

比较ISE终端安全评估重定向流与ISE终端安全评估无重定向流

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[ISE 2.2之前的终端安全评估流量](#)

[ISE 2.2之后的终端安全评估流程](#)

[配置](#)

[网络图](#)

[配置](#)

[客户端调配配置](#)

[安全评估策略和条件](#)

[配置客户端调配门户](#)

[配置授权配置文件和策略](#)

[验证](#)

[故障排除](#)

[一般信息](#)

[常见问题故障排除](#)

[SSO相关问题](#)

[客户端调配策略选择故障排除](#)

[状态流程故障排除](#)

简介

本文档介绍ISE 2.2及更高版本中支持的状态无重定向流与自更早的ISE版本以来支持的状态重定向流的比较。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE上的终端安全评估流程
- 在ISE上配置终端安全评估组件
- 用于虚拟专用网络(VPN)安全状态的自适应安全设备(ASA)配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本2.2
- 带软件9.6(2)的Cisco ASA v


本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍身份服务引擎(ISE)2.2中引入的一项新功能，该功能允许ISE支持安全评估流程，而无需在网络访问设备(NAD)或ISE上支持任何类型的重定向。

终端安全评估是Cisco ISE的核心组件。作为组件的状态可以用三个主要元素表示：

1. ISE作为策略配置分发和决策点。
从ISE的管理员角度，您可以配置终端安全评估策略（必须将设备标记为符合公司要求的确切条件）、客户端调配策略（必须在哪种类型的设备上安装哪种代理软件）和授权策略（必须分配哪种类型的权限，取决于其终端安全评估状态）。
2. 作为策略实施点的网络接入设备。
在NAD端，在用户身份验证时应用实际授权限制。作为策略点的ISE提供授权参数，如已下载ACL(dACL)/VLAN/重定向URL/重定向访问控制列表(ACL)。传统上，为了进行终端安全评估，需要NAD支持重定向（指示必须联系哪个ISE节点的用户或代理软件）和授权更改（CoA），以在终端安全评估状态确定后重新验证用户。
3. 代理软件，作为数据收集和与最终用户交互的点。
Cisco ISE使用三种类型的代理软件：AnyConnect ISE终端安全评估模块、NAC代理和Web代理。代理从ISE接收有关安全评估要求的信息，并向ISE提供要求状态报告。

 注意：本文档基于Anyconnect ISE终端安全评估模块，这是唯一一个完全支持终端安全评估而不重定向的模块。

在ISE 2.2之前的流量安全评估中，NAD不仅用于验证用户和限制访问，还用于向代理软件提供有关必须联系的特定ISE节点的信息。在重定向过程中，有关ISE节点的信息会返回到代理软件。

过去，NAD或ISE端重定向支持是终端安全评估实施的基本要求。在ISE 2.2中，初始客户端调配和安全评估流程不再需要支持重定向。

无重定向的客户端调配 — 在ISE 2.2中，您可以通过门户完全限定域名(FQDN)访问客户端调配门户(CPP)。这与访问发起人门户或MyDevice门户的方式类似。

无重定向的安全评估流程 — 代理安装期间，从CPP门户保存有关ISE服务器的信息在客户端，使直

接通信成为可能。

ISE 2.2之前的终端安全评估流量

此图显示了ISE 2.2之前的Anyconnect ISE终端安全评估模块流的逐步说明：

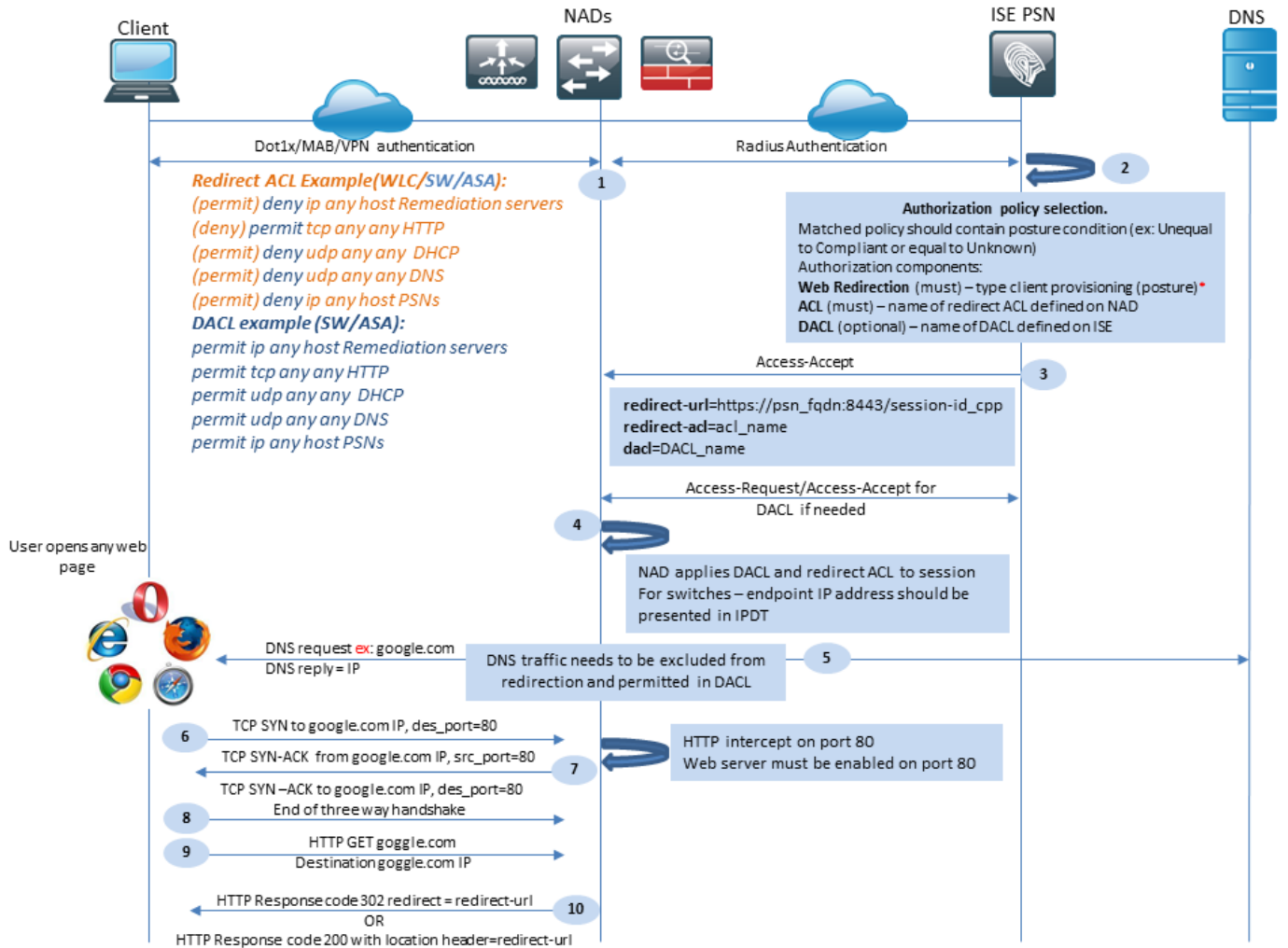


图 1-1

步骤1:身份验证是流程的第一步，可以是dot1x、MAB或VPN。

第二步：ISE需要为用户选择身份验证和授权策略。在安全评估情景中，所选授权策略必须包含对安全评估状态的引用，该引用最初必须为未知或不适用。要同时涵盖这两种情况，可以使用状况状态为不等合规性的条件。

所选授权配置文件必须包含有关重定向的信息：

- Web Redirection — 对于终端安全评估案例，必须将网络重定向类型指定为客户端调配（终端安全评估）。
- ACL — 本部分需要包含在NAD端配置的ACL名称。此ACL用于指示NAD哪些流量必须绕过重定向，哪些流量必须实际重定向。
- DACL — 它可以与重定向访问列表一起使用，但您必须记住，不同的平台以不同的顺序处理

DAACL和重定向ACL。

例如，ASA在重定向ACL之前始终会处理DAACL。同时，某些交换机平台处理流量的方式与ASA相同，而其他交换机平台首先处理重定向ACL，然后在必须丢弃或允许流量时检查DAACL/接口ACL。

 注意：在授权配置文件中启用Web重定向选项后，必须选择重定向的目标门户。

第三步：ISE返回具有授权属性的Access-Accept。授权属性中的重定向URL由ISE自动生成。它包含以下组件：

- 进行身份验证的ISE节点的FQDN。在某些情况下，动态FQDN可能会被Web重定向部分中的授权配置文件配置（静态IP/主机名/FQDN）覆盖。如果使用静态值，则必须指向处理身份验证的同一ISE节点。对于负载均衡器(LB)，此FQDN可以指向LB VIP，但仅当LB配置为将Radius和SSL连接结合在一起时。
- 端口 — 端口值从目标门户配置获取。
- Session ID — 此值由ISE从Access-Request中提供的Cisco AV对审核会话ID获取。值本身由NAD动态生成。
- 门户ID - ISE端上的目标门户的标识符。

第四步：NAD向会话应用授权策略。此外，如果配置了DAACL，则在应用授权策略之前请求其内容。

重要注意事项：

- 所有NAD — 设备必须具有本地配置的ACL，其名称必须与Access-Accept as redirect-acl中接收的ACL的名称相同。
- 交换机 — 客户端的IP地址必须显示在 `show authentication session interface details` 命令成功应用重定向和ACL。客户端IP地址通过IP设备跟踪功能(IPDT)获取。

第五步：客户端发送DNS请求，请求输入到Web浏览器中的FQDN。在此阶段，DNS流量必须绕过重定向，DNS服务器必须返回正确的IP地址。

第六步：客户端将TCP SYN发送到DNS应答中收到的IP地址。数据包中的源IP地址是客户端IP，而目的IP地址是所请求资源的IP。目标端口等于80，但在客户端Web浏览器中配置直接HTTP代理的情况除外。

第7.NAD拦截客户端请求并准备SYN-ACK数据包，其中源IP等于请求的资源IP，目标IP等于客户端IP，源端口等于80。

重要注意事项：

- NAD必须在客户端发送请求的端口上运行HTTP服务器。默认情况下，它是端口80。
- 如果客户端使用直接HTTP代理Web服务器，则HTTP服务器必须在NAS上的代理端口上运行。此场景不在本文档的讨论范围之内。
- 如果NAD在客户端中没有本地IP地址，则子网SYN-ACK将与NAD路由表一起发送（通常通过管理接口）。在此场景中，数据包通过L3基础设施路由，并且必须通过L3上游设备路由回客

户端。如果L3设备是有状态防火墙，则必须为此类非对称路由提供额外的例外情况。

步骤 8 客户端通过ACK完成TCP三次握手。

步骤 9 客户端发送目标资源的HTTP GET。

步骤 10 NAD将重定向URL返回到HTTP代码为302的客户端（页面已移动），某些NAD重定向可以在位置报头的HTTP 200 OK消息内返回。

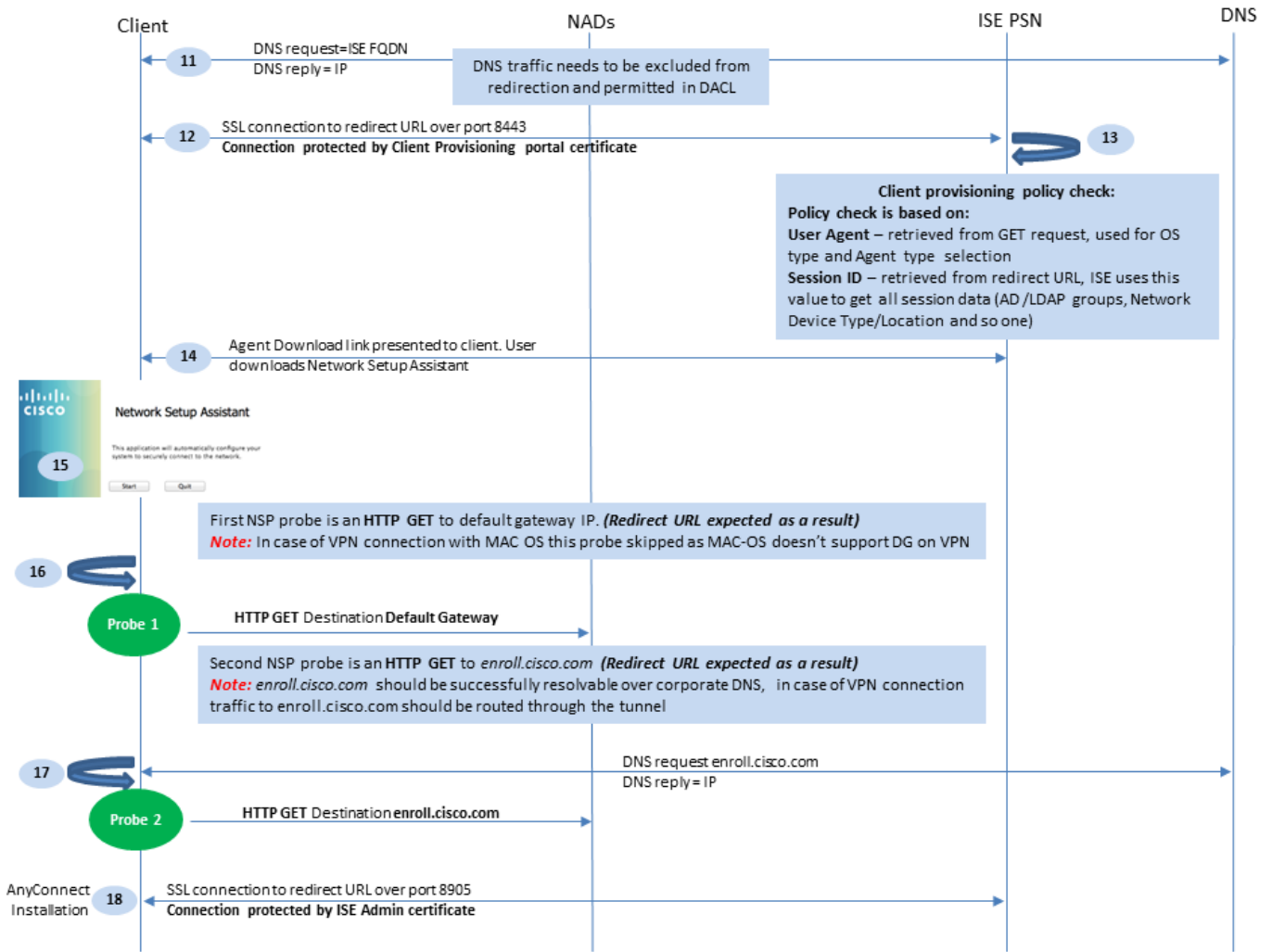


图 1-2

步骤 11 客户端从重定向URL发送FQDN的DNS请求。FQDN必须在DNS服务器端可解析。

步骤 12 通过重定向URL中接收的端口建立SSL连接（默认8443）。此连接受来自ISE端的门户证书保护。向用户显示客户端调配门户(CPP)。


第13步：在为客户端提供下载选项之前，ISE必须选择目标客户端调配(CP)策略。从身份验证会话（如AD/LDAP组等）检索从浏览器用户代理检测到的客户端的操作系统(OS)以及CPP策略选择所需的其他信息。ISE通过重定向URL中显示的会话ID了解目标会话。

步骤 14 网络设置助理(NSA)下载链接返回到客户端。客户端下载应用。

 注意：通常您可以将NSA视为Windows和Android自带设备流的一部分，但也可以使用此应用程序从ISE安装Anyconnect或其组件。

步骤15.用户运行NSA应用。

步骤 16 NSA将第一个发现探测 — HTTP /auth/discovery发送到默认网关。因此，NSA预计会重定向URL。

 注意：对于MAC OS设备上的VPN连接，此探测功能将被忽略，因为MAC OS在VPN适配器上没有默认网关。

步骤17.如果第一个探测功能失败，NSA将发送第二个探测。第二个探测功能是HTTP GET /auth/discovery enroll.cisco.com. 此FQDN必须能由DNS服务器成功解析。在使用分割隧道的VPN场景中，流量发送到 enroll.cisco.com 必须通过隧道路由。

步骤 18. 如果任何探测成功，NSA会使用从redirect-url获取的信息通过端口8905建立SSL连接。此连接受ISE管理员证书保护。在此连接内，NSA下载Anyconnect。

重要注意事项：

- 在ISE 2.2版本之前，通过端口8905进行SSL通信是安全评估的一项要求。
- 为了避免证书警告，客户端必须信任门户和管理员证书。
- 在多接口ISE部署中，除G0外的接口可以绑定到FQDN，与系统FQDN不同(使用 ip host CLI命令)。这会导致主题名称(SN)/主题备用名称(SAN)验证出现问题。例如，如果客户端从接口G1重定向到FQDN，则系统FQDN可以不同于8905通信证书的重定向URL中的FQDN。作为此方案的解决方案，您可以在管理员证书SAN字段中添加其他接口的FQDN，也可以在管理员证书中使用通配符。

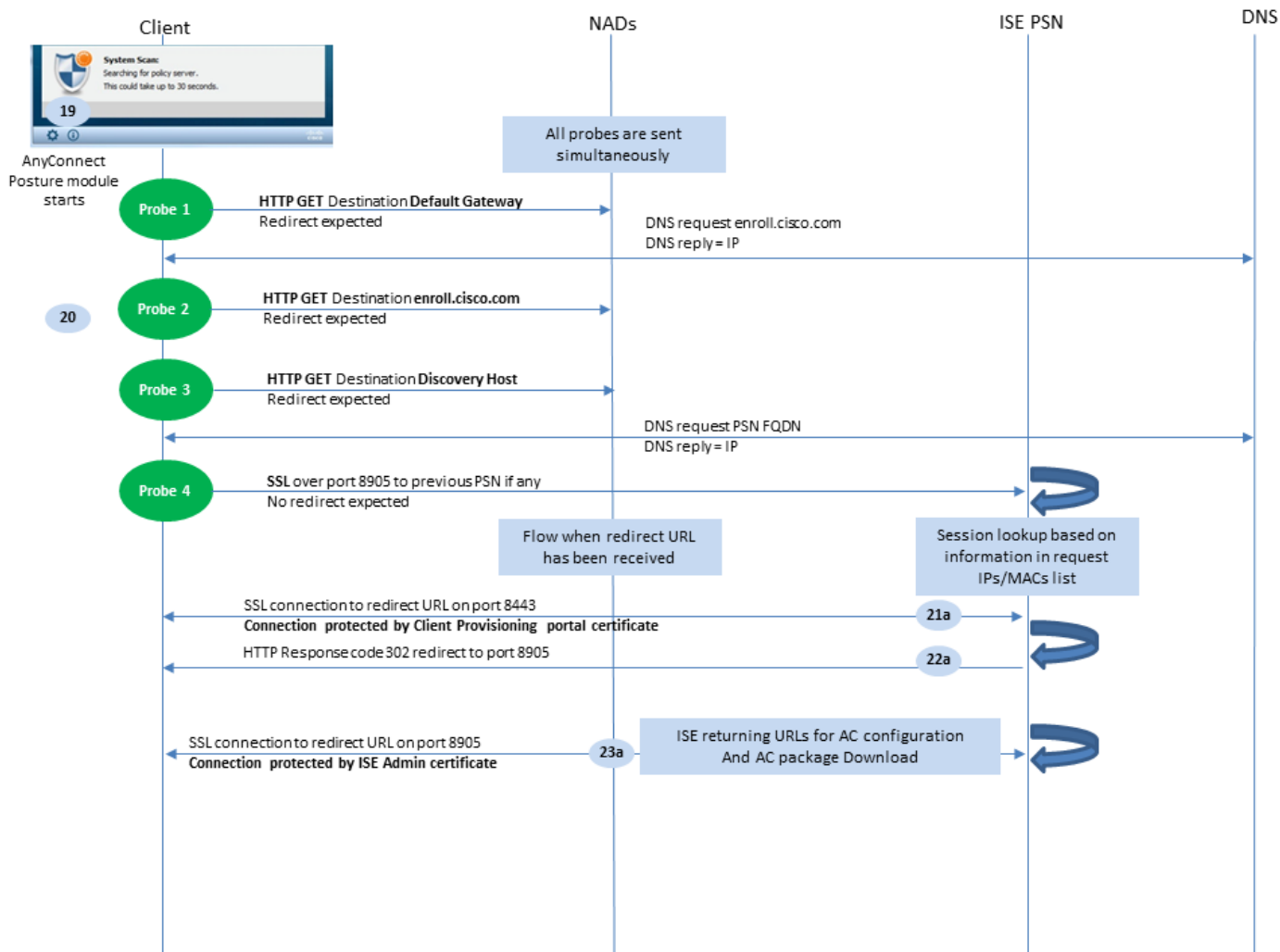


图 1-3

第19步：启动Anyconnect ISE终端安全评估流程。

Anyconnect ISE终端安全评估模块在以下任一情况下启动：

- 安装后
- 默认网关值更改后
- 在系统用户登录事件之后
- 系统电源事件后

步骤 20. 在此阶段，Anyconnect ISE终端安全评估模块启动策略服务器检测。这通过一系列同时由Anyconnect ISE终端安全评估模块发送的探测实现。

- 探测1 - HTTP获取/auth/discovery到默认网关IP。必须记住，MAC OS设备在VPN适配器上没有默认网关。探测的预期结果为redirect-url。
- 探测2 - HTTP GET /auth/discovery到 enroll.cisco.com. 此FQDN需要由DNS服务器成功解析。在使用分割隧道的VPN场景中，流量发送到 enroll.cisco.com 必须通过隧道路由。探测的预期结果为redirect-url。
- 探测3 — 将/auth/discovery发送到发现主机。在AC终端安全评估配置文件中安装时，会从ISE返回发现主机值。探测的预期结果为redirect-url。
- 探测4 — 通过SSL将端口8905上的HTTP GET /auth/status发送到先前连接的PSN。此请求包

含有关在ISE端进行会话查找的客户端IP和MAC列表的信息。此问题在第一次状态尝试期间不会出现。连接受ISE管理员证书保护。由于此探测，如果探测器着陆的节点与用户已经过身份验证的节点相同，则ISE可以将会话ID返回给客户端。

注意：由于此探测，即使在某些情况下没有工作重定向，也可以成功完成安全评估。无重定向的成功状况要求验证会话的当前PSN必须与之前成功连接的PSN相同。请记住，在ISE 2.2之前，无重定向的成功终端安全评估不是规则，而是例外。

以下步骤说明在由于其中一个探测功能而收到重定向URL（以字母a标记的流）时的状态过程。

步骤 21. Anyconnect ISE终端安全评估模块使用发现阶段检索的URL建立到客户端调配门户的连接。在此阶段，ISE使用来自自己身份验证会话的信息再次进行客户端调配策略验证。

第22步：如果检测到客户端调配策略，ISE将返回重定向到端口8905。

步骤 23. 代理通过端口8905与ISE建立连接。在此连接期间，ISE返回状态配置文件、合规性模块和anyconnect更新的URL。

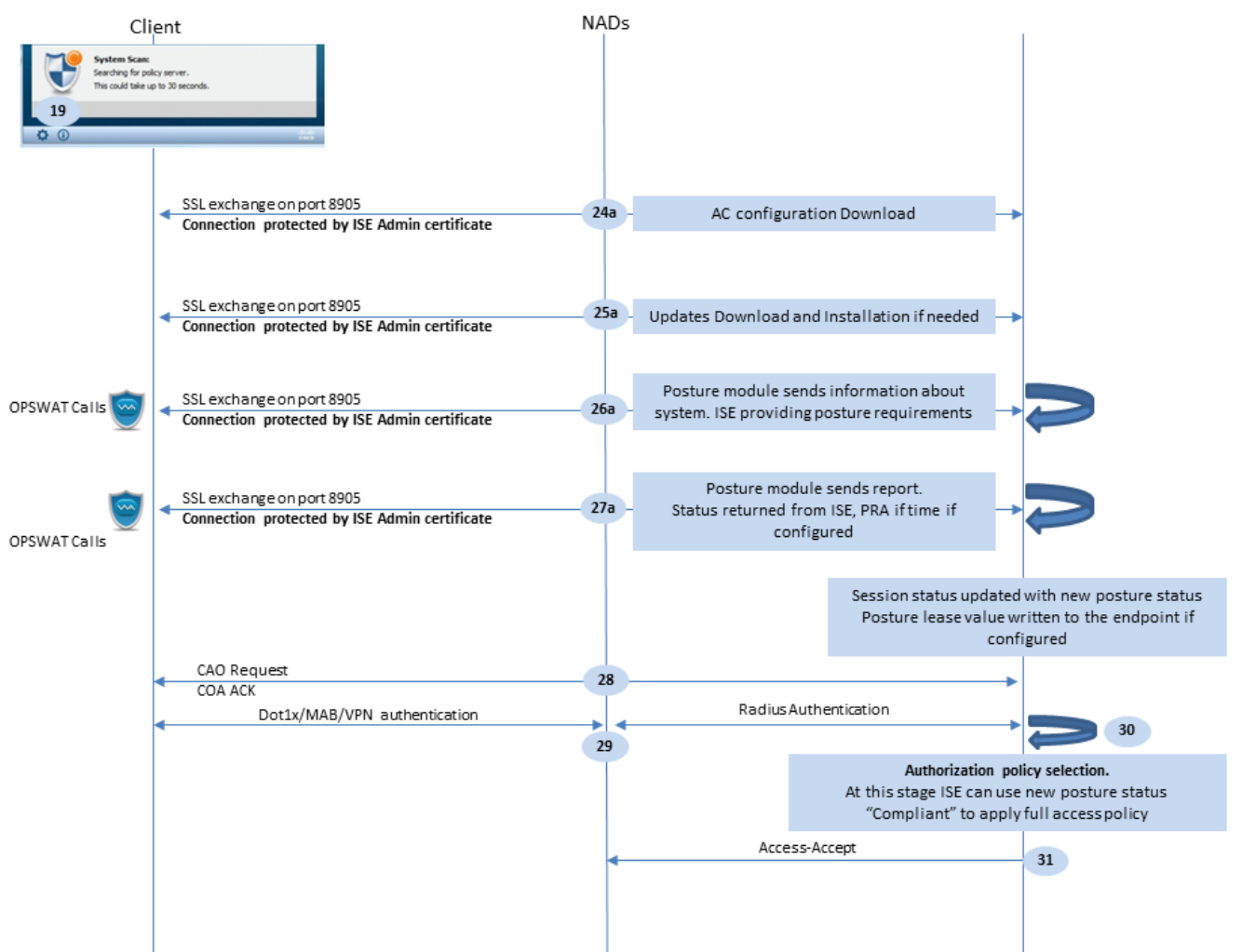


图1-4

第24步：从ISE下载AC ISE终端安全评估模块配置。

第25步：如有需要，更新下载和安装。

步骤 26 AC ISE终端安全评估模块收集有关系统的初始信息（如操作系统版本、已安装的安全产品及其定义版本）。在此阶段，AC ISE终端安全评估模块涉及OPSWAT API，用于收集有关安全产品的信息。收集的数据将发送到ISE。作为对此请求的回复，ISE提供安全评估要求列表。由于状态策略处理，需求列表被选定。要匹配正确的策略，ISE使用设备操作系统版本（存在于请求中）和会话ID值选择其他所需的属性（AD/LDAP组）。会话ID值也由客户端发送。

步骤 27在此步骤中，客户端涉及OPSWAT呼叫和其他机制来检查状况要求。包含要求列表及其状态的最终报告将发送到ISE。ISE需要对终端合规性状态做出最终决定。如果终端在此步骤中标记为不合规，将返回一组补救操作。对于合规终端，ISE将合规状态写入会话，并且如果配置了终端安全评估租用，ISE会将最后一个终端安全评估时间戳设置为终端属性。终端安全评估结果将发送回终端。在状况重新评估(PRA)情况下，PRA的时间也由ISE放入此数据包。

在不符合的情形中，请考虑以下几点：

- 某些补救操作（如显示文本消息、链接补救、文件补救等）由状况代理本身执行。
- 其他补救类型(例如AV、AS、WSUS和SCCM)要求终端安全评估代理和目标产品之间进行OPSWAT API通信。在此场景中，终端安全评估代理仅向产品发送补救请求。补救本身由安全产品直接完成。



注意：当安全产品必须与外部资源（内部/外部更新服务器）通信时，必须确保重定向ACL/DACL中允许此通信。

第28步：ISE向NAD发送COA请求，NAD必须为用户触发新的身份验证。NAD必须通过COA ACK确认此请求。请记住，对于VPN案例，使用COA推送，因此不会发送新的身份验证请求。相反，ASA会从会话中删除之前的授权参数（重定向URL、重定向ACL和DACL），并从COA请求应用新参数。

步骤29.用户的新身份验证请求。

重要注意事项：

- 通常，对于思科NAD COA，ISE使用重新身份验证，这指示NAD使用之前的会话ID发起新的身份验证请求。
- 在ISE端，相同的会话ID值表示必须重复使用之前收集的会话属性（在本例中为complaint status），并且必须分配基于这些属性的新授权配置文件。
- 如果会话ID发生更改，此连接将被视为新连接，并重新启动整个终端安全评估流程。
- 为了避免重新设置安全状态，每次会话id更改时，都可以使用状态租用。在此方案中，即使会话ID为，终端属性中仍存储有关终端安全评估状态的信息，该终端属性保存在ISE上ts已更改。

步骤 30 ISE端会根据安全评估状态选择新的授权策略。

步骤 31 具有新授权属性的Access-Accept将发送到NAD。

下一个流程描述了以下场景：任何终端安全评估探测未检索重定向URL（用字母b标记），并且之前连接的PSN已由最后一个探测查询。此处的所有步骤与重定向URL的情况完全相同，只不过重播由PSN作为探测4的结果而返回。如果此探测功能位于当前身份验证会话的所有者的同一PSN上，则重播包含会话ID值，该值（稍后将由状态代理用于完成该进程）。如果之前连接的前端与当前会话所有者不同，会话查找会失败，并且空响应返回到AC ISE终端安全评估模块。最终，No Policy Server Detected 将消息返回给最终用户。

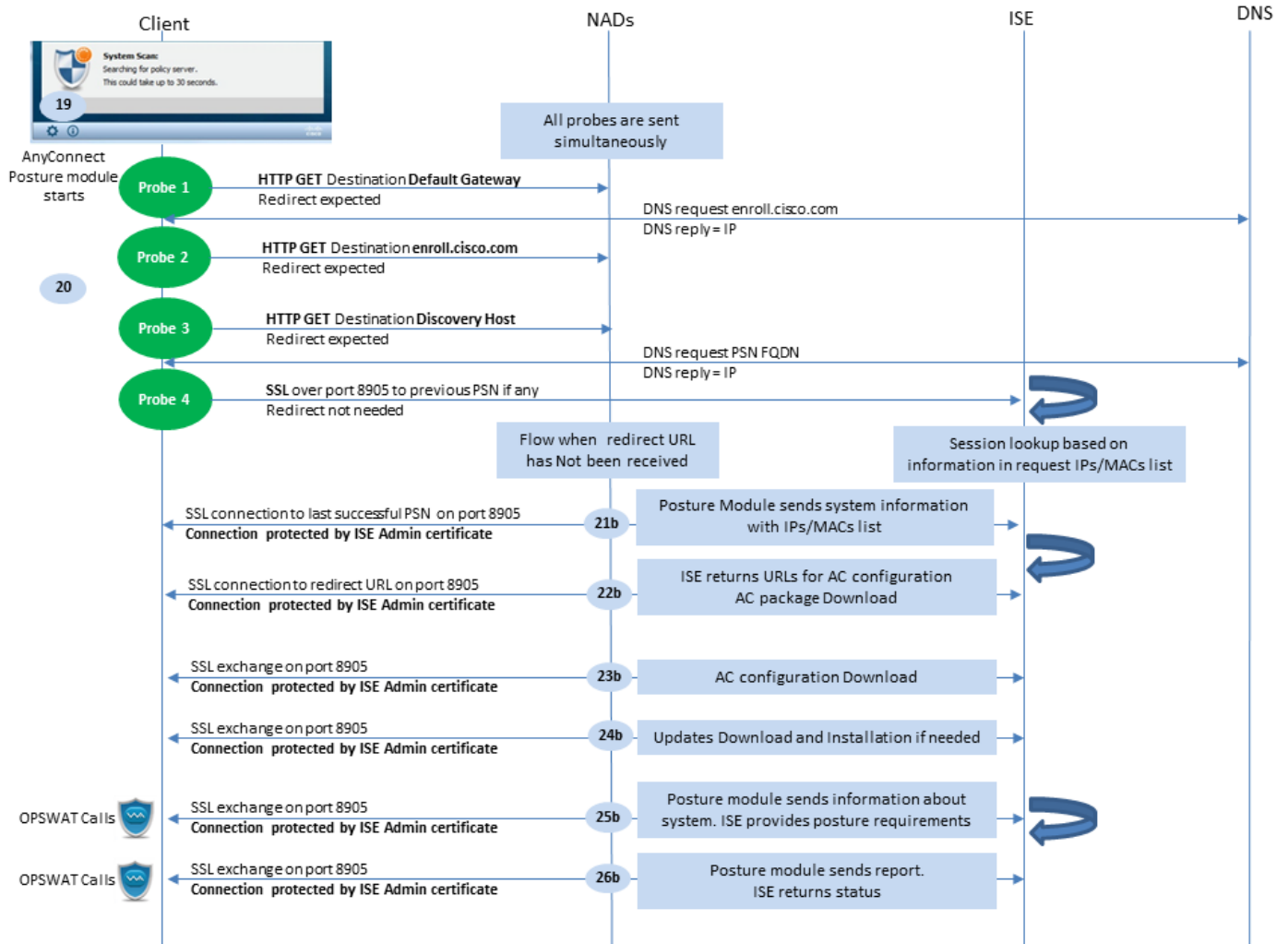


图 1-5

ISE 2.2之后的终端安全评估流程

ISE 2.2及更高版本同时支持重定向和无重定向流。 以下是无重定向状态流的详细解释：

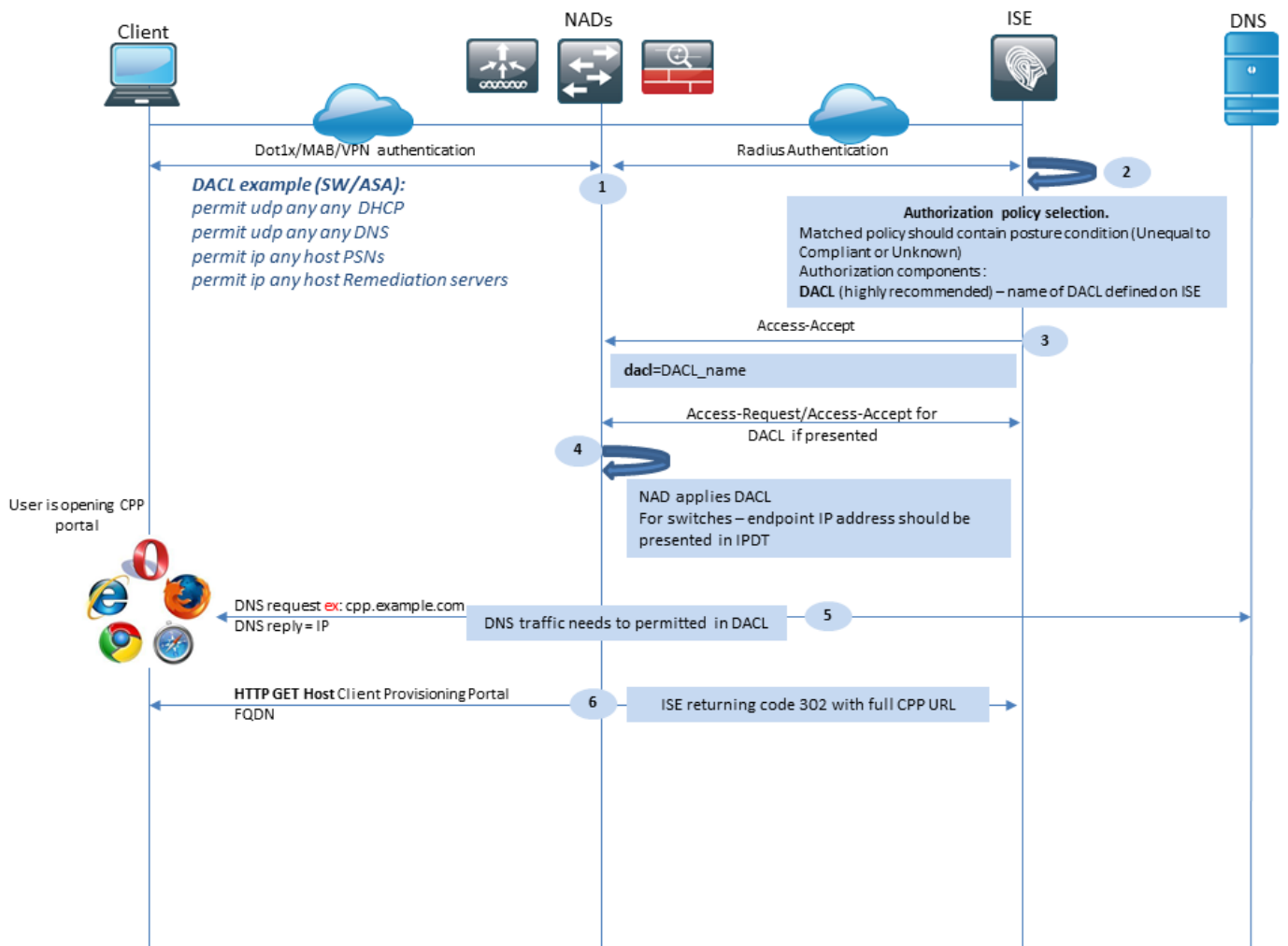


图2-1

步骤1.身份验证是流程的第一步。它可以是dot1x、MAB或VPN。

第2步：ISE必须为用户选择身份验证和授权策略。在安全评估中，所选授权策略必须包含对安全评估状态的引用，该引用最初必须为未知或不适用。要同时涵盖这两种情况，可以使用状况状态为不等合规性的条件。对于没有重定向的安全状态，无需在授权配置文件中使用的任何网络重定向配置。您仍然可以考虑使用DACL或空域ACL来限制用户访问安全评估状态不可用的阶段。

第3步：ISE返回具有授权属性的Access-Accept。

第四步：如果在Access-Accept中返回DACL名称，则NAD会启动DACL内容下载，并在获得授权配置文件后将其应用于会话。

第五步：新方法假设无法进行重定向，因此用户必须手动输入客户端调配门户FQDN。必须在ISE端的门户配置中定义CPP门户的FQDN。从DNS服务器的角度来看，A记录必须指向已启用PSN角色的ISE服务器。

第六步：客户端发送HTTP以获取客户端调配门户FQDN，此请求在ISE端解析，并将完整的门户URL返回给客户端。

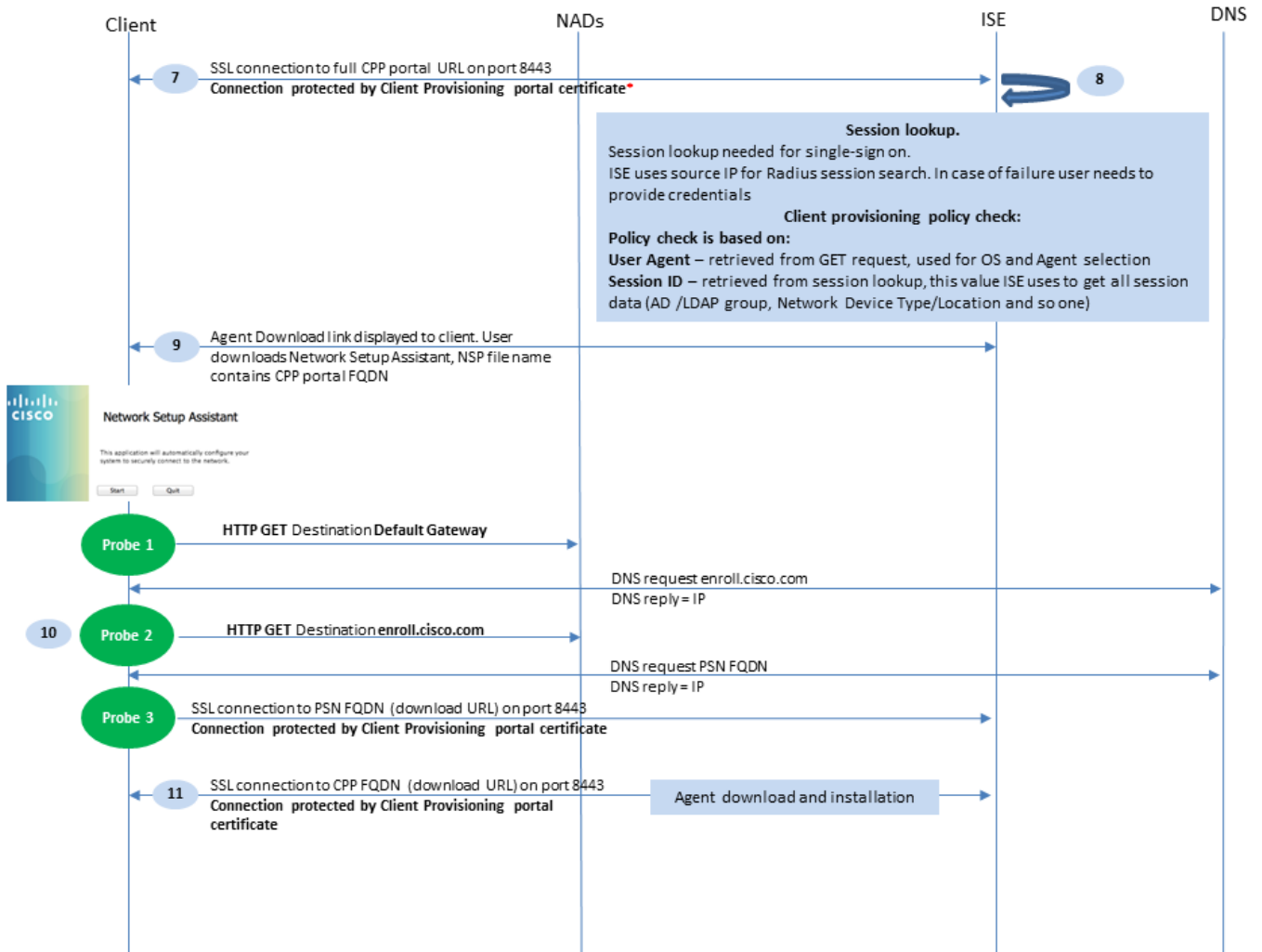


图2-2


第7步：通过重定向URL中接收的端口建立SSL连接（默认8443）。此连接受来自ISE端的门户证书保护。向用户显示客户端调配门户(CPP)。

步骤 8 在此步骤中，在ISE上发生两个事件：

- 单点登录(SSO)- ISE尝试查找以前成功的身份验证。ISE使用数据包的源IP地址作为实时RADIUS会话的搜索过滤器。

注意：根据数据包中的源IP与会话中的成帧IP地址之间的匹配来检索会话。成帧IP地址通常由ISE从临时记账更新中检索，因此需要在NAD端启用记账。此外，您必须记住，SSO仅在拥有会话的节点上可用。例如，如果会话在PSN 1上进行身份验证，但FQDN本身指向PSN2，则SSO机制将失败。

- 客户端调配策略查找 — 如果SSO成功，ISE可以使用来自身份验证会话的数据和来自客户端浏览器的用户代理。如果SSO不成功，用户必须提供凭证，并且在从内部和外部身份库（AD/LDAP/内部组）中检索用户身份验证信息后，该信息可用于客户端调配策略检查。

 注：由于Cisco Bug ID [CSCvd11574](#)，当外部用户是添加到外部身份库配置中的多个AD/LDAP组成员时，您会看到非SSO案例的客户端调配策略选择时出错。上述缺陷是从ISE 2.3 FCS开始修复的，并且修复要求在AD组的条件下使用CONTAINS而不是EQUAL。

步骤 9 选择客户端调配策略后，ISE向用户显示代理下载URL。点击下载NSA后，应用将被推送到用户。NSA文件名包含CPP门户的FQDN。

步骤10.在此步骤中，NSA运行探测功能建立到ISE的连接。两个探测功能是传统探测功能，第三个探测功能旨在允许在不进行url重定向的环境中进行ISE发现。

- NSA将第一个发现探测 — HTTP /auth/discovery发送到默认网关。因此，NSA预计会重定向URL。
- 如果第一个探测失败，NSA会发送第二个探测。第二个探测功能是HTTP GET /auth/discovery enroll.cisco.com. 此FQDN必须能由DNS服务器成功解析。在使用分割隧道的VPN场景中，流量发送到 enroll.cisco.com 必须通过隧道路由。
- NSA通过CPP门户端口将第三个探测发送到客户端调配门户FQDN。此请求包含有关门户会话ID的信息，允许ISE确定必须提供哪些资源。

步骤 11 NSA下载Anyconnect和/或特定模块。下载过程通过客户端调配门户端口完成。

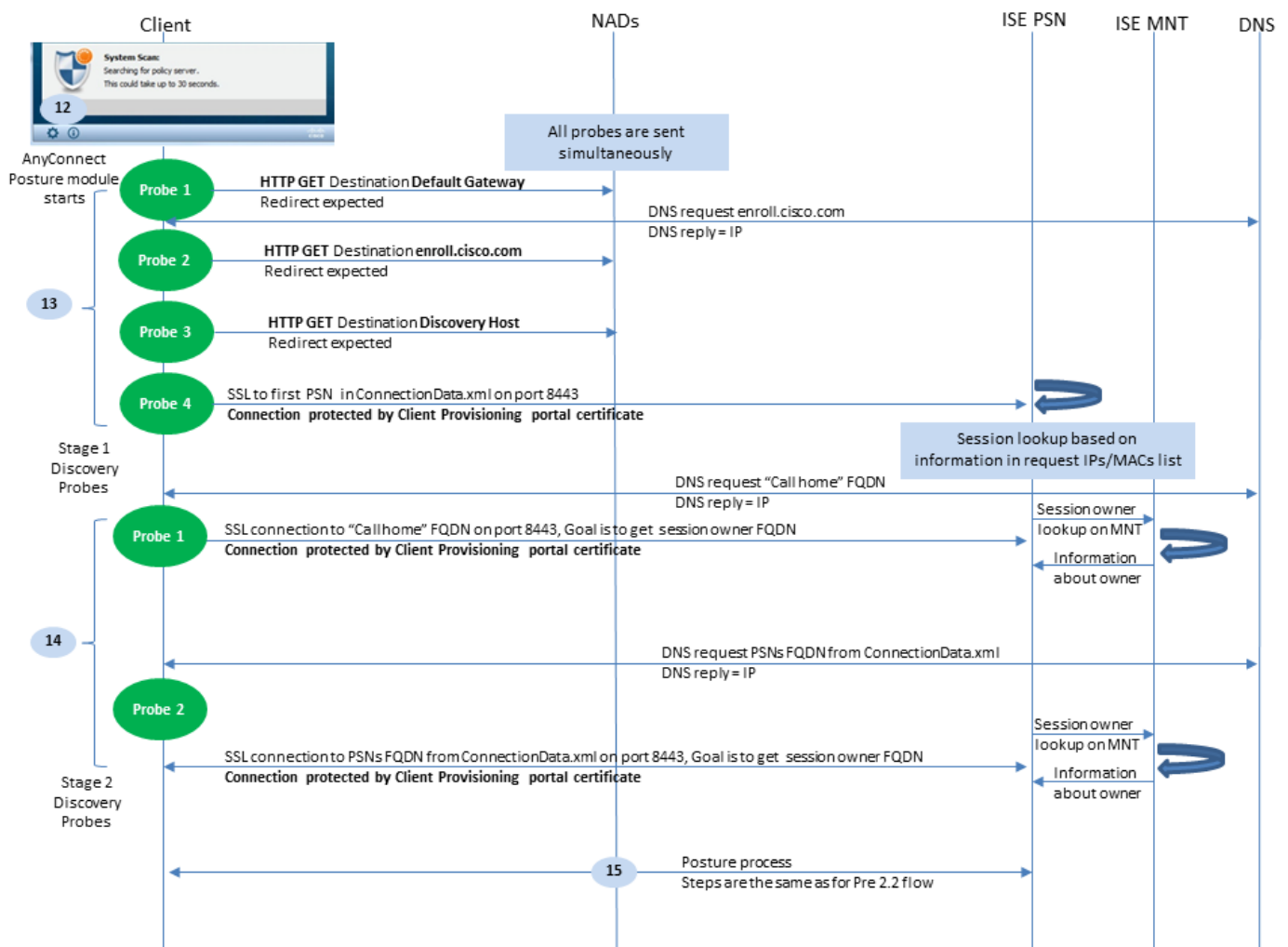


图2-3

步骤 12在ISE 2.2中，终端安全评估流程分为两个阶段。第一阶段包含一组传统状态发现探测功能，以支持与依赖url重定向的部署向后兼容。

步骤13.第一阶段包含所有传统状态发现探测。要获取有关探测功能的详细信息，请查看ISE 2.2之前安全评估流程中的步骤20。

第14步。第2阶段包含两个发现探测，允许AC ISE终端安全评估模块建立到PSN的连接，其中会话在不支持重定向的环境中进行身份验证。在第二阶段，所有探测都是连续的。

- 探测1 — 在第一个探测期间，AC ISE终端安全评估模块尝试建立来自“Call Home List”的IP/FQDN。必须在ISE端的AC终端安全评估配置文件中配置探测的目标列表。您可以定义以逗号分隔的IP/FQDN，可以使用冒号定义每个Call Home目标的端口号。此端口必须等于运行客户端调配门户的端口。在客户端，有关Call Home服务器的信息位于 ISEPostureCFG.xml，可在文件夹中找到该文件 — C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

如果call home目标不拥有会话，则在此阶段需要查找所有者。AC ISE终端安全评估模块指示ISE使用特殊目标URL开始所有者查找 — /auth/ng-discovery 请求。它还包含客户端IP和MAC列表。PSN会话收到此消息后，首先在本地执行查找（此查找使用来自AC ISE终端安全评估模块发送的请求的IP和MAC）。如果未找到会话，PSN将启动MNT节点查询。此请求仅包含MAC列表，因此，必须从MNT获取所有者的FQDN。之后，PSN将所有者FQDN返回客户端。来自客户端的下一个请求将发送到会话所有者FQDN，其auth/status位于URL和IP和MAC列表中。

- 探测2 — 在此阶段，AC ISE终端安全评估模块尝试位于以下位置的PSN FQDN ConnectionData.xml.您可以在以下位置找到此文件： C:\Users\

\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\

.AC ISE终端安全评估模块在首次终端安全评估尝试后创建此文件。文件包含ISE PSN FQDN列表。列表的内容可以在下一次连接尝试期间动态更新。此探测的最终目标是获取当前会话所有者的FQDN。实现方式与探测1相同。在探测目的地选择方面唯一的差异。如果多个用户使用设备，则文件本身位于当前用户的文件夹中。其他用户无法使用此文件中的信息。这会导致用户在不指定Call home目标的情况下在没有重定向的情况下在环境中遇到鸡和蛋问题。

步骤 15 获得有关会话所有者的信息后，所有后续步骤均与ISE 2.2之前的流程相同。

配置

本文档将ASA v用作网络接入设备。所有测试均通过VPN进行安全评估。通过VPN支持安全评估的ASA配置不属于本文档的范围。有关详细信息，请参阅[ASA 9.2.1版VPN终端安全评估与ISE配置示例](#)。

 注意：对于使用VPN用户的部署，建议设置为基于重定向的安全状态。不建议配置呼叫列表。

 对于所有基于VPN的用户，请确保应用DACL，使其不与配置了终端安全评估的PSN通信。

网络图

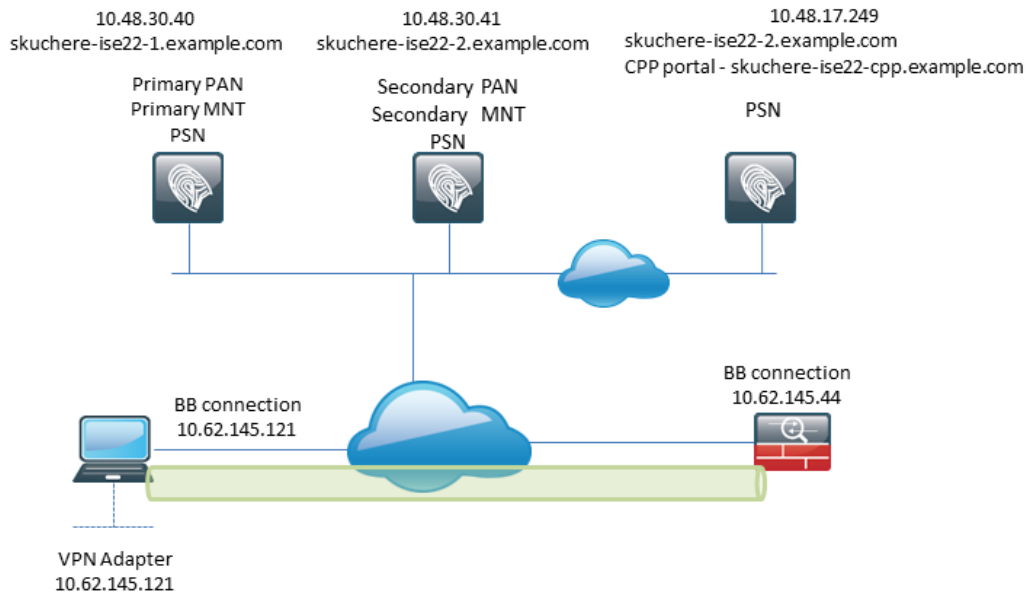


图3-1

此拓扑用于测试。使用ASA，由于NAT功能，当客户端调配门户的SSO机制在PSN端发生故障时，可以轻松模拟场景。对于通过VPN的常规安全评估流，SSO必须正常工作，因为当用户进入企业网络时，通常不会对VPN IP实施NAT。

配置

客户端调配配置

以下是准备Anyconnect配置的步骤。

步骤1: Anyconnect软件包下载。Anyconnect软件包本身无法从ISE直接下载，因此开始之前，请确保您的PC上提供交流电源。此链接可用于AC下载 —

<https://www.cisco.com/site/us/en/products/security/secure-client/index.html>。在本文档中，anyconnect-win-4.4.00243-webdeploy-k9.pkg 已使用软件包。

第二步：要将AC软件包上传到ISE，请导航至 Policy > Policy Elements > Results > Client Provisioning > Resources 并点击 Add. 从本地磁盘选择代理资源。在新窗口中，选择 Cisco Provided Packages, 点击 browse 并选择PC上的AC软件包。

Agent Resources From Local Disk

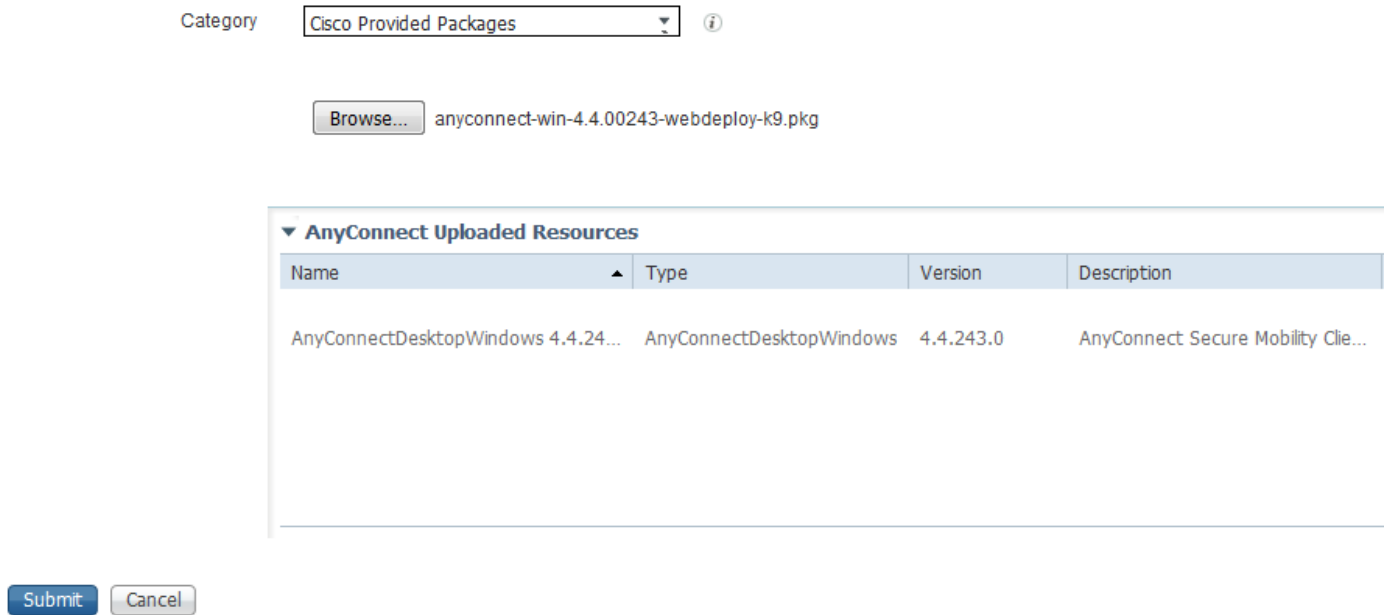


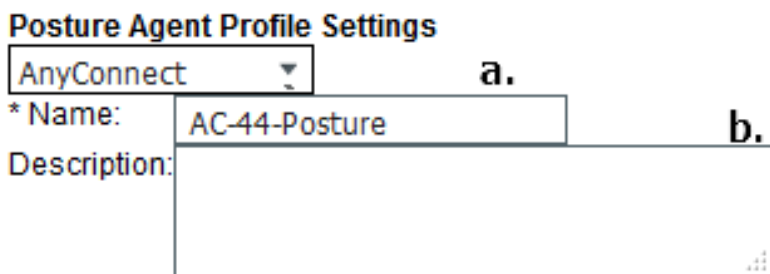
图3-2

点击 **Submit** 完成导入。

第三步：合规性模块必须上传到ISE。在同一页上，点击 **Add** 并选择 **Agent resources from Cisco site**. 在资源列表中，必须检查合规性模块。对于本文档， **AnyConnectComplianceModuleWindows 4.2.508.0** 使用合规性模块。

第四步：现在必须创建交流终端安全评估配置文件。点击 **Add** 并选择 **NAC agent or Anyconnect posture profile**.

ISE Posture Agent Profile Settings > New Profile



Agent Behavior

图3-3


- 选择配置文件的类型。此场景必须使用AnyConnect。
- 指定配置文件名称。导航至 **Posture Protocol 截面梁的截面梁**。

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/> a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	<input type="text" value="skuchere-ise22-2.examp"/> b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

图3-4

- 指定 `Server Name Rules`，此字段不能为空。该字段可以包含带有通配符的FQDN，从而限制从相应命名空间到PSN的AC ISE终端安全评估模块连接。如果必须允许任何FQDN，请放置星号。
- 此处指定的名称和IP正在状态发现的第2阶段使用。您可以按逗号分隔名称，也可以使用冒号在FQDN/IP后添加端口号。如果AC使用GPO或任何其他软件调配系统部署带外（不是从ISE客户端调配门户）部署，且存在Call Home地址，则此情况变得至关重要，因为只有一次探测可以成功到达ISE PSN。这意味着在带外AC调配的情况下，管理员必须使用AC配置文件编辑器创建AC ISE终端安全评估配置文件，并随AC安装调配此文件。

 **注：**请记住，Call home地址的存在对于多用户PC至关重要。在ISE 2.2之后的终端安全评估流程中查看步骤14。

步骤5.创建交流电配置。 导航至 `Policy > Policy Elements > Results > Client Provisioning > Resources`，点击 `Add`，然后选择 `AnyConnect Configuration`。

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0 **a.**

* Configuration Name: AC-44-CCO **b.**

Description:

DescriptionValue **Notes**

* Compliance Module: AnyConnectComplianceModuleWindows 4.2.508.0 **c.**

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Dagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC-44-Posture **d.**

图3-5

- 选择AC包。
- 提供AC配置名称。
- 选择合规性模块版本。
- 从下拉列表中选择AC状态配置文件。

第六步：配置客户端调配策略。导航至 Policy > Client Provisioning。如果是初始配置，您可以在默认策略中填充空值。如果需要将策略添加到现有的终端安全评估配置，请导航到可重用的策略，然后选择 Duplicate Above 或 Duplicate Below。也可以创建全新的策略。

这是文档中使用的策略示例。

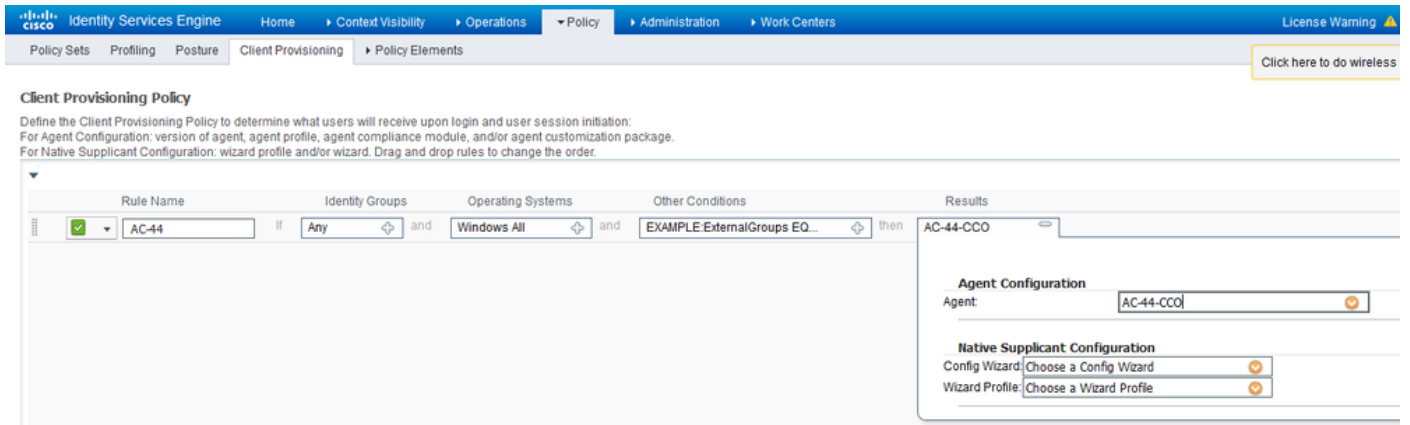


图3-6

在结果部分选择您的AC配置。请记住，在SSO失败的情况下，ISE只能拥有从登录到门户的属性。这些属性仅限于可从内部和外部身份库检索到的用户相关信息。在本文档中，AD组用作客户端调配策略中的条件。

安全评估策略和条件

使用简单的状态检查。ISE配置为检查终端设备端Window Defender服务的状态。实际场景可能更为复杂，但一般配置步骤是相同的。

步骤1: 创建状态条件。状态条件位于 Policy > Policy Elements > Conditions > Posture. 选择状况条件的类型。下面是一个服务条件示例，必须检查Windows Defender服务是否正在运行。

Service Conditions List > WinDefend

Service Condition

* Name	<input type="text" value="WinDefend"/>
Description	<input type="text"/>
* Operating Systems	<input type="text" value="Windows All"/>
Compliance Module	Any version
* Service Name	<input type="text" value="WinDefend"/>
Service Operator	<input type="text" value="Running"/>

图3-7

步骤2. 状况要求配置。导航至 Policy > Policy Elements > Results > Posture > Requirements. 下面是Window Defender检查的一个示例：

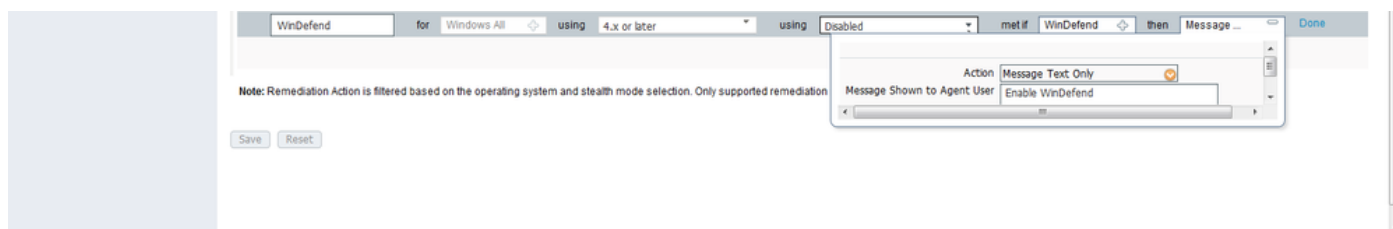


图3-8

在新要求中选择您的状况条件，并指定补救操作。

第三步：状态策略配置。导航至 Policy > Posture. 在这里，您可以找到用于此文档的策略示例。策略已将Windows Defender要求指定为强制要求，并且仅包含外部AD组名称作为条件。

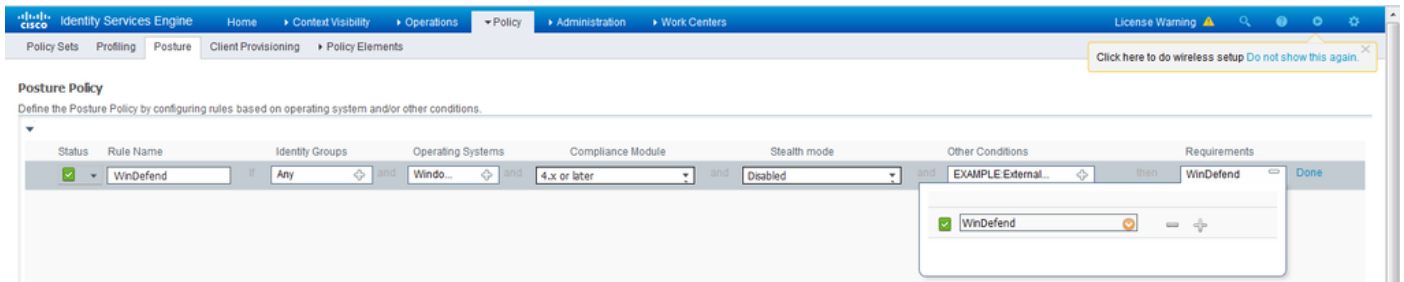


图3-9

配置客户端调配门户

对于无重定向的安全状态，必须编辑客户端调配门户的配置。导航至 Administration > Device Portal Management > Client Provisioning。您可以使用默认门户，也可以创建您自己的门户。同一门户可用于有重定向和无重定向的姿态。

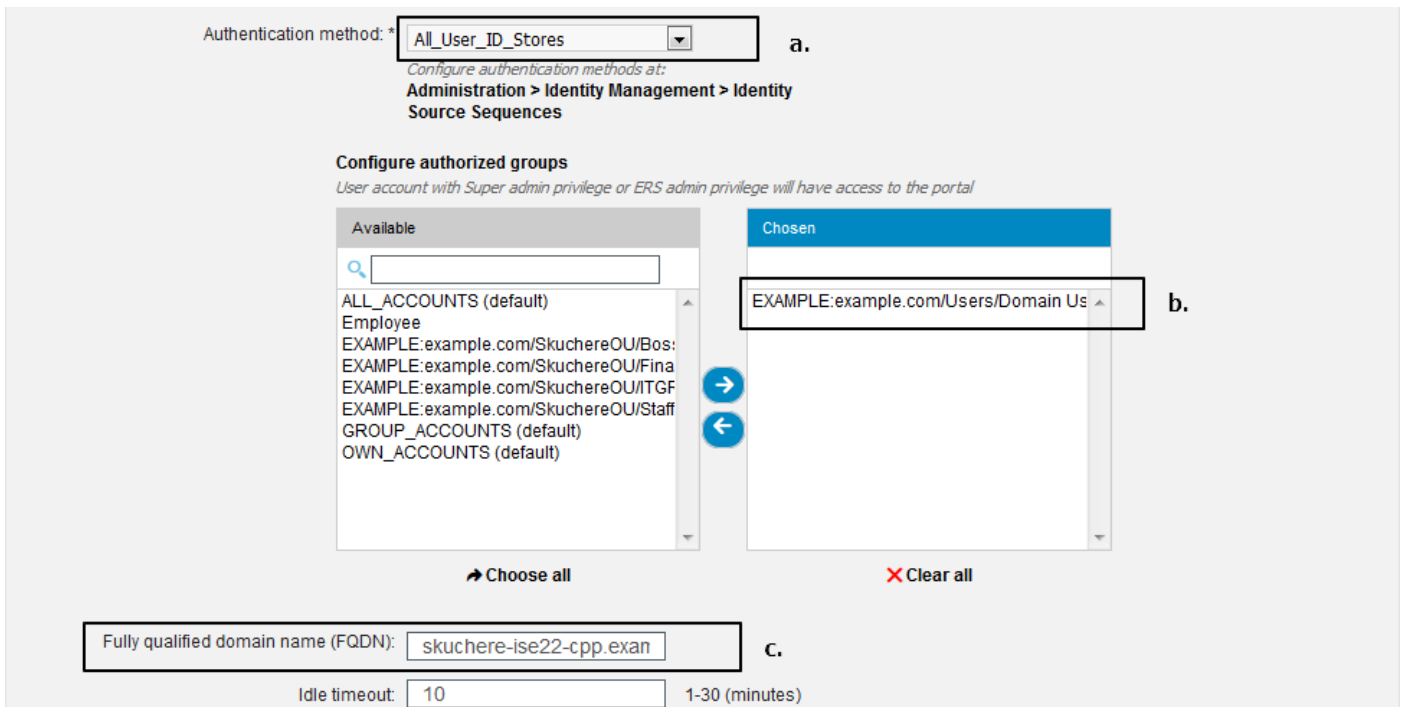


图3-10

以下设置必须在非重定向方案的门户配置中编辑：

- 在Authentication中，指定SSO找不到用户会话时必须使用的身份源序列。
- 根据选定的身份源序列列表，系统会填充可用组。此时，您必须选择授权进行门户登录的组。
- 当需要从客户端调配门户部署AC时，必须为场景指定客户端调配门户的FQDN。此FQDN必须可解析为ISE PSN IP。在首次连接尝试期间，必须指示用户在Web浏览器中指定FQDN。

配置授权配置文件和策略

终端安全评估状态不可用时客户端的初始访问必须受到限制。这可以通过多种方式实现：

- DACL分配 — 在限制访问阶段，可以将DACL分配给用户以限制访问。此方法可用于Cisco网

络接入设备。

- VLAN分配 — 在将成功的终端安全评估用户置于受限制的VLAN之前，此方法对于几乎任何NAD供应商都必须运行良好。
- Radius Filter-Id — 使用此属性，可以在NAD上本地定义的ACL可以分配给状态未知的用户。由于这是标准RFC属性，此方法必须适用于所有NAD供应商。

步骤1:配置DAACL。由于此示例基于ASA，因此可以使用NAD DAACL。对于实际场景，必须考虑将VLAN或Filter-ID作为可能的选项。

要创建DAACL，请导航至 Policy > Policy Elements > Results > Authorization > Downloadable ACLs 并点击 Add.

在未知状态期间，必须至少提供以下权限：

- DNS流量
- DHCP流量
- 到ISE PSN (端口80和443) 的流量，用于打开门户的友好FQDN。运行CP门户的端口默认为8443，端口8905向后兼容)
- 必要时流向补救服务器的流量

以下是不使用补救服务器的DAACL示例：

Downloadable ACL List > **New Downloadable ACL**

Downloadable ACL

* Name

Description

* DACL Content

```
1 permit udp any any eq 53
2 permit udp any any eq bootps
3 permit tcp any host 10.48.30.40 eq 80
4 permit tcp any host 10.48.30.40 eq 443
5 permit tcp any host 10.48.30.40 eq 8443
6 permit tcp any host 10.48.30.40 eq 8905
7 permit tcp any host 10.48.30.41 eq 80
8 permit tcp any host 10.48.30.41 eq 443
9 permit tcp any host 10.48.30.41 eq 8443
10 permit tcp any host 10.48.30.41 eq 8905
```

▶ Check DACL Syntax

图3-11

第二步：配置授权配置文件。

与往常一样，安全评估需要两个授权配置文件。第一个必须包含任何类型的网络访问限制（本示例中使用了DAACL的配置文件）。此配置文件可应用于状态不等于合规的身份验证。第二个授权配置文件可以只包含允许访问，并且可以应用于状态状态等于合规性的会话。

要创建授权配置文件，请导航至 Policy > Policy Elements > Results > Authorization > Authorization Profiles.

受限访问配置文件示例：

Authorization Profiles > VPN-No-Redirect-Unknown

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

DACL Name

图3-12

在本示例中，默认ISE配置文件PermitAccess用于成功状态检查后的会话。

第三步：配置授权策略。在此步骤中，必须创建两个授权策略。一个是匹配初始身份验证请求与未知的安全评估状态，第二个是在成功的安全评估流程后分配完全访问权限。

以下是适用于此情况的简单授权策略示例：

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Posture-Compliant	if (Session:PostureStatus EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then PermitAccess
✓	Posture-Unknown-No-Redirect	if (Session:PostureStatus NOT_EQUALS Compliant AND EXAMPLE:ExternalGroups EQUALS example.com/Users/Domain Users)	then VPN-No-Redirect-Unknown
✓	Default	if no matches, then	DenyAccess

图3-13

身份验证策略的配置不是本文档的一部分，但您必须记住，在授权策略处理成功身份验证之前，必须先进行身份验证。

验证

流的基本验证可包含三个主要步骤：

步骤1:身份验证流验证。

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization Profiles	IP Address
Feb 23, 2017 06:00:07.028 PM	✓			e.	10.62.145.95				PermitAccess	
Feb 23, 2017 06:00:04.368 PM	ⓘ		0	d. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	172.16.31.12
Feb 23, 2017 05:59:04.750 PM	✓			c. user1						
Feb 23, 2017 05:44:57.921 PM	✓			b. #ACSACL#-IP-VPN-No-Redi...						
Feb 23, 2017 05:44:57.680 PM	✓			a. user1	00:0B:7F:D0:F8:F4	Windows7-...	VPN-LAB >>...	VPN-LAB >>...	VPN-No-Redirect-Unknown	

图4-1

1. 初始身份验证。对于此步骤，您可能会对已应用授权配置文件的验证感兴趣。如果应用了意外的授权配置文件，请调查详细的身份验证报告。单击“详细信息”列中的放大镜即可打开此报告。您可以将详细身份验证报告中的属性与授权策略中预期匹配的条件进行比较。
2. DACL下载事件。仅当为初始身份验证选择的授权配置文件包含DACL名称时，才会显示此字符串。
3. 门户身份验证 — 流程中的此步骤表明SSO机制未能定位用户会话。发生此问题可能有多种原因：
 - 未将NAD配置为发送记账消息，或者其中不存在帧IP地址
 - CPP门户FQDN已解析为ISE节点的IP，与已处理初始身份验证的节点不同
 - 客户端位于NAT之后

4. 会话数据更改。在此特定示例中，会话状态已从“未知”更改为“兼容”。
5. COA连接到网络接入设备。此COA必须成功才能从NAD端推送新的身份验证，并在ISE端推送新的授权策略分配。如果COA失败，您可以打开详细报告以调查原因。COA最常见的问题包括：
 - COA超时 — 在这种情况下，已发送请求的PSN未配置为NAD端的COA客户端，或者COA请求已在途中的某个位置被丢弃。
 - COA负ACK — 表示NAD已收到COA，但由于某种原因无法确认COA操作。对于此方案，详细报告必须包含更详细的说明。

由于本示例将ASA用作NAD，因此您不会看到用户的后续身份验证请求。发生这种情况的原因是ISE对ASA使用COA推送，从而避免VPN服务中断。在这种情况下，COA本身包含新的授权参数，因此不需要重新身份验证。

第2步：客户端调配策略选择验证 — 为此，您可以在ISE上运行报告，该报告可帮助您了解哪些客户端调配策略已应用于用户。

导航至 **Operations > Reports Endpoint and Users > Client Provisioning** 并运行所需日期的报告。

Logged At	Server	Event	Identity	Client Provisioning Policy Matched	Failure Reason
2017-02-24 18:33:46...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 18:46:42...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	
2017-02-23 17:59:07...	skuchere-ise22-3	Client provisioning succeeded	user1	AC-44	

图4-2

通过此报告，您可以验证选择了哪个客户端调配策略。此外，如果失败，原因必须显示在 Failure Reason 列。

第3步：状态报告验证 — 导航至 **Operations > Reports Endpoint and Users > Posture Assessment by Endpoint**。

Logged At	Status	Details	Identity	Endpoint ID	IP Address	Endpoint OS
2017-02-24 18:34:31...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-
2017-02-23 19:33:35...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-

图4-3

您可以从此处打开每个特定事件的详细报告，例如，检查此报告属于哪个会话ID、ISE为终端选择的确切状态要求以及每个要求的状态。

故障排除

一般信息

对于安全评估流程故障排除，必须启用以下ISE组件才能在可能发生安全评估流程的ISE节点上进行调试：

- client-webapp — 负责代理程序调配的组件。目标日志文件 `guest.log` 和 `ise-psc.log`。
- guestaccess — 负责客户端调配门户组件和会话所有者查找的组件（当请求到达错误的PSN时）。目标日志文件 — `guest.log`。
- provisioning — 负责客户端调配策略处理的组件。目标日志文件 — `guest.log`。
- posture — 所有状态相关事件。目标日志文件 — `ise-psc.log`。

对于客户端故障排除，可以使用以下命令：

- acisensa.log — 如果客户端的客户端调配失败，此文件会在下载NSA的同一文件夹中创建（通常为Windows下载目录）。
- AnyConnect_ISEPosture.txt — 此文件可在目录中的DART捆绑包中找到 Cisco AnyConnect ISE Posture Module。有关ISE PSN发现和状态流程常规步骤的所有信息均记录在此文件中。

常见问题故障排除

SSO相关问题

如果SSO成功，您可以在中看到这些消息 `ise-psc.log`，此组消息表示会话查找已成功完成，可以跳过门户上的身份验证。

```
<#root>
```

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
looking for Radius session with input values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121

2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][] cisco.cpm.posture.runtime.PostureRu

Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

文本窗口5-1

您可以使用终端IP地址作为搜索密钥来查找此信息。

稍后在访客日志中，您必须看到已跳过身份验证：

```
<#root>
```

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] com.cisco.ise.portalSessionManager.
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] guestaccess.flowmanager.step.cp.CPI
```

```
Login step will be skipped, as the session =c0a801010002600058232bb8 already established for mac address
```

```
2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12] [] cpm.guestaccess.flowmanager.process
```

文本窗口5-2

如果SSO不起作用，ise-psc log 文件包含有关会话查找失败的信息：

```
<#root>
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
```

```
looking for session using IP 10.62.145.44
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cisco.cpm.posture.runtime.PostureRu
```

```
No Radius session found
```

文本窗口5-3

如果 guest.log 在这种情况下，您必须在门户上看到完整的用户身份验证：

```
<#root>
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.St
```

```
Returning next step =LOGIN
```

```
2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2] [] cpm.guestaccess.flowmanager.step.Ste
```

文本窗口5-4

如果门户上的身份验证失败，您必须专注于门户配置验证 — 哪个身份库正在使用中？哪些组有权登录？

客户端调配策略选择故障排除

如果客户端调配策略失败或策略处理不正确，您可以检查 `guest.log` 有关更多详细信息，请查看：

```
<#root>
```

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] cpm.guestaccess.common.utils.OSMap  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.  
  
:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

文本窗口5-5

在第一个字符串中，您可以看到如何将有关会话的信息注入到策略选择引擎中，如果策略不匹配或不正确策略匹配，则可以将来自此处的属性与客户端调配策略配置进行比较。最后一个字符串表示策略选择状态。

状态流程故障排除

在客户端，您必须对探测功能及其结果的调查感兴趣。以下是成功的第1阶段探测的示例：

```
*****
```

```
Date : 02/23/2017  
Time : 17:59:57  
Type : Unknown  
Source : acise
```

```
Description : Function: Target::Probe  
Thread Id: 0x4F8  
File: SwiftHttpRunner.cpp  
Line: 1415  
Level: debug
```

```
PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..
```

文本窗口5-6

在此阶段，PSN将返回有关会话所有者的AC信息。稍后您可以看到以下几条消息：

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

文本窗口5-7

会话所有者将所需的所有信息返回座席：

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
 <IP></IP>
 <FQDN>skuchere-ise22-2.example.com</FQDN>
 <PostureDomain>posture_domain</PostureDomain>
 <sessionId>c0a801010009e00058af0f7b</sessionId>
 <configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
 <AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>

```
<AcPackPort>8443</AcPackPort>
<AcPackVer>4.4.243.0</AcPackVer>
<PostureStatus>Unknown</PostureStatus>
<PosturePort>8443</PosturePort>
<PosturePath>/auth/perfigo_validate.jsp</PosturePath>
<PRAConfig>0</PRAConfig>
<StatusPath>/auth/status</StatusPath>
<BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
```

文本窗口5-8

从PSN端，您可以集中注意以下消息：`guest.log` 当您预期到节点的初始请求不拥有会话时：

```
<#root>
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
mac_list from http request ==> 00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
iplist from http request ==> 172.16.31.12,10.62.145.95
```

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
```

```
Session Info is null
```

```
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
Performing MNT look up for macAddress ==> 00-0B-7F-D0-F8-F4
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
Performed MNT lookup, found session 0 with session id c0a801010009e00058af0f7b
```

```
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10] [] cisco.cpm.client.posture.NextGenDi
```

```
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][] cpm.client.provisioning.utils.Prov
```

文本窗口5-9

在这里，您可以看到PSN首先尝试在本地查找会话，并且在失败后使用IP和MAC列表向MNT发起请求以查找会话所有者。

稍后，您必须在正确的PSN上看到来自客户端的请求：

```
<#root>
```

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
ooking for session using session ID: null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
Found session c0a801010009e00058af0f7b using ipAddr 172.16.31.12
```

文本窗口5-10

下一步，PSN将为此会话执行客户端调配策略查找：

```
<#root>
```

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PostureRun
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][] cisco.cpm.posture.runtime.PosturePo
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][] com.cisco.cpm.swiss.SwissServer -:::
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][] cisco.cpm.posture.util.AgentUtil -:
Increase Mnt counter at CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

文本窗口5-11

在下一步中，您可以看到状况要求选择的过程。在步骤结束时，会准备要求列表并返回给座席：

```
<#root>
```

2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan

About to query posture policy for user user1 with endpoint mac 00-0b-7f-d0-f8-f4

2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMan
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PosturePo1
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cpm.posture.runtime.agent.AgentXmlGe
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan

```
<version>ISE: 2.2.0.470</version>  
<encryption>0</encryption>  
<package>  
<id>10</id>
```

WinDefend

Enable WinDefend

3

0

3

WinDefend

3

301

WinDefend

running

(WinDefend)

```
</package>  
</cleanmachines>
```

文本窗口5-12

稍后，您可以看到PSN已收到状态报告：

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan  
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureHan
```

文本窗口5-13

在流程结束时，ISE将终端标记为合规并启动COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureMana  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA  
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8] [] cisco.cpm.posture.runtime.PostureCoA
```

文本窗口5-14

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）。