采用思科身份服务引擎从监控模式过渡

安全访问操作指南系列

作者：Faye Lee

日期：2012 年 8 月

目录

从监控模式迁移

有关通用交换机配置的《TrustSec 操作指南》介绍一种面向 TrustSec 2.1 版本部署的交换机配置的普遍适用方法。此方法使交换机最终处于监控模式，以开始第一阶段的 TrustSec 部署。

在监控模式下，会进行身份验证，但是不会根据身份验证结果限制网络访问。通过结合使用思科身份服务引擎 (ISE) 策略和交换机端口命令，可向所有设备授予对网络的完全访问权限。在监控模式下，网络管理员可以确定身份验证失败的用户或设备及其原因。

本指南介绍如何成功地从监控模式过渡至部署实施阶段（低影响模式或封闭模式），其中对网络的访问仅限于那些正确执行身份验证的设备或用户。

从监控模式转至低影响模式

除监控模式之外的部署模式通常通过基于端口的 ACL、dACL 和/或 VLAN 逐步将访问控制纳入设计中。基于端口的 ACL 是在交换机端口上进行本地定义，用于在流量成功通过身份验证之前过滤流量。dACL 和 VLAN 分配是在思科 ISE 上身份验证配置文件内进行集中定义，并且可以在身份验证成功之后下载至交换机。

使用分阶段方法

请务必注意，授权策略适用于*每个*已通过身份验证的会话。换句话说，所有交换机会同时从监控模式转至低影响模式，并且对于所有通过身份验证的用户，访问控制都是由过滤其网络访问的身份验证提供的。

在部署实施期间，您可能不想安排所有人同时迁移。本节介绍两种分阶段迁移方法：一次迁移一台交换机，以及转至低影响模式。

一次迁移一台交换机

分阶段迁移的其中一种方法是指定处于低影响模式而非监控模式的交换机。通过创建一个名为“Stage”的网络设备组，并在此“Stage”组中创建名为“Low Impact”或“Closed”的组，可完成此操作。

创建一个网络设备组以指示处于低影响模式的交换机

步骤 1. 导航至 Administration → Network Resources → Network Device Groups → Groups。
步骤 2. 点击 Add 添加组，将名称和设备类型设置为 **Stage**。

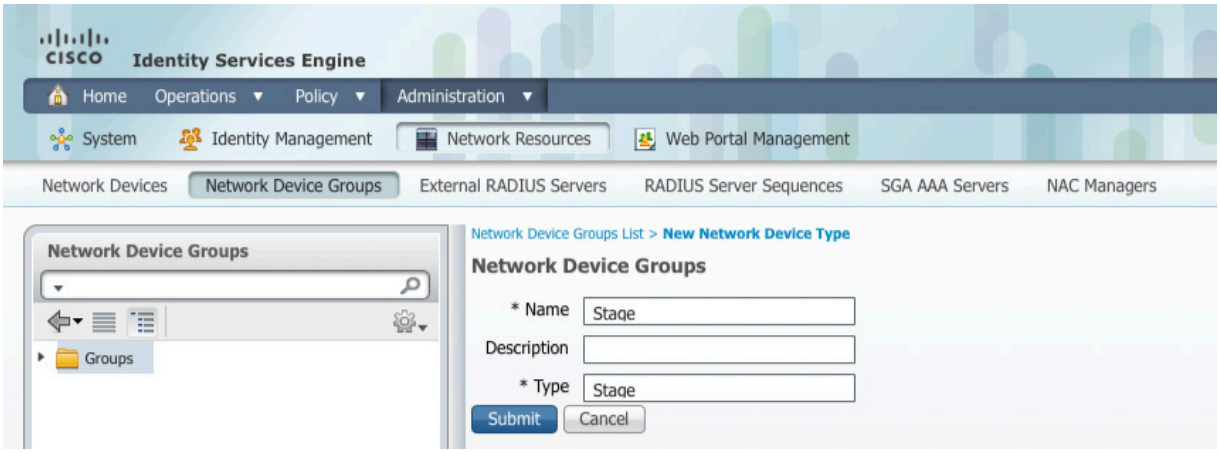

图 1. Stage 网络设备组

步骤 3. 点击 Submit。
步骤 4. 导航至新创建的 Stage 组。
步骤 5. 添加组，将名称设置为 **LowImpact**。

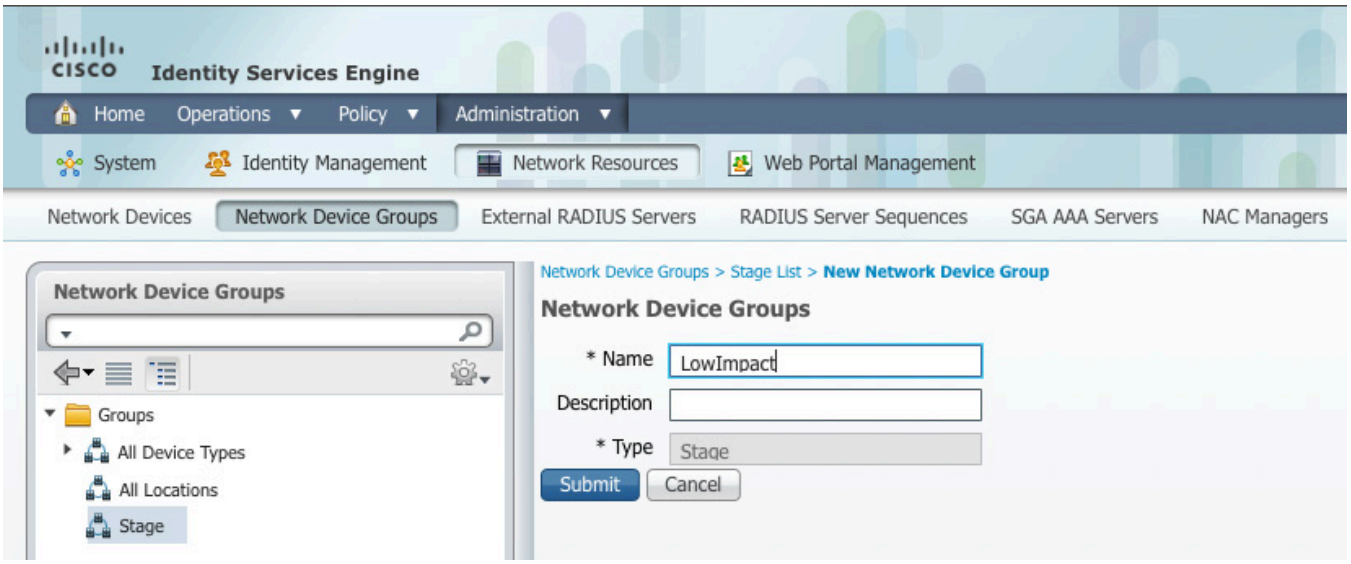

图 2. 低影响网络设备组

步骤 6. 点击 Submit。
步骤 7. 导航至 Administration → Network Resources → Network Devices。
步骤 8. 编辑要转至低影响模式的接入层交换机。
步骤 9. 将 Stage 设置为 LowImpact。

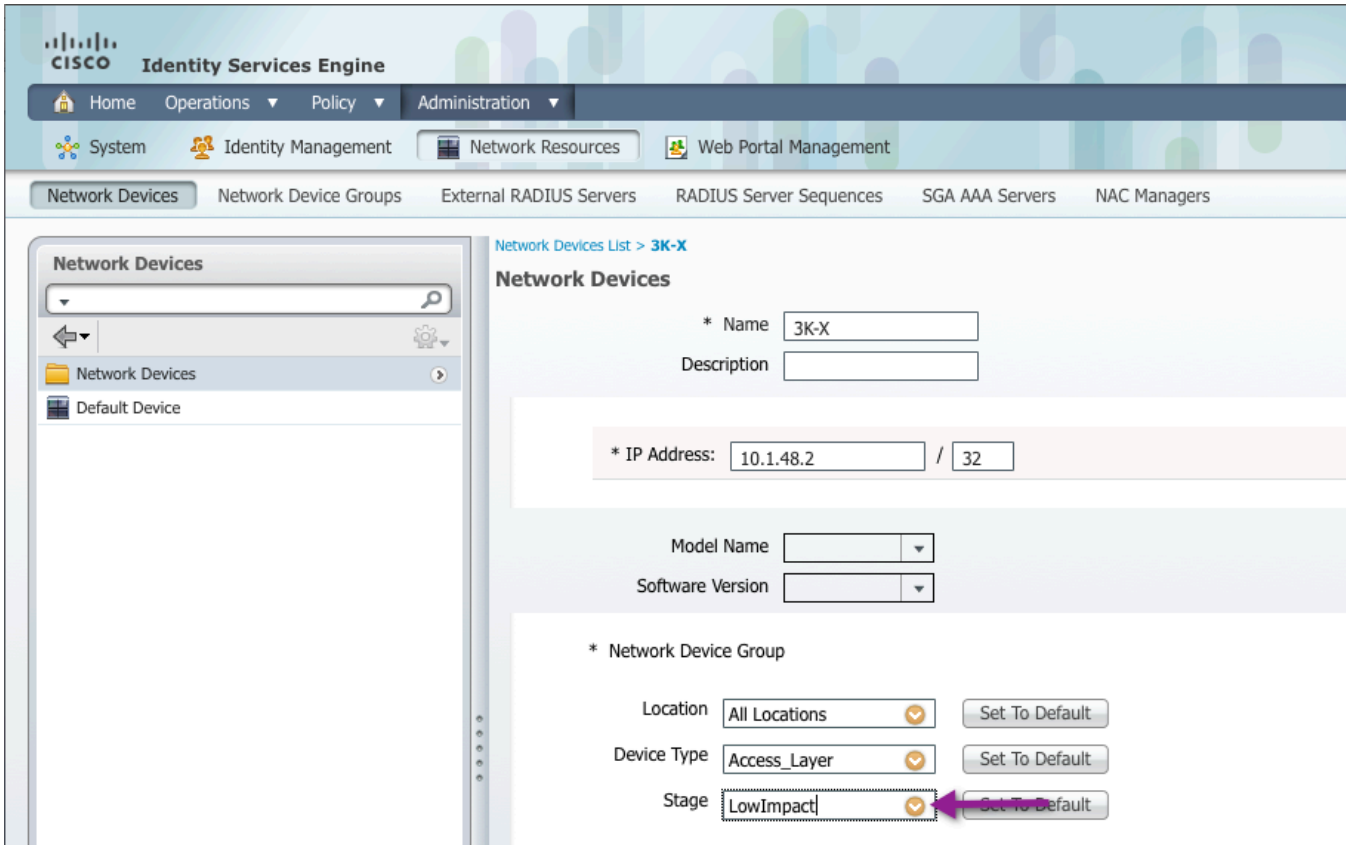

图 3. 将网络设备添加至网络设备组

步骤 10. 点击 Save。

转至低影响模式

低影响模式有两个阶段。阶段 1 是在身份验证之前提供过滤的访问权限，并在用户或设备身份验证成功之后提供对网络的完全访问权限。阶段 2 是提供角色特定的访问控制，而不是完全开放的网络访问权限。有关不同部署模式的详细信息，请参阅介绍部署选项的《TrustSec 操作指南》。

阶段 1

在此阶段，我们的目标是将默认端口 ACL 更改为限制访问的端口，限制程度完全取决于部署计划。我们将检查一些现场已使用的默认端口 ACL，并讨论您的部署中存在哪些问题以及如何对默认端口 ACL 进行相应的调整。

以下是两个建议的默认端口 ACL。

ACL-DEFAULT（推荐的安全默认端口 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
 remark 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。您还可通过计算机身份验证打开 Microsoft 特定端口。

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
```

登录速度慢

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，确定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。将默认端口 ACL 留为 ACL-ALLOW (permit ip any any)。

更改默认端口 ACL

在交换机上将 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
```

阶段 2

有线访问-802.1X 和 MAB 身份验证

在此阶段，所有有线设备都应通过 802.1X 或 MAB 进行身份验证，从而提供对网络的完全访问权限。现在，我们应该通过区分每个用户获得的访问权限，更有效地保护网络。对于有些部署来说，通过身份验证后再提供完全访问权限可能已经足够安全了，但是，对大多数企业来说，这样还不够安全。

向每个用户或设备会话应用特定 dACL 可实现这种访问权限区分。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）。没有 dACL，设备仍会使用默认端口 ACL。此阶段与前一个阶段的明显区别在于，根据用户角色对用户或设备产生的具体授权结果不同。

图 4. 最终状态的低影响模式流程

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 → External Identity Sources → Active Directory。
步骤 2. 点击 Groups 选项卡。
步骤 3. 点击 Add → Select Groups from Active Directory。

步骤 4. 点击 Retrieve Groups。

注：当 AD 有 100 多个组时，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。我们最终的组选择屏幕截图如下：

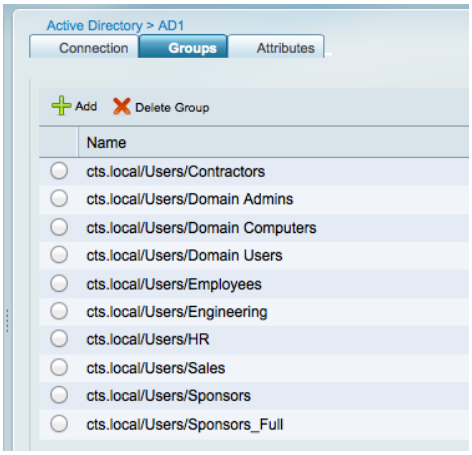

图 5. 从 AD 选择组

步骤 7. 滚动到底部，点击 Save Configuration。

注：如果保存配置，在授权过程中，将不会从 Active Directory 中检索到其他组。

角色特定访问权限的配置

为每个主要角色创建其他可下载 ACL

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。

思科最佳实践：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 (Enforcement Mode)
DACL Content =
Deny ip any <ip_address_range_of_engineering_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。

以下是我们示例中使用的最终 dACL 列表的屏幕截图：

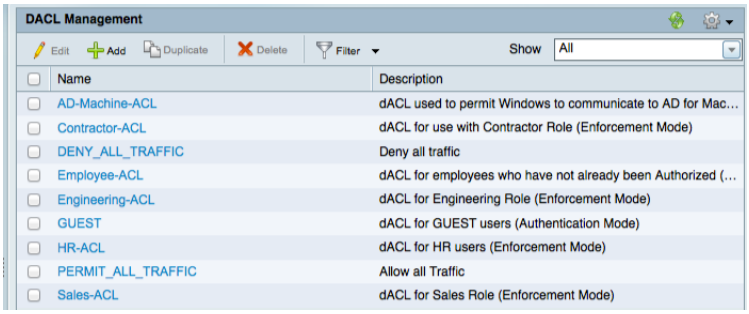

图 6. dACL 列表

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。正如在程序 1 中一样，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 (Enforcement Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑  DACL Name = HR-ACL
☑  Wireless LAN Controller (WLC) = HR-ACL
```

注：无线局域网控制器 (WLC) 字段用于应用在 WLC 上本地定义的无线 ACL (wACL)。WLC 目前不支持 dACL。

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 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 = Employee-Profile
Description = Authorization Profile for Employees (Enforcement Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = Employee-ACL
☑ Wireless LAN Controller (WLC) = Employee-ACL
```

步骤 4. 点击 Submit。

以下是我们示例中使用的最终授权配置文件列表的屏幕截图：

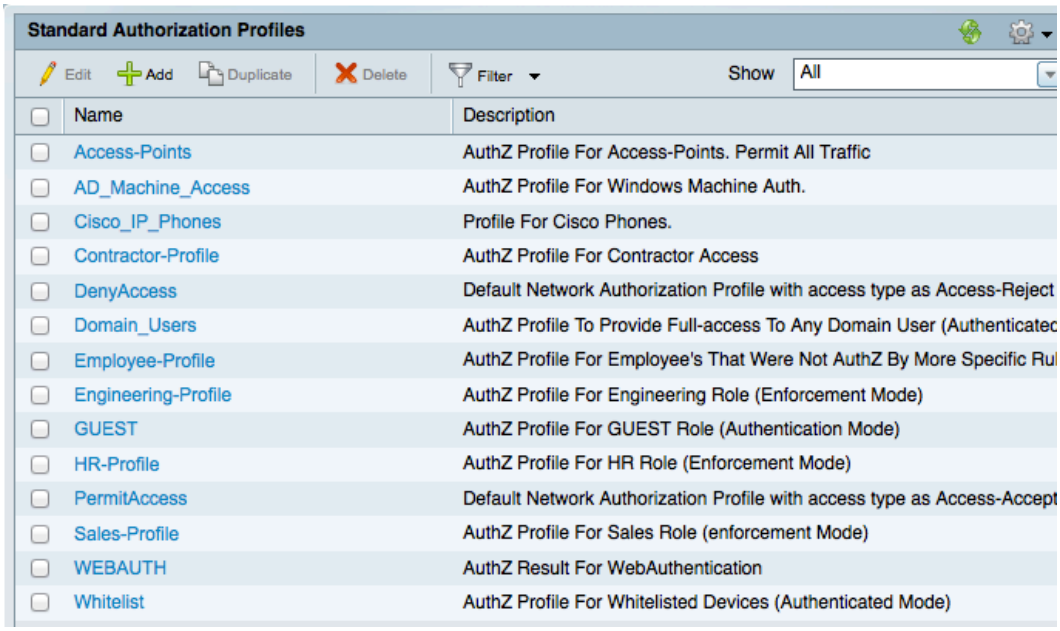

图 7. 标准授权配置文件

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并通过使用 PERMIT_ALL_TRAFFIC dACL 来允许所有流量。在实施模式下，应锁定流量，确保只有那些 Windows 域成员的所需端口可与 Active Directory 通信。

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 (Enforcement Mode)
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. 在无线局域网控制器上创建与此相同的 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
☑ Wireless LAN Controller (WLC) = 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. 点击齿轮图标。 
步骤 7. 添加属性。
步骤 8. 将表达式设置为 Device:Stage → Equals → LowImpact。
步骤 9. 在权限方面，选择 Standard → HR-Profile。
步骤 10. 点击 Save。
步骤 11. 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. 最终规则表应该与下表类似：

表 1. 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	并	条件	那么	DenyAccess
☑	已分析的 Cisco IP 电话	如果	Cisco IP 电话	并	条件	那么	Cisco_IP_Phones
☑	已分析的思科 AP	如果	思科接入点	并	条件	那么	接入点
☑	白名单	如果	白名单	并	条件	那么	白名单
☑	HR 规则	如果	任意	并	AD1：外部组等于 HR 且 设备：阶段等于 Stage#LowImpact	那么	HR-Profile
☑	工程规则	如果	任意	并	AD1：外部组等于 Engineering 且 设备：阶段等于 Stage#LowImpact	那么	Engineering-Profile
☑	销售规则	如果	任意	并	AD1：外部组等于 Sales 且 设备：阶段等于 Stage#LowImpact	那么	Sales-Profile
☑	员工规则	如果	任意	并	AD1：外部组等于 Employees 且 设备：阶段等于 Stage#LowImpact	那么	Employee-Profile
☑	承包商规则	如果	任意	并	AD1：外部组等于 Contractors 且 设备：阶段等于 Stage#LowImpact	那么	Contractor-Profile
☑	机器身份验证	如果	任意	并	AD1：外部组等于 Domain Computers 且 设备：阶段等于 Stage#LowImpact	那么	AD_Machine_Access

状态	规则名称		身份组		其他条件		权限
x	域用户	如果	任意	并	AD1：外部组等于 Domain Users 且 设备：阶段等于 Stage#LowImpact	那么	Domain_Users
☑	访客	如果	访客	并	条件	那么	访客
☑	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

正如开始的《操作指南-10-通用交换机配置指南》中所述，我们已配置使用多重身份验证 (Multi-Auth)。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。

建议使用多域身份验证模式，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（端点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。

封闭模式（以前称为高安全性模式）

封闭模式表示默认的 802.1X 行为。在封闭模式下，交换机端口在从 AAA 服务器获得授权结果之前不会允许除局域网扩展认证协议 (EAPoL) 之外的任何流量。这通常是部署的理想最终状态，因为它提供了非常强的安全性。像低影响模式一样，封闭模式能够使用 TrustSec 部署中的所有可用实施机制（dVLAN、dACL、SGA 等），但是封闭模式可能会对 IT 部署的运行模式产生某些影响。

删除开放式身份验证

步骤 1. 删除开放式身份验证。

```
C3750X(config-if-range)# no authentication open
```

步骤 2. 删除端口 ACL。

```
C3750X(config-if-range)# no ip access-group ACL-DEFAULT in
```

附录 A：参考

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
- 对于思科无线局域网控制器：
  http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html