使用iPEP ISE和ASA的VPN內聯狀態

目錄

簡介

本文提供有關如何使用自適應安全裝置(ASA)和身份服務引擎(ISE)設定內聯狀態的資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於ASA版本8.2(4)和ISE版本1.1.0.665。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

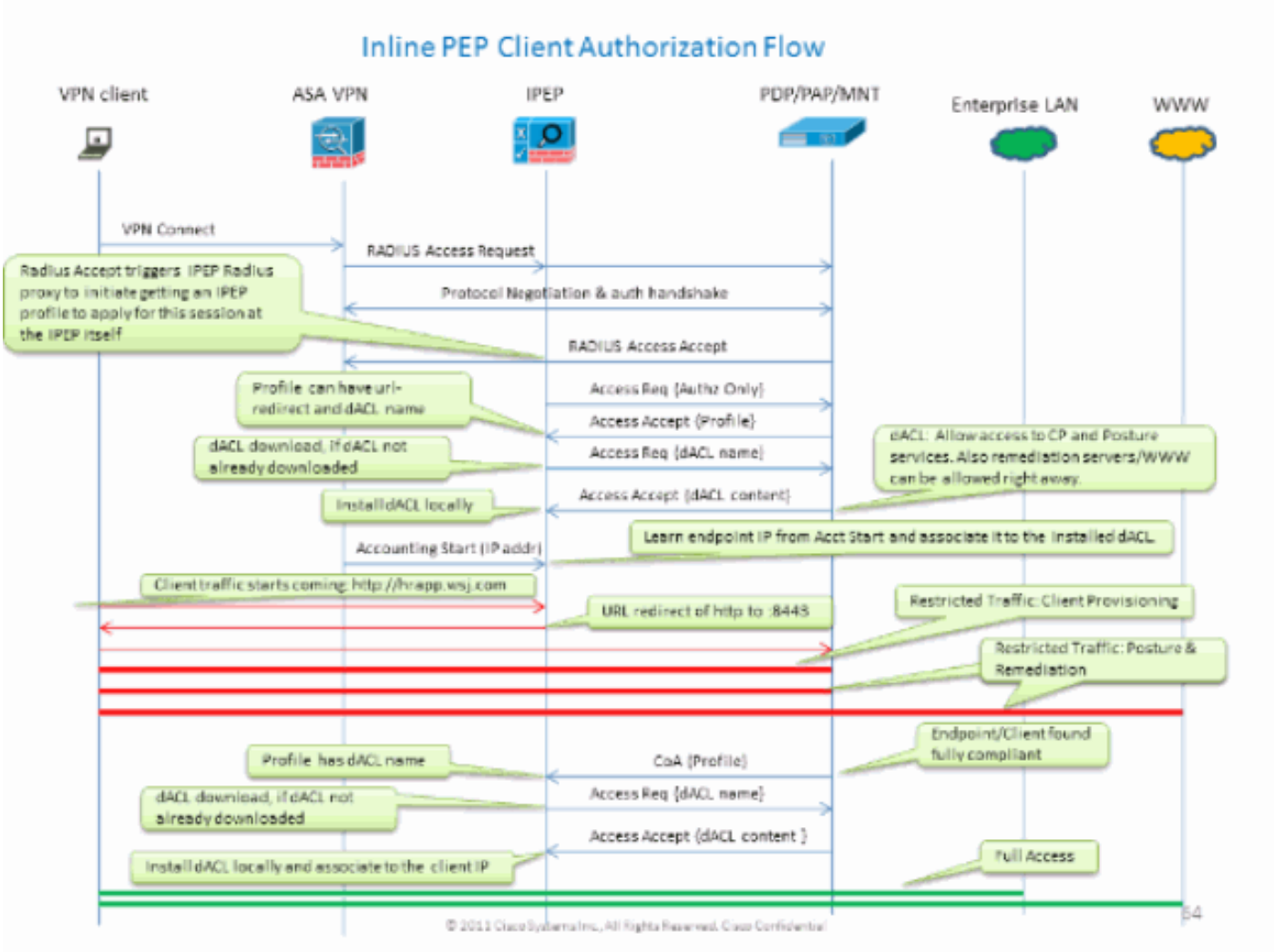
ISE提供許多AAA服務（狀態、分析、身份驗證等）。 某些網路裝置(NAD)支援Radius授權變更(CoA)，允許根據終端裝置的狀態或設定檔結果動態變更其授權設定檔。其他NAD（如ASA）尚不支援此功能。這意味著需要以內聯狀態實施模式(iPEP)運行的ISE來動態更改終端裝置的網路訪問策略。

基本概念是所有使用者流量將通過iPEP，節點同時充當Radius代理。

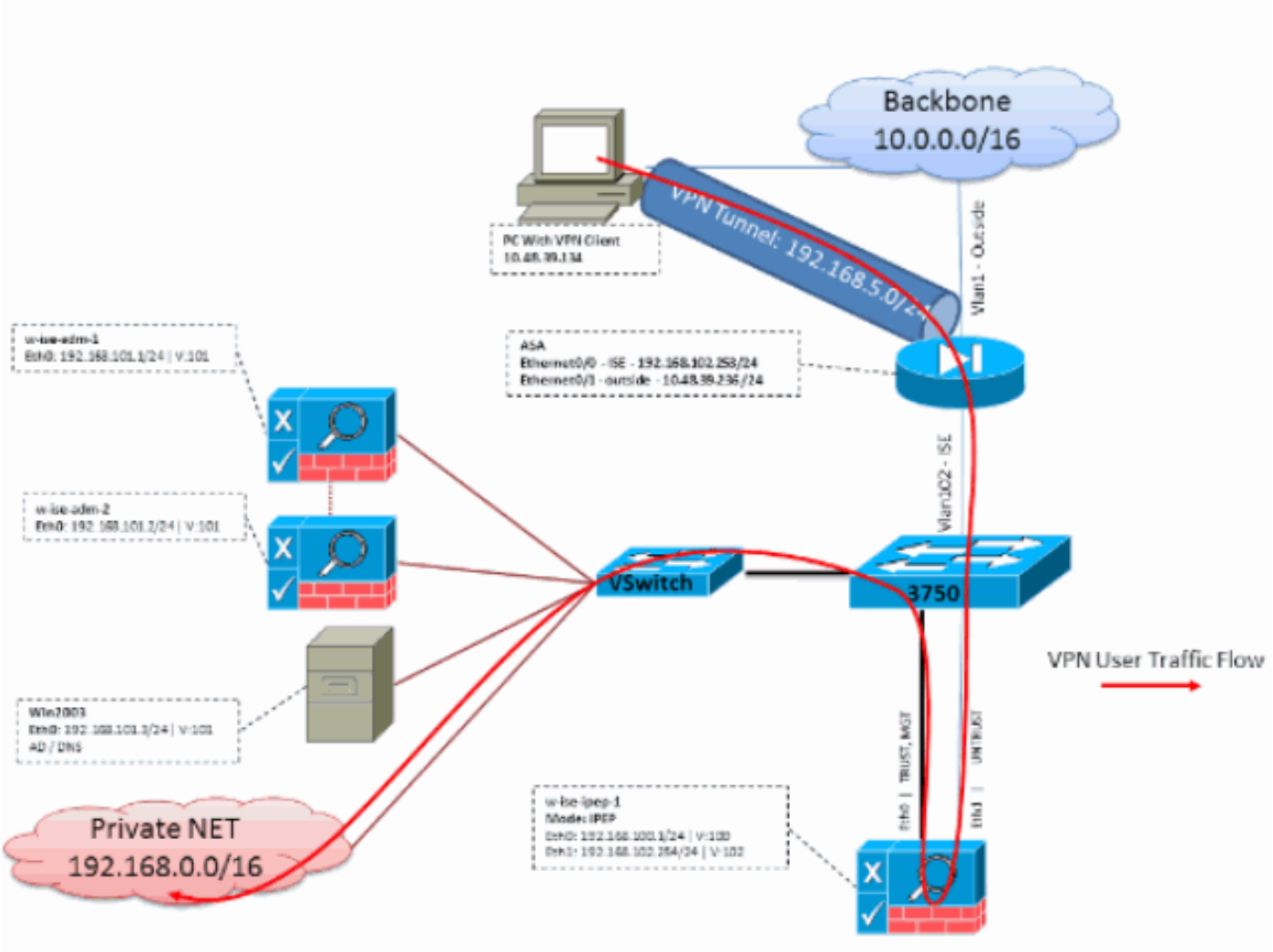
基本流程

1. VPN使用者登入。
2. ASA將請求傳送到iPEP節點(ISE)。
3. iPEP重寫請求（通過新增Cisco AV配對屬性來指示這是iPEP身份驗證），並將請求傳送到ISE策略節點(PDP)。
4. PDP回覆將轉發到NAD的iPEP。
5. 如果使用者通過驗證，則NAD必須傳送計費啟動要求(請參閱CSCtz84826)。 這將觸發iPEP上的會話啟動。在這個階段，使用者被重新導向以尋找安全狀態。此外，您需要為從WEBVPN門戶建立的隧道啟用臨時記賬更新，因為ISE預期在radius記賬中具有屬性framed-ip-address。但是，當連線到入口時，由於未建立隧道，客戶端的VPN IP地址未知。這將確保ASA傳送臨時更新，例如何時建立隧道。
6. 使用者完成狀態評估，並根據評估結果，PDP將使用iPEP上的CoA更新會話。

此螢幕截圖說明了此過程：



拓撲示例



ASA配置

ASA配置是一個簡單的IPSEC遠端VPN:

```
!
interface Ethernet0/0
nameif ISE
security-level 50
ip address 192.168.102.253 255.255.255.0
!
interface Ethernet0/1
nameif outside
security-level 0
ip address 10.48.39.236 255.255.255.0
!
access-list split extended permit ip 192.168.0.0 255.255.0.0 any
!
aaa-server ISE protocol radius
interim-accounting-update
!--- Mandatory if tunnel established from WEBVPN Portal aaa-server ISE (ISE) host
192.168.102.254 !--- this is the iPEP IP key cisco crypto ipsec transform-set TS1 esp-aes esp-
sha-hmac crypto ipsec security-association lifetime seconds 28800 crypto ipsec security-
association lifetime kilobytes 4608000 crypto dynamic-map DMAP1 10 set transform-set TS1 crypto
```

```
dynamic-map DMAP1 10 set reverse-route crypto map CM1 10 ipsec-isakmp dynamic DMAP1 crypto map
CM1 interface outside crypto isakmp enable outside crypto isakmp policy 1 authentication pre-
share encryption aes hash sha group 2 lifetime 86400 ! ip local pool VPN 192.168.5.1-
192.168.5.100 ! group-policy DfltGrpPolicy attributes dns-server value 192.168.101.3 !--- The
VPN User needs to be able to resolve the CN from the !--- ISE HTTPS Certificate (which is sent
in the radius response) vpn-tunnel-protocol IPSec svc webvpn split-tunnel-policy tunnelspecified
split-tunnel-network-list value split address-pools value VPN ! tunnel-group cisco general-
attributes address-pool VPN authentication-server-group ISE accounting-server-group ISE !---
Does not work without this (see introduction) ! tunnel-group cisco ipsec-attributes pre-shared-
key cisco ! route outside 0.0.0.0 0.0.0.0 10.48.39.5 1 route ISE 192.168.0.0 255.255.0.0
192.168.102.254 1 !--- You need to make sure the traffic to the local subnets !--- are going
through the inline ISE !
```

ISE 組態

iPEP配置

首先要將ISE新增為iPEP節點。您可在此處找到有關流程的其他資訊：

http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_ipep_deploy.html#wp1110248。

這基本上就是您在各個頁籤中必須配置的內容（本節提供的螢幕截圖說明了此內容）：

- 配置不受信任的IP和全域性IP設定（在這種情況下，不受信任的IP為192.168.102.254）。
- 部署為路由模式。
- 為ASA放置一個靜態過濾器，使其可以通過iPEP框（否則，通過iPEP框與ISE的連線將被丟棄）。
- 將策略ISE配置為Radius伺服器，將ASA配置為Radius客戶端。
- 將路由新增到指向ASA的VPN子網。
- 將監控ISE設定為日誌記錄主機(預設情況下為20514接埠);在本例中，策略ISE也在監控)。

重要證書配置要求：

在嘗試註冊iPEP節點之前，請確保滿足以下證書擴展金鑰使用要求。如果未在iPEP和Admin節點上正確配置證書，註冊過程將完成。但是，您將失去對iPEP節點的管理員訪問許可權。從ISE 1.1.x iPEP部署指南推斷出以下詳細資訊：

在管理和內聯狀態節點的本地證書中存在某些屬性組合可能會阻止相互身份驗證正常工作。

屬性包括：

- 擴展金鑰使用(EKU) — 伺服器身份驗證
- 擴展金鑰使用(EKU) — 客戶端身份驗證
- Netscape證書型別 — SSL伺服器身份驗證
- Netscape證書型別 — SSL客戶端身份驗證

管理證書需要以下任一組合：

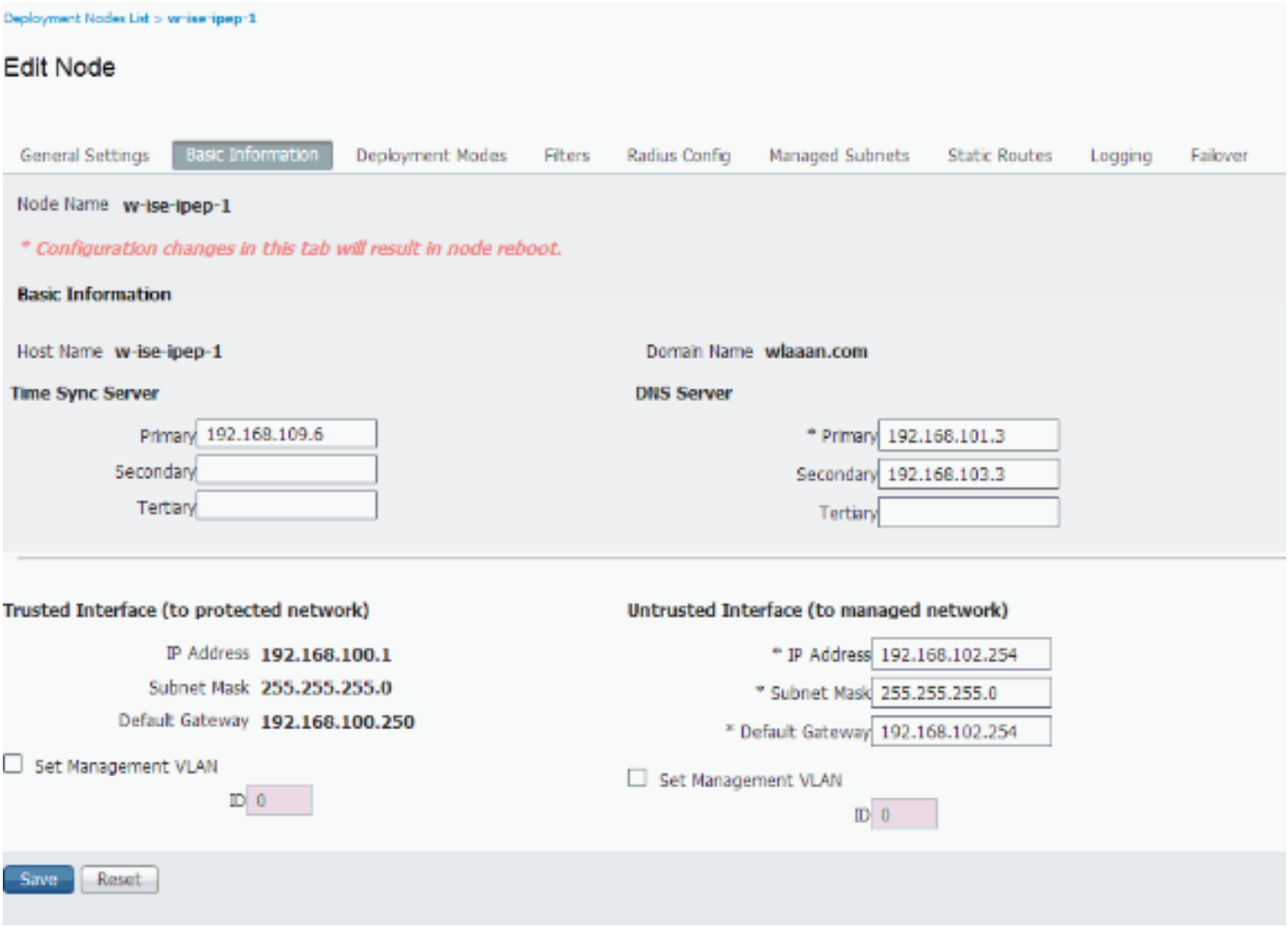
- 如果在內聯狀態證書中禁用了兩個EKU屬性，則應禁用兩個EKU屬性；如果在內聯狀態證書中啟用了伺服器屬性，則應啟用兩個EKU屬性。
- 應禁用兩個Netscape證書型別屬性，或者同時啟用這兩個屬性。

內聯狀態證書需要以下任一組合：

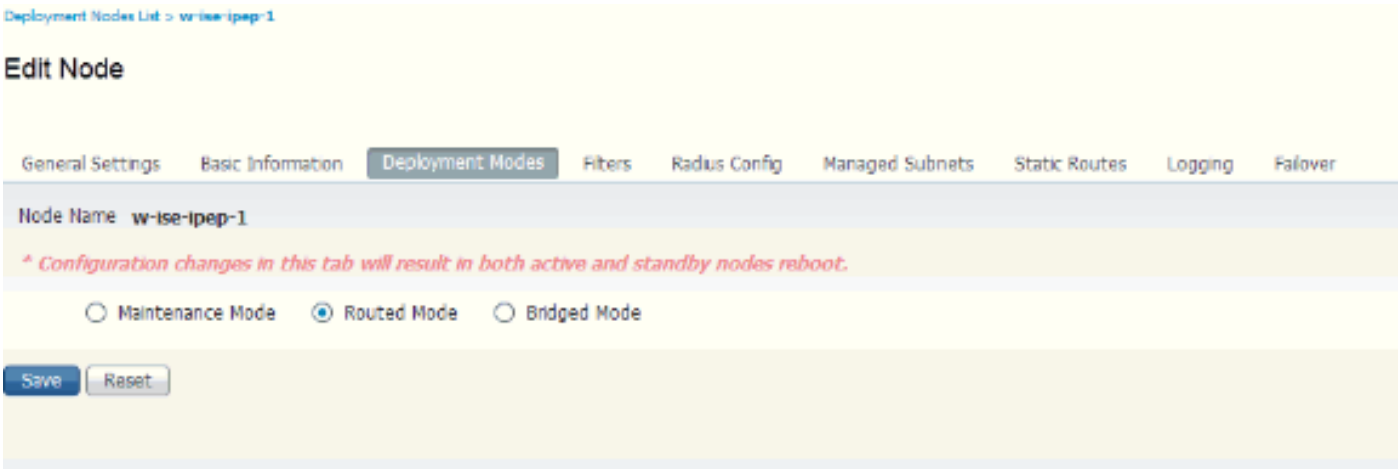
- 應禁用兩個EKU屬性，或者同時啟用兩者，或者只啟用伺服器屬性。

- 應禁用兩個Netscape證書型別屬性，或者同時啟用這兩個屬性，或者只啟用伺服器屬性。
- 如果自簽名本地證書用於管理節點和內聯狀態節點，則必須在內聯狀態節點的信任清單中安裝管理節點的自簽名證書。此外，如果部署中同時具有主要和輔助管理節點，則必須在Inline Posture節點的信任清單中安裝兩個管理節點的自簽名證書。
- 如果管理節點和內聯狀態節點上使用CA簽名的本地證書，則相互身份驗證應正常工作。在這種情況下，簽名CA的證書在註冊之前安裝在管理節點上，並且此證書被複製到Inline Posture節點。
- 如果CA頒發的金鑰用於保護管理節點和內聯狀態節點之間的通訊，則在註冊Inline Posture節點之前，必須將公鑰（CA證書）從管理節點新增到內聯狀態節點的CA證書清單中。

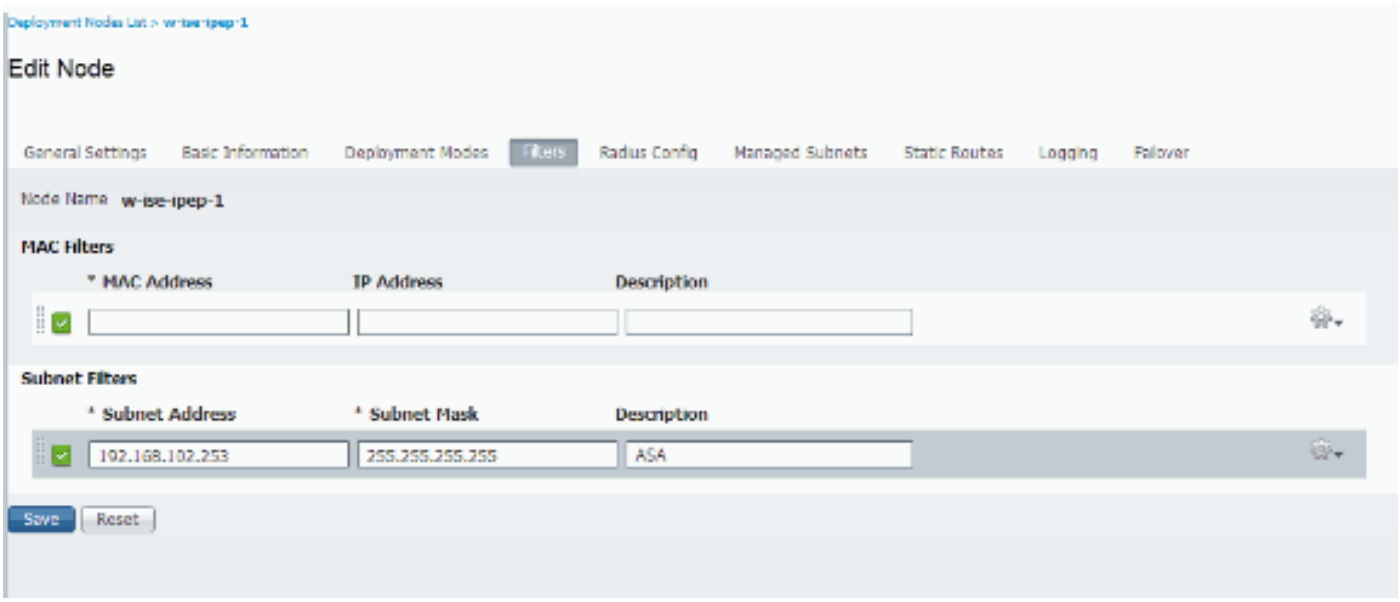
基本配置：



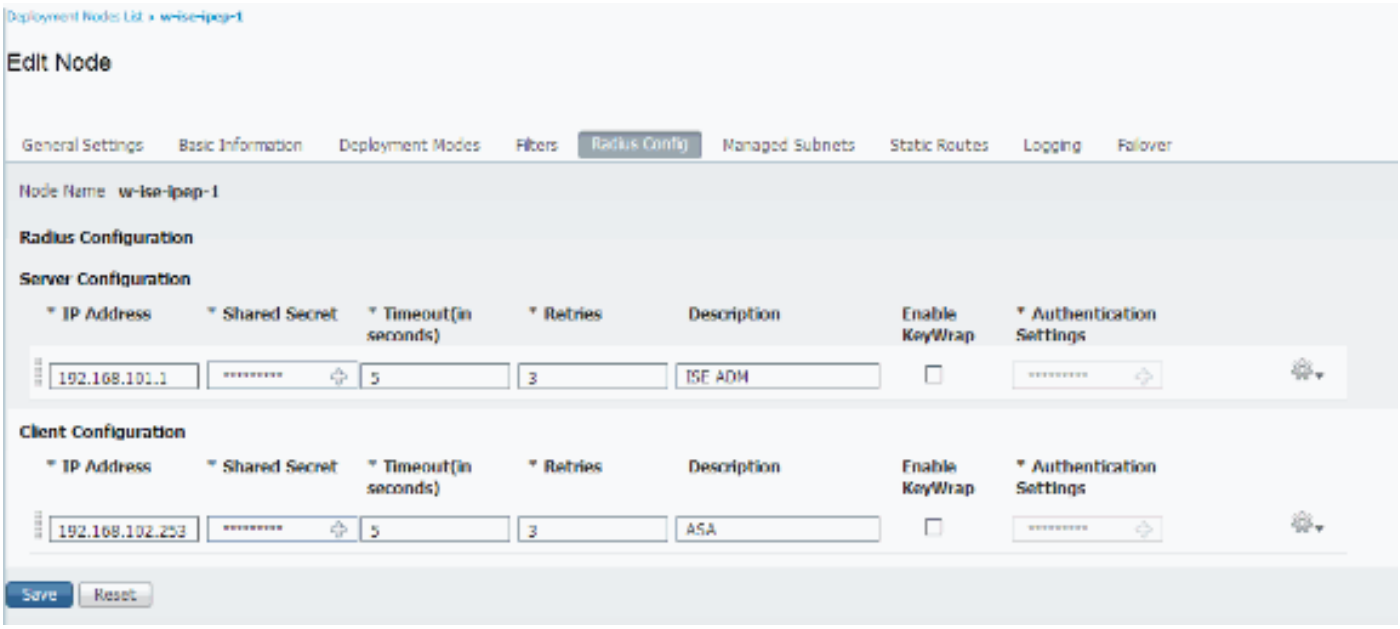
部署模式配置：



過濾器配置：

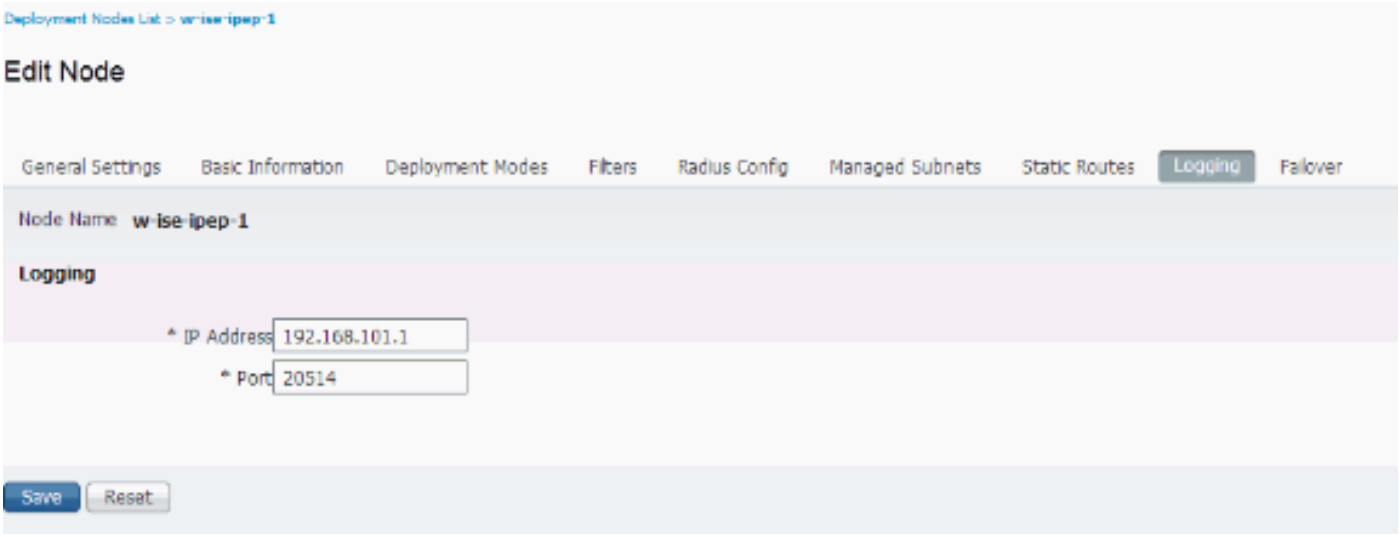


Radius組態：



靜態路由：

日誌記錄：



驗證和安全狀態配置

有三種狀態狀態：

- 未知：尚未建立狀態
- 合規：已建立狀態且系統符合要求
- 不符合：已建立狀態，但系統至少一次檢查失敗

現在必須建立授權配置檔案（將為內聯授權配置檔案）：這將在Cisco AV對中新增ipep-authz=true屬性)，該屬性將用於不同情況。

通常，未知配置檔案會返回重定向URL（狀態發現），此重定向URL會將使用者的流量轉發到ISE並請求安裝NAC代理。如果已安裝NAC代理，這將允許將其HTTP發現請求轉發到ISE。

在此配置檔案中，使用至少允許到ISE和DNS的HTTP流量的ACL。

合規和不合規配置檔案通常會返回可下載ACL，以便根據使用者配置檔案授予網路訪問許可權。非合規配置檔案可允許使用者訪問Web伺服器，例如下載防病毒軟體，或授予有限的網路訪問許可權。

在此示例中，將建立未知和符合的配置檔案，並檢查是否存在notepad.exe作為要求。

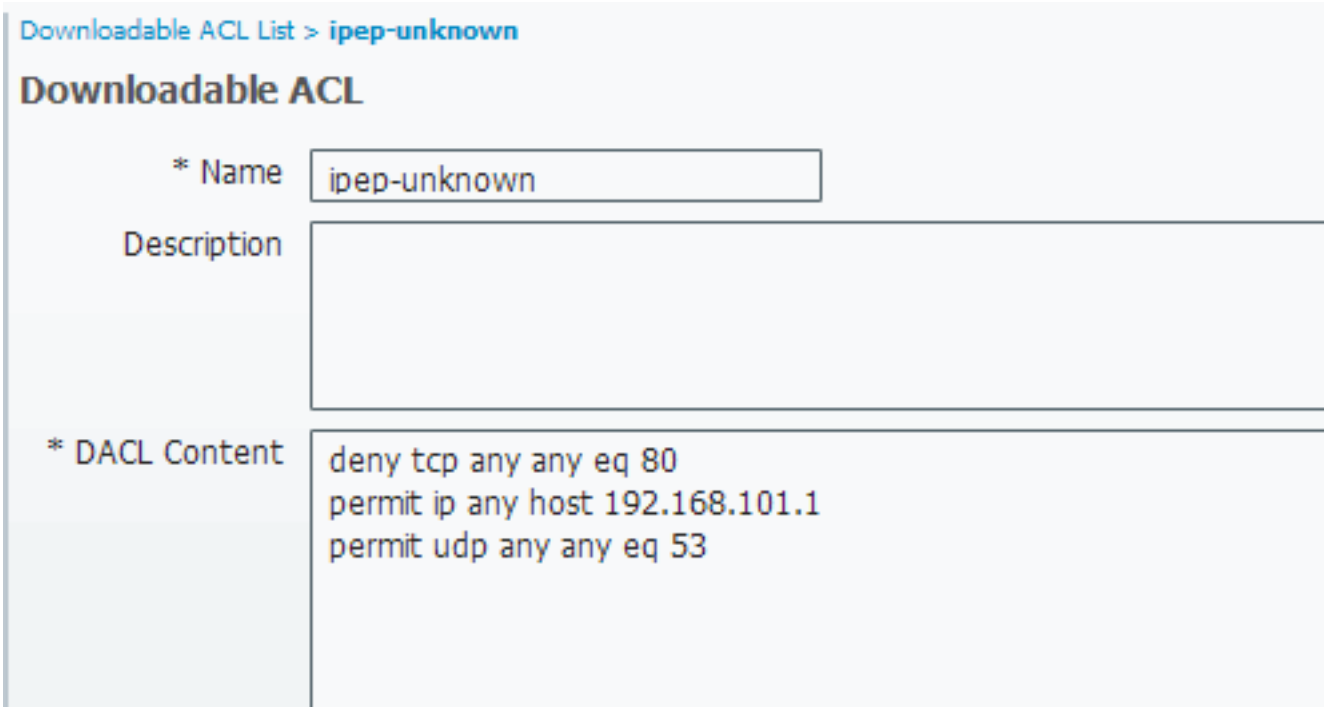
狀態配置檔案配置

首先要做的是建立可下載ACL(dACL)和配置檔案：

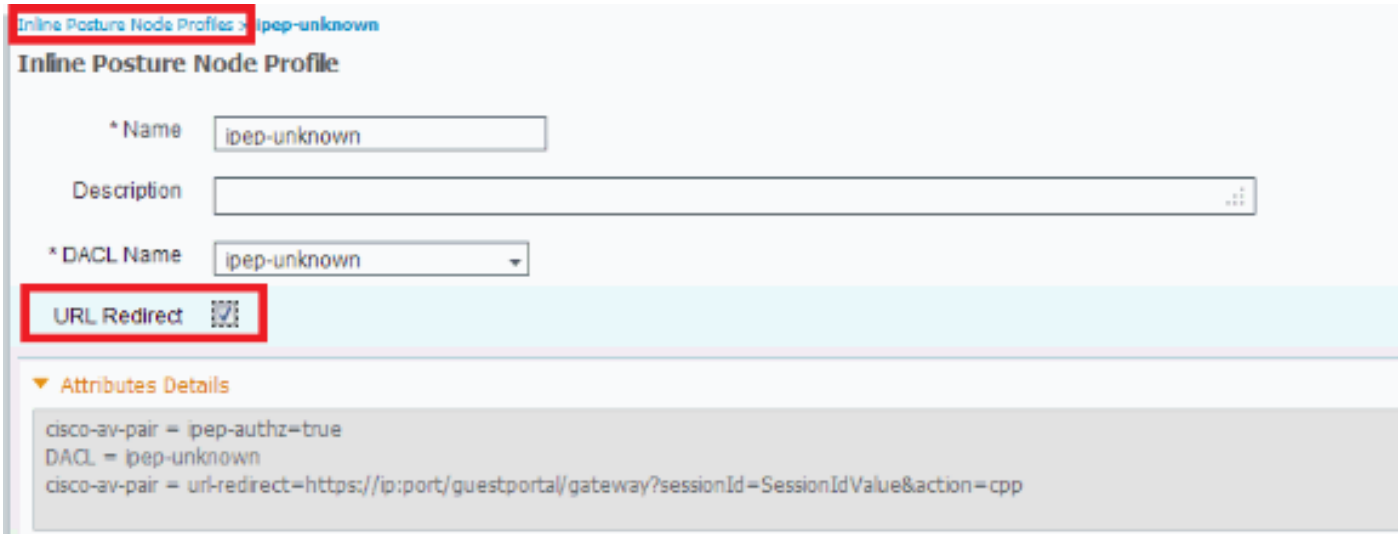
注意：要使該dACL名稱與配置檔名稱匹配，這不是必須的。

- 合規ACL:ipep-unknown授權配置檔案：ipep-unknown
- 不符合ACL:IPEP不符合授權配置檔案：IPEP不符合

未知dACL:

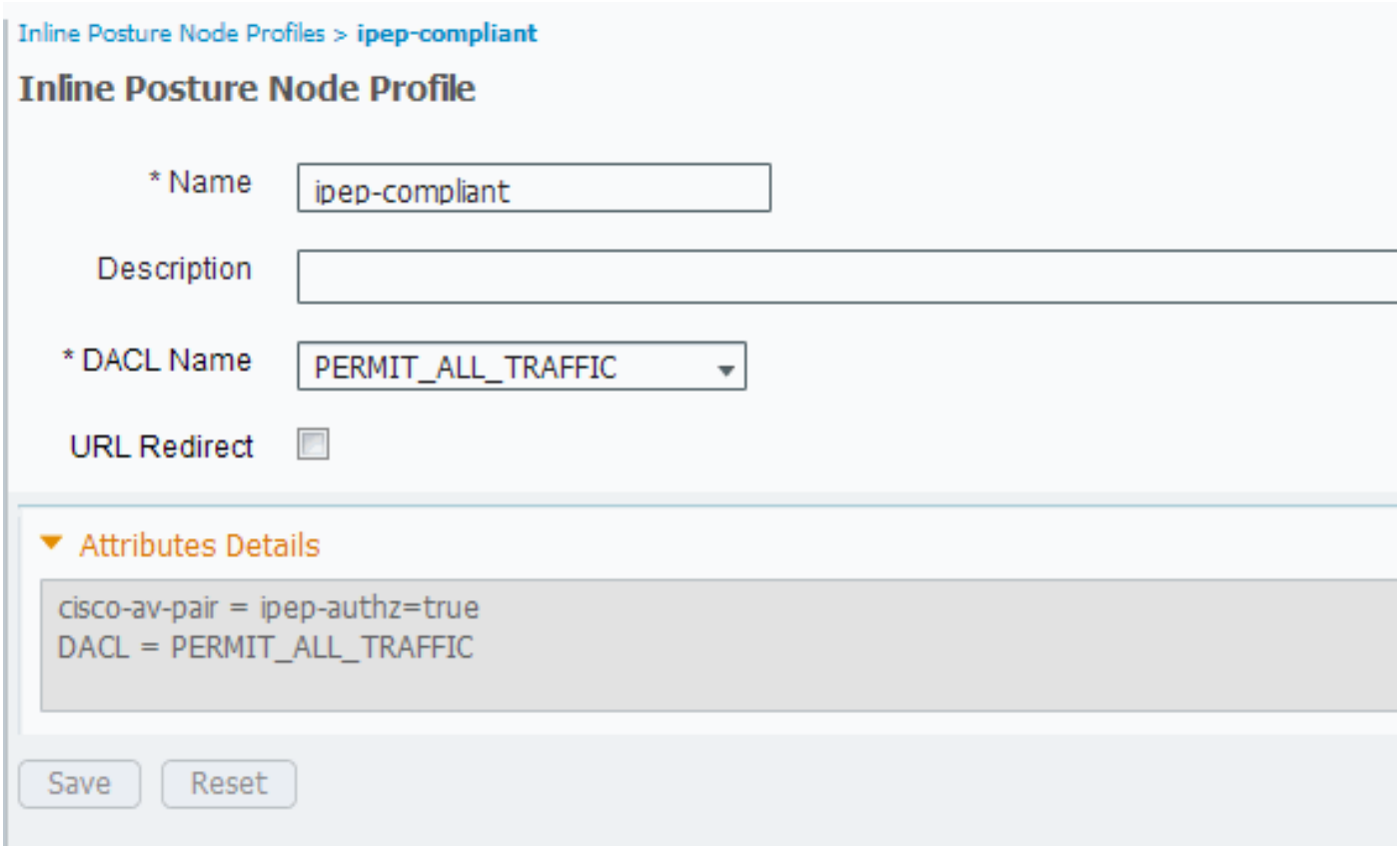


未知配置檔案：



相容的dACL:

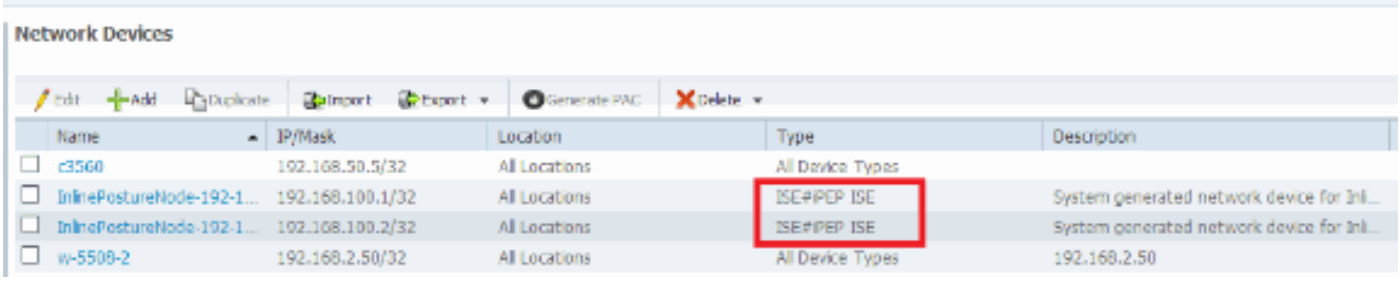
符合性配置檔案：



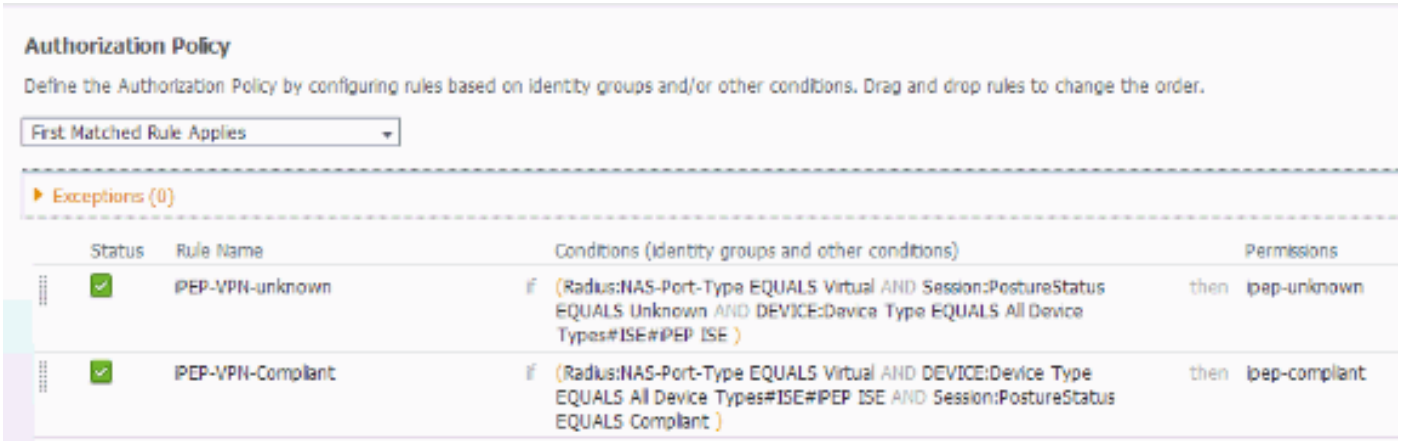
授權配置

建立配置檔案後，您需要匹配來自iPEP的Radius請求，並將正確的配置檔案應用到它們。iPEP ISE使用將在Authorization規則中使用的特殊裝置型別定義：

NAD:

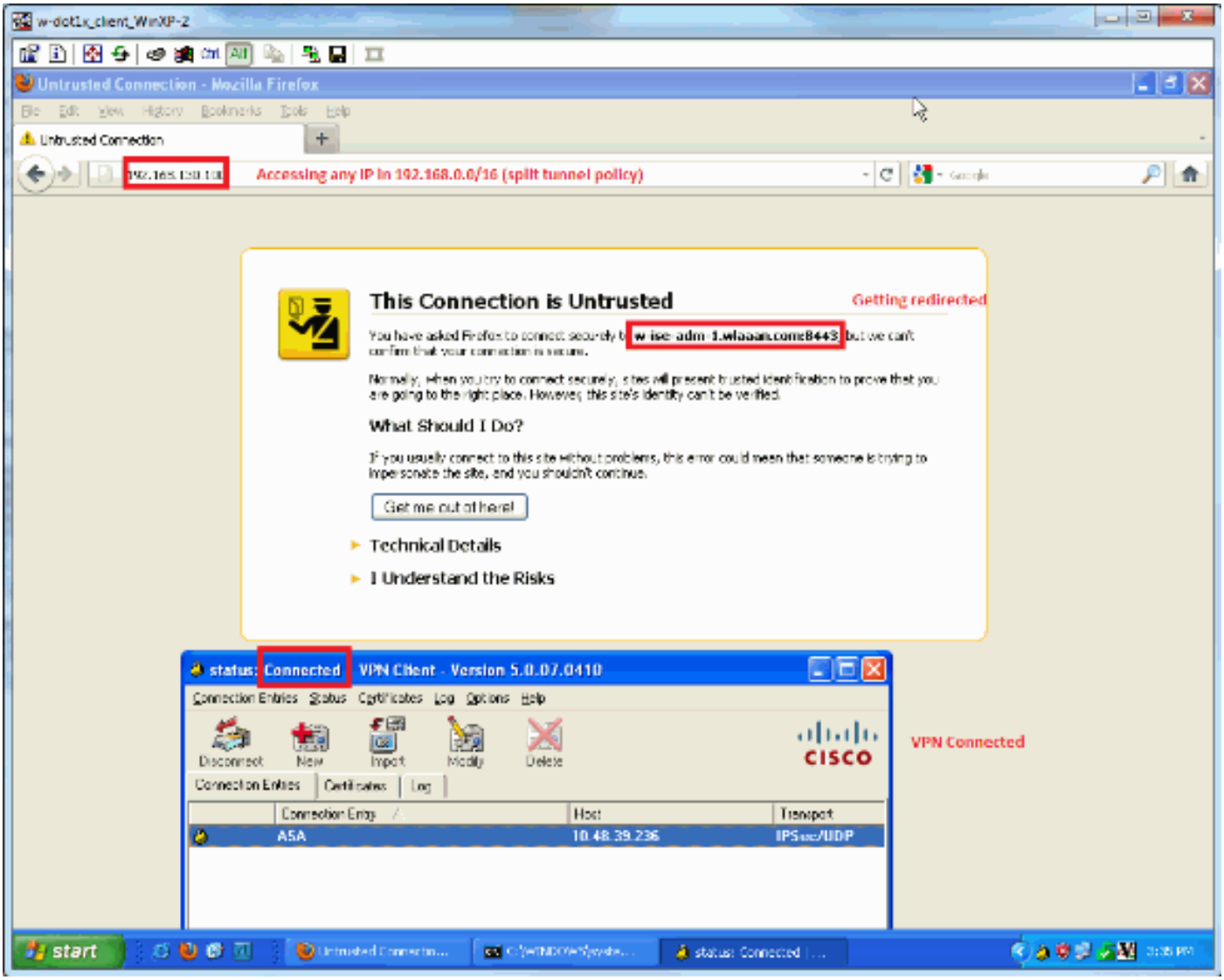


Authorization:

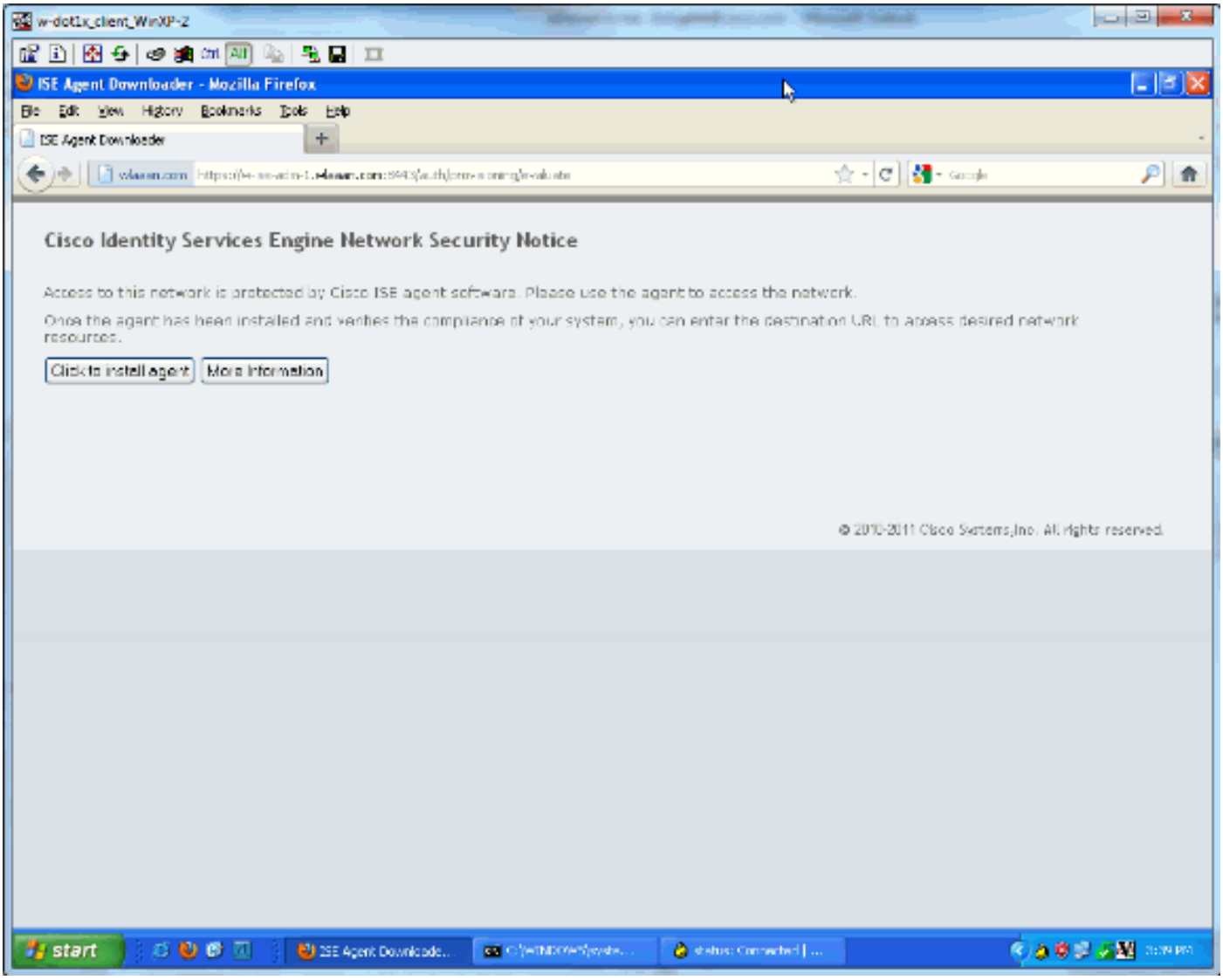


注意：如果電腦上未安裝代理，則可以定義客戶端調配規則。

結果



系統將提示您安裝代理（在本示例中，已設定客戶端調配）：



此階段的一些輸出：

```
ciscoasa# show vpn-sessiondb remote

Session Type: IPsec
Username     : cisco                  Index        : 26
Assigned IP  : 192.168.5.2            Public IP    : 10.48.39.134
Protocol     : IKE IPsec
License      : IPsec
Encryption   : AES128                 Hashing      : SHA1
Bytes Tx     : 143862                 Bytes Rx     : 30628
Group Policy : DfltGrpPolicy          Tunnel Group : cisco
Login Time   : 13:43:55 UTC Mon May 14 2012
Duration     : 0h:09m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

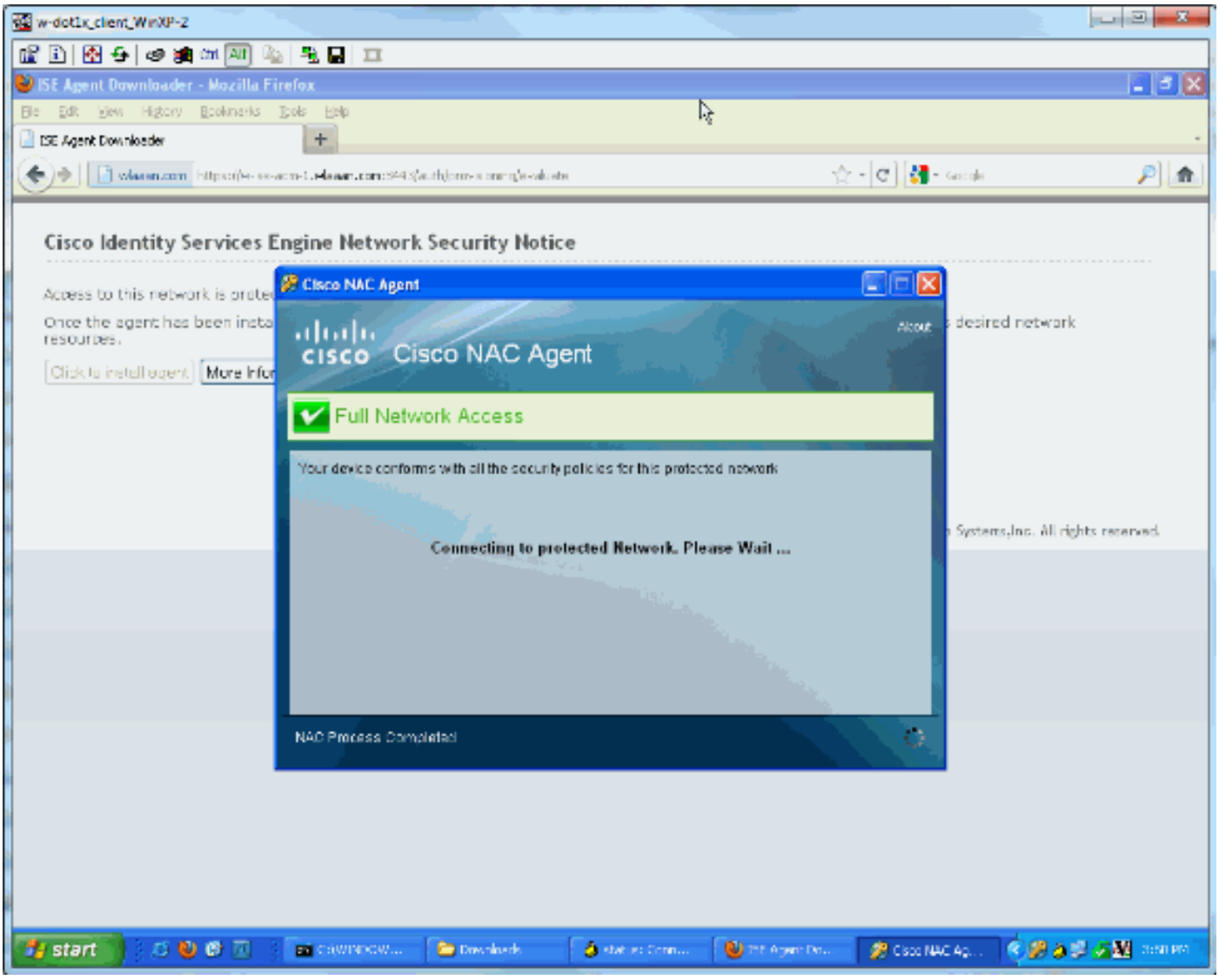
在iPEP上：

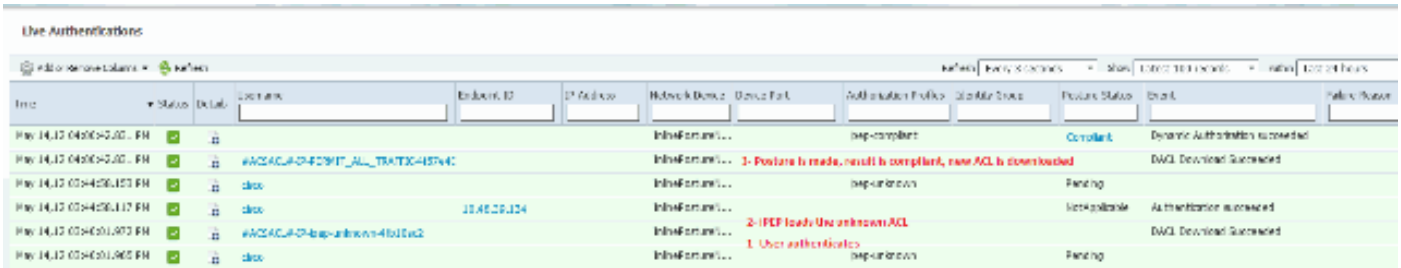
```
w-ise-ipep-1/admin# show pep table session

Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 2 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-ipep-unknown-4fb10ac2:
```

```
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
```

下載並安裝代理後：

代理應自動檢測ISE並運行狀態評估（假設您已經定義了狀態規則，這是另一個主題）。 在此範例中，狀態成功，且顯示：





注意：上面的螢幕截圖中有兩個身份驗證。但是，由於iPEP框會快取ACL，因此不會每次都下載它。

在iPEP上：

```
w-ise-ipep-1/admin# show pep table session
```

```
Current Sessions (IP, MAC(if available), Profile ID, VLAN (if any)):
192.168.5.2 00:00:00:00:00:00 3 0
w-ise-ipep-1/admin# show pep table accesslist normal
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406:
permit ip any any

#ACSACL#-IP-ipep-unknown-4fb10ac2:
deny tcp any host 192.168.101.1 eq 80
deny tcp any host 192.168.101.1 eq 443
permit ip any host 192.168.101.1
permit udp any any eq 53
w-ise-ipep-1/admin#
```

相關資訊

- 技術支援與文件 - Cisco Systems