

# 將ISE終端安全評估重定向流量與ISE終端安全評估無重定向流量進行比較

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

#### [終端安全評估流量Pre ISE 2.2](#)

#### [ISE狀態流量後2.2](#)

### [設定](#)

#### [網路圖表](#)

#### [組態](#)

##### [客戶端調配配置](#)

##### [終端安全評估策略和條件](#)

##### [配置客戶端調配門戶](#)

##### [配置授權配置檔案和策略](#)

### [驗證](#)

### [疑難排解](#)

#### [一般資訊](#)

#### [常見問題故障排除](#)

##### [SSO相關問題](#)

##### [客戶端調配策略選擇故障排除](#)

##### [狀態過程故障排除](#)

---

## 簡介

本檔案將介紹ISE 2.2及更高版本支援的終端安全評估無重定向流量與自較早的ISE版本以來支援的終端安全評估重定向流量的比較。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ISE上的狀態流
- 在ISE上配置狀態元件
- 用於虛擬專用網路(VPN)安全狀態的自適應安全裝置(ASA)配置

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本2.2
- Cisco ASAv與軟體9.6(2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本檔案介紹身分識別服務引擎(ISE)2.2中引入的新功能，該功能允許ISE支援狀態流程，而無需在網路存取裝置(NAD)或ISE上提供任何型別的重新導向支援。

終端安全評估是Cisco ISE的核心元件。作為元件的狀態可以用三個主要元素表示：

1. ISE作為策略配置分發和決策點。  
從ISE的管理員角度來看，您可以配置終端安全評估策略（必須將裝置標籤為符合公司要求的確切條件）、客戶端調配策略（必須在哪種型別的裝置上安裝哪種代理軟體）和授權策略（必須分配哪種型別的許可權，取決於其終端安全評估狀態）。
2. 作為策略實施點的網路接入裝置。  
在NAD端，在使用者身份驗證時應用實際授許可權制。ISE作為策略點提供授權引數，如下載ACL(dACL)/VLAN/Redirect-URL/重定向訪問控制清單(ACL)。傳統上，為了進行安全評估，需要需要NAD支援重定向（指示必須聯絡哪個ISE節點的使用者或代理軟體）和授權更改(CoA)，以便在終端安全評估狀態確定後重新驗證使用者。
3. 代理軟體作為資料收集和與終端使用者互動的點。  
Cisco ISE使用三種型別的代理軟體：AnyConnect ISE終端安全評估模組、NAC代理和Web代理。代理從ISE接收有關終端安全評估要求的資訊，並向ISE提供要求狀態報告。

---

 注意：本文檔基於Anyconnect ISE終端安全評估模組，該模組是唯一一個完全支援終端安全評估而無需重定向的模組。

---

在ISE 2.2之前的流量狀態中，NAD不僅用於驗證使用者和限制訪問，還用於為代理軟體提供有關必須聯絡的特定ISE節點的資訊。作為重定向過程的一部分，有關ISE節點的資訊將返回到代理軟體。

過去，在NAD或ISE端提供重定向支援是終端安全評估實施的基本要求。在ISE 2.2中，初始客戶端調配和終端安全評估流程不再需要支援重定向。

無重定向的客戶端調配 — 在ISE 2.2中，您可以直接通過門戶完全限定域名(FQDN)訪問客戶端調配門戶(CPP)。這與訪問發起人門戶或MyDevice門戶的方式類似。

無重定向的終端安全評估流程 — 代理安裝期間從CPP門戶儲存有關ISE伺服器的資訊，使直接通訊

成為可能。

## 終端安全評估流量Pre ISE 2.2

此圖顯示ISE 2.2之前的Anyconnect ISE終端安全評估模組流量的逐步說明：

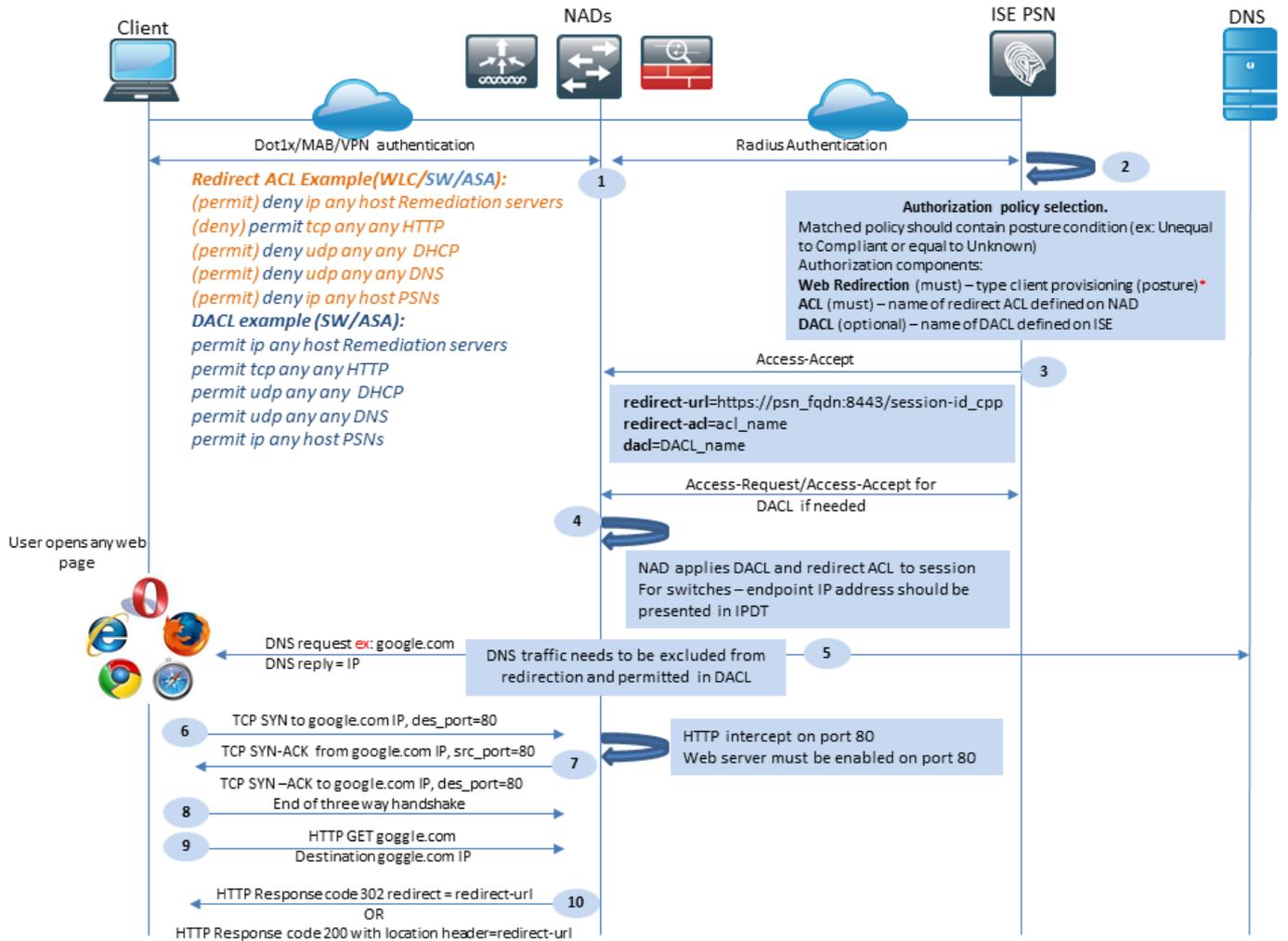


圖1-1

步驟 1. 身份驗證是流程的第一步，可以是dot1x、MAB或VPN。

步驟 2. ISE需要為使用者選擇身份驗證和授權策略。在終端安全評估方案中，選擇的授權策略必須包含對終端安全評估狀態的引用，該引用最初必須為未知或不適用。為了同時涵蓋這兩種情況，可以使用狀況狀態不等的合規性條件。

所選授權配置檔案必須包含有關重新導向的資訊：

- Web重新導向 — 對於狀態情況，必須將Web重新導向型別指定為客戶端調配（狀態）。
- ACL — 本節需要包含在NAD端設定的ACL名稱。此ACL用於指示NAD哪些流量必須繞過重定向，哪些流量必須實際重定向。
- DACL — 它可以與重定向訪問清單一起使用，但您必須記住，不同的平台會以不同的順序處理DACL和重定向ACL。

例如，ASA始終在重定向ACL之前處理DACL。同時，某些交換器平台會以與ASA相同的方式處理它，而其它交換器平台會先處理重新導向ACL，然後在必須捨棄或允許流量時檢查DACL/介面ACL。

---

 注意：在授權配置檔案中啟用Web重新導向選項後，必須選擇用於重新導向的目標門戶。

---

步驟 3. ISE返回具有授權屬性的Access-Accept。授權屬性中的重定向URL由ISE自動生成。它包含以下元件：

- 進行身份驗證的ISE節點的FQDN。在某些情況下，授權配置檔案配置（靜態IP/主機名/FQDN）可能會在「Web重定向」部分覆蓋動態FQDN。如果使用靜態值，則必須指向處理身份驗證的同一ISE節點。對於負載平衡器(LB)，此FQDN可以指向LB VIP，但僅當LB配置為將Radius和SSL連線結合在一起時。
- 埠 — 從目標門戶配置獲取埠值。
- 會話ID — 此值由ISE從Access-Request中提供的Cisco AV對稽核會話ID獲取。值本身由NAD動態生成。
- 門戶ID - ISE端目標門戶的識別符號。

步驟 4.NAD向會話應用授權策略。此外，如果已配置DACL，則在應用授權策略之前會請求其內容。

重要注意事項：

- 所有NAD — 裝置必須具有本地配置的ACL，其名稱必須與Access-Accept as redirect-acl中接收的名稱相同。
- 交換機 — 客戶端的IP地址必須顯示在 `show authentication session interface details` 命令成功應用重定向和ACL。客戶端IP地址通過IP裝置跟蹤功能(IPDT)獲取。

步驟 5.客戶端傳送輸入到Web瀏覽器中的FQDN的DNS請求。在這個階段，DNS流量必須繞過重定向，並且DNS伺服器必須返回正確的IP地址。

步驟 6.使用者端會將TCP SYN傳送到DNS回覆中收到的IP位址。資料包中的源IP地址是客戶端IP，而目標IP地址是所請求資源的IP。目的地連線埠等於80，但在使用者端Web瀏覽器中設定直接HTTP Proxy的情況除外。

步驟7.NAD攔截客戶端請求並準備源IP等於請求的資源IP、目標IP等於客戶端IP和源埠等於80的SYN-ACK資料包。

重要注意事項：

- NAD必須在客戶端傳送請求的埠上運行HTTP伺服器。預設情況下，它是埠80。
- 如果客戶端使用直接HTTP代理Web伺服器，則HTTP伺服器必須在NAS上的代理埠上運行。此案例不在本文的範圍內。
- 如果NAD在客戶端中沒有本地IP地址，則子網SYN-ACK將與NAD路由表一起傳送（通常通過管理介面）。在此案例中，封包是透過第3層基礎架構路由，且必須透過第3層上游裝置路由回使用者端。如果L3裝置是有狀態防火牆，則必須為此類非對稱路由提供額外例外。

步驟 8. 客戶端通過ACK完成TCP三次握手。

步驟 9. 目標資源的HTTP GET由客戶端傳送。

步驟 10. NAD使用HTTP代碼302 ( 頁面已移動 ) 將重定向URL返回給客戶端，對於某些可在位置標頭中的HTTP 200 OK消息內返回的NAD重定向。

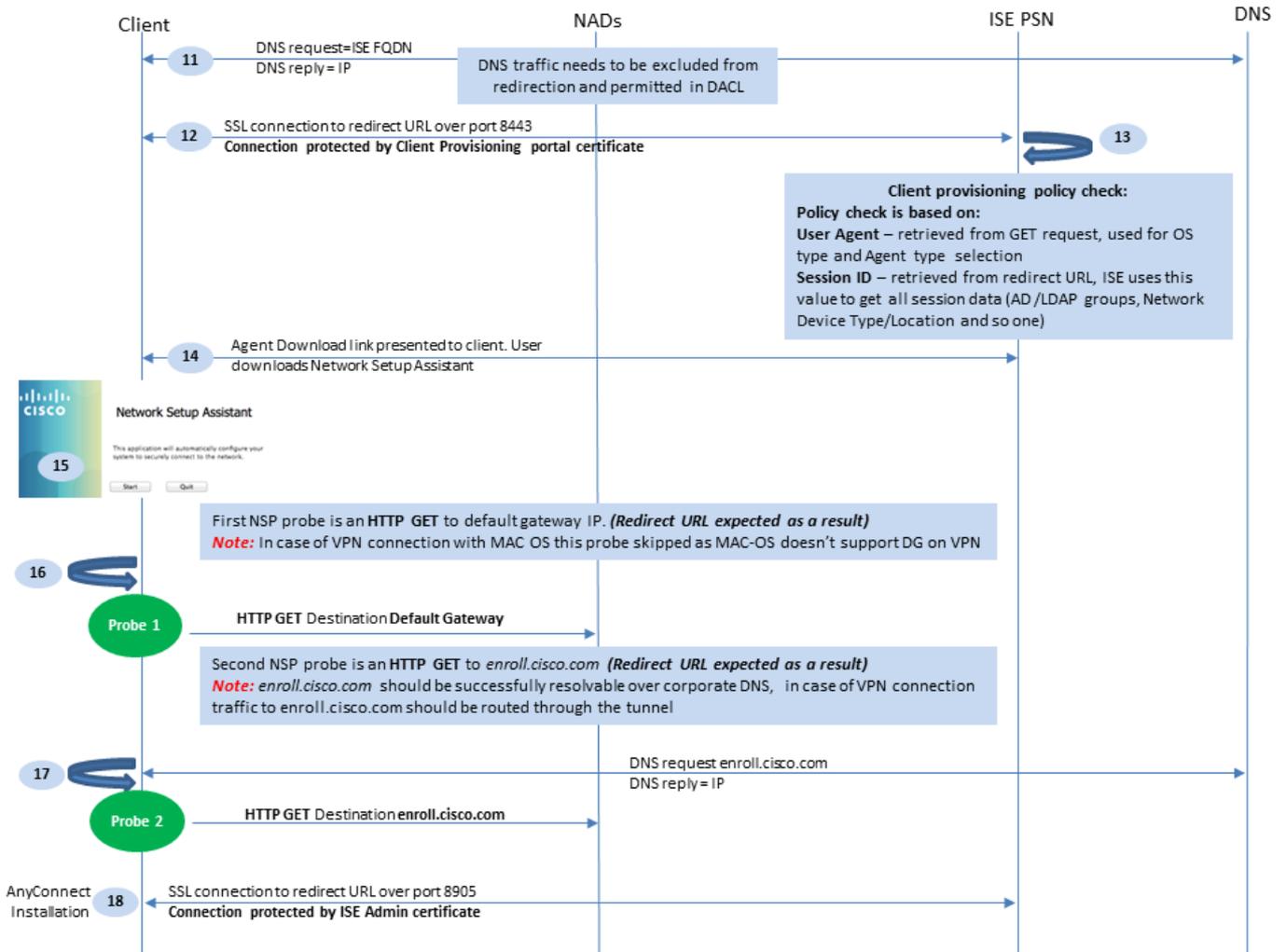


圖1-2

步驟 11. 客戶端從重定向URL傳送FQDN的DNS請求。FQDN必須在DNS伺服器端可解析。

步驟 12. 通過重定向URL中接收的埠建立SSL連線 ( 預設8443 )。此連線受來自ISE端的門戶證書保護。客戶端調配門戶(CPP)提供給使用者。

步驟13.在向客戶端提供下載選項之前，ISE必須選擇目標客戶端調配(CP)策略。從身份驗證會話 ( 如AD/LDAP組等 ) 檢索從瀏覽器使用者代理檢測到的客戶端的作業系統(OS)以及CPP策略選擇所需的其他資訊。ISE通過重定向URL中顯示的會話ID瞭解目標會話。

步驟 14. 網路設定助理(NSA)下載連結返回到客戶端。客戶端下載應用程式。

---

 注意：通常您可以將NSA視為Windows和Android自帶裝置流的一部分，但也可以使用此應用程式從ISE安裝Anyconnect或其元件。

---

步驟15.使用者運行NSA應用程式。

步驟 16. NSA將第一個發現探測 — HTTP /auth/discovery傳送到預設網關。NSA預期結果為redirect-url。

---

 注意：對於MAC OS裝置上的VPN連線，將忽略此探測，因為MAC OS在VPN介面卡上沒有預設網關。

---

步驟17.如果第一個探測失敗，NSA將傳送第二個探測。第二個探測是HTTP GET /auth/discovery enroll.cisco.com. 此FQDN必須由DNS伺服器成功解析。在具有拆分隧道的VPN場景中，到 enroll.cisco.com 必須通過隧道路由。

步驟 18. 如果任何探測成功，NSA會使用從redirect-url獲取的資訊通過埠8905建立SSL連線。此連線受ISE管理員證書保護。在此連線中，NSA下載Anyconnect。

重要注意事項：

- 在ISE 2.2版本之前，通過埠8905進行SSL通訊是安全評估的要求。
- 要避免證書警告，客戶端必須信任門戶和管理員證書。
- 在多介面ISE部署中，G0以外的介面可以繫結到FQDN，與系統FQDN不同(使用 ip host CLI命令)。這可能會導致使用者名稱(SN)/使用者替代名稱(SAN)驗證出現問題。例如，如果從介面G1將客戶端重定向到FQDN，則系統FQDN可以與8905通訊證書的重定向URL中的FQDN不同。作為此方案的解決方案，您可以在管理員證書SAN欄位中新增其他介面的FQDN，也可以在管理員證書中使用萬用字元。

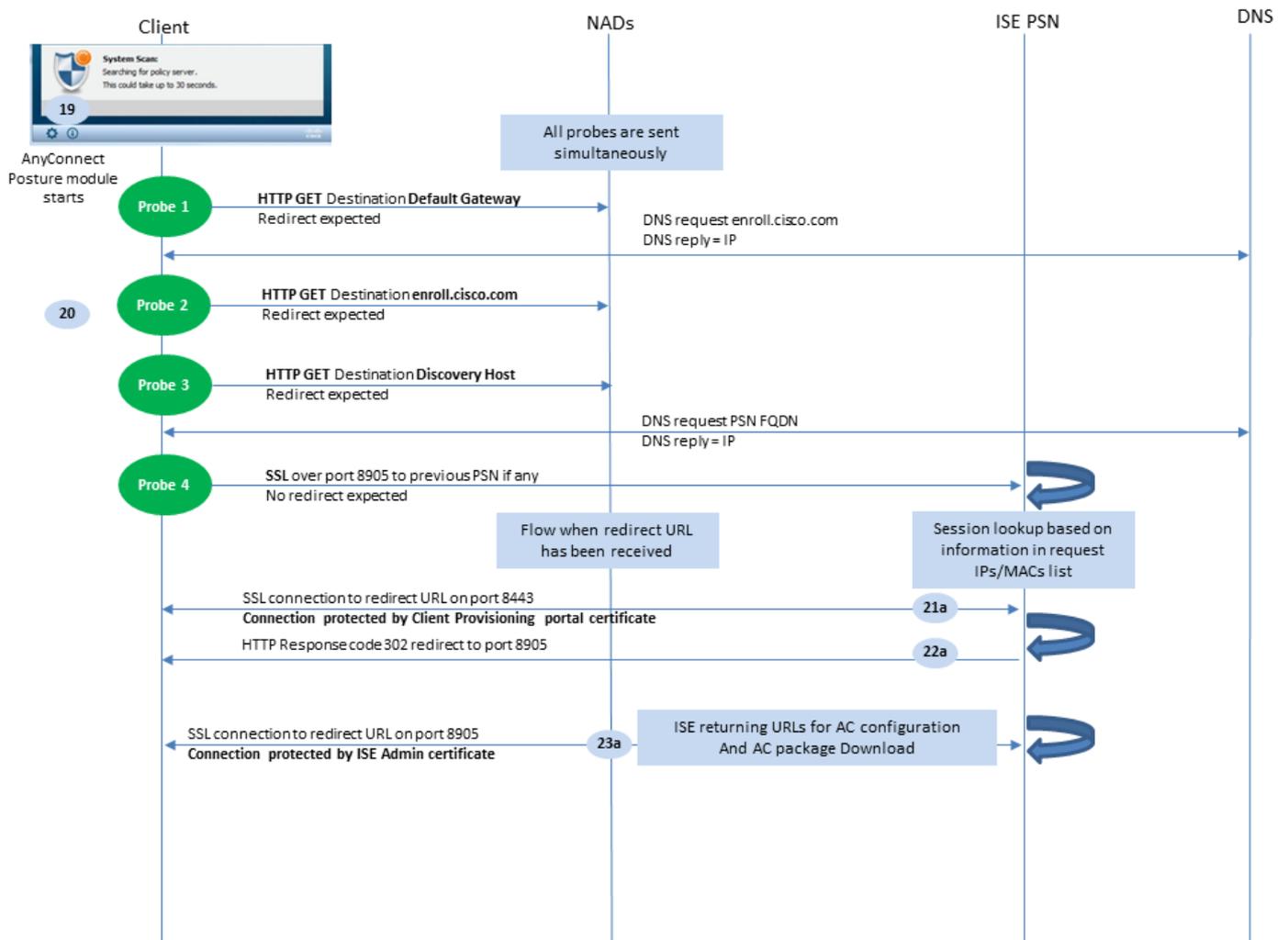


圖 1-3

步驟 19. 啟動 Anyconnect ISE 終端安全評估流程。

Anyconnect ISE 終端安全評估模組在以下任何情況下啟動：

- 安裝後
- 預設閘道值變更後
- 系統使用者登入事件之後
- 系統電源事件之後

步驟 20. 在此階段，Anyconnect ISE 終端安全評估模組啟動策略伺服器檢測。這通過一系列同時由 Anyconnect ISE 終端安全評估模組傳送的探測器來實現。

- 探測 1 - HTTP 獲取預設網關 IP 的 /auth/discovery。您必須記住，MAC OS 裝置在 VPN 介面卡上沒有預設網關。探查的預期結果為 redirect-url。
- 探測 2 - HTTP GET /auth/discovery 到 enroll.cisco.com。此 FQDN 需要由 DNS 伺服器成功解析。在具有拆分隧道的 VPN 場景中，到 enroll.cisco.com 必須通過隧道路由。探查的預期結果為 redirect-url。
- 探測 3 - HTTP get /auth/discovery 到發現主機。在 AC 終端安全評估配置檔案中安裝期間，從 ISE 返回發現主機值。探查的預期結果為 redirect-url。
- 探測 4 — 通過 SSL 將埠 8905 上的 HTTP GET /auth/status 連線到先前連線的 PSN。此請求包含

有關在ISE端查詢會話的客戶端IP和MAC清單的資訊。第一次姿勢嘗試期間不會出現此問題。連線受ISE管理員證書保護。由於此探測，如果探測到達的節點與使用者經過身份驗證的節點相同，則ISE可以將會話ID返回給客戶端。

**注意：**通過此探測，即使在某些情況下沒有工作重定向，也可以成功完成狀態。成功的安全狀態而不重定向要求驗證會話的當前PSN必須與之前成功連線的PSN相同。請記住，在ISE 2.2之前的版本中，無重定向的成功終端安全評估不是規則，而是例外。

接下來的步驟描述在由於其中一個探測器而收到重定向URL（以字母a標籤的流）時的狀態過程。

步驟 21. Anyconnect ISE終端安全評估模組使用發現階段檢索的URL建立到客戶端調配門戶的連線。在此階段，ISE使用來自己驗證會話的資訊再次進行客戶端調配策略驗證。

步驟22.如果檢測到客戶端調配策略，ISE將返回重定向到埠8905。

步驟 23. 代理通過埠8905建立與ISE的連線。在此連線期間，ISE返回狀態配置檔案、合規性模組和anyconnect更新的URL。

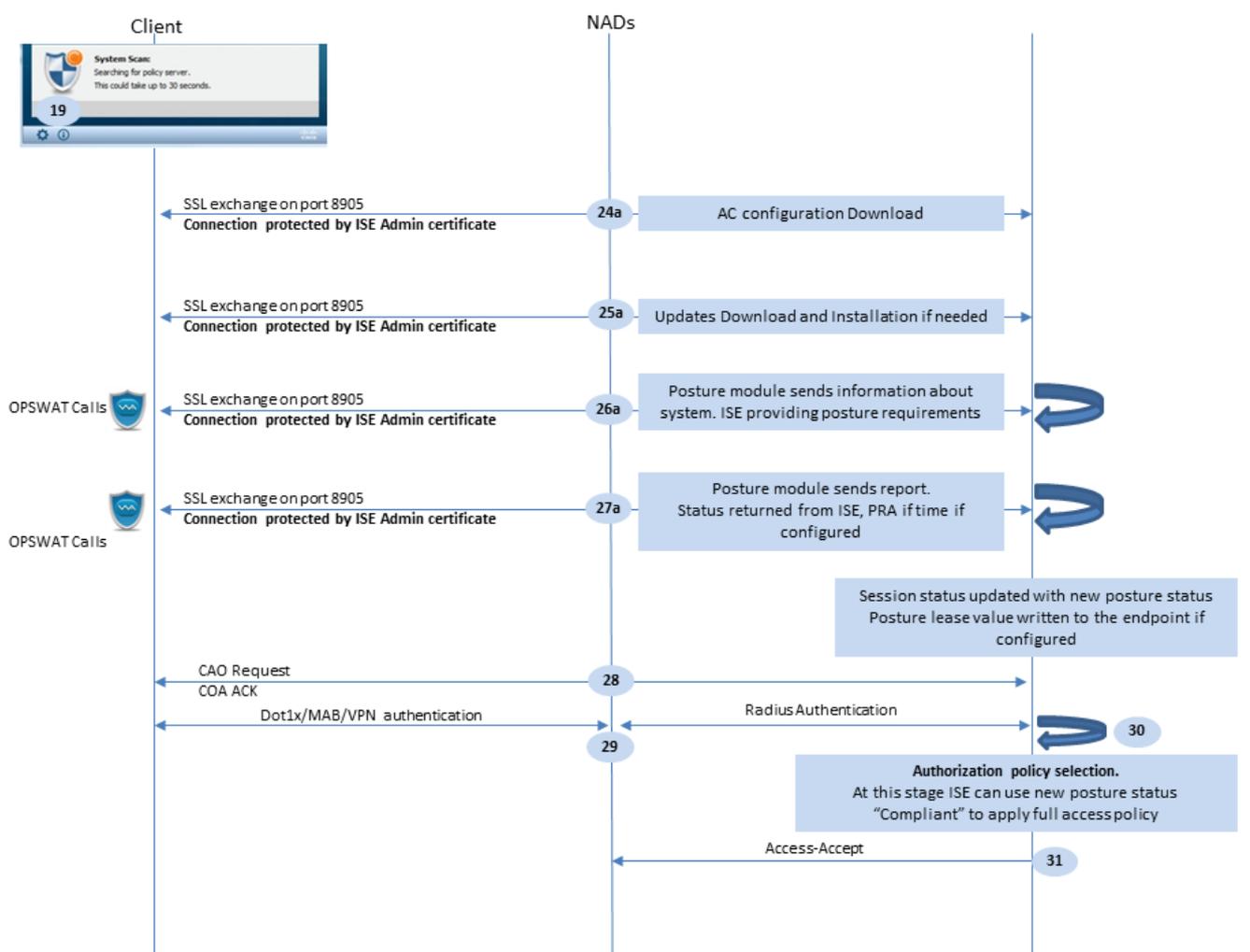


圖1-4

步驟24.AC ISE終端安全評估模組配置從ISE下載。

步驟25.如有需要，更新下載和安裝。

步驟 26.AC ISE終端安全評估模組收集有關系統的初始資訊（如作業系統版本、已安裝的安全產品及其定義版本）。在這個階段，AC ISE終端安全評估模組包括OPSWAT API來收集有關安全產品的資訊。收集的資料將傳送到ISE。作為對此請求的回覆，ISE提供終端安全評估要求清單。需求清單是狀態策略處理的結果。為了匹配正確的策略，ISE使用裝置OS版本（存在於請求中）和會話ID值選擇其他所需的屬性（AD/LDAP組）。會話ID值也由客戶端傳送。

步驟 27.在此步驟中，客戶端涉及OPSWAT呼叫和其他機制來檢查終端安全評估要求。將包含要求清單及其狀態的最終報告傳送到ISE。ISE需要對終端合規性狀態做出最終決定。如果終結點在此步驟中標籤為不相容，將返回一組補救操作。對於符合策略的端點，ISE將符合性狀態寫入會話，並在配置終端安全評估租賃時將最後一個安全評估時間戳設定為終端屬性。終端安全評估結果將傳送回終端。在這種情況下，PRA的終端安全評估(PRA)時間也由ISE置於此封包中。

在不符合的情況下，請考慮以下幾點：

- 某些補救操作（如顯示文本消息、連結補救、檔案補救等）由狀態代理本身執行。
- 其他補救型別(例如AV、AS、WSUS和SCCM)要求終端安全評估代理和目標產品之間進行OPSWAT API通訊。在此場景中，終端安全評估代理僅向產品傳送補救請求。補救本身由安全產品直接執行。

---

 注意：如果安全產品必須與外部資源（內部/外部更新伺服器）通訊，則必須確保在Redirect-ACL/DACL中允許此通訊。

---

步驟28.ISE向NAD傳送COA請求，NAD必須為使用者觸發新身份驗證。NAD必須通過COA ACK確認此請求。請記住，對於VPN案例，使用COA推送，因此不會傳送新的身份驗證請求。相反，ASA從會話中刪除以前的授權引數（重定向URL、重定向ACL和DACL）並從COA請求應用新引數。

步驟29.使用者的新身份驗證請求。

重要注意事項：

- 對於思科NAD COA，ISE使用reauth，這指示NAD使用以前的會話ID啟動新的身份驗證請求。
- 在ISE端，相同的會話ID值表示必須重複使用以前收集的會話屬性（在本案例中是投訴狀態），並且必須分配基於這些屬性的新授權配置檔案。
- 如果會話ID發生更改，此連線將被視為新連線，並重新啟動整個狀態進程。
- 為了避免重新設定安全狀態 每次更改會話id時，都可以使用狀態租用。在此場景中，終端屬性中儲存有關終端狀態的資訊，即使會話ID為ts已更改。

步驟 30.在ISE端根據終端安全評估狀態選擇新的授權策略。

步驟 31.具有新授權屬性的Access-Accept將傳送到NAD。

下一個流程描述了以下場景：任何終端安全評估探測均未檢索到重定向URL（用字母b標籤），並且上次探測已查詢之前連線的PSN。此處的所有步驟與重新導向URL的情況完全相同，除了作為探測4的結果由PSN返回的重放。如果此探測器著陸到當前身份驗證會話的所有者同一個PSN上，則重放將包含會話ID值，狀態代理稍後將使用該值完成該過程。如果先前連線的頭端與當前會話所有者不同，會話查詢將失敗，並向AC ISE終端安全評估模組返回空響應。最終結果是，No Policy Server Detected 將消息返回給終端使用者。

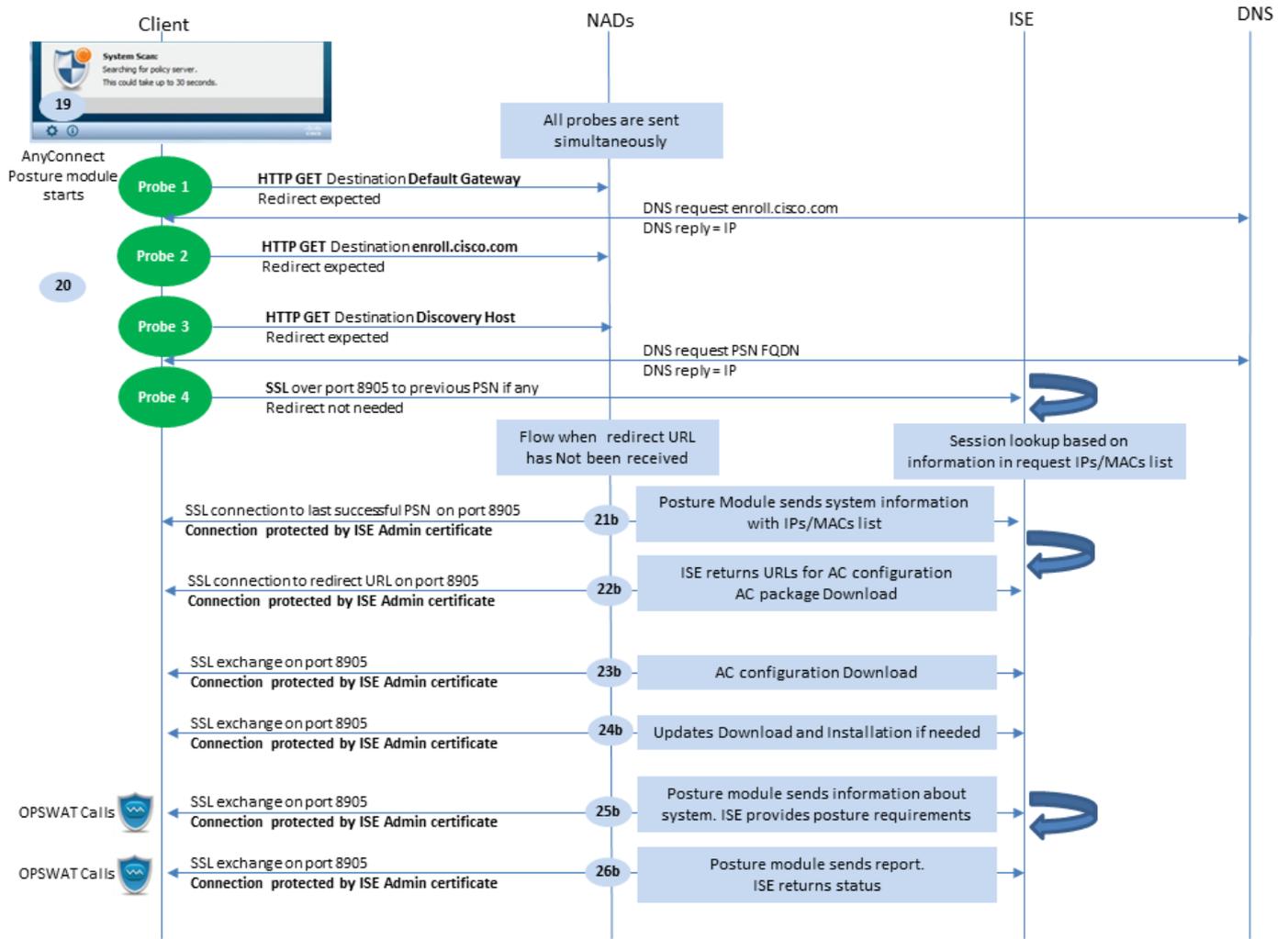


圖1-5

## ISE狀態流量後2.2

ISE 2.2和更新版本同時支援重定向和無重定向流。 以下是無重定向狀態流的詳細解釋：

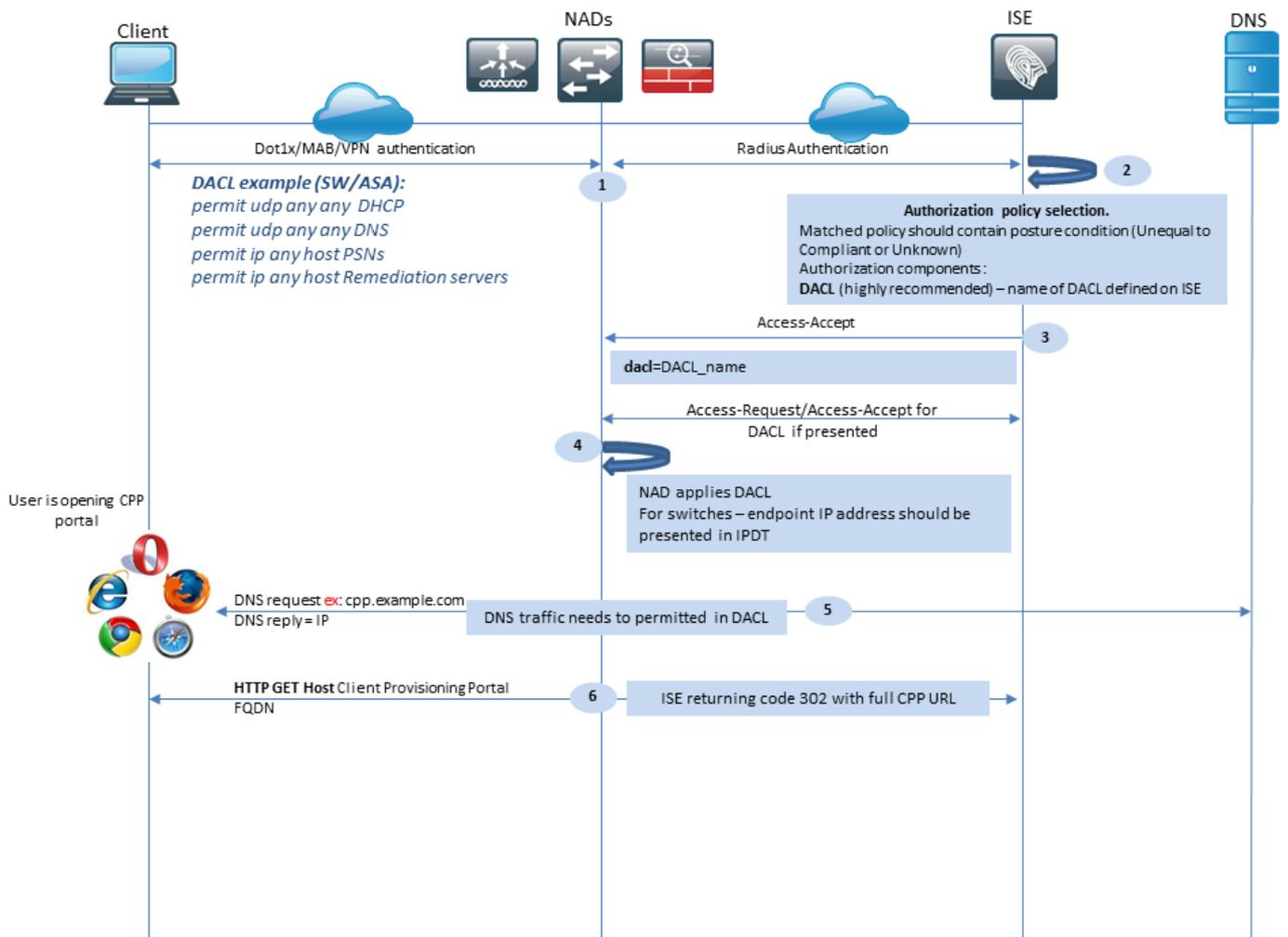


圖2-1

步驟1.身份驗證是流程的第一步。它可以是dot1x、MAB或VPN。

步驟2.ISE必須為使用者選擇身份驗證和授權策略。在終端安全評估中，方案選擇的授權策略必須包含對終端安全評估狀態的引用，該引用最初必須為未知或不適用。為了同時涵蓋這兩種情況，可以使用狀況狀態不等的合規性條件。對於無重定向的安全狀態，無需在授權配置檔案中使用任何Web重定向配置。當終端安全評估狀態不可用時，您仍可以考慮使用DACL或空域ACL來限制使用者訪問。

步驟3.ISE返回具有授權屬性的Access-Accept。

步驟 4. 如果在Access-Accept中返回DACL名稱，則NAD會啟動DACL內容下載，並在獲得授權配置檔案後將其應用到會話。

步驟 5.新方法假設無法進行重定向，因此使用者必須手動輸入客戶端調配門戶FQDN。必須在ISE端的門戶配置中定義CPP門戶的FQDN。從DNS伺服器的角度來看，A-record必須指向已啟用PSN角色的ISE伺服器。

步驟 6.客戶端傳送HTTP以獲取客戶端調配門戶FQDN，在ISE端分析此請求，並將完整的門戶URL返回給客戶端。

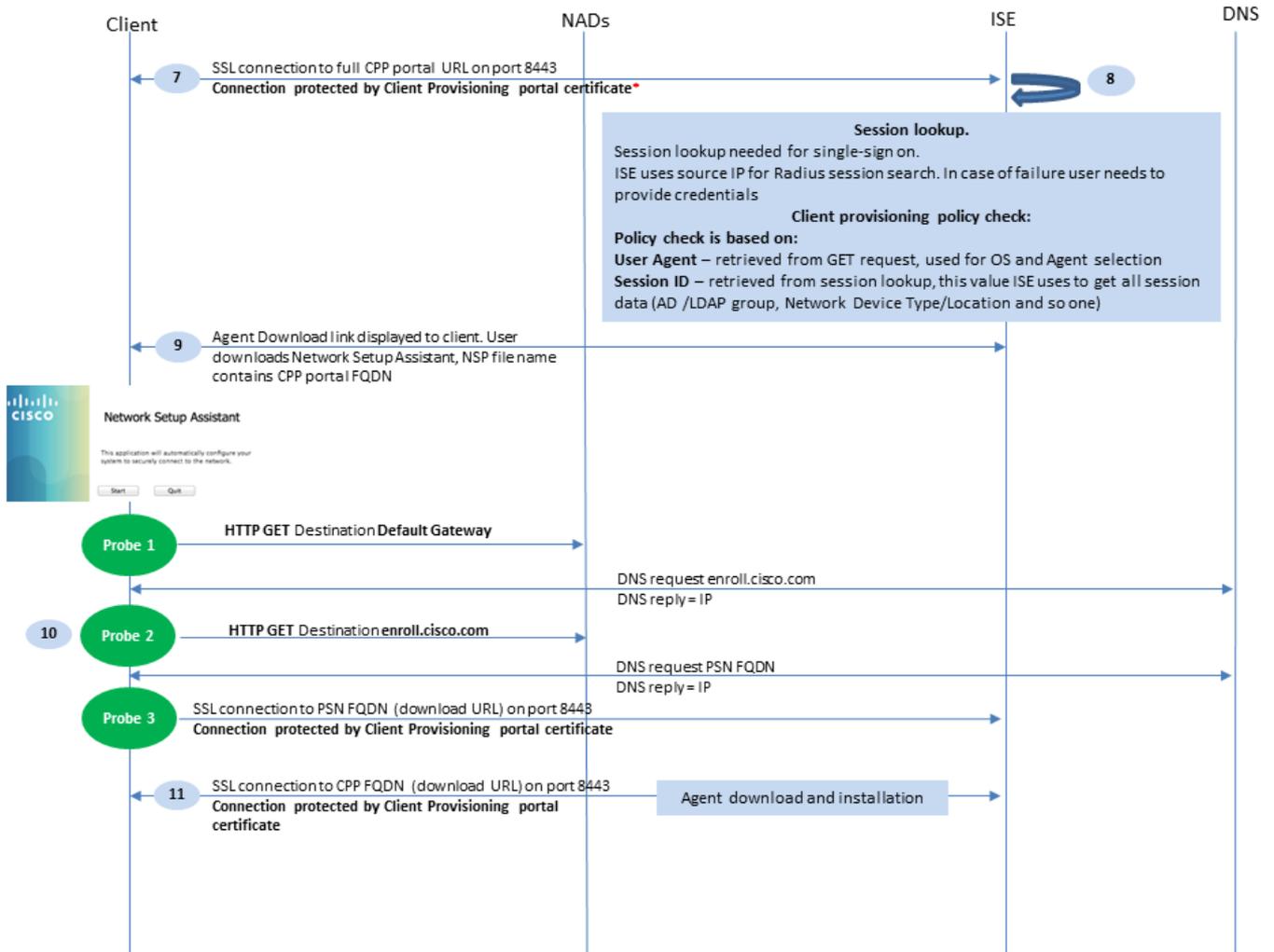


圖2-2

步驟7.通過重定向URL中接收的埠建立SSL連線（預設8443）。此連線受來自ISE端的門戶證書保護。客戶端調配門戶(CPP)呈現給使用者。

步驟 8. 在此步驟中，在ISE上發生兩個事件：

- 單一登入(SSO)- ISE嘗試查詢以前成功的身份驗證。ISE使用資料包的源IP地址作為即時RADIUS會話的搜尋過濾器。

**注意：**根據資料包中的源IP與會話中的已框架化IP地址之間的匹配檢索會話。框架的IP地址通常由ISE從臨時記帳更新中檢索，因此需要在NAD端啟用記帳。此外，您必須記住，SSO僅在擁有會話的節點上可用。例如，如果會話在PSN 1上進行身份驗證，但FQDN本身指向PSN2，則SSO機制將失敗。

- 客戶端調配策略查詢 — 在成功的SSO的情況下，ISE可以使用來自身份驗證會話的資料和來自客戶端瀏覽器的使用者代理。如果SSO失敗，使用者必須提供憑據，並且從內部和外部身份庫（AD/LDAP/內部組）中檢索使用者身份驗證資訊後，該資訊可用於客戶端調配策略檢查。

 注意：由於思科錯誤ID [CSCvd11574](#)，當外部使用者是新增到外部身份儲存配置中的多個AD/LDAP組成員時，在選擇非SSO案例的客戶端調配策略時會顯示錯誤。所提到的缺陷是從ISE 2.3 FCS開始修復的，並且修復要求在AD組而不是EQUAL的條件下使用CONTAINS。

步驟 9. 選擇客戶端調配策略後，ISE向使用者顯示代理下載URL。點選下載NSA後，該應用程式會被推送給使用者。NSA檔名包含CPP門戶的FQDN。

步驟10.在此步驟中，NSA運行探測來建立與ISE的連線。兩個探測器是傳統探測器，第三個探測器旨在允許在不進行url重定向的環境中的ISE發現。

- NSA將第一個發現探測 — HTTP /auth/discovery傳送到預設網關。NSA預期結果為redirect-url。
- 如果第一個探測失敗，NSA會傳送第二個探測。第二個探測是HTTP GET /auth/discovery enroll.cisco.com. 此FQDN必須由DNS伺服器成功解析。在具有拆分隧道的VPN場景中，到 enroll.cisco.com 必須通過隧道路由。
- NSA通過CPP門戶埠將第三個探測傳送到客戶端調配門戶FQDN。此請求包含有關門戶會話ID的資訊，允許ISE確定必須提供哪些資源。

步驟 11. NSA下載Anyconnect和/或特定模組。下載過程通過客戶端調配門戶埠完成。

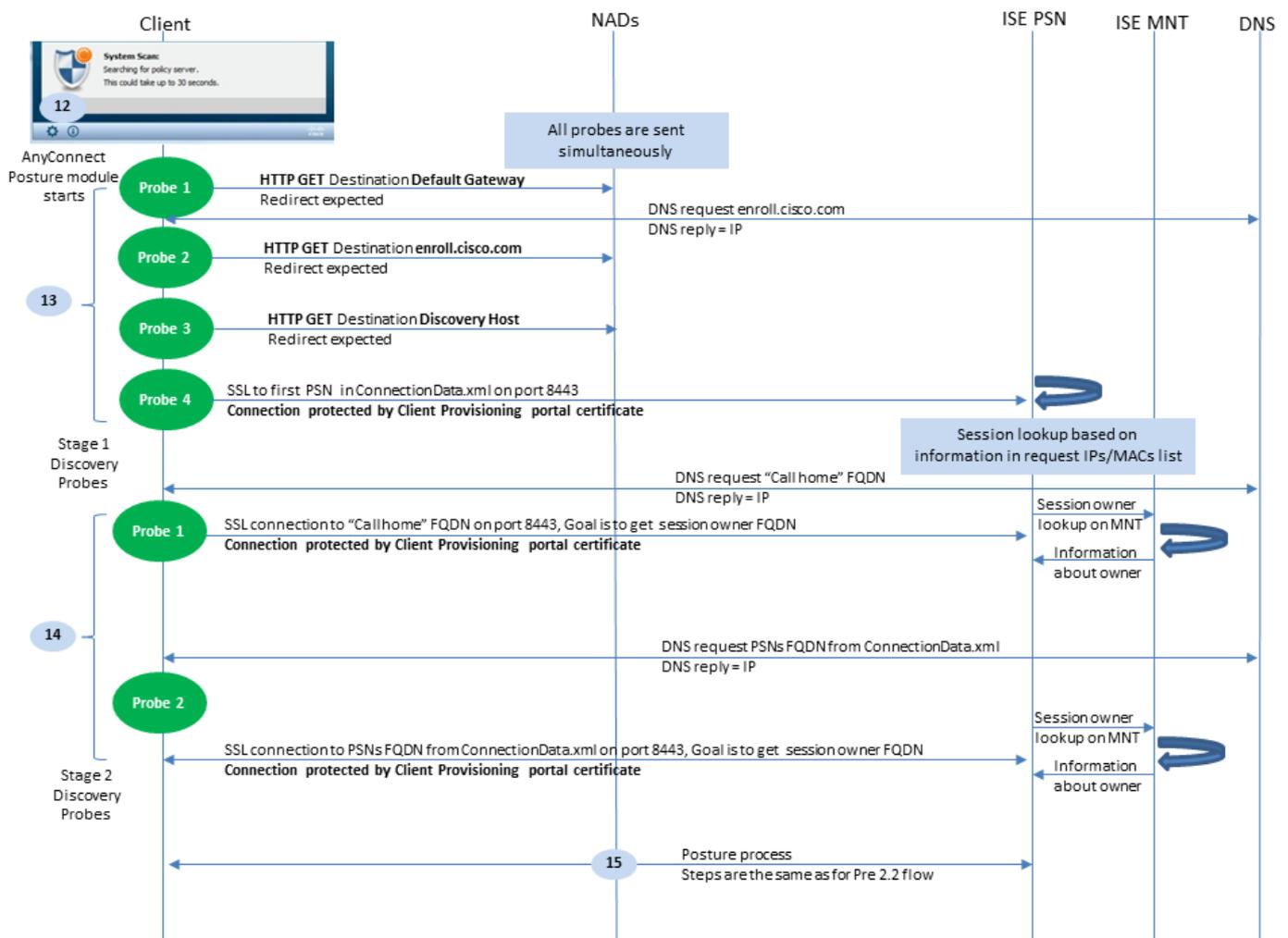


圖2-3

步驟 12. 在ISE 2.2中，終端安全評估過程分為兩個階段。第一階段包含一組傳統的狀態發現探測器，以支援與依賴於url重定向的部署的後向相容性。

步驟13. 第一階段包含所有傳統的狀態發現探測。要獲取有關探測的更多詳細資訊，請檢視ISE 2.2之前的狀態流中的步驟20。

步驟14. 階段二包含兩個發現探測，允許AC ISE終端安全評估模組建立到PSN的連線，其中會話在不支援重定向的環境中進行身份驗證。在階段2中，所有探測器都是按順序進行的。

- 探測1 — 在第一個探測期間，AC ISE終端安全評估模組嘗試使用「呼叫總部清單」中的IP/FQDN建立。必須在ISE端的AC狀態配置檔案中配置探測的目標清單。您可以定義IP/FQDN（用逗號分隔），可以使用冒號定義每個Call Home目標的埠號。此埠必須等於運行客戶端調配門戶的埠。在客戶端，有關呼叫總部伺服器的資訊位於 ISEPostureCFG.xml，此檔案可以在資料夾 — C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

如果call home目標不擁有會話，則在此階段需要查詢所有者。AC ISE終端安全評估模組指示ISE使用特定目標URL開始所有者查詢 — /auth/ng-discovery 請求。還包含客戶端IP和MAC清單。PSN會話收到此消息後，首先在本地執行查詢（此查詢使用來自AC ISE終端安全評估模組傳送的請求的IP和MAC）。如果未找到會話，PSN將啟動MNT節點查詢。此請求僅包含MACs清單，因此，必須從MNT獲取所有者的FQDN。之後，PSN將所有者FQDN返回給客戶端。來自客戶端的下一個請求將傳送到會話所有者FQDN，身份驗證/狀態位於URL以及IP和MAC清單中。

- 探測2 — 在此階段，AC ISE終端安全評估模組嘗試位於以下位置的PSN FQDN ConnectionData.xml. 您可以在以下位置找到此檔案：

C:\Users\  
          \AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client\

.AC ISE終端安全評估模組在第一次終端安全評估嘗試後建立此檔案。該檔案包含ISE PSN FQDN清單。清單的內容可以在下一次連線嘗試期間動態更新。此探測的最終目標是獲取當前會話所有者的FQDN。實現方式與探測1相同。在探測目標選擇方面，唯一的區別是。如果多個使用者使用裝置，則檔案本身位於當前使用者的資料夾中。其他使用者無法使用此檔案中的資訊。這會導致使用者在不指定Call home目標的情況下在不重定向的情況下發現環境中的雞和蛋問題。

步驟 15. 獲得有關會話所有者的資訊後，所有後續步驟都與ISE 2.2之前的流程相同。

## 設定

本文檔將ASA v用作網路接入裝置。所有測試均通過VPN進行狀態測試。通過VPN支援安全狀態的ASA配置不在本檔案的範圍之內。有關詳細資訊，請參閱[ASA 9.2.1版VPN安全評估和ISE配置示例](#)。

---

 注意：對於使用VPN使用者的部署，推薦的設定是基於重定向的安全狀態。建議不要配置呼叫

---

者。對於所有基於VPN的使用者，確保應用DACL以便他們不與配置終端安全評估的PSN通訊。

## 網路圖表

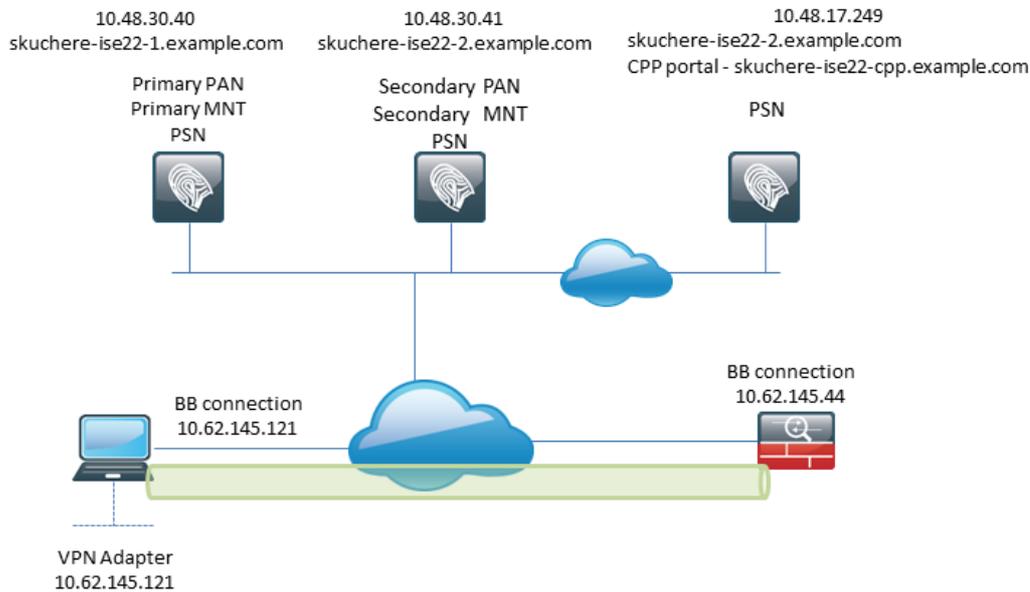


圖3-1

此拓撲用於測試。使用ASA，由於NAT功能，可以輕鬆模擬客戶端調配門戶的SSO機制在PSN端發生故障時的場景。對於通過VPN的常規狀態流量，SSO必須正常工作，因為當使用者進入公司網路時，通常不會對VPN IP實施NAT。

## 組態

### 客戶端調配配置

以下是準備Anyconnect配置的步驟。

步驟 1. Anyconnect軟體包下載。Anyconnect軟體包本身無法從ISE直接下載，因此開始之前，請確保您的PC上有AC。此連結可用於AC下載 —

<https://www.cisco.com/site/us/en/products/security/secure-client/index.html>。在本檔案中，anyconnect-win-4.4.00243-webdeploy-k9.pkg 已使用包。

步驟 2. 若要將AC包上傳到ISE，請導航至 Policy > Policy Elements > Results > Client Provisioning > Resources 然後按一下 Add. 從本地磁碟中選擇Agent resources。在新視窗中，選擇 Cisco Provided Packages，按一下 browse 並選擇PC上的AC軟體包。

### Agent Resources From Local Disk

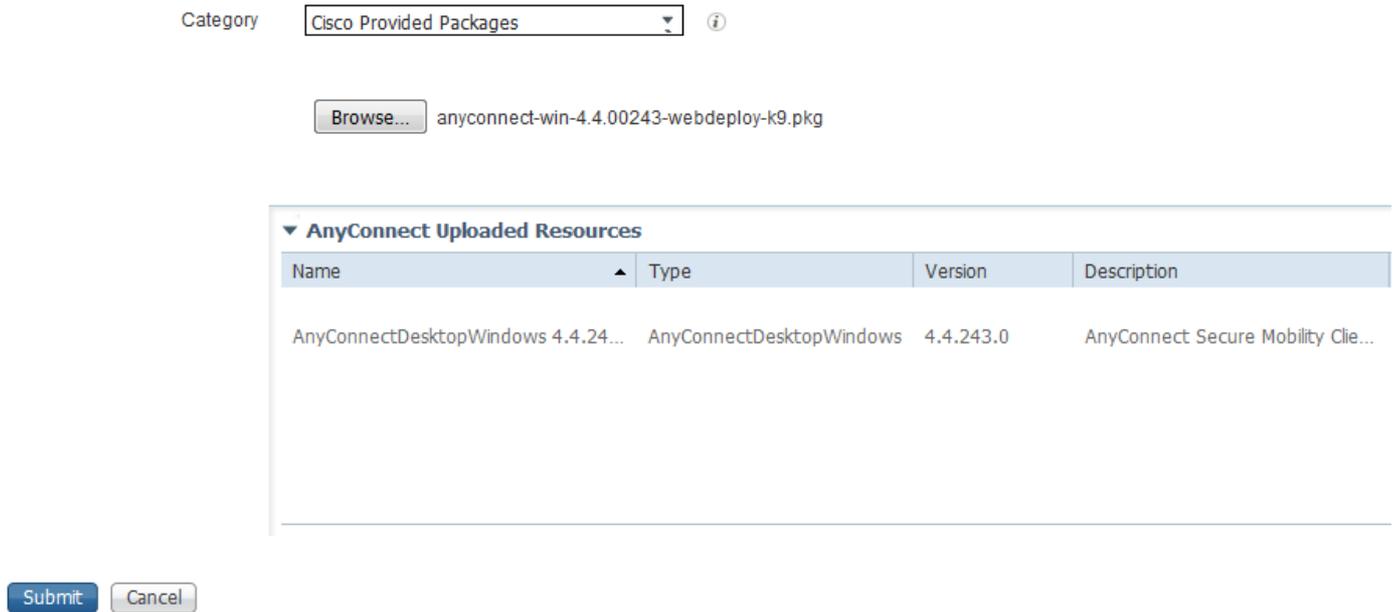


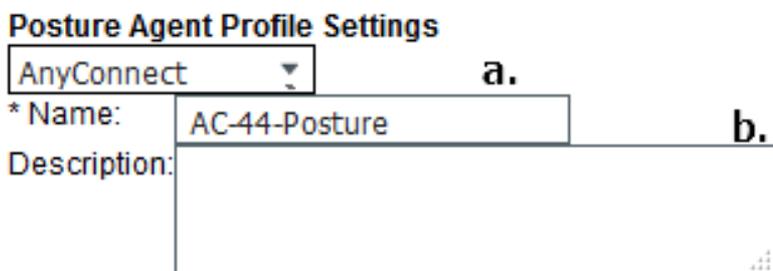
圖3-2

按一下 **Submit** 以完成匯入。

步驟 3. 合規性模組必須上傳到ISE。在同一頁上，按一下 **Add** 並選擇 **Agent resources from Cisco site**. 在資源清單中，必須檢查符合性模組。在本檔案中， **AnyConnectComplianceModuleWindows 4.2.508.0** 使用遵從性模組。

步驟 4. 現在必須建立AC狀態配置檔案。按一下 **Add** 並選擇 **NAC agent or Anyconnect posture profile**.

### ISE Posture Agent Profile Settings > New Profile



### Agent Behavior

圖3-3

- 選擇配置檔案的型別。此案例必須使用AnyConnect。
- 指定配置檔名稱。導航至 **Posture Protocol** 剖面的截面。

## 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="*"/> <b>a.</b>	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>b.</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.

圖3-4

- 指定 Server Name Rules，此欄位不能為空。該欄位可以包含帶有萬用字元的FQDN，該萬用字元限制從相應名稱空間到PSN的AC ISE終端安全評估模組連線。如果必須允許任何FQDN，請放置星號。
- 此處指定的名稱和IP正在狀態發現的第2階段使用。您可以按逗號分隔名稱，也可以使用冒號在FQDN/IP之後新增埠號。如果AC使用GPO或任何其他軟體調配系統部署帶外（不是從ISE客戶端調配門戶），且存在呼叫總部地址時，AC變得至關重要，因為只有一次探測可以成功到達ISE PSN。這意味著在帶外AC調配的情況下，管理員必須使用AC配置檔案編輯器建立AC ISE終端安全評估配置檔案，並隨交流安裝調配此檔案。

 **注意：**請記住，Call home地址的存在對於多使用者PC至關重要。檢視步驟14.在ISE 2.2之後的狀態流程中。

**步驟5.建立交流電配置。** 導航至 Policy > Policy Elements > Results > Client Provisioning > Resources 中，按一下 Add，然後選擇 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

Diagnostic and Reporting Tool

---

**Profile Selection**

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

圖3-5

- 選擇AC包。
- 提供AC配置名稱。
- 選擇合規性模組版本。
- 從下拉選單中選擇AC狀態配置檔案。

步驟 6. 配置客戶端調配策略。導航至 Policy > Client Provisioning. 如果是初始配置，則可以在預設策略中填充空值。如果您需要將策略新增到現有的終端安全評估配置，請導航到可重用的策略並選擇 Duplicate Above 或 Duplicate Below . 也可以建立全新的策略。

這是文檔中使用的策略示例。

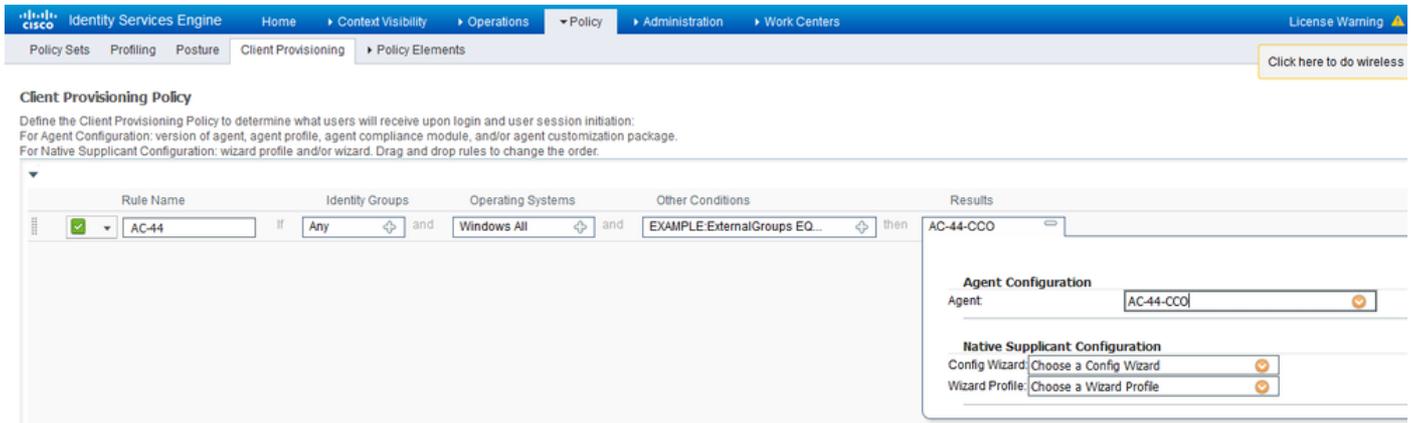


圖3-6

在結果部分選擇您的AC配置。請記住，在SSO失敗的情況下，ISE只能擁有從登入到門戶的屬性。這些屬性僅限於可從內部和外部身份儲存庫中檢索到的有關使用者的資訊。在本文檔中，AD組用作客戶端調配策略中的條件。

### 終端安全評估策略和條件

使用簡單的狀態檢查。ISE配置為檢查終端裝置端的Window Defender服務的狀態。實際場景可能更為複雜，但一般配置步驟是相同的。

步驟 1. 建立狀態條件。安全狀態條件位於 Policy > Policy Elements > Conditions > Posture。選擇狀態條件的型別。以下是必須檢查Windows Defender服務是否正在運行的服務條件示例。

## 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"/>

圖3-7

步驟2.狀態要求配置。導航至 Policy > Policy Elements > Results > Posture > Requirements. 以下是「視窗保護器」檢查的示例：



圖3-8

在新要求中選擇您的狀態條件並指定補救操作。

步驟 3. 狀態策略配置。導航至 Policy > Posture. 您可以在此處找到用於本文檔的策略的示例。策略將 Windows Defender 要求指定為強制要求，並且僅包含外部AD組名稱作為條件。

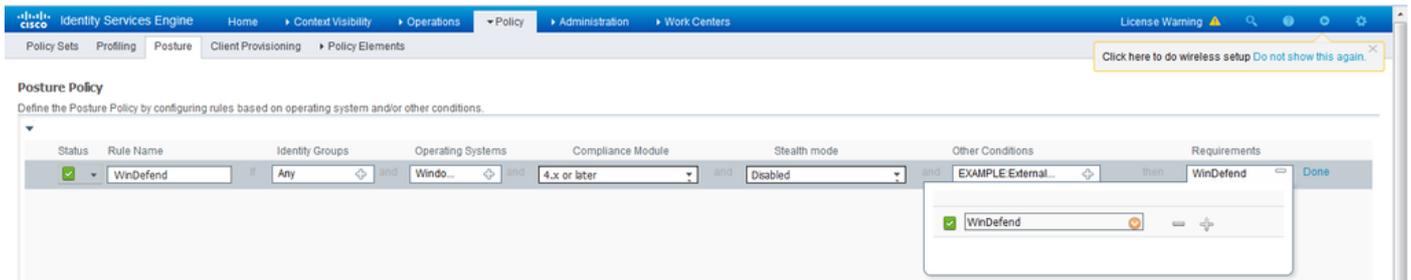


圖3-9

## 配置客戶端調配門戶

對於無重定向的安全狀態，必須編輯客戶端調配門戶的配置。導航至 Administration > Device Portal Management > Client Provisioning. 您可以使用預設門戶，也可以建立您自己的門戶。相同入口可用於有重定向和無重定向兩種姿勢。

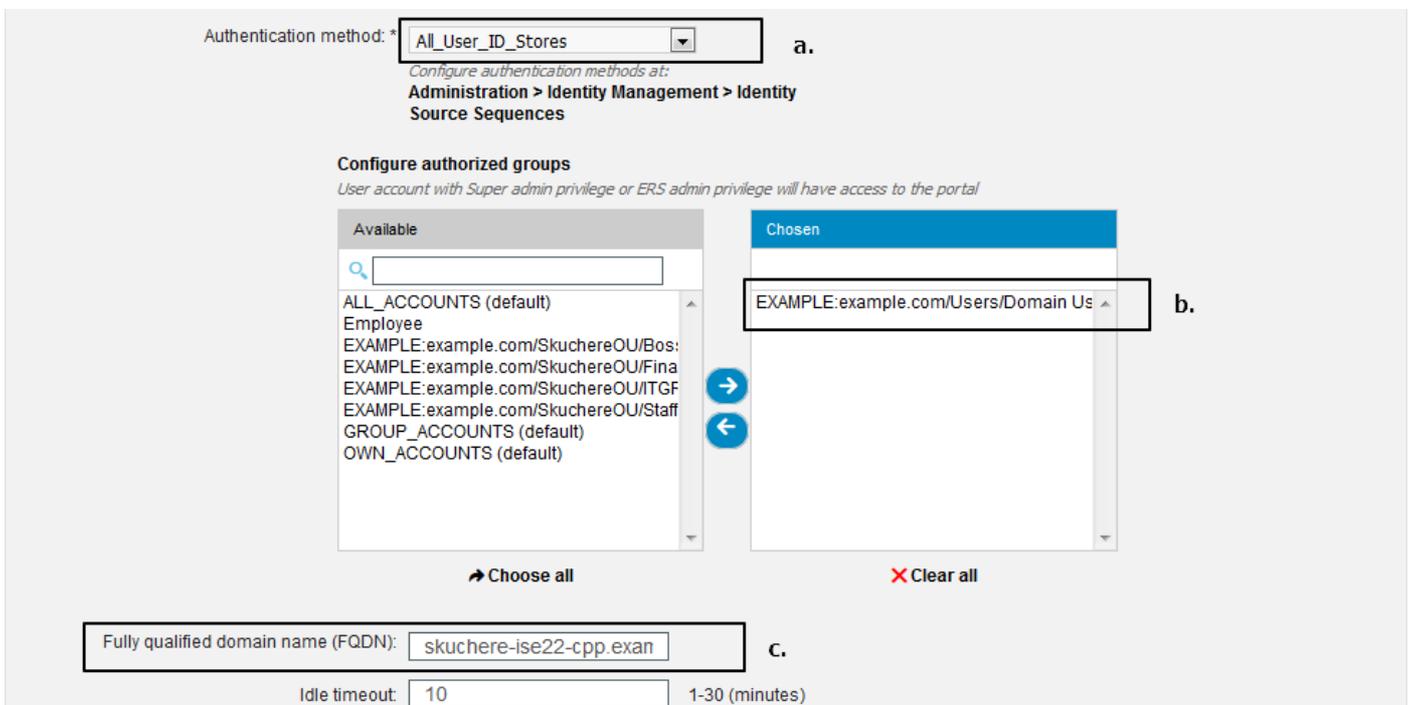


圖3-10

必須在非重定向方案的門戶配置中編輯這些設定：

- 在身份驗證中，指定SSO找不到使用者會話時必須使用的身份源序列。
- 根據選定的身份源序列，填充可用組的清單。此時，您必須選擇授權進行門戶登入的組。
- 當需要從客戶端調配門戶部署AC時，必須為方案指定客戶端調配門戶的FQDN。此FQDN必須可解析為ISE PSN IP。在第一次嘗試連線期間，必須指示使用者在Web瀏覽器中指定FQDN。

## 配置授權配置檔案和策略

當終端安全評估狀態不可用時，必須限制客戶端的初始訪問。這可以通過多種方式實現：

- **DAACL分配** — 在限制訪問階段，可以將DAACL分配給使用者以限制訪問。此方法可用於Cisco網路接入裝置。
- **VLAN分配** — 在成功的安全評估使用者能夠置於受限制的VLAN之前，此方法對於幾乎所有NAD供應商都必須運行良好。
- **Radius Filter-Id** — 使用此屬性，可以將NAD上本地定義的ACL分配給狀態未知的使用者。由於這是標準RFC屬性，因此此方法必須適用於所有NAD供應商。

步驟 1. 配置DAACL。由於此示例基於ASA，因此可以使用NAD DAACL。對於實際案例，您必須考慮將VLAN或Filter-ID作為可能的選項。

要建立DAACL，請導航至 [Policy > Policy Elements > Results > Authorization > Downloadable ACLs](#) 然後按一下 **Add**。

在未知狀態期間，必須至少提供以下許可權：

- DNS流量
- DHCP流量
- 到ISE PSN的流量(埠80和443，用於開啟門戶的友好FQDN。運行CP門戶的埠預設為8443，埠8905為向後相容)
- 必要時流向補救伺服器的流量

以下是沒有修正伺服器的DAACL範例：

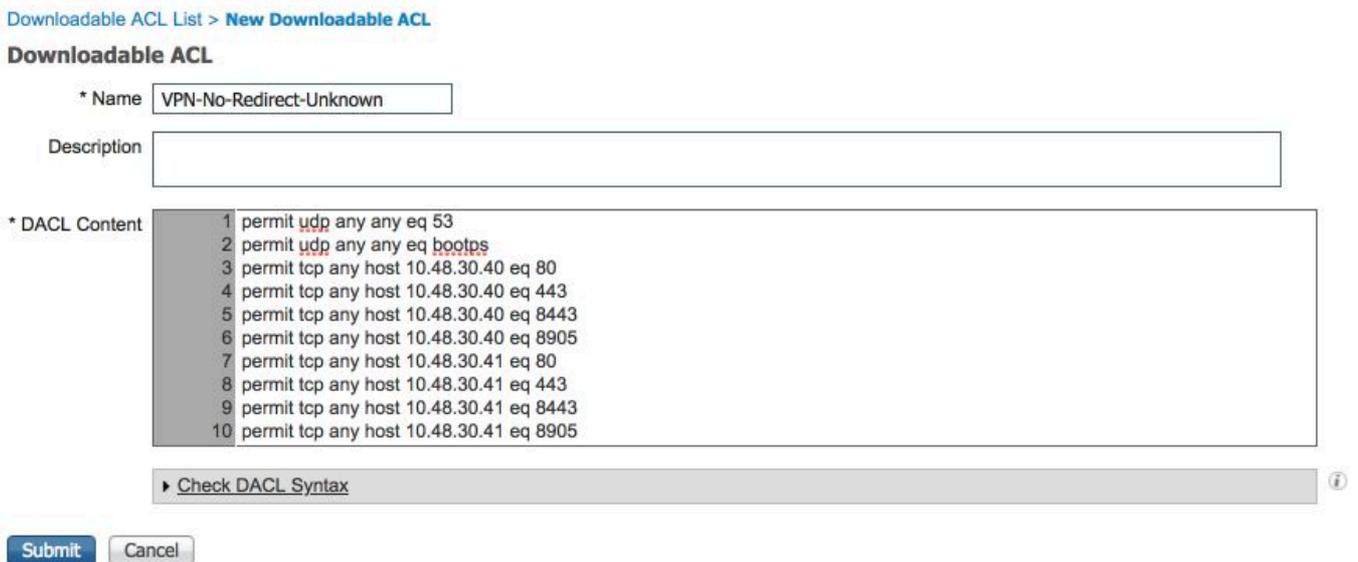


圖3-11

步驟 2. 配置授權配置檔案。

與往常一樣，安全狀態需要兩個授權配置檔案。第一個必須包含任何型別的網路訪問限制（本示例中使用了DAACL配置檔案）。此配置檔案可應用於狀態不等於合規性的身份驗證。第二個授權配置檔案可以只包含允許訪問，並且可以應用於狀態等於合規性的會話。

要建立授權配置檔案，請導航至 [Policy > Policy Elements > Results > Authorization > Authorization Profiles](#)。

受限訪問配置檔案示例：

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

圖3-12

在本示例中，預設的ISE配置檔案PermitAccess用於成功狀態檢查後的會話。

步驟 3.配置授權策略。在此步驟中，必須建立兩個授權策略。一個是匹配初始身份驗證請求與未知狀態匹配，另一個是在成功狀態過程後分配完全訪問許可權。

以下是適用於此案例的簡單授權原則範例：

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

圖3-13

身份驗證策略的配置不是本文檔的一部分，但您必須記住，在授權策略處理成功身份驗證之前，必須執行此步驟。

## 驗證

基本驗證流程可包含三個主要步驟：

### 步驟 1. 驗證流驗證。

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	

圖4-1

1. 初始身份驗證。對於此步驟，您可能會對已應用授權配置檔案的驗證感興趣。如果已應用意外授權配置檔案，請調查詳細的身份驗證報告。您可以通過按一下「詳細資訊」列中的放大鏡來開啟此報告。您可以將詳細身份驗證報告中的屬性與授權策略中預期匹配的條件進行比較。
2. DACL下載事件。僅當為初始身份驗證選擇的授權配置檔案包含DACL名稱時，才會顯示此字串。
3. Portal authentication — 流中的此步驟表示SSO機制找不到使用者會話。發生這種情況的原因有多種：
  - 未將NAD配置為傳送記帳消息或其中不存在已框架的IP地址
  - CPP門戶FQDN已解析為ISE節點的IP，與處理初始身份驗證的節點不同
  - 客戶端位於NAT之後

4. 會話資料更改。在此特定示例中，會話狀態已從「未知」更改為「相容」。
5. 網路接入裝置的COA。此COA必須成功從NAD端推送新身份驗證，並在ISE端推送新授權策略分配。如果COA失敗，您可以開啟詳細報告以調查原因。COA最常見的問題包括：
  - COA超時 — 在這種情況下，已傳送請求的PSN未配置為NAD端的COA客戶端，或者COA請求已在途中的某個位置被丟棄。
  - COA負ACK — 表示NAD已接收COA，但由於某種原因無法確認COA操作。對於此情況，詳細報告必須包含更詳細的說明。

由於本示例將ASA用作NAD，因此您看不到使用者的後續身份驗證請求。這是因為ISE使用ASA的COA推送避免了VPN服務中斷。在這種情況下，COA本身包含新的授權引數，因此不需要重新身份驗證。

步驟2. 客戶端調配策略選擇驗證 — 為此，您可以在ISE上運行報告，該報告可幫助您瞭解為使用者應用了哪些客戶端調配策略。

導航至 [Operations > Reports Endpoint and Users > Client Provisioning](#) 並運行所需日期的報告。

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	

圖4-2

通過此報告，您可以驗證選擇了哪個客戶端調配策略。此外，如果出現故障，必須在中說明原因。Failure Reason 列。

步驟3. 狀態報告驗證 — 導航至 [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-bit
2017-02-23 19:33:35...	✓		user1	00:0B:7F:D0:F8:F4	10.62.145.44	Windows 7 Professional 64-bit

圖4-3

您可以從此處開啟每個特定事件的詳細報告，以檢查該報告所屬的會話ID、ISE為終端選擇的確切狀態要求以及每個要求的狀態。

## 疑難排解

## 一般資訊

為了進行終端安全評估流程故障排除，必須啟用這些ISE元件以在可以發生終端安全評估流程的ISE節點上進行調試：

- client-webapp — 負責代理程式調配的元件。目標日誌檔案 `guest.log` 和 `ise-psc.log`。
- guestaccess — 負責客戶端調配門戶元件和會話所有者查詢的元件（當請求指向錯誤的PSN時）。目標日誌檔案 — `guest.log`。
- provisioning — 負責客戶端調配策略處理的元件。目標日誌檔案 — `guest.log`。
- posture — 所有狀態相關事件。目標日誌檔案 — `ise-psc.log`。

對於客戶端故障排除，可以使用以下命令：

- `acisensa.log` — 如果客戶端上的客戶端調配失敗，則此檔案會在下載NSA的同一資料夾中建立（通常為Windows下載目錄）。
- `AnyConnect_ISEPosture.txt` — 此檔案可以在目錄中的DART捆綁包中找到 `Cisco AnyConnect ISE Posture Module`。所有有關ISE PSN發現和狀態流程常規步驟的資訊均記錄在此檔案中。

## 常見問題故障排除

### SSO相關問題

如果SSO成功，您可以在以下位置檢視這些消息：`ise-psc.log`，此組消息表示會話查詢已成功完成，並且可以跳過門戶上的身份驗證。

```
<#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
```

```
Found session c0a801010002600058232bb8 using ipAddr 10.62.145.121
```

### 文本視窗5-1

您可以使用終端IP地址作為搜尋金鑰來查詢此資訊。

稍後，在訪客日誌中，您必須看到已跳過身份驗證：

<#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
```

### 文本視窗5-2

如果SSO不起作用， ise-psc log 檔案包含有關會話查詢失敗的資訊：

<#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
```

### 文本視窗5-3

在 guest.log 在這種情況下，您必須在門戶上看到完整的使用者身份驗證：

<#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
```

### 文本視窗5-4

如果門戶上的身份驗證失敗，您必須專注於門戶配置驗證 — 哪個身份儲存正在使用中？哪些組有權

登入？

## 客戶端調配策略選擇故障排除

如果客戶端調配策略失敗或策略處理不正確，您可以檢查 `guest.log` 檔案以瞭解更多詳細資訊：

<#root>

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.C

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 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][] guestaccess.flowmanager.step.guest.

:user1:- CP Policy Status =SUCCESS, needToDoVlan=false, CoaAction=NO_COA
```

### 文本視窗5-5

在第一個字串中，您可以看到如何將有關會話的資訊注入到策略選擇引擎中，如果沒有策略匹配或不正確的策略匹配，您可以將此處的屬性與客戶端調配策略配置進行比較。最後一個字串表示策略選擇狀態。

## 狀態過程故障排除

在客戶端，您必須關注探測器及其結果的調查。以下是成功的第1階段探測的範例：

\*\*\*\*\*

```
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..
```

\*\*\*\*\*

## 文本視窗5-6

在這個階段，PSN將返回有關會話所有者的AC資訊。稍後您可以看到以下幾條消息：

```
*****  
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..  
  
*****
```

## 文本視窗5-7

會話所有者將所需的所有資訊返回給座席：

```
*****  
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>
.
*****
```

### 文本視窗5-8

從PSN方面，您可以集中精力處理 `guest.log` 當您預期到達節點的初始請求不擁有會話時：

```
<#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
```

## 文本視窗5-9

在這裡，您可以看到PSN首先嘗試在本地查詢會話，並在失敗後使用IP和MAC清單向MNT發起請求以查詢會話所有者。

稍後，您必須在正確的PSN上看到來自客戶端的請求：

```
<#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 Addr [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
```

## 文本視窗5-10

下一步，PSN將為此會話執行客戶端調配策略查詢：

```
<#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
```

## 文本視窗5-11

在下一步中，您可以看到終端安全評估需求選擇的過程。在步驟結束時，將準備一個要求清單並返回給代理：

```
<#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 18:00:03,884 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>
```

### 文本視窗5-12

稍後，您可以看到PSN已收到狀態報告：

```
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
```

### 文本視窗5-13

在流程結束時，ISE將終端標籤為符合併啟動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
```

### 文本視窗5-14

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。