VPN Inline Posture con iPEP ISE e ASA

Sommario

Introduzione

In questo documento viene illustrato come configurare la postura in linea con un'appliance ASA (Adaptive Security Appliance) e un Identity Services Engine (ISE).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulla versione 8.2(4) per l'ASA e sulla versione 1.1.0.65 per l'ISE.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

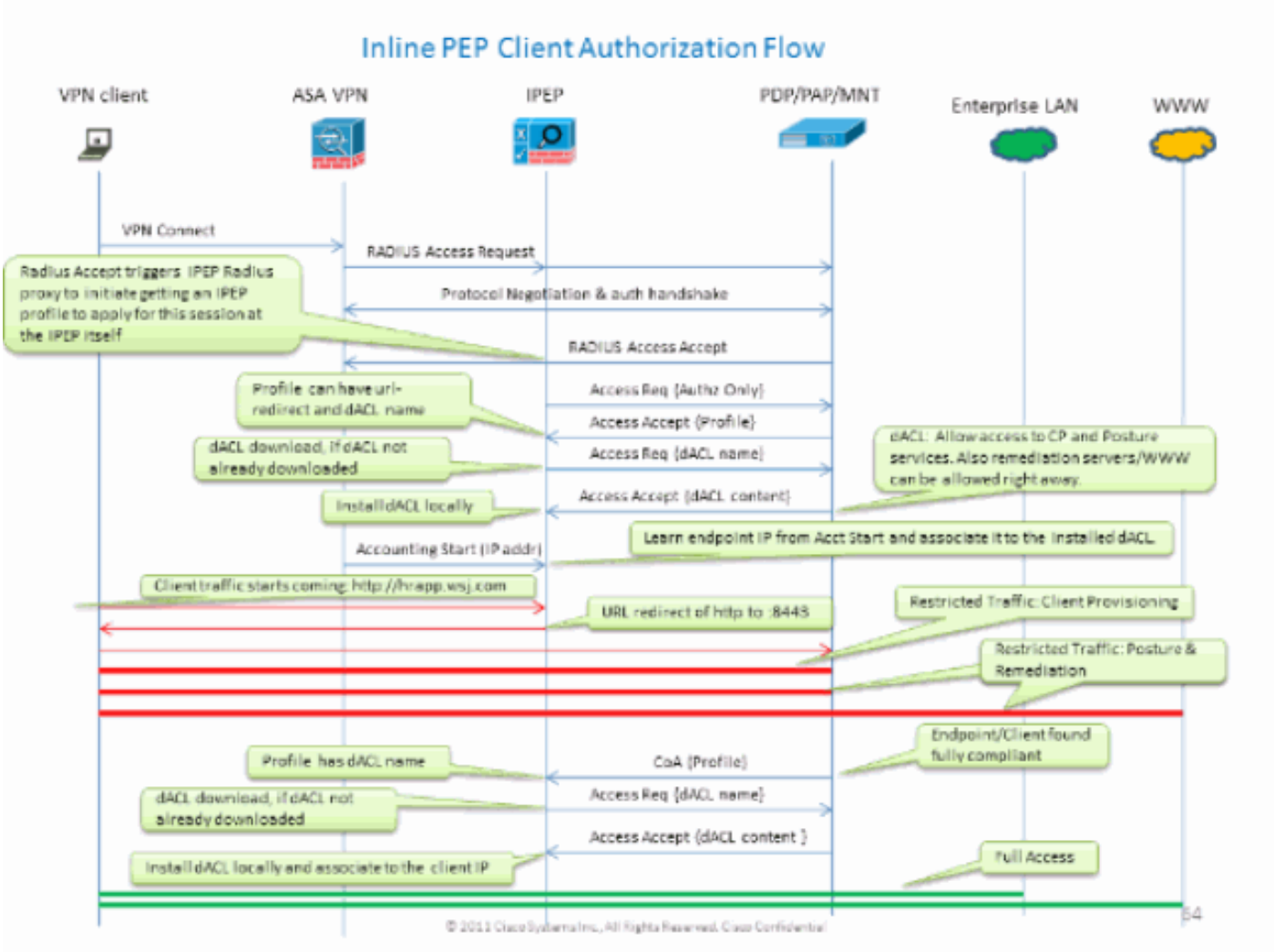
L'ISE offre molti servizi AAA (postura, profilatura, autenticazione, ecc.). Alcuni dispositivi di rete (NAD) supportano la modifica dell'autorizzazione Radius (CoA, Radius Change Of Authorization) che consente di modificare in modo dinamico il profilo di autorizzazione di un dispositivo terminale in base alla postura o al risultato della profilatura. Altre appliance NAD, come l'ASA, non supportano ancora questa funzione. Ciò significa che è necessaria un'ISE in esecuzione in modalità iPEP (Inline Posture Enforcement mode) per modificare in modo dinamico i criteri di accesso alla rete di un dispositivo terminale.

Il concetto di base è che tutto il traffico degli utenti passerà attraverso l'iPEP, con il nodo che agirà anche come proxy Radius.

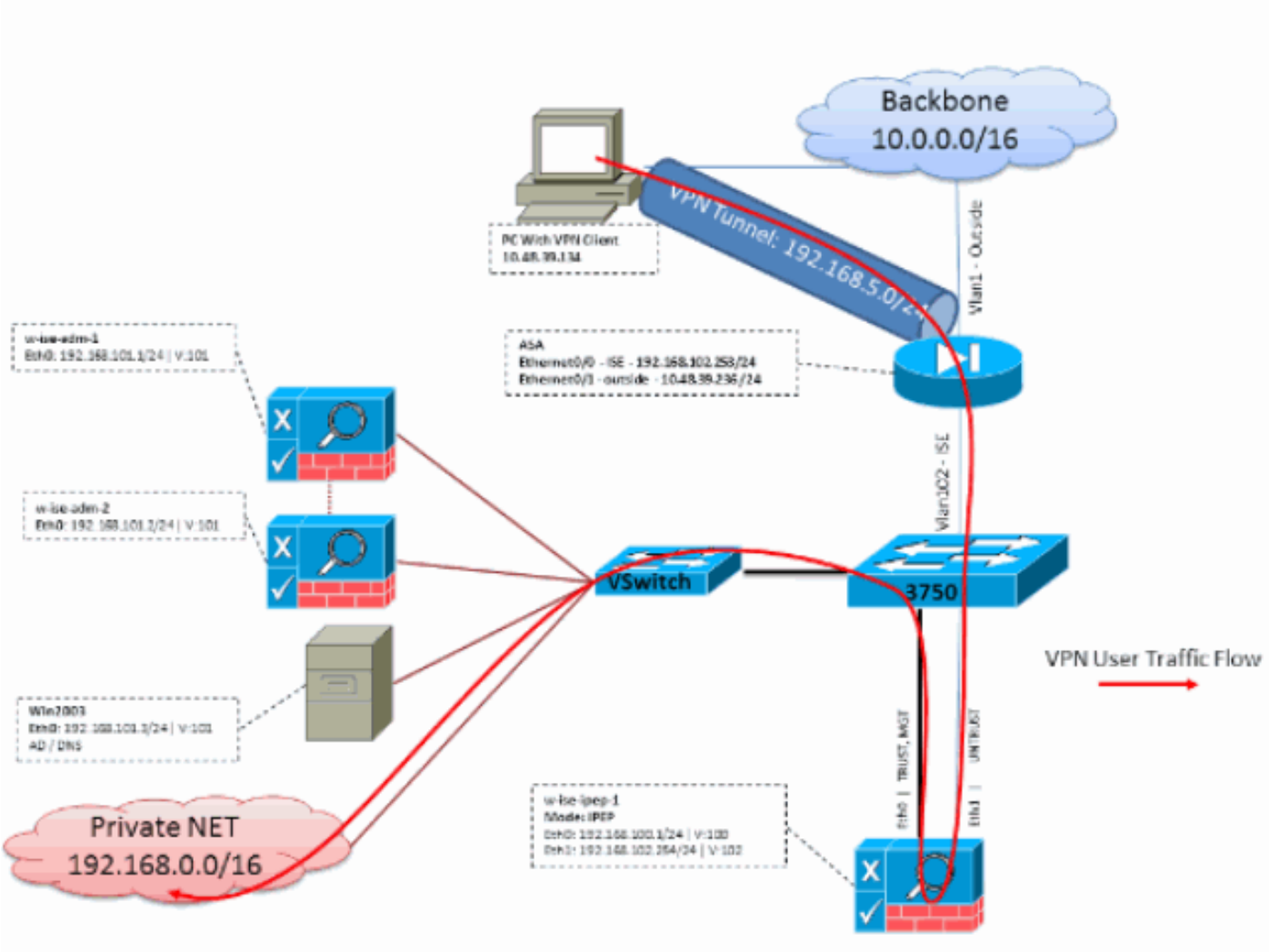
Flusso di base

1. Accesso utente VPN.
2. L'ASA invia la richiesta al nodo iPEP (ISE).
3. L'iPEP riscrive la richiesta (aggiungendo gli attributi Cisco AV-PAIR per indicare che si tratta di autenticazione iPEP) e invia la richiesta all'ISE Policy Node (PDP).
4. Il PDP risponde all'iPEP che lo inoltrerà alla NAD.
5. Se l'utente è autenticato, NAD DEVE inviare una richiesta di avvio dell'accounting (vedere CSCtz84826). In questo modo viene avviata l'avvio della sessione sull'iPEP. In questa fase, l'utente viene reindirizzato per la postura. Inoltre, è necessario abilitare l'aggiornamento temporaneo-accounting-per il tunnel stabilito dal portale WEBVPN, in quanto ISE prevede di avere l'attributo framed-ip-address nell'accounting radius. Tuttavia, quando ci si connette al portale, l'indirizzo IP VPN del client non è ancora noto perché il tunnel non è stato stabilito. In questo modo, l'ASA invierà aggiornamenti intermedi, ad esempio quando verrà stabilito il tunnel.
6. L'utente esegue la valutazione della postura e, in base ai risultati ottenuti, il PDP aggiorna la sessione utilizzando il CoA sull'iPEP.

In questa schermata viene illustrato questo processo:



Topologia di esempio



Configurazione ASA

La configurazione ASA è una semplice VPN remota 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 !
```

Configurazione di ISE

Configurazione iPEP

La prima cosa da fare è aggiungere un ISE come nodo iPEP. Per ulteriori informazioni sul processo, vedere:

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

Questo è sostanzialmente ciò che dovete configurare nelle varie schede (gli screenshot forniti in questa sezione illustrano questo):

- Configurare le impostazioni IP e IP globale non attendibili (in questo caso, l'indirizzo IP non attendibile è 192.168.102.254).
- Distribuzione in modalità di routing.
- Posizionare un filtro statico in modo che l'ASA possa passare attraverso la scatola iPEP (in caso contrario, la connettività da/verso la scatola ISE-iPEP viene interrotta).
- Configurare Policy ISE come server Radius e ASA come client Radius.
- Aggiungere una route alla subnet VPN che punti all'ASA.
- Impostare Monitoring ISE come Logging Host (porta 20514 per impostazione predefinita; in questo caso, la policy ISE è monitorata).

Requisiti importanti per la configurazione dei certificati:

Prima di tentare di registrare un nodo iPEP, verificare che siano soddisfatti i seguenti requisiti di utilizzo chiavi avanzato del certificato. Se i certificati non sono configurati correttamente sui nodi iPEP e Admin, il processo di registrazione verrà completato. Tuttavia, si perderà l'accesso amministrativo al nodo iPEP. I seguenti dettagli sono stati estrapolati dalla Guida all'implementazione di ISE 1.1.x iPEP:

La presenza di determinate combinazioni di attributi nei certificati locali dei nodi Amministrazione e Postura in linea può impedire il funzionamento dell'autenticazione reciproca.

Gli attributi sono:

- Utilizzo chiave esteso (EKU): autenticazione server
- Utilizzo chiave esteso (EKU): autenticazione client
- Tipo di certificato Netscape: autenticazione server SSL
- Tipo di certificato Netscape: autenticazione client SSL

Per il certificato di amministrazione è necessaria una delle combinazioni seguenti:

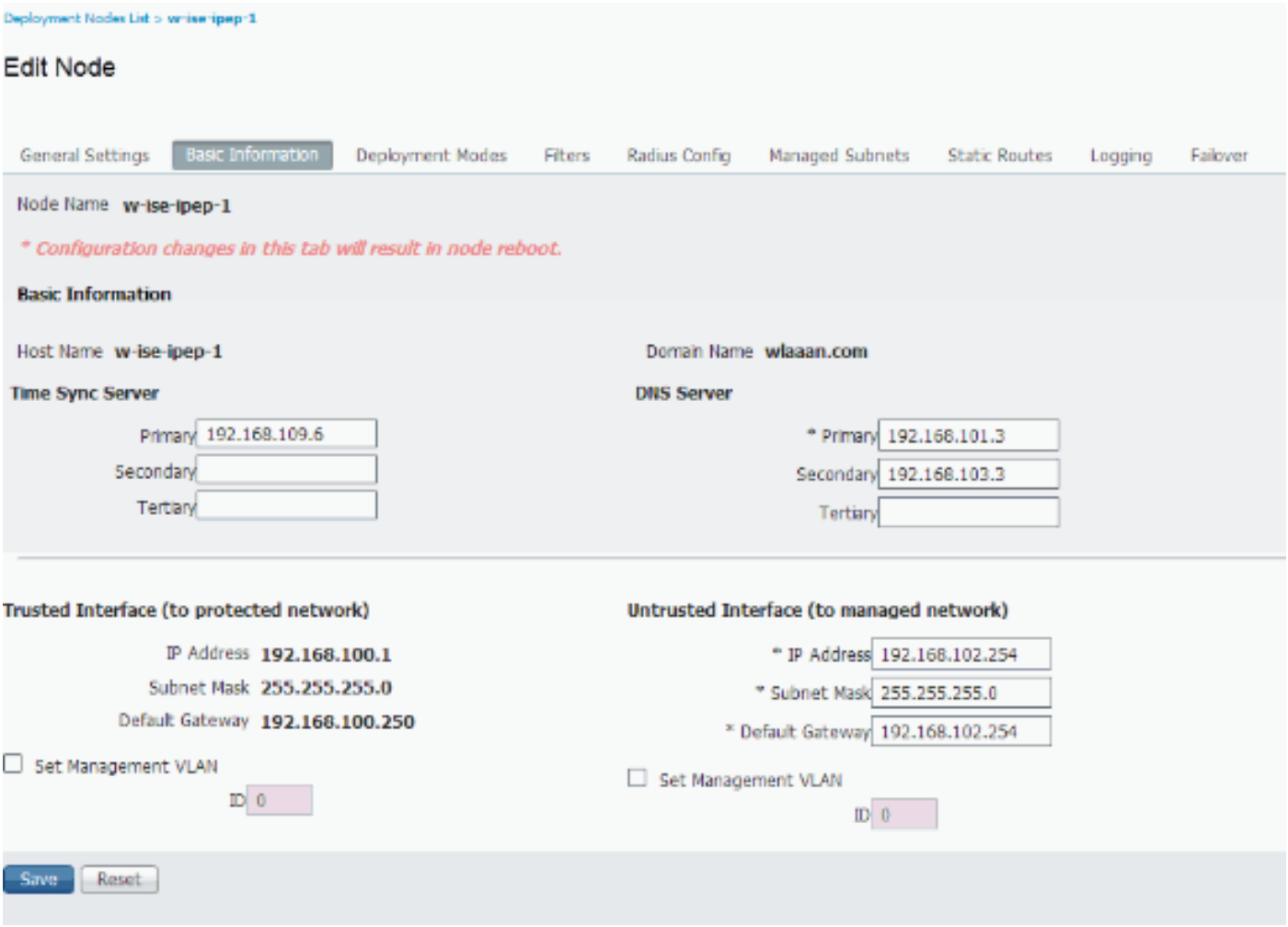
- Entrambi gli attributi EKU devono essere disattivati, se entrambi gli attributi EKU sono disattivati nel certificato di postura in linea, oppure devono essere attivati entrambi, se

l'attributo server è attivato nel certificato di postura in linea.
- Entrambi gli attributi del tipo di certificato Netscape devono essere disattivati o attivati.

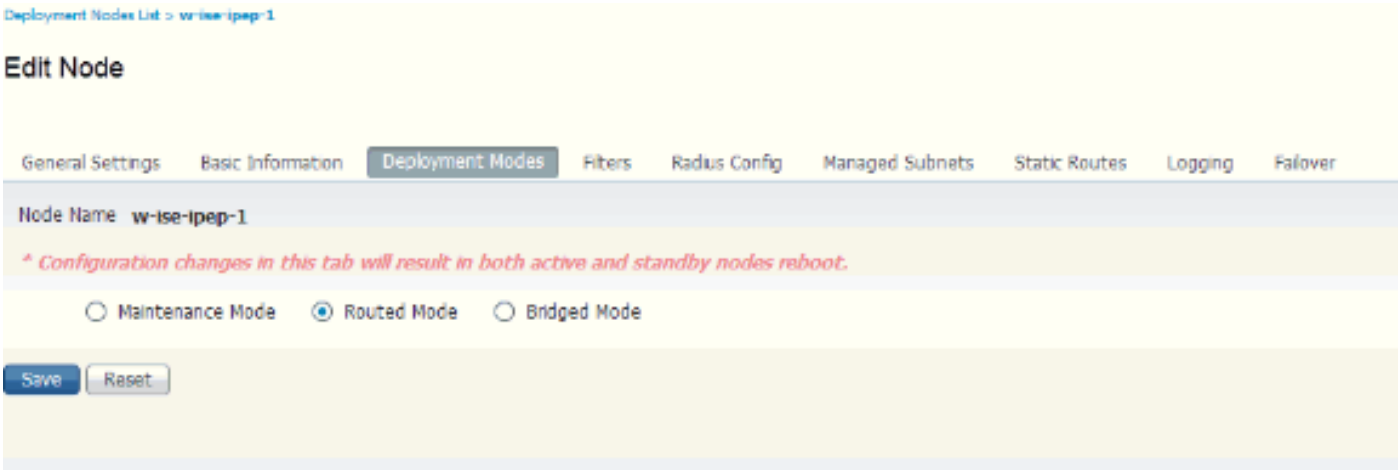
Per il certificato di Postura in linea è richiesta una delle seguenti combinazioni:

- Entrambi gli attributi EKU devono essere disabilitati, oppure entrambi devono essere abilitati, oppure solo l'attributo server deve essere abilitato.
- Entrambi gli attributi del tipo di certificato Netscape devono essere disattivati, oppure entrambi devono essere attivati, oppure deve essere attivato solo l'attributo server.
- Se nei nodi Amministrazione e Postura in linea vengono utilizzati certificati locali autofirmati, è necessario installare il certificato autofirmato del nodo Amministrazione nell'elenco di attendibilità del nodo Postura in linea. Inoltre, se nella distribuzione sono presenti sia nodi di amministrazione primari che nodi di amministrazione secondari, è necessario installare il certificato autofirmato di entrambi i nodi di amministrazione nell'elenco di attendibilità del nodo Postura in linea.
- Se nei nodi Amministrazione e Postura in linea vengono utilizzati certificati locali con firma CA, l'autenticazione reciproca dovrebbe funzionare correttamente. In questo caso, il certificato della CA di firma viene installato nel nodo Amministrazione prima della registrazione e viene replicato nel nodo Postura in linea.
- Se le chiavi rilasciate dalla CA vengono utilizzate per proteggere la comunicazione tra i nodi Amministrazione e Postura in linea, prima di registrare il nodo Postura in linea è necessario aggiungere la chiave pubblica (certificato CA) dal nodo Amministrazione all'elenco dei certificati CA del nodo Postura in linea.

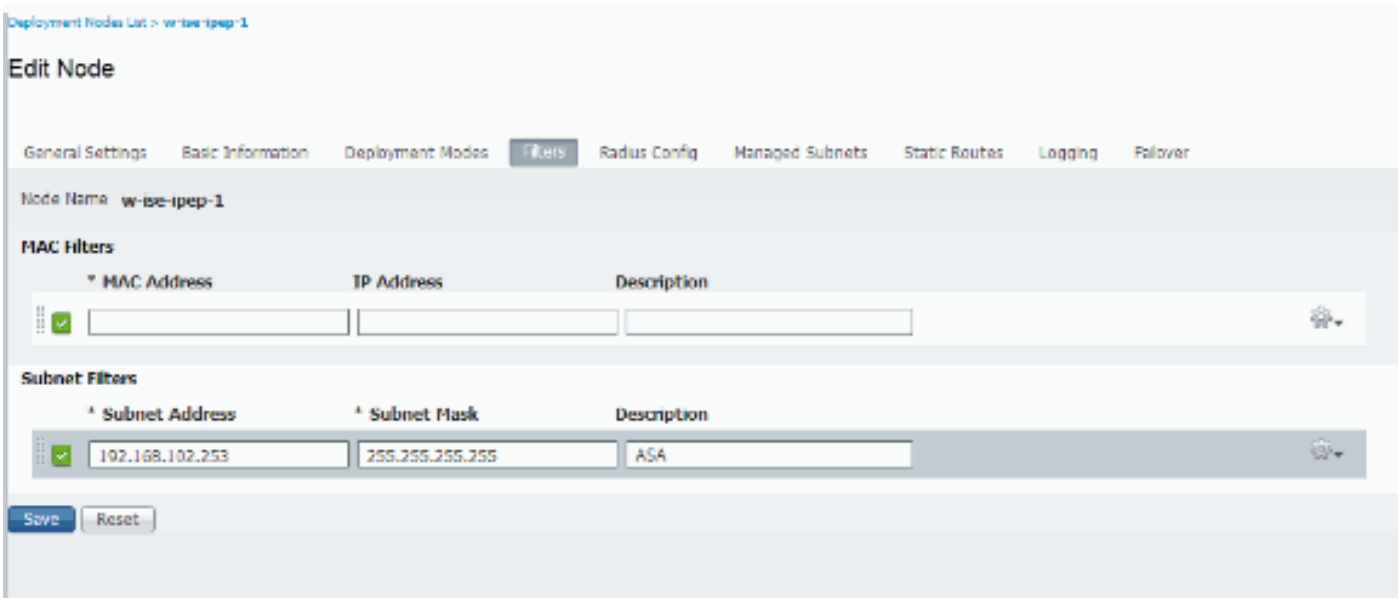
Configurazione di base:



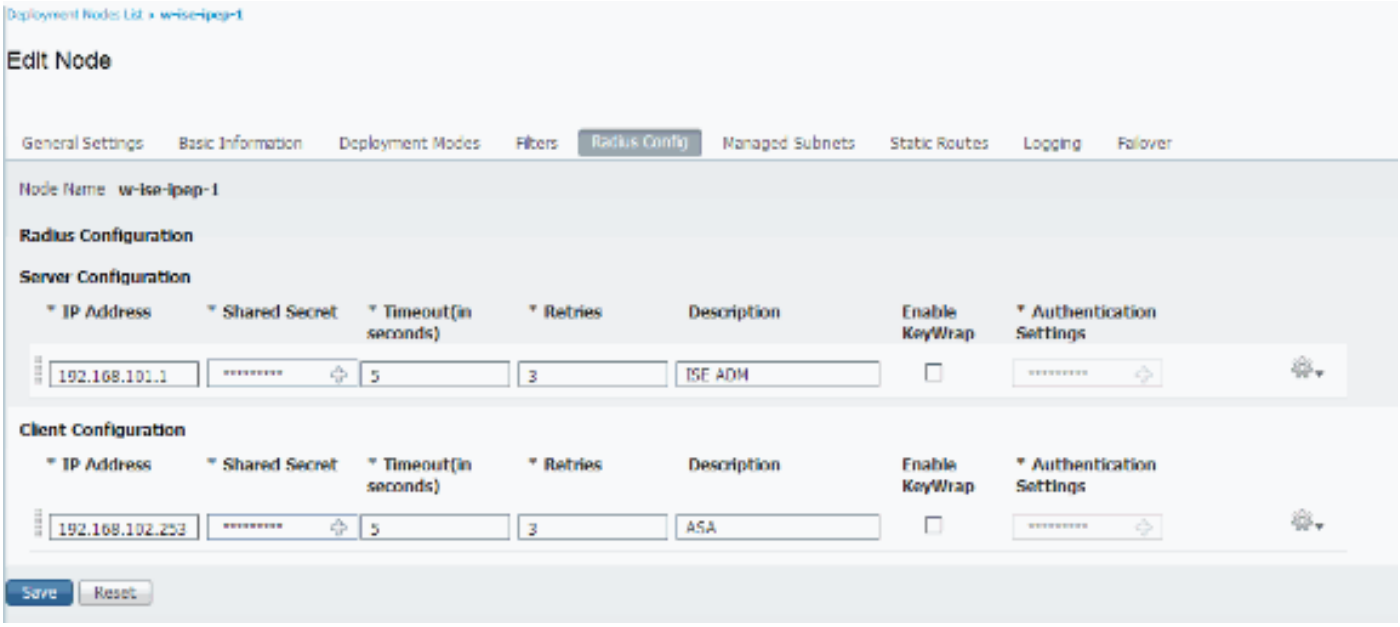
Configurazione modalità di distribuzione:



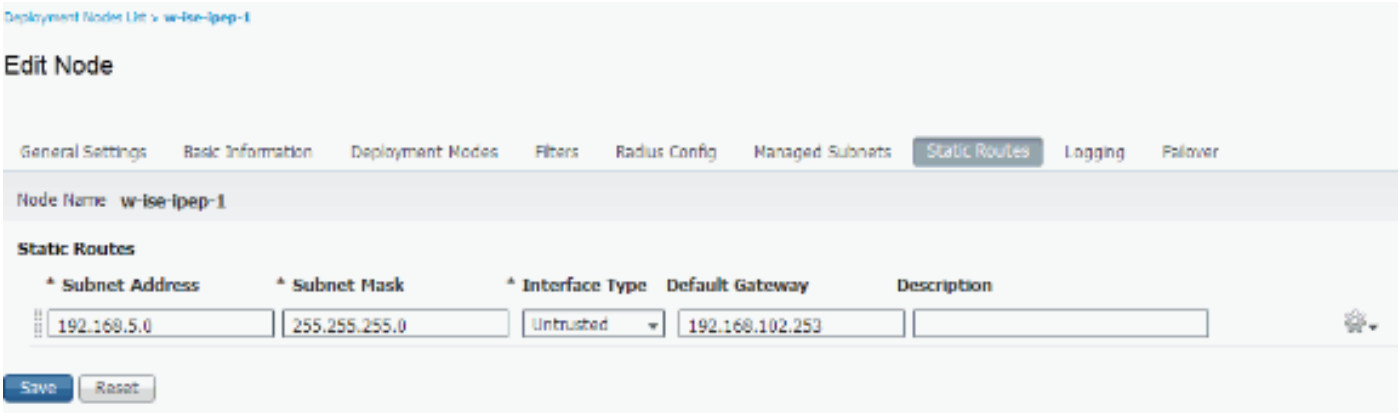
Configurazione filtri:



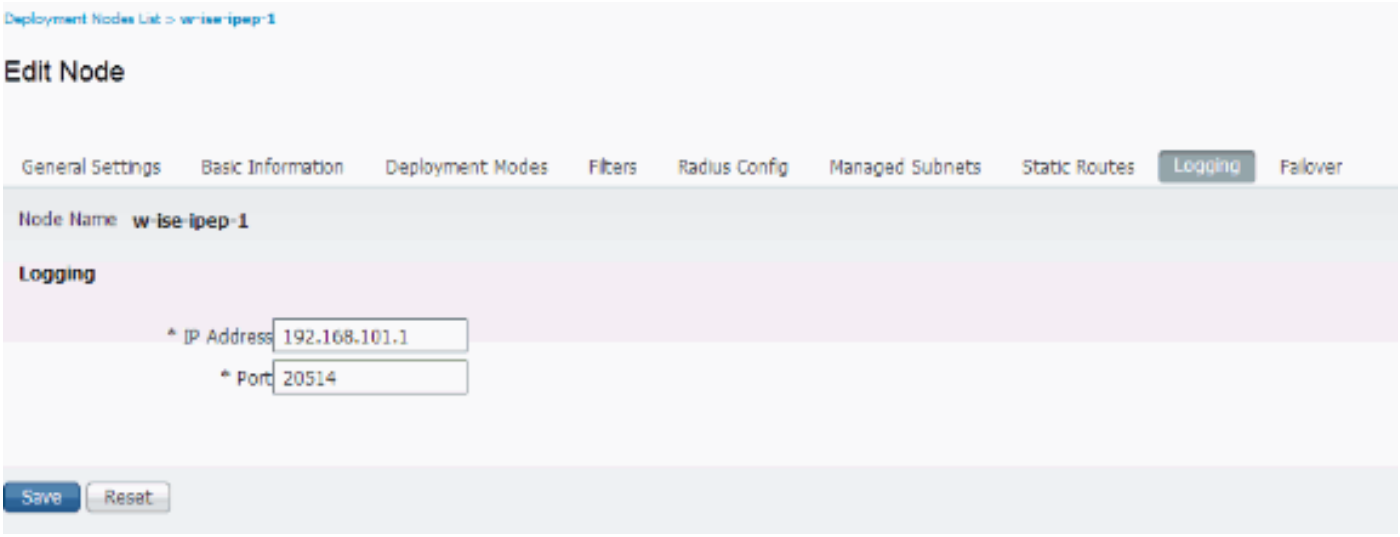
Configurazione Radius:



Route statiche:



Registrazione:



Configurazione autenticazione e postura

Sono disponibili tre stati di postura:

- Sconosciuto: Postura non ancora definita
- Conforme: La postura è stata creata e il sistema è conforme
- Non conforme: La postura è stata creata, ma il sistema non ha superato almeno un controllo

A questo punto è necessario creare i profili di autorizzazione, ovvero i profili di autorizzazione in linea: In questo modo viene aggiunto l'attributo ipep-authz=true nella coppia Cisco AV) che verrà utilizzata per i diversi casi.

In genere, il profilo Unknown restituisce l'URL di reindirizzamento (rilevamento postura) che inoltrerà il traffico dell'utente all'ISE e chiederà di installare l'agente NAC. Se l'agente NAC è già installato, la richiesta di rilevamento HTTP potrà essere inoltrata all'ISE.

In questo profilo, viene usato un ACL che permette il traffico HTTP verso ISE e il DNS almeno.

I profili Conforme e Non conforme in genere restituiscono un ACL scaricabile per concedere l'accesso alla rete in base al profilo utente. Un profilo non conforme può consentire agli utenti di accedere a un server Web per scaricare un antivirus, ad esempio, o concedere un accesso limitato alla rete.

In questo esempio vengono creati i profili Sconosciuto e Conforme e viene verificata la presenza

di notepad.exe come requisiti.

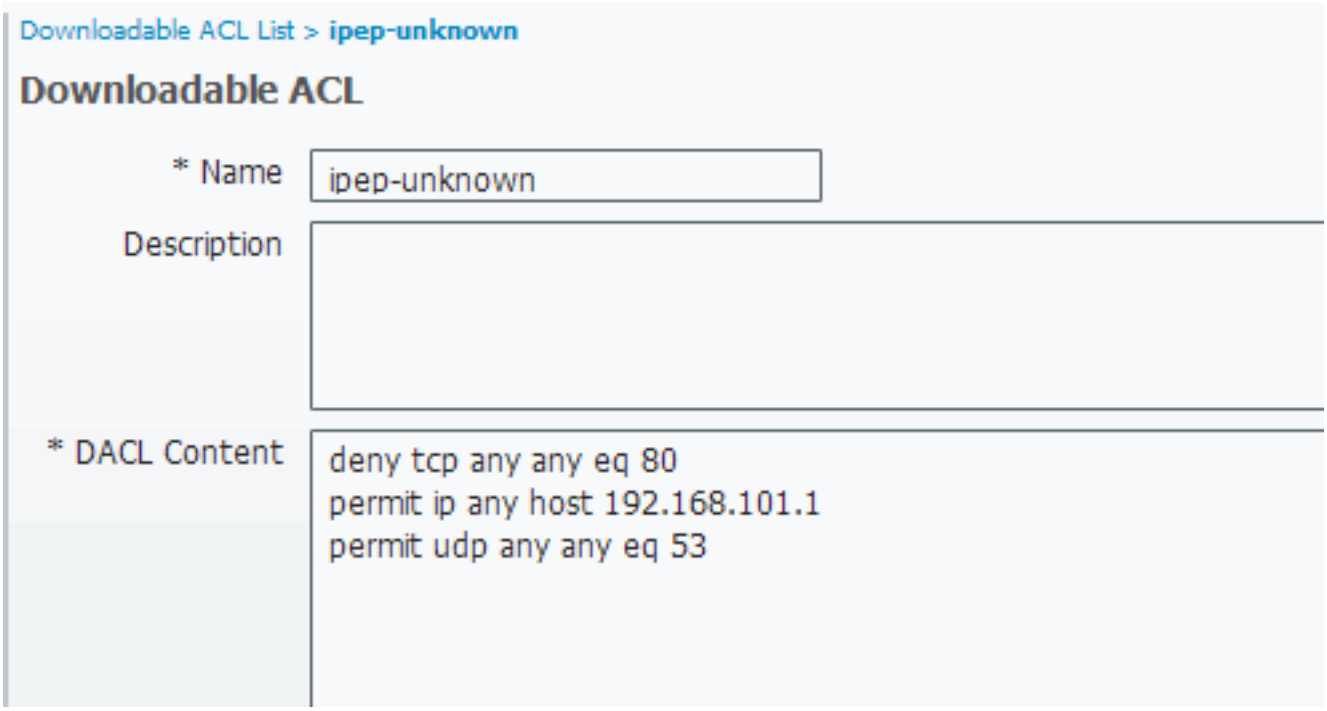
Configurazione profili postura

La prima cosa da fare è creare gli ACL scaricabili (dACL) e i profili:

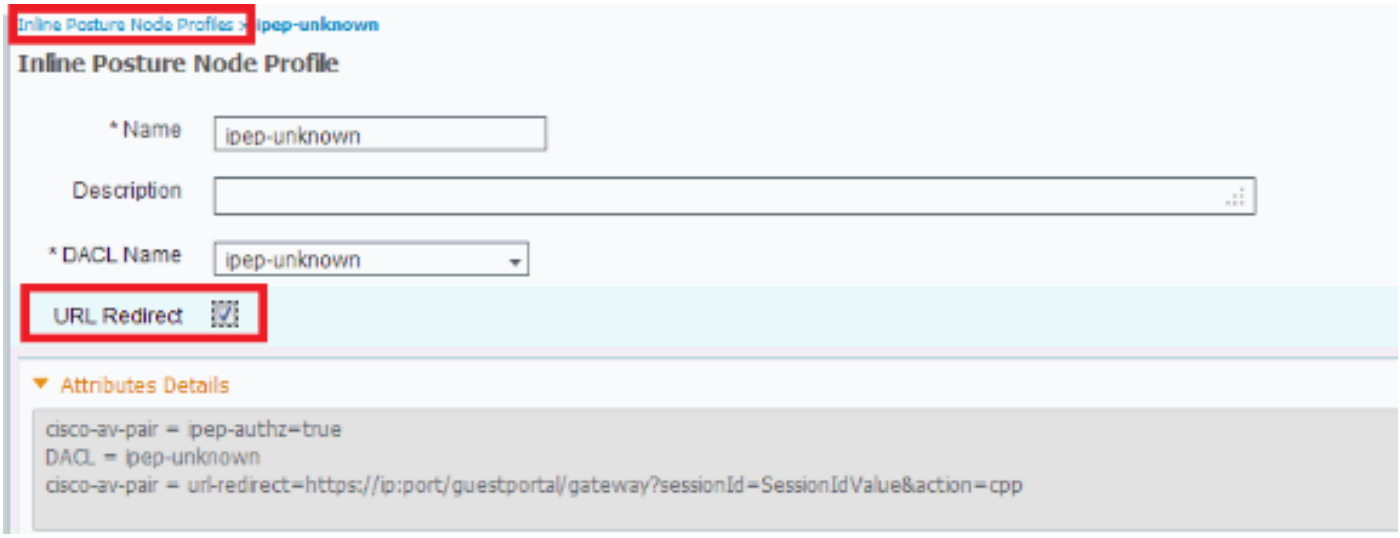
Nota: non è obbligatorio che il nome dell'ACL corrisponda al nome del profilo.

- ConformeACL: ipep sconosciutoProfilo autorizzazione: ipep sconosciuto
- Non conformeACL: non conforme a ipepProfilo autorizzazione: non conforme a ipep

dACL sconosciuto:

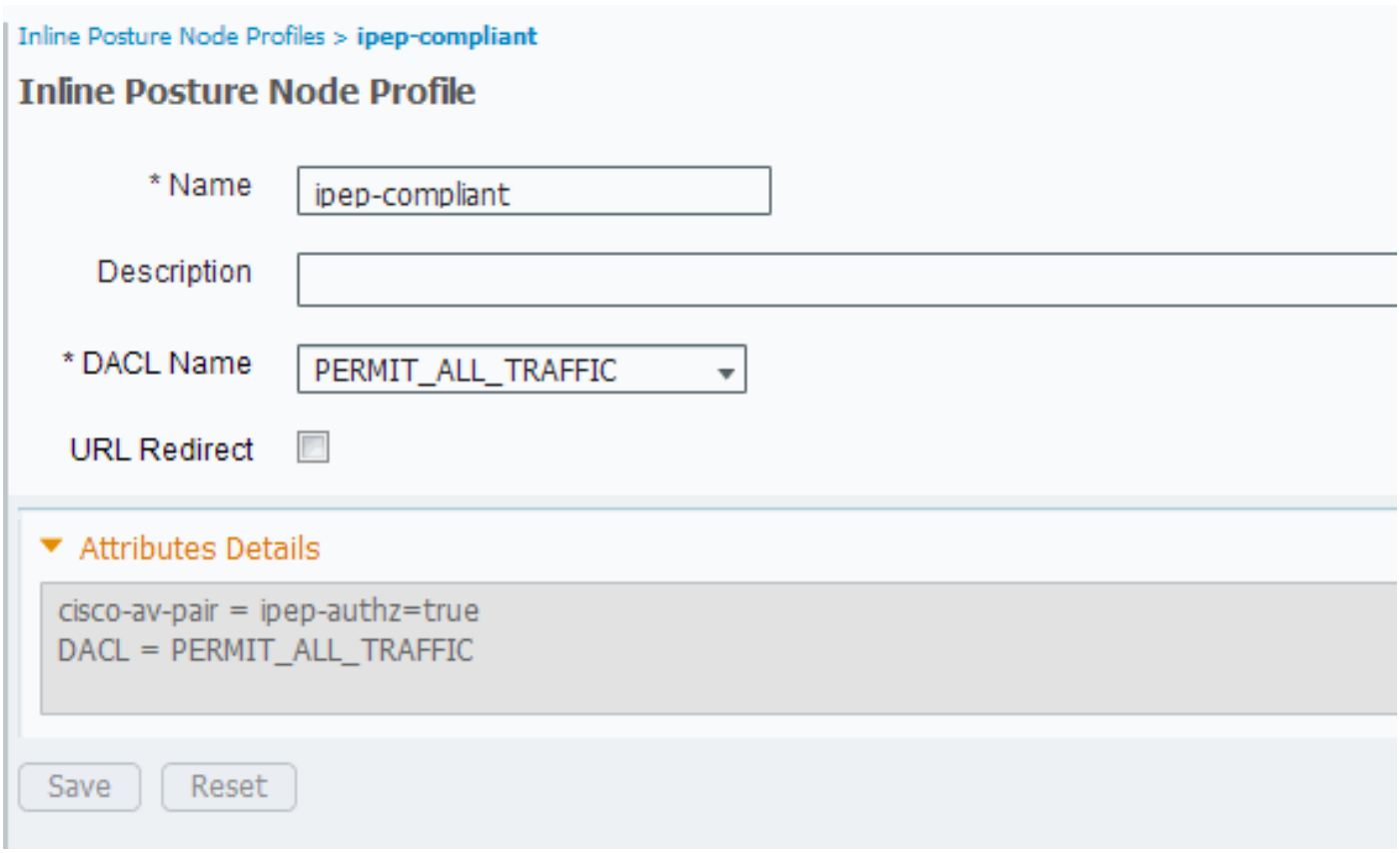


Profilo sconosciuto:



dACL conforme:

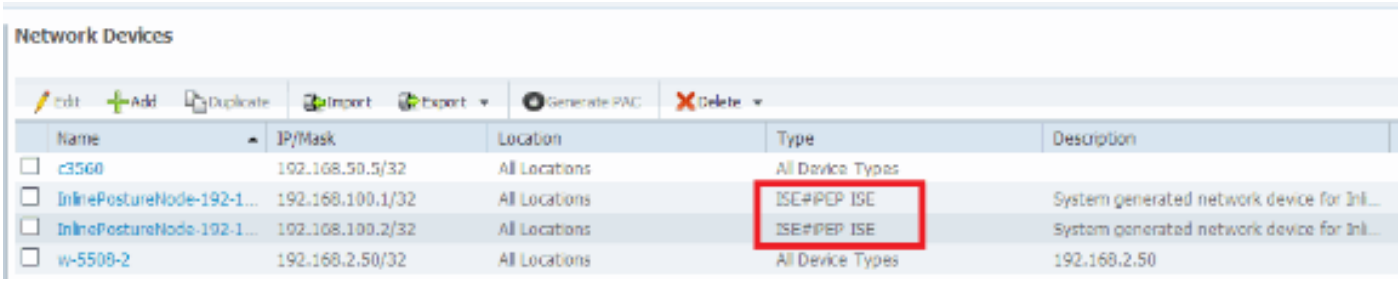
Profilo conforme:



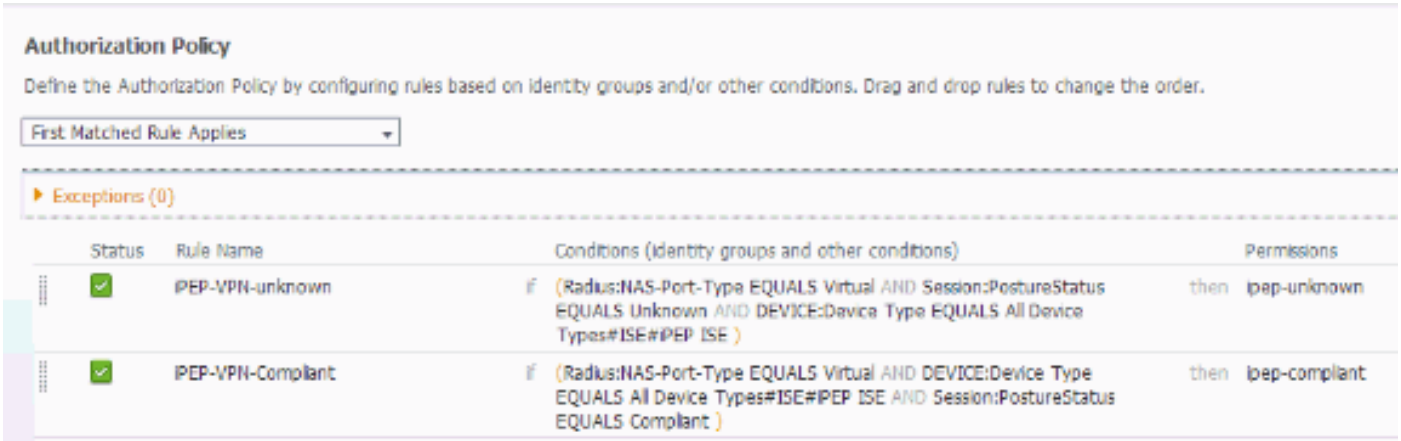
Configurazione autorizzazione

Una volta creato il profilo, è necessario che la richiesta Radius proveniente dall'iPEP corrisponda a quella appropriata e applichi i profili corretti. Gli iPEP ISE sono definiti con un tipo di dispositivo speciale che verrà utilizzato nelle regole di autorizzazione:

NAD:

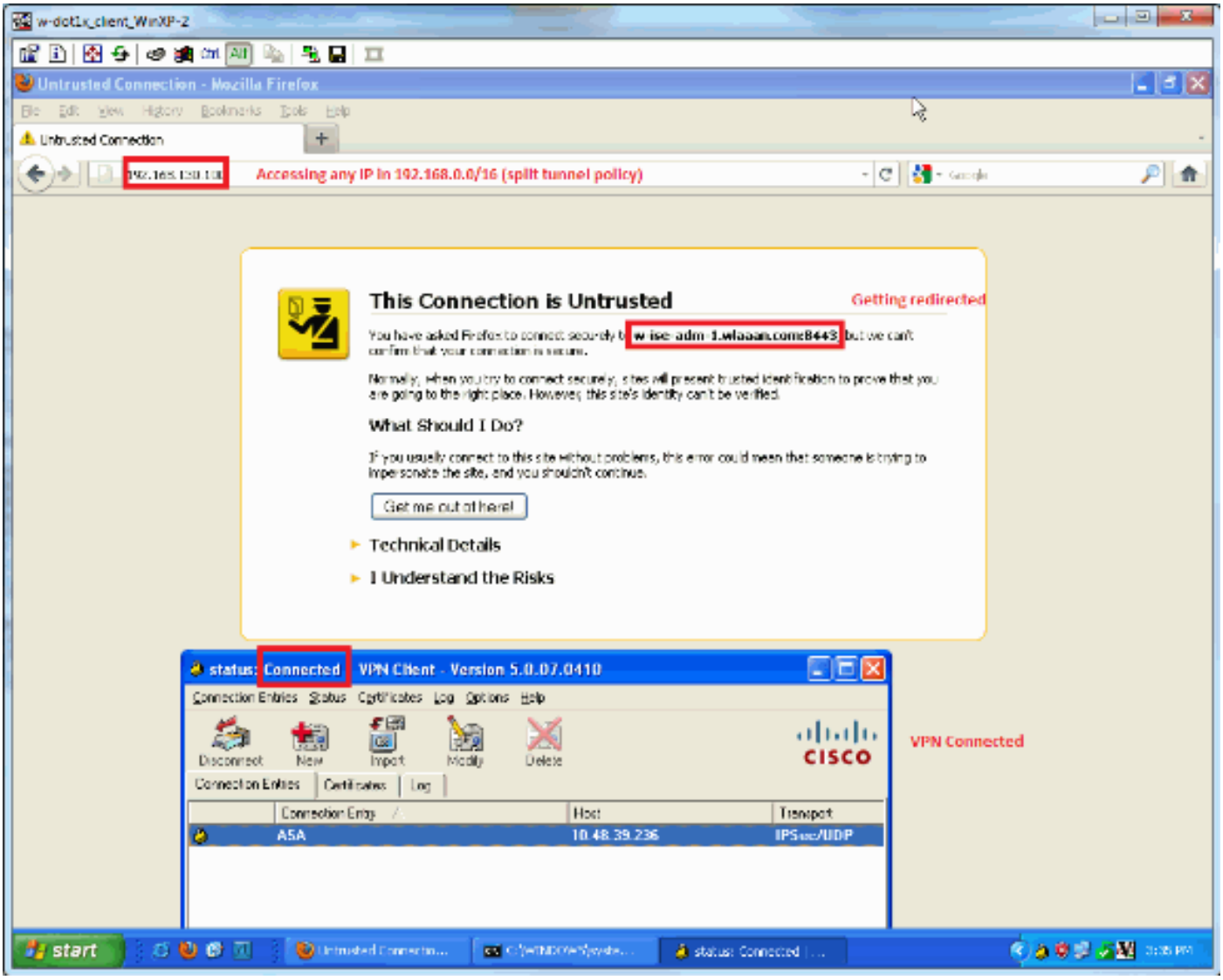


Authorization:

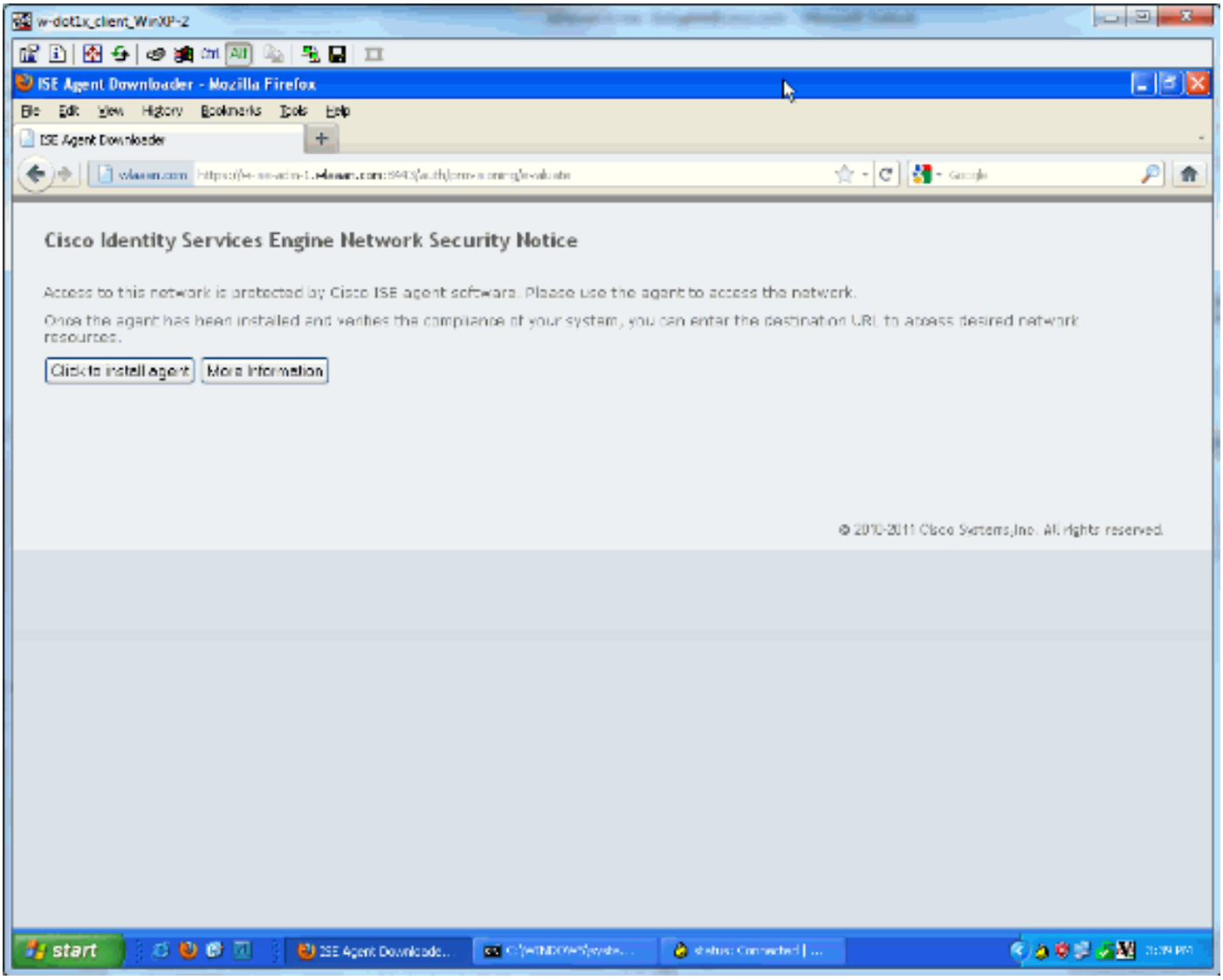


Nota: se l'agente non è installato sul computer, è possibile definire le regole di provisioning client.

Risultato



Viene richiesto di installare l'agente (in questo esempio, il provisioning del client è già impostato):



Alcuni output in questa 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
```

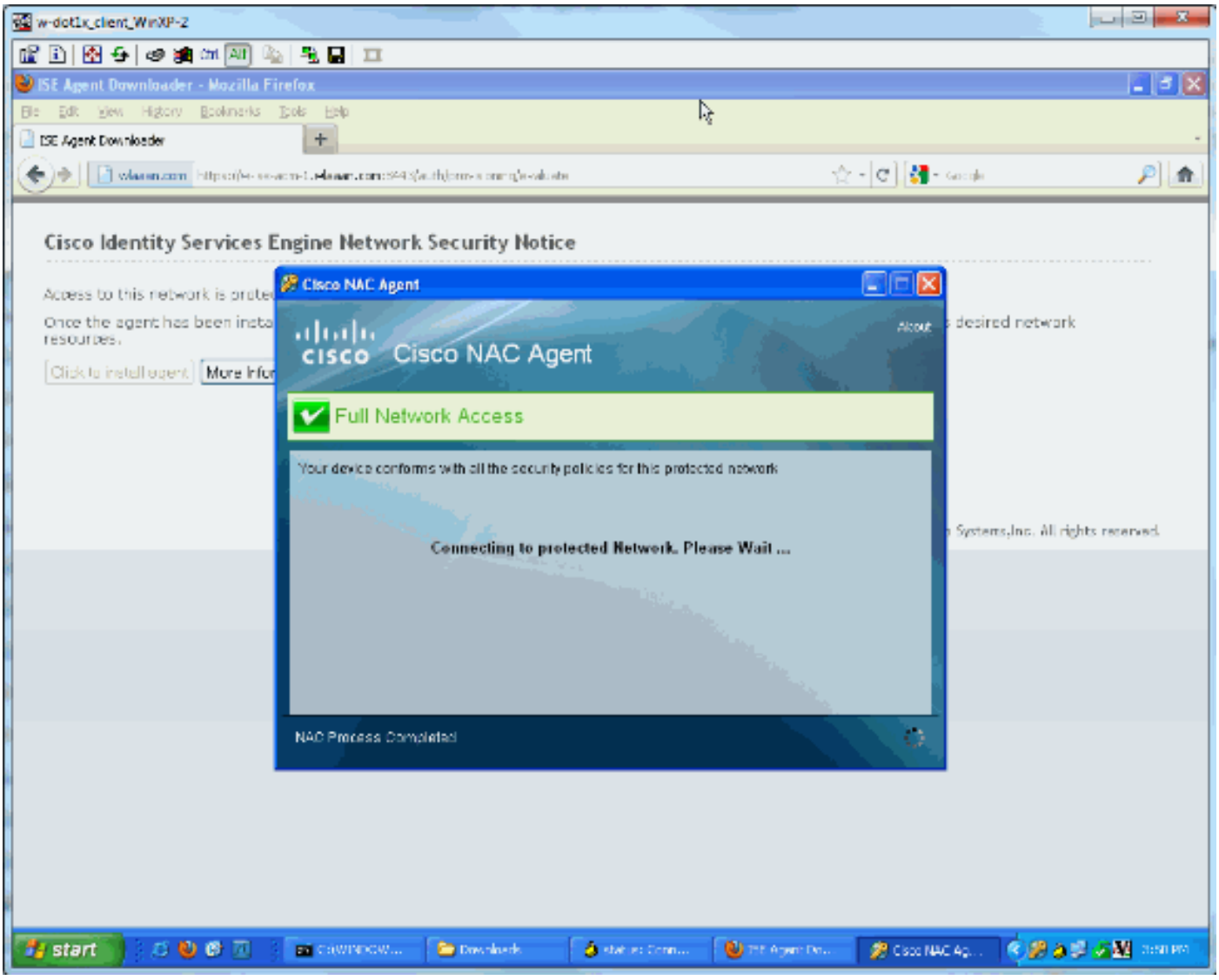
E dall'iPEP:

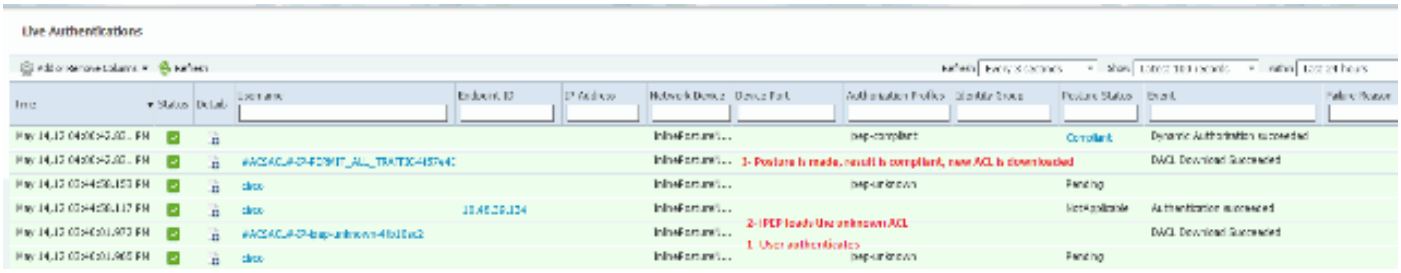
```
w-ise-ipep-1/admin# show pep table session

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
```

Dopo aver scaricato e installato l'agente:

L'agente deve rilevare automaticamente l'ISE ed eseguire la valutazione della postura (supponendo che le regole di postura siano già state definite, che è un altro argomento). In questo esempio, la postura ha esito positivo e viene visualizzato quanto segue:





Nota: nella schermata precedente sono presenti due autenticazioni. Tuttavia, poiché la casella iPEP memorizza gli ACL nella cache, non viene scaricata ogni volta.

Sull'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#
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems