PPPP)
202	2	白名单	3 个允许规则 (PPP)
101	1	黑名单	4 个拒绝规则 (DDDD)
102	1	白名单	4 个允许规则 (PPPP)

最后，ASA会将网络ACL条目合并到动态生成的网络ACL中，然后返回动态网络ACL的名称，作为要实施的新网络ACL，如表9所示。

表 9.动态DAP网络ACL

DAP 网络 ACL 名称	网络 ACL 条目
DAP-Network-ACL-1	DDDD DDD PPPP PPP DDDD PPP

DAP 实施

管理员必须考虑实施DAP的原因有很多。一些深层次的原因就存在于要强制执行终点状态评估的情况下，和/或授权用户访问网络资源时要考虑更多细粒度 AAA 或策略属性的情况下。在下一个示例中，您可以配置DAP及其组件以标识连接终端并授权用户访问各种网络资源。

测试案例-客户端请求了具有以下VPN访问要求的概念验证：

- 能够检测员工终端并将其标识为受管或非受管。如果确定某终点为受管型（工作 PC），但是不满足状态要求，则必须拒绝该终点的访问。另一方面，如果确定员工的终点为非受管型（家庭 PC），则必须为该终点授予无客户端访问权限。
- 在无客户端连接终止时调用会话 cookie 和缓存清理的能力。
- 能够检测并强制在受管理的员工端点（如McAfee AntiVirus）上运行应用程序。如果没有此类应用程序，则必须拒绝该终点的访问。
- 能够使用AAA身份验证确定授权用户必须有权访问的网络资源。安全设备必须支持本地 MS LDAP 身份验证并支持多个 LDAP 组成员角色。
- 通过客户端/基于网络的连接进行连接时，允许本地LAN访问网络资源（例如网络传真和打印机）的能力。
- 对承包商提供授权访客访问的能力。承包商及其终端必须获得无客户端访问，而且与员工访问相比，他们对应用的门户访问必须受到限制。

在本示例中，您可以执行一系列配置步骤以满足客户端的VPN访问要求。可能有必要的配置步骤，但不直接与DAP相关，而其他配置则可以直接与DAP相关。ASA非常动态，可以适应许多网络环境。因此，可以通过多种方式定义 VPN 解决方案，并且在某些情况下会提供相同的最终解决方案。但是，所采用的方法受客户需求及其环境的驱动。

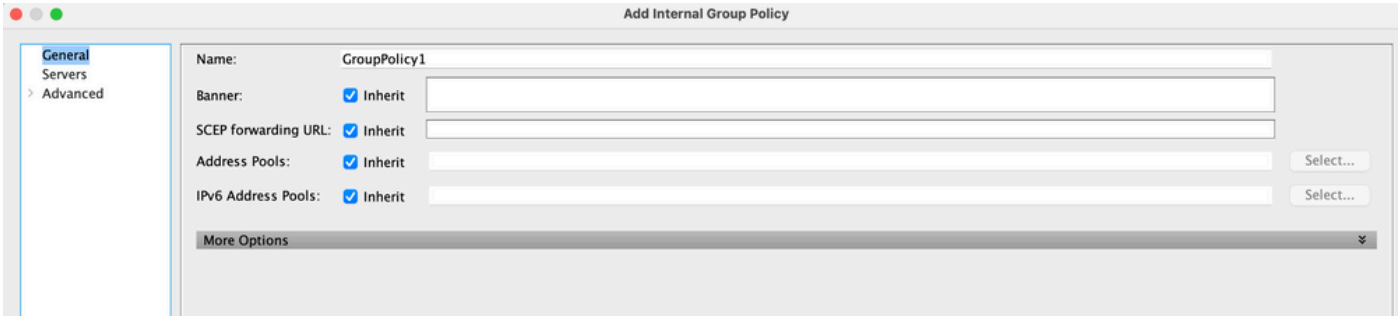
根据本文的性质和定义的客户端要求，您可以使用自适应安全设备管理器(ASDM)，并将大多数配置集中在DAP上。但是，您也可以配置本地组策略，以显示DAP如何补充和/或覆盖本地策略属性。在

此测试案例的基础上，您可以假设LDAP服务器组、分割隧道网络列表和基本IP连接（包括IP池和DefaultDNS服务器组）已预配置。

定义组策略 - 要定义本地策略属性，必须进行此配置。此处定义的部分属性在 DAP 中是无法配置的（例如，Local LAN Access）。（此策略也可用于定义无客户端和基于客户端的属性）。

导航到Configuration > Remote Access VPN > Network (Client) Access > Group Policies，然后添加内部组策略，如下所示：

图 17.组策略 - 定义特定于本地 VPN 的属性。

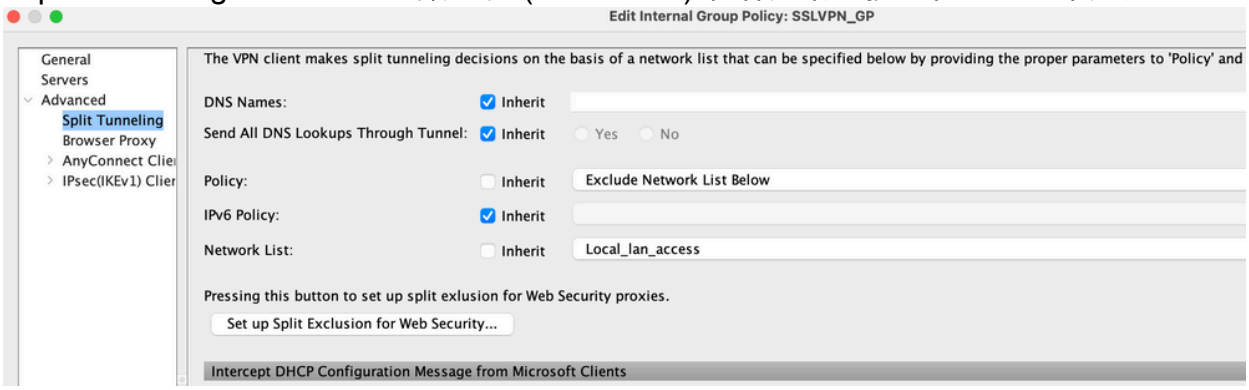


a. 在General链接下，为组策略配置nameSSLVPN_GP。

b. 还是在General链接下，单击More Optionsand configure only the Tunneling Protocol：Clientless SSLVPN。（您可以配置DAP以覆盖和管理访问方法。）

c. 在Advanced > Split Tunneling链接下，配置以下步骤：

图 18.Split Tunneling - 允许指定的数据流（本地网络）在客户端连接过程中绕过未加密的隧道。

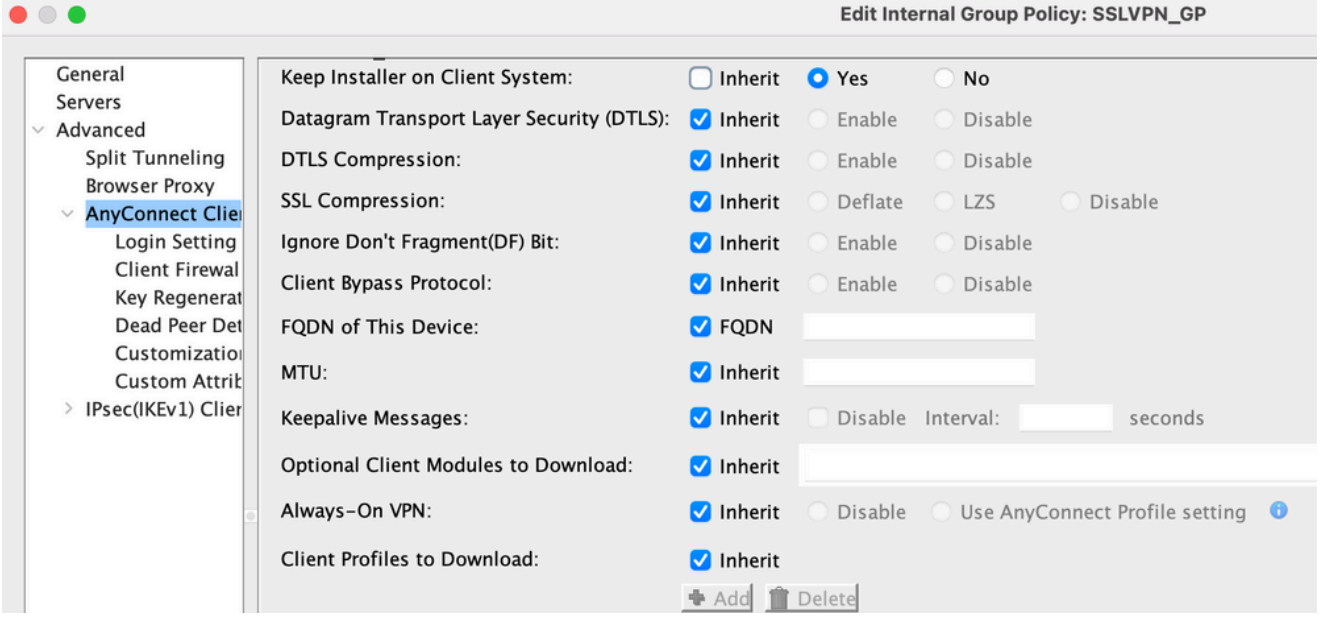


a. 策略：取消选中Inheritand selectExclude Network List。

b. Network List：取消选中Inheritand并选择列表名称Local_Lan_Access。（假设已预配置。）

d. 在Advanced > ANYCONNECT Client链接下，配置以下后续步骤：

图 19.SSL VPN 客户端安装程序 - 在 VPN 终止时，可将 SSL 客户端保留在终点上或进行卸载。



e. Keep Installer on Client System：取消选中Inheritand然后选择Yes。

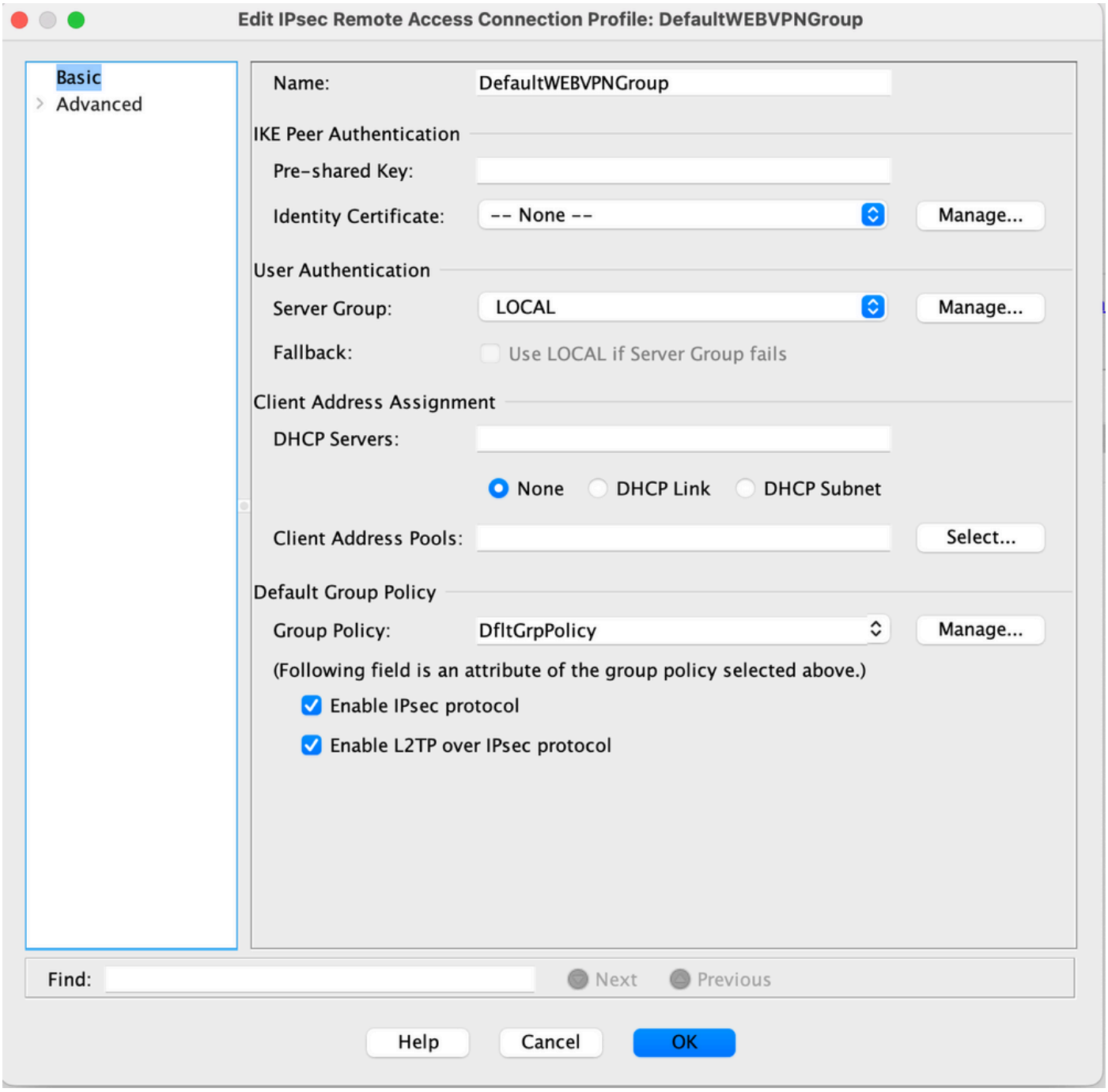
f. 单击“确定”>“应用”。

g. 应用您所做的配置更改。

定义连接配置文件-要定义AAA身份验证方法（例如LDAP）并将先前配置的组策略(SSLVPN_GP)应用于此连接配置文件，必须进行此配置。通过此连接配置文件进行连接的用户可受此处定义的属性以及在SSLVPN_GP组策略中定义的属性的限制。（此配置文件还可用于定义无客户端和基于客户端的属性）。

导航到Configuration > Remote Access VPN > Network (Client) Access > IPsec Remote Access Connection Profile并进行配置：

图 20.连接配置文件-定义本地VPN特定属性。



a. 在Connection Profiles部分下，编辑DefaultWEBVPNGroup，并在Basic链接下配置以下步骤：

   a. 身份验证-方法：AAA

   b. 身份验证- AAA服务器组：LDAP（假设已预配置）

   c. Client Address Assignment -客户端地址池：IP_Pool（假设已预配置）

   d. 默认组策略-组策略：SelectSSLVPN_GP

b. 应用您所做的配置更改。

为SSL VPN连接定义IP接口— 要在指定接口上终止客户端和无客户端SSL连接，必须进行此配置。

在接口上启用客户端/网络访问之前，必须先定义SSL VPN客户端映像。

1. 导航到Configuration > Remote Access VPN > Network (Client)Access > Anyconnect Client Software，然后从ASA闪存文件系统中添加下一个映像（“SSL VPN Client”映像）：(此映像可以从CCO，https://www.cisco.com下载)

   图 21.SSL VPN Client Image Install -定义要推送到连接终端的AnyConnect客户端映像。

   a. anyconnect-mac-4.x.xxx-k9.pkg

   b. 单击OK、OK再次单击，然后Apply。

2. 导航到配置(Configuration) >远程接入VPN (Remote Access VPN) >网络（客户端）接入(Network [Client] Access) > AnyConnect连接配置文件(AnyConnect Connection Profiles)，然后使用后续步骤启用此功能：

   图 22.SSL VPN Access Interface -定义用于终止SSL VPN连接的接口。 

   a. 在Access Interface部分下，启用：在下表中选择的接口上启用Cisco AnyConnect VPN客户端或传统SSL VPN客户端访问。

   b. 还是在Access Interfaces部分下，选中外部接口上的Allow Access。（此配置也可以在外部接口上启用SSL VPN无客户端访问。）

   c. 点击应用。

定义无客户端访问的书签列表（URL列表）-要定义要在门户上发布的基于Web的应用程序，必须进行此配置。您可以定义两个URL列表，一个用于员工，另一个用于承包商。

1. 导航到Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks，单击+添加，然后配置下一步：

   图 23.书签列表 - 定义将发布在 Web 门户上供用户访问的 URL。（专为员工访问而定制。）

   a. 将List Name：Employees加入书签，然后点击Add。

   b. 书签标题：公司内部网

   c. URL 值： https://company.resource.com

   •

   单击“确定”，然后再次单击“确定”。

   •

单击+添加并配置第二个书签列表（URL列表），如下所示：

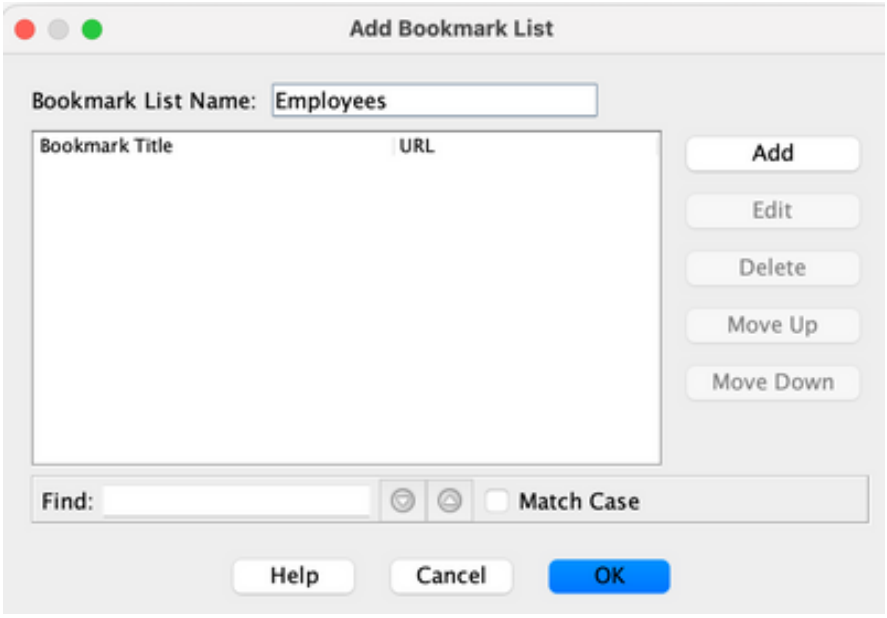


图 24.书签列表 - 专为访客访问而定制。

a.

将列表名称加入书签：**Contractors**，然后点击**Add**。

b.

书签标题：访客接入

c.

URL 值： https://company.contractors.com

- 单击“确定”，然后再次单击“确定”。
- 点击应用。

配置Hostscan：

-

导航到**Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image**，然后配置下一步：

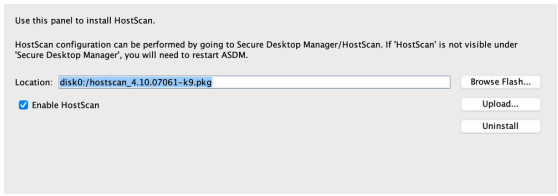


图 25.**HostScan Image Install -定义要推送到连接终端的HostScan映像。**

a.

从ASA闪存文件系统安装**disk0：/hostscan_4.xx.xxxxx-k9.**pkgimage。

b.

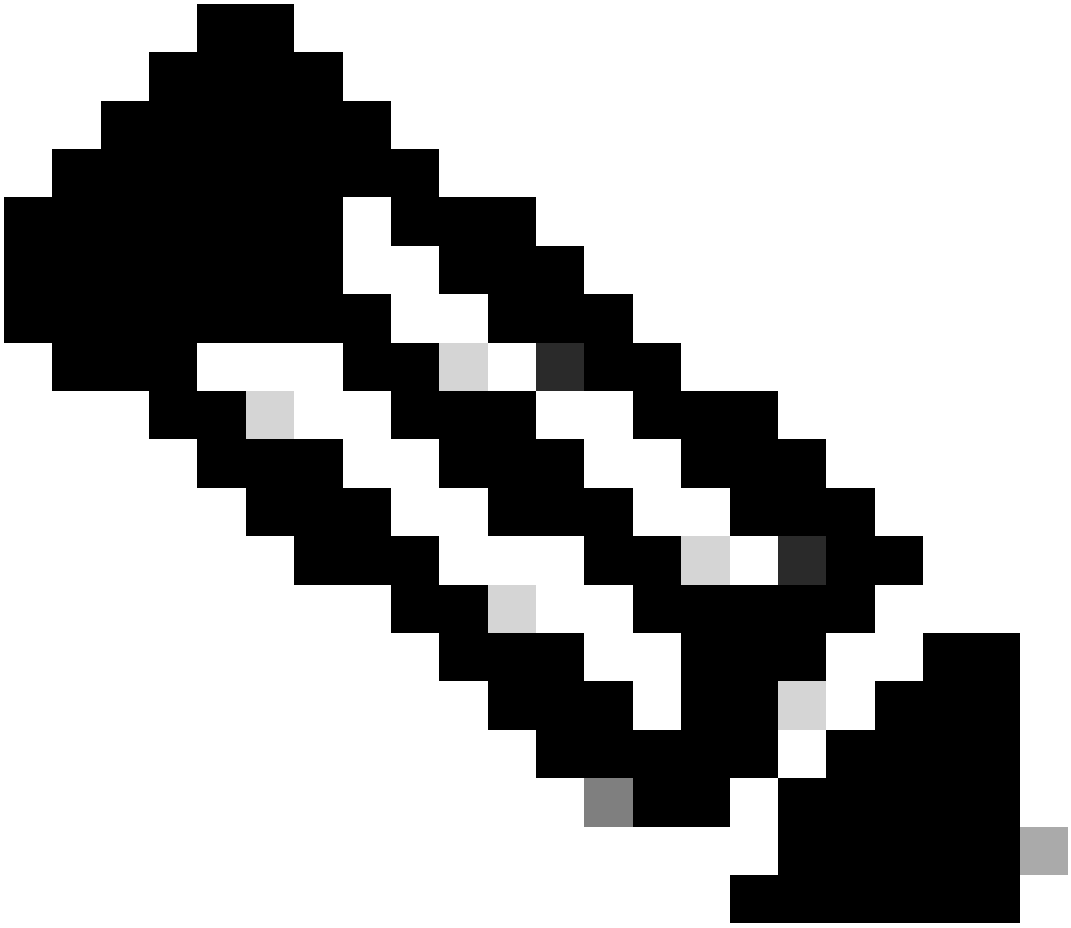
选中**Enable HostScan**。

c.

点击应用。

动态访问策略 - 要根据定义的 **AAA 和**终点评估标准验证连接的用户及其终点，必须进行此配置。如果满足DAP记录的已定义标准，则连接用户可以访问与该DAP记录相关联的网络资源。DAP 授权在身份验证过程中执行。

要确保SSL VPN连接可以在默认情况下终止（例如，当终端与任何已配置的动态访问策略不匹配时），可以使用以下步骤对其进行配置：



注意：首次配置动态访问策略时，会显示DAP.xml错误消息，指示DAP配置文件(DAP.XML)不存在。修改初始DAP配置并保存后，此消息将不再显示。

-

导航到**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**，然后配置以下步骤：

图 30.默认动态访问策略-如果未匹配预定义的**DAP**记录，则可以实施此**DAP**记录。因此，可以拒绝**SSL VPN**访问。 

a.

编辑DfltAccessPolicyand将Action设置为**Terminate**。

b.

点击**确定**。

-

添加一个名为**Managed_Endpoints**的新动态访问策略，如下所示：

a.

说明：员工客户端访问

b.

添加终端属性类型（防病毒），如图31所示。完成后单击“确定”。

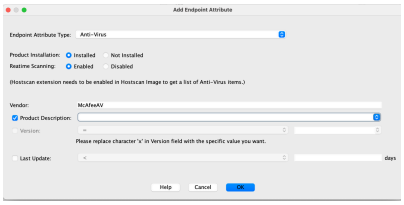


图 31.**DAP**终端属性-高级终端评估防病毒可用作客户端/网络访问的**DAP**标准。

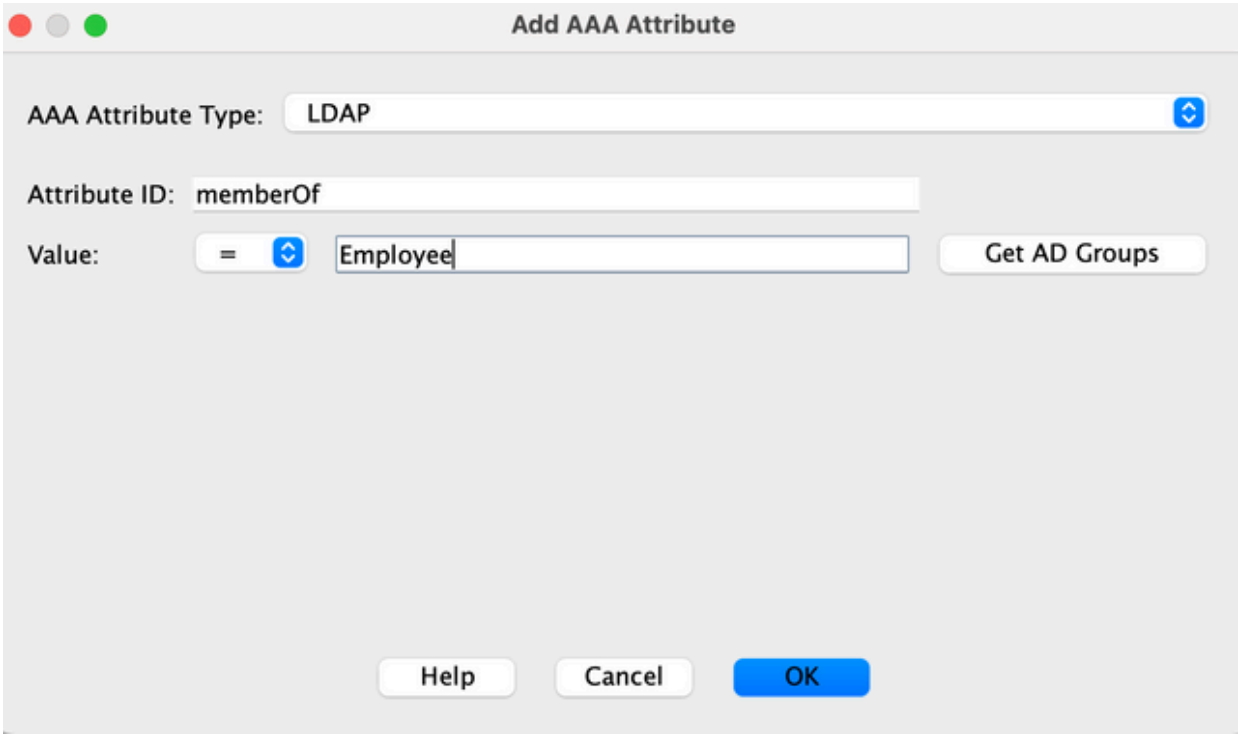
c.

如上图所示，从AAA Attribute部分的下拉列表中选择User has ALL of the following AAA Attributes Values。

-

如图33和图34所示，添加（位于AAA Attribute框的右侧）AAA Attribute Type (LDAP)。完成后单击“确定”。

图 33.**DAP AAA**属性- **AAA**组成员资格可用作识别员工的**DAP**条件。



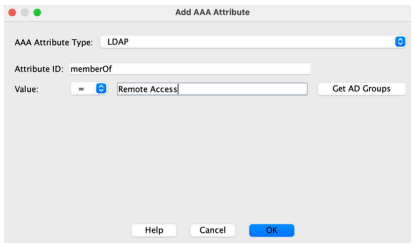
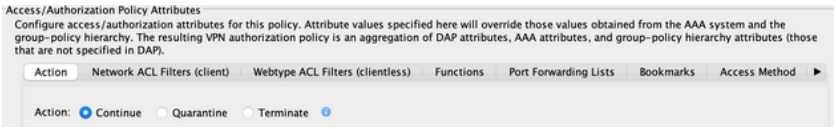


图 34.**DAP AAA属性- AAA组成员资格可用作允许远程访问功能的DAP条件。**

-

在Action选项卡下，验证Action是否已设置为**Continue**，如图35所示。

图 35.**Action** 选项卡 - 要为特定的连接或会话定义特殊处理，必须进行此配置。如果**DAP**记录匹配，并且**Action**设置为**Terminate**，则可以拒绝**VPN**访问。



-

如图36所示，在Access Method选项卡下，选择Access **MethodAnyConnect Client**。

图 36.**Access Method** 选项卡 - 要定义 **SSL VPN** 客户端连接类型，必须进行此配置。

-

单击**OK**，然后**Apply**。

-

添加第二个动态访问策略**Unmanaged_Endpoints**，如下所示：

a.

说明：**Employee Clientless Access**。

b.

从AAA Attribute部分前一映像的下拉列表中选择User has ALL of the following AAA Attributes Values。

-

如图38和图39所示，添加（位于AAA Attribute Type的右侧）AAA Attribute Type (LDAP)。完成后单击“确定”。

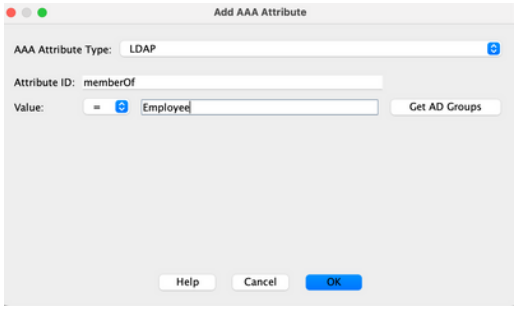


图 38.**DAP AAA属性- AAA组成员资格可用作识别员工的DAP条件。**

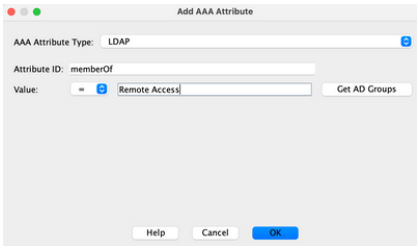


图 39.**DAP AAA属性- AAA组成员资格可用作允许远程访问功能的DAP条件。**

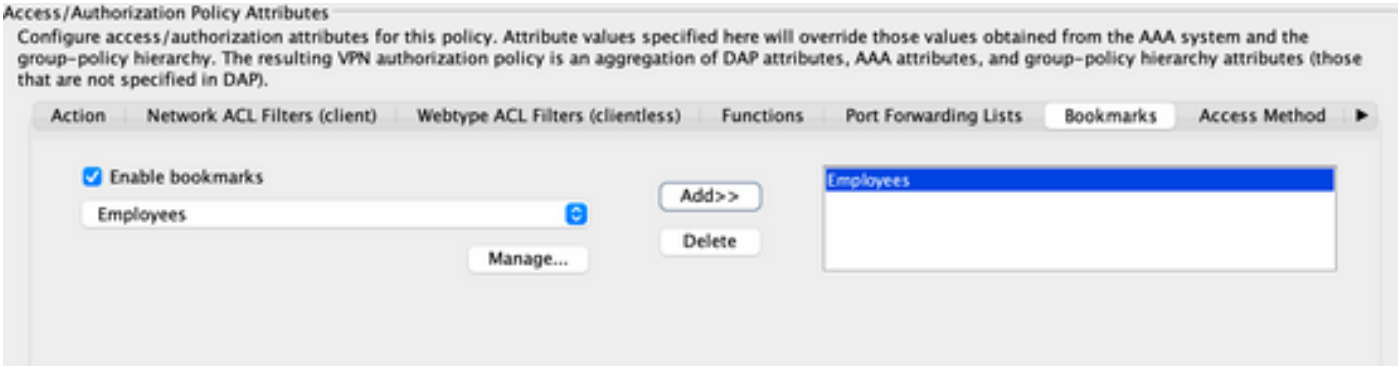
-

在Action选项卡下，验证Action是否已设置为**Continue**。（图35）

-

在Bookmarks选项卡下，从下拉菜单中选择列表nameEmployees，然后点击**Add**。此外，请验证是否已选中Enable书签（如图40所示）。

图 40.**Bookmarks选项卡-用于为用户会话选择和配置URL列表。**



-

  a.

  在Access Method选项卡下，选择Access Method **Web Portal**。（图36）

- 单击**OK**，然后**Apply**。

1. 承包商只能通过DAP AAA属性识别。因此，无法在步骤4中配置终端属性类型：（策略）。此方法只用于显示 DAP 内的多功能性。

3. 使用以下设置添加第三个动态访问策略**Guest_Access**：

-

  说明：**Guest Clientless Access**。

-

  添加（在 Endpoint Attribute 框右边）一个 Endpoint Attribute Type (Policy)，如图 37 所示。完成后单击“确定”。

-

  在图40中，从AAA Attribute部分的下拉列表中选择User has ALL of the following AAA Attributes Values。

-

如图41和图42所示，添加（位于AAA Attribute框的右侧）AAA Attribute Type (LDAP)。完成后单击“确定”。

图 41.您可以使用**DAP AAA**属性- **AAA**组成员身份作为**DAP**标准来识别承包商

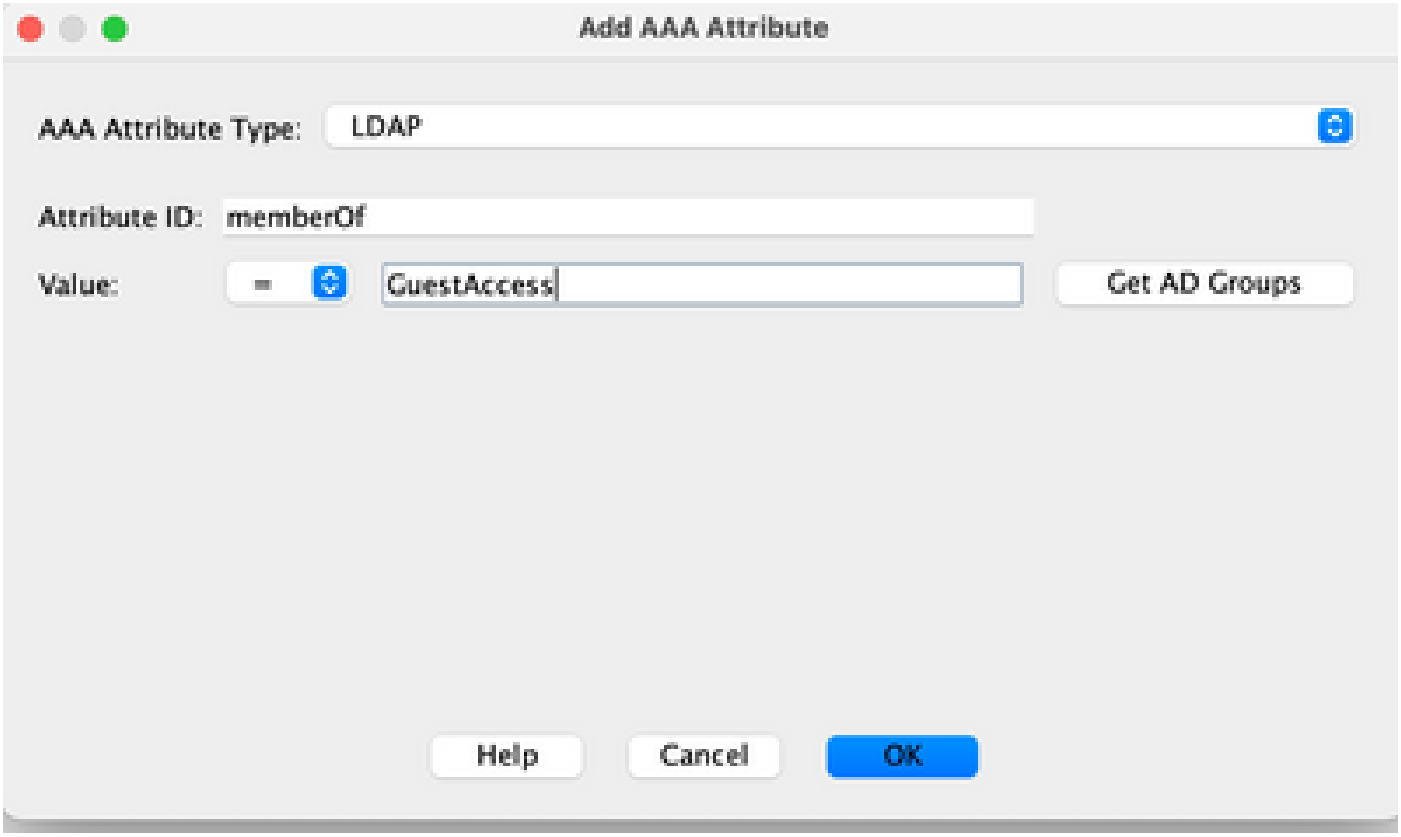
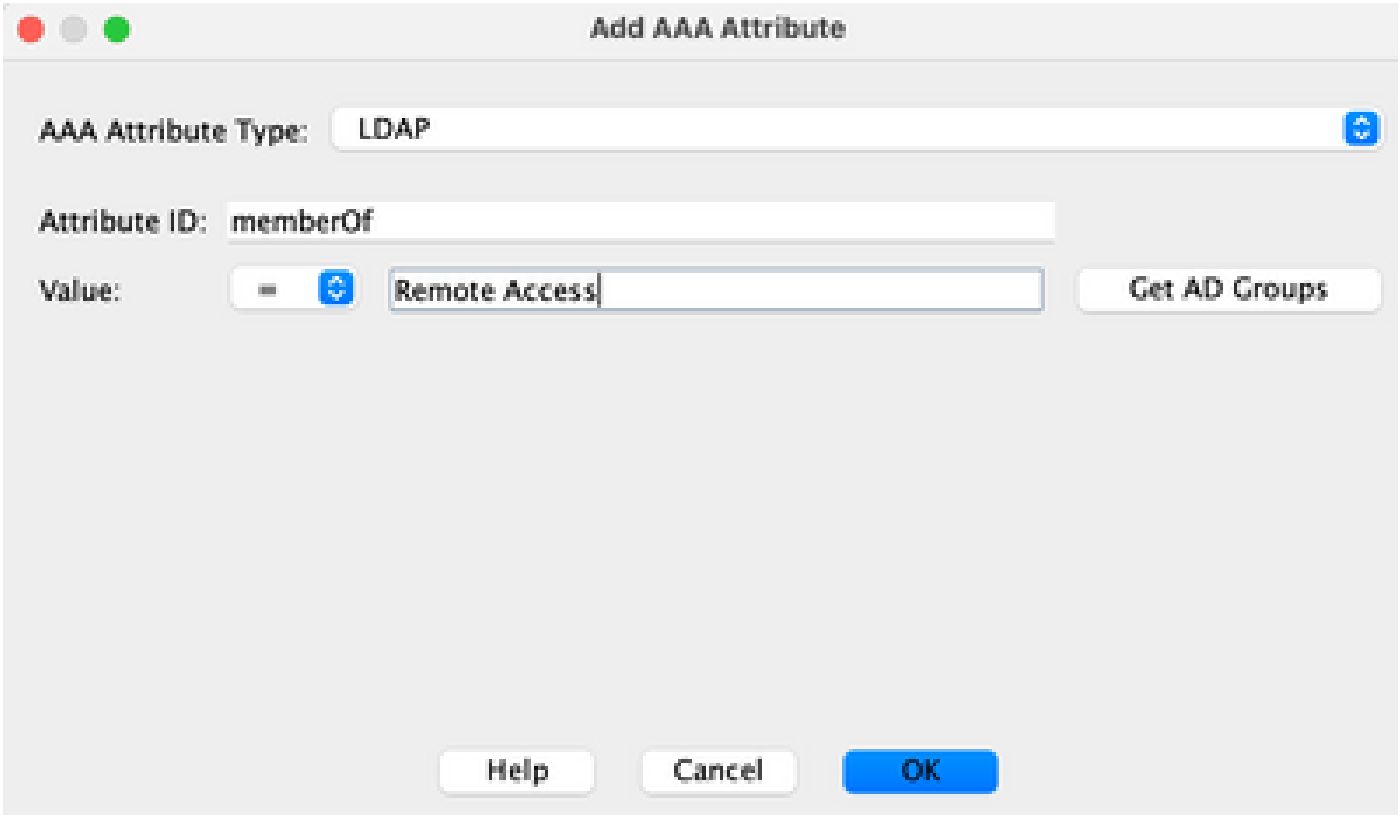


图 42.**DAP AAA Attribute** -可将**AAA**组成员身份用作**DAP**条件以允许远程访问功能



-

a.

在 Action 选项卡下，验证 Action 是否已设置为 Continue。（图35）

b.

在“Bookmarks”选项卡下，从下拉列表中选择列表名**Contractors**，然后单击“Add”。并且，验证是否已选中**Enable bookmarks**。（参考图 40。）

c.

在Access Method选项卡下，选择Access Method Web门户。 （图36）

d.

单击 OK，然后单击 Apply

结论

根据本示例中所述的客户端远程访问SSL VPN要求，此解决方案满足客户端远程访问VPN要求。

随着不断发展和动态的VPN环境不断融合，动态访问策略可以适应并扩展为频繁发生的互联网配置更改、每个用户可在组织内担任的各种角色，以及从具有不同配置和安全级别的托管和非托管远程访问站点登录。

动态访问策略由新的和经过验证的传统技术作为补充，这些技术包括高级终端评估、主机扫描、安全桌面、AAA和本地访问策略。这样，组织就可以放心地从任何位置提供对所有网络资源的安全 VPN 访问。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。