部署ISE安全评估

目录

[简介](#)

[限制](#)

[安全评估客户端行为](#)

[使用案例](#)

- [使用案例1 — 客户端重新身份验证强制NAD生成新的会话ID](#)
- [使用案例2 — 交换机配置有订单MAB DOT1X和优先级DOT1X MAB（有线）](#)
- [使用案例3 — 无线客户端漫游和不同AP的身份验证将转至不同的控制器](#)
- [使用案例4 — 具有负载均衡器的部署（Pre 2.6 Patch 6、2.7 Patch P2和3.0）](#)
- [使用案例5 — 第2阶段发现探测由经过身份验证的客户端以外的其他服务器响应（Pre 2.6 Patch 6、2.7 Patch 2和3.0）](#)

[2.6补丁6、2.7补丁2和3.0后的行为更改](#)

[维护相同SessionID时的注意事项](#)

简介

本文档介绍一些基本配置，这些配置通过基于重定向的安全状态解决多个使用案例。

限制

本文档中的配置适用于思科NAD，但不一定适用于第三方NAD。

安全评估客户端行为

状态客户端可以在以下时间触发探测：

- 初始登录
- 第3层(L3)更改/网络接口卡(NIC)更改（新IP地址、NIC状态更改）

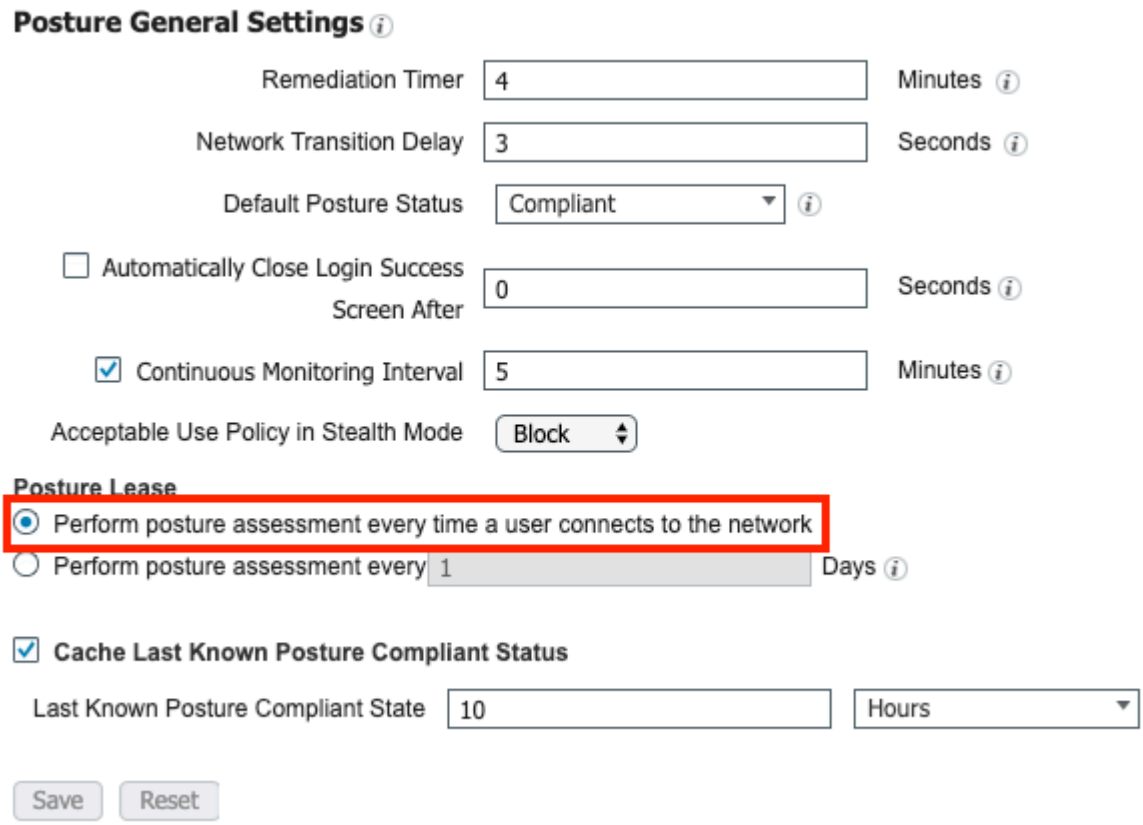
使用案例

使用案例1 — 客户端重新身份验证强制NAD生成新的会话ID

在此使用案例中，客户端仍然兼容，但由于重新身份验证，NAD处于重定向状态（重定向URL和访问列表）。

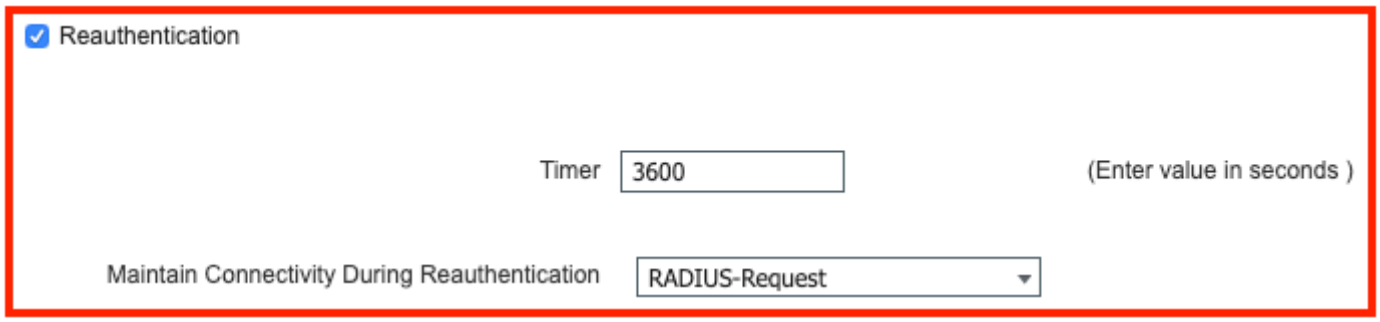
默认情况下，身份服务引擎(ISE)配置为在每次连接到网络时执行状态评估，更具体地说，是每个新会话。

此设置在Work Centers > Posture > Settings > Posture General Settings下配置。

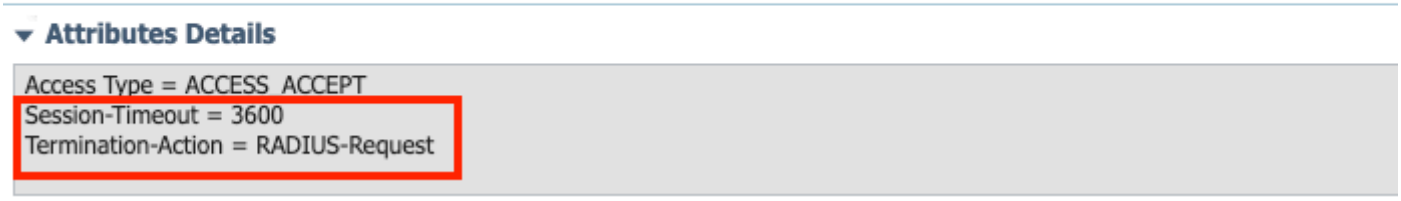


为了防止NAD在重新身份验证时生成新的会话ID，请在授权配置文件中配置这些重新身份验证值。显示的重新身份验证计时器不是标准建议，应根据连接类型（无线/有线）、设计（负载均衡器上的持久性规则是什么）等考虑每个部署的重新身份验证计时器。

Policy > Policy Elements > Results > Authorization > Authorization Profiles







在交换机上，您需要配置每个接口或模板，以便从ISE获取其重新身份验证计时器。

```
authentication timer reauthenticate server
```

注意：如果存在负载均衡器，您需要确保配置持久性，以使重新身份验证可以返回到原始策略服务(PSN)。

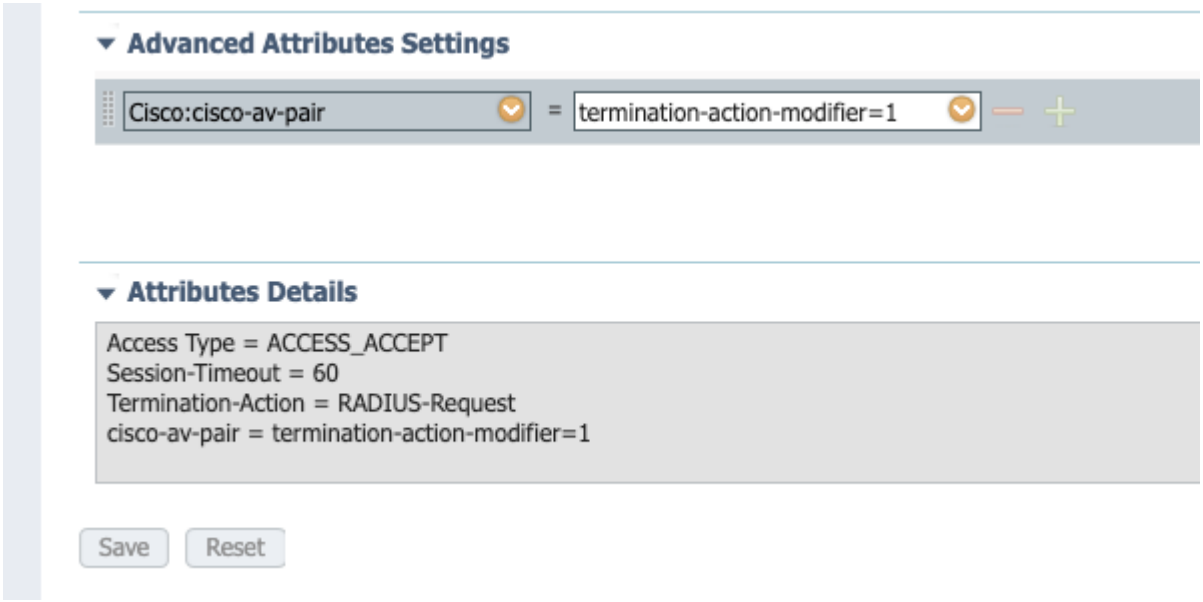
使用案例2 — 交换机配置有订单MAB DOT1X和优先级DOT1X MAB（有线）

在这种情况下，重新身份验证可以终止，因为在重新身份验证期间尝试MAC身份验证绕行(MAB)时，可以发送802.1x会话的记账停止。

- 当身份验证失败时，为MAB进程发送的记帐停止是正确的，因为客户端的用户名从802.1X用户名更改为MAB用户名。
- 记账停止时作为方法ID的Dot1x也是正确的，因为授权方法是dot1x。
- 当Dot1x方法成功时，它会发送一个记账开始，其中方法id为dot1x。此行为也符合预期。

要解决此问题，请在终端合规时使用的authZ配置文件中配置cisco-av-pair:termination-action-

modifier=1。此属性值(AV)对指定NAD重新使用在原始身份验证中选择的方法，而不考虑配置的顺序。



使用案例3 — 无线客户端漫游和不同AP的身份验证将转至不同的控制器

对于这种情况，需要设计无线网络，使处于可达范围的接入点(AP)能够漫游到其他AP，使用同一个主用控制器。一个示例是无线局域网控制器(WLC)状态化切换(SSO)故障切换。有关适用于WLC的高可用性(HA)SSO的详细信息，请参阅高可用性(SSO)部署指南。

使用案例4 — 具有负载均衡器的部署（Pre 2.6 Patch 6、2.7 Patch P2和3.0）

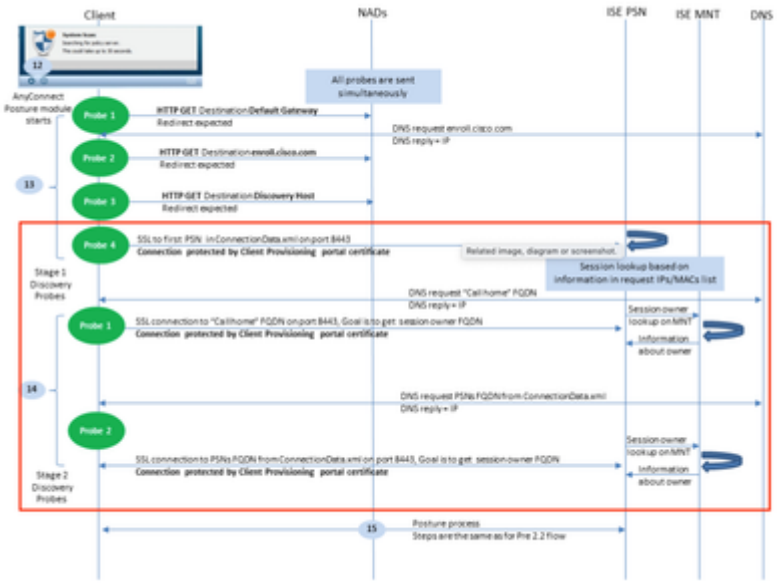
在涉及负载均衡器的部署中，必须确保在对之前的使用案例进行更改后，会话继续转到同一PSN。在此步骤列出的版本/修补程序之前，状态状态不会通过轻量数据分发（以前称为轻量会话目录）在节点之间复制。 因此，不同的PSN可能会返回不同的状态结果。

如果暂留配置不正确，重新进行身份验证的会话可能会转到与最初使用的PSN不同的PSN。如果发生这种情况，新PSN可以将会话合规性状态标记为未知，并使用重定向访问控制列表(ACL)/URL传递授权结果并限制终端访问。同样，状况模块不会识别此更改并且不会触发探测。

有关如何配置负载均衡器的详细信息，请参阅Cisco & F5部署指南：使用BIG-IP的ISE负载均衡。它提供负载平衡环境中ISE部署的最佳实践设计的高级概述和F5特定配置。

使用案例5 — 第2阶段发现探测由经过身份验证的客户端以外的其他服务器响应（Pre 2.6 Patch 6、2.7 Patch 2和3.0）

请查看此图中的红色框中的探测器。



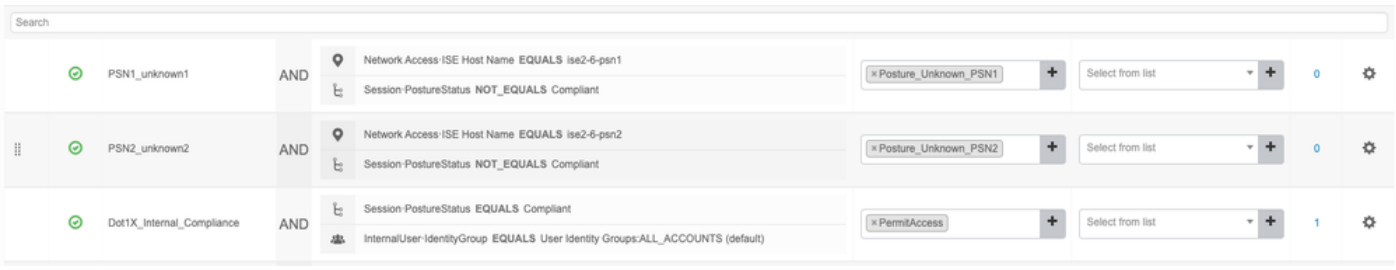
PSN存储会话数据五天，因此，即使客户端不再使用该节点进行身份验证，合规会话的会话数据有时仍会保留在原始PSN上。如果在红色框中包含的探测由当前验证会话的PSN以外的其他PSN响应，并且PSN先前拥有并标记了此终端兼容，则终端上的终端安全评估模块的状态与当前验证PSN之间可能存在不匹配。

以下是可能发生这种不匹配的几种常见情况：

- 当终端从网络断开时，不会收到该终端的记账停止。
- NAD从一个PSN故障切换到另一个PSN。
- 负载均衡器将身份验证转发到同一端点的不同PSN。

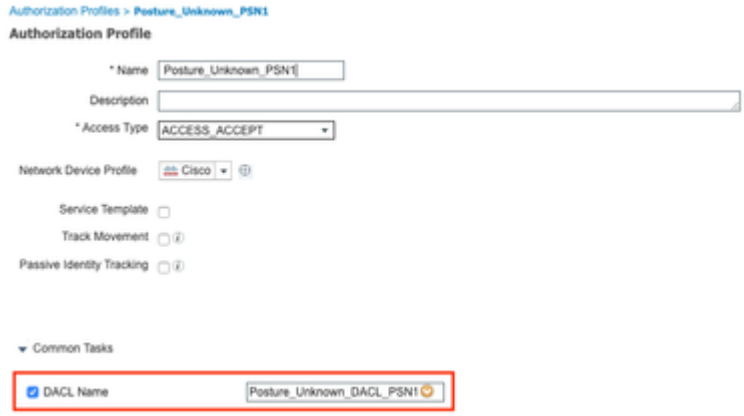
为了防止此行为，可以将ISE配置为仅允许来自特定终端的发现探针访问其当前身份验证到的PSN。为此，请为部署中的每个PSN配置不同的授权策略。在这些策略中，引用包含可下载访问控制列表(DACL)的其他authZ配置文件，该DACL仅允许对authZ条件中指定的PSN进行探测。请参阅以下示例：

每个PSN都有一个未知状态规则：

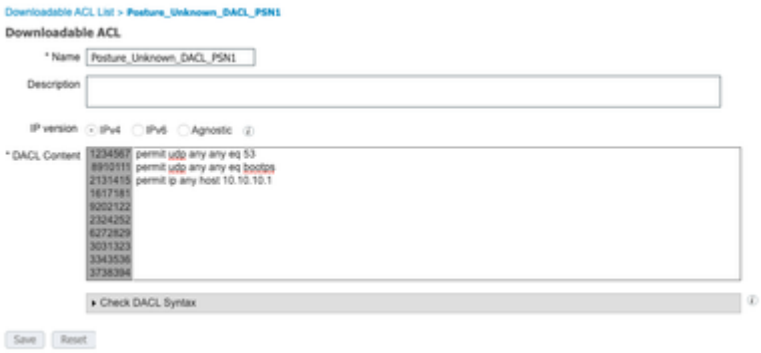


每个配置文件引用不同的DACL。

> 注意：对于无线，请使用Airespace ACL。



每个DACL仅允许对处理身份验证的PSN进行探测访问。



在上一个示例中，10.10.10.1是PSN 1的IP地址。可以根据需要为任何其他服务/IP更改所引用的DACL，但仅限制对处理身份验证的PSN的访问。

2.6补丁6、2.7补丁2和3.0后的行为更改

状态已通过光数据分发框架添加到RADIUS会话目录。每次在任何PSN上收到终端安全评估状态更新时，都会将其复制到部署中的所有PSN。此更改生效后，到达不同身份验证上的不同PSN的身份验证和/或探测功能的影响将被删除，任何PSN都可以回复所有终端，无论它们当前在何处进行身份验证。

在本文档的五个使用案例中，请考虑以下行为：

使用案例1 — 客户端重新身份验证会强制NAD生成新的会话ID。客户端仍然兼容，但由于重新身份

验证，NAD处于重定向状态（重定向URL和访问列表）。

— 此行为不会改变，此配置仍可在ISE和NAD上实施。

使用案例2 — 交换机配置有顺序MAB DOT1X和优先级DOT1X MAB（有线）。

— 此行为不会改变，此配置仍可在ISE和NAD上实施。

使用案例3 — 无线客户端漫游，不同AP的身份验证将转至不同的控制器。

— 此行为不会改变，此配置仍可在ISE和NAD上实施。

使用案例4 — 具有负载均衡器的部署。

— 仍然可以遵循负载均衡指南中定义的最佳实践，但如果负载均衡器将身份验证转发到不同的PSN，则客户端可以返回正确的状态状态。

使用案例5 — 第2阶段发现探测由不同的服务器响应，而不是使用进行身份验证的客户端

— 这不能是新行为的问题，每个PSN授权配置文件是不必要的。

维护相同SessionID时的注意事项

当您使用本文档中列出的方法时，保持网络连接的用户可能会长时间保持合规性。即使他们重新进行身份验证，会话ID也不会更改，因此ISE继续传递其规则与合规状态匹配的授权结果。

在这种情况下，需要配置Periodic Reassessment，以便要求终端安全评估确保终端在定义的间隔内保持符合公司策略。

这可以在工作中心>状态>设置>重新评估配置下配置。



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）。