OmniVista UPAM 和 Palo Alto Networks 零信任网络访问 (ZTNA) 协同应用

应用说明

OmniVista UPAM 和 Palo Alto Networks 用户 ID 零信任网络访问 (ZTNA) 协同应用说明

Alcatel·Lucent Enterprise

目录

1. 关于本集成指南

本文档旨在帮助阿尔卡特朗讯企业通信 (ALE) 的业务合作伙伴和客户将阿尔卡特朗讯 OmniVista® 统一策略身份验证管理器 (UPAM)，通过与 Palo Alto Networks (PAN) 下一代防火墙的用户 ID 功能集成，实现零信任网络访问 (ZTNA) 协同。通过该协同应用方案，实现基于 LAN 和/或 WLAN 网络身份验证的用户或设备也可以同时无缝利用 PAN 防火墙进行身份验证。OmniVista UPAM 可以与防火墙安全联动，同步用户或设备的连接状态、身份或角色信息，以增强可见性、实现更精细的策略控制并提升安全威胁管理，优化日志记录、报告和取证分析。

2. 零信任范式

在传统防火墙中，“信任”的边界基于连接点：“内部”用户默认受信任，而“外部”用户则不受信任。以机场为例，这相当于允许登机乘客不受检查地通过安检。随着移动性和物联网 (IoT) 等趋势的发展，这种“信任”的概念已经完全过时。例如，自带设备 (BYOD) 可能会将恶意软件带入组织机构，物联网设备可能存在内在漏洞并成为攻击的载体，甚至企业用户也可能是存在安全威胁的。

现在的安全趋势是“零信任”：即无论用户或设备连接到哪里，永远不要信任并始终要进行验证。身份验证是零信任范式的核心。还是以机场为例，机场工作人员（安全、入境）要做的第一件事就是检查护照。签证检查、数据库核对等其他检查都是在使用护照和指纹匹配等验证身份后进行的。此外，由于身份验证是零信任范式核心的基本检查，下一代防火墙有多种机制来确定身份。

3. 关于 Palo Alto Networks 用户 ID

用户 ID 是 Palo Alto Networks (PAN) 防火墙上的一项标准功能，使防火墙能够利用各种信息存库和技术识别用户。了解用户的身份和/或角色而不仅仅是其 IP 地址，是具有一定优势的，不仅包括仅允许具有合法需求的用户/角色访问应用和/或资源（最低权限原则）通过以提高使用模式的可见性并实现更精细的策略控制，还包括通过引用用户身份或角色而不仅仅是 IP 地址来增强日志记录、报告和取证。有关用户 ID 功能的更多信息，请参阅 Palo Alto Networks 的文档。

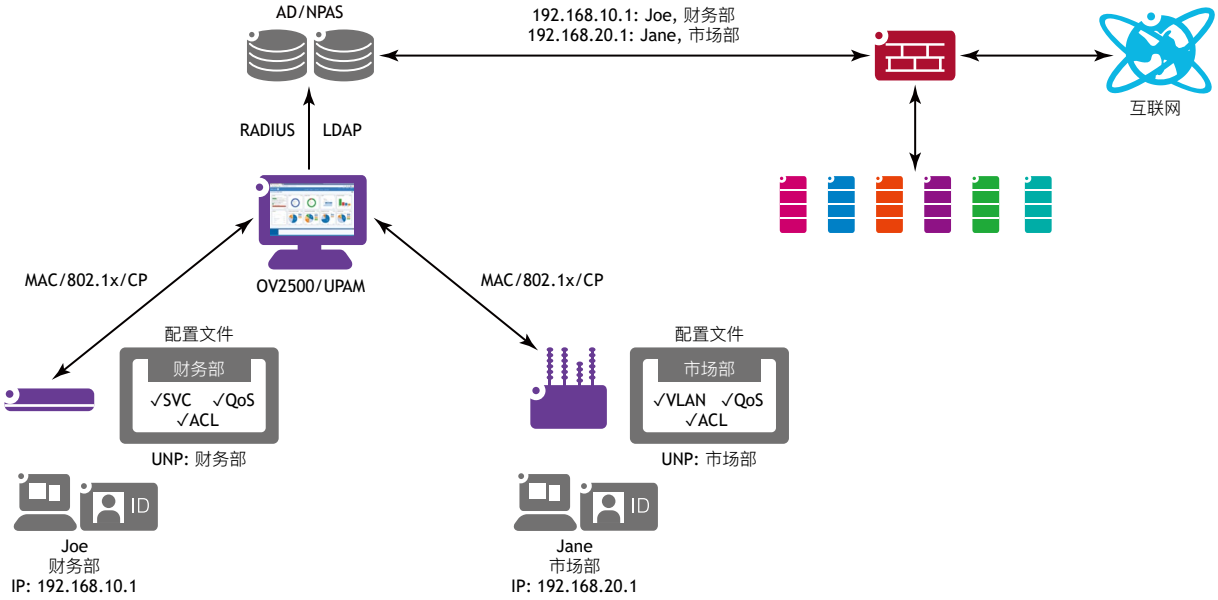
4. 关于阿尔卡特朗讯 OmniVista UPAM

OmniVista 的统一策略身份验证管理是个统一接入管理平台，面向阿尔卡特朗讯 OmniSwitch® 以太网交换机和阿尔卡特朗讯 OmniAccess® Stellar 接入点。UPAM 包括专属门户和 RADIUS 服务器，可以实现多种身份验证方法，如 MAC 身份验证、802.1x 身份验证和专属门户身份验证。用户可以根据 UPAM 本地数据库或外部数据库（包括 Microsoft Active Directory、LDAP 和外部 RADIUS）进行身份验证。UPAM 的可定制专属门户可以通过电子邮件、短信和社交软件（例如 Facebook、谷歌、微信和 Rainbow）进行集成的凭证管理，为访客和自带设备 (BYOD) 用户实施灵活的身份验证策略。

5. 用例

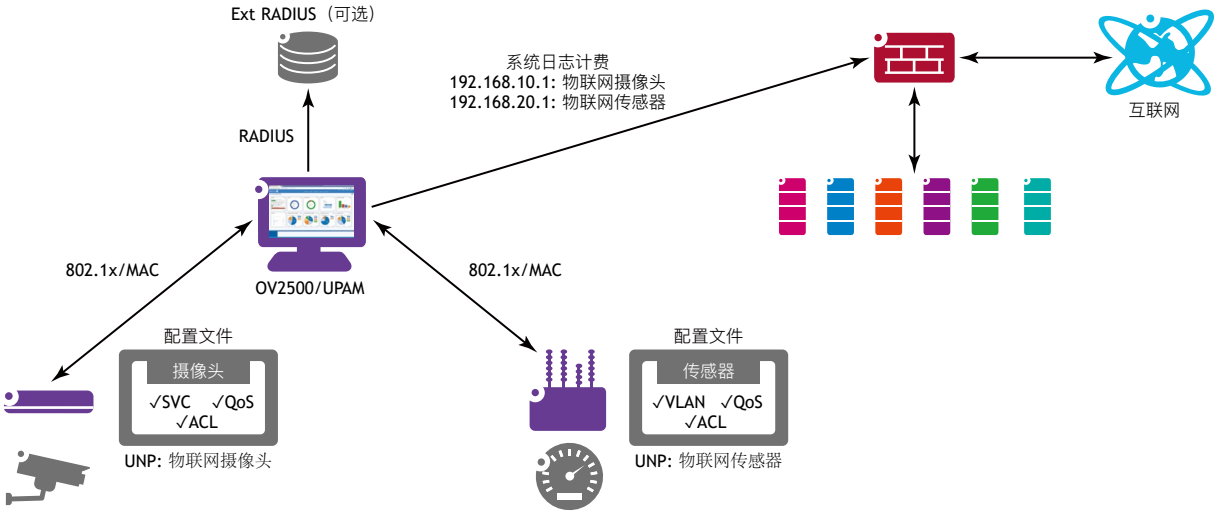
对于有线和无线用户，主要有两种用例：企业 (AD) 设备和自带设备 (BYOD) 或物联网设备。对于企业设备，例如企业笔记本电脑上的企业用户，OmniVista 统一策略身份验证管理器 (UPAM) 可以将身份验证交给 AD 来执行，首选直接在 AD 上集成，而不是在 UPAM 上集成。本指南不会进一步详细说明这一用例。有关基于 AD 的集成的更多详细信息，请参阅 Palo Alto Networks 文档。

图 1. 基于 AD 的集成



在本指南中，我们将重点介绍其他用例，其中 BYOD 或 IoT 设备直接根据 UPAM 数据库进行身份验证或代理到外部 RADIUS 数据库（不包括 Microsoft 网络策略和接入服务或 NPAS）进行身份验证，因为这些设备可能不与 AD 帐户关联。这种用例如下图所示，以物联网为例。本文档着重介绍这种用例，因为在 OmniVista UPAM 上直接集成。

图 2：基于系统日志的集成



6. 机制

登录后，有线或无线设备就通过 MAC 或 802.1x 认证根据 UPAM RADIUS 进行身份验证。UPAM 将身份验证和计费事件记录到 PAN 内置系统日志接收器。PAN 防火墙上定义了一个解析筛选器，用于从这些消息中提取角色或用户名。有关 UPAM 生成的一些系统日志消息示例，请参阅下面的代码段。

图 3：UPAM 系统日志记录示例

<14>Mar 30 18:26:27 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"E8E732A48A230003E6A6FB74","authType":"MAC",
"changeType":"Access","deviceIP":"","deviceMac":"0003E6A6FB74","filterId":
"IOT_STB","time":"2020-03-30 18:26:27","username":"0003E6A6FB74"}

<14>Mar 30 18:26:27 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"192.168.114.22_03/30/2020
18:26:27_0003e6a6fb74","authType":"MAC","changeType":"Accounting","deviceIP":
"10.211.5.51","deviceMac":"0003E6A6FB74","filterId":"IOT_STB","time":"2020-03-30
18:26:27","username":"0003E6A6FB74"}

<14>Mar 30 18:26:13 localhost
{"APMAC":"E8E732A48A23","acctSessionId":"192.168.114.22_03/30/2020
18:19:10_0003e6a6fb74","authType":"MAC","changeType":"Disconnect","deviceIP":
"10.211.5.51","deviceMac":"0003E6A6FB74","filterId":"IOT_STB","time":"2020-03-30
18:26:12","username":"0003E6A6FB74"}

我们来看看这些消息中的一些相关字段：

APMAC: The RADIUS NAS（交换机或接入点）MAC 地址。

authType: 此字段指定身份验证机制（例如 MAC 或 802.1x 认证）。

changeType: 可以是“Access（接入）”，表示身份验证成功，“Accounting（计费）”表示定期的 RADIUS 计费消息，“Disconnect（断开连接）”表示注销/断开连接事件。

设备 IP（deviceIP）：终端设备的 IP 地址。

筛选器 ID（filterID）：filter ID 表示 uNP（用户网络配置文件）或 ARP（接入角色配置文件），也就是分配给设备的角色。

用户名（username）：顾名思义，就是用户名。使用 MAC 认证时，用户名只是终端设备的 MAC 地址。

我们想提醒大家注意以下几个方面：

- 防火墙执行策略需要设备的 IP 地址，包含在“Accounting（计费）”和“Disconnect（断开连接）”消息中，但通常不包含在“Access（接入）”消息中。这是因为通过 DHCP 获取 IP 地址需要一段时间，而且必须先进行身份验证。
- 因此，除了身份验证功能外，还需要启用 RADIUS 临时计费功能。
- 只有一个系统日志解析配置文件可以应用于防火墙上的任何给定系统日志源。我们将为“Accounting（计费）”消息创建筛选器，因为这是包含所有必要信息（设备 IP、用户名和/或筛选器 ID）的消息类型。我们无法为“Disconnect（断开连接）”消息配置筛选器。因此，用户断开连接不会立即从防火墙注销。如果在用户 ID 超时（默认为 45 分钟）到时之前未收到“计费”更新，则用户将被注销。
- 因此，RADIUS 临时计费间隔应设置为低于用户 ID 超时时间。

7. 程序概述

以下是 OmniVista/UPAM 和 PAN 防火墙所需不同步骤的摘要。

OmniVista UPAM

1. 配置 AAA 配置文件，用于根据 UPAM 进行 802.1x/MAC 认证
2. 配置 UPAM 接入策略和身份验证策略
3. 配置 UPAM，将外部系统日志记录迁移到 PAN 防火墙
4. 针对 MAC/M802.1x 认证在 UPAM 中创建接入身份验证配置文件

PAN 防火墙

1. 在所需防火墙区域启用用户 ID
2. 在接口的管理配置文件上启用 UDP 系统日志监听功能
3. 为 UPAM 日志创建系统日志解析配置文件
4. 配置系统日志服务器监控
5. 启用用户 ID 防火墙策略
6. 验证用户 ID 映射
7. 验证用户 ID 策略

8. OmniVista：配置 AAA 配置文件

在 OmniVista 界面，进入“Unified Access（统一接入）->Template（模板）->AAA Server Profile（AAA 服务器配置文件）”，点击“+”。

创建一个新的 AAA 服务器配置文件，指向 UPAM Radius 服务器进行身份验证和计费。选择所需的身份验证方法（802.1x、MAC 或专属门户）执行这一操作。下面的示例仅显示了 802.1x 和 MAC，因为物联网设备通常不使用专属门户身份验证。

图 4：AAA 服务器配置文件——身份验证

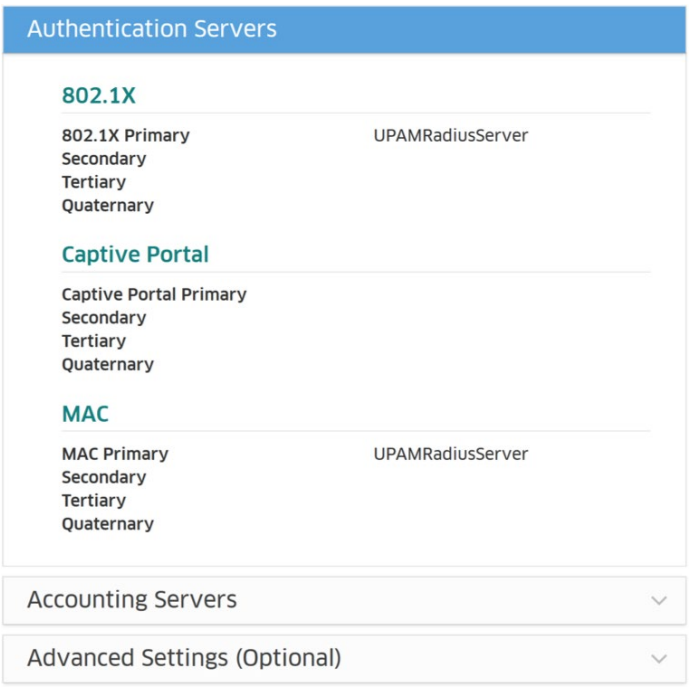
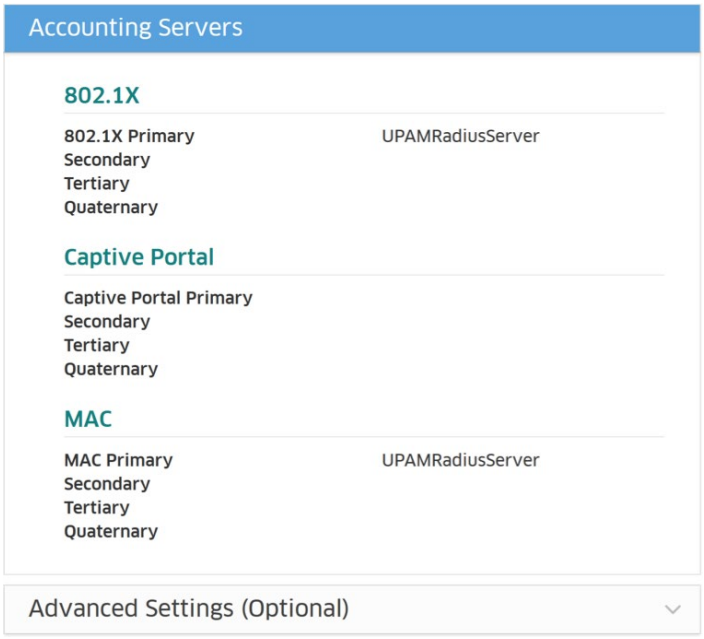


图 5：AAA 服务器配置文件——计费



你还可以指定临时计费间隔（默认为 600 秒），也可以信任 RADIUS 服务器（UPAM 或外部服务器）设置的临时计费间隔，但必须在 RADIUS 服务器上配置这个临时计费间隔。在大多数情况下，身份验证成功后不久发送的第一条计费消息将包含设备 IP 地址，并允许防火墙识别用户。然而在其他情况下，设备 IP 地址只会出现在第二个和后续的计费消息中。在这种情况下，设置较低的临时间隔会导致此类信息在防火墙上更新更快。

无论临时计费间隔是受 RADIUS 服务器信任的还是在 AAA 服务器配置文件上设置的，都必须低于防火墙上设置的用户身份验证超时时间，默认值为 45 分钟。默认设置为 600 秒，可以满足这一要求。

图 6：MAC——临时计费间隔

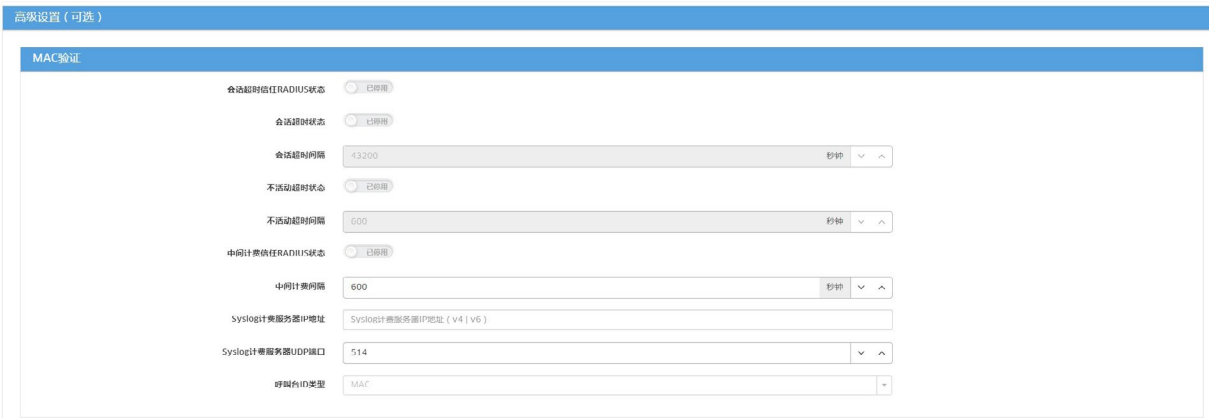


图 7：802.1x 临时计费间隔

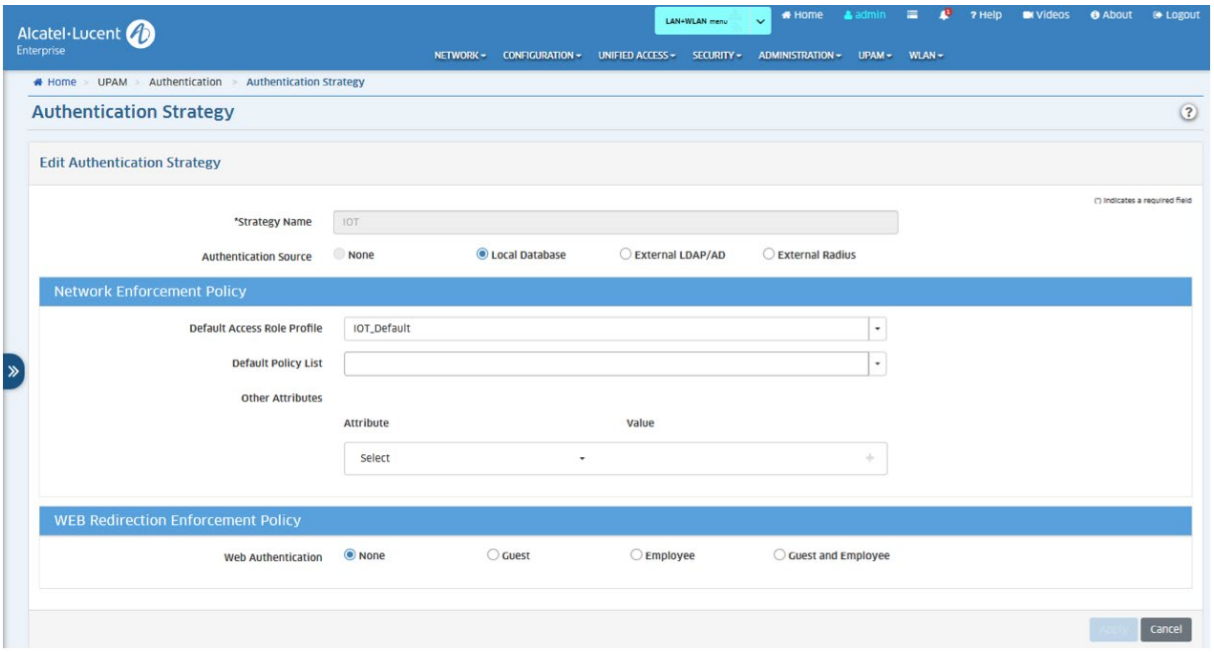
9. OmniVista：配置 UPAM 接入策略和身份验证策略

备注：身份验证策略定义将使用哪个身份验证数据库和其他参数，而接入策略根据 SSID 或交换机 NAS IP 等条件将身份验证请求匹配到合适的策略。

要创建身份验证策略，进入“UPAM->Authentication（身份验证）->Authentication Strategy（身份验证策略）”，点击“+”。使用 UPAM 内部数据库的身份验证策略示例如下所示。默认的访问角色配置文件 (ARP) 是在未向设备分配特定角色、或交换机或 AP 组未在本地定义指定角色时要应用的角色。

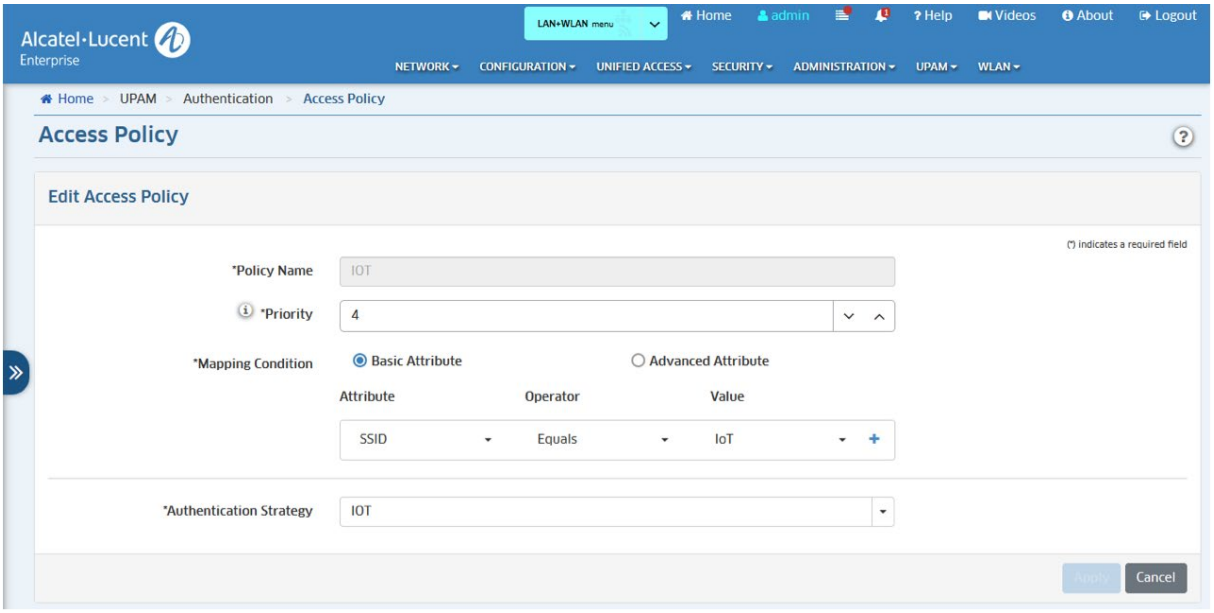
注：在创建身份验证策略之前，必须先创建默认访问角色配置文件。此外，必须创建所有相关访问角色配置文件并将其映射到交换机和 AP 组。本指南不显示这些步骤。

图 8：身份验证策略



要创建一条接入策略，进入“UPAM->Authentication（身份验证）->Access Policy（接入策略）”，点击“+”。接入策略基于 SSID（如示例中所示）、NAS IP、位置等条件，将身份验证请求映射到先前创建的身份验证策略

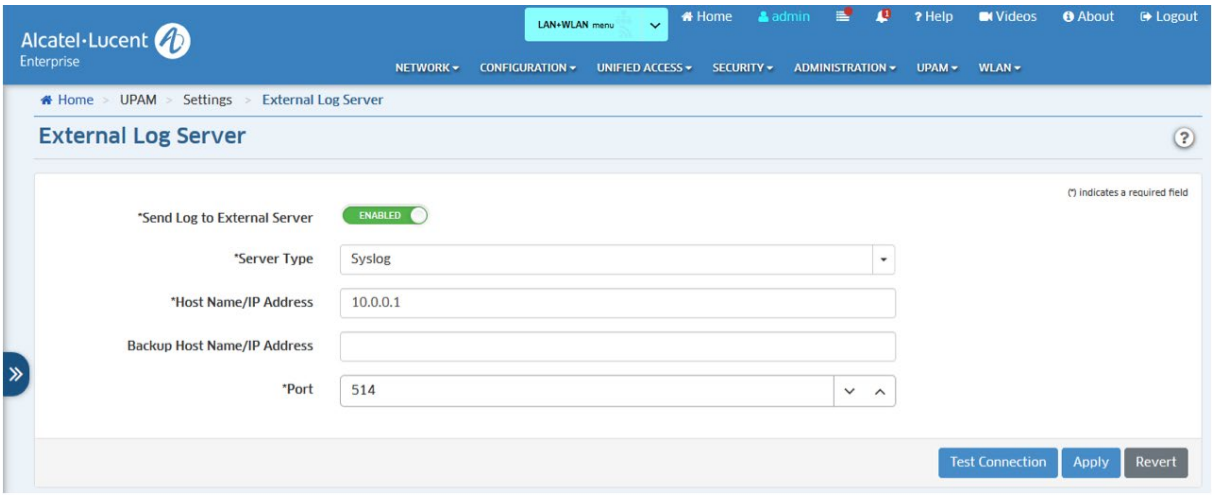
图 9：接入策略



10. OmniVista：配置 UPAM，将外部系统日志记录迁移到 PAN 防火墙

进入“UPAM->Settings（设置）->External Log Server（外部日志服务器）”。启用日志记录并选择默认端口 (514) 的系统日志记录，如下例所示。输入其他系统日志记录服务器的 IP 地址或主机名（可选）。

图 10：外部系统日志记录

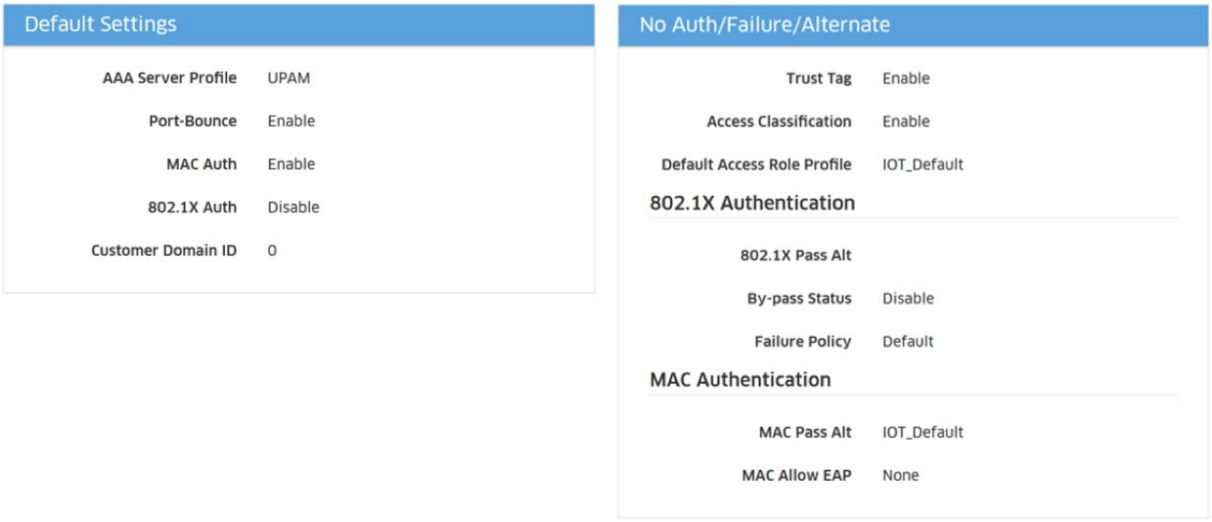


注：PAN 防火墙不对系统日志记录连接测试做出响应。连接测试会导致“The server cannot connect（服务器无法连接）”消息。这是预期的行为。您仍应验证 UPAM 和防火墙之间是否可以连接 UDP 端口 514。

11. OmniVista：配置和应用接入身份验证配置文件

进入“Unified Access（统一接入）->Unified Profile（统一配置文件）->Templates（模板）->Access Auth Profile（接入身份验证配置文件）”，点击“+”。选择前面定义的 UPAM AAA 服务器配置文件，并根据需要配置 MAC/802.1x 认证选项。下面的示例显示了 MAC 认证，使用“IOT_Default”配置文件作为默认 pass-alternate（当返回的属性与交换机或 AP 组上本地定义的配置文件不匹配时使用）。完成后，将其应用到所需的交换机和 AP 组。

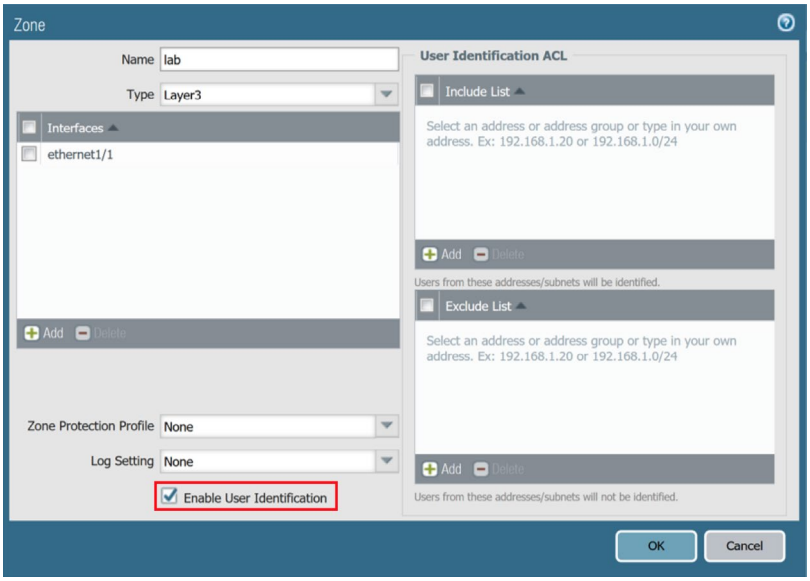
图 11：接入身份验证配置文件



12. PAN：在所需防火墙区域启用用户 ID

在 PAN 防火墙界面，进入“Network（网络）->Zones（区域）”，选择要启用用户 ID 的一个或多个区域。启用复选框，如下例所示。根据需要配置包含/排除 ACL。

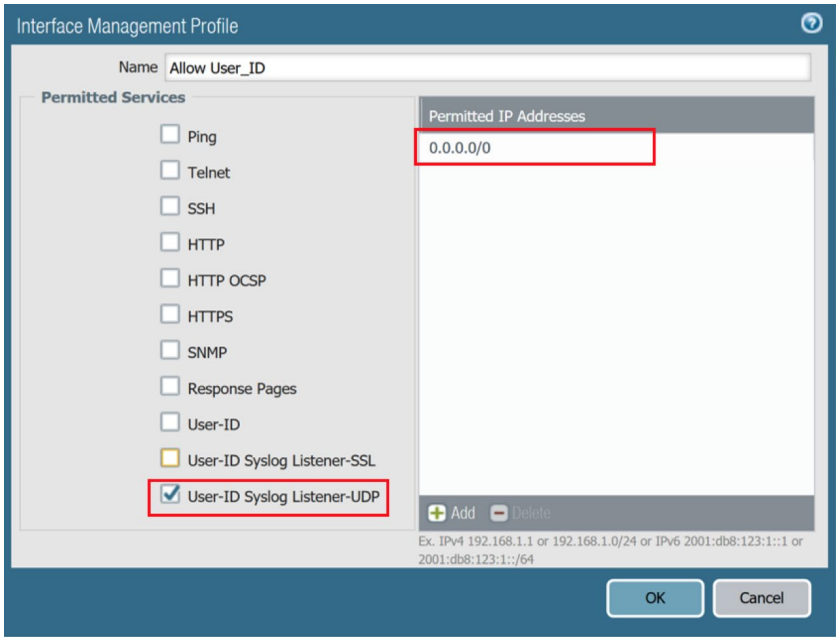
图 12：在防火墙区域启用用户 ID



13. PAN：在接口管理配置文件上启用 UDP 用户 ID 系统日志监听功能

在防火墙界面，进入“Network（网络）->Network Profiles（网络配置文件）->Interface Management（接口管理）”。添加或选择现有配置文件。启用“User-ID Syslog Listener UDP（用户 ID 系统日志监听功能 UDP）”复选框，并将 UPAM 的 IP 地址添加到列表，如下例所示。此配置文件必须应用于要接收 UPAM 系统日志消息的管理接口。

图 13：接口管理配置文件



14. PAN：为 UPAM 日志创建系统日志解析配置文件

系统日志解析配置文件帮助防火墙识别 OmniVista UPAM 系统日志消息中的用户名和地址字段。要创建解析配置文件，进入“Device（设备）->User Identification（用户 ID）”，在“ User Mapping（用户映射）”选项卡中，点击“Palo Alto Networks User ID Agent Setup（Palo Alto Networks 用户 ID 代理设置）”右侧的齿轮图标。

在“Palo Alto Networks User ID Agent Setup（Palo Alto Networks 用户 ID 代理设置）”窗口中，点击“Syslog Filters（系统日志筛选器）”选项卡，点击“Add（添加）”。

图 14：用户映射

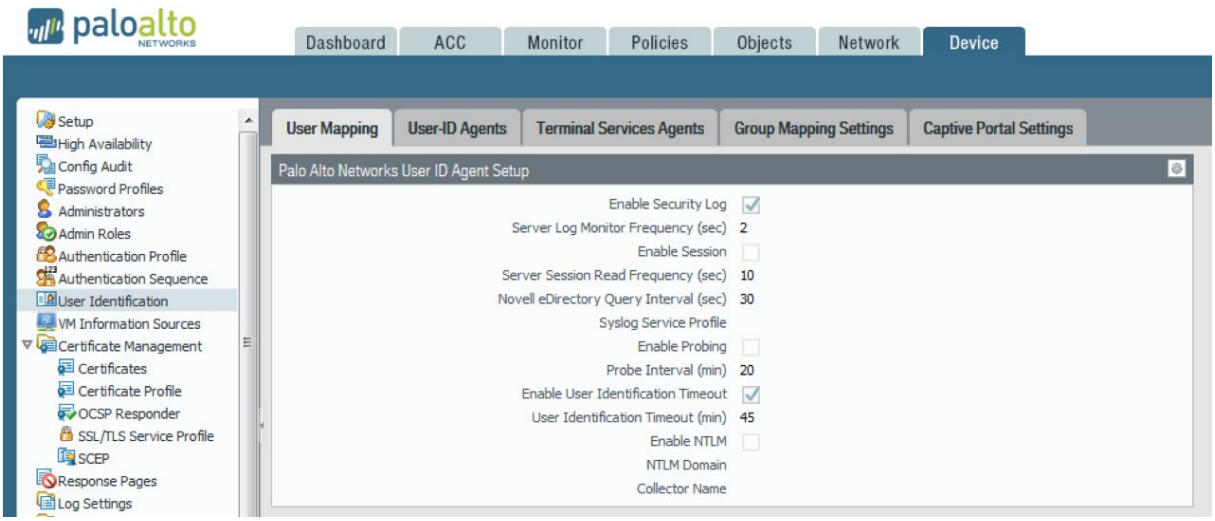
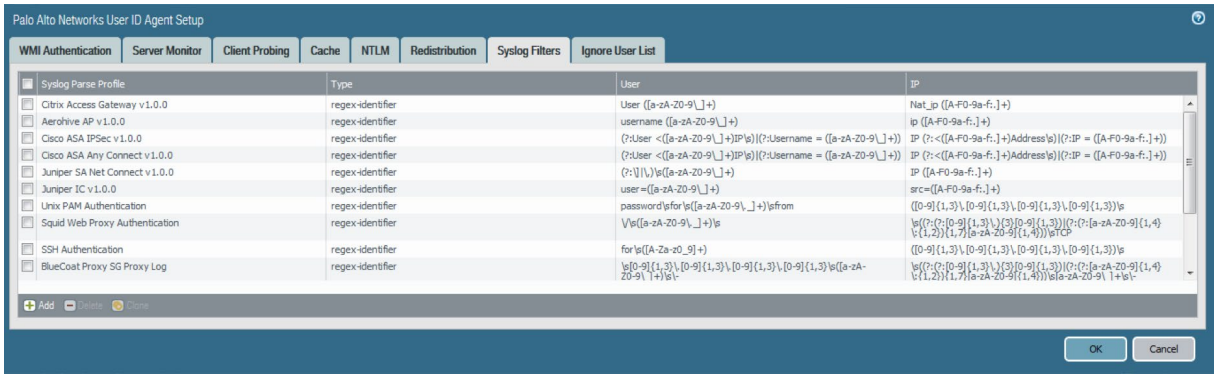


图 15：系统日志筛选器



下面的第一个示例映射计费消息中的用户名和设备 IP 字段。要使 PAN 防火墙基于这些用户名应用策略，必须在防火墙的本地数据库中创建包含这些用户的用户组，或者在防火墙策略中列出每个用户名。这可能是有问题的，特别是在使用 MAC 认证时，因为用户名将只是设备的 MAC 地址。

有个更简单的替代方法，即映射筛选器 ID（即 UNP、ARP 或“角色”），在第二个示例中显示。在这种情况下，防火墙策略可以简单地引用 UNP/ARP 或设备的角色（例如“传感器”），无需在防火墙的数据库中创建用户。这种替代方法的缺点是，防火墙日志不包含实际的用户名，而是包含角色。但是除了 PAN 防火墙之外，OmniVista UPAM 还可以将消息记录迁移到其他服务器，这有助于在给定时间检索与 IP 地址相关联的实际用户名（如果需要进行取证等）。日志关联需要 OmniVista、PAN 防火墙和系统日志服务器实现时间同步。

图 16：系统日志解析配置文件——用户映射

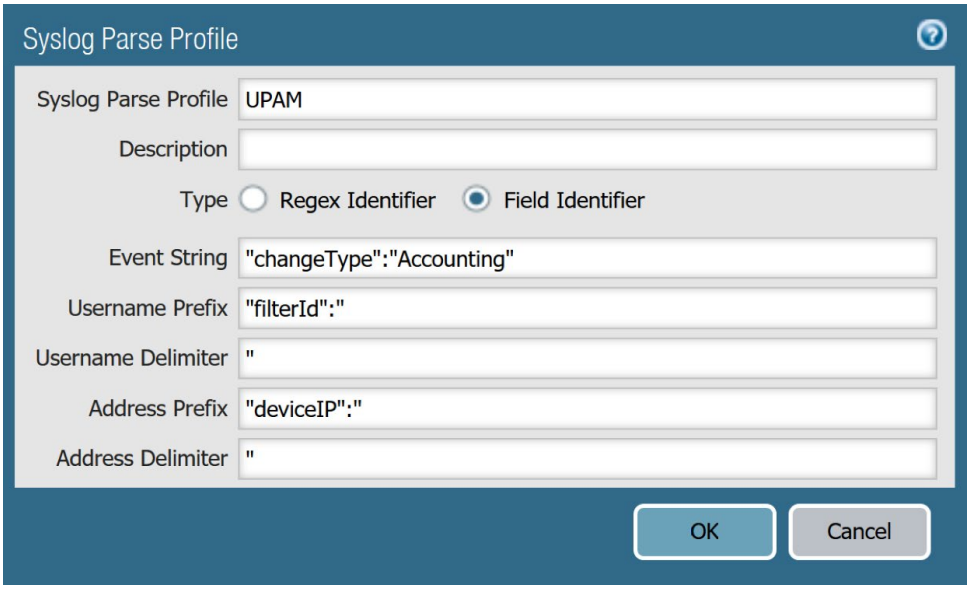
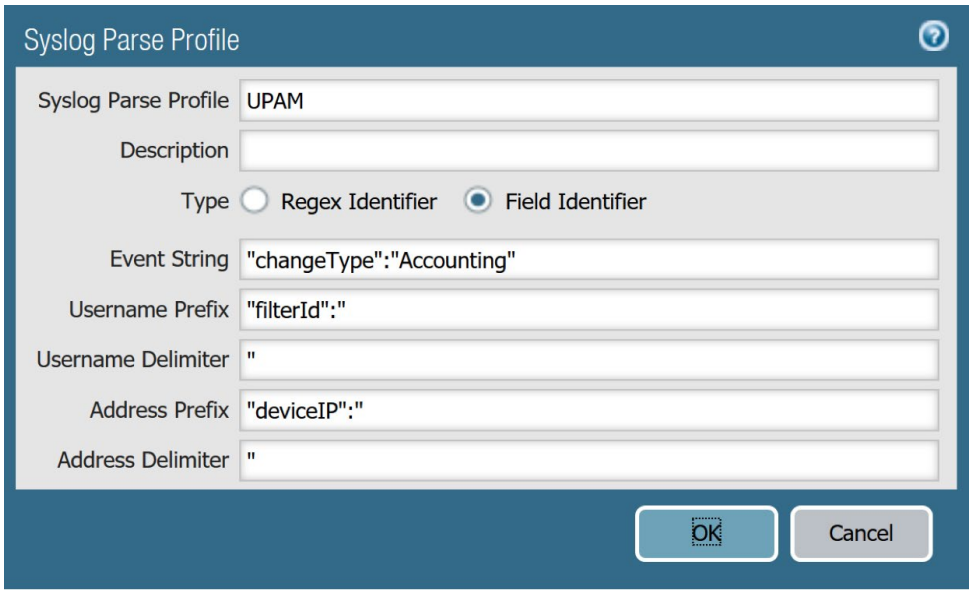


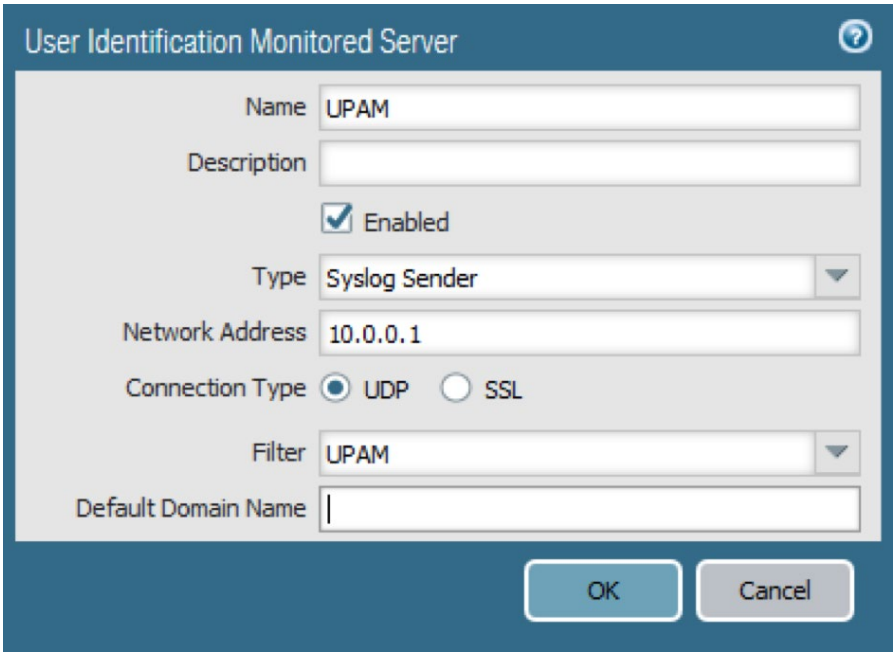
图 17：系统日志解析配置文件——角色映射



15. PAN：配置系统日志服务器监控

进入“Device（设备）->User Identification（用户 ID）->Server Monitoring（服务器监控）”，点击“Add（添加）”。输入名称，选择“Syslog Sender（系统日志发送者）”类型，填写 UPAM IP 地址，选择连接类型“UDP”以及上一步中定义的系统日志解析筛选器。如果日志条目没有域名，则输入域名作为用户名的前缀，这是根据 UPAM 本地数据库进行身份验证的情况（可选）。

图 18：用户 ID 监控服务器



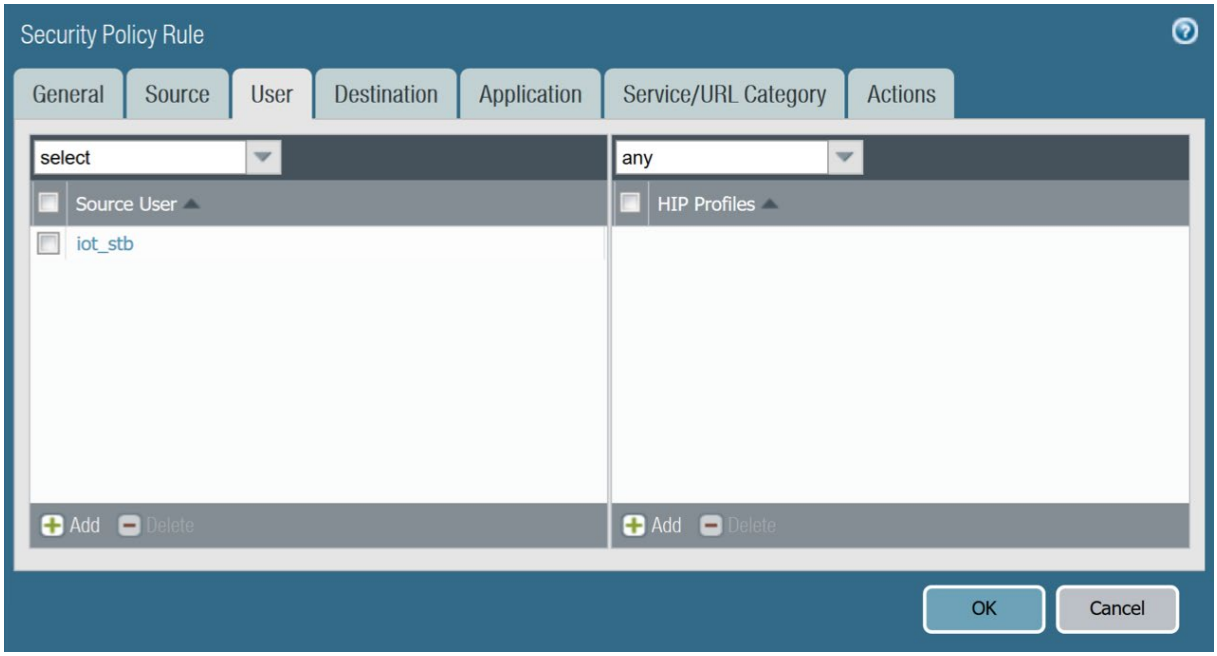
定义要在用户映射中包含或排除的子网络（可选）。

16. PAN：在防火墙策略中启用用户 ID

进入“Policies（策略）->Security（安全）”，创建或选择现有策略。选择“User（用户）”选项卡，在左侧面板上点击“Add（添加）”。如果将系统日志解析筛选器配置为映射筛选器 ID（即角色），则只需将其添加到列表。在下面的例子中，筛选器 ID 是“ iot_stb”，其中 stb 代表“机顶盒”。请注意，包含大写字符的用户名将变为小写。因此，在策略中应该使用小写字符。

如果将系统日志解析筛选器配置为映射用户名，则需要在策略中列出每个用户名或者创建包含所有所需用户名的本地用户组。

图 19：用户 ID 策略



17. PAN：验证用户 ID 映射

用户映射可以使用命令“show user ip-user-mapping all（显示用户的全部 IP 映射）”通过 CLI 进行验证。请参考以下示例。您可以验证收到的用户名（或本例中的角色）是否以小写显示，尽管 OmniVista 中使用了大写。

图 20：验证用户 ID 映射

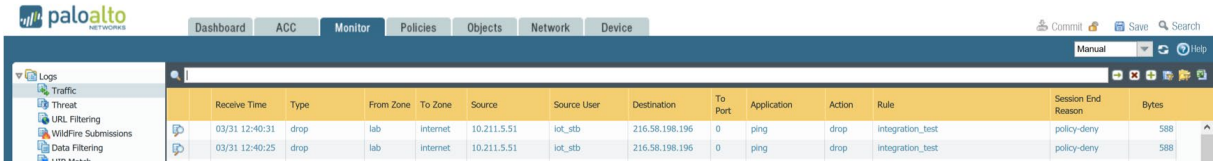
```
admin@PAN-1> show user ip-user-mapping all

IP              Vsys   From    User                             IdleTimeout(s) MaxTimeout(s)
--------------- ------ ------- -------------------------------- -------------- -------------
192.168.200.10  vsys1  GP      patricio                         2590970        2590970
10.211.5.51     vsys1  SYSLOG  iot_stb                          2644           2644
```

18. PAN：验证用户 ID 策略

为了验证防火墙策略是否正确识别用户，请进入“Monitor（监控）->Logs（日志）->Traffic（流量）”。根据需要配置筛选器。在下面的示例中，“integration_test（集成测试）”策略被配置为阻止“iot_stb”用户或角色的 ping。

图 21：验证用户 ID 策略



19. 结语

将 OmniVista UPAM 与 PAN 防火墙实施的零信任网络访问 (ZTNA) 协同应用方案，可以更好地了解有线和无线用户、设备以及他们所使用的资源和应用。这种集成只允许具有合法业务需求的用户和设备访问，从而实现了更精细的控制，减少了攻击面。凭借用户和设备信息，其日志记录和报告功能得到了增强。报告可以通过筛选特定用户、角色或设备的活动来改进，取证分析可以快速识别用户名或角色，而不仅仅是 IP 地址。