

ISE终端安全评估部署最佳实践和注意事项

目录

[简介](#)

[限制](#)

[状态客户端行为](#)

[使用案例](#)

[使用案例1 — 客户端重新身份验证强制NAD生成新会话ID。](#)

[使用案例2 — 交换机配置了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的身份验证将发往不同的控制器。](#)

[使用案例4 — 使用负载均衡器 \(2.6之前版本的补丁6、2.7补丁P2和3.0 \) 进行部署。](#)

[使用案例5 — 第2阶段发现探测功能由不同的服务器响应，而客户端则使用 \(2.6版补丁6、2.7版补丁2和3.0版 \) 进行身份验证。](#)

[2.6版补丁6、2.7版补丁2和3.0版后的行为更改](#)

[维护相同会话ID时的注意事项](#)

简介

本文档介绍一些基线配置，这些配置通过基于重定向的状态解决多个使用案例。在这些配置中，客户端保持合规，但网络访问设备(NAD)会限制访问，因为它处于重定向状态。

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。

状态客户端行为

终端安全评估客户端将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生成新会话ID。

在此使用案例中，客户端仍兼容，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，尤其是针对每个新会话。

此设置在工作中心(Work Centers)>状态(Posture)>设置(Settings)>状态常规设置(Posture General Settings)下配置。

Posture General Settings ?

Remediation Timer Minutes ?

Network Transition Delay Seconds ?

Default Posture Status ?

Automatically Close Login Success Screen After Seconds ?

Continuous Monitoring Interval Minutes ?

Acceptable Use Policy in Stealth Mode

Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every Days ?

Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

Save

Reset

为了防止NAD在重新身份验证时生成新会话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。

策略>策略元素>结果>授权>授权配置文件

Reauthentication

Timer (Enter value in seconds)

Maintain Connectivity During Reauthentication

▼ Advanced Attributes Settings

Select an item = - +

▼ Attributes Details

Access Type = ACCESS_ACCEPT

Session-Timeout = 3600

Termination-Action = RADIUS-Request

在交换机上，您需要配置每个接口或模板，以从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，您需要确保以重新身份验证将返回原始策略服务(PSN)的方式配置持久性。

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

在这种情况下，重新身份验证将终止，因为在重新身份验证期间尝试MAC身份验证绕行(MAB)时，将发送802.1x会话的记帐停止。

- 当MAB进程身份验证失败时为其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。
- 记帐停止中的method-id为dot1x的授权方法也正确。
- 当Dot1x方法成功时，它会发送一个记帐开始，其中method-id为dot1x。在这里，这种行为也符合预期。

要解决此问题，请在终端兼容时使用的authZ配置文件上配置cisco-av-pair:termination-action-modifier = 1。此属性值(AV)对指定NAD应重用原始身份验证中选择的方法，而不管配置的顺序如何。

Advanced Attributes Settings

Cisco:cisco-av-pair = termination-action-modifier=1

Attributes Details

Access Type = ACCESS_ACCEPT
Session-Timeout = 60
Termination-Action = RADIUS-Request
cisco-av-pair = termination-action-modifier=1

Save

Reset

使用案例3 — 无线客户端漫游和不同AP的身份验证将发往不同的控制器。

在这种情况下，需要设计无线网络，使其中的接入点(AP)可以到达其他AP进行漫游，并使用相同的主用控制器。无线局域网控制器(WLC)状态切换(SSO)故障切换就是一个例子。有关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 — 使用负载均衡器 (2.6之前版本的补丁6、2.7补丁P2和3.0) 进行部署。

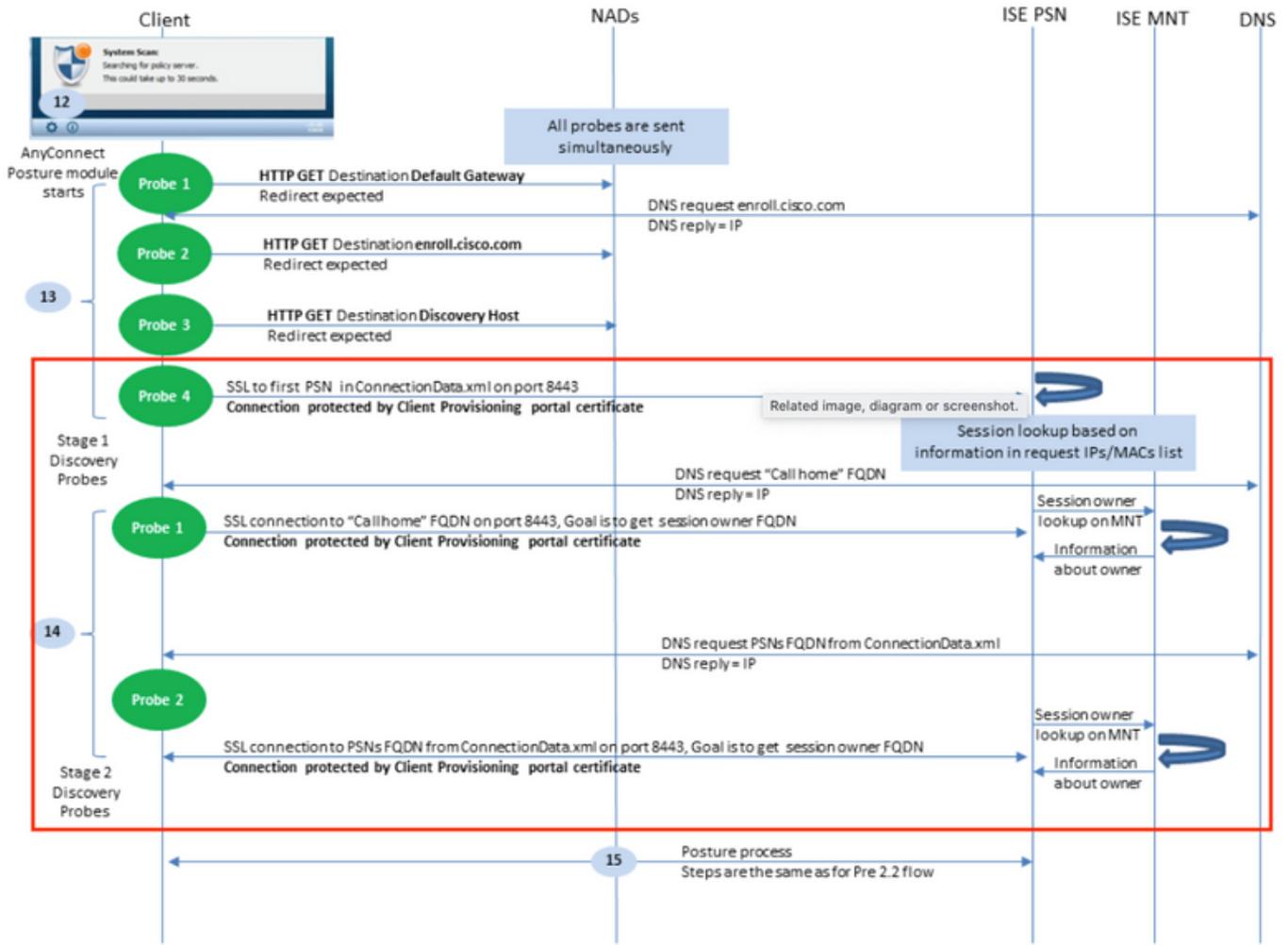
在涉及负载均衡器的部署中，必须确保在您对以前的使用案例进行更改后，会话继续转到相同的PSN。在此步骤中列出的版本/补丁之前，状态不会通过轻量数据分发 (以前称为轻量会话目录) 在节点之间复制。因此，不同PSN可以返回不同的状态结果。

如果持久性配置不正确，则重新进行身份验证的会话可能会转到与最初使用的会话不同的PSN。如果发生这种情况，新PSN可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，终端安全评估模块无法识别NAD上的此更改，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](#)。它提供高级概述和F5特定配置，以在负载均衡环境中为ISE部署提供最佳实践设计。

使用案例5 — 第2阶段发现探测功能由不同的服务器响应，而客户端则使用 (2.6版补丁6、2.7版补丁2和3.0版) 进行身份验证。

查看此图中红色框中的探测器。



PSN将会存储5天的会话数据，因此有时，“兼容”会话的会话数据仍在原始PSN上，即使客户端不再与该节点进行身份验证也是如此。如果红框中包含的探测器由PSN响应，而不是当前对会话进行身份验证的PSN，并且PSN以前拥有并标记此终端兼容的PSN，则终端上的终端安全评估模块的状态与当前的身份验证PSN之间可能存在不匹配。

以下是可能出现这种不匹配的几种常见情况：

- 终端断开网络时，不会收到终端的记帐停止。
- 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终端的不同PSN。

为防止此行为，ISE可配置为仅允许来自特定终端的发现探测到其当前进行身份验证的PSN。要实现此目的，请为部署中的每个PSN配置不同的授权策略。在这些策略中，请引用包含可下载访问控制列表(DACL)的其他授权配置文件，该列表仅允许探测到授权条件中指定的PSN。请参阅以下示例：

每个PSN将具有未知状态的规则：

Search	AND	Network Access-ISE Host Name EQUALS ise2-6-psn1	Posture_Unknown_PSN1	Select from list	0	⚙️
PSN1_unknown1	AND	Session-PostureStatus NOT_EQUALS Compliant				
PSN2_unknown2	AND	Network Access-ISE Host Name EQUALS ise2-6-psn2	Posture_Unknown_PSN2	Select from list	0	⚙️
		Session-PostureStatus NOT_EQUALS Compliant				
Dot1X_Internal_Compliance	AND	Session-PostureStatus EQUALS Compliant	PermitAccess	Select from list	1	⚙️
		InternalUser-IdentityGroup EQUALS User Identity Groups:ALL_ACCOUNTS (default)				

每个配置文件都引用不同的DAACL。

注意：对于无线，请使用Airespace ACL。

[Authorization Profiles > Posture_Unknown_PSN1](#)

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

每个DAACL仅允许对处理身份验证的PSN进行探测访问。

[Downloadable ACL List > Posture_Unknown_DACL_PSN1](#)

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic

* DACL Content

1234567	permit udp any any eq 53
8910111	permit udp any any eq bootps
2131415	permit ip any host 10.10.10.1
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

在上一个示例中，10.10.10.1是PSN 1的IP地址。可以根据需要更改所引用的DAACL，但应仅限访问处理身份验证的PSN。

2.6版补丁6、2.7版补丁2和3.0版后的行为更改

状态已通过轻量数据分发框架添加到RADIUS会话目录。每次在任何PSN上收到状态更新时，都会

将其复制到部署中的所有PSN。一旦此更改生效，将删除在不同身份验证上到达不同PSN的身份验证和或探测的影响，任何PSN都应能够回复所有终端，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强制NAD生成新会话ID。客户端仍兼容，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）。

— 此行为不会更改，此配置仍应在ISE和NAD上实施。

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

— 此行为不会更改，此配置仍应在ISE和NAD上实施。

使用案例3 — 无线客户端漫游和不同AP的身份验证将发往不同的控制器。

— 此行为不会更改，此配置仍应在ISE和NAD上实施。

使用案例4 — 使用负载均衡器进行部署。

— 仍应遵循负载均衡指南中定义的最佳实践，但是，如果负载均衡器将身份验证转发到不同的PSN，则应将正确的状态返回给客户端。

使用案例5 — 第2阶段发现探测由不同的服务器响应，而客户端使用身份验证

— 这不应是新行为的问题，并且不需要每PSN授权配置文件。

维护相同会话ID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期保持合规。即使它们重新进行身份验证，会话ID也不会更改，因此ISE将继续为其符合合规状态的规则传递授权结果。

在这种情况下，需要配置定期重新评估，以便需要安全评估，以确保终端在定义的时间间隔内保持符合公司策略。

这可以在工作中心(Work Centers)>状态(Posture)>设置(Settings)>重新评估(Ressment)配置下配置。

