Postura Inline VPN usando o iPEP ISE e ASA

Índice

Introdução

Este documento fornece a informação em como estabelecer a postura inline com uma ferramenta de segurança adaptável (ASA) e um Identity Services Engine (ISE).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 8.2(4) para o ASA e na versão 1.1.0.665 para o ISE.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

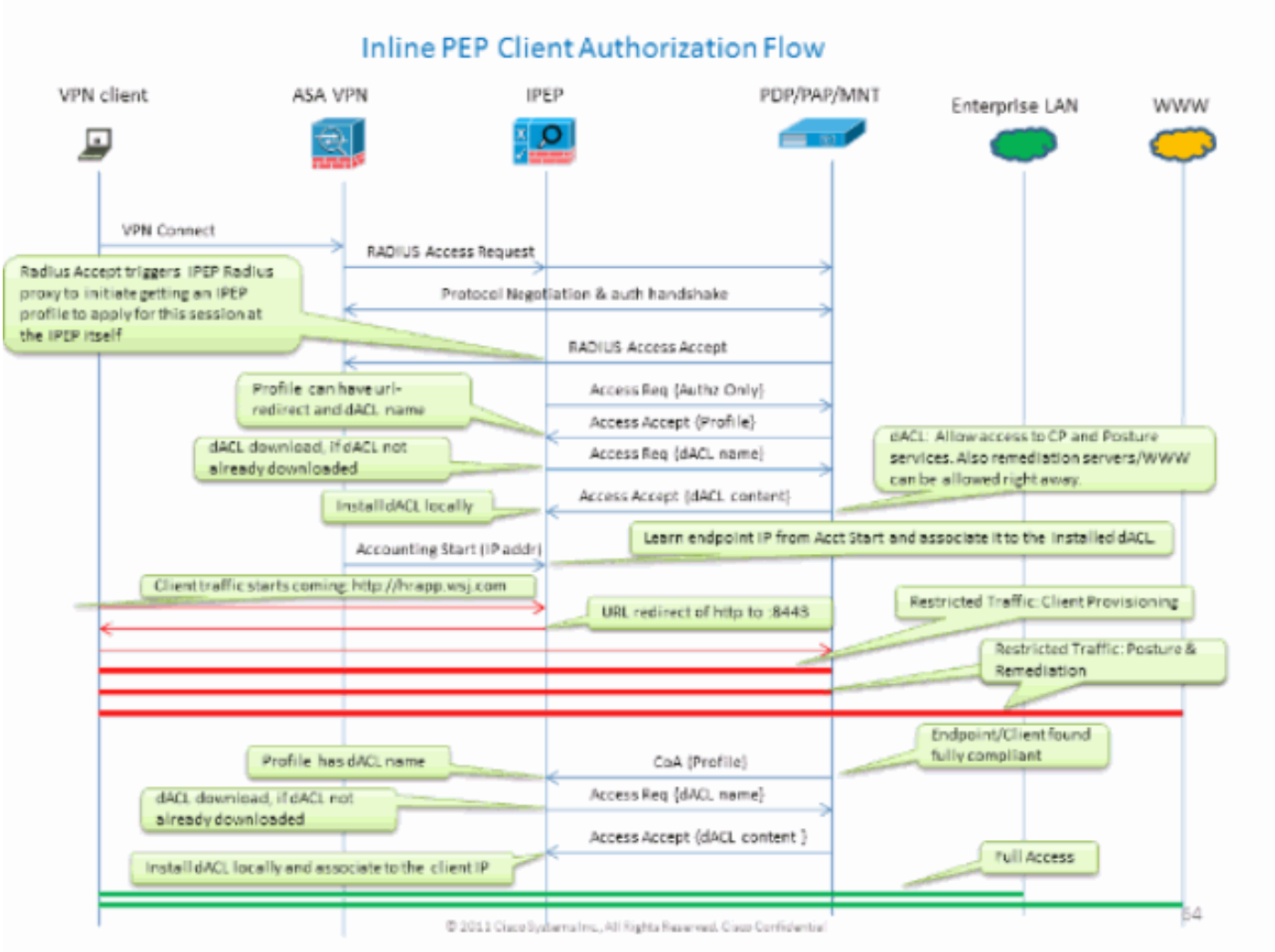
O ISE proporciona muitos serviços AAA (postura, perfilamento, autenticação, etc.). A mudança do raio do apoio de alguns dispositivos de rede (NAD) da autorização (CoA) que reserva mudar dinamicamente o perfil da autorização de um dispositivo final baseou em sua postura ou resultado do perfilamento. O outro NADs tal como o ASA não apoia esta característica ainda. Isto significa que um ISE que é executado no modo Inline da aplicação da postura (iPEP) está precisado de mudar dinamicamente a política do acesso de rede de um dispositivo final.

O conceito básico é que todo o tráfego de usuário atravessará o iPEP, com o nó igualmente que atua como um proxy RADIUS.

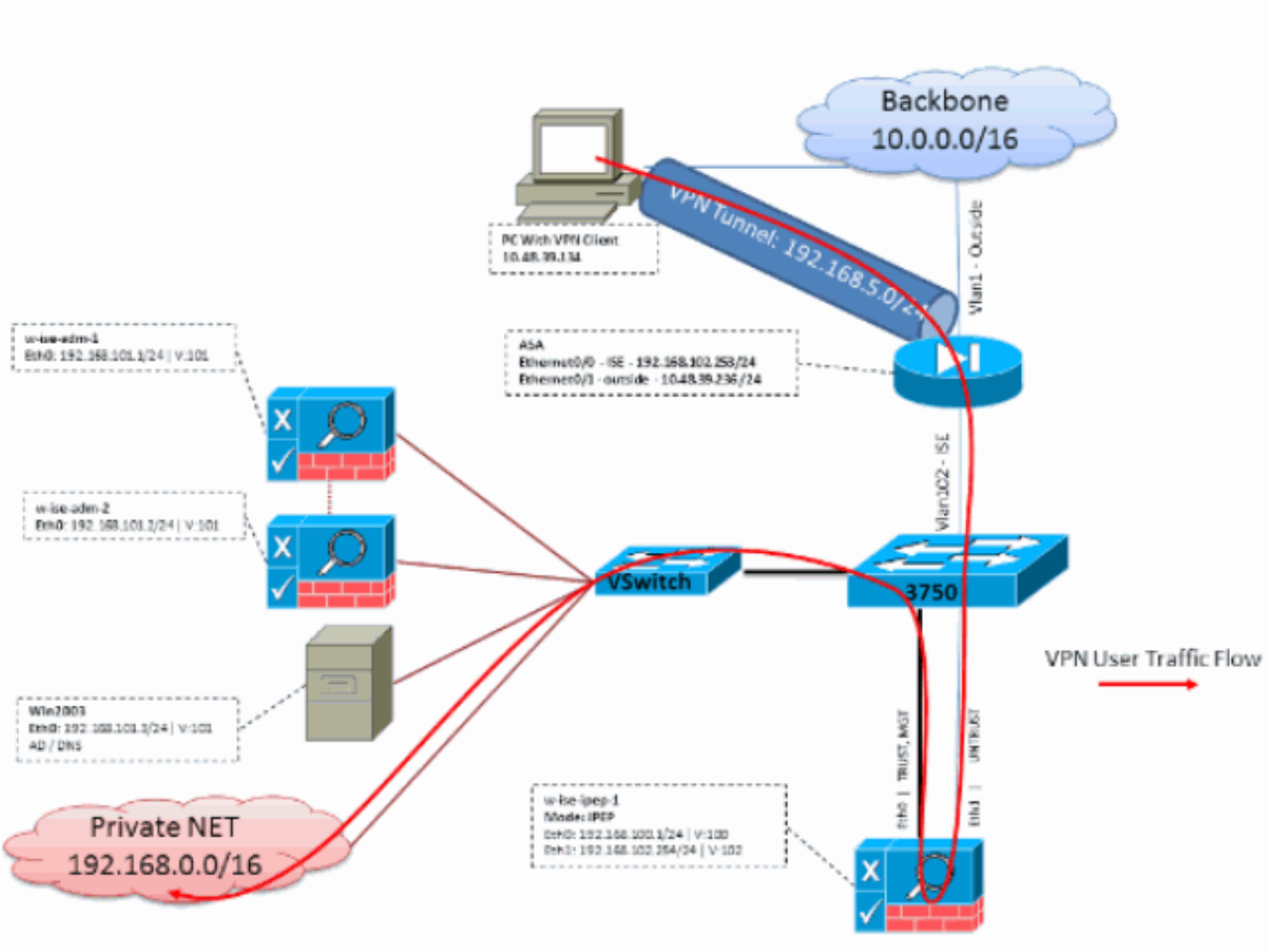
Fluxo básico

1. O usuário VPN entra.
2. O ASA envia o pedido ao nó do iPEP (ISE).
3. O iPEP reescreve o pedido (adicionando atributos do par Cisco AV para indicar isto é uma autenticação do iPEP) e envia o pedido ao nó da política ISE (PDP).
4. O PDP responde de volta ao iPEP que enviará ao NAD.
5. Se o usuário é autenticado, o NAD DEVE enviar um pedido do contabilidade-início (veja CSCtz84826). Isto provocará a iniciação de sessão no iPEP. Nesta fase, o usuário é reorientado para a postura. Adicionalmente, você precisa de permitir a ínterim-contabilidade-atualização para o túnel estabelecido do portal WebVPN, porque o ISE espera ter o Framed-IP-endereço do atributo na contabilidade do raio. Contudo, ao conectar ao portal, o endereço IP de Um ou Mais Servidores Cisco ICM NT VPN do cliente não é sabido ainda porque o túnel não está estabelecido. Isto assegurar-se-á de que o ASA envie atualizações provisórias, como quando o túnel será estabelecido.
6. O usuário atravessa a avaliação da postura, e baseado nos resultados o PDP atualizará a sessão usando o CoA no iPEP.

Este tiro de tela ilustra este processo:



Topologia de exemplo



Configuração ASA

A configuração ASA é um IPSec simples VPN remoto:

```
!
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 !
```

Configuração ISE

configuração do iPEP

A primeira coisa a fazer é adicionar um ISE como um nó do iPEP. Você pode encontrar a informação adicional sobre o processo aqui:

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

Este é basicamente o que você tem que configurar nas várias abas (os screenshots fornecidos nesta seção ilustram este):

- Configurar o IP do não-confiável e os ajustes do IP global (neste caso, o IP do não-confiável é 192.168.102.254).
- O desenvolvimento é modo distribuído.
- Põe um filtro estático para que o ASA seja reservado atravessar a caixa do iPEP (se não, a Conectividade para/desde o ISE através da caixa do iPEP é deixada cair).
- Configurar a política ISE como o servidor Radius e o ASA como o cliente RADIUS.
- Adicionar uma rota à sub-rede VPN esses pontos ao ASA.
- Ajuste o ISE de monitoração como o logging host (porta 20514 à revelia; neste caso, a política ISE está monitorando também).

Requisitos de configuração importantes do certificado:

Antes de tentar registrar um nó do iPEP, assegure-se de que o seguinte certificado Requisitos para Utilização chaves estendidos esteja encontrado. Se os Certificados não são configurados corretamente no iPEP e em Nós Admin, o processo de registro terminará. Contudo, você perderá o acesso admin ao nó do iPEP. Os seguintes detalhes foram extrapolados do guia de distribuição do iPEP ISE 1.1.x:

A presença de determinadas combinações de atributos nos Certificados locais da administração e dos Nós Inline da postura pode impedir que a autenticação mútua trabalhe.

Os atributos são:

- Uso chave prolongado (EKU) — Autenticação de servidor
- Uso chave prolongado (EKU) — Authenticação do cliente
- Tipo CERT de Netscape — Autenticação de servidor SSL
- Tipo CERT de Netscape — Autenticação de cliente SSL

Qualquer uma das seguintes combinações é exigida para o certificado da administração:

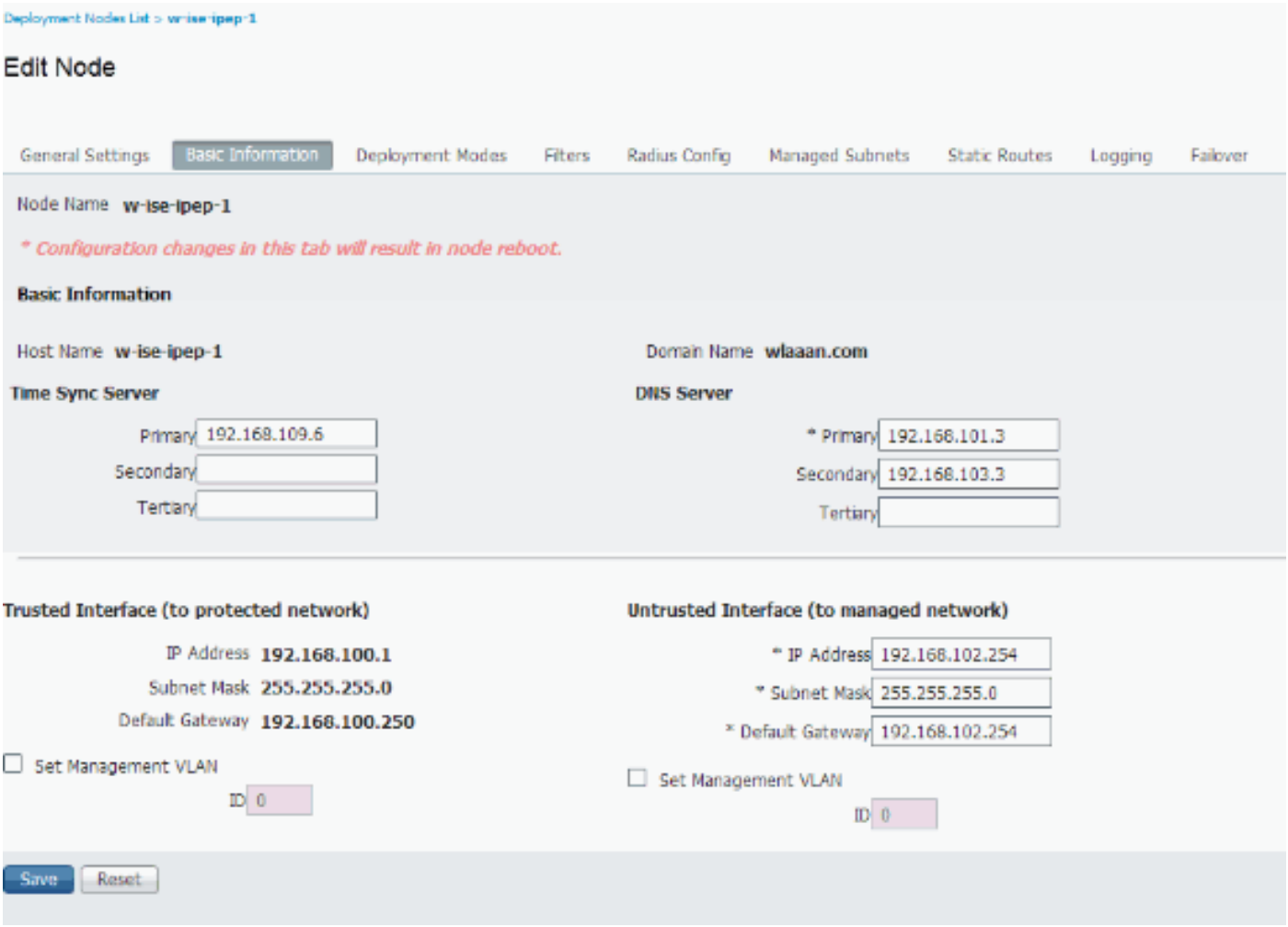
- Ambos os atributos EKU devem ser desabilitados, se ambos os atributos EKU são desabilitados no certificado Inline da postura, ou ambos os atributos EKU devem ser

permitidos, se o atributo do server é permitido no certificado Inline da postura.
- Ambo o tipo atributos CERT de Netscape deve ser desabilitado, ou ambos devem ser permitidos.

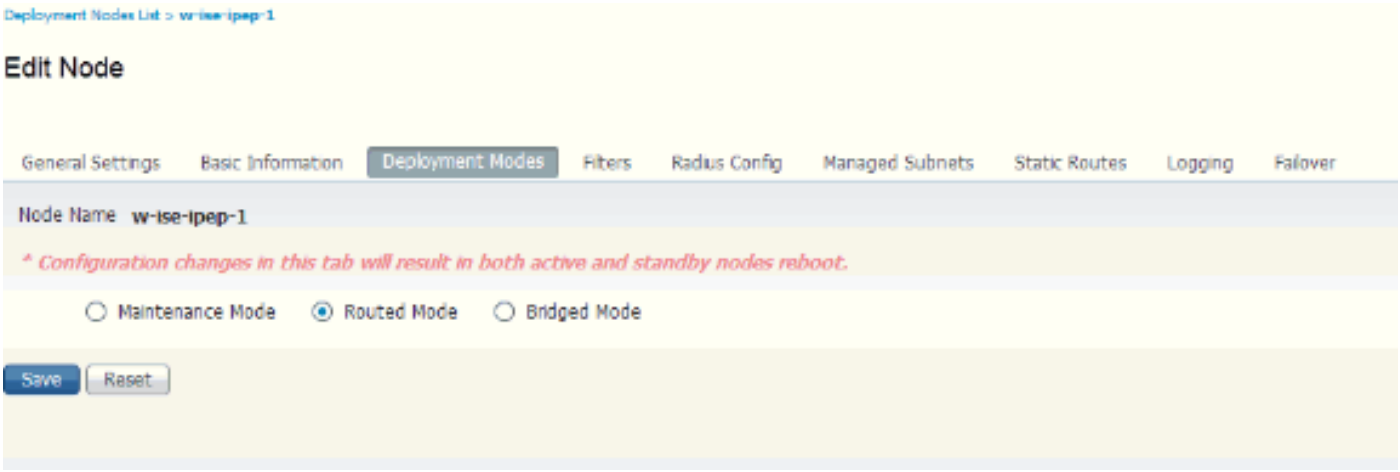
Qualquer uma das seguintes combinações é exigida para o certificado Inline da postura:

- Os atributos EKU devem ser desabilitados, ou ambos devem ser permitidos, ou o atributo do server apenas deve ser permitido.
- Ambo o tipo atributos CERT de Netscape deve ser desabilitado, ou ambos devem ser permitidos, ou o atributo do server apenas deve ser permitido.
- Onde os Certificados locais auto-assinados são usados na administração e nos Nós Inline da postura, você deve instalar o certificado auto-assinado do nó da administração na lista da confiança do nó Inline da postura. Além, se você tem Nós preliminares e secundários da administração em seu desenvolvimento, você deve instalar o certificado auto-assinado de ambos os Nós da administração na lista da confiança do nó Inline da postura.
- Onde os Certificados locais CA-assinados são usados na administração e nos Nós Inline da postura, a autenticação mútua deve trabalhar corretamente. Neste caso, o certificado de CA de assinatura é instalado no nó da administração antes do registro, e este certificado replicated ao nó Inline da postura.
- Se as chaves CA-emitidas estão usadas para uma comunicação de fixação entre a administração e os Nós Inline da postura, antes que você registre o nó Inline da postura, você deve adicionar a chave pública (certificado de CA) do nó da administração à lista do certificado de CA do nó Inline da postura.

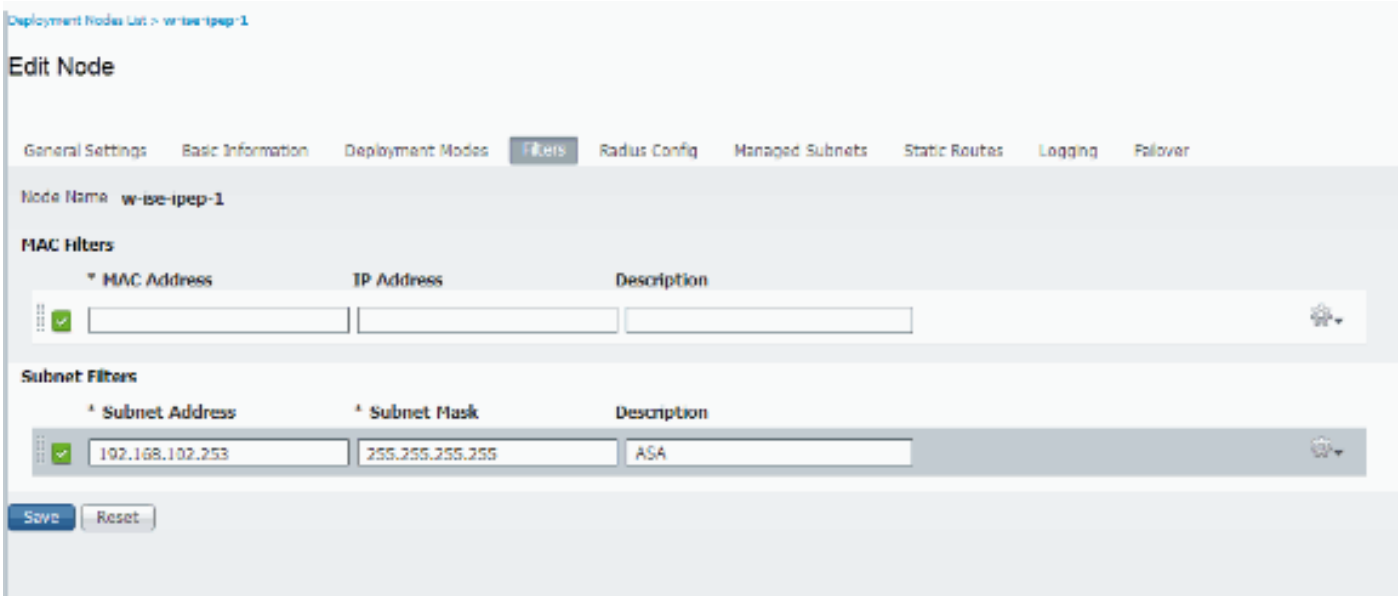
Configuração básica:



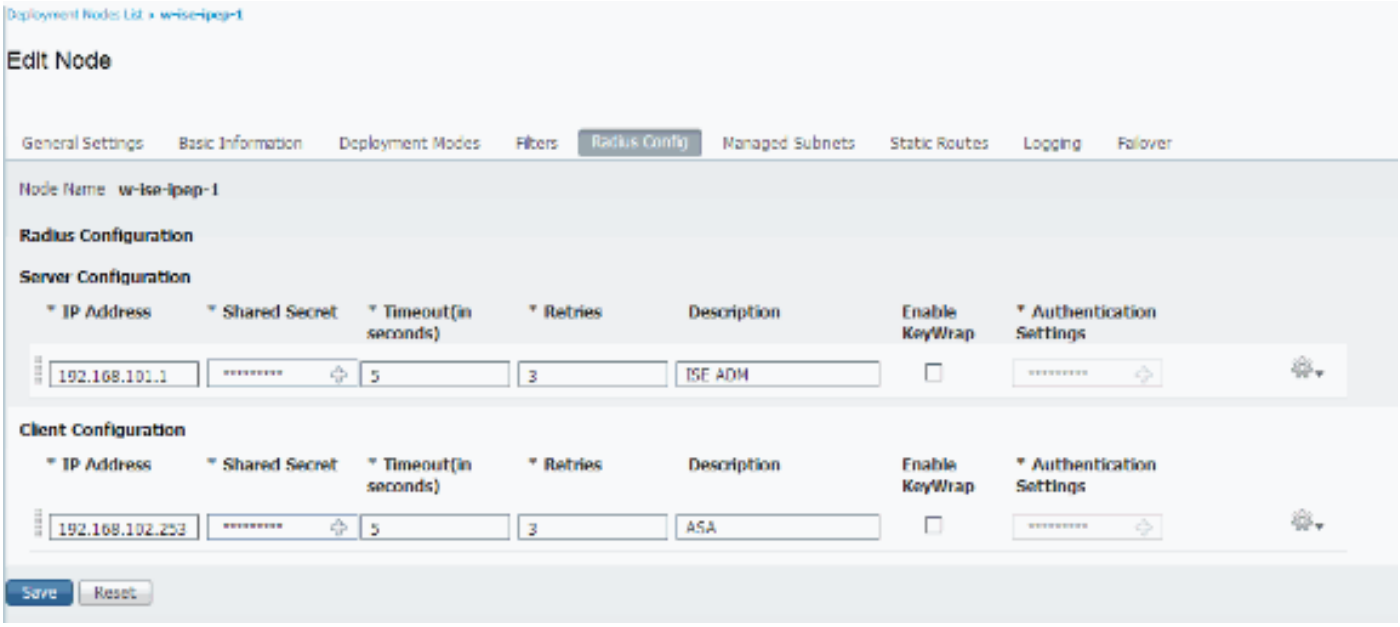
Configuração de modo do desenvolvimento:



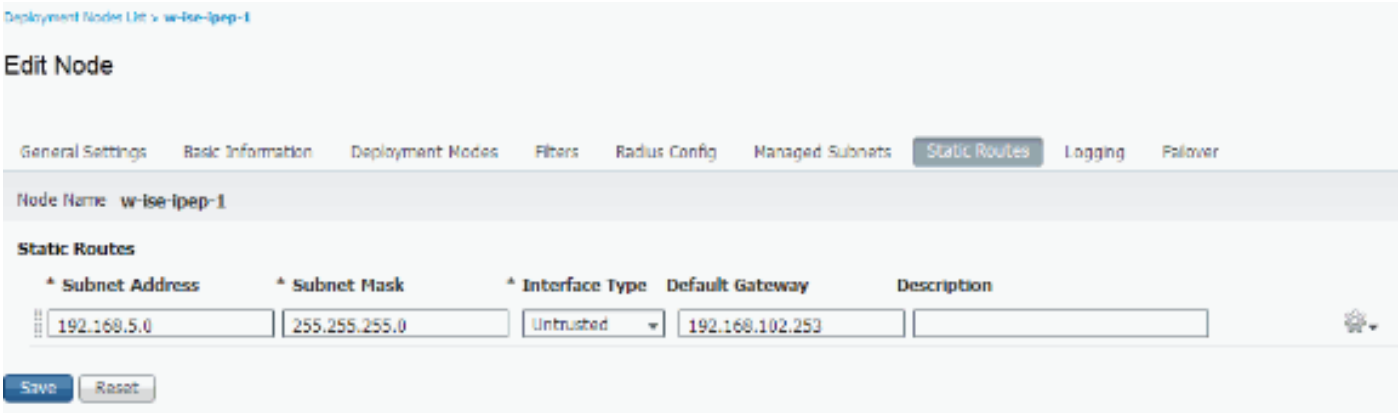
Configuração de filtros:



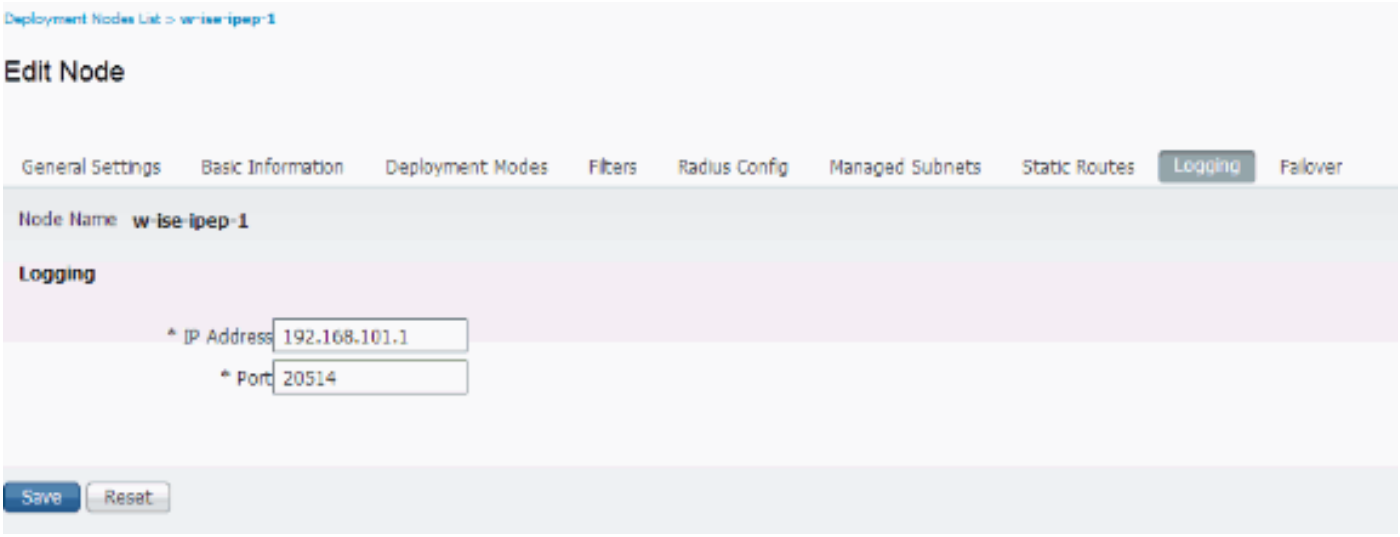
Configuração RADIUS:



Rotas estáticas:



Registro:



Autenticação e configuração da postura

Há três estados da postura:

- Desconhecido: A postura não é feita ainda
- Complacente: A postura é feita e o sistema é complacente
- NON-complacente: A postura é feita, mas o sistema falhou pelo menos uma verificação

Agora os perfis da autorização têm que ser criados (que serão autorização Inline perfilam: Isto adicionará o atributo do ipep-authz=true no par Cisco AV) que será usado para o caso diferente.

Geralmente, o perfil desconhecido retorna a reorientação URL (descoberta da postura) que enviará o tráfego do usuário ao ISE e o pedirá para instalar o agente NAC. Se o agente NAC é instalado já, este permitirá que seu pedido da descoberta HTTP esteja enviado ao ISE.

Neste perfil, um ACL que reserve tráfego de HTTP ao ISE e o DNS pelo menos são usados.

Os perfis complacentes e NON-complacentes retornam geralmente um ACL baixável para conceder o acesso de rede baseado no perfil de usuário. o perfil NON-complacente pode permitir que os usuários alcancem um servidor de Web para transferir um Antivirus por exemplo, ou conceda acesso de rede limitado.

Neste exemplo, os perfis desconhecidos e complacentes estão criados, e a presença de notepad.exe enquanto as exigências são verificadas.

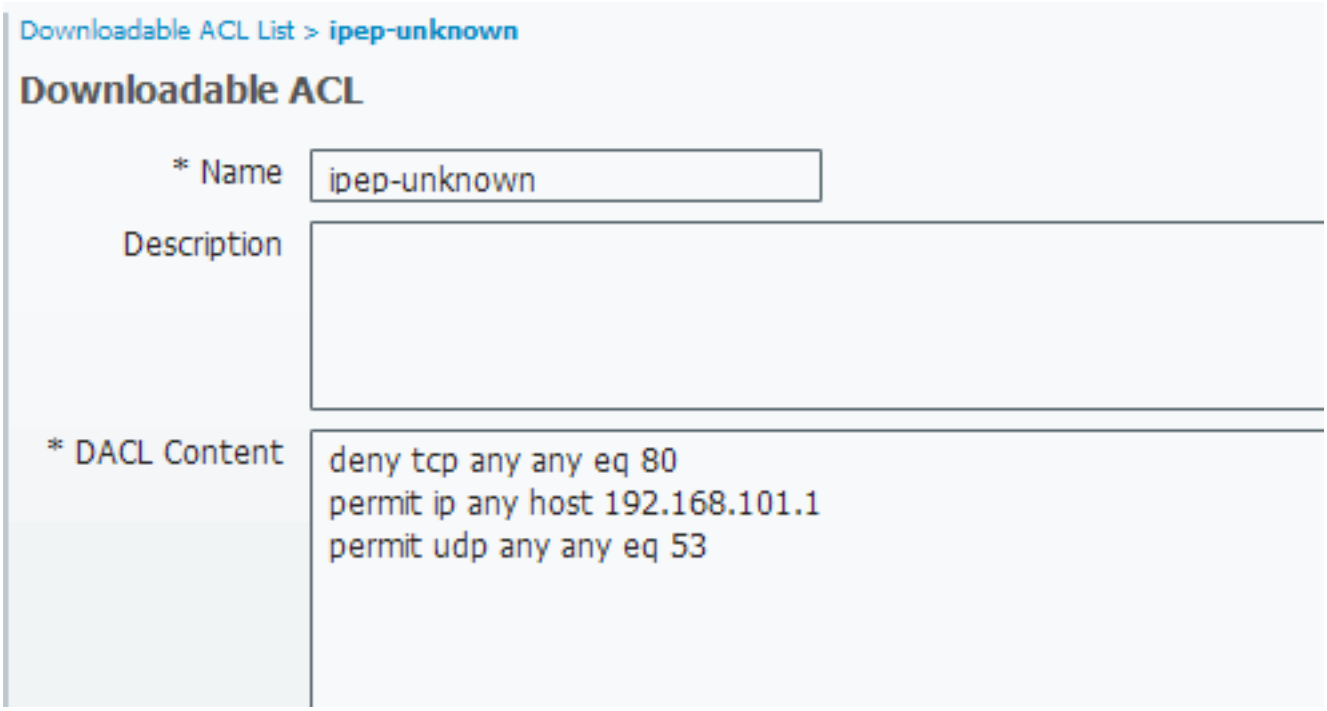
A postura perfila a configuração

A primeira coisa a fazer é criar os ACL carregável (dACL) e perfis:

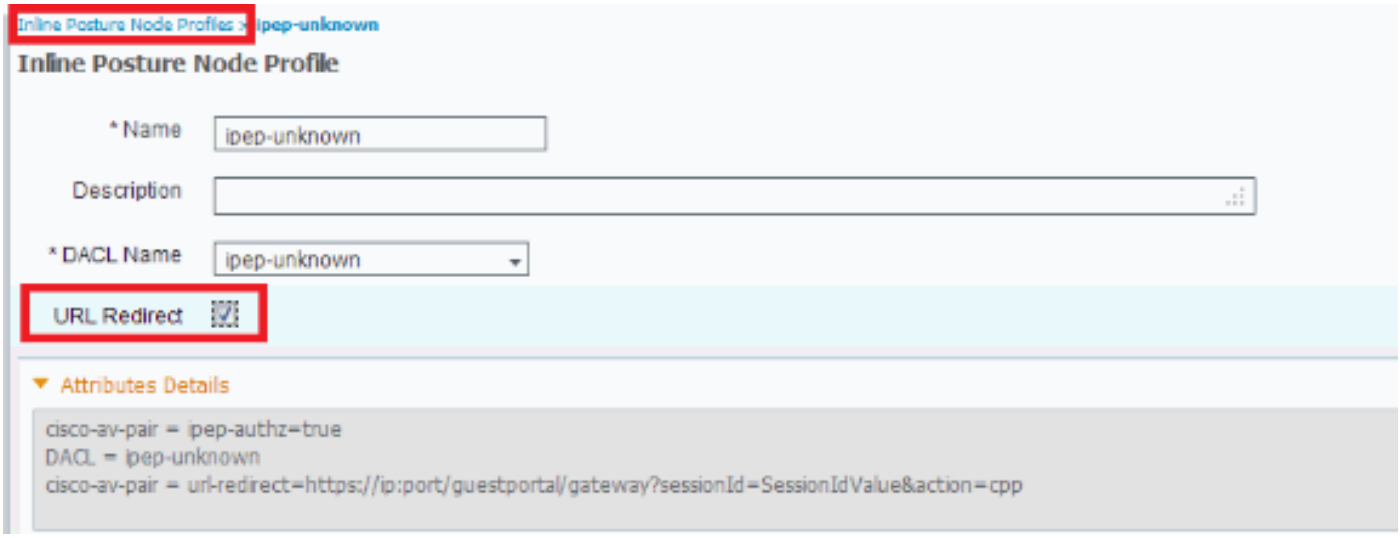
Note: Isto não é imperativo para ter o nome do dACL que combina o nome de perfil.

- ComplacenteACL: ipep-desconhecidoPerfil da autorização: ipep-desconhecido
- NON-complacenteACL: ipep-NON-complacentePerfil da autorização: ipep-NON-complacente

DACL desconhecido:

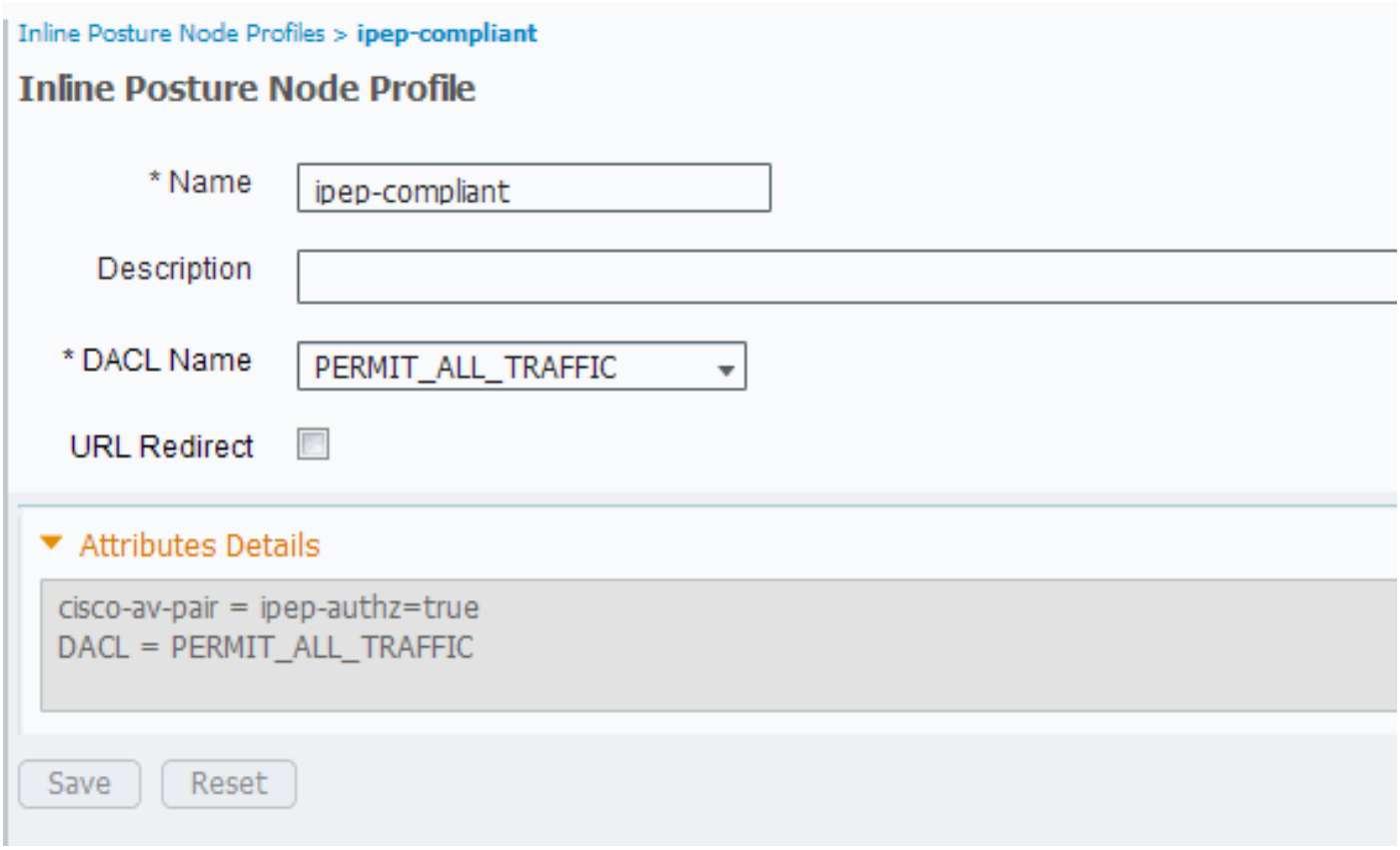


Perfil desconhecido:



DACL complacente:

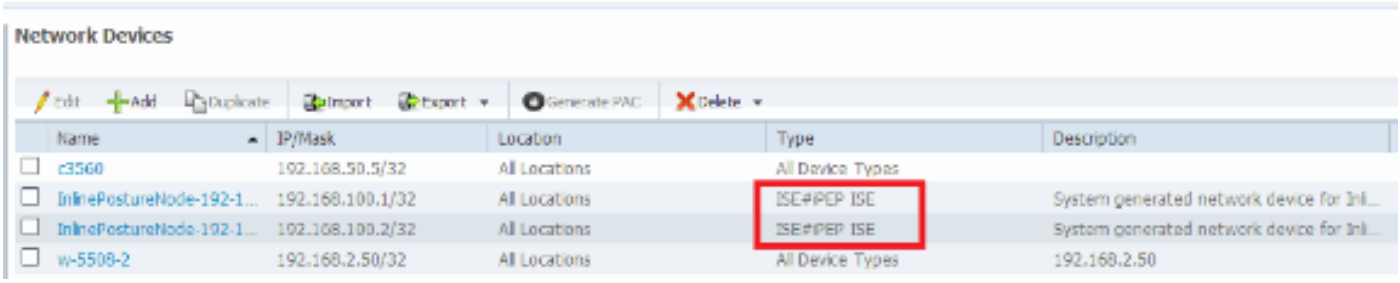
Perfil complacente:



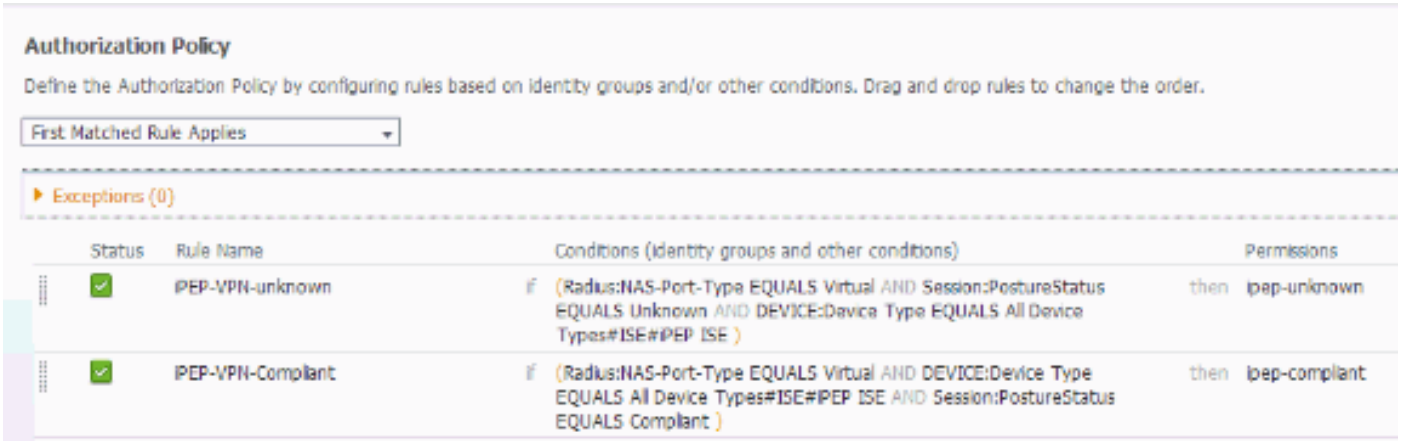
Configuração de autorização

Agora que o perfil é criado, você precisa de combinar a requisição RADIUS que vem do iPEP e de aplicar-lhes os perfis do direito. O iPEP ISE é definido com um tipo de dispositivo especial que seja usado nas regras da autorização:

NADs:

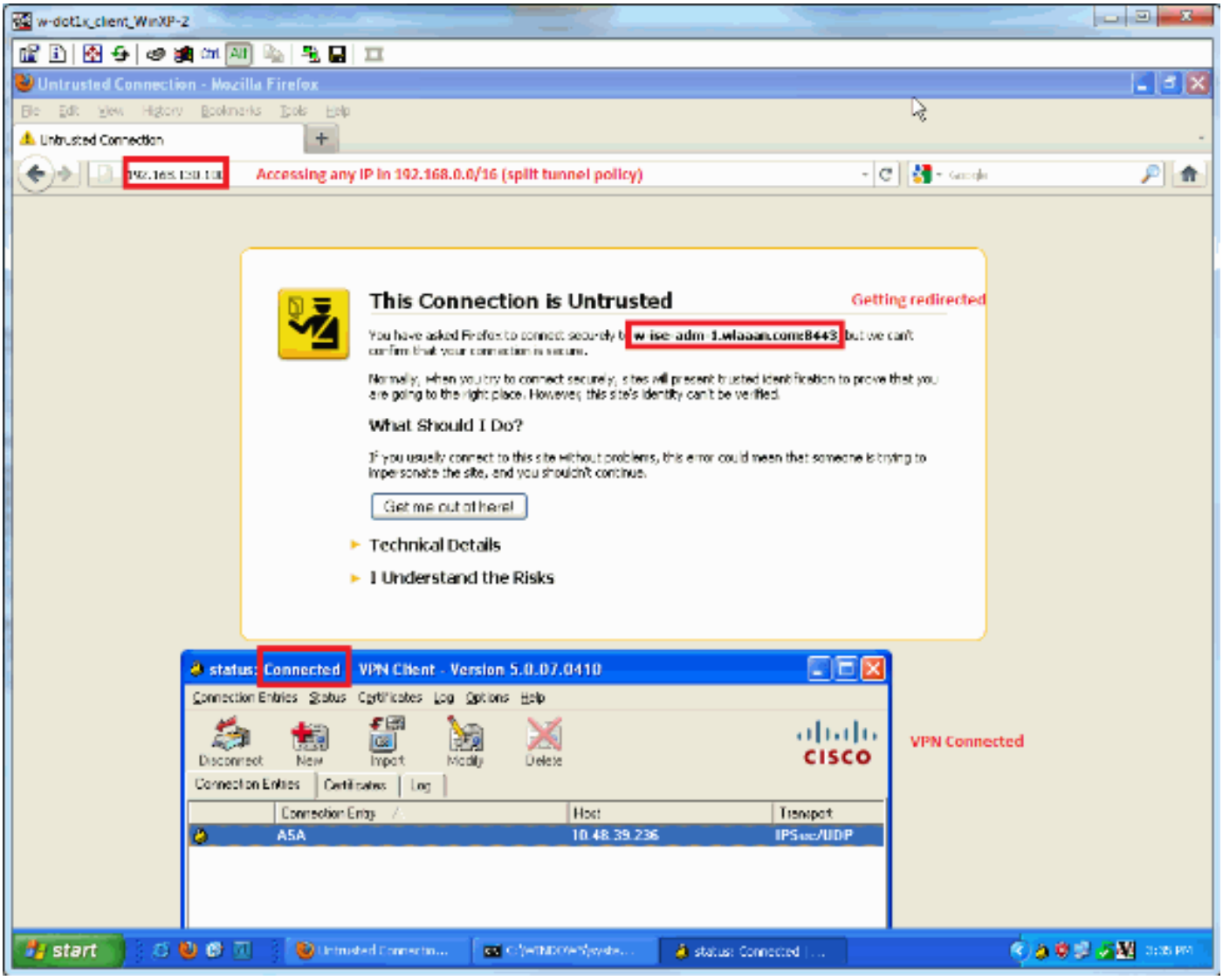


Autorização:

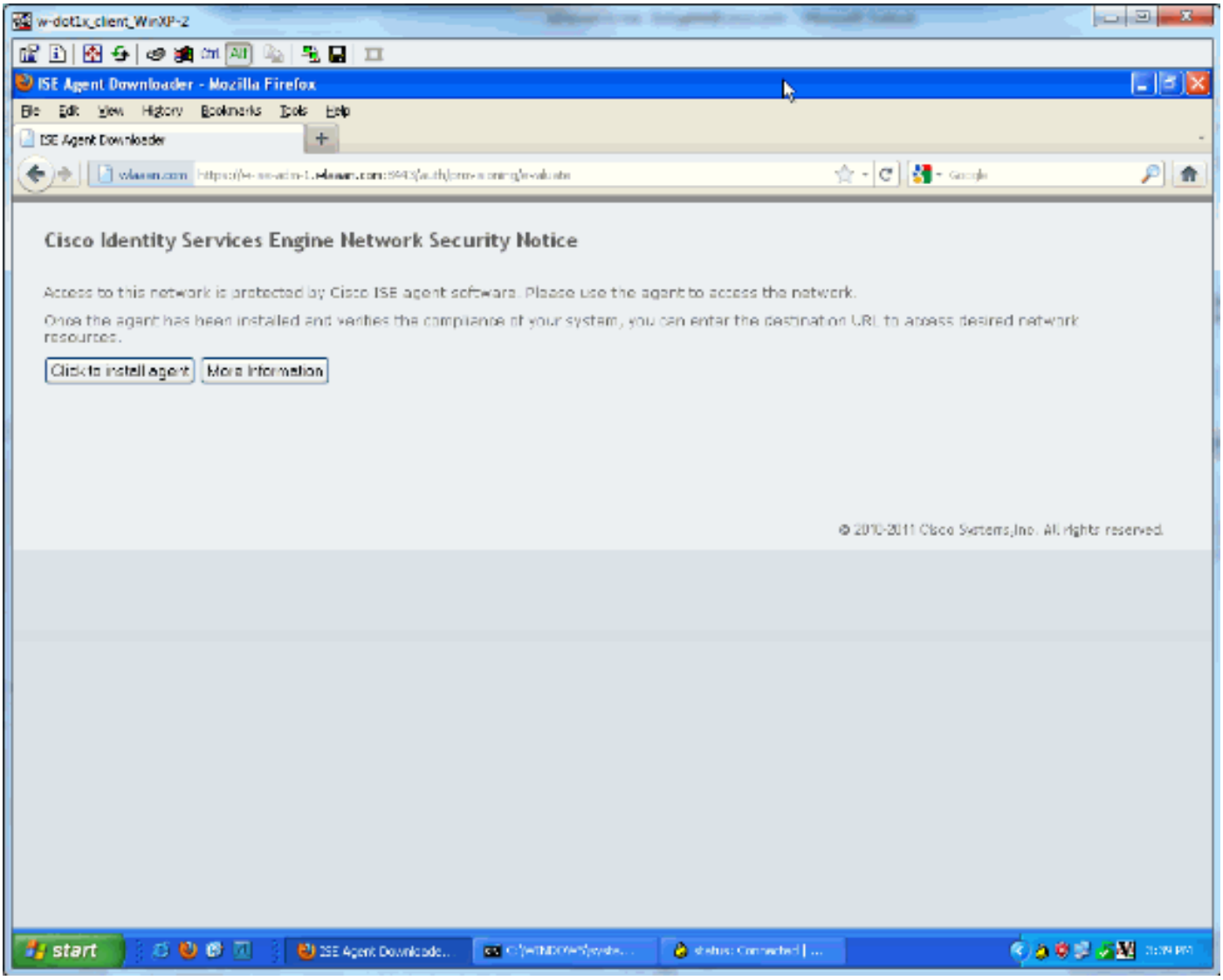


Note: Se o agente não é instalado na máquina, você pode definir regras do abastecimento do cliente.

Resultado



Você é alertado instalar o agente (neste exemplo, o abastecimento do cliente é ajustado já):



Alguma saída nesta fase:

```
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
```

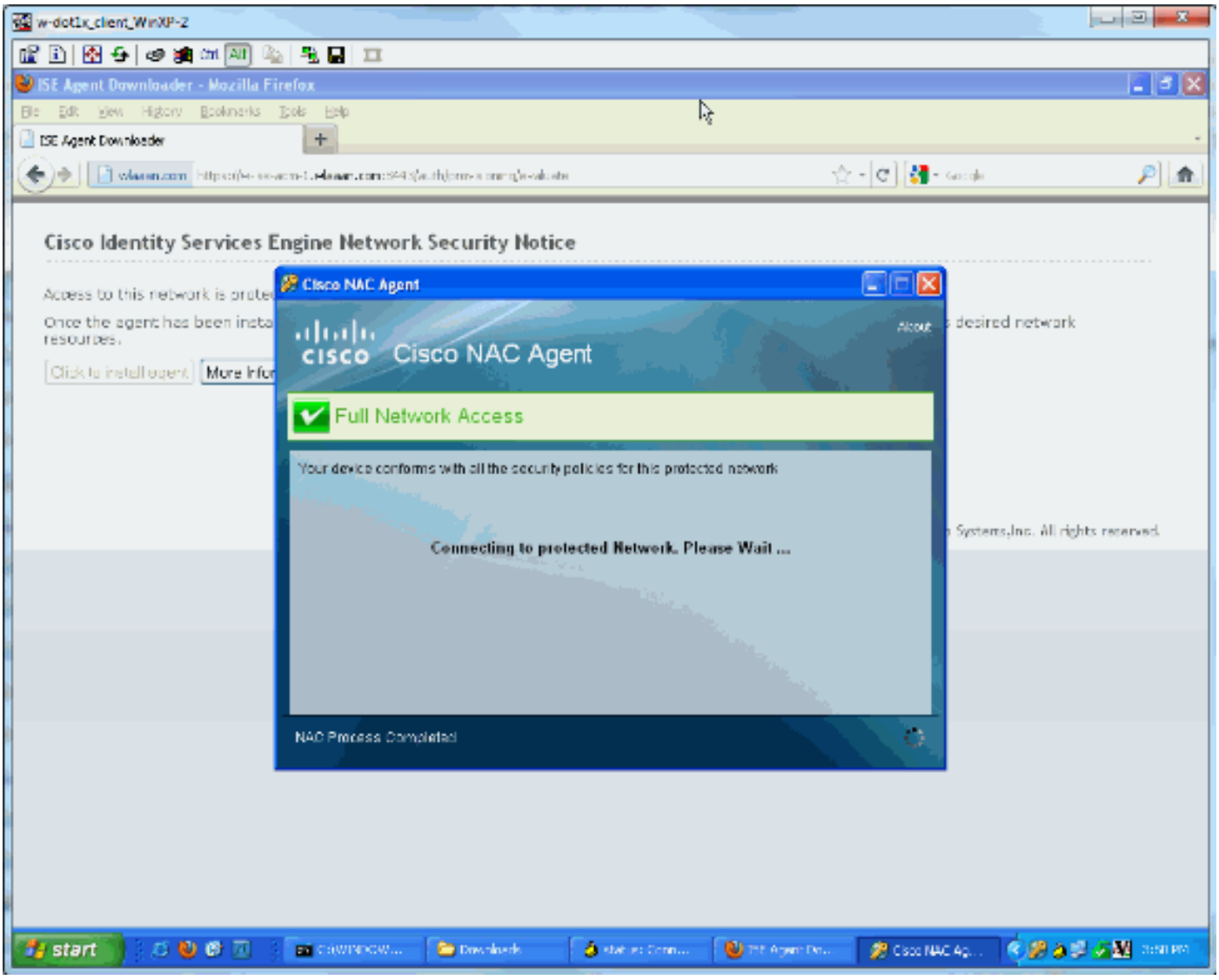
E do iPEP:

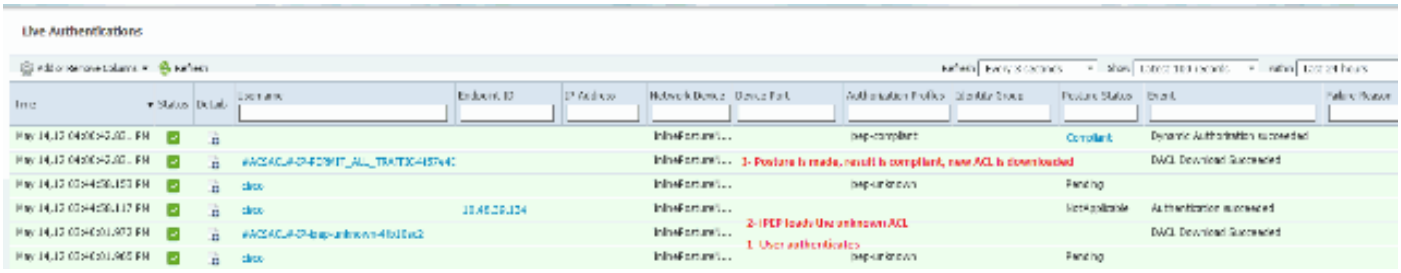
```
w-ise-ipep-1/admin# show pep table session

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
```

Uma vez que o agente é transferido e instalado:

O agente deve automaticamente detectar o ISE e executa a avaliação da postura (que supõe o tenha as regras da postura definidas já, que é um outro assunto). Neste exemplo, a postura é bem sucedida, e esta aparece:





Note: Há duas autenticações no tiro de tela acima. Contudo, porque a caixa do iPEP põe em esconderijo os ACL, não é transferido todas as vezes.

No 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#
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems