Posture intégrée VPN utilisant l'iPEP ISE et ASA

Contenu

Introduction

Ce document fournit des informations sur la façon dont installer la posture intégrée avec une appliance de sécurité adaptable (ASA) et un Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version 8.2(4) pour l'ASA et la version 1.1.0.665 pour l'ISE.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

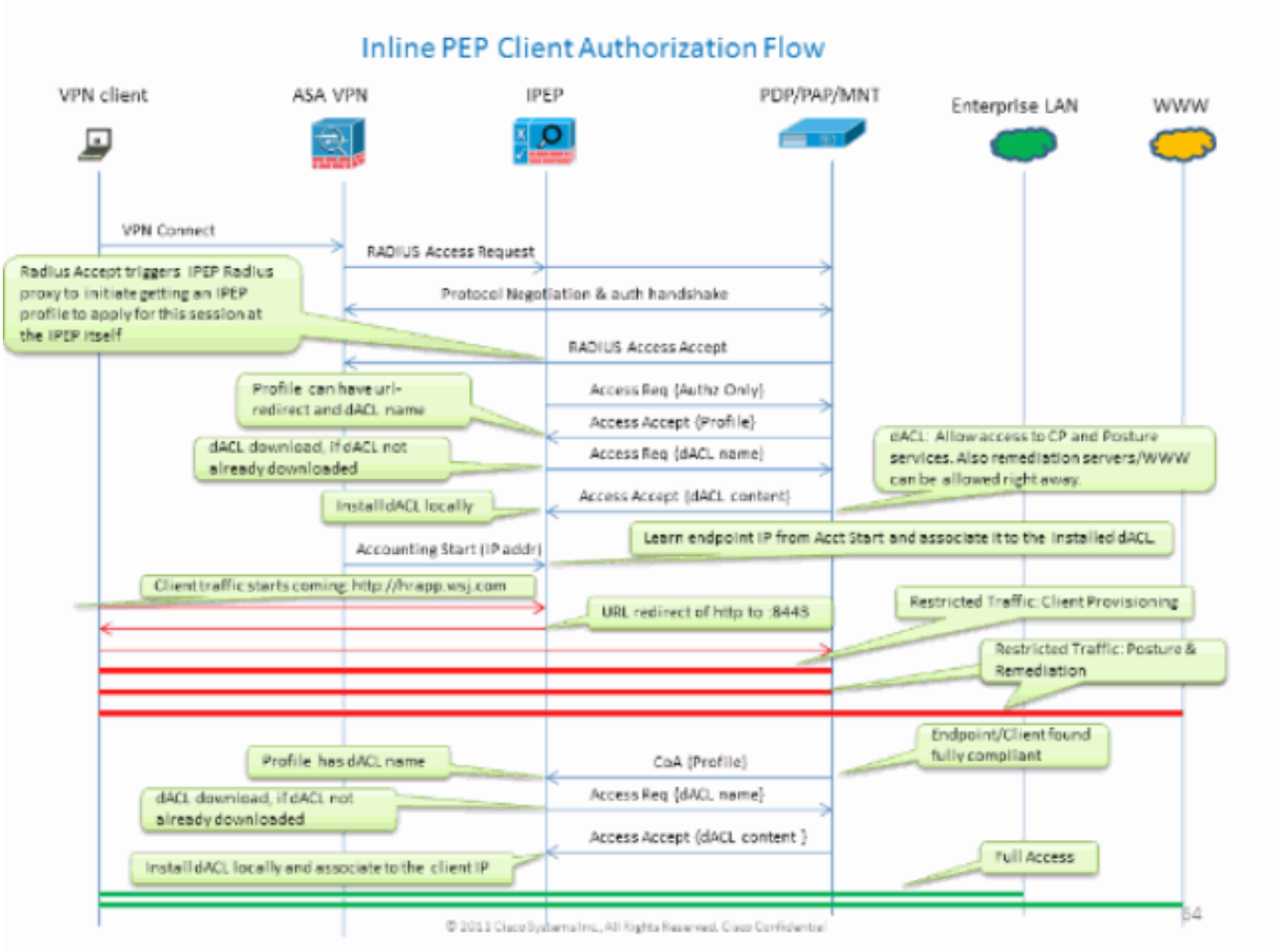
L'ISE fournit beaucoup de services d'AAA (posture, profilage, authentification, etc.). Une certaine modification de Radius de support des périphériques de réseau (NAD) de l'autorisation (CoA) qui laisse changer dynamiquement le profil d'autorisation d'une extrémité périphérique basée sur sa posture ou profilante le résultat. L'autre NADs tel que l'ASA ne prennent en charge pas cette caractéristique encore. Ceci signifie qu'une exécution ISE en mode intégré d'application de posture (iPEP) est nécessaire pour changer dynamiquement la stratégie d'accès au réseau d'un périphérique d'extrémité.

Le concept de base est que tout le trafic d'utilisateur passera par l'iPEP, avec le noeud agissant également en tant que proxy RADIUS.

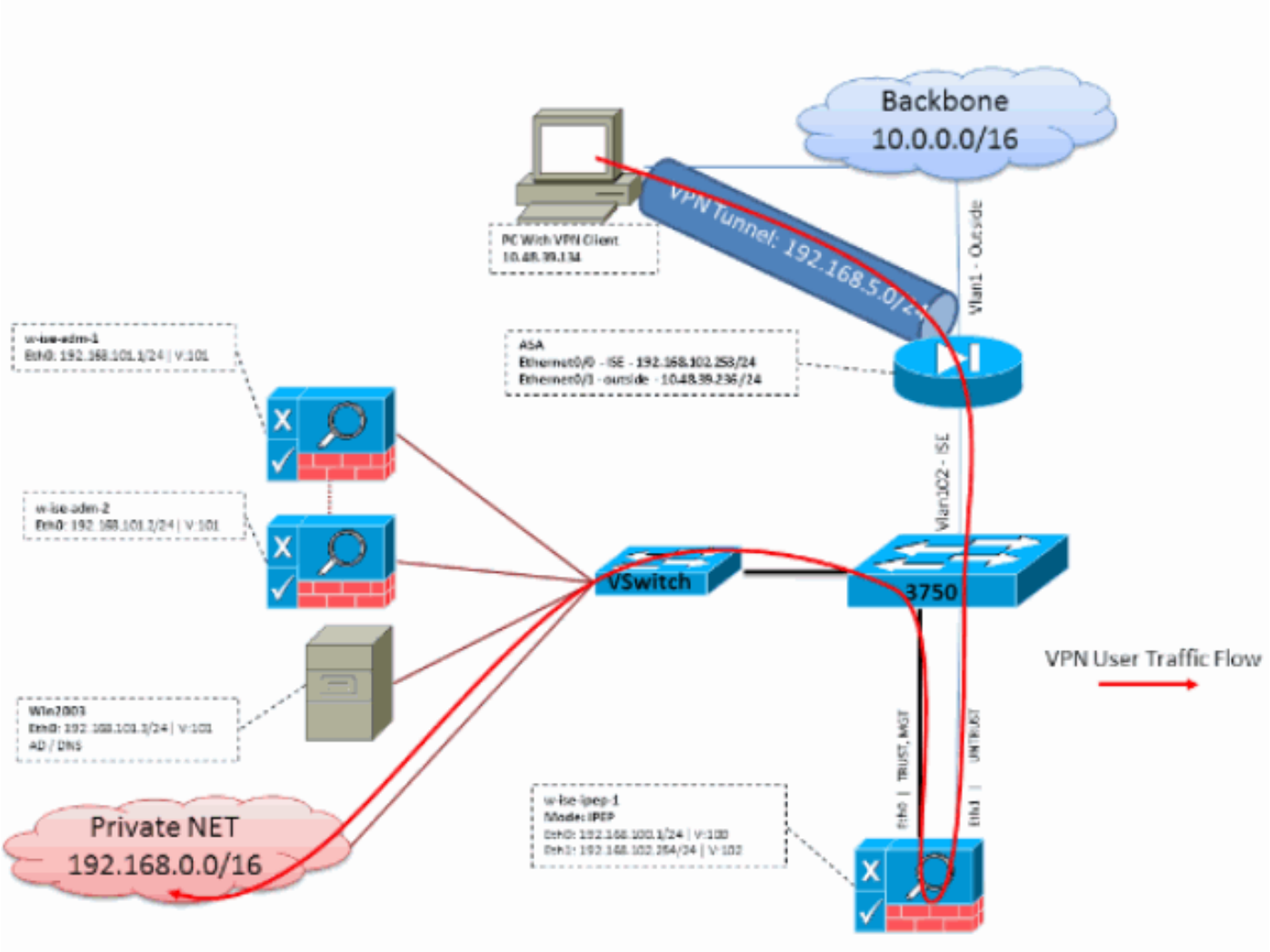
Écoulement de base

1. Logins d'utilisateur VPN.
2. L'ASA envoie la demande au noeud d'iPEP (ISE).
3. L'iPEP réécrit la demande (en ajoutant des attributs de PAIRE AV de Cisco pour indiquer ceci est une authentification d'iPEP) et envoie la demande au noeud de stratégie ISE (PDP).
4. Le PDP répond de nouveau à l'iPEP qui expédiera au NAD.
5. Si l'utilisateur est authentifié, le NAD DOIT envoyer une demande de comptabilité-commencement (voir le CSCtz84826). Ceci déclenchera l'initiation de session sur l'iPEP. À ce stade, l'utilisateur est réorienté pour la posture. Supplémentaire, vous devez activer l'intérim-comptabilité-mise à jour pour le tunnel établi du portail de WEBVPN, car l'ISE compte avoir l'encadrer-IP-adresse d'attribut en comptabilité de rayon. Cependant, en se connectant au portail, l'adresse IP VPN du client n'est pas encore connue parce que le tunnel n'est pas établi. Ceci s'assurera que l'ASA enverra les mises à jour intérimaires, comme quand le tunnel sera établi.
6. L'utilisateur passe par l'estimation de posture, et basé sur les résultats le PDP mettra à jour la session utilisant le CoA sur l'iPEP.

Ce tir d'écran illustre ce processus :



Exemple de topologie



Configuration ASA

La configuration ASA est un distant simple VPN IPSEC :

```
!
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 !
```

Configuration ISE

configuration d'iPEP

La première chose à faire est d'ajouter un ISE comme noeud d'iPEP. Vous pouvez trouver les informations complémentaires au sujet du processus ici :

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

Est fondamentalement ce ce que vous devez configurer dans les divers onglets (les captures d'écran fournies dans cette section illustrent ceci) :

- Configurez l'IP non approuvé et les paramètres IP globaux (dans ce cas, l'IP non approuvé est 192.168.102.254).
- Le déploiement est mode conduit.
- Mettez un filtre statique pour qu'on laisse l'ASA passer par la case d'iPEP (autrement, la Connectivité à/de l'ISE par la case d'iPEP est abandonnée).
- Configurez la stratégie ISE comme serveur de Radius et l'ASA comme client RADIUS.
- Ajoutez une artère au sous-réseau VPN ces points à l'ASA.
- Placez l'ISE de surveillance comme hôte de journalisation (port 20514 par défaut ; dans ce cas, la stratégie ISE surveille aussi bien).

Importantes configurations requises de certificat :

Avant de tenter pour enregistrer un noeud d'iPEP, assurez-vous que le certificat suivant des conditions requises étendues d'utilisation principale sont rencontrés. Si les Certificats ne sont pas correctement configurés sur l'iPEP et les Noeuds d'admin, la procédure d'enregistrement se terminera. Cependant, vous perdrez l'accès d'admin au noeud d'iPEP. Les détails suivants ont été extrapolés du guide de déploiement d'iPEP ISE 1.1.x :

La présence de certaines combinaisons des attributs dans les Certificats locaux des Noeuds de posture de gestion et d'en ligne peut empêcher l'authentification mutuelle de fonctionner.

Les attributs sont :

- Utilisation principale étendue (EKU) — Authentification de serveur
- Utilisation principale étendue (EKU) — Authentification client
- Type de CERT de Netscape — Authentification de serveur SSL
- Type de CERT de Netscape — Authentification client SSL

L'un ou l'autre des combinaisons suivantes est exigée pour le certificat de gestion :

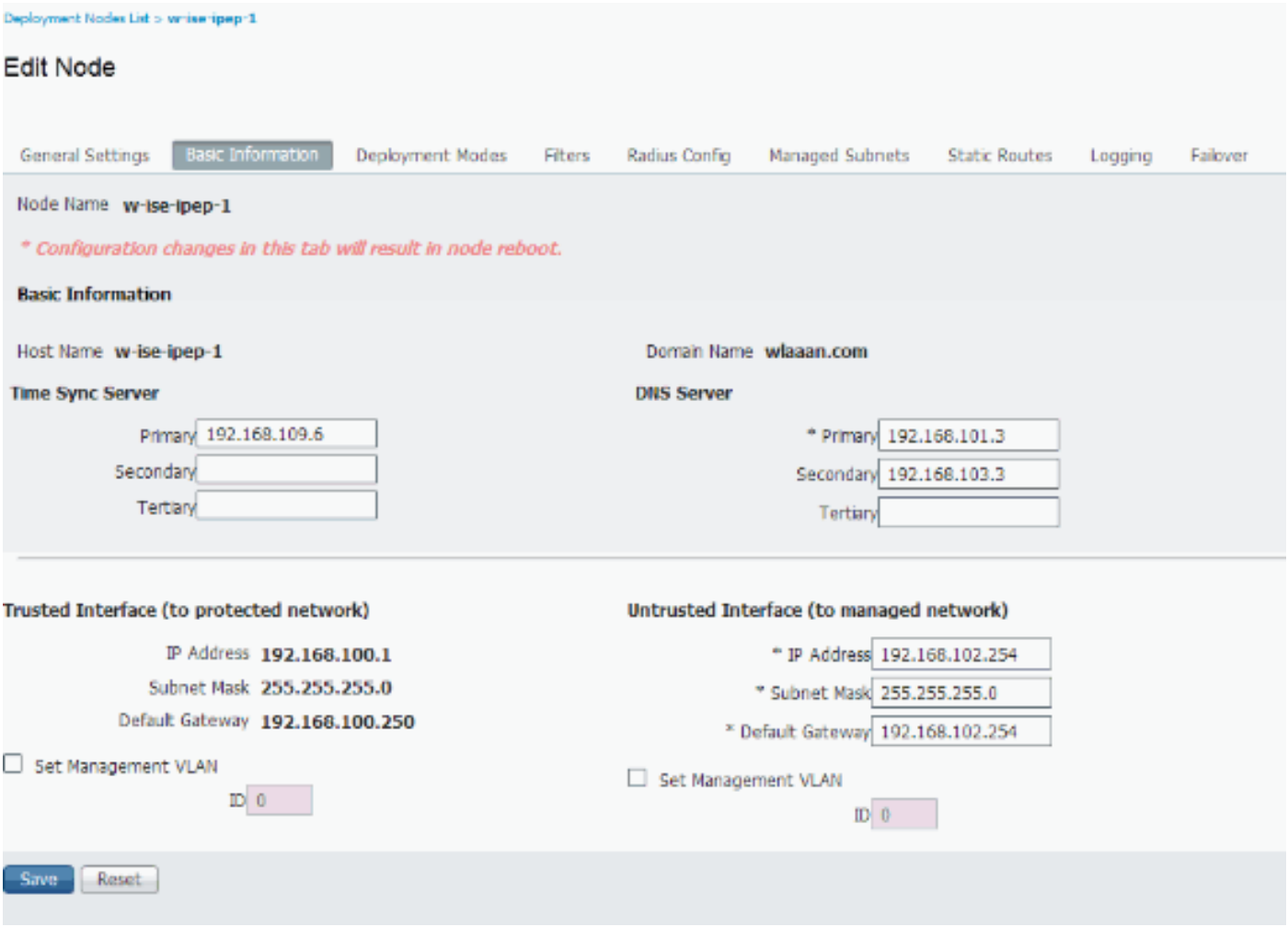
- Les deux attributs EKU devraient être désactivés, si les deux attributs EKU sont désactivés dans le certificat intégré de posture, ou les deux attributs EKU devraient être activés, si

l'attribut de serveur est activé dans le certificat intégré de posture.
- Les deux attributs de type de CERT de Netscape devraient être désactivés, ou chacun des deux devraient être activés.

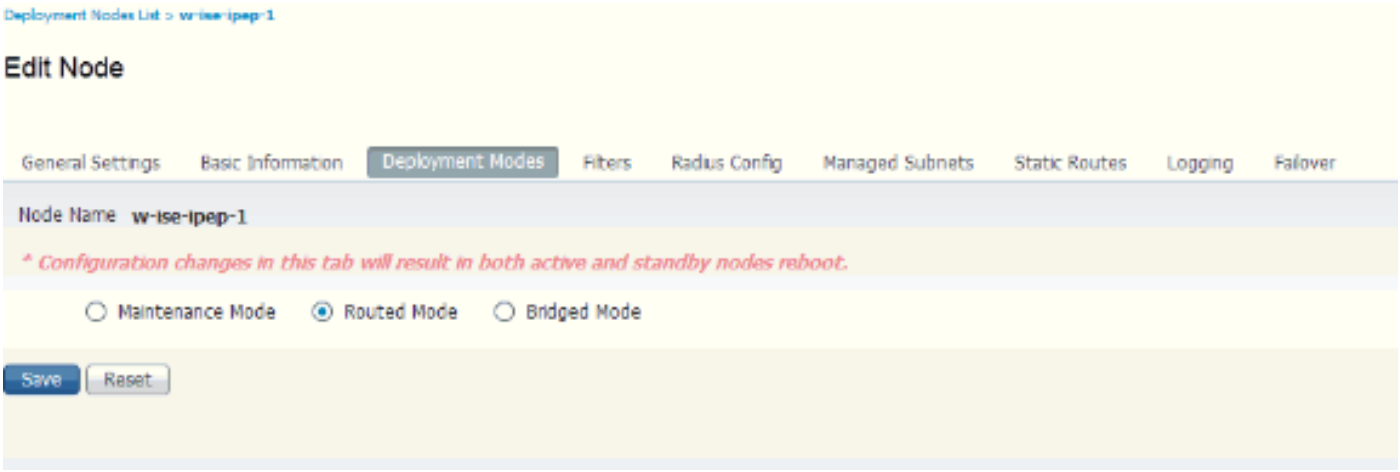
L'un ou l'autre des combinaisons suivantes est exigée pour le certificat intégré de posture :

- Les deux attributs EKU devraient être désactivés, ou chacun des deux devraient être activés, ou seul l'attribut de serveur devrait être activé.
- Les deux attributs de type de CERT de Netscape devraient être désactivés, ou chacun des deux devraient être activés, ou seul l'attribut de serveur devrait être activé.
- Là où des Certificats locaux auto-signés sont utilisés sur les Noeuds de posture de gestion et d'en ligne, vous devez installer le certificat auto-signé du noeud de gestion dans la liste de confiance du noeud intégré de posture. En outre, si vous avez les Noeuds primaires et secondaires de gestion dans votre déploiement, vous devez installer le certificat auto-signé des deux Noeuds de gestion dans la liste de confiance du noeud intégré de posture.
- Là où des Certificats locaux Ca-signés sont utilisés sur les Noeuds de posture de gestion et d'en ligne, l'authentification mutuelle devrait fonctionner correctement. Dans ce cas, le certificat du CA de signature est installé sur le noeud de gestion avant l'enregistrement, et ce certificat est répliqué vers le noeud intégré de posture.
- Si des clés Ca-émises sont utilisées pour sécuriser la transmission entre la gestion et les Noeuds de posture d'en ligne, avant que vous enregistriez le noeud intégré de posture, vous devez ajouter la clé publique (certificat de CA) du noeud de gestion à la liste de certificat de CA du noeud intégré de posture.

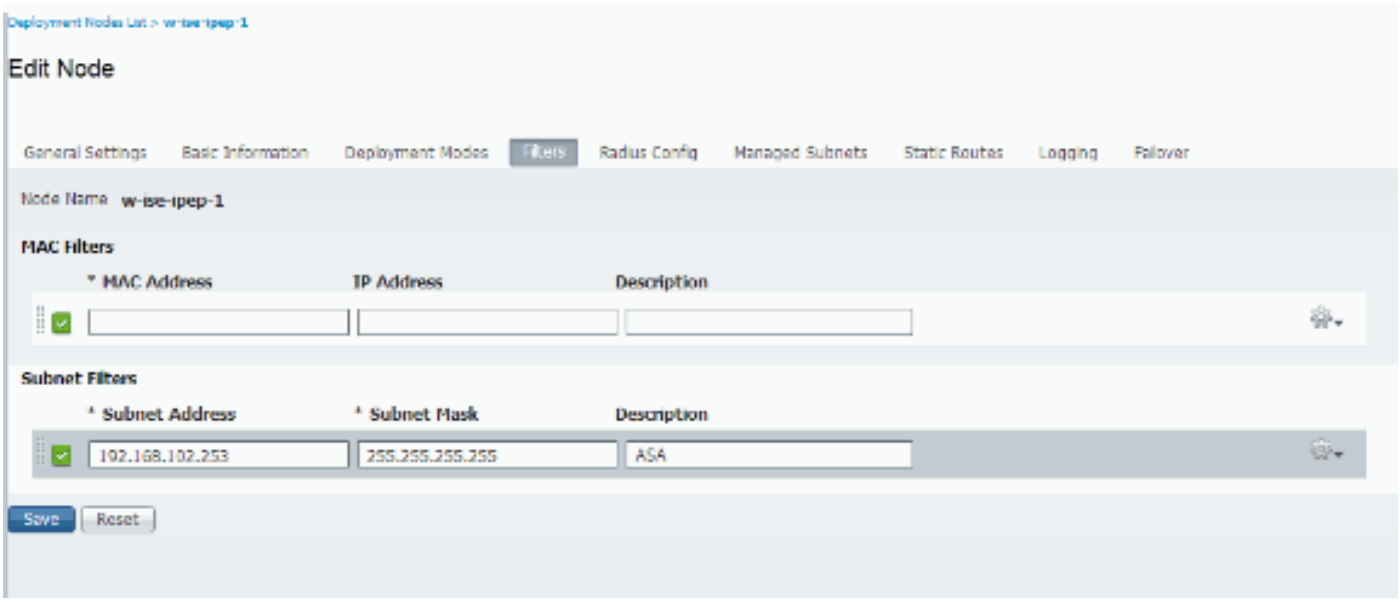
Configuration de base :



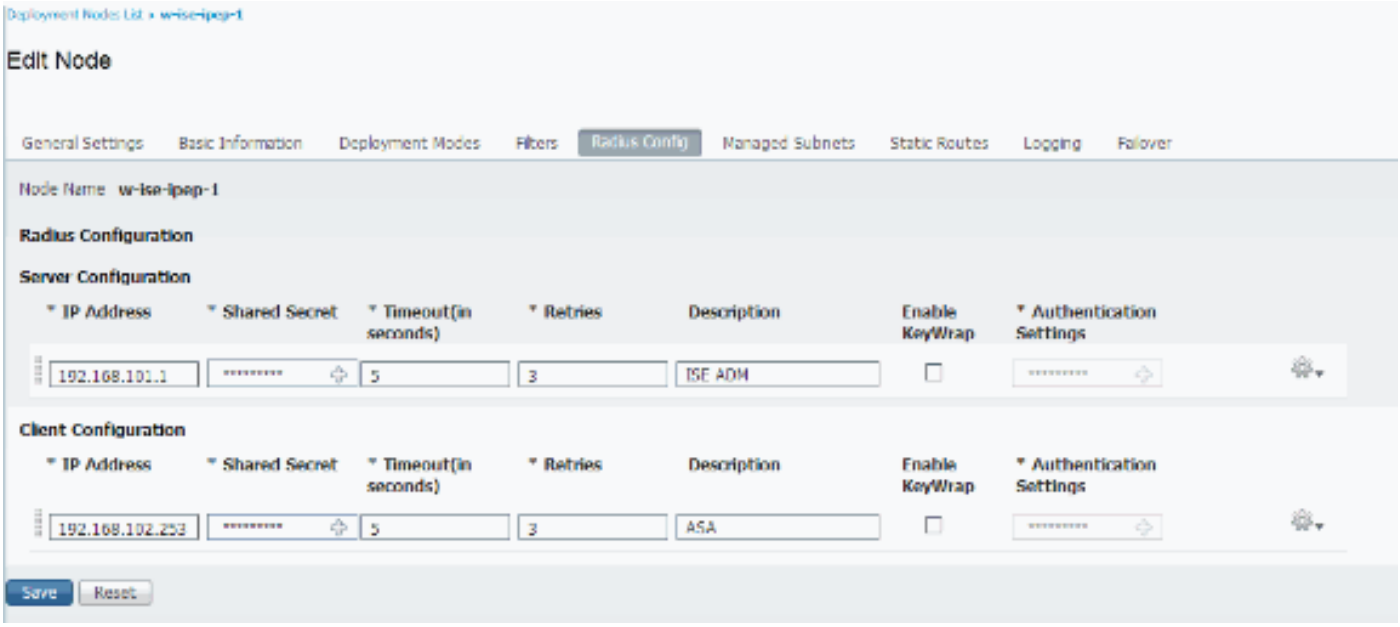
Configuration de mode de déploiement :



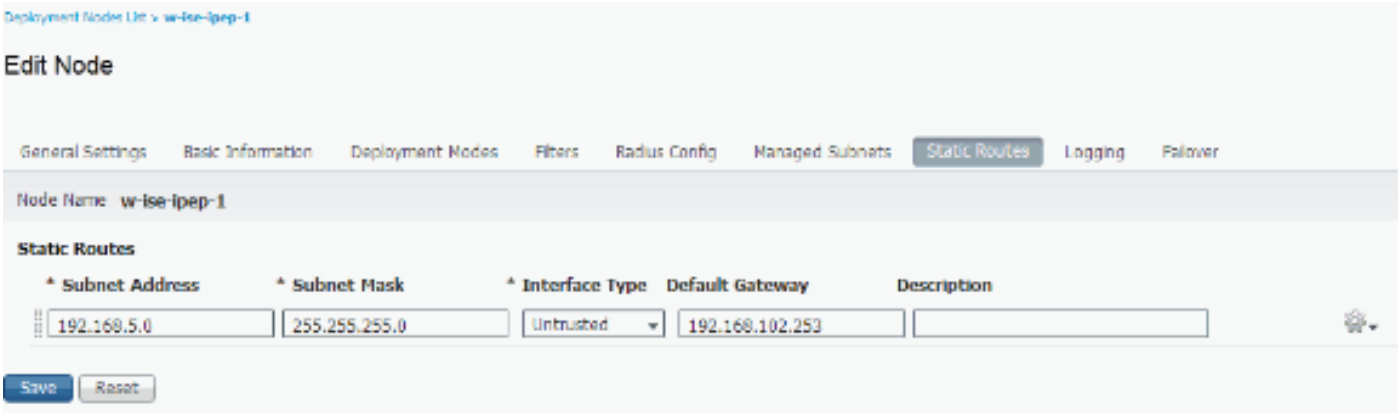
Configuration de filtres :



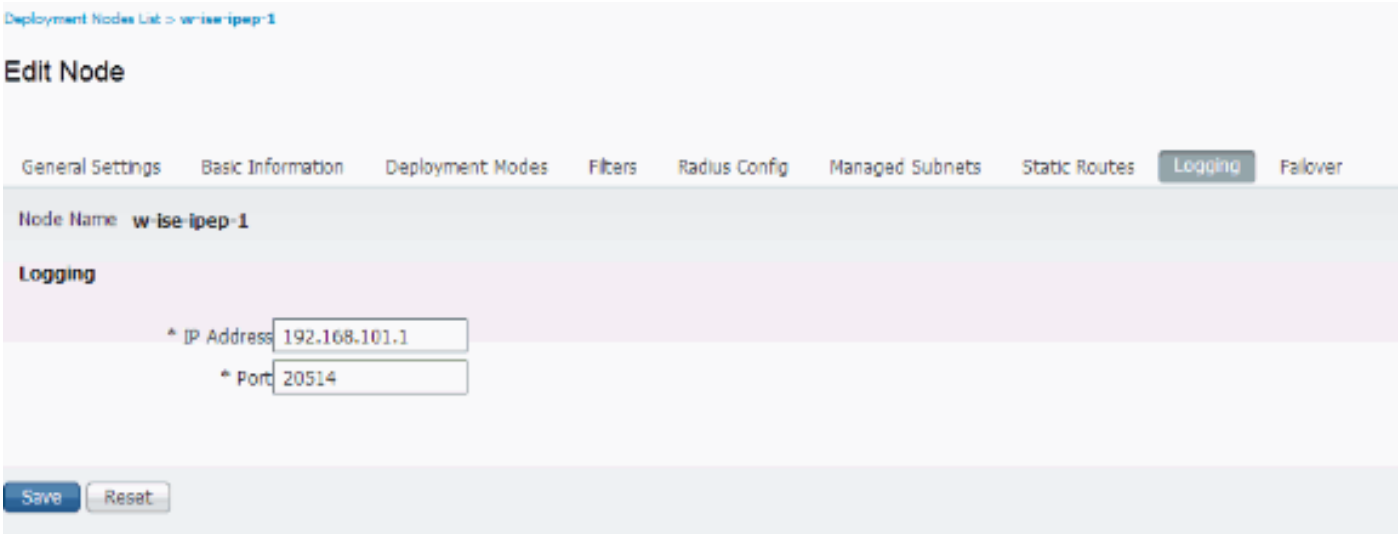
Configuration RADIUS :



Artères de charge statique :



Se connecter :



Configuration d'authentification et de posture

Il y a trois états de posture :

- Inconnu : La posture n'est pas encore faite
- Conforme : La posture est faite et le système est conforme
- Non-conforme : La posture est faite, mais le système a manqué au moins un contrôle

Maintenant les profils d'autorisation doivent être créés (qui seront autorisation intégrée profilent : Ceci ajoutera l'attribut d'ipep-authz=true dans la paire AV de Cisco) qui sera utilisée pour le cas différent.

Généralement, le profil inconnu renvoie l'URL de réorientation (détection de posture) qui expédiera le trafic de l'utilisateur à l'ISE et demandera à installer l'agent NAC. Si l'agent NAC est déjà installé, ceci permettra sa demande de détection de HTTP d'être expédié à l'ISE.

Dans ce profil, un ACL qui laisse le trafic http à l'ISE et des DN au moins est utilisé.

Les profils conformes et Non-conformes renvoient habituellement un ACL téléchargeable pour accorder l'accès au réseau basé sur le profil utilisateur. le profil Non-conforme peut permettre aux utilisateurs pour accéder à un web server pour télécharger un antivirus par exemple, ou accordez l'accès au réseau limité.

Dans cet exemple, les profils inconnus et conformes sont créés, et la présence de notepad.exe

pendant que des conditions requises est vérifiées.

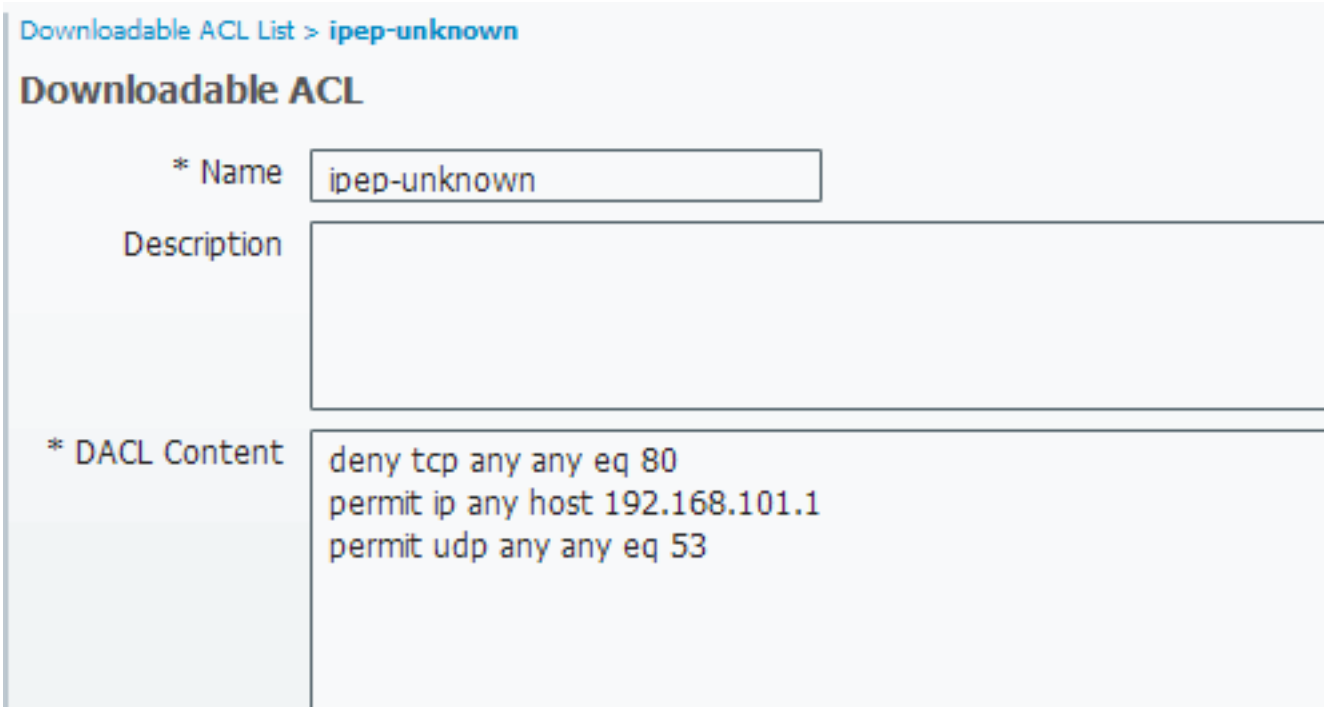
La posture profile la configuration

La première chose à faire est de créer l'ACLs téléchargeable (dACL) et des profils :

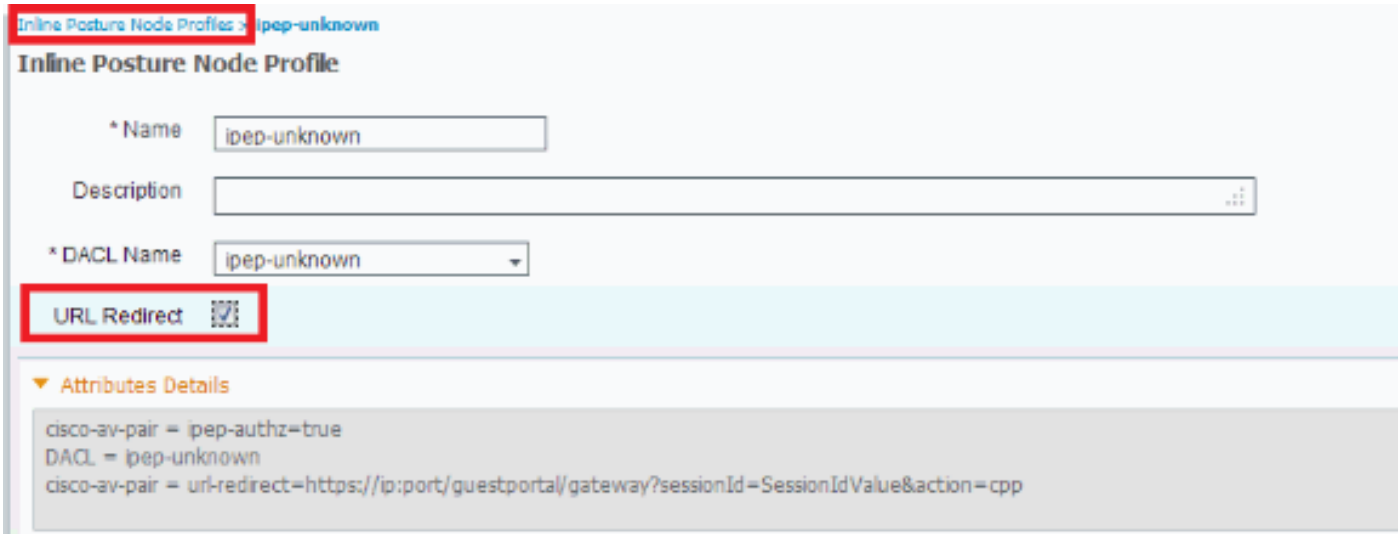
Note: Ce n'est pas obligatoire pour avoir le nom de dACL appariant le nom de profil.

- ConformeACL : ipep-UNKNOWNProfil d'autorisation : ipep-UNKNOWN
- Non-conformeACL : ipep-non-conformeProfil d'autorisation : ipep-non-conforme

DACL inconnu :

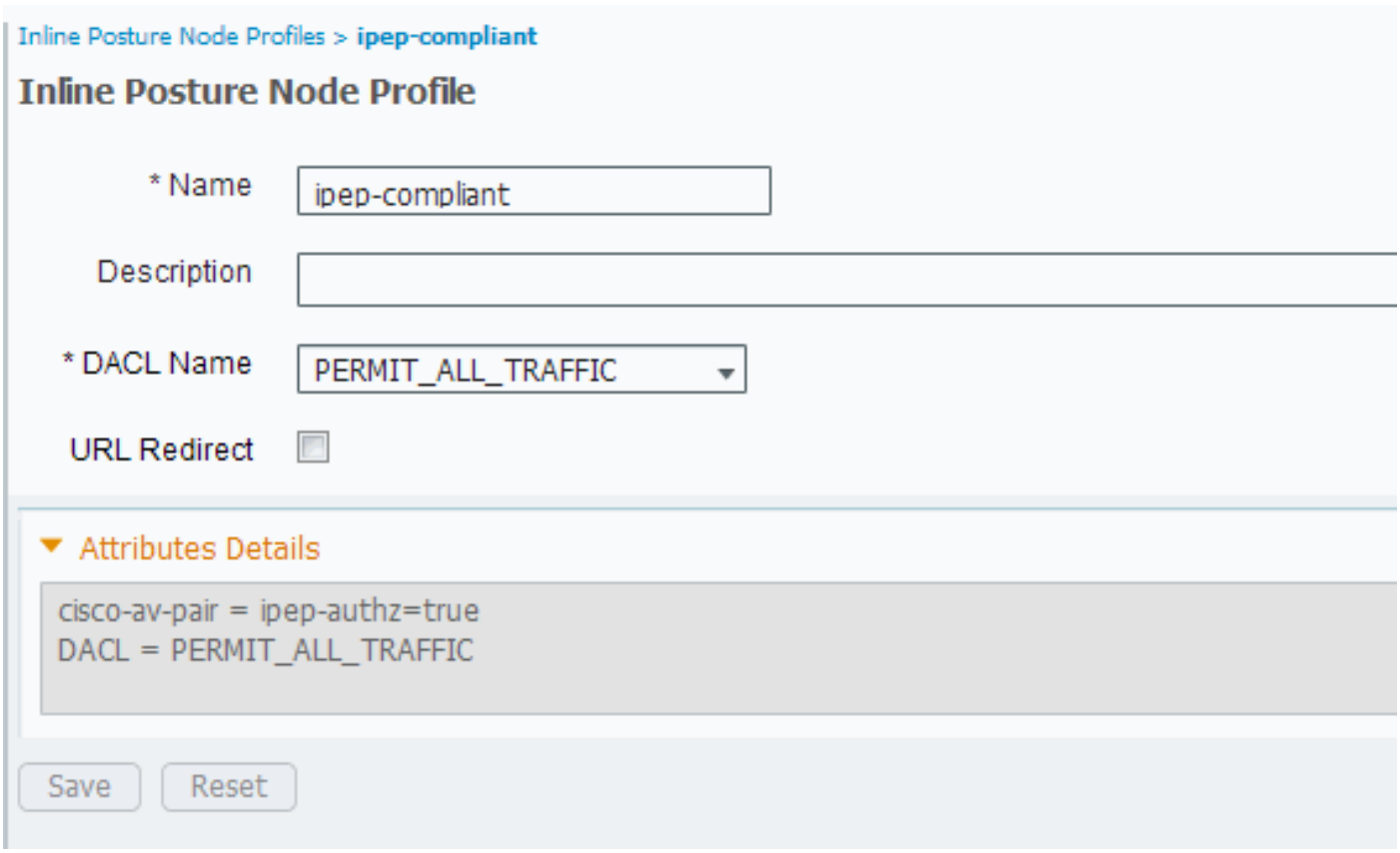


Profil inconnu :



DACL conforme :

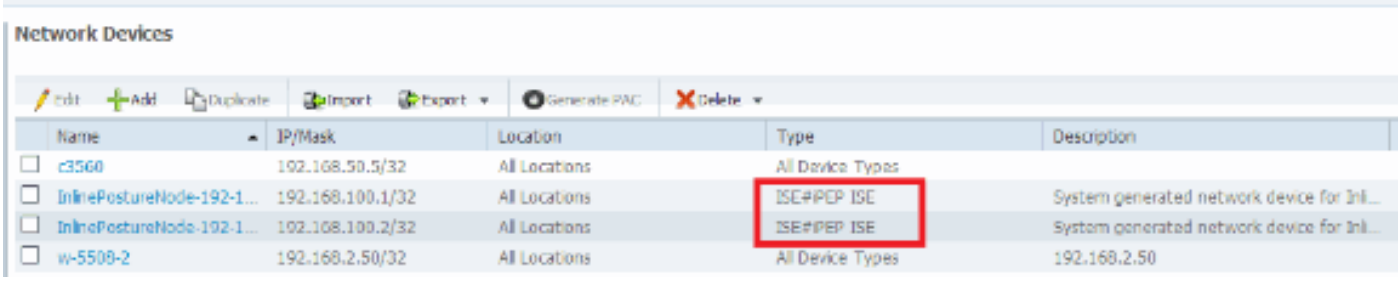
Profil conforme :



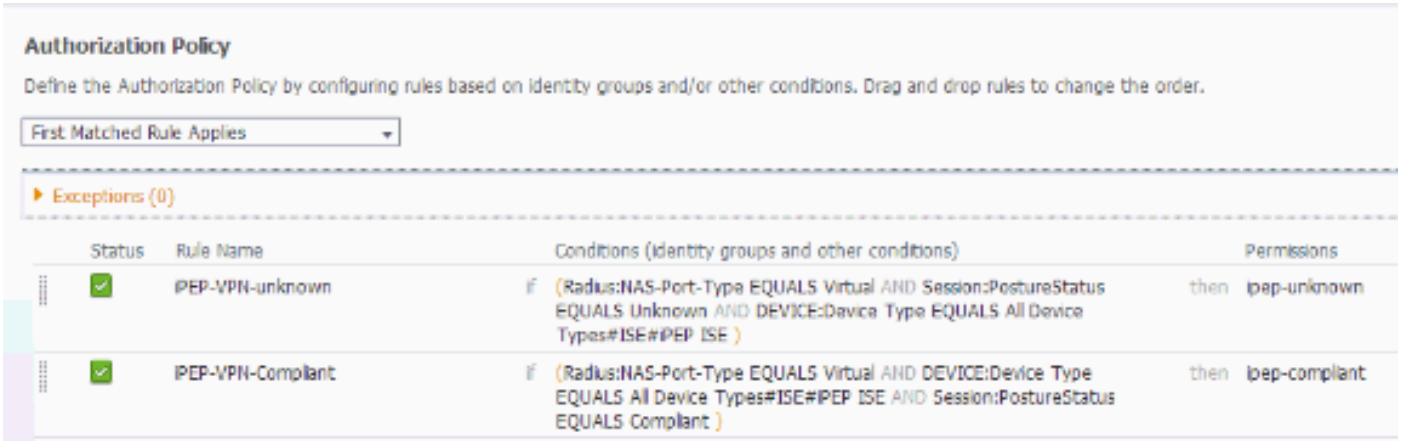
Configuration d'autorisation

Maintenant que le profil est créé, vous devez apparier la demande RADIUS provenant l'iPEP et s'appliquer à eux les profils de droite. Les ISISs d'iPEP sont définis avec un type d'engin spécial qui sera utilisé dans les règles d'autorisation :

NADs :

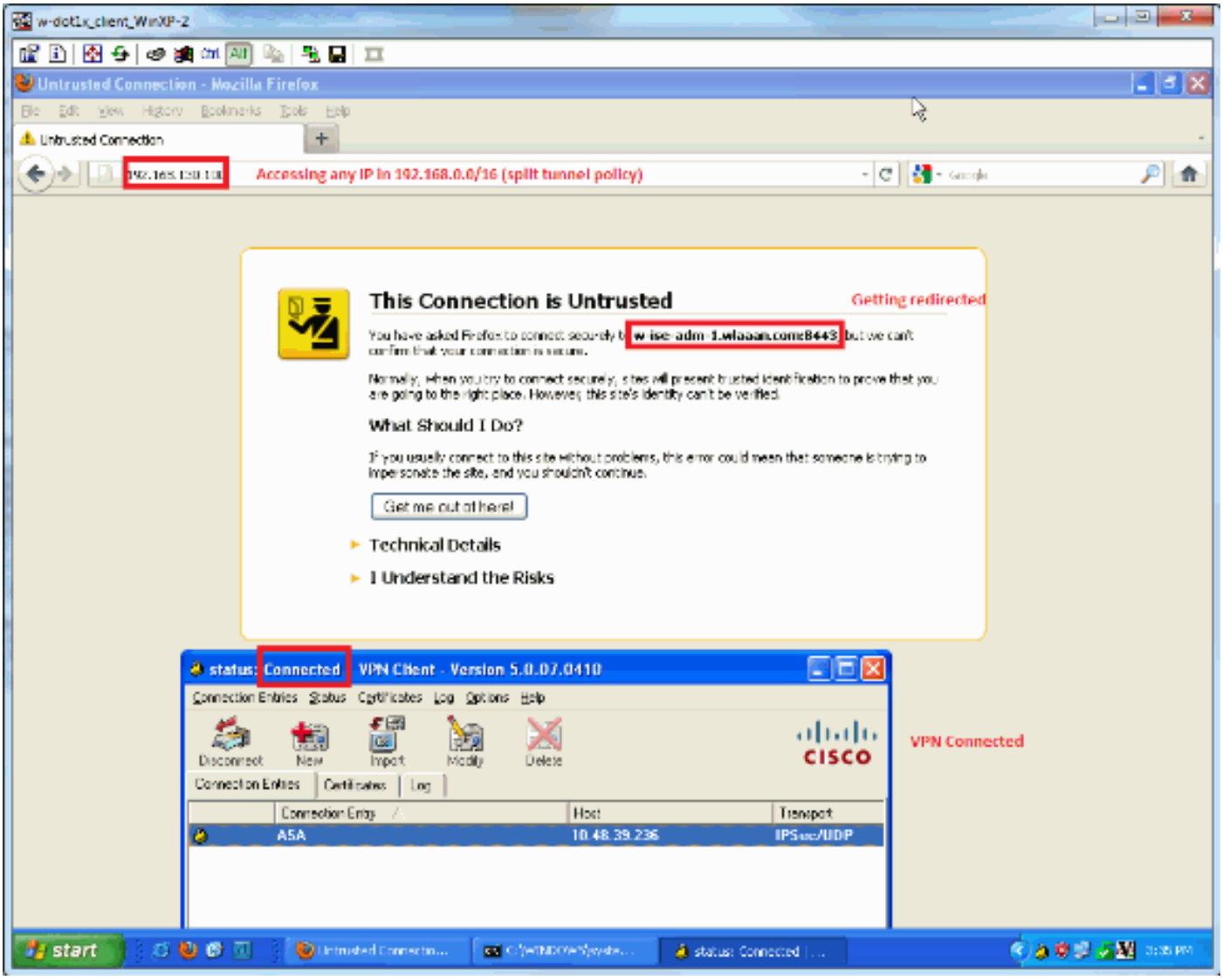


Autorisation :

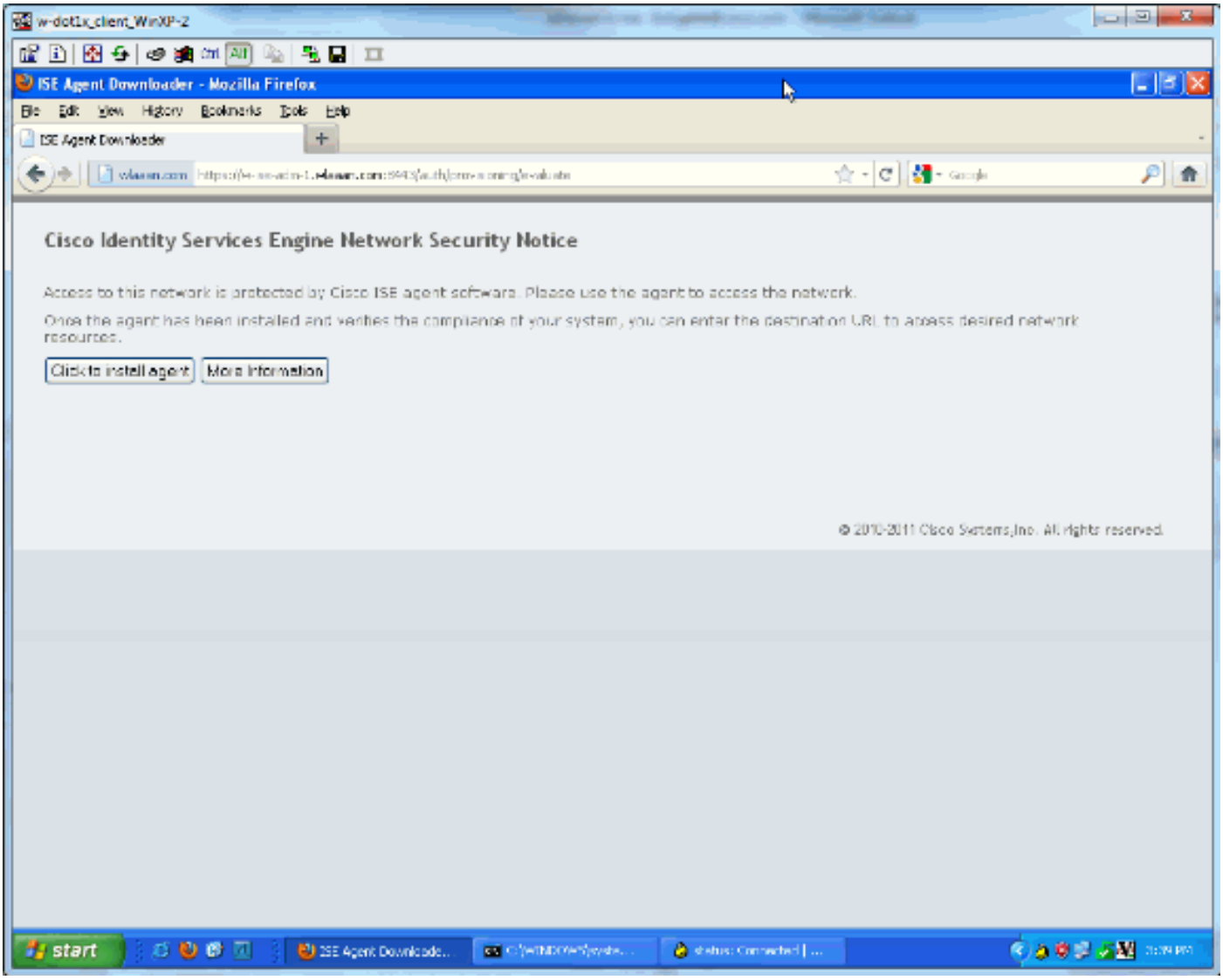


Note: Si l'agent n'est pas installé sur l'ordinateur, vous pouvez définir des règles de ravitaillement de client.

Résultat



Vous êtes incité à installer l'agent (dans cet exemple, le ravitaillement de client est déjà placé) :



Une certaine sortie à ce stade :

```
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
```

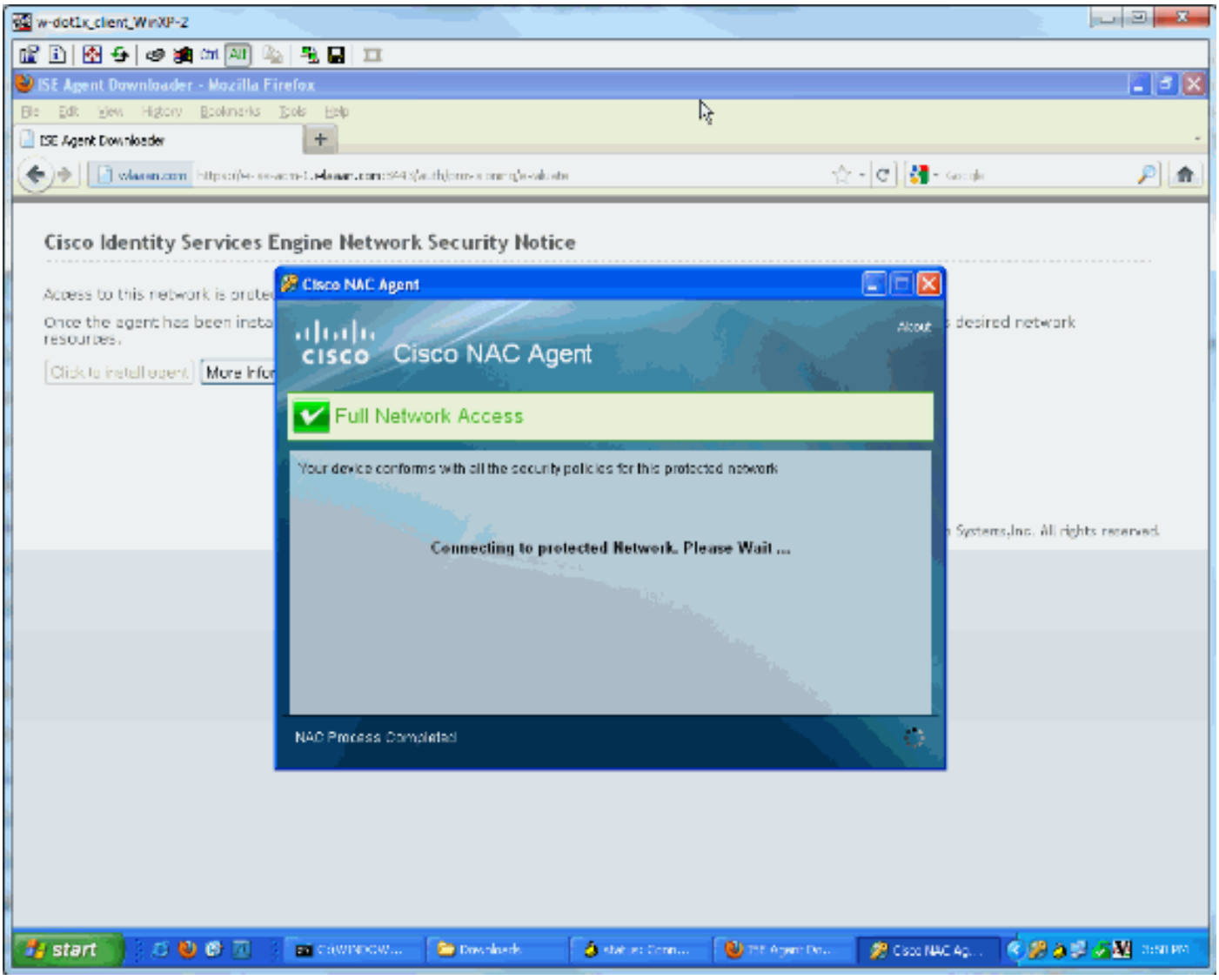
Et de l'iPEP :

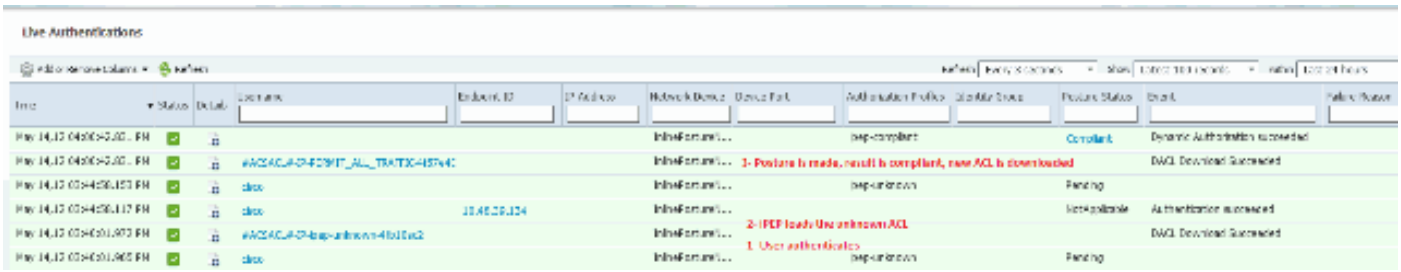
```
w-ise-ipep-1/admin# show pep table session

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
```

Une fois que l'agent est téléchargé et installé :

L'agent devrait automatiquement détecter l'ISE et exécute l'estimation de posture (vous assumant ayez les règles de posture définies déjà, qui est un autre sujet). Dans cet exemple, la posture est réussie, et ceci apparaît :





Note: Il y a deux authentifications dans le tir d'écran ci-dessus. Cependant, parce que la case d'iPEP cache l'ACLs, il n'est pas téléchargé chaque fois.

Sur l'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#
```

Informations connexes

- Support et documentation techniques - Cisco Systems