思科身份服务引擎低影响模式

安全访问操作指南系列

日期：2012 年 8 月

作者：Adrianne Wang

目录

低影响模式

低影响模式概述

与监控模式相比，低影响模式通过在启用 TrustSec 的开放访问端口上配置入口端口 ACL，可逐步提高网络的安全级别。利用此模式，可为访客、承包商和未经身份验证的主机提供基本连接，同时选择性地限制访问权限，从而引入更高的安全级别。此模式通过将可下载访问控制列表 (dACL) 与启用 TrustSec 的端口结合（使用 802.1X、MAC 身份验证绕行 [MAB] 和/或 Web 身份验证），实现基于成功身份验证和授权的访问权限区分。

在低影响模式下，我们通过如下方式为我们在监控模式下构建的框架添加安全功能：对交换机端口应用 ACL，从而在身份验证之前只允许非常有限的网络访问。用户或设备成功通过身份验证之后，会获得完整的网络访问权限。

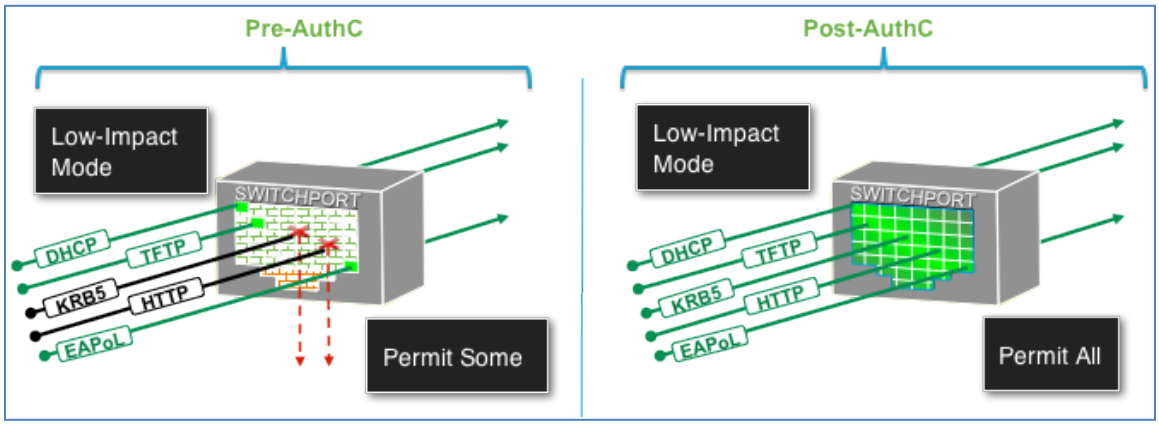


图 1. 低影响模式端口行为

例如，此功能可用于使所有连接至网络的设备都能够使用 DHCP 和 DNS 连接至互联网，同时阻止其对内部资源的访问。连接至启用此模式的交换机端口的设备在通过身份验证后，会应用允许所有流量的可下载 ACL。

此模式持续地在交换机端口上使用开放式身份验证，同时为非身份验证设备提供可靠的安全级别。但是，由于无论设备的身份验证状态如何，始终会有有限的流量通过，而且此模式支持进行“常规”IT 操作活动（如利用预启动执行环境 [PXE] 解决方案再次对工作站进行映像操作），因此成为当今企业的理想务实之选。

我们将遵循与无线接入类似的流程，使用有效凭证进行无线网络身份验证的用户或设备会获取完整网络访问授权，应通过其他安全功能以及基于用户或设备角色的特定访问权限限制访问权限。

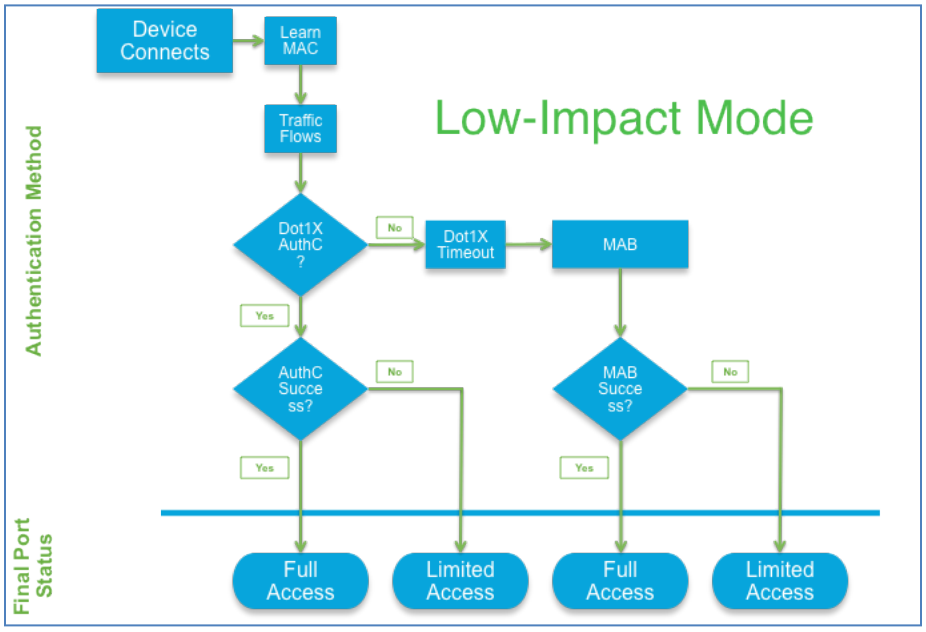


图 2. 低影响模式流程图

在部署之前了解流程

与《TrustSec 监控模式操作指南》类似，本指南涵盖园区和远程办公室的有线接入。我们在解决方案测试中使用了集成多业务路由器 (ISR) 中适用于远程办公室的 Cisco EtherSwitch® 服务模块。在添加了身份验证的情况下，我们还可以将无线接入引入到网络；本指南也提供了有关无线部署的分步说明。

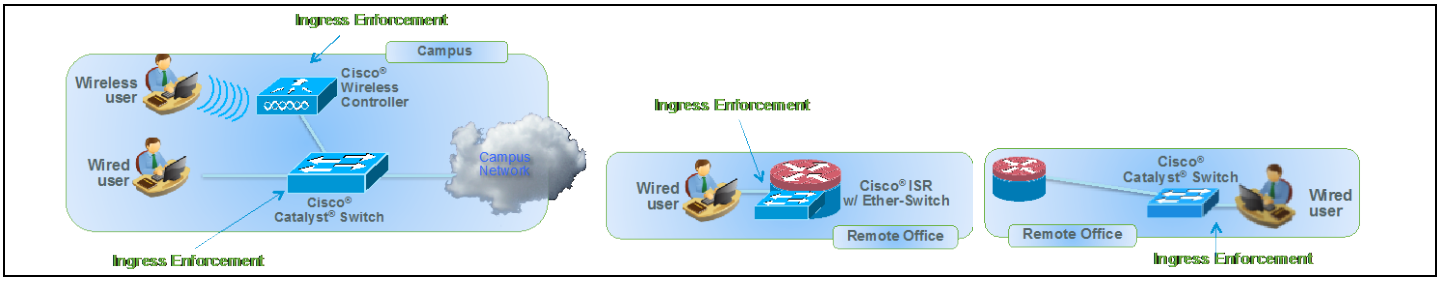


图 3. 身份验证访问的典型场景

有线访问

在此阶段，所有有线设备都应通过 802.1X 或 MAB 进行身份验证。现在我们将添加安全功能，以限制未通过身份验证的设备的流量，并引入 Web 身份验证和访客接入主题。

低影响模式是向监控模式下构建的框架添加安全功能的部署策略。它通过对交换机端口应用 ACL，从而在身份验证之前只允许非常有限的网络访问来实现这一目的。我们将该 ACL 看作“默认 ACL”或“端口 ACL”。此 ACL 的配置将在 HowTo-10-Universal_Switch_Configuration 指南中详述，其名称被指定为 ACL-DEFAULT。此 ACL 的目的是在通过身份验证之前允许重要流量通过。根据您的环境情况，可能需要开放更多流量。

当用户或设备成功通过身份验证后，他们通过一个允许所有流量的可下载 ACL (dACL) 获得完整的网络访问权限。这是此阶段 TrustSec 部署的一个重要过程。对于通过身份验证的特定设备，dACL 优先于默认端口 ACL（根据会话进行处理）。若没有 dACL，设备会继续受控于为该端口分配的 ACL-DEFAULT。

图 4. 身份验证模式的过程

低影响模式的部署

为其他网络设备（思科无线接入点）创建授权规则

思科 IP 电话和无线接入点是更为常见的两种需要访问网络的终端设备。它们都使用可配置请求方，且可能需要特殊访问权限。IP 电话将需要访问语音域。无线接入点通常需要特定类型的网络访问权限。至少，它们需要使用域名系统 (DNS)、简单文件传输协议 (TFTP)、动态主机控制协议 (DHCP)、轻量级接入点协议 (LWAP)，以及无线接入点控制和分配 (CAPWAP) 协议。出于这一原因，我们将为接入点创建一个允许所有流量的单独授权规则。

根据分析策略创建身份组

步骤 1 导航至 Policy > Profiling。
步骤 2 展开 Profiling Policies 容器。展开 Cisco-Device。
步骤 3 突出显示 Cisco-Access-Point。
步骤 4 选择 Create Matching Identity Group。

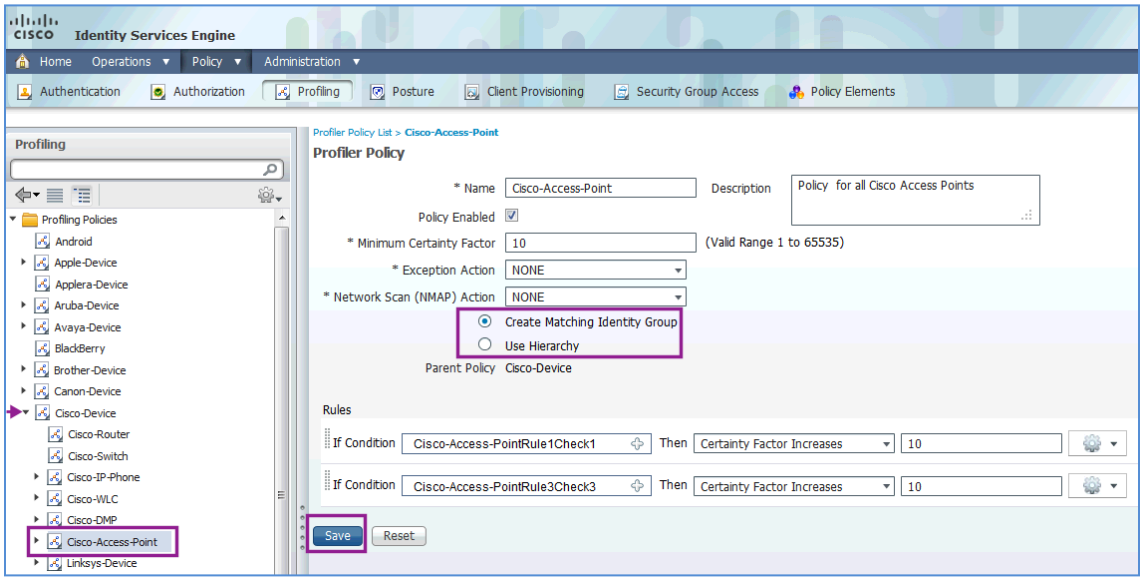


图 5. 创建分析器策略

步骤 5 点击 **Save**。

创建新的授权配置文件

注：授权配置文件将与预构建的“允许访问”配置文件完全相同。构建新的授权配置文件是为了获得一个唯一的授权配置文件，可在部署低影响模式期间进行更改。

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。

图 1 添加授权配置文件

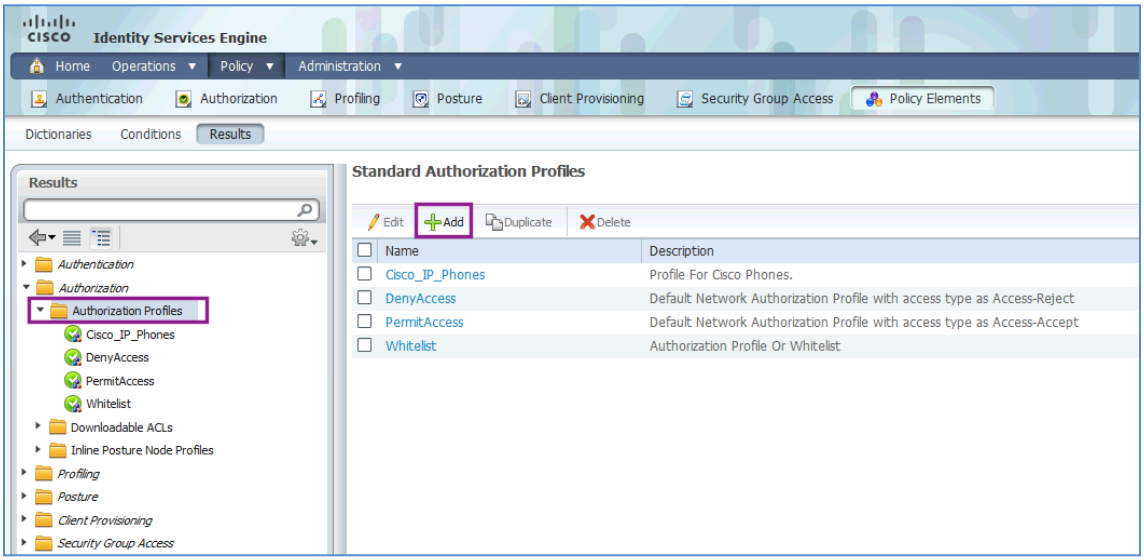


图 6.

步骤 2 点击 **Add**。

步骤 3 配置新的授权配置文件。

```
Name = Access-Points
Description = Authorization Profile for Access-Points
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = PERMIT_ALL_TRAFFIC
```

步骤 4 点击 **Submit**。

为接入点的授权策略添加规则

步骤 1 导航至 Policy → Authorization。

步骤 2 点击白名单授权策略末尾的 Actions 下拉菜单，选择 Insert New Rule Above。

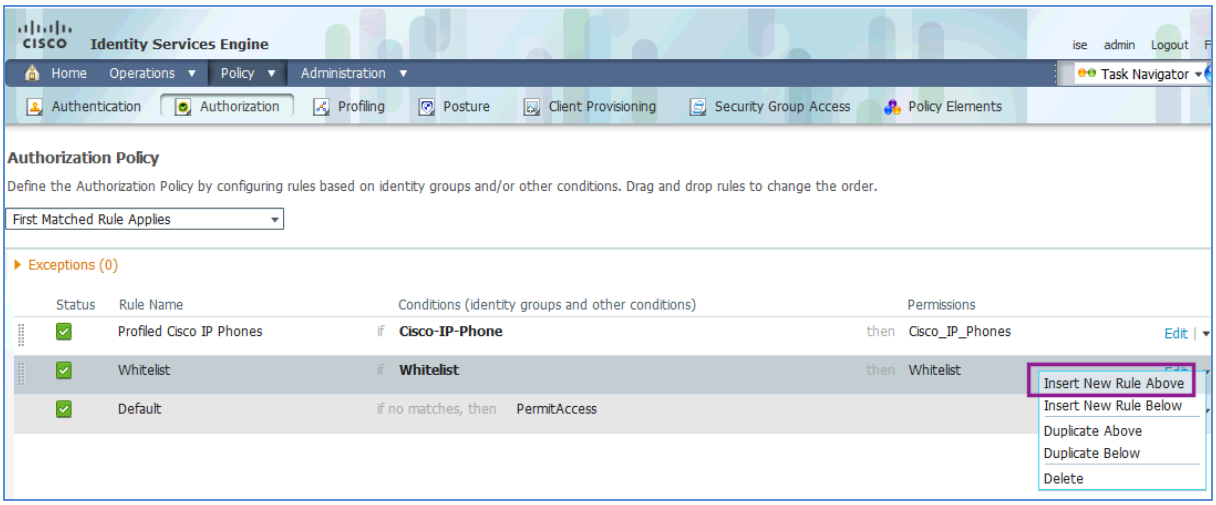


图 7. 添加授权策略

步骤 3 将新规则命名为：已分析的思科 AP。

步骤 4 点击“身份组”列下面的“+”符号。

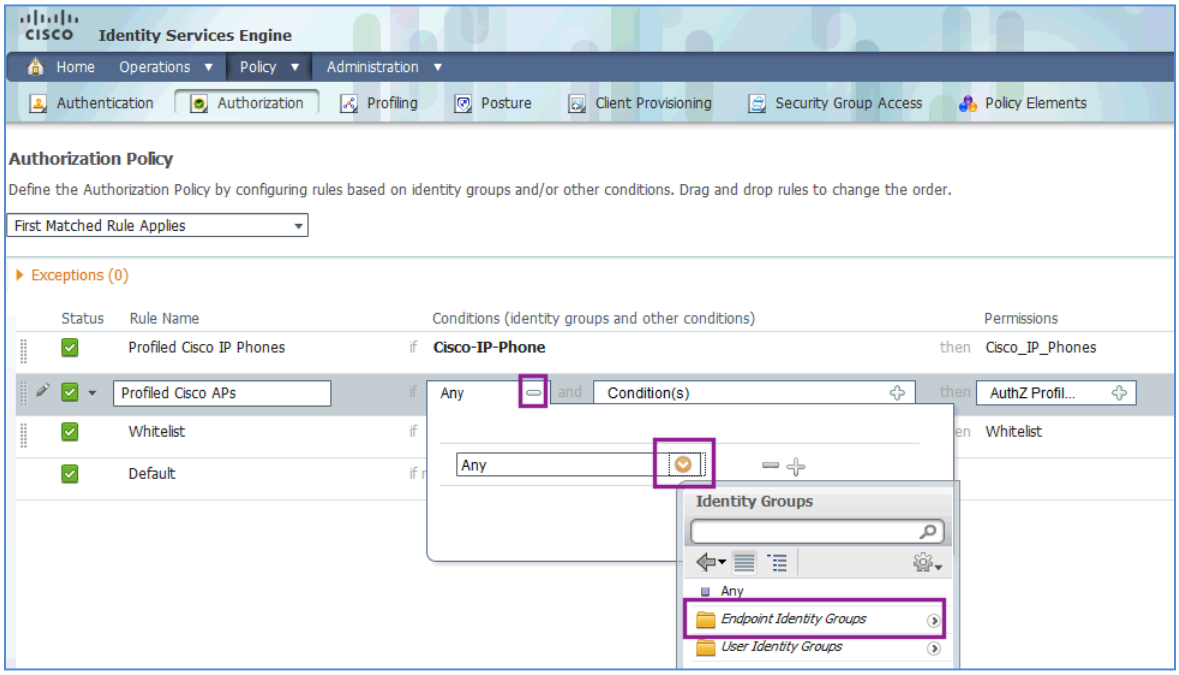


图 8. 添加已分析的思科 AP 策略

步骤 5 选择 Endpoint Identity Groups > Profiled > Cisco-Access-Point。

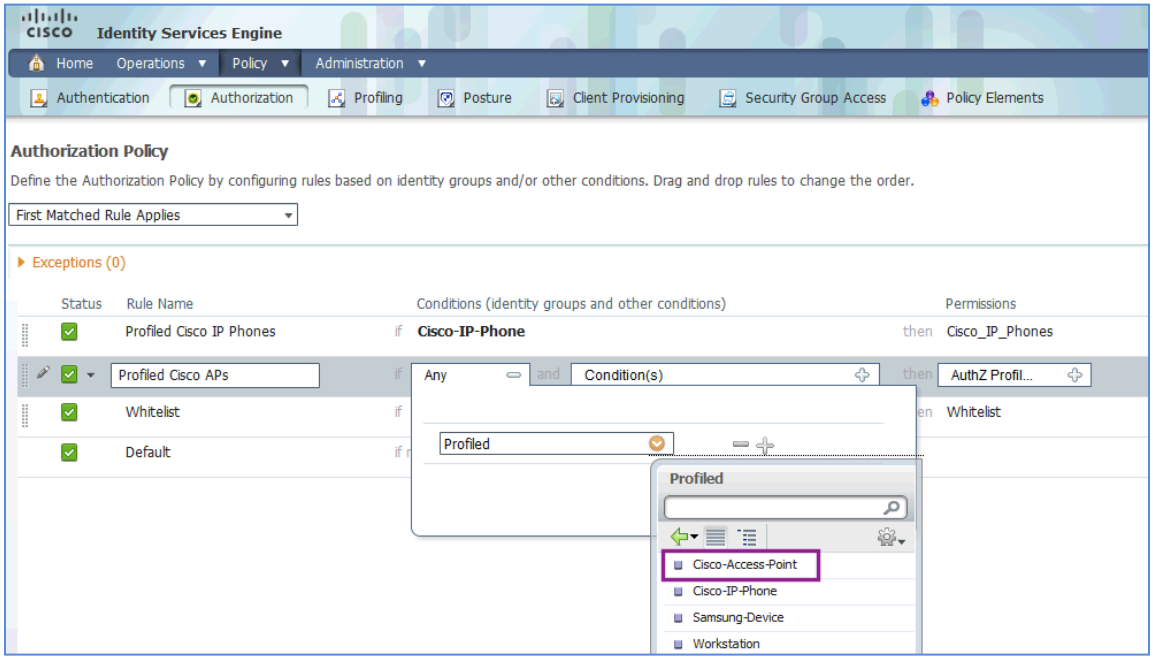


图 9. 选择策略的条件

步骤 6 点击“权限”列中的“+”符号。

图 2 选择策略的权限

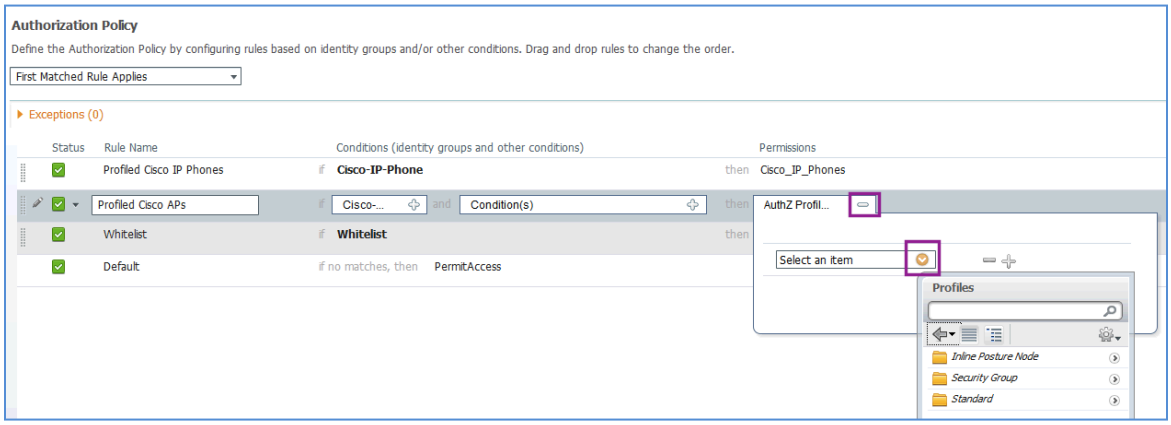


图 10. 选择策略的权限

步骤 7 选择 Standard > Access-Points。

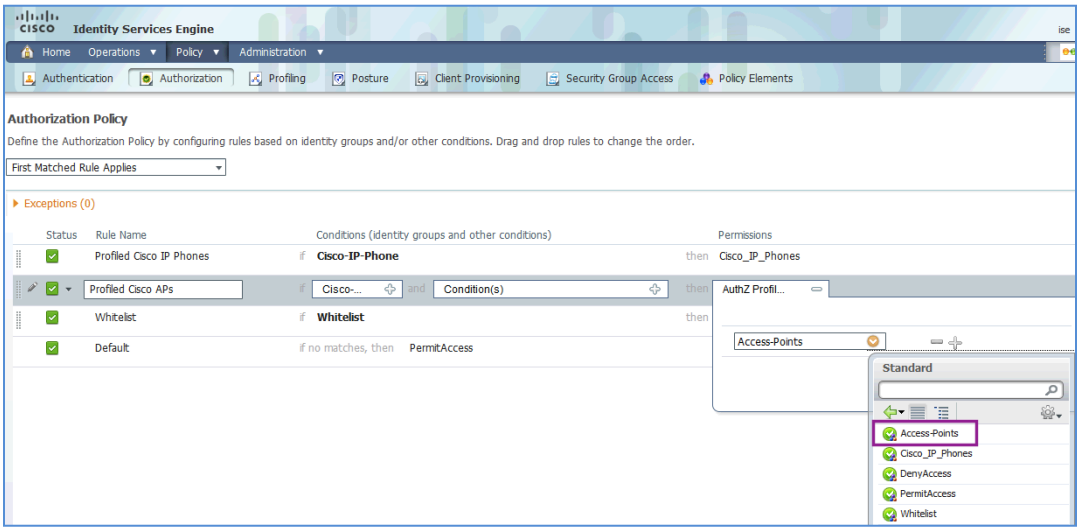


图 11. 选择策略的接入点

步骤 8 点击 **Save**。

为 Windows 计算机身份验证创建授权规则

Windows 计算机身份验证用于在用户未登录的情况下，允许基于 Windows 的计算机与组策略及其他更新的 Active Directory 域进行通信。这更适合企业环境，那里的计算机可能会在无交互式用户登录的情况下运行。

注：目前，尚无法同时实施计算机和用户双重身份验证。在标准主体和 EAP-FASTv2 中的思科 EAP-Chaining 方面，正在进行一项功能增强。EAP-Chaining 可在单个身份验证中加入计算机和用户凭证。有关 EAP-Chaining 的详细信息，请参阅《TrustSec EAP Chaining 部署操作指南》。

有多种方法可用于完成计算机身份验证；例如使用证书和可扩展身份验证协议传输层安全 (EAP-TLS)。但是，当使用不基于 EAP 的方法时，比如受保护的可扩展身份验证协议 (PEAP) 及 Microsoft 质询握手身份验证协议版本 2 (PEAP-MSCHAPv2)，Windows Supplicants 请求方能够将计算机名称作为凭证发送。可对思科 ISE 进行配置，以确认该计算机是否存在于 Active Directory 中，如果存在，即提供连接。

因为这是在部署的监控模式阶段，我们将配置授权规则，允许完全访问计算机。

注：当用户登录时已通过计算机身份验证的 Windows 终端时，请求方将通过局域网 (EAPoL) 启动消息向交换机端口发送 EAP，以重新开始新的身份验证。在新的身份验证完成后，如果需要，将向交换机端口发送新的身份验证结果，以更新授权配置文件。

为域计算机创建授权配置文件

步骤 1 导航至 Policy → Policy Elements → Results。

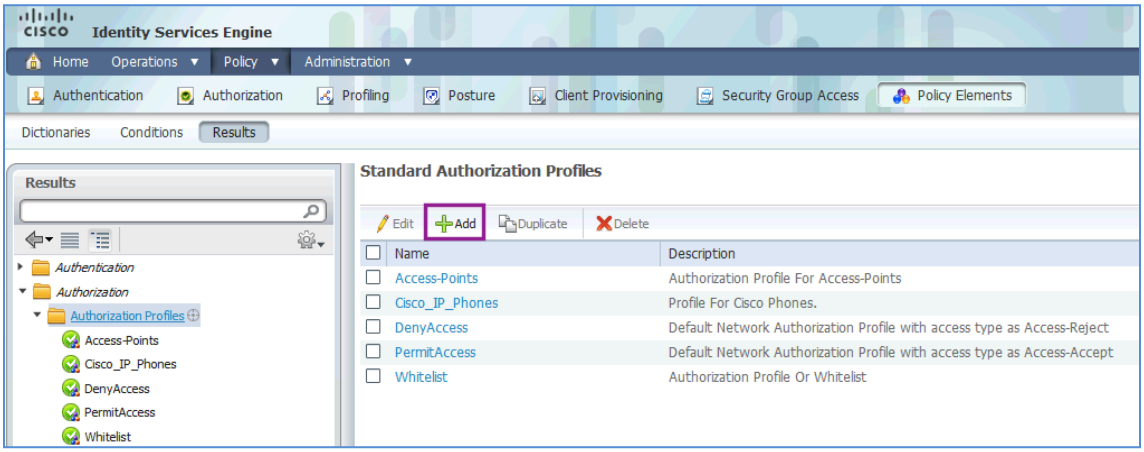


图 12. 为域计算机添加授权配置文件

步骤 2 点击 Add。

步骤 3 配置新的授权配置文件。

```
Name = AD_Machine_Access
Description = Authorization Profile for Windows Machine Auth
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = PERMIT_ALL_TRAFFIC
☑ Airespace ACL Name = PERMIT_ALL_TRAFFIC
```

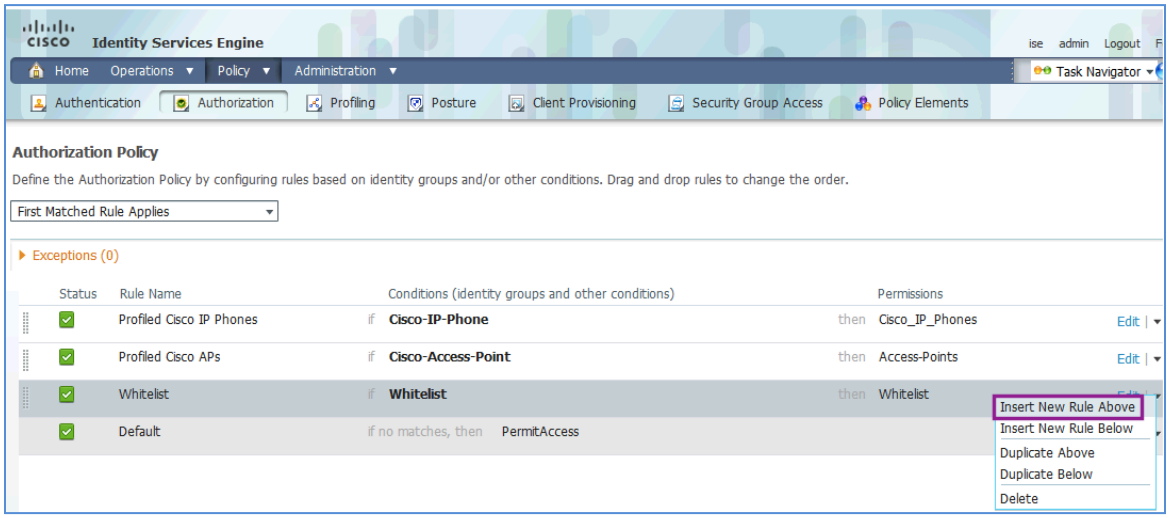
步骤 4 滚动至底部，点击 Submit。

程序 1　创建域计算机授权规则

步骤 1　导航至 Policy → Authorization。

步骤 2　点击白名单规则旁边的 Action 按钮，然后选择 Insert New Rule Below。

图 3 为白名单添加授权策略



步骤 3　将规则命名为**计算机授权**。

步骤 4　请勿更改 Identity Group；将其保留为 Any。

步骤 5　点击“+”号选择条件。

步骤 6　点击 Create New Condition。

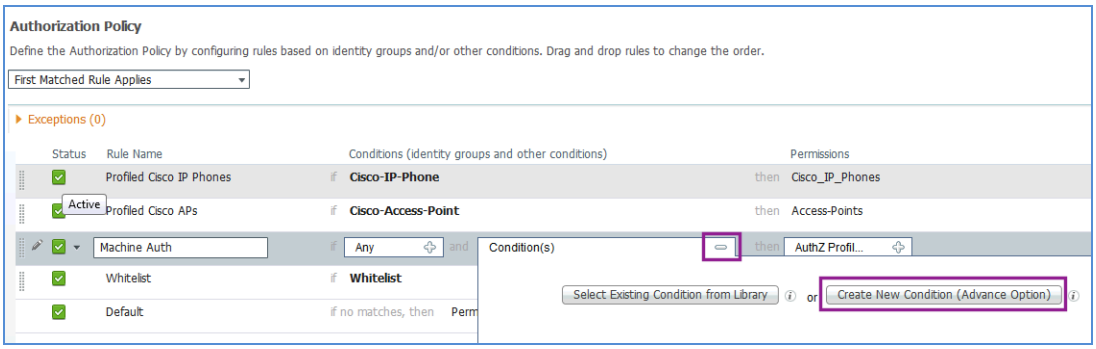


图 13.　创建计算机授权的新条件

步骤 7 使用 Expression 下拉菜单选择属性 AD1。

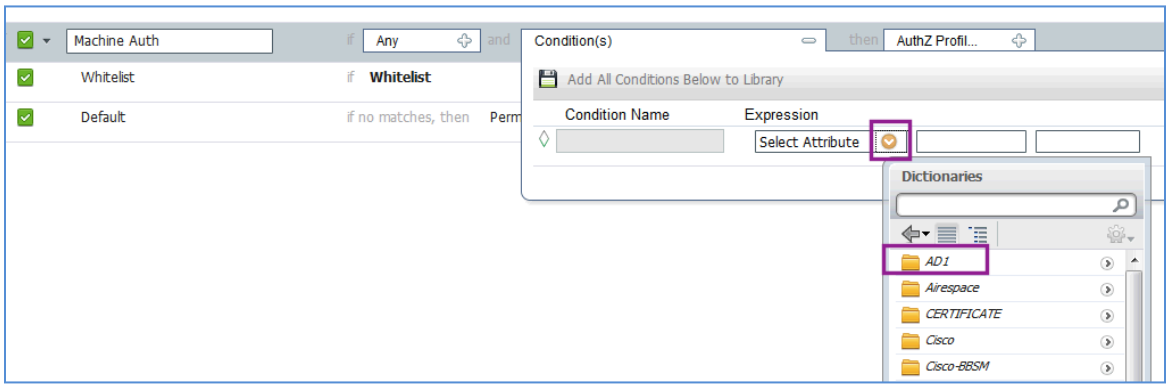


图 14. 选择计算机授权的属性

步骤 8 选择 AD1 → ExternalGroups。

图 4 选择计算机授权的 AD 组

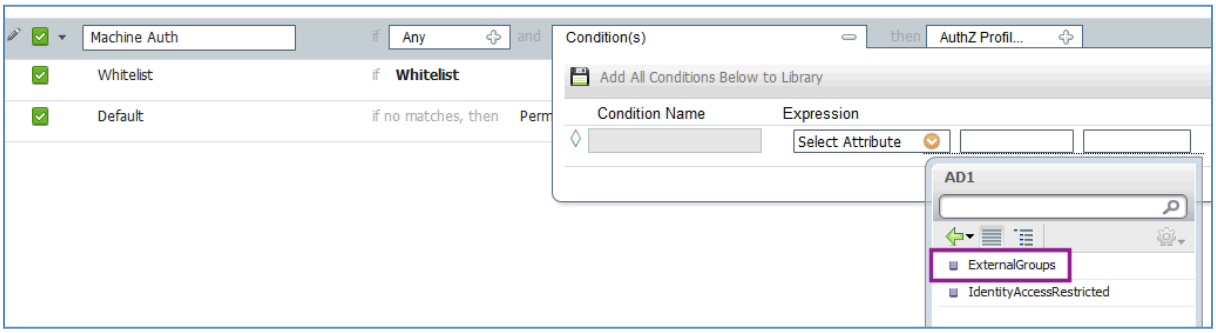


图 15.

步骤 9 选择 Equals。

步骤 10 选择 cts.local/Users/Domain Computers。

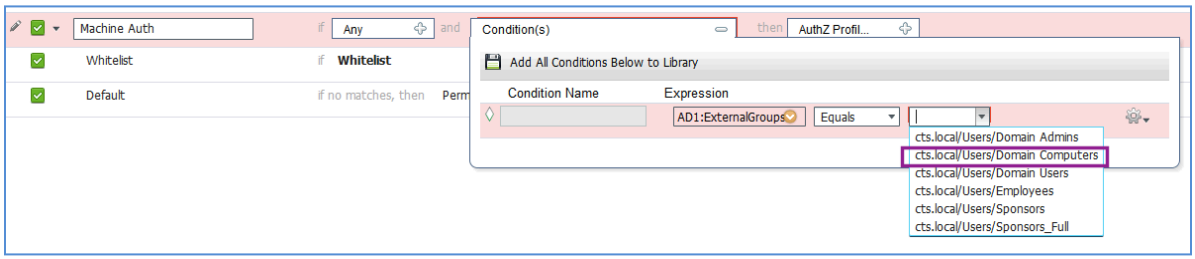


图 16. 选择计算机授权的域计算机

步骤 11 在 Permissions 列中，从下拉菜单中选择 Standard > AD_Machine_Access。

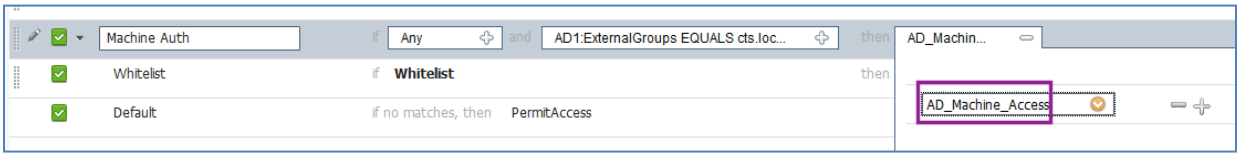


图 17. 选择计算机授权的 AD 权限

步骤 12 点击 **Save**。

为通过身份验证的用户创建授权规则

监控模式和低影响模式的一个重要区别就是，在低影响模式下，要想获得网络的访问权限，用户或设备必须成功通过该网络的身份验证。因此，我们需要为每个用户或设备类型制定具体的授权规则。若要完成此工作，我们将创建一个新的授权规则，为域用户 Active Directory 组的所有成员提供完全访问权限。

注：当需要创建特定访问策略时，强烈建议为 AD 中的每个安全组创建一个授权规则，并停止使用此域用户规则。

创建域用户授权配置文件

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。
步骤 2 点击 Add。
步骤 3 如下所述，配置新的授权配置文件。

```
Name = Domain_Users
Description = Authorization Profile to provide full-access to Users (Low-Impact Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = PERMIT_ALL_TRAFFIC
```

步骤 4 点击 Save。

创建域用户授权规则

步骤 1 导航至 Policy > Authorization。
步骤 2 在 **Machine Auth** 下面插入一个新规则。
步骤 3 将新规则命名为“域用户”。
步骤 4 保留 Identity Groups 为 Any。
步骤 5 创建一个新条件，选择 AD1 → External Groups。
步骤 6 将条件设为等于，选择 cts.local/Users/Domain Users。

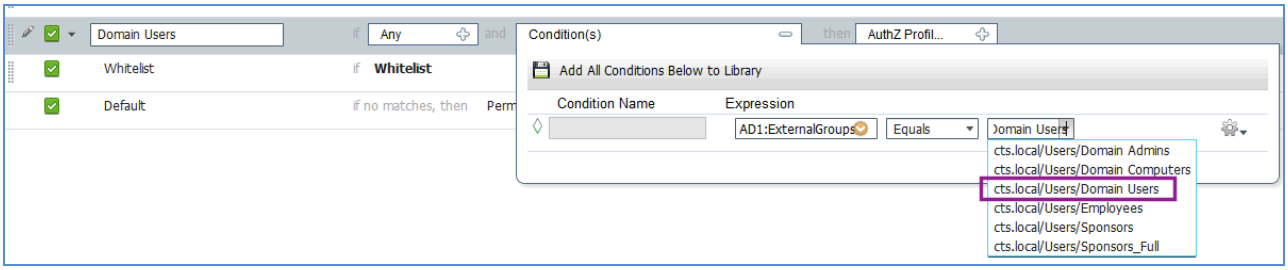


图 18. 选择授权策略的域用户

步骤 7 将权限设为 Domain_Users。

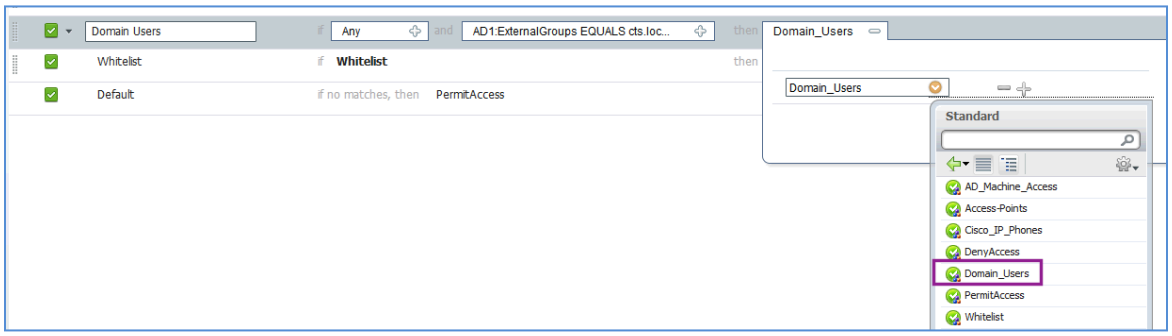


图 19. 设置域用户策略的权限

步骤 8 点击 **Save**。

无线接入

无线网络已经从一种非必需连接媒介变成大多数人使用的主要媒介。无线技术方面的科技进步和笔记本电脑、移动电话和平板电脑等支持 Wi-Fi 的设备的激增使无线安全成为 IT 管理员面临的最大挑战之一。IT 管理员需要确定连接至其无线网络的用户身份，并需要能够区分在公司网络上使用公司资产的用户和使用个人资产的用户。

我们将使用以下实例：

1. 员工使用公司设备（笔记本电脑/平板电脑：EAP-TLS）并且状态合规 = 完全访问权限（VLAN + 无 ACL）。
2. 员工使用个人设备 (PEAP) = 仅限于互联网访问（相同的 VLAN + 指定的 ACL 限制访问）。
3. 访客 = 仅限互联网访问（强制使用 ACL）。

TrustSec 利用 IEEE 802.1X 身份验证和分析等技术，使 IT 管理员能够以可扩展且可轻松管理的方式区分提供对于无线网络的访问权限。TrustSec 将思科 ISE 用作一台中央策略管理服务器，有助于提供安全的无线网络，并使组织能够使用自己的设备访问网络（一项标准，现称为“BYOD”）。

本文概述配置思科 ISE 和思科无线局域网控制器 (WLC) 以现对于无线网络使用 BYOD 进行区分访问的步骤。我们还将重点介绍 TrustSec 如何为访客提供无线访问权限。

我们将使用以下实例：

1. 员工使用公司设备（笔记本电脑/平板电脑：EAP-TLS）并且状态合规 = 完全访问权限（VLAN + 无 ACL）。
2. 员工使用个人设备 (PEAP) = 仅限于互联网访问（相同的 VLAN + 指定的 ACL 限制访问）。
3. 访客 = 仅限互联网访问（强制使用 ACL）。

无线接入详细说明

思科 ISE 能够同时实施有线和无线访问策略，IT 管理员能够跨两种访问媒介轻松向用户提供类似的网络访问体验。通过思科 ISE，我们可以在配置了 IEEE 802.1X 身份验证的无线网络上进行用户身份验证、设备分析和状况评估。无线用户的身份验证和授权流程如下图所示。

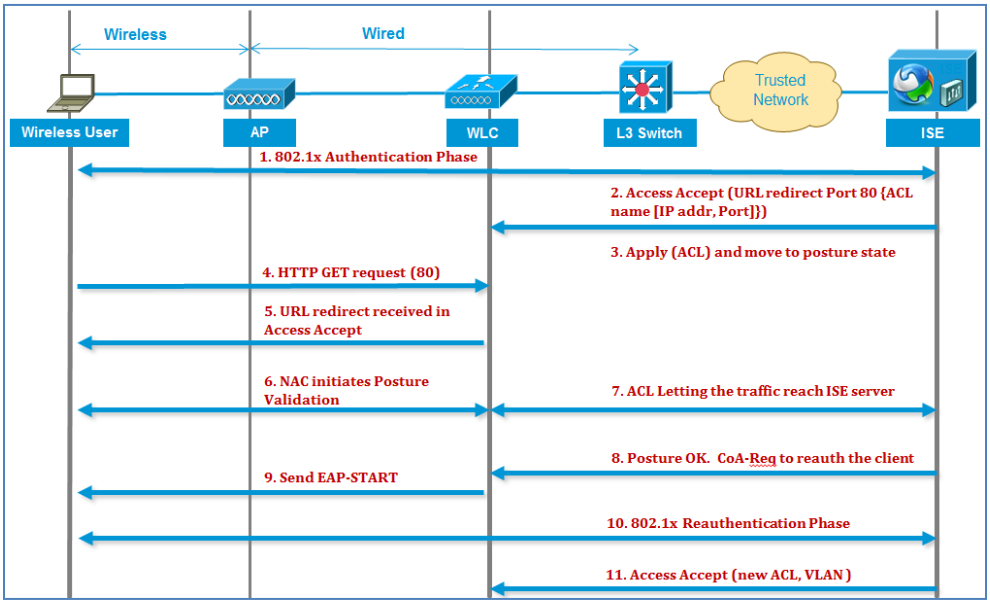


图 20. 无线 802.1X 身份验证流程

1. 客户端使用 dot1x 身份验证成功通过身份验证。
2. RADIUS Access Accept 承载重定向的端口 80 URL 和预先身份验证的 ACL，其中包括允许通过的 IP 地址和端口或者隔离 VLAN。
3. 客户端将重定向至 Access Accept 中提供的 URL，并加入到 Posture_Req 中，直到状况确认完成。
4. 客户端上的 NAC 代理启动状况确认（流向端口 80）：代理向端口 80 发送 HTTP 发现请求，控制器重新定向至 Access Accept 中提供的 URL。思科 ISE 得知客户端试图访问，然后直接对客户端做出响应。这样，客户端将获悉思科 ISE 服务器的 IP，随后，客户端即可与思科 ISE 服务器直接对话。
5. WLC 将允许此流量通过，因为我们已将 ACL 配置为允许此流量通过。在 VLAN 优先的情况下，我们只需桥接该流量，使之能够达到思科 ISE 服务器。
6. 当思科 ISE 客户端完成评估时，即会向 WLC 发送一个带有重新身份验证服务的 RADIUS CoA-Req，该请求将发起对于客户端的重新身份验证（通过发送 EAP-START）。重新身份验证一经成功通过，思科 ISE 即会发送带有新的 ACL 的已接受访问（如果存在），且不会重定向 URL 或访问 VLAN。
7. 依照 RFC 3576，WLC 可支持 CoA-Req 和 Disconnect-Req。依照 RFC 5176，WLC 需支持 CoA-Req，以提供重新身份验证服务。
8. 我们需要在 WLC 上使用预配置 ACL，而不是可下载 ACL。思科 ISE 服务器发送 ACL 名称，其已在 WLC 中配置。
9. 这种设计应该适用于 VLAN 和 ACL 情况。如果 VLAN 优先的情况下，我们只需重定向端口 80，并允许（桥接）隔离 VLAN 上的其余流量通过。对于 ACL 情况，我们将应用我们在已接受访问中获得的预先身份验证 ACL。

分支机构中的无线网络

在一个典型的无线部署中，所有来自接入点的流量都将传送回网络上将其引入的 WLC 中。我们将此隧道称为无线网络的分离 MAC 架构。因为所有流量都是在 WLC 进行中心交换，由思科 ISE 将策略向下推送至 WLC。

虽然分离 MAC 架构在园区 WLAN 部署中工作效果不错，但是，我们并不建议将其用于远程站点部署。在远程站点安装的接入点通常将与位于数据中心中的 WLAN 进行通信。若使用分离 MAC 架构，需要将所有用户流量首先通过 WAN 流向 WLC，然后才能进行交换，这将增加 WAN 链路上的负载。思科建议使用混合远程边缘接入点 (H-REAP) 或本地 MAC 架构。H-REAP 模式只在 WAN 链路上将控制流量转发至 WLC，所有用户数据都在远程站点本地进行交换（表 1）。

表 1. 无线控制器的 TrustSec 功能

TrustSec 功能	思科 5508 无线控制器和思科无线服务模块 2 (WiSM-2)		思科 Flex 7500 系列无线控制器 [1]	
	中心交换	本地交换	中心交换	本地交换
基本 AAA 功能	是	是	N/A	是
分析	是	否	N/A	否
状态	是	否	N/A	否
VLAN 优先	是	否	N/A	否
ACL 优先	是	否	N/A	否
访客配置	否	否	否	否

网络身份验证

在从监控模式透明地转至低影响模式时，Web 身份验证配置是关键的一步。到目前为止，授权策略中的默认规则（“终极规则”）设置为 PermitAccess，这意味着，如果设备不符合前面提到的任何更具体的条件，我们仍将允许它全面访问网络。

通过实施 Web 身份验证，我们将提供一个不同的终极授权规则。如果您未通过任何一个更具体的规则获得授权，用户/设备会被强制指定为授权状态，流量将极度受限，且交换机/WLC 会将所有 Web 流量重定向至 Web 身份验证限定性门户。这种重定向会为用户提供一个（类似访客和员工的）网页，以通过网络的身份验证，并获得授权结果。

Web 身份验证分为两种不同的类型。一种是本地网络身份验证，对于交换机或 WLC 的网络页面和身份验证事务都在本地进行；另一种是更高级的集中 Web 身份验证方法，交换机或 WLC 将网络流量重定向至 ISE 上的一个集中限定性门户，身份验证事务在 ISE 进行而非在 WLC 本地进行。

1 WLC 7.2.110.0 已通过 HREAP 增加了对 TrustSec 的支持，但其尚未针对 TrustSec 版本进行测试，因此本文未涵盖。

思科 ISE 配置 – 配置 Web 身份验证

创建 WEBAUTH 授权配置文件

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。

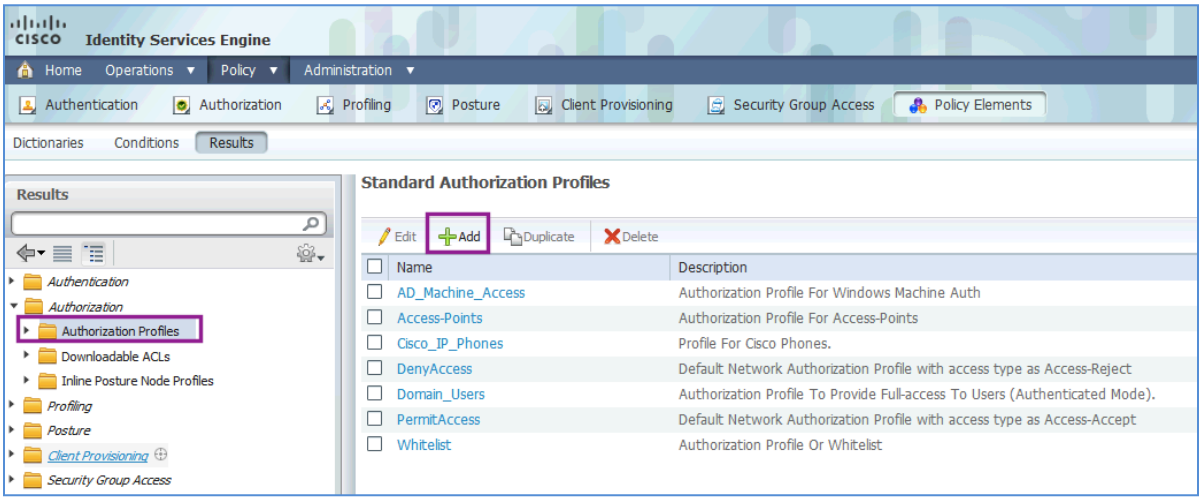


图 21. 创建 WebAuth 授权配置文件

步骤 2 将授权配置文件命名为 **WEBAUTH**。

步骤 3 保留访问类型为 ACCESS_ACCEPT。

步骤 4 将 dACL 设为 PERMIT_ALL_TRAFFIC。

步骤 5 启用集中 Web 身份验证，并输入 **ACL-WEBAUTH-REDIRECT** 作为 ACL。

ACL-WEBAUTH-REDIRECT ACL 在交换机上构建。该 ACL 可确定“引人注意的”流量。符合该 ACL 的流量将重定向至集中网络身份验证门户。该 ACL 与限制通过端口流量的 dACL 截然不同。

步骤 6 保留重定向为“默认”。

图 5 WebAuth 授权配置文件详细信息

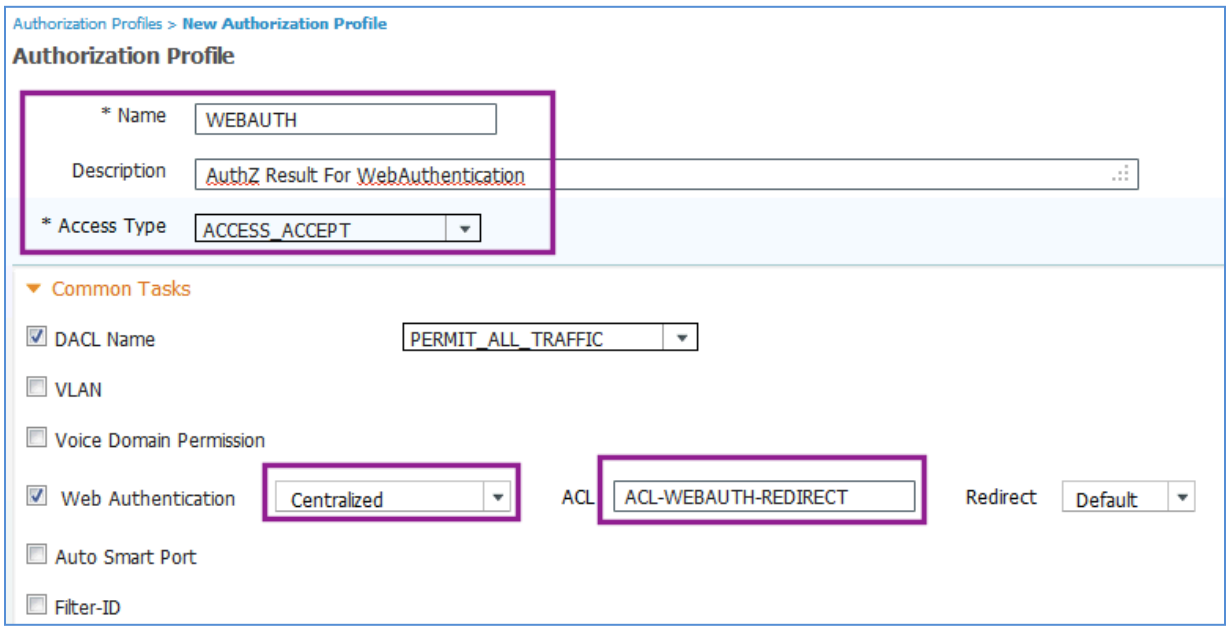


图 22. WebAuth 授权配置文件详细信息

步骤 7 滚动至页面底部，确认“属性详细信息”与图 26 中显示的一样。

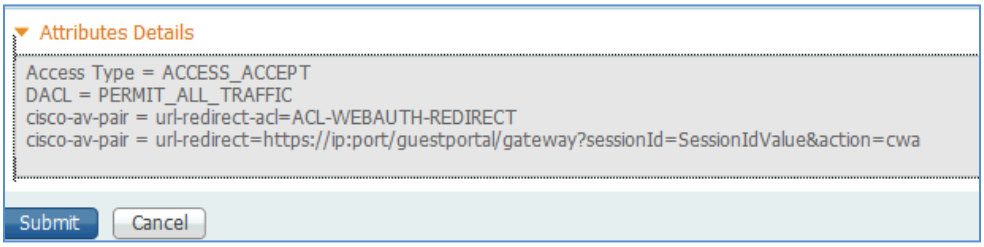


图 23. WebAuth 授权配置文件属性详细信息

步骤 8 点击 **Submit**。

访客访问

我们刚刚配置的 Web 身份验证可能适用于员工和访客。虽然生命周期被称为访客生命周期管理，但是，也可以指需要访问网络的任意用户。思科 ISE 可提供多种机制来创建多种访客类型，并控制对于每种访客类型，哪些保证人组能够创建。

在本文档中，我们将只有一个访客类型。将需要为该访客类型创建一个授权规则。

思科 ISE 配置 – 配置访客授权

访客用户的授权是一个复杂的主题。出于本设计指南的目的，我们将授权访客用户访问访客 VLAN，并提供一个可下载 ACL，允许所有流量流入交换机。

这种授权较为常用，并假定网络基础架构能够隔离访客用户与其余的公司网络。这种隔离通常是使用网络虚拟化（VRF 实例）或者甚至干脆在 3 层边缘使用访问列表来完成的。

创建访客可下载 ACL。

步骤 1 导航至 Policy > Policy Elements > Results > Authorization > Downloadable ACLs。

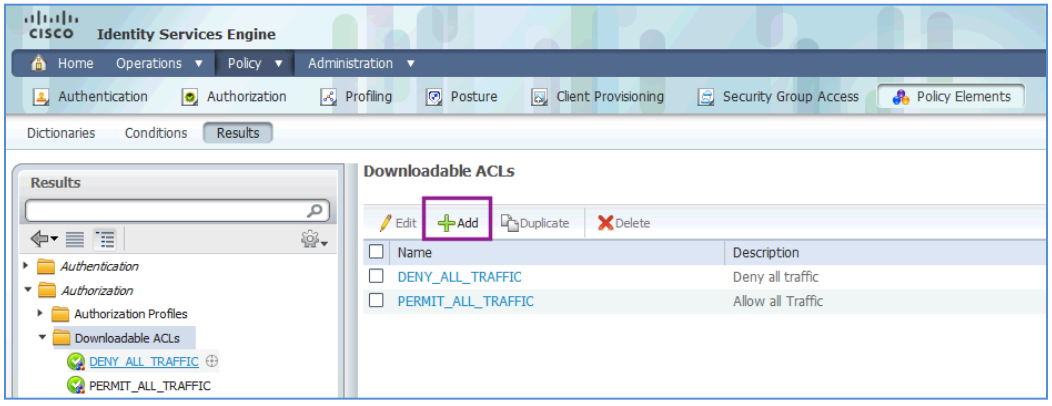


图 24. 创建 dACL

步骤 2 点击 Add。

步骤 3 配置新的 dACL。

```
Name = GUEST
Description = dACL for GUEST users (Authentication Mode)
DACL Content = permit ip any any
```

警告：思科 ISE 中没有语法检查，如果 dACL 语法不正确，将不能应用至会话。

步骤 4 点击 Submit。

创建访客授权配置文件

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。

步骤 2 点击 Add。

步骤 3 配置新的授权配置文件。

```
Name = GUEST
Description = Authorization Profile for GUEST role (Authentication Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = GUEST
☑ VLAN = GUEST
```

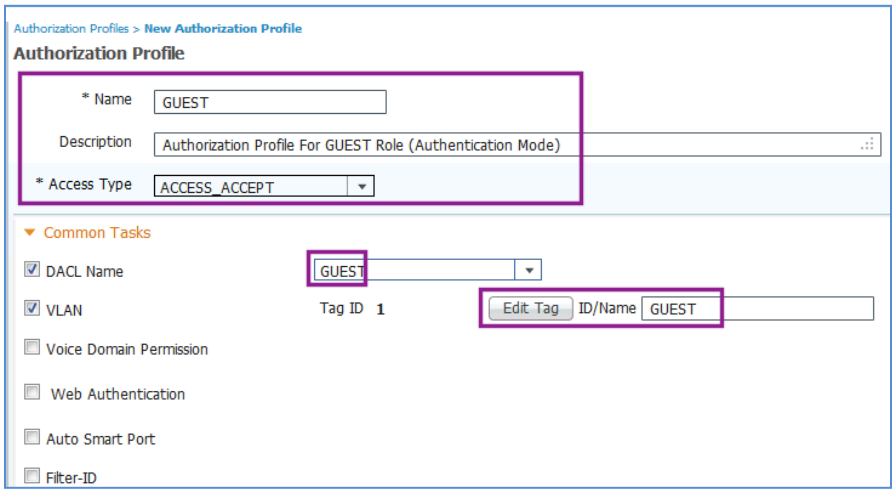


图 25. 创建访客授权配置文件

步骤 4 滚动至页面底部。请确保属性详细信息如图 29 所示，然后点击 Submit。

图 6 访客授权配置文件属性详细信息

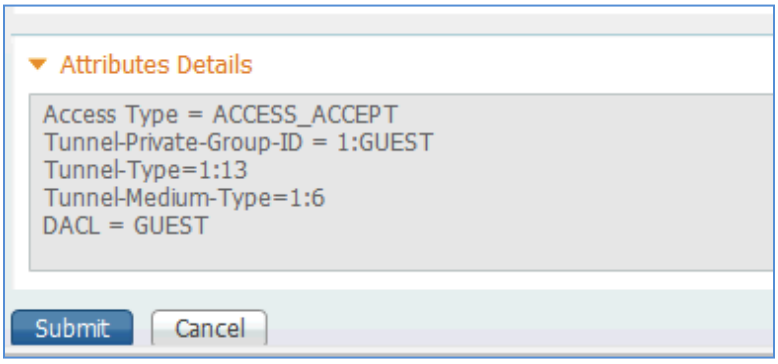


图 26. 访客授权配置文件属性详细信息

注：使用 VLAN 分配时，交换机端口主机模式极为重要。当使用多重身份验证或多主机模式时，我们不建议使用 VLAN 分配。只能给数据域分配一个 VLAN，另一个 VLAN 分配给语音域。多重身份验证和多主机模式可以在数据域中使用多台设备，因此向端口分配的第一个 VLAN 将对所有交换机端口生效。

创建访客授权策略规则

步骤 1 导航至 Policy → Authorization。
步骤 2 在“默认”规则上方（在“策略”表的底部）插入一个新规则。
步骤 3 将新规则命名为**访客**。
步骤 4 在“身份组”下面，点击选择器上的“+”号。
步骤 5 选择 User Identity Groups → GUEST。
步骤 6 保持其他条件不变。
步骤 7 对于 Permissions，点击“+”号，选择 **Standard → GUEST**。

图 7 创建访客授权策略

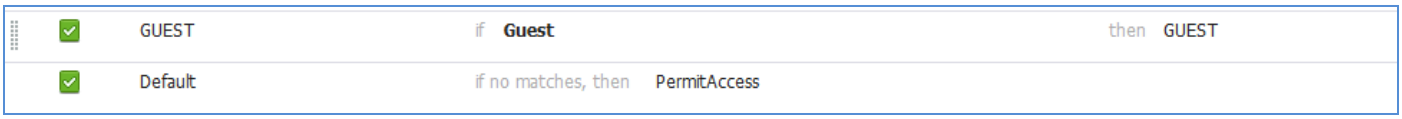


图 27. 创建访客授权策略

步骤 8 点击 **Save**。

思科 ISE 配置 – 访客帐户创建

在保证人门户中配置访客用户

步骤 1 从您的 Web 浏览器导航至保证人门户，网址为：https://<portal_host_or_IP_address>:8443/sponsorportal。
步骤 2 使用保证人用户的凭证登录到该门户。
步骤 3 导航至“创建访客帐户”。

步骤 4 至少配置图 31 所示的必填字段。

步骤 5 点击 **Submit**。

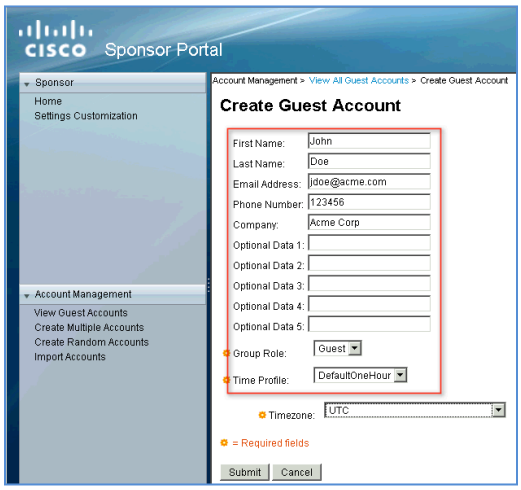


图 28. 创建访客帐户

将默认授权更改为 WebAuth 和测试

将默认授权规则更改为 WebAuth

警告：在完成此步骤之前，请确保您已经为低影响模式做好准备。此过程进行后，没有制定具体授权规则的所有设备都将变成 WEBAUTH 授权状态。

步骤 1 导航至 Policy > Authorization。

步骤 2 滚动到底部，点击选择器中 if no matches, then 旁边的“+”号。

步骤 3 选择 Standard > WEBAUTH，点击 Save。

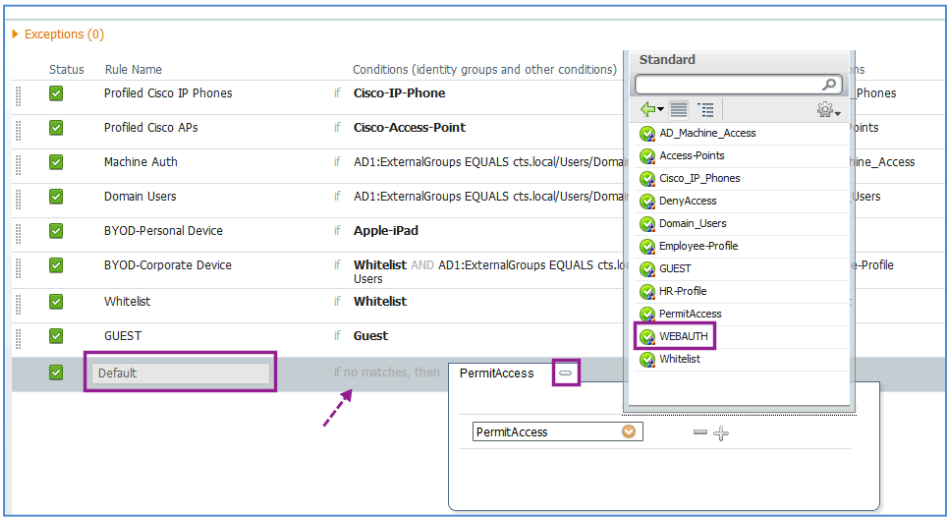


图 29. 将默认授权规则更改为 WebAuth

测试网络身份验证

步骤 1 既然我们已将“终极授权”设为网络身份验证，我们现在来确认一下，看看网络身份验证功能是否运作正常。

步骤 2 通过一台没有配置请求方的 Windows 或 Mac 设备连接至网络。

步骤 3 在交换机上确认授权结果。

```
C3750X#show authentication session interface <interface_name>
```

```
C3750X#show authentication session int gig1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5687.0004
           IP Address:  10.1.10.50
            User-Name:  00-50-56-87-00-04
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Group:  N/A
            ACS ACL:  xACSACLx-IP-PERMIT ALL_TRAFFIC-4dc4ad0d
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:
https://ise.cts.local:8443/guestportal/gateway?sessionId=0A0130020000000F2703ACFF&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0130020000000F2703ACFF
      Acct Session ID:  0x00000012
               Handle:  0x7E00000F

Runnable methods list:

       Method   State
       dot1x    Failed over
       mab      Authc Success
```

步骤 4 查看该会话的思科 ISE 实时身份验证日志。

图 8 Web 身份验证日志

图 30. Web 身份验证日志

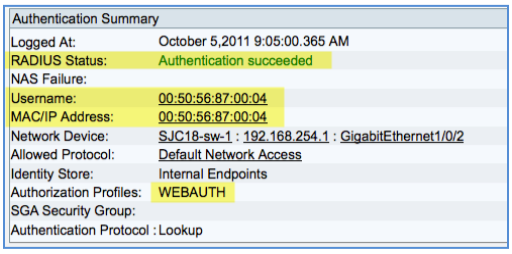


图 31. Web 身份验证日志详细信息

步骤 5 在客户端，打开 Web 浏览器，流量将自动重定向至思科 ISE。

图 9 Web 重定向

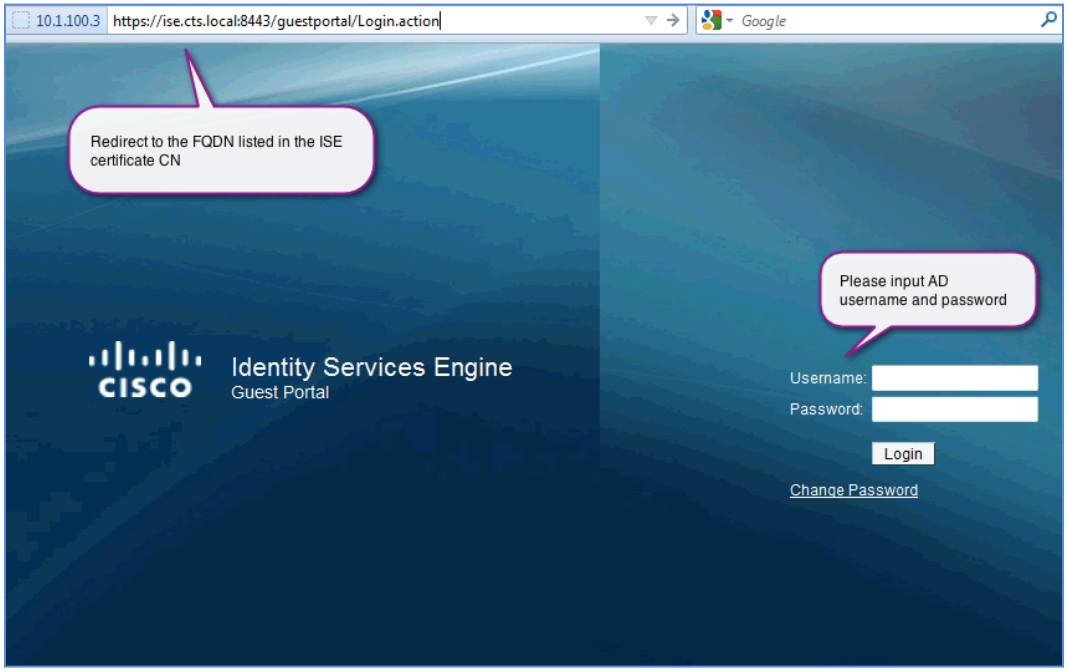


图 32. Web 重定向

常见问题：如果思科 ISE 不在 DNS 中，此重定向将失败。确保所有思科 ISE 节点都正确无误地列在 DNS 中。我们输入“employee1”，这是一个有效的 AD 用户帐户。

步骤 6 系统会显示可接受的使用策略，并显示 Employee1 已接受这些策略。

步骤 7 系统会显示一项新的授权，查看交换机和实时身份验证日志上的结果：

```
C3750X#show authentication session interface <interface_name>
```

```
C3750X#show authen sess int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5687.0004
          IP Address:  10.1.10.50
           User-Name:  employee1
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Group:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4dc4ad0d
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A0130020000001127DC1A50
     Acct Session ID:  0x00000014
              Handle:  0x53000011

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

注：请注意输出信息有何不同之处。此过程将不再重定向 URL，用户名为已知。

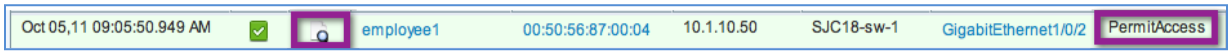


图 33. Employee1 身份验证日志

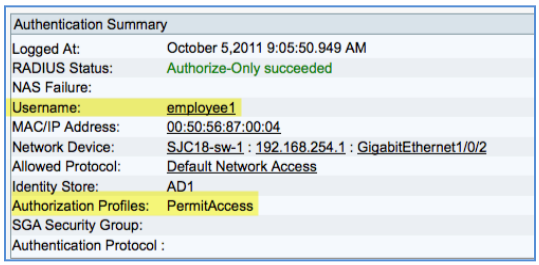


图 34. Employee1 身份验证日志详细信息

配置思科 ISE 的无线访客访问

组织通常会使用一个开放的 SSID，以提供访客访问。访客用户连接到 SSID 时，他们将被重定向至思科 ISE 的访客门户。在此过程中，他们可以使用其访客凭证（由保证人创建）获得网络的访问权限。

注：使用 DMZ 中的锚控制器，将访客流量与企业流量完全隔离，这是一个我们建议的最佳实践。但是，这不属于 TrustSec 系统测试的一部分，因此本文未涵盖。即使这样也请注意，因为思科 ISE 通常都位于数据中心中，所以流量流经 DMZ 中锚控制器的客户端再将流量发送回数据中心是很困难的。这一问题将在思科 ISE 的未来版本中解决。

在 WLC 上定义访客 ACL

有关创建 wACL 的详细信息，请参阅 HowTo-11-Universal_WLC_Configuration。

步骤 1 添加访客 wACL 规则（表 2）。

表 2. 访客 wACL

访客 wACL			
序列	1	2	3
信息来源	任何环境	任何环境	任何环境
目标	IP 地址 10.1.20.1 255.255.255.255	IP 地址 10.1.0.0 255.255.0.0	任何环境
协议	任何环境	任何环境	任何环境
DSCP	任何环境	任何环境	任何环境
方向	任何环境	任何环境	任何环境
操作	允许	拒绝	允许

注：默认情况下，预先通过身份验证的终端设备可以使用 DNS。

在思科 ISE 上的访客授权配置文件中添加 wACL

步骤 1 在思科 ISE 上，导航至 Policy > Policy Elements > Results。

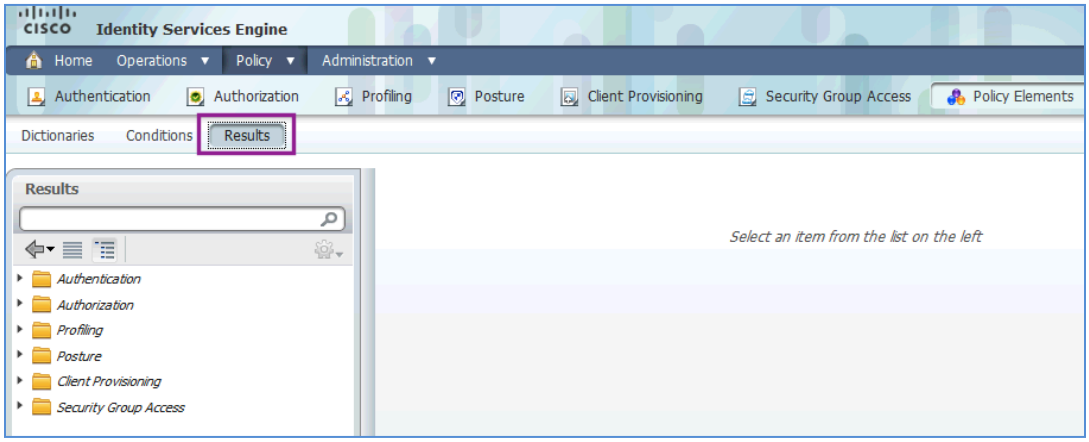


图 35. 向访客配置文件添加 wACL

步骤 2 选择 Authorization > Authorization Profiles > GUEST。

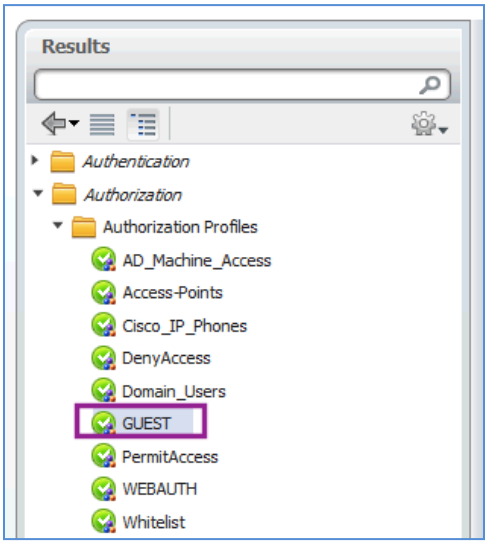


图 36. 选择 GUEST。

步骤 3 在 Common Tasks 部分下添加 wACL 值。

☑ **DACL Name** = PERMIT_ALL_TRAFFIC
☑ **Airespace ACL Name** = GUEST-ACL

转至低影响模式

在此阶段：所有思科 ISE 策略均创建为允许所有通过身份验证的设备完全访问网络。已配置 Web 身份验证、已发起访客访问且访客帐户创建已运行。但是，交换机上的默认端口 ACL 依然允许所有流量。

若要完整交付低影响模式阶段，我们必须将默认端口 ACL 更改为可以限制访问权限的 ACL。限制程度完全取决于部署计划。我们将检查现场一些一直使用的默认 ACL，并讨论您的部署中存在哪些并发问题以及如何对默认 ACL 进行相应的调整。

以下是两个建议的默认 ACL。我们在 HowTo-10-Universal_Switch_Configuration 操作指南中配置了第一个 ACL。

ACL-DEFAULT（推荐的安全默认 ACL）：

```
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 ping <
 permit icmp any any
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny   ip any any log
```

第二个建议的默认端口 ACL 可打开多个 Microsoft 端口，允许设备在登录前与 Active Directory 进行通信，以缩短登录时间。打开 Microsoft 特定端口还可以通过我们在“为域计算机创建授权配置文件”过程中完成的计算机身份验证完成。

ACL-DFLT-LESS-RESTRICT：

```
ip access-list extended ACL-DFLT-LESS-RESTRICT
 remark DHCP, DNS, ICMP
 permit udp any eq bootpc any eq bootps !DHCP
 permit udp any any eq domain           !DNS
 permit icmp any any                    !ICMP Ping
 remark Allow Microsoft Ports (used for better login performance)
 permit tcp any host 10.1.100.10 eq 88  !Kerberos
 permit udp any host 10.1.100.10 eq 88  !Kerberos
 permit udp any host 10.1.100.10 eq 123 !NTP
 permit tcp any host 10.1.100.10 eq 135 !RPC
 permit udp any host 10.1.100.10 eq 137 !NetBIOS-Nameservice
 permit tcp any host 10.1.100.10 eq 139 !NetBIOS-SSN
 permit tcp any host 10.1.100.10 eq 389 !LDAP
 permit udp any host 10.1.100.10 eq 389 !LDAP
 permit tcp any host 10.1.100.10 eq 445 !MS-DC/SMB
 permit tcp any host 10.1.100.10 eq 636 !LDAP w/ SSL
 permit udp any host 10.1.100.10 eq 636 !LDAP w/ SSL
 permit tcp any host 10.1.100.10 eq 1025 !non-standard RPC
 permit tcp any host 10.1.100.10 eq 1026 !non-standard RPC
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny   ip any any log
```

注：如果登录速度仍然很慢，则可能是其他应用的原因。如今的企业环境常常是在其中安装了许多企业应用。有些应用很“繁琐”，会不断地试图与其管理服务器进行通信。下面我们将给出几个建议的方法，用来确定导致登录速度慢的应用：
方法 1：使用一个网络包监听应用程序，确定在登录前的所有流量尝试。
方法 2：在思科 ASA 自适应安全设备上实施一个类似的访问列表，记录所有尝试和所有丢弃。保留默认端口 ACL 为 ACL-ALLOW（允许任何 IP）。

更改默认端口 ACL

将 ACL-ALLOW 替换为 ACL-DEFAULT

步骤 1 应用初始 ACL (ACL-ALLOW)。

```
C3750X(config-if-range)#ip access-group ACL-DEFAULT in
```

检查其他用户信息

直到此时，如果用户是域用户组的成员，则该用户可以获得完全访问网络的权限。为了提高安全性，我们将查看其他组，并对每个组提供有区别的访问权限。请参阅 Active Directory 用户和组成员表。

向 Active Directory 连接器添加其他组

步骤 1 导航至 Administration → Identity Management → External Identity Sources → Active Directory。
步骤 2 点击 Groups 选项卡。

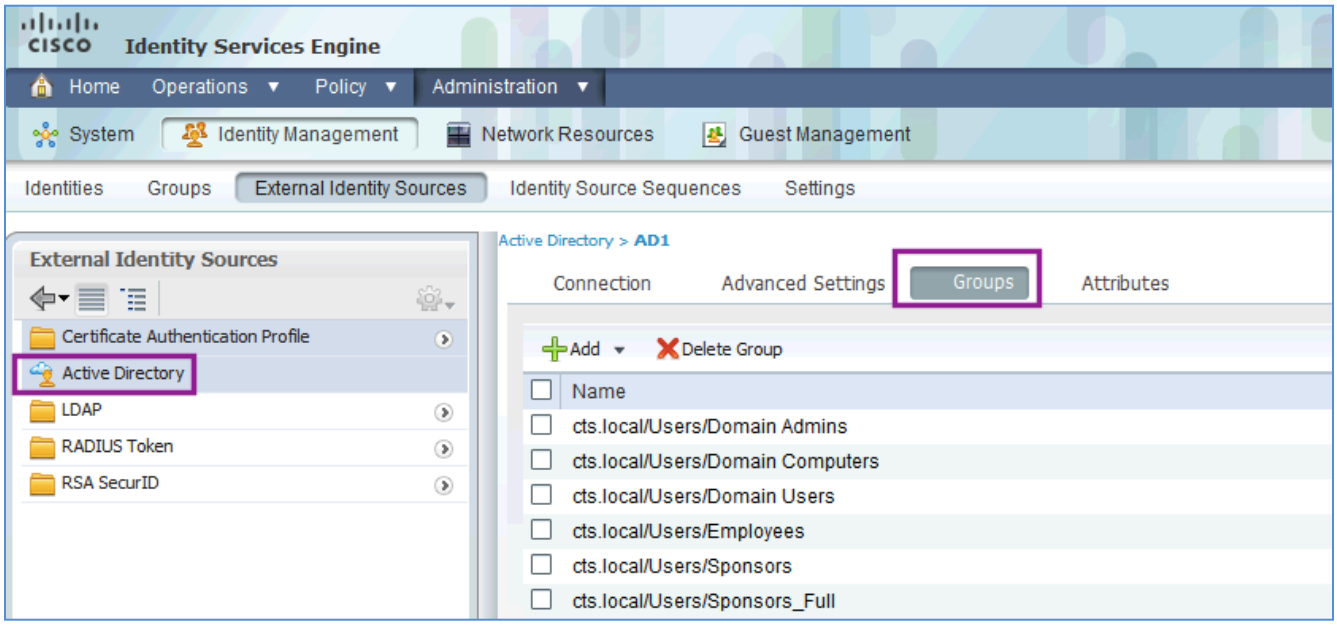


图 37. 添加额外组

步骤 3 点击 Add > Select Groups From Directory。

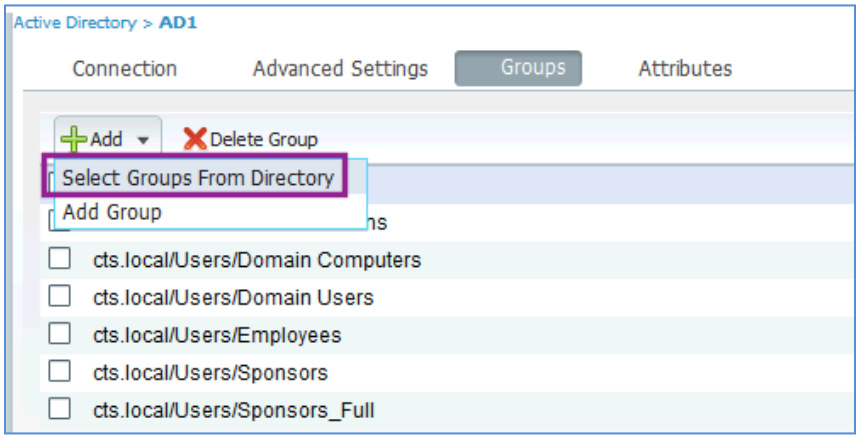


图 38. 选择 Groups from Active Directory

步骤 4 点击 Retrieve Groups。

注：当 Active Directory 超过 100 个组时，可以使用过滤器选项找到您正在寻找的特定组。

步骤 5 选择其他组。

在我们的示例中，我们将选择工程组、销售组和 HR 组。

步骤 6 点击 **OK**。下图显示了我们的最终组选择屏幕截图。

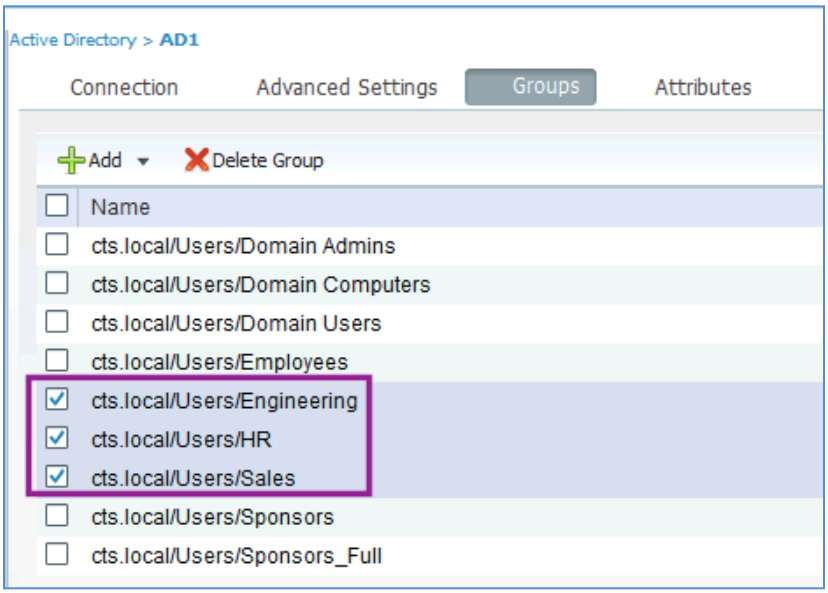


图 39. 最终组选择

步骤 7 滚动至页面底部并点击 Save Configuration。

注：若不保存该配置，在授权过程中，将不会从 Active Directory 中检索到其他组。

思科 ISE 配置 – 特定访问的连续配置

为每个主要角色创建其他 dACL

为每个需要不同授权的角色重复此程序。在本文中，我们将讲解如何创建 HR dACL，并显示包括所有已定义 dACL 的最终屏幕。

最佳实践：精简所有 dACL 的尺寸。交换机上的 dACL 支持与三态内容可寻址存储器 (TCAM) 的可用空间大小有关。交换机中的每个 ASIC 都有其自身的 TCAM，而每个端口的 ASIC 数量也因交换机型号而异。为每个 ASIC 分配的 TCAM 数量也因交换机型号而异（例如，Cisco Catalyst 3750 交换机上的 TCAM 数量就比 Cisco Catalyst 2960 交换机上的 TCAM 数量多）。思科交换机支持的 dACL 上限是 64 个 ACE（64 行）。

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Downloadable ACLs。
步骤 2 点击 Add。

```
Name = HR-ACL
Description = dACL for HR users
DACL Content =
Deny ip any <ip_address_range_of_HR_servers>
permit ip any any
```

警告：思科 ISE 中没有语法检查。如果 dACL 语法不正确，将不能应用至会话。

步骤 3 点击 Submit。
步骤 4 对每个不同的角色类型重复整个程序。

为每个主要角色创建 wACL

为每个需要不同授权的角色重复此程序。显示的 HR 用户的 wACL 可用于参考。

最佳实践：在一致性方面，所有 wACL 都应该使用与对有线访问定义的 dACL 相同的名称。

表 3. HR wACL 规则

HR-ACL						
序列	信息来源	目标	协议	DSCP	方向	操作
1	任何环境	IP 地址 10.1.100.87 255.255.255.255	任何环境	任何环境	任何环境	拒绝
2	任何环境	任何环境	任何环境	任何环境	任何环境	允许

为每个主要角色创建其他授权配置文件

为每个需要不同授权的角色重复此程序。在本文中，我们将讲解如何创建 HR 授权配置文件，并显示包括所有已定义授权配置文件的最终屏幕。

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。
步骤 2 点击 **Add**。

步骤 3 使用以下信息完成授权配置文件：

```
Name = HR-Profile
Description = Authorization Profile for HR role.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = HR-ACL
☑ Airespace ACL Name = HR-ACL
```

注：WLC 字段用于应用在 WLC 上本地定义的 wACL。

步骤 4 点击 Submit。

步骤 5 对每个不同的角色类型重复整个程序。

为员工创建另一个授权配置文件

我们已经挑选出此特定的授权配置文件来替换当前的域用户授权规则。此授权配置文件及其相关规则可作为一个“通用配置”，供尚未获得更具体角色授权的所有员工使用。

步骤 6 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。

步骤 7 点击 Add。

步骤 8 使用以下信息完成授权配置文件：

```
Name = Employee-Profile
Description = Authorization Profile for Employees
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = Employee-ACL
☑ Airespace ACL Name = Employee-ACL
```

步骤 9 对每个不同的角色类型重复整个程序。

步骤 10 点击 Submit。

调整域计算机授权

在低影响模式下，我们创建了域计算机授权配置文件，其通过使用 PERMIT_ALL_TRAFFIC dACL 来允许所有流量。

步骤 1 导航至 Policy → Policy Elements → Results → Authorization → Downloadable ACLs。

步骤 2 点击 Add。

步骤 3 如下所述，完成新的 dACL。

```
Name = AD-Machine-ACL
Description = dACL used to permit Windows to communicate to AD for Machine Auth
DACL Content =
permit udp any eq bootpc any eq bootps !DHCP
permit udp any any eq domain      !DNS
permit icmp any any           !ICMP Ping
permit tcp any host 10.1.100.10 eq 88  !Kerberos
permit udp any host 10.1.100.10 eq 88  !Kerberos
permit udp any host 10.1.100.10 eq 123 !NTP
permit tcp any host 10.1.100.10 eq 135 !RPC
permit udp any host 10.1.100.10 eq 137 !NetBIOS-Nameservice
permit tcp any host 10.1.100.10 eq 139 !NetBIOS-SSN
permit tcp any host 10.1.100.10 eq 389 !LDAP
permit udp any host 10.1.100.10 eq 389 !LDAP
permit tcp any host 10.1.100.10 eq 445 !MS-DC/SMB
permit tcp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit udp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit tcp any host 10.1.100.10 eq 1025 !non-standard RPC
permit tcp any host 10.1.100.10 eq 1026 !non-standard RPC
```

步骤 4 在 WLC 上创建与此相同的 ACL。
步骤 5 导航至 Policy → Policy Elements → Results → Authorization → Authorization Profiles。
步骤 6 点击 AD_Machine_Access。
步骤 7 如下修改授权配置文件：

```
Name = AD_Machine_Access
Description = Authorization Profile for Windows Machine Auth
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = AD-Machine-ACL
☑ Airespace ACL Name = AD-Machine-ACL
```

为每个主要角色创建其他授权策略规则

为每个需要不同授权的角色重复此程序。在本文中，我们将讲解如何创建 HR 授权策略规则，并显示包括所有已定义授权策略规则的最终屏幕。

步骤 1 导航至 Policy → Authorization。
步骤 2 在“白名单”规则下面插入一个新的策略规则。
步骤 3 将该规则命名为 **HR-Rule。**
步骤 4 将 Identity Group 留为 Any。
步骤 5 在 Other Conditions 中，选择 AD1:External Groups → Equals → HR。
步骤 6 在权限方面，选择 Standard → HR-Profile。
步骤 7 点击 Save。
步骤 8 对每个不同的角色类型重复整个程序。

禁用域用户规则

步骤 1 导航至 Policy → Authorization。
步骤 2 点击 Status 下的绿色箭头，找到 Domain Users Rule。
步骤 3 更改为 Disabled。
步骤 4 点击 Save。
步骤 5 最终规则表应该与表 4 类似。

表 4. 最终规则表

状态	规则名称		身份组		其他条件		权限
☑	已列入黑名单	如果	已列入黑名单	与	条件	那么	DenyAccess
☑	已分析的 Cisco IP 电话	如果	Cisco IP 电话	与	条件	那么	Cisco_IP_Phones
☑	已分析的思科 AP	如果	思科接入点	与	条件	那么	Access-Points
☑	Whitelist	如果	Whitelist	与	条件	那么	Whitelist
☑	HR 规则	如果	任何环境	与	AD1:外部组 等于 HR	那么	HR-Profile
☑	工程人员规则	如果	任何环境	与	AD1:外部组 等于工程人员	那么	Engineering-Profile
☑	销售规则	如果	任何环境	与	AD1:外部组 等于销售人员	那么	Sales-Profile
☑	员工规则	如果	任何环境	与	AD1:外部组 等于员工	那么	Employee-Profile
☑	承包商规则	如果	任何环境	与	AD1:外部组 等于合同工	那么	Contractor-Profile
☑	机器身份验证	如果	任何环境	与	AD1:外部组 等于域计算机	那么	AD_Machine_Access
x	域用户	如果	任何环境	与	AD1:外部组 等于域用户	那么	Domain_Users
☑	来宾	如果	来宾	与	条件	那么	来宾
☑	默认	如果未找到匹配项，那么			网络身份验证		

考虑转到多域身份验证 (MDA) 模式

多重身份验证模式可允许每个交换机端口使用虚拟的、不限数量的 MAC 地址，并要求每个 MAC 地址进行通过身份验证的会话。多重身份验证有助于防止用户在办公隔间使用未经授权的集线器或由于其他异常情况而导致偶发拒绝服务。

对于需要特定访问类型的设计场景，建议使用多域身份验证 (MDA) 模式，因为它是最安全的并且从安全的角度看提供的价值最大。对于每个端口，MDA 模式在数据域中支持一个 MAC 地址，在语音域中支持一个 MAC 地址。

注：MACSec（终端设备和交换机端口间的第 2 层加密）等未来功能需要 MDA 或单一身份验证模式，在多重身份验证模式下将不起作用。

附录 A：参考

Cisco TrustSec 系统：

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

- 思科身份服务引擎用户指南：
  http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

- 对于 Cisco Catalyst 2900 系列交换机：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000 系列交换机：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000-X 系列交换机：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 4500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 6500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- 对于 Cisco ASR 1000 系列路由器：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线 LAN 控制器：

- http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html