

# VPN Inline Posture met iPEP ISE en ASA

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Basisstroom](#)

[Topologie](#)

[ASA-configuratie](#)

[ISE-configuratie](#)

[iPEP-configuratie](#)

[Configuratie van verificatie en opslag](#)

[Configuratie van beveiligingsprofielen](#)

[Configuratie van autorisatie](#)

[Resultaat](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document bevat informatie over het instellen van inline-poster met een adaptieve security applicatie (ASA) en een Identity Services Engine (ISE).

## [Voorwaarden](#)

### [Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

### [Gebruikte componenten](#)

De informatie in dit document is gebaseerd op versie 8.2(4) voor de ASA en versie 1.1.0.665 voor de ISE.

### [Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

## Achtergrondinformatie

ISE biedt veel AAA-services (polijsten, profileren, verificatie, enzovoort). Sommige netwerkapparaten (NAD) ondersteunen Radius Change of Authorization (CoA), die het autorisatieprofiel van een eindapparaat dynamisch kan veranderen op basis van zijn Posture of Profiling resultaat. Andere NAD's zoals de ASA ondersteunen deze optie nog niet. Dit betekent dat een ISE die in Inline Posture EnHandhaving Mode (iPEP) actief is nodig is om het beleid voor netwerktoegang van een eindapparaat dynamisch te wijzigen.

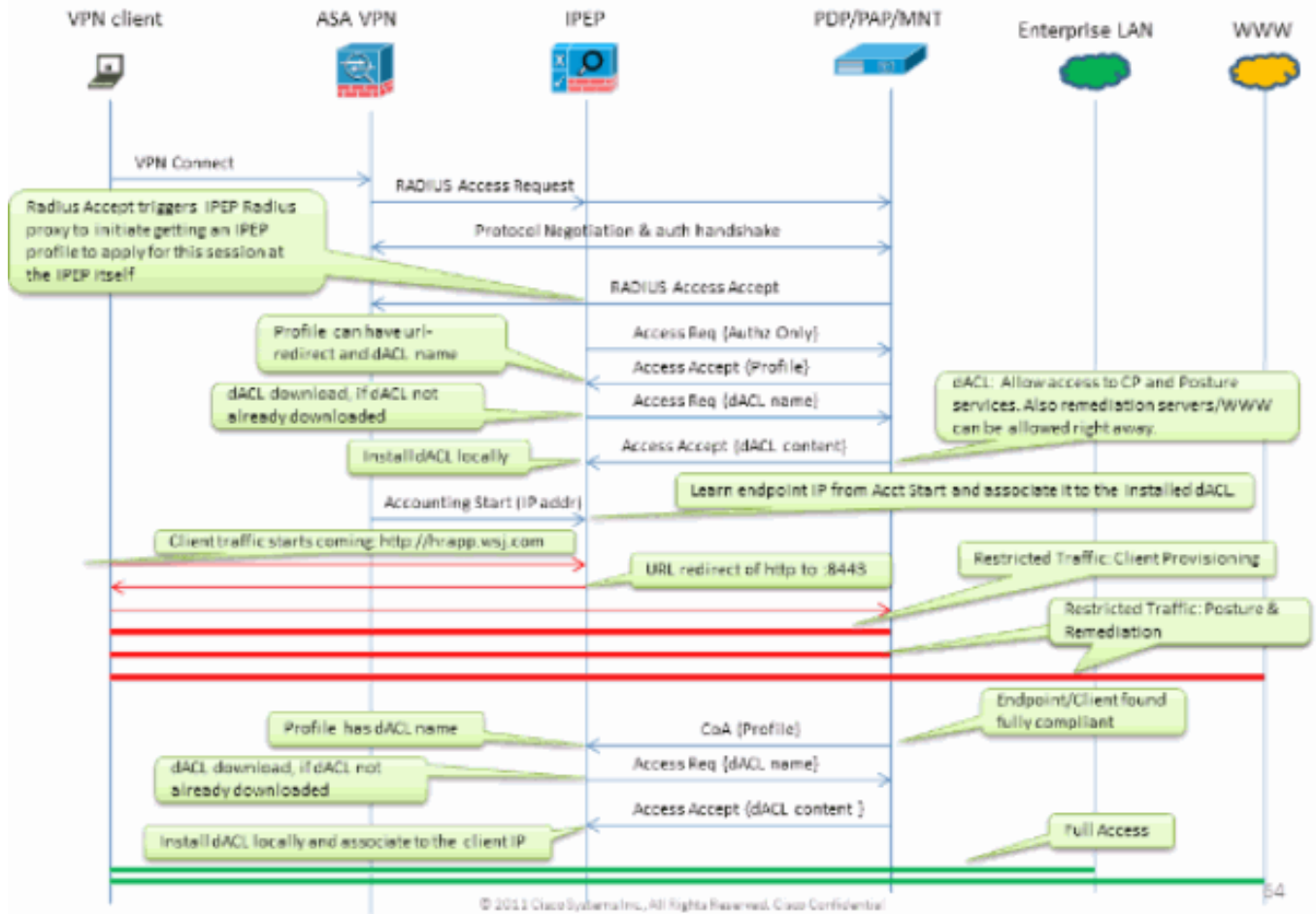
Het basisconcept is dat al het gebruikersverkeer via de iPEP zal gaan, waarbij het knooppunt ook fungeert als een RADIUS-proxy.

## Basisstroom

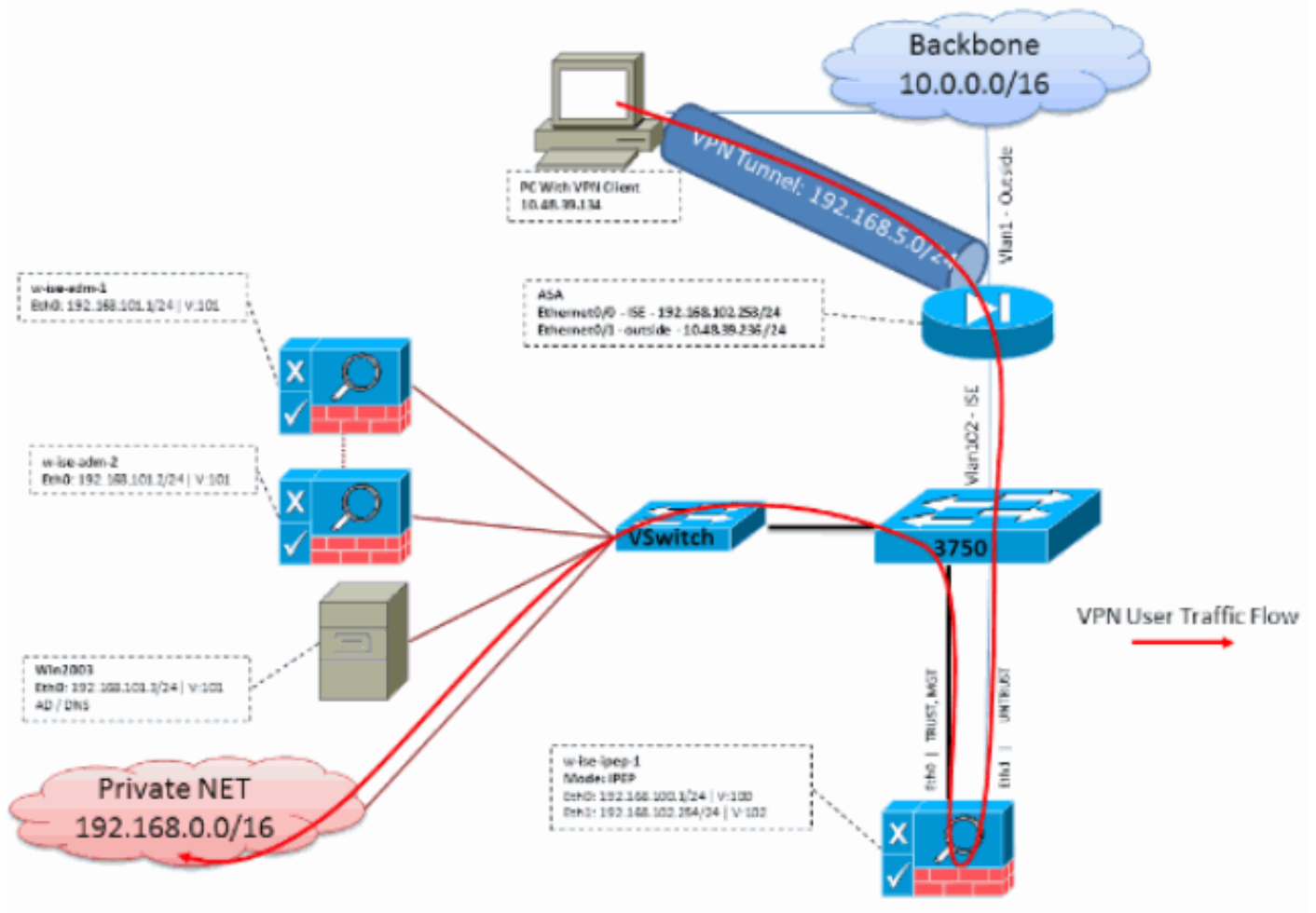
1. VPN-gebruiker logt in.
2. ASA stuurt het verzoek naar het iPEP-knooppunt (ISE).
3. iPEP schrijft het verzoek opnieuw (door de eigenschappen van Cisco AV-PAIR toe te voegen om aan te geven dat dit een iPEP-verificatie is) en stuurt het verzoek naar het ISE Policy Node (PDP).
4. Het VOB antwoordt op het iPEP, dat aan het NAD zal worden toegezonden.
5. Als de gebruiker echt is bevonden, DIENT DE NAD een accounting-start aanvraag te verzenden (zie CSCtz84826 ). Dit zal het begin van de sessie op de iPEP starten. In deze fase wordt de gebruiker opnieuw georiënteerd op posterijen. Daarnaast moet u tijdelijke accounting-update voor tunnels mogelijk maken die vanaf het WEBVPN Portal is gemaakt, omdat ISE verwacht dat het attribueert framed-ip-adres in de Straal accounting is. Wanneer u echter een verbinding maakt met het portal, is het VPN IP-adres van de client nog niet bekend omdat de tunnel niet is aangelegd. Dit zal ervoor zorgen dat de ASA tijdelijke updates zal sturen, zoals wanneer de tunnel zal worden ingericht.
6. De gebruiker gaat de beoordeling van de positie door en op basis van de resultaten zal de PDP de sessie met CoA op de iPEP bijwerken.

Dit screenshot illustreert dit proces:

## Inline PEP Client Authorization Flow



## Topologie



## ASA-configuratie

ASA Configuration is een eenvoudige IPSEC Remote 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-configuratie

### iPEP-configuratie

Het eerste wat je moet doen is een ISE toevoegen als iPEP knooppunt. U vindt hier meer informatie over het proces:

[http://www.cisco.com/en/US/docs/security/ise/1.1/user\\_guide/ise\\_ipeg\\_deploy.html#wp1110248](http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_ipeg_deploy.html#wp1110248).

Dit is eigenlijk wat u in de verschillende tabbladen moet configureren (er worden screenshots gegeven in deze paragraaf):

- Het configureren van onvertrouwde IP- en Global IP-instellingen (in dit geval is onbetrouwbare IP 192.168.102.254).
- De implementatie wordt routinematig uitgevoerd.
- Plaats een statisch filter zodat de ASA door het iPEP vakje kan gaan (anders wordt de verbinding naar/van de ISE via iPEP verbroken).
- Configureer de Policy ISE als Radius server en de ASA als RADIUS-client.
- Voeg een route aan het Subnet van VPN toe die aan de ASA wijst.
- Stel de ISE van de bewaking in als de Logging Host (poort 20514); in dit geval volgt ook de ISE het beleid).

### **Belangrijke eisen voor configuratie van het certificaat:**

Zorg er voordat u probeert een iPEP-knooppunt te registreren voor dat aan de volgende vereisten voor uitgebreid certificaat is voldaan. Als de certificaten niet goed zijn geconfigureerd op de iPEP- en de Admin-knooppunten, wordt het registratieproces voltooid. U verliest echter de toegang tot de beheerder van het iPEP-knooppunt. De volgende details zijn geëxtrapoleerd uit de ISE 1.1.x iPEP-implementatiegids:

De aanwezigheid van bepaalde combinaties van eigenschappen in de plaatselijke certificaten van de Administratie- en Inline Posture-knooppunten kan wederzijdse authenticatie verhinderen.

De eigenschappen zijn:

- Extended Key Application (EKA) - serververificatie
- Extended Key Gebruik (EKA) - Clientverificatie
- NetFlow Type-SSL serververificatie
- NetFlow Type-SSL clientverificatie

Voor het toedieningscertificaat is één van de volgende combinaties vereist:

- Beide eigenschappen van EKA moeten worden uitgeschakeld, indien beide eigenschappen van EKA in het certificaat van inline Posture worden uitgeschakeld, of als beide

eigenschappen van ECU moeten worden ingeschakeld, als de servereigenschap is ingeschakeld in het certificaat van inline Posture.

- Zowel de eigenschappen van het type Netscape wilden worden uitgeschakeld, als beide moeten worden ingeschakeld.

Voor het Inline Posture-certificaat is één van de volgende combinaties vereist:

- Zowel de ECU eigenschappen moeten worden uitgeschakeld, als beide moeten worden ingeschakeld of de servereigenschap alleen moet worden ingeschakeld.
- Zowel de eigenschappen van het Type Netscape Cert moeten worden uitgeschakeld, als beide moeten worden ingeschakeld of de servereigenschap alleen moet worden ingeschakeld.
- Wanneer zelfondertekende lokale certificaten op de knooppunten van de administratie en van de Inline Posture worden gebruikt, moet u het zelf ondertekende certificaat van het knooppunt van de Administratie in de vertrouwenslijst van het knooppunt van de Inline Posture installeren. Als u zowel de primaire als de secundaire knooppunten van het Toezicht in uw plaatsing hebt, moet u het zelf-ondertekende certificaat van beide knopen van het Toezicht in de vertrouwenslijst van het Online Posture knooppunt installeren.
- Wanneer CA-ondertekende lokale certificaten worden gebruikt op de knooppunten voor de administratie en inline Posture, dient wederzijdse authenticatie correct te werken. In dit geval is het certificaat van de ondertekenende CA voor registratie op het beheerknooppunt geïnstalleerd en wordt dit certificaat gekopieerd naar het knooppunt Inline Posture.
- Als CA-uitgegeven toetsen worden gebruikt om communicatie tussen de knooppunten voor de administratie en inline Posture te beveiligen, voordat u het inline Posture-knooppunt registreert, moet u de openbare sleutel (CA-certificaat) van het beheerknooppunt aan de CA-certificaatlijst van het inline Posture-knooppunt toevoegen.

**Basisconfiguratie:**

## Edit Node

General Settings Basic Information Deployment Modes Filters Radius Config Managed Subnets Static Routes Logging Failover

Node Name **w-lse-ipep-1**

*\* Configuration changes in this tab will result in node reboot.*

### Basic Information

Host Name **w-lse-ipep-1**

Domain Name **wlaaan.com**

#### Time Sync Server

Primary   
Secondary   
Tertiary

#### DNS Server

\* Primary   
Secondary   
Tertiary

### Trusted Interface (to protected network)

IP Address **192.168.100.1**  
Subnet Mask **255.255.255.0**  
Default Gateway **192.168.100.250**

Set Management VLAN

ID

### Untrusted Interface (to managed network)

\* IP Address   
\* Subnet Mask   
\* Default Gateway

Set Management VLAN

ID

Save

Reset

## Configuratie implementatiemodus:

## Edit Node

General Settings Basic Information Deployment Modes Filters Radius Config Managed Subnets Static Routes Logging Failover

Node Name **w-lse-ipep-1**

*\* Configuration changes in this tab will result in both active and standby nodes reboot.*

Maintenance Mode  Routed Mode  Bridged Mode

Save

Reset

## Configuratie filters:

## Edit Node

General Settings Basic Information Deployment Modes **Filters** Radius Config Managed Subnets Static Routes Logging Fallover

Node Name wise-ipep-1

## MAC Filters

MAC Address	IP Address	Description
<input type="text"/>	<input type="text"/>	<input type="text"/>

## Subnet Filters

Subnet Address	Subnet Mask	Description
<input type="text" value="192.168.102.253"/>	<input type="text" value="255.255.255.255"/>	<input type="text" value="ASA"/>

## Configuratie straat:

## Edit Node

General Settings Basic Information Deployment Modes Filters **Radius Config** Managed Subnets Static Routes Logging Fallover

Node Name wise-ipep-1

## Radius Configuration

## Server Configuration

IP Address	Shared Secret	Timeout(in seconds)	Retries	Description	Enable KeyWrap	Authentication Settings
<input type="text" value="192.168.101.1"/>	<input type="text" value="*****"/>	<input type="text" value="5"/>	<input type="text" value="3"/>	<input type="text" value="ISE ADM"/>	<input type="checkbox"/>	<input type="text" value="*****"/>

## Client Configuration

IP Address	Shared Secret	Timeout(in seconds)	Retries	Description	Enable KeyWrap	Authentication Settings
<input type="text" value="192.168.102.253"/>	<input type="text" value="*****"/>	<input type="text" value="5"/>	<input type="text" value="3"/>	<input type="text" value="ASA"/>	<input type="checkbox"/>	<input type="text" value="*****"/>

## Statische routes:

## Edit Node

General Settings Basic Information Deployment Modes Filters Radius Config Managed Subnets **Static Routes** Logging Fallover

Node Name wise-ipep-1

## Static Routes

Subnet Address	Subnet Mask	Interface Type	Default Gateway	Description
<input type="text" value="192.168.5.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="Untrusted"/>	<input type="text" value="192.168.102.253"/>	<input type="text"/>

## Vastlegging:



## Edit Node

General Settings Basic Information Deployment Modes Filters Radius Config Managed Subnets Static Routes **Logging** Failover

Node Name wise-ipep-1

**Logging**

\* IP Address

\* Port

## Configuratie van verificatie en opslag

Er zijn drie postuur-staten:

- Onbekend: Posture is nog niet gemaakt
- Conforme: Post wordt gemaakt en het systeem is compatibel
- Niet-conforme: Er wordt een wachttijd gemaakt, maar het systeem heeft ten minste één controle gefaald

Nu moeten de vergunningsprofielen worden gecreëerd (dit zijn inline autorisatieprofielen: Dit zal de eigenschap `ipep-auz=True` in Cisco (aav-paar) toevoegen die voor de verschillende case zal worden gebruikt.

Vaak keert het Onbekende profiel de herdirect URL (plaatsontdekking) terug die het verkeer van de gebruiker aan ISE door zal sturen en zal vragen om de NAC Agent te installeren. Als de NAC Agent al geïnstalleerd is, zal deze zijn HTTP Discovery- aanvraag aan ISE kunnen doorsturen.

In dit profiel wordt een ACL gebruikt die HTTP-verkeer naar ISE en DNS ten minste toestaat.

De conforme en niet-conforme profielen retourneren doorgaans een downloadbare ACL-toegangsapparaat om netwerktoegang te verlenen op basis van het gebruikersprofiel. Het niet-conforme profiel kan de gebruikers toegang geven tot een webserver om bijvoorbeeld een antivirus te downloaden of beperkte netwerktoegang te verlenen.

In dit voorbeeld worden de profielen Onbekend en Compliant gemaakt, en wordt de aanwezigheid van `notepad.exe` gecontroleerd als vereisten.

## Configuratie van beveiligingsprofielen

Het eerste wat u moet doen is het maken van de downloadbare ACL's (dACL's) en profielen:

**Opmerking:** Dit is niet verplicht om de dACL-naam te hebben die bij de profielnaam hoort.

- conformeACL: `ipep onbekendRegistratieprofiel: ipep onbekend`
- niet-conformeACL: `ipep-niet-conformeRegistratieprofiel: ipep-niet-conforme`

**Onbekende dACL:**

## Downloadable ACL

\* Name

Description

\* DACL Content  
deny tcp any any eq 80  
permit ip any host 192.168.101.1  
permit udp any any eq 53


### Onbekend profiel:

#### Inline Posture Node Profile

\* Name

Description

\* DACL Name

**URL Redirect** 

#### Attributes Details

```
cisco-av-pair = ipep-authz=true  
DACL = ipep-unknown  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cpp
```

### Voldoende dACL:

Downloadable ACL List > PERMIT\_ALL\_TRAFFIC

## Downloadable ACL

\* Name PERMIT ALL TRAFFIC

Description Allow all Traffic

\* DACL Content permit ip any any

Voldoende profiel:

Inline Posture Node Profiles > ipep-compliant

## Inline Posture Node Profile

\* Name ipep-compliant

Description

\* DACL Name PERMIT\_ALL\_TRAFFIC

URL Redirect

### Attributes Details

```
cisco-av-pair = ipep-authz=true  
DACL = PERMIT_ALL_TRAFFIC
```

Save

Reset

## Configuratie van autorisatie

Nu het profiel is gemaakt, moet u het Radius-verzoek van de iPEP benaderen en de juiste profielen toepassen. De iPEP ISE's zijn gedefinieerd met een speciaal hulpmiddeltype dat in de machtigingsregels zal worden gebruikt:

**NAD's:**

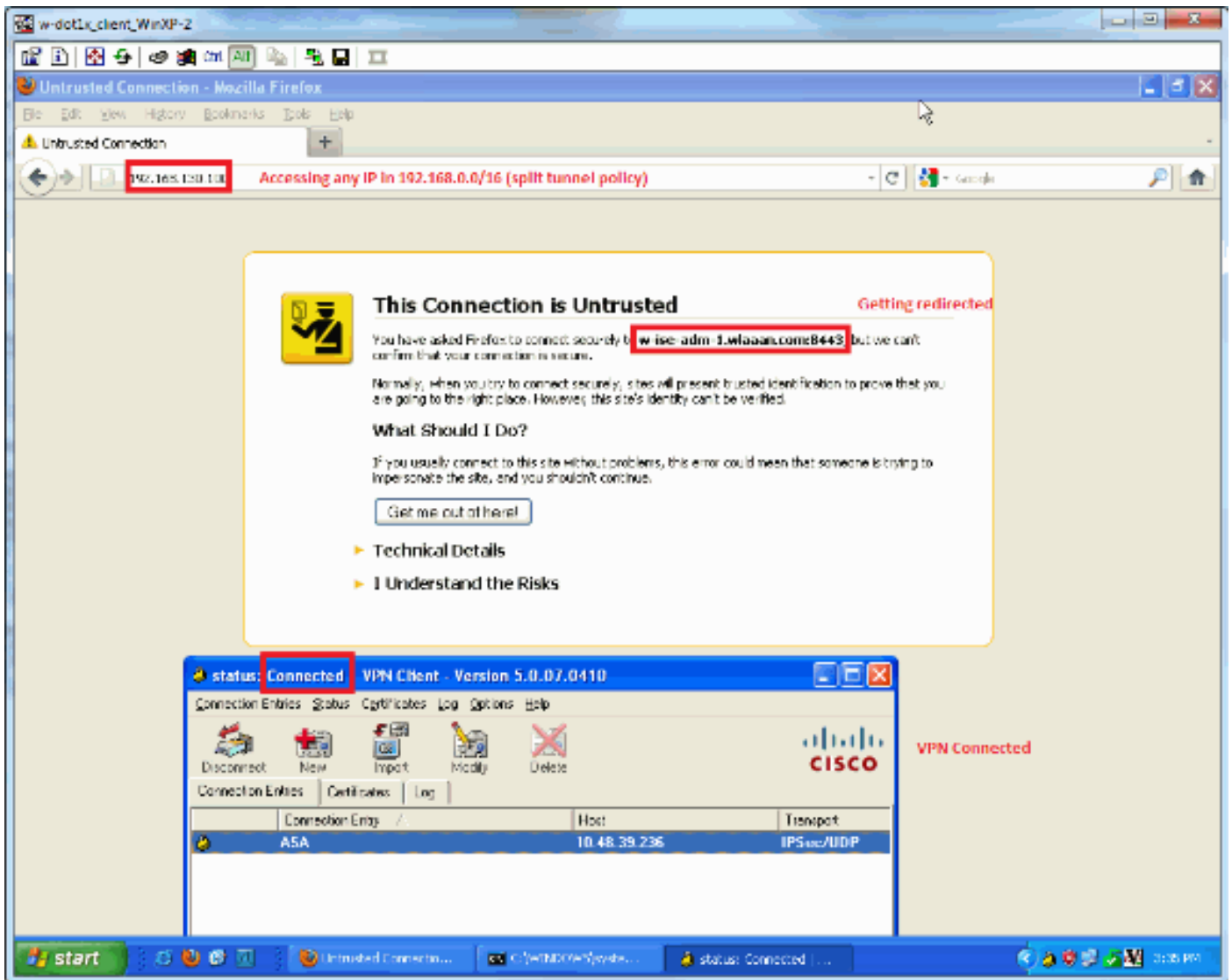
Network Devices					
Name	IP/Mask	Location	Type	Description	
<input type="checkbox"/> c3560	192.168.50.5/32	All Locations	All Device Types		
<input type="checkbox"/> InlinePostureNode-192-1...	192.168.100.1/32	All Locations	ISE#PEP ISE	System generated network device for Inl...	
<input type="checkbox"/> InlinePostureNode-192-1...	192.168.100.2/32	All Locations	ISE#PEP ISE	System generated network device for Inl...	
<input type="checkbox"/> w-5508-2	192.168.2.50/32	All Locations	All Device Types	192.168.2.50	

## Authorization:

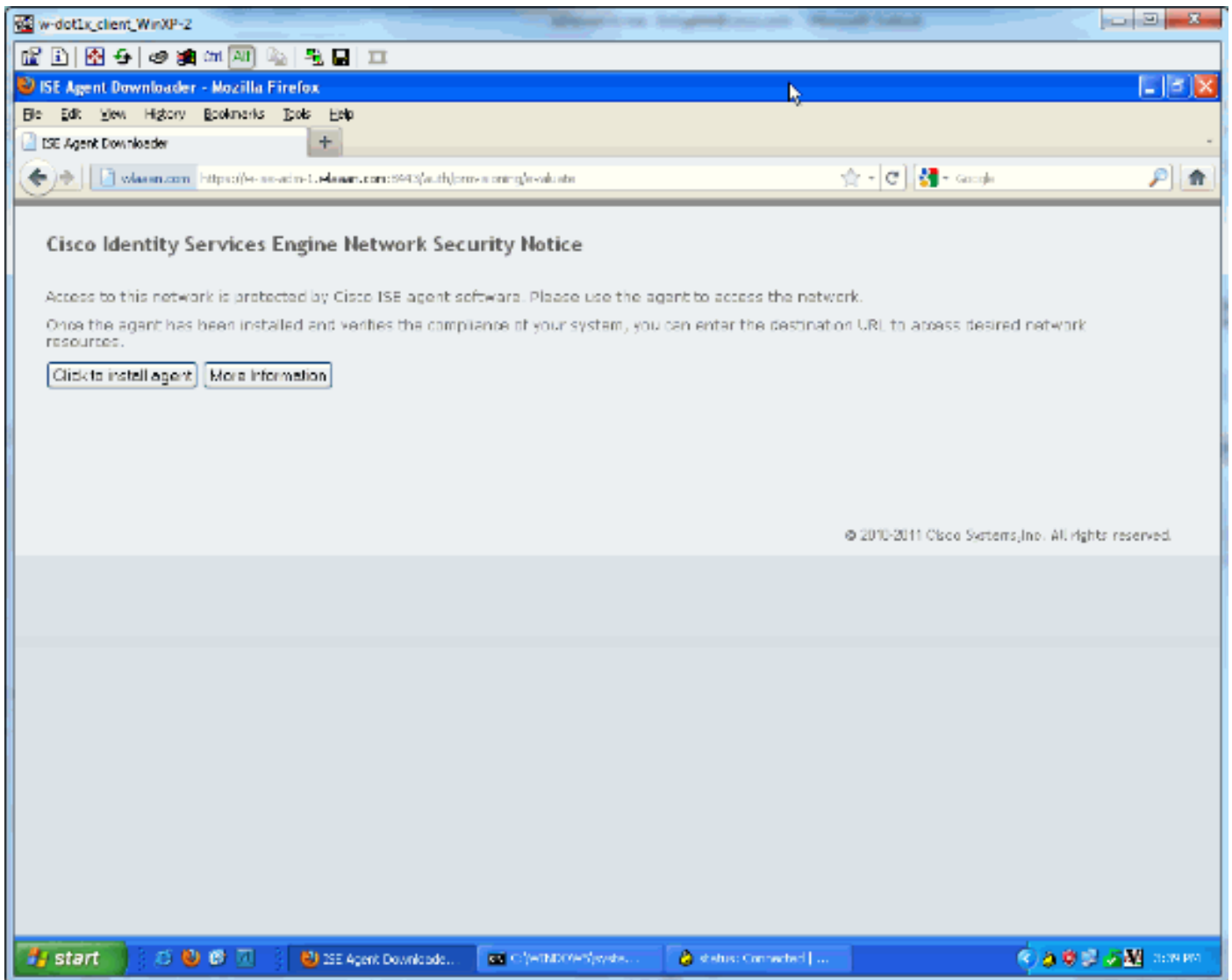
Authorization Policy				
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.				
First Matched Rule Applies				
▶ Exceptions (0)				
Status	Rule Name	Conditions (Identity groups and other conditions)		Permissions
<input checked="" type="checkbox"/>	PEP-VPN-unknown	if (Radius:NAS-Port-Type EQUALS Virtual AND Session:PostureStatus EQUALS Unknown AND DEVICE:Device Type EQUALS All Device Types#ISE#PEP ISE )	then	!pep-unknown
<input checked="" type="checkbox"/>	PEP-VPN-Compliant	if (Radius:NAS-Port-Type EQUALS Virtual AND DEVICE:Device Type EQUALS All Device Types#ISE#PEP ISE AND Session:PostureStatus EQUALS Compliant )	then	!pep-compliant

**N.B.:** Als de agent niet op de machine is geïnstalleerd, kunt u regels voor clientprovisioning definiëren.

## Resultaat



U wordt gevraagd de agent te installeren (in dit voorbeeld is de instelling van de client al ingesteld):



## Een deel van de productie in deze 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
```

## En van de iPEP:

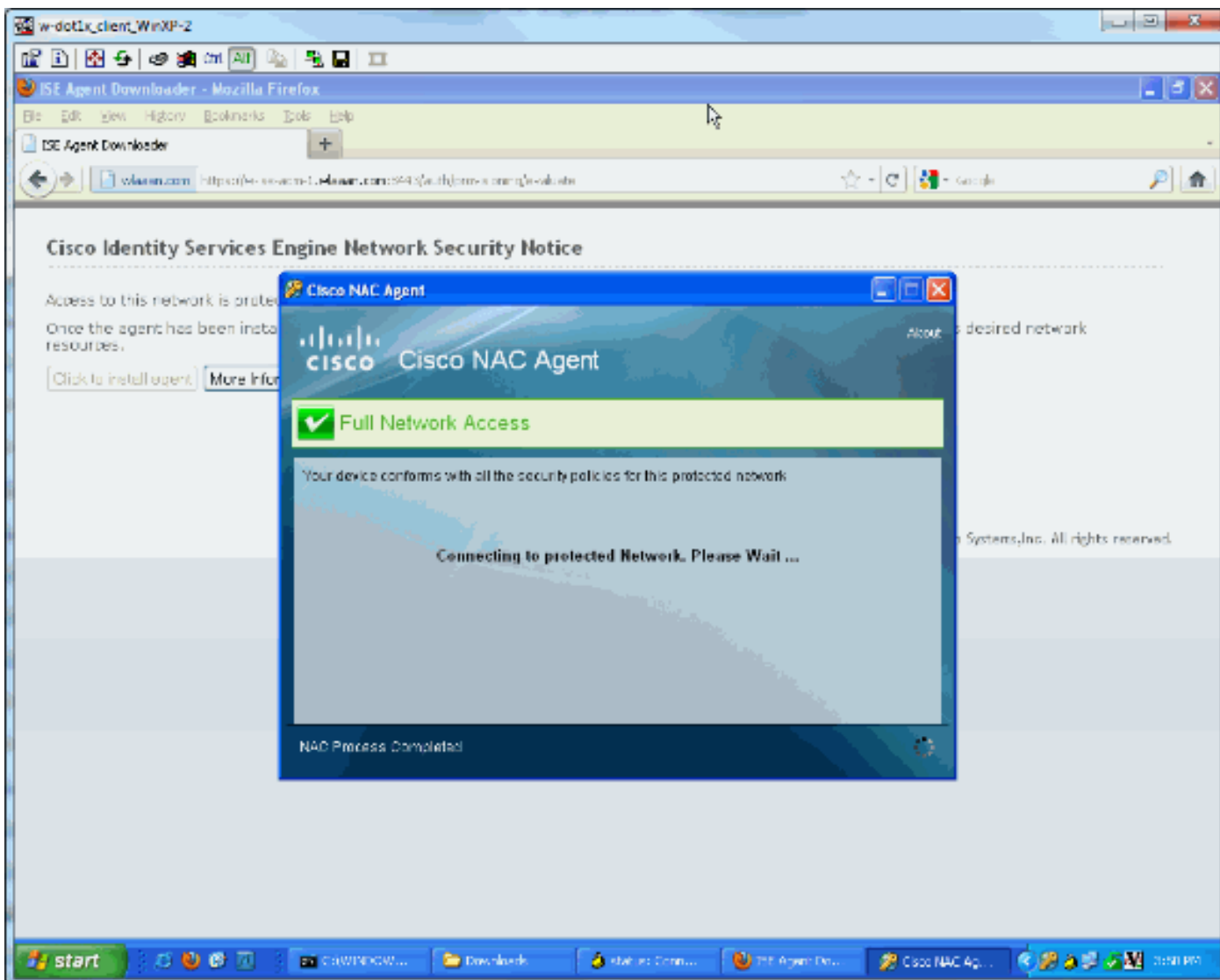
```
w-ise-ipep-1/admin# show pep table session
```

```
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
```

**Nadat de agent is gedownload en geïnstalleerd:**

De agent dient automatisch de ISE te detecteren en de beoordeling van de positie uit te voeren (ervan uitgaande dat u de regels voor de houding al hebt gedefinieerd, wat een ander onderwerp is). In dit voorbeeld is de opstelling succesvol, en dit lijkt:



Use Authentications

Time	Status	Detail	Endpoint ID	IP Address	Network Device	Device Port	Authentication Policy	Device Status	Policy Status	Event	Policy Reason
Nov 14 12:04:26:2012 FR	OK				InfoForum...		isp-compliant	Compliant	Compliant	Dynamic Authentication successful	
Nov 14 12:04:26:2012 FR	OK				InfoForum...		1- Posture is made, result is compliant, new ACL is downloaded	Compliant	Compliant	DACL Download Succeeded	
Nov 14 12:02:42:6117 FR	OK				InfoForum...		isp-compliant	Pending	Pending		
Nov 14 12:02:42:6117 FR	OK		12.46.22.124		InfoForum...		2- iPEP loads the unknown ACL	NotCompliant	NotCompliant	Authentication successful	
Nov 14 12:02:42:6117 FR	OK				InfoForum...		1- User authenticates	Pending	Pending	DACL Download Succeeded	

**Opmerking:** het bovenstaande screenshot bevat twee authenticaties. Maar omdat het iPEP-vak de ACL's caches geeft, wordt het niet elke keer gedownload.

Op de 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#
```

## [Gerelateerde informatie](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)