线型VPN摆姿势使用iPEP ISE和ASA

目录

简介

本文提供信息关于怎样设置轴向状态用可适应安全工具(ASA)和身份服务引擎(ISE)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据ASA的ISE的版本8.2(4)和版本1.1.0.665。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

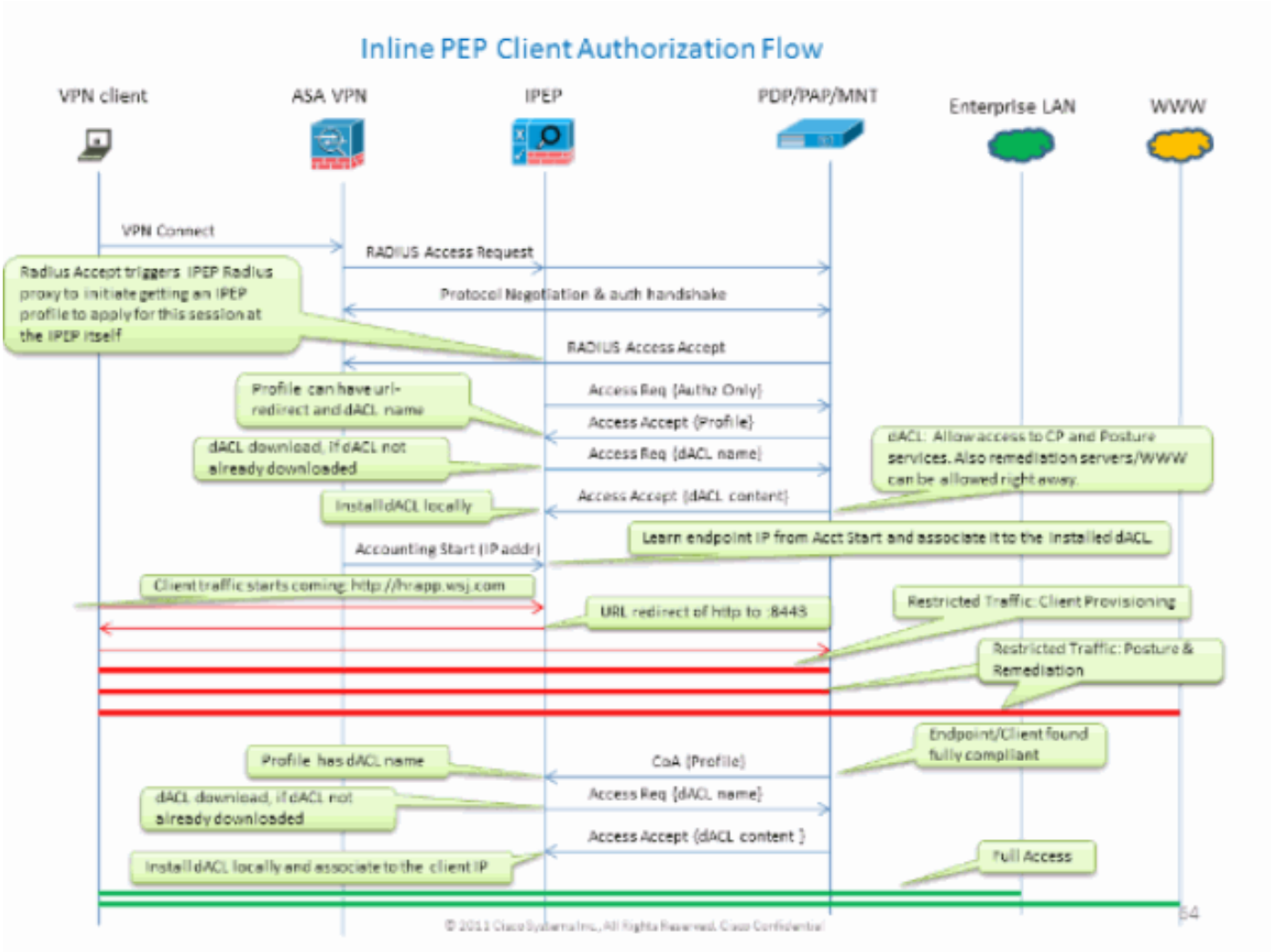
ISE提供很多AAA服务(状态，描出，验证等等)。一些网络设备(纳季)支持Radius准许动态地更改根据其状态或描出结果的终端设备授权配置文件的崔凡吉莱授权(CoA)。其他NAD例如ASA不支持此功能。这意味着运行在轴向状态执行模式(iPEP)的ISE是需要的动态地更改终端设备的网络访问策略。

基本概念是所有用户数据流将通过iPEP，也作为RADIUS代理的节点。

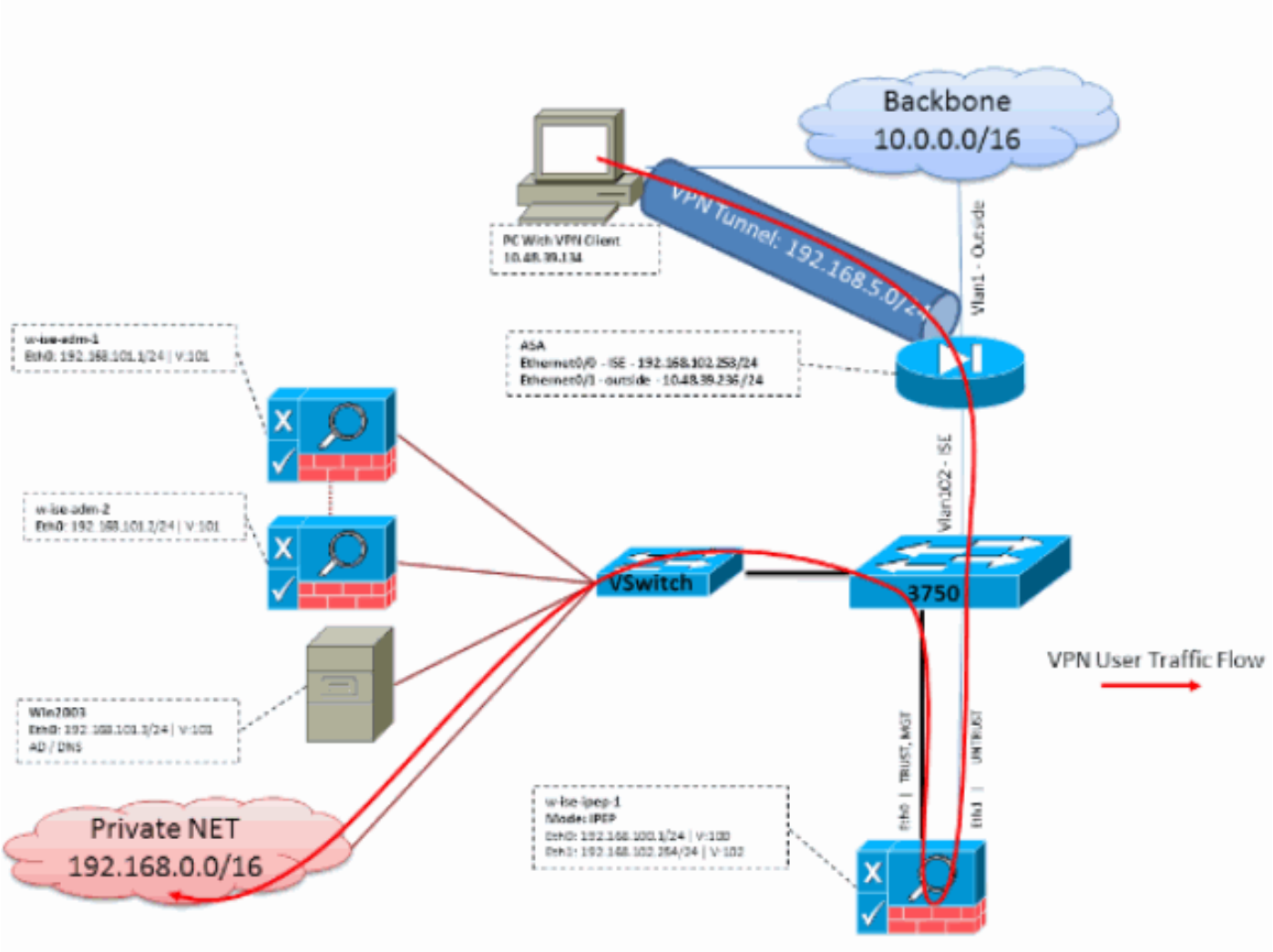
基本流

1. VPN用户登录。
2. ASA发送请求对iPEP节点(ISE)。
3. iPEP重写请求(通过添加Cisco AV对属性指示此是iPEP验证)并且发送请求对ISE策略节点(PDP)。
4. 回到将转发给纳季的iPEP的PDP回复。
5. 如果用户验证，纳季必须发送核算开始请求(请参阅CSCtz84826)。这将触发在iPEP的会话开始。在此阶段，用户为状态重定向。另外，因为ISE期望有属性framed-ip-address在radius核算，您需要启用为从WEBVPN门户设立的通道的过渡技术核算更新。然而，当连接对门户，客户端的VPN IP地址不知道时，因为通道没有设立。这保证ASA将发送临时更新，例如，当通道将设立。
6. 用户通过状态评估，并且基于结果PDP将更新使用在iPEP的会话CoA。

此屏幕画面说明此进程：



示例拓扑



ASA 配置

ASA配置是一简单IPSEC远程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配置

iPEP配置

要执行的第一件事是添加每ISE作为iPEP节点。您能找到关于进程的其他信息此处：

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

这基本上是什么您在多种选项卡必须配置(在此部分提供的屏幕画面说明此) ：

- 配置不信任IP和全球IP设置(在这种情况下，不信任IP是192.168.102.254)。
- 部署是路由的模式。
- 放置能将允许的ASA的一个静态过滤器通过iPEP方框(否则，到/从ISE的连接通过iPEP方框丢弃)。
- 配置策略ISE作为RADIUS服务器和ASA作为RADIUS客户端。
- 添加一个路由到VPN子网对ASA的该点。
- 设置监听ISE作为日志主机(端口20514默认情况下;在这种情况下，策略ISE监控)。

重要身份验证配置需求：

在尝试前注册iPEP节点，请保证以下证书扩展的密钥用法需求满足。如果证书在iPEP和Admin节点没有适当地配置，注册过程将完成。然而，您将丢失对iPEP节点的admin访问。以下详细信息从ISE 1.1.x iPEP部署指南被外推了：

属性的某些组合出现在管理的本地证书和轴向状态节点的可以防止相互验证工作。

属性是：

- 延长的密钥用法(EKU) —服务器验证
- 延长的密钥用法(EKU) —客户端验证
- Netscape Cert类型— SSL服务器验证
- Netscape Cert类型— SSL客户端验证

以下组合之一为管理证书要求：

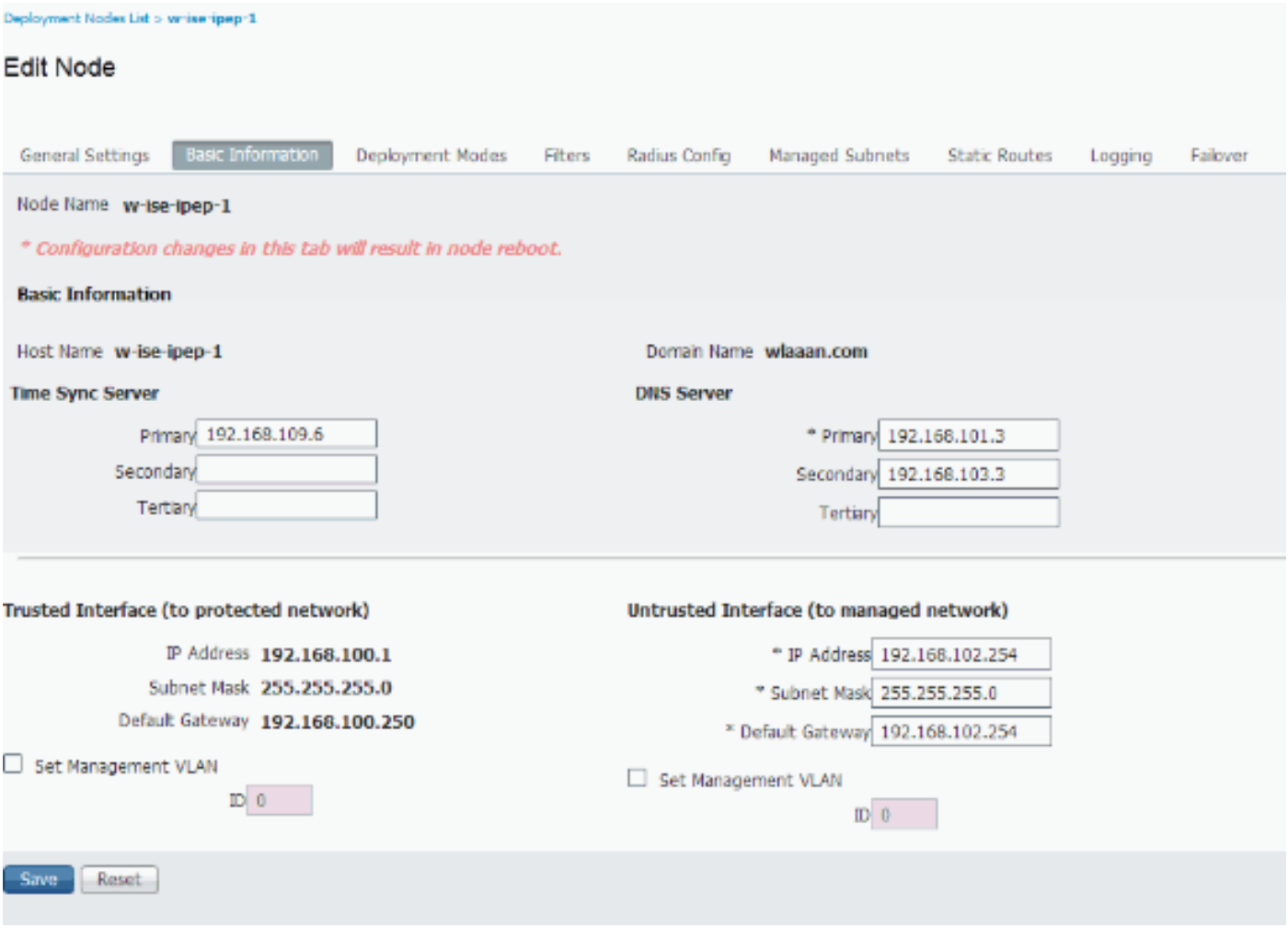
- 应该禁用两个EKU属性，如果两个EKU属性在轴向状态证书禁用，或者应该启用两个EKU属性，如果服务器属性在轴向状态证书启用。
- 应该禁用两个Netscape Cert类型属性，或者应该启用两个。

以下组合之一为轴向状态证书要求：

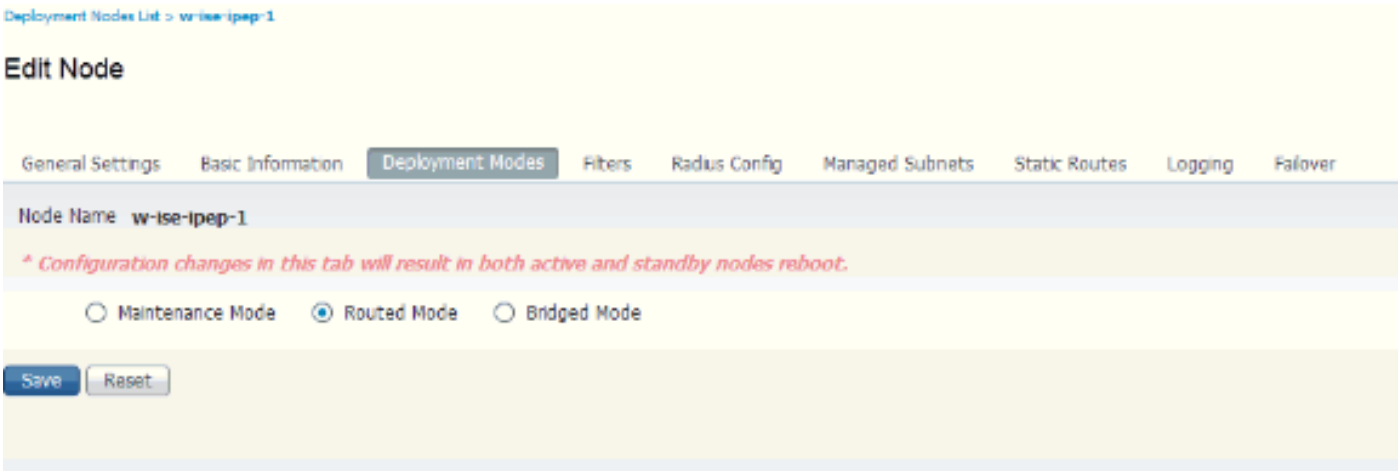
- 应该禁用两个EKU属性，或者应该启用两个，或者应该启用单独服务器属性。

- 应该禁用两个Netscape Cert类型属性，或者应该启用两个，或者应该启用单独服务器属性。
- 那里自己签署的本地证书在管理和轴向状态节点使用，您必须安装管理节点的自签名证书在轴向状态节点的信任列表的。另外，如果有主要的和附属管理节点在您的部署，您必须安装两管理节点自签名证书在轴向状态节点的信任列表的。
- 那里CA签名的本地证书在管理和轴向状态节点使用，相互验证应该正确地运作。在这种情况下，签署的CA的证书在管理节点安装在注册之前，并且此证书复制对轴向状态节点。
- 如果CA发出的密钥使用管理和轴向状态节点之间的保护的通信，在您注册轴向状态节点前，您必须从管理节点添加公共密钥(CA证书)到轴向状态节点的CA证书列表。

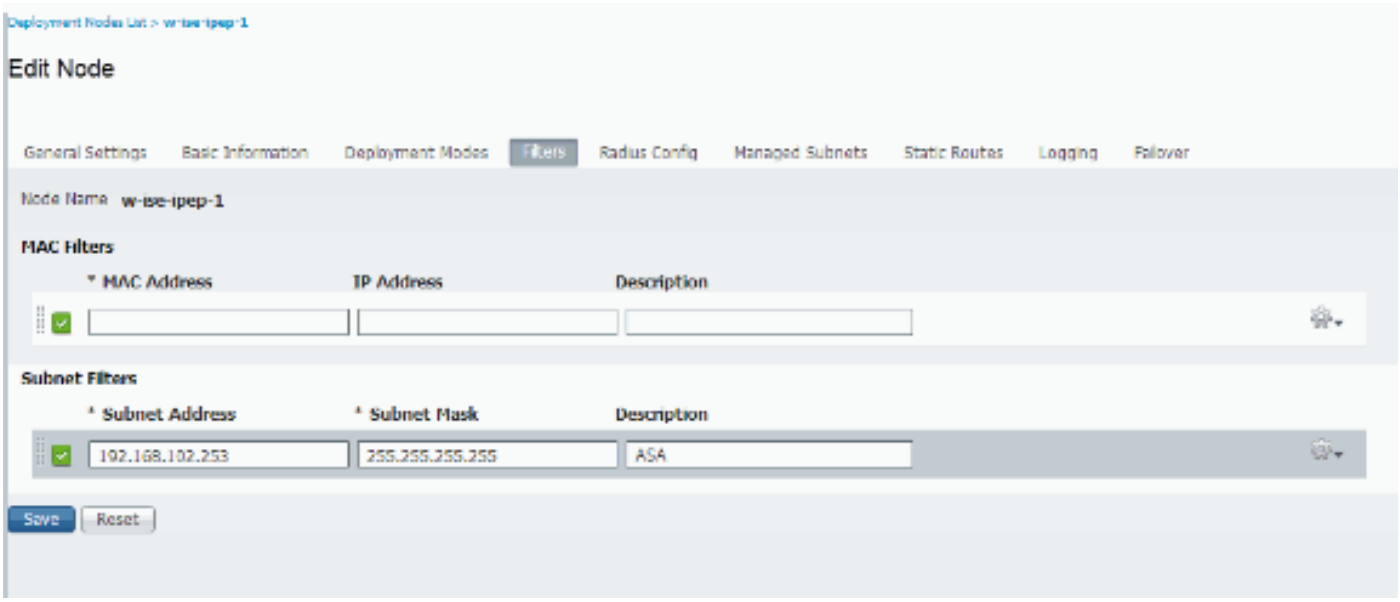
基本配置:



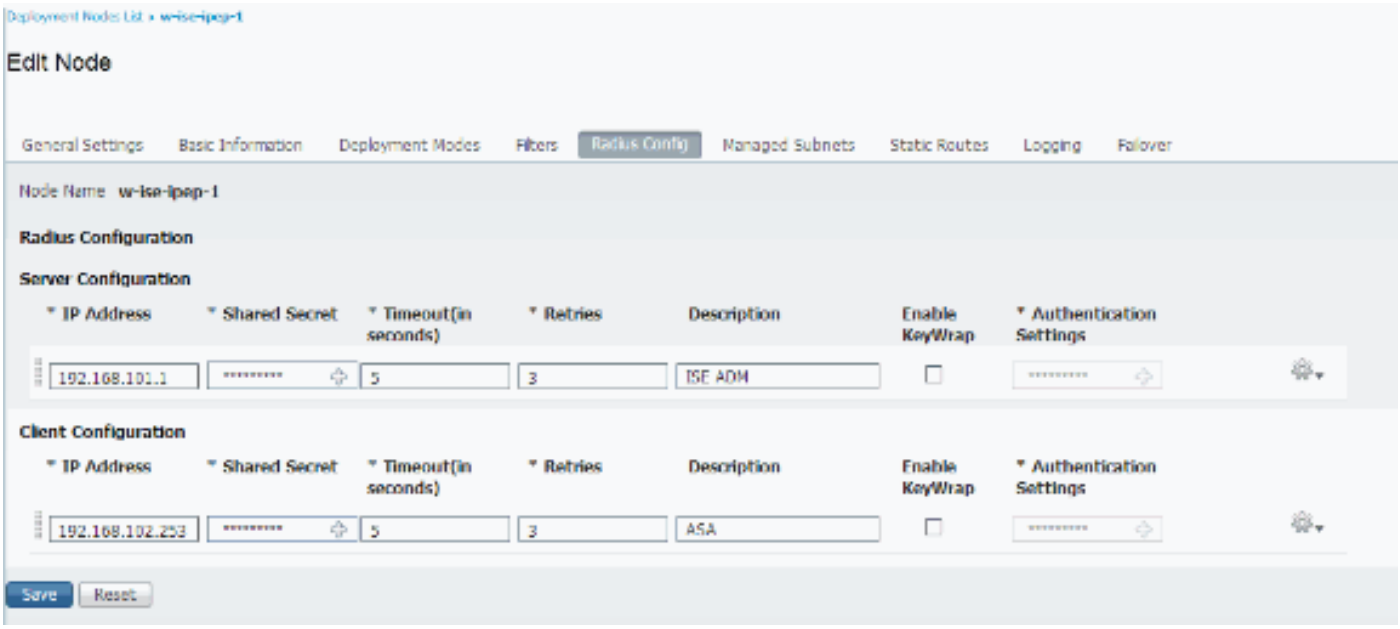
部署模式配置：



过滤器配置：

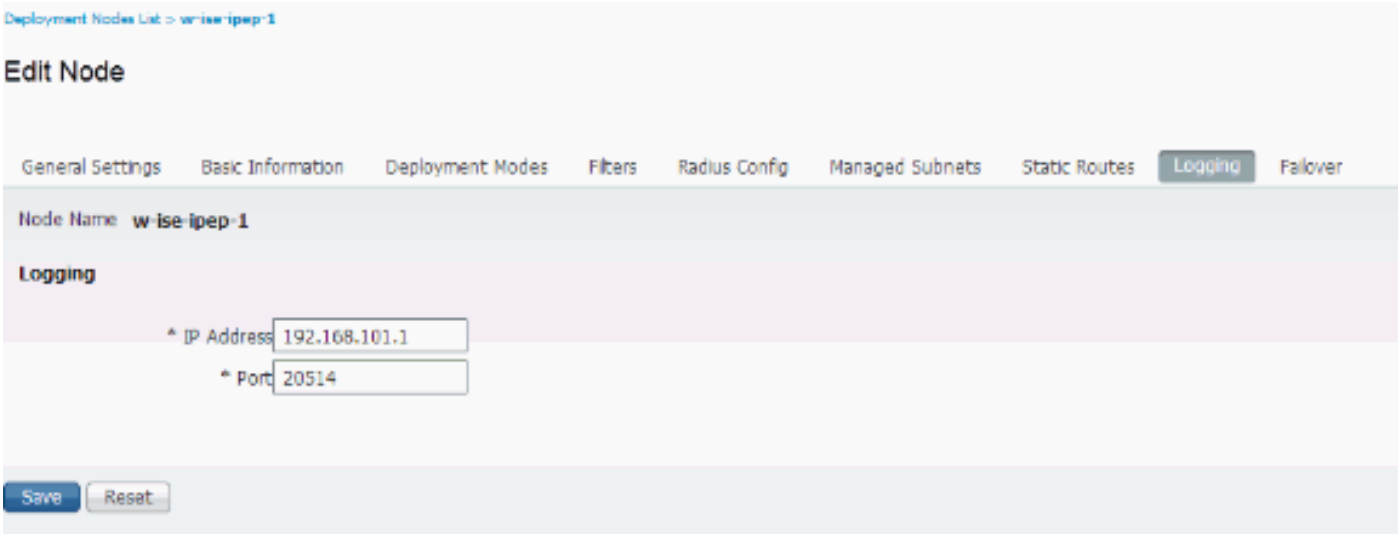


RADIUS配置：



静态路由：

记录：



验证和状态配置

有三状态状态：

- 未知：状态没有做
- 兼容：状态做，并且系统是兼容的
- 固执：状态做，但是系统失败至少一检查

现在授权配置文件必须创建(将是轴向授权配置文件：这将添加在将使用另外案件的Cisco AV对的ipep-authz=true属性)。

通常，未知配置文件返回将转发用户流量对ISE，并且请要求安装美洲台代理程序的重定向URL (状态发现)。如果美洲台代理程序已经安装，这将允许其HTTP发现号请求转发到ISE。

在准许的此配置文件，使用至少ACL对ISE的HTTP数据流和DNS。

兼容和固执的配置文件通常返回可下载的ACLs准许根据用户配置文件的网络访问。固执的配置文件能允许用户访问Web服务器下载例如防病毒，或者请准许有限的网络访问。

在本例中，当需求被检查，未知和兼容配置文件创建和notepad.exe出现。

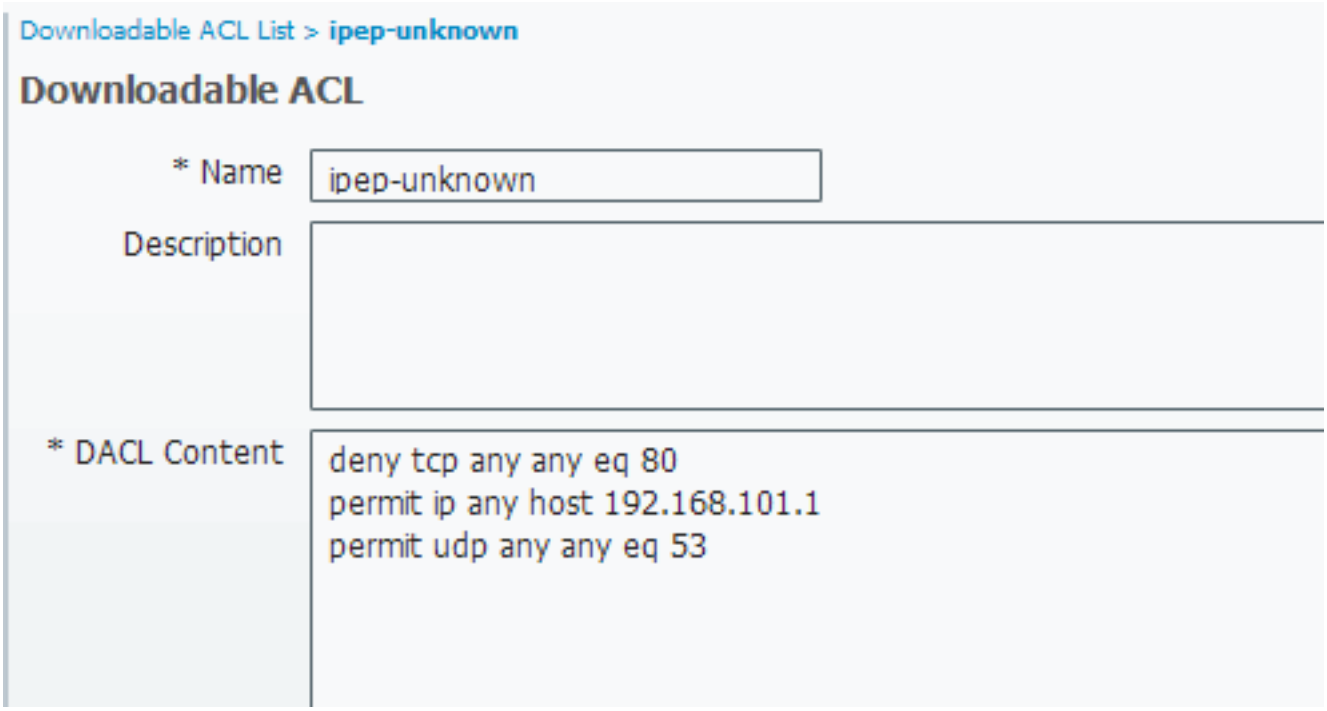
状态配置文件配置

要执行的第一件事是创建可下载的ACLs (dACL)和配置文件：

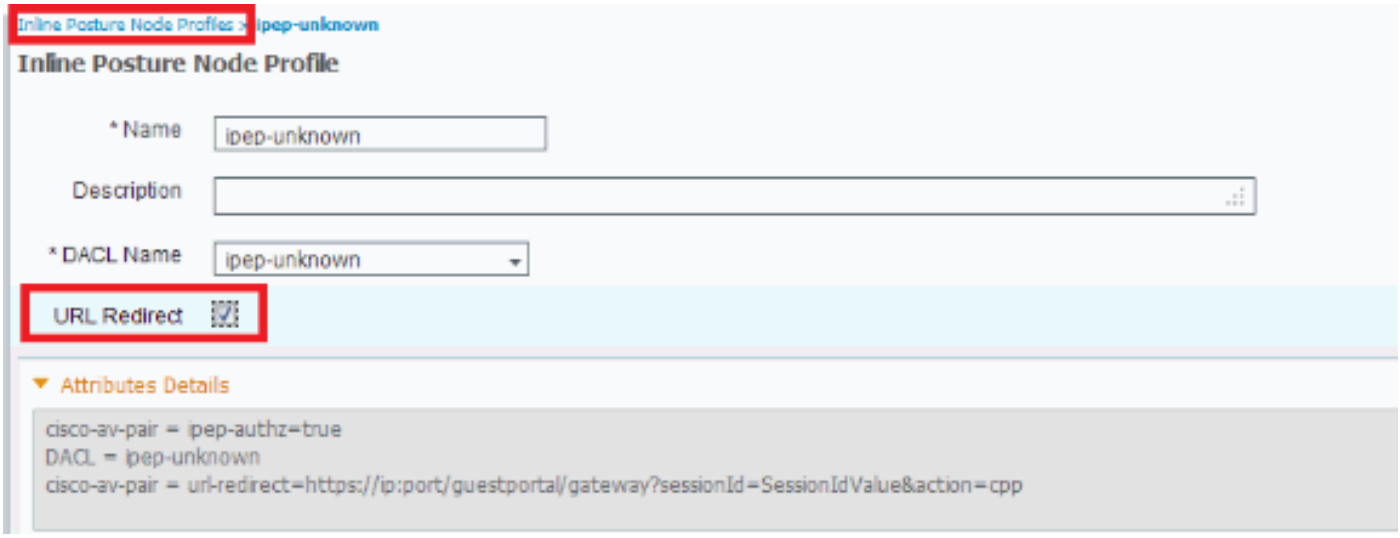
注意： 这不是必须有匹配配置文件名称的dACL名称。

- 兼容ACL ：ipep未知授权配置文件：ipep未知
- 固执ACL ：ipep非兼容授权配置文件：ipep非兼容

未知dACL ：

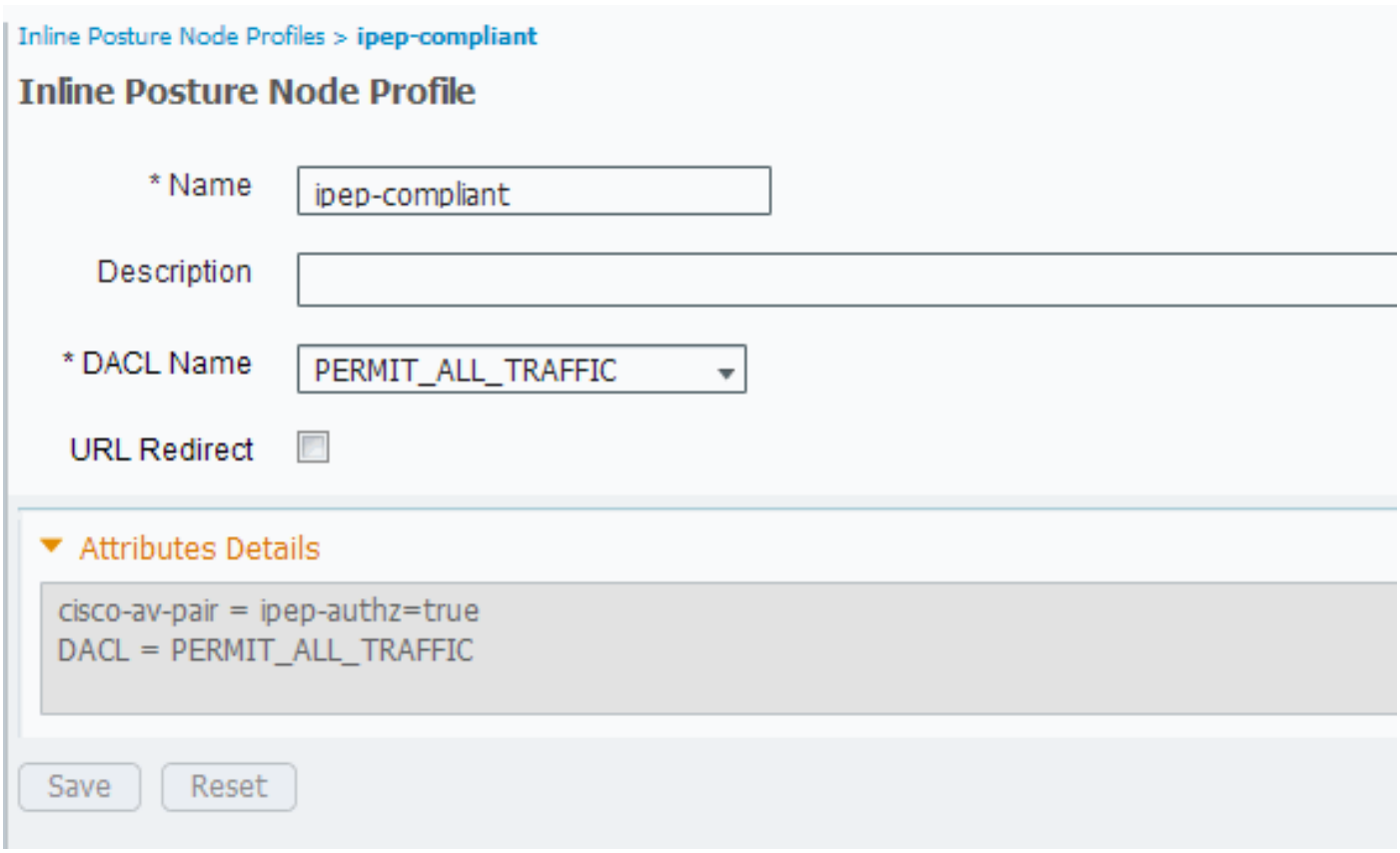


未知配置文件：



兼容dACL ：

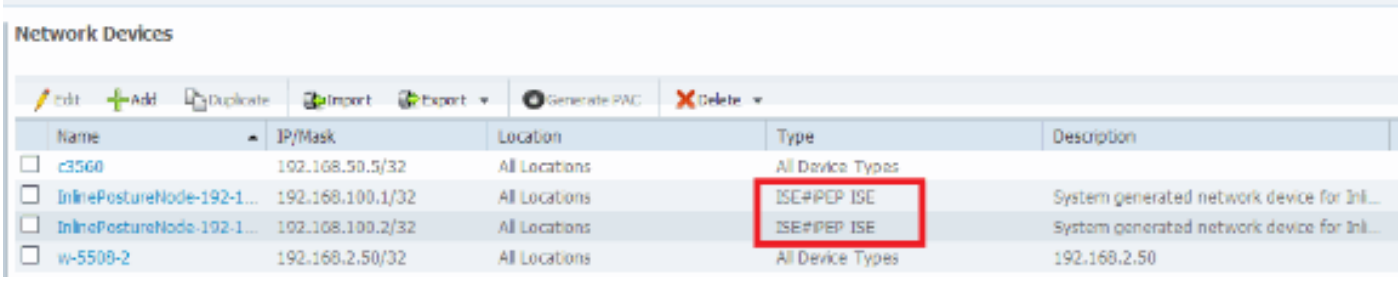
兼容配置文件：



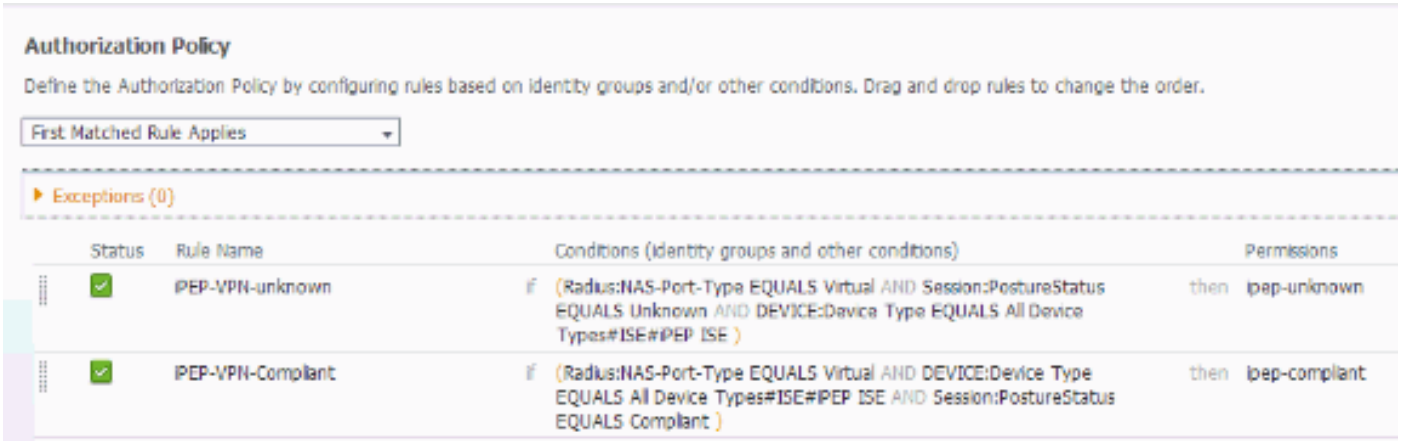
授权配置

即然配置文件创建，您需要匹配来自iPEP的RADIUS请求和应用到他们正确的配置文件。iPEP ISEs定义与在授权规则将使用的一种特殊设备类型：

NAD ：

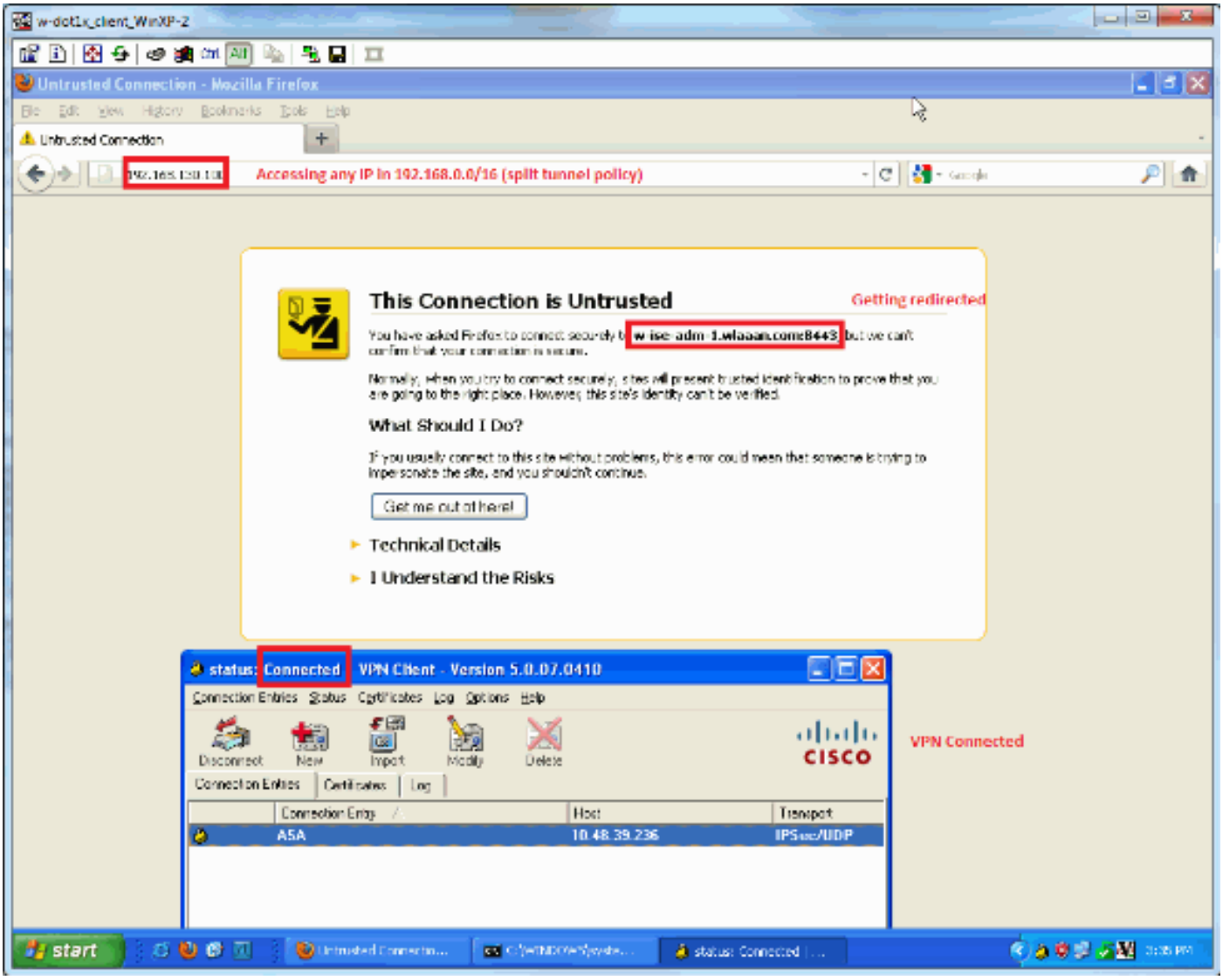


授权：

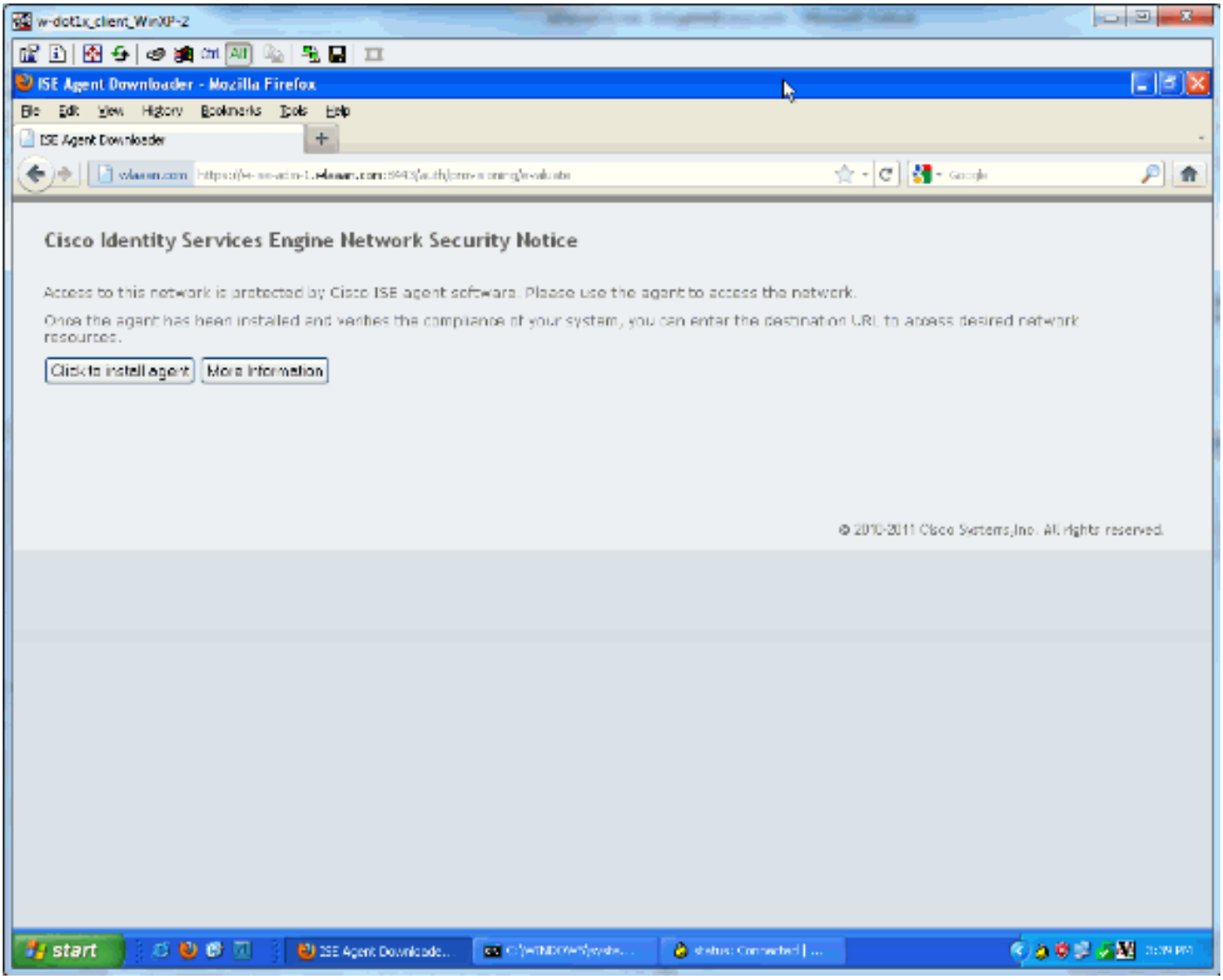


注意： 如果代理程序在计算机没有安装，您能定义客户端供应规则。

结果



提示您安装代理程序(在本例中，客户端供应已经设置)：



在此阶段若干输出：

```
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
```

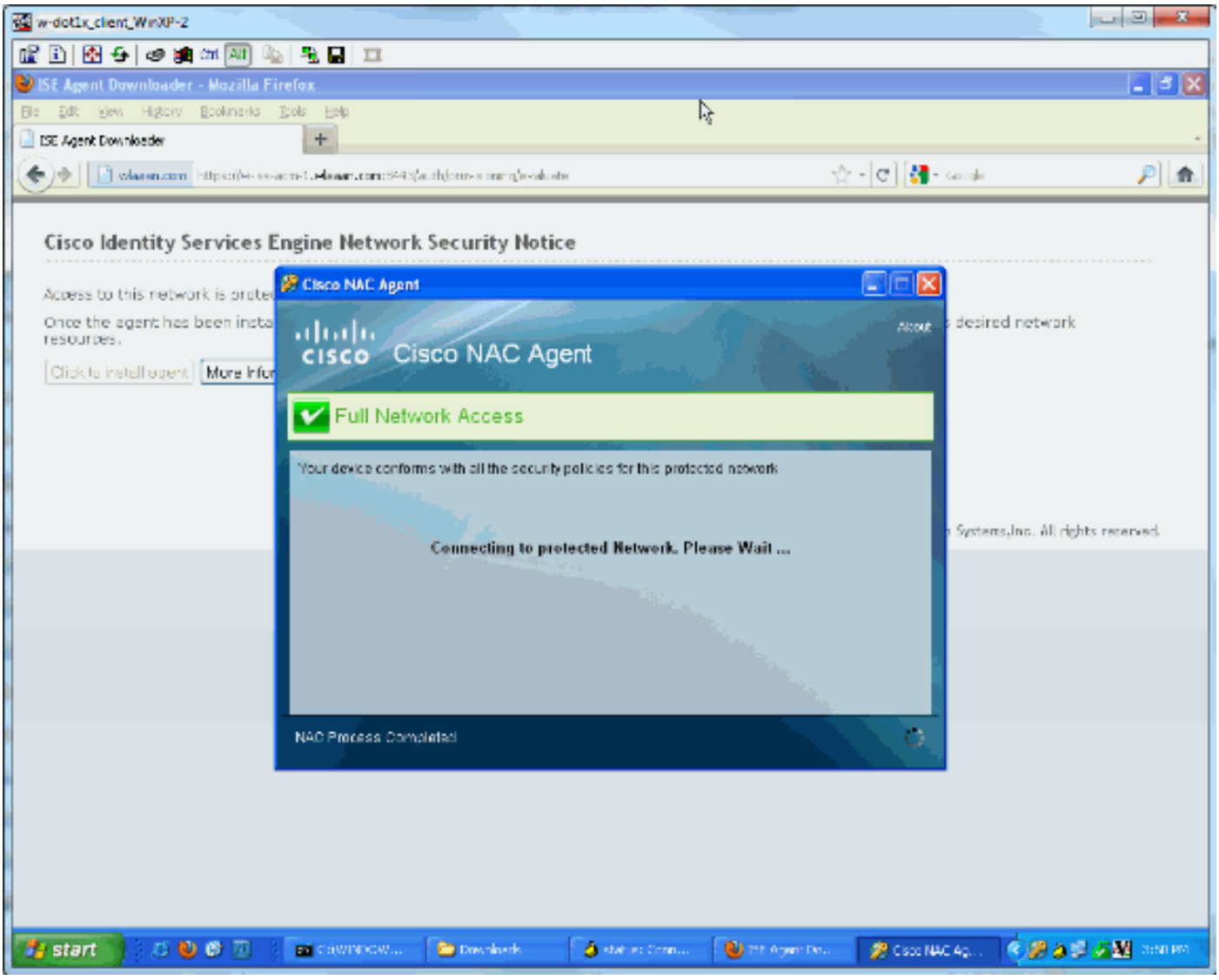
并且从iPEP ：

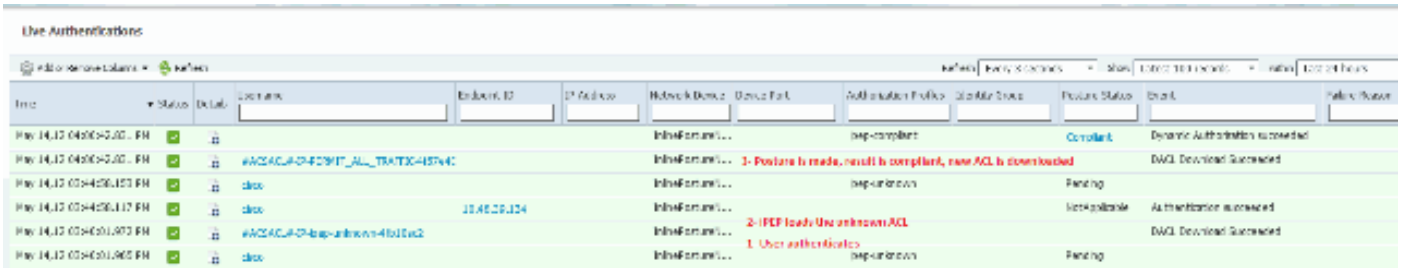
```
w-ise-ipep-1/admin# show pep table session

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
```

一旦代理程序下载并且安装：

代理程序应该自动地检测ISE并且运行状态评估(假设您把状态规则已经定义，是另一个主题)。在本例中，状态是成功的，并且这出现：





注意： 有在上面屏幕画面的两个认证。然而，因为iPEP方框缓存ACL，它每次没有下载。

在iPEP ：

```
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#
```

相关信息

- 技术支持和文档 - Cisco Systems