# VPN Inline Posture using iPEP ISE and ASA

**Document ID: 115724**

Contributed by Bastien Migette, Cisco TAC Engineer.
Mar 19, 2013

## Contents

## Introduction

This document provides information on how to set up inline posture with an Adaptive Security Appliance (ASA) and an Identity Services Engine (ISE).

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on version 8.2(4) for the ASA and version 1.1.0.665 for the ISE.

### Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

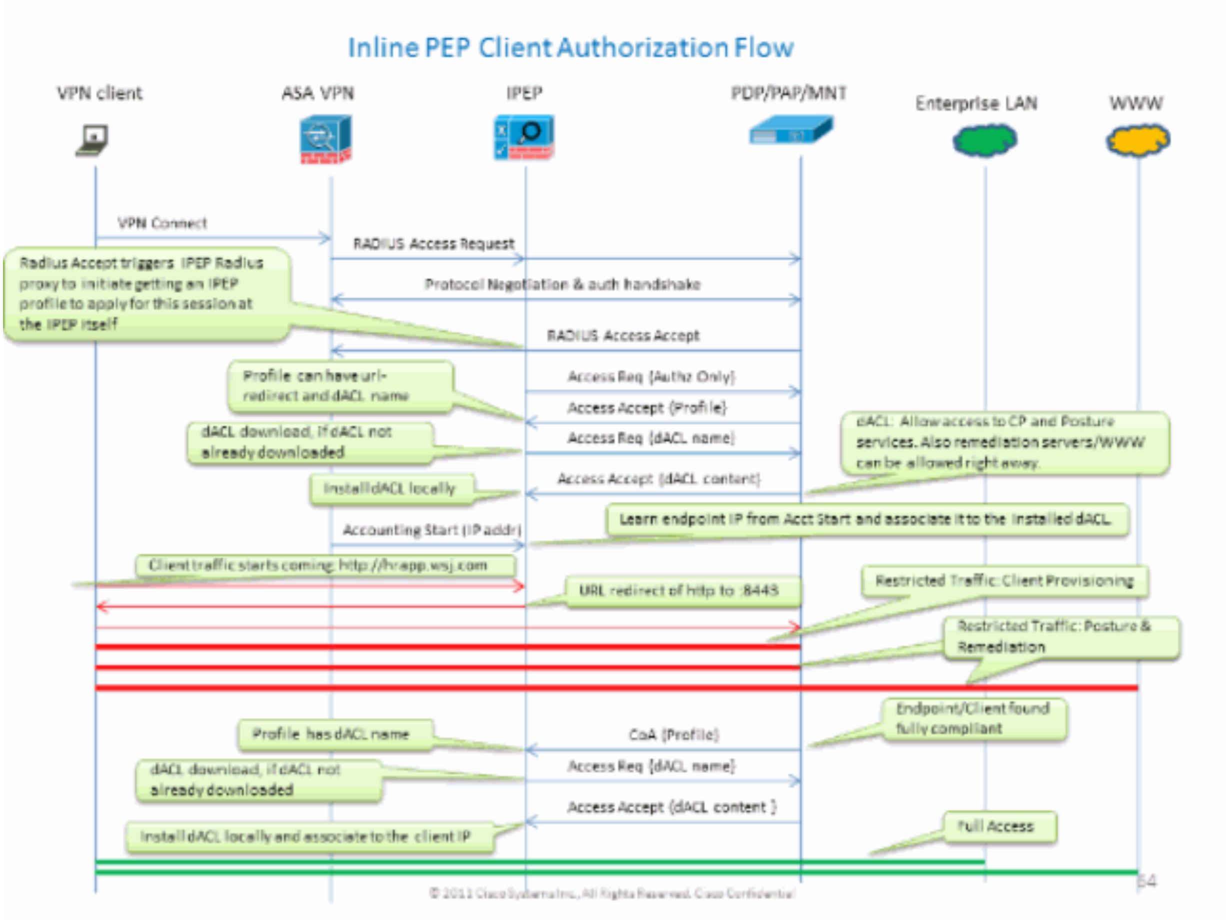
The ISE provides a lot of AAA Services (Posture, Profiling, Authentication, etc). Some Network Devices (NAD) support Radius Change Of Authorization (CoA) that allows to dynamically change the authorization profile of an end device based on its Posture or Profiling result. Other NADs such as the ASA do not support this feature yet. This means that an ISE running in Inline Posture Enforcement mode (iPEP) is needed to dynamically change the network access policy of an end device.

The basic concept is that all user traffic will go through the iPEP, with the node also acting as a Radius Proxy.

## Basic Flow

1. VPN User logs in.
2. ASA sends the request to the iPEP node (ISE).
3. The iPEP rewrites the request (by adding Cisco AV−PAIR attributes to indicate this is an iPEP authentication) and sends the request to the ISE Policy Node (PDP).
4. The PDP replies back to the iPEP which will forward to the NAD.
5. If the user is authenticated, the NAD MUST send an accounting−start request (see CSCtz84826 ). This will trigger the session initiation on the iPEP. At this stage, the user is redirected for posture. Additionally, you need to enable interim−accounting−update for tunnel established from the WEBVPN Portal, as the ISE expects to have the attribute framed−ip−address in the radius accounting. However, when connecting to the portal, the VPN IP Address of the client is not yet known because the tunnel is not established. This will ensure that the ASA will send interim updates, such as when the tunnel will be established.
6. The user goes through the posture assessment, and based on the results the PDP will update the session using CoA on the iPEP.

This screenshot illustrates this process:



Inline PEP Client Authorization Flow

Radius Accept triggers IPEP Radius proxy to initiate getting an IPEP profile to apply for this session at the IPEP itself

Profile can have url-redirect and dACL name

dACL download, if dACL not already downloaded

dACL: Allow access to CP and Posture services. Also remediation servers/WWW can be allowed right away.

Install dACL locally

Learn endpoint IP from Acct Start and associate it to the installed dACL

Client traffic starts coming: http://hrapp.wsj.com

URL redirect of http to :8443

Restricted Traffic: Client Provisioning

Restricted Traffic: Posture & Remediation

Endpoint/Client found fully compliant

Profile has dACL name

dACL download, if dACL not already downloaded

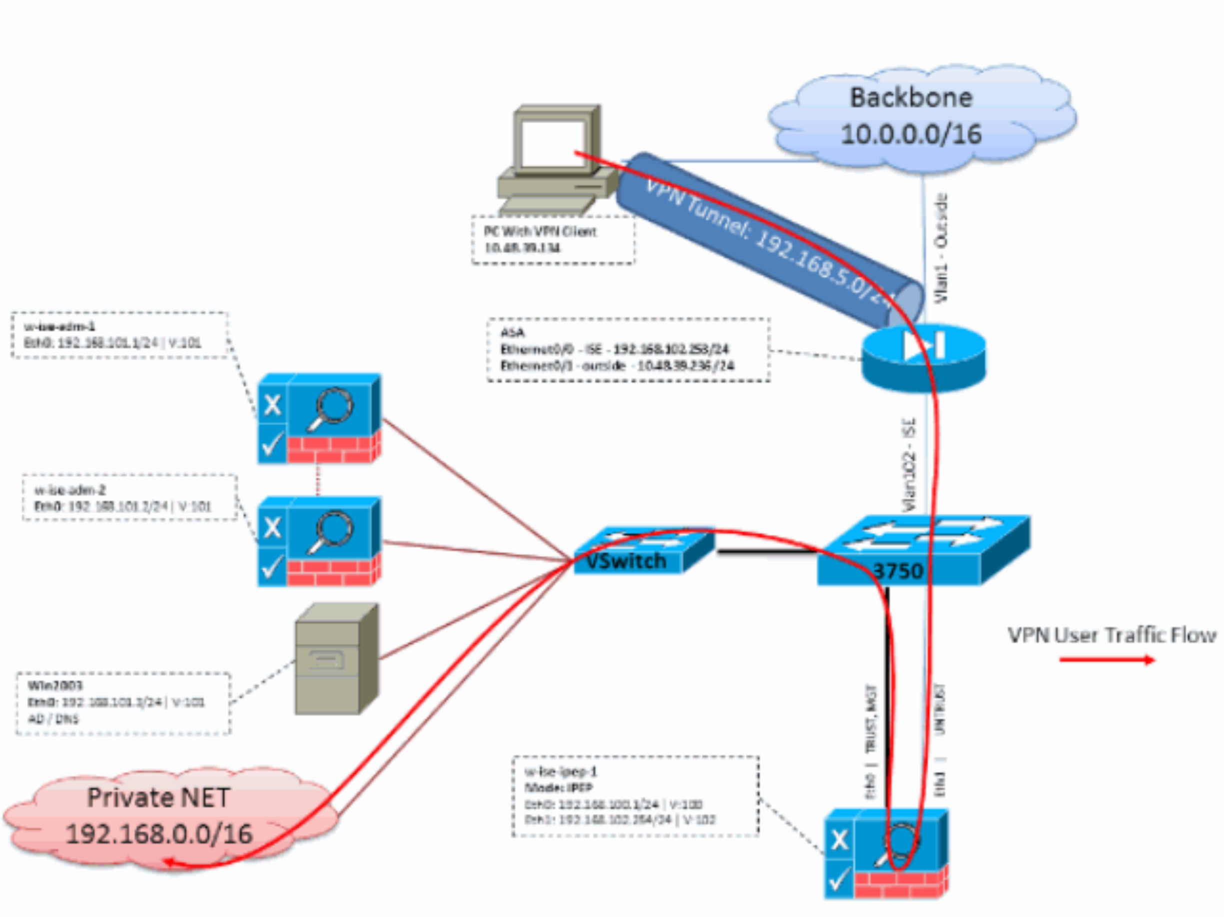
Install dACL locally and associate to the client IP

Full Access

64

© 2011 Cisco Systems Inc., All Rights Reserved. Cisco Confidential

## Example Topology



Backbone
10.0.0.0/16
PC With VPN Client
10.48.39.134
VPN Tunnel: 192.168.5.0/24
Vlan1 - Outside
w-ise-adm-1
Eth0: 192.168.101.1/24 | V:101
ASA
Ethernet0/0 - ISE - 192.168.102.253/24
Ethernet0/1 - outside - 10.48.39.236/24
Vlan102 - ISE
w-ise-adm-2
Eth0: 192.168.101.2/24 | V:101
VSwitch
3750
VPN User Traffic Flow
Win2003
Eth0: 192.168.101.3/24 | V:101
AD / DNS
Eth0 | TRUST, MGT
Eth1 | UNTRUST
w-ise-ipep-1
Mode: IPEP
Eth0: 192.168.100.1/24 | V:100
Eth1: 192.168.102.254/24 | V:102
Private NET
192.168.0.0/16

## ASA Configuration

The ASA Configuration is a simple 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 Configuration

## iPEP Configuration

The first thing to do is to add an ISE as an iPEP Node. You can find additional information about the process here:

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

This is basically what you have to configure in the various tabs (screenshots provided in this section illustrate this):

- Configure untrusted IP and Global IP settings (in this case, untrusted IP is 192.168.102.254).
- Deployment is routed mode.
- Put a static filter for the ASA to be allowed to go through the iPEP box (otherwise, connectivity to/from the ISE thru iPEP box is dropped).
- Configure the Policy ISE as Radius server and the ASA as Radius client.
- Add a route to the VPN Subnet that points to the ASA.

- Set the Monitoring ISE as the Logging Host (port 20514 by default; in this case, the policy ISE is monitoring as well).

**Important Certificate Configuration Requirements:**

Before attempting to register an iPEP node, ensure that the following certificate Extended Key Usage requirements are met. If the certificates are not properly configured on the iPEP and Admin nodes, the registration process will complete. However, you will lose admin access to the iPEP node. The following details have been extrapolated from the ISE 1.1.x iPEP Deployment Guide:

The presence of certain combinations of attributes in the local certificates of the Administration and Inline Posture nodes can prevent mutual authentication from working.

The attributes are:

- Extended Key Usage (EKU) Server Authentication
- Extended Key Usage (EKU) Client Authentication
- Netscape Cert Type SSL Server Authentication
- Netscape Cert Type SSL Client Authentication

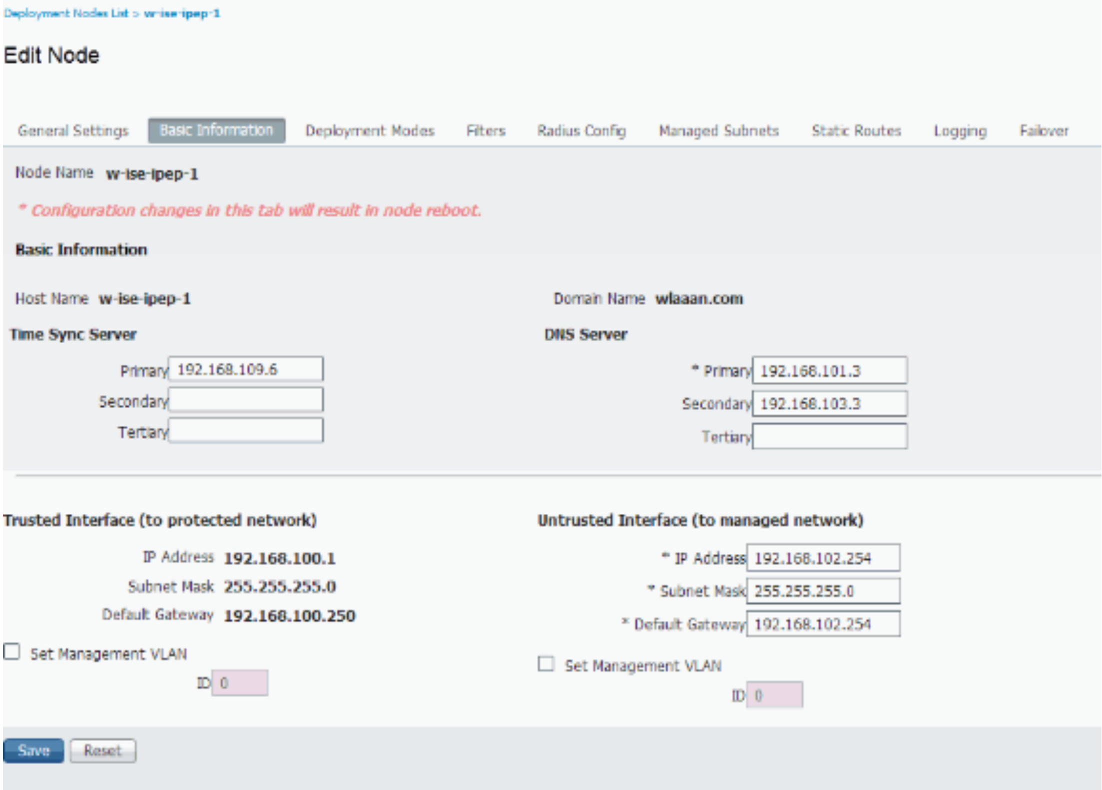
Either of the following combinations is required for the Administration certificate:

- Both EKU attributes should be disabled, if both EKU attributes are disabled in the Inline Posture certificate, or both EKU attributes should be enabled, if the server attribute is enabled in the Inline Posture certificate.
- Both Netscape Cert Type attributes should be disabled, or both should be enabled.

Either of the following combinations is required for the Inline Posture certificate:

- Both EKU attributes should be disabled, or both should be enabled, or the server attribute alone should be enabled.
- Both Netscape Cert Type attributes should be disabled, or both should be enabled, or the server attribute alone should be enabled.
- Where self−signed local certificates are used on the Administration and Inline Posture nodes, you must install the self−signed certificate of the Administration node in the trust list of the Inline Posture node. In addition, if you have both primary and secondary Administration nodes in your deployment, you must install the self−signed certificate of both Administration nodes in the trust list of the Inline Posture node.
- Where CA−signed local certificates are used on the Administration and Inline Posture nodes, mutual authentication should work correctly. In this case, the certificate of the signing CA is installed on the Administration node prior to registration, and this certificate is replicated to the Inline Posture node.
- If CA−issued keys are used for securing communication between the Administration and Inline Posture nodes, before you register the Inline Posture node, you must add the public key (CA certificate) from the Administration node to the CA certificate list of the Inline Posture node.

**Basic Configuration:**



Deployment Nodes List > w-ise-ipep-1

Edit Node

Node Name w-ise-ipep-1

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

Basic Information

Host Name w-ise-ipep-1

Domain Name wlaaan.com

Time Sync Server

Primary 192.168.109.6

Secondary

Tertiary

DNS Server

* Primary 192.168.101.3

Secondary 192.168.103.3

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 0

Untrusted Interface (to managed network)

* IP Address 192.168.102.254

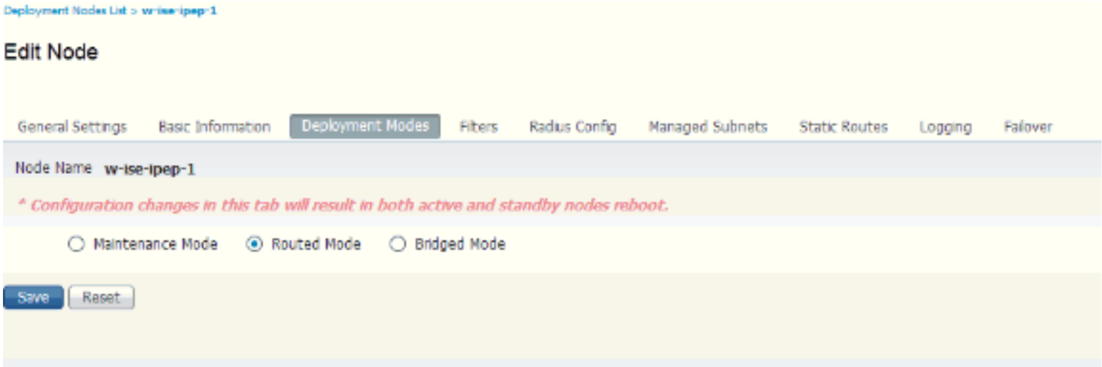
* Subnet Mask 255.255.255.0

* Default Gateway 192.168.102.254

□ Set Management VLAN

ID 0

## Deployment Mode Configuration:



Deployment Nodes List > w-ise-ipep-1

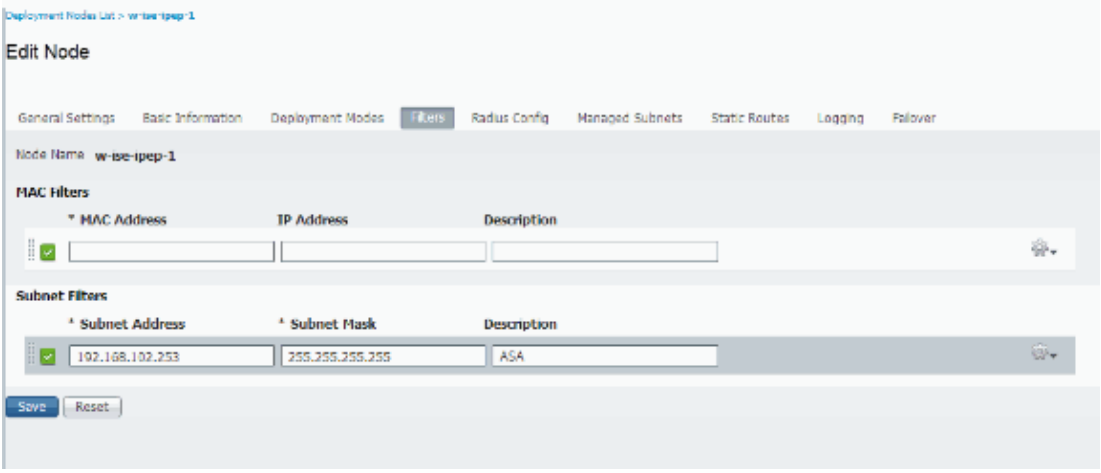
Edit Node

Node Name w-ise-ipep-1

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

○ Maintenance Mode ● Routed Mode ○ Bridged Mode

## Filters Configuration:



Deployment Nodes List > w-ise-ipep-1

Edit Node

Node Name w-ise-ipep-1

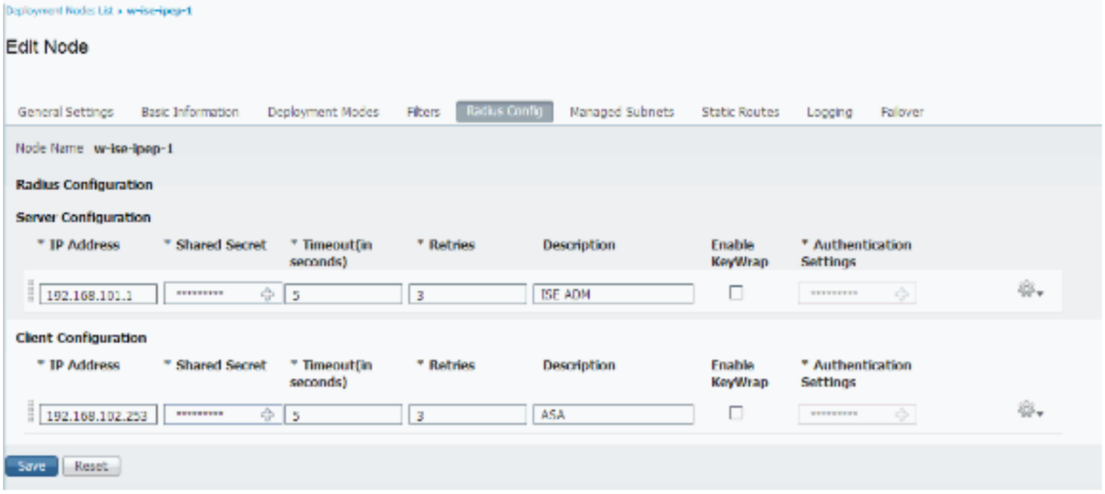
MAC Filters

|  | * MAC Address | IP Address | Description |
|---|---|---|---|
| ☑ |  |  |  |

Subnet Filters

|  | * Subnet Address | * Subnet Mask | Description |
|---|---|---|---|
| ☑ | 192.168.102.253 | 255.255.255.255 | ASA |

## Radius Configuration:



Deployment Nodes List > w-ise-ipep-1

Edit Node

Node Name w-ise-ipep-1

Radius Configuration

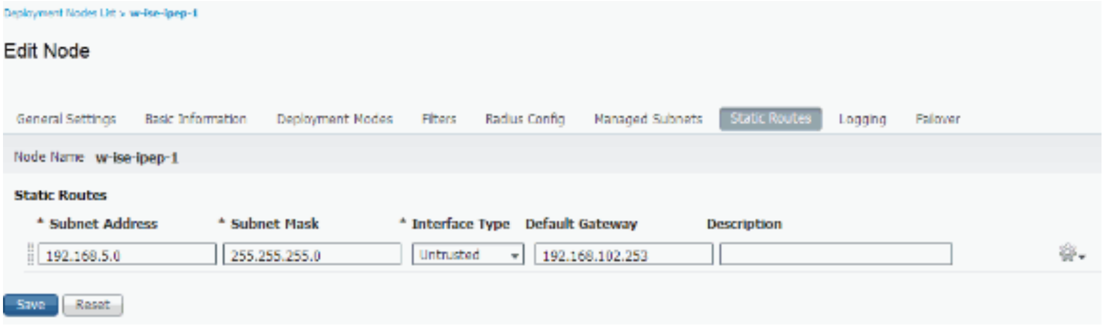
Server Configuration

| * IP Address | * Shared Secret | * Timeout(in seconds) | * Retries | Description | Enable KeyWrap | * Authentication Settings |
|---|---|---|---|---|---|---|
| 192.168.101.1 | ********* | 5 | 3 | ISE ADM | □ | ********* |

Client Configuration

| * IP Address | * Shared Secret | * Timeout(in seconds) | * Retries | Description | Enable KeyWrap | * Authentication Settings |
|---|---|---|---|---|---|---|
| 192.168.102.253 | ********* | 5 | 3 | ASA | □ | ********* |

**Static Routes:**



Deployment Nodes List > w-ise-ipep-1

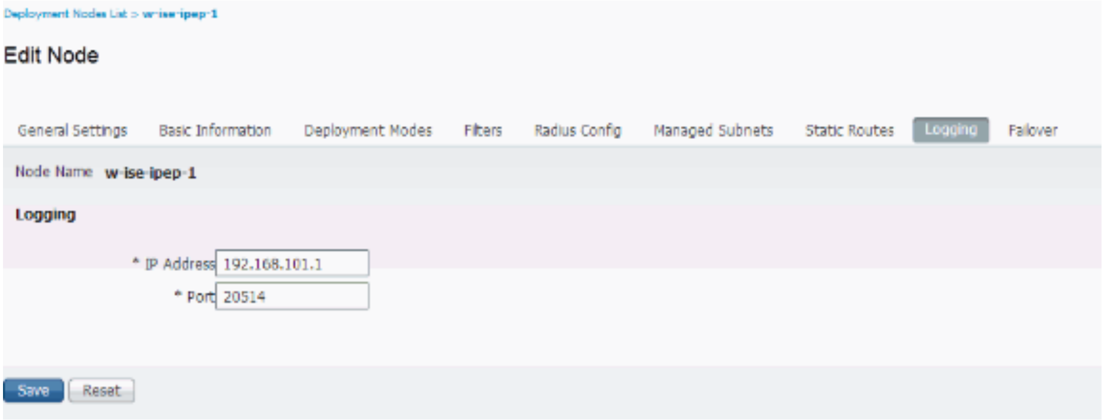
Edit Node

Node Name w-ise-ipep-1

Static Routes

| * Subnet Address | * Subnet Mask | * Interface Type | Default Gateway | Description |
|---|---|---|---|---|
| 192.168.5.0 | 255.255.255.0 | Untrusted | 192.168.102.253 | |

**Logging:**



Deployment Nodes List > w-ise-ipep-1

Edit Node

Node Name w-ise-ipep-1

Logging

* IP Address 192.168.101.1

* Port 20514

# Authentication and Posture Configuration

There are three posture states:

- Unknown: Posture is not yet made
- Compliant: Posture is made and the system is Compliant
- Non−Compliant: Posture is made, but the system failed at least one check

Now the authorization profiles have to be created (which will be Inline Authorization Profiles: This will add the ipep−authz=true attribute in the Cisco AV−Pair) that will be used for the differents case.

Commonly, the Unknown profile returns the redirect URL (posture discovery) which will forward the traffic of the user to the ISE and will ask to install the NAC Agent. If the NAC Agent is already installed, this will allow its HTTP Discovery request to be forwarded to the ISE.

In this profile, an ACL that allows HTTP Traffic to the ISE and DNS at least is used.

The Compliant and Non−compliant profiles usually return a downloadable ACL to grant network access based on the user profile. Non−compliant profile can allow the users to access a web server to download an Antivirus for example, or grant limited network access.

In this example, the Unknown and Compliant profiles are created, and the presence of notepad.exe as requirements is checked.

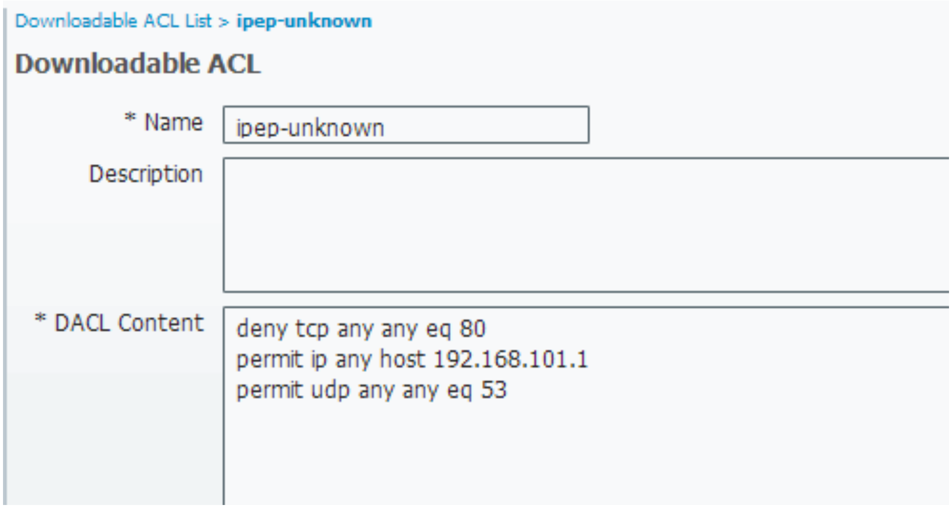
## Posture Profiles Configuration

The first thing to do is to create the Downloadable ACLs (dACL) and profiles:

**Note:** This is not mandatory to have the dACL name matching the profile name.

- Compliant
    - ACL: ipep−unknown
    - Authorization Profile: ipep−unknown
- Non−Compliant
    - ACL: ipep−non−compliant
    - Authorization Profile: ipep−non−compliant

**Unknown dACL:**



Downloadable ACL List > ipep-unknown

Downloadable ACL

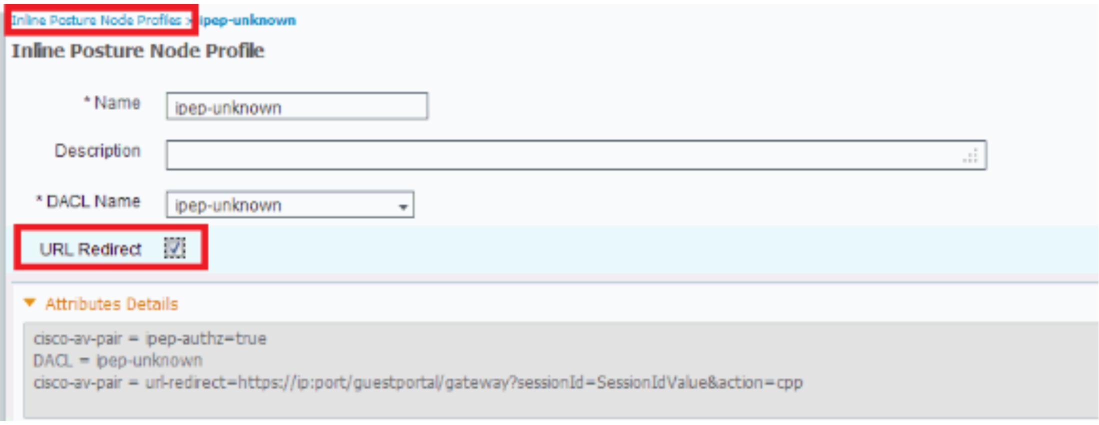
* Name: ipep-unknown

Description:

* DACL Content:

```
deny tcp any any eq 80
permit ip any host 192.168.101.1
permit udp any any eq 53
```

**Unknown Profile:**



Inline Posture Node Profiles > ipep-unknown

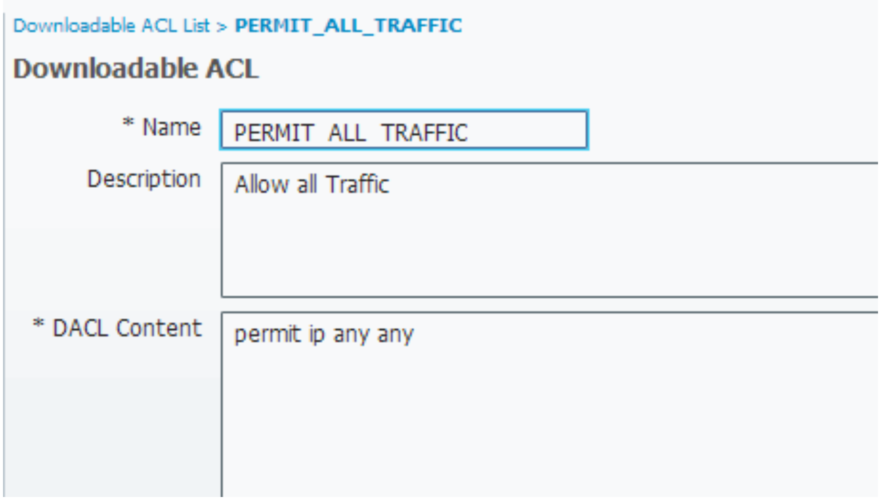
Inline Posture Node Profile

| | |
|---|---|
| * Name | ipep-unknown |
| Description | |
| * DACL Name | ipep-unknown |
| 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
```

**Compliant dACL:**

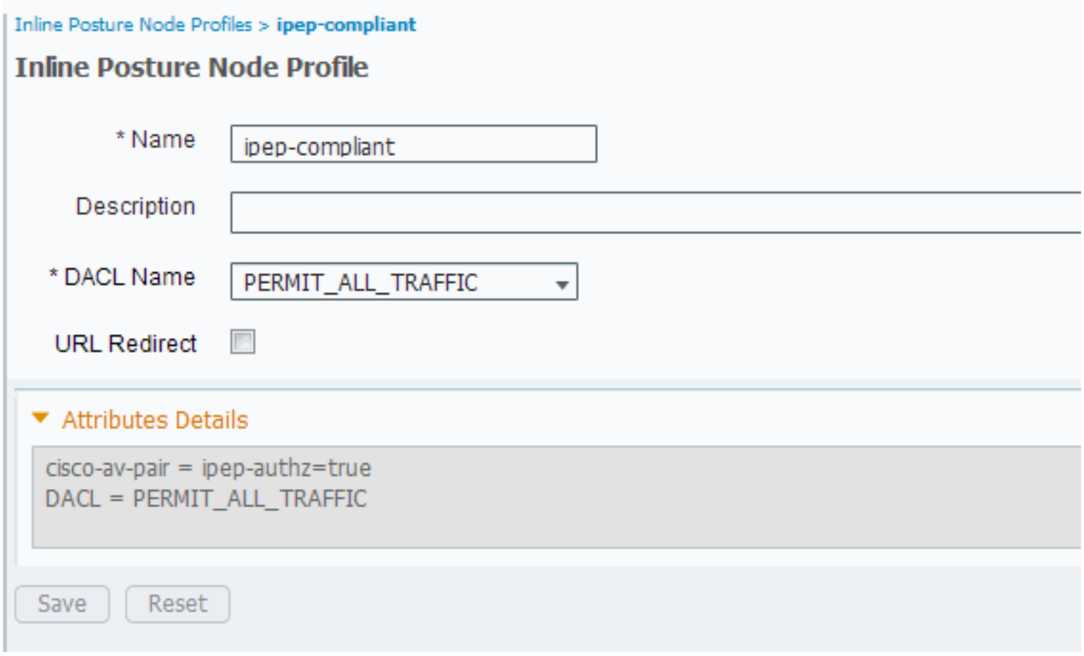


Downloadable ACL List > PERMIT_ALL_TRAFFIC

Downloadable ACL

| | |
|---|---|
| * Name | PERMIT_ALL_TRAFFIC |
| Description | Allow all Traffic |
| * DACL Content | permit ip any any |

**Compliant Profile:**



Inline Posture Node Profiles > ipep-compliant

Inline Posture Node Profile

| | |
|---|---|
| * Name | ipep-compliant |
| Description | |
| * DACL Name | PERMIT_ALL_TRAFFIC |
| URL Redirect | □ |

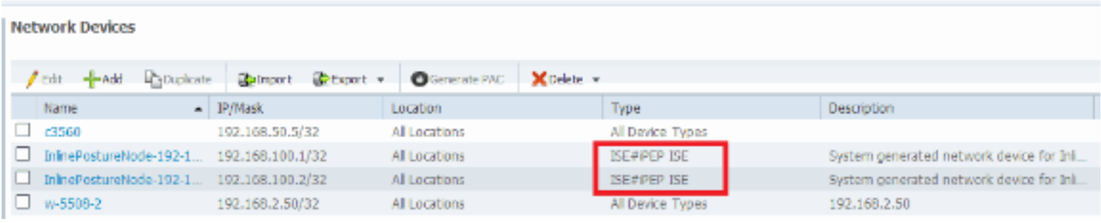
Attributes Details

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

## Authorization Configuration

Now that the profile is created, you need to match the Radius Request coming from the iPEP and apply to them the right profiles. The iPEP ISEs are defined with a special device type that will be used in the Authorization rules:

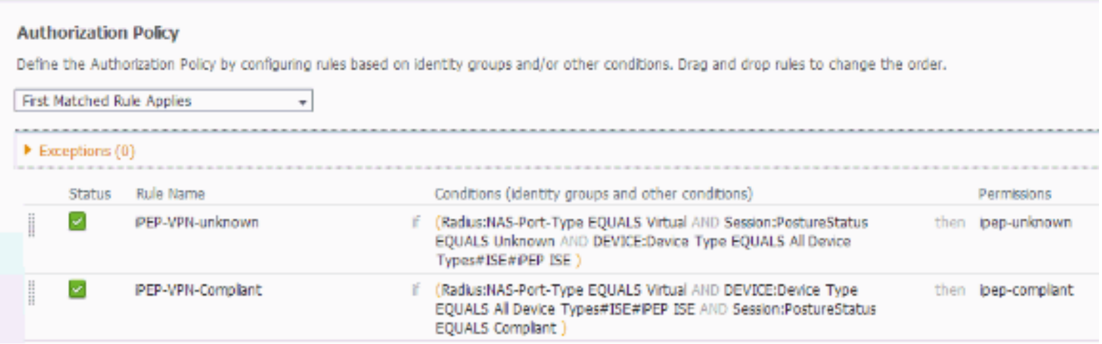
**NADs:**



Network Devices

| | Name | IP/Mask | Location | Type | Description |
|---|---|---|---|---|---|
| ☐ | c3560 | 192.168.50.5/32 | All Locations | All Device Types | |
| ☐ | InlinePostureNode-192-1... | 192.168.100.1/32 | All Locations | ISE#IPEP ISE | System generated network device for Inl... |
| ☐ | InlinePostureNode-192-1... | 192.168.100.2/32 | All Locations | ISE#IPEP ISE | System generated network device for Inl... |
| ☐ | 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.

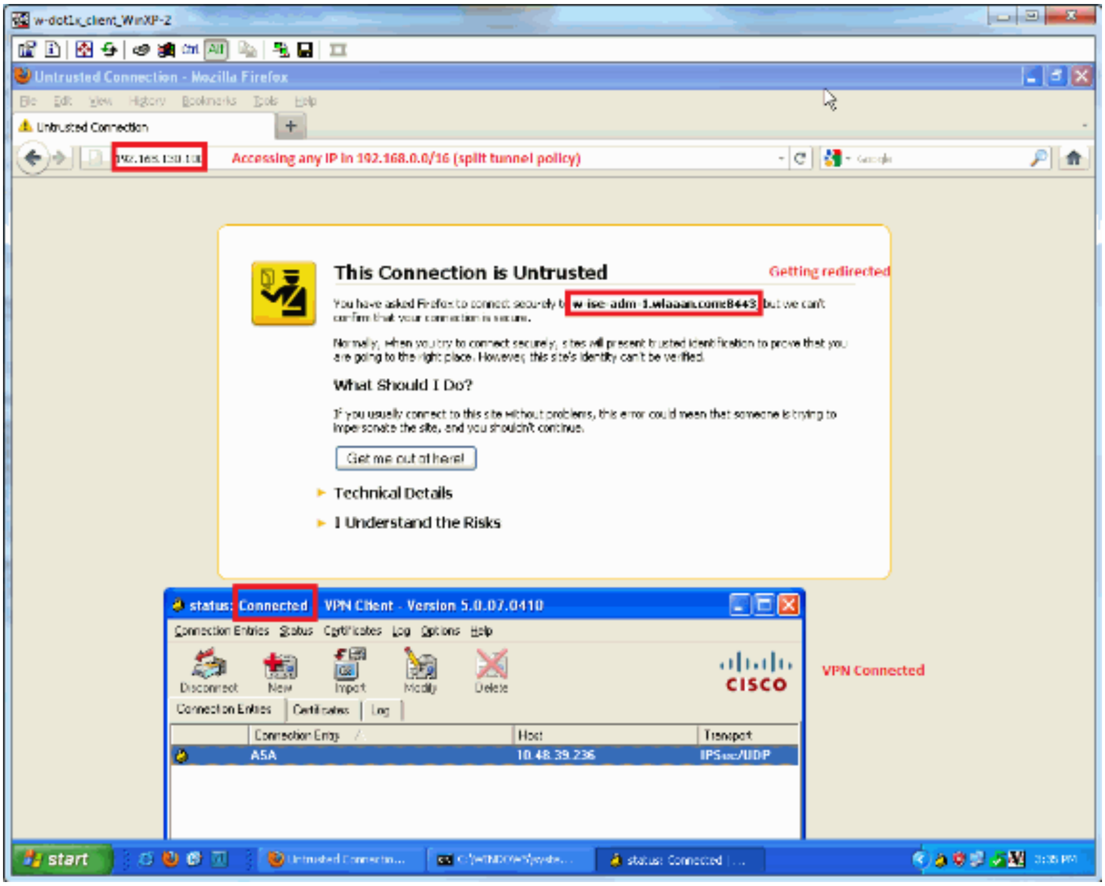
First Matched Rule Applies

Exceptions (0)

| Status | Rule Name | | Conditions (identity groups and other conditions) | | Permissions |
|---|---|---|---|---|---|
| ☑ | IPEP-VPN-unknown | if | (Radius:NAS-Port-Type EQUALS Virtual AND Session:PostureStatus EQUALS Unknown AND DEVICE:Device Type EQUALS All Device Types#ISE#IPEP ISE ) | then | ipep-unknown |
| ☑ | IPEP-VPN-Compliant | if | (Radius:NAS-Port-Type EQUALS Virtual AND DEVICE:Device Type EQUALS All Device Types#ISE#IPEP ISE AND Session:PostureStatus EQUALS Compliant ) | then | ipep-compliant |

**Note:** If the agent is not installed on the machine, you can define Client Provisioning rules.

# Result



w-dot1x_client_WinXP-2

Untrusted Connection - Mozilla Firefox

192.168.120.10

Accessing any IP in 192.168.0.0/16 (split tunnel policy)

This Connection is Untrusted

Getting redirected

You have asked Firefox to connect securely to w-ise-adm-1.wlaaan.com:8443, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

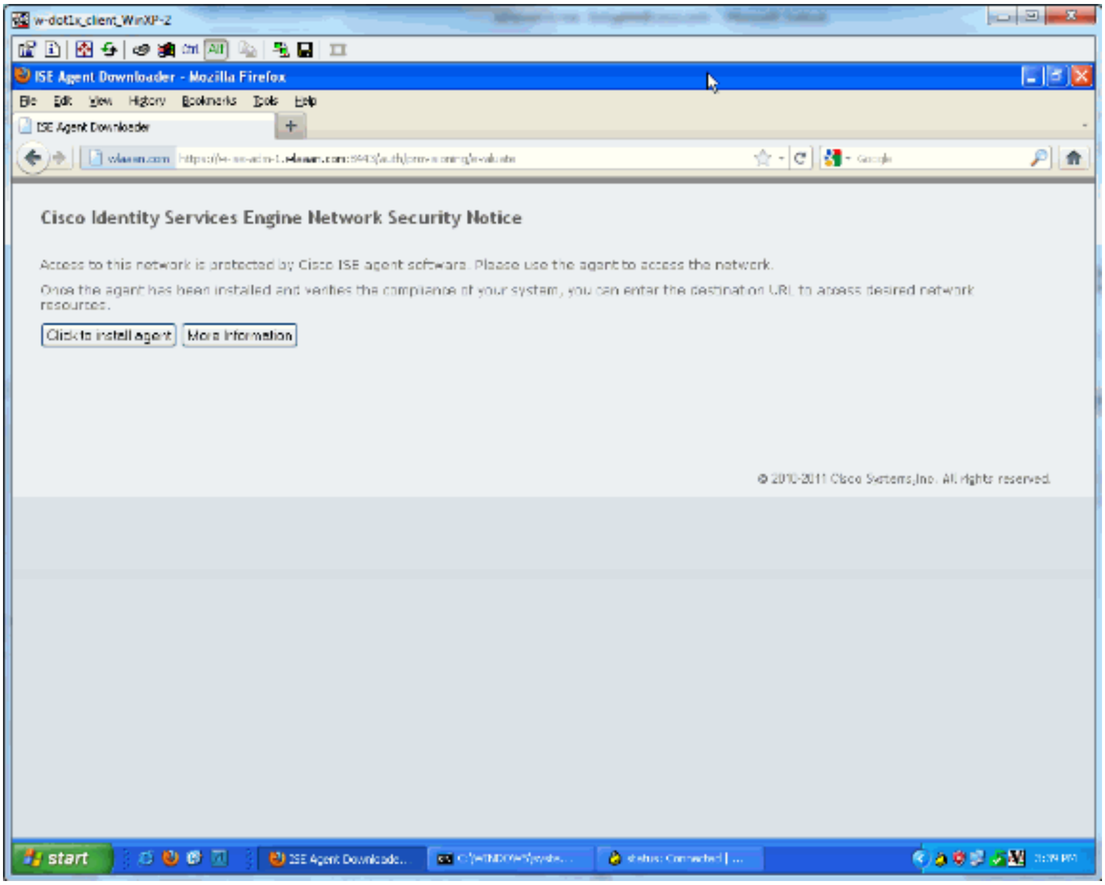
I Understand the Risks

status: Connected | VPN Client - Version 5.0.07.0410

VPN Connected

| Connection Entry | Host | Transport |
|---|---|---|
| ASA | 10.48.39.236 | IPSec/UDP |

You are prompted to install the agent (in this example, client provisioning is already set):



w-dot1x_client_WinXP-2

ISE Agent Downloader - Mozilla Firefox

Cisco Identity Services Engine Network Security Notice

Access to this network is protected by Cisco ISE agent software. Please use the agent to access the network.

Once the agent has been installed and verifies the compliance of your system, you can enter the destination URL to access desired network resources.

Click to install agent | More information

© 2010-2011 Cisco Systems,Inc. All rights reserved.

**Some output at this stage:**

```
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
```

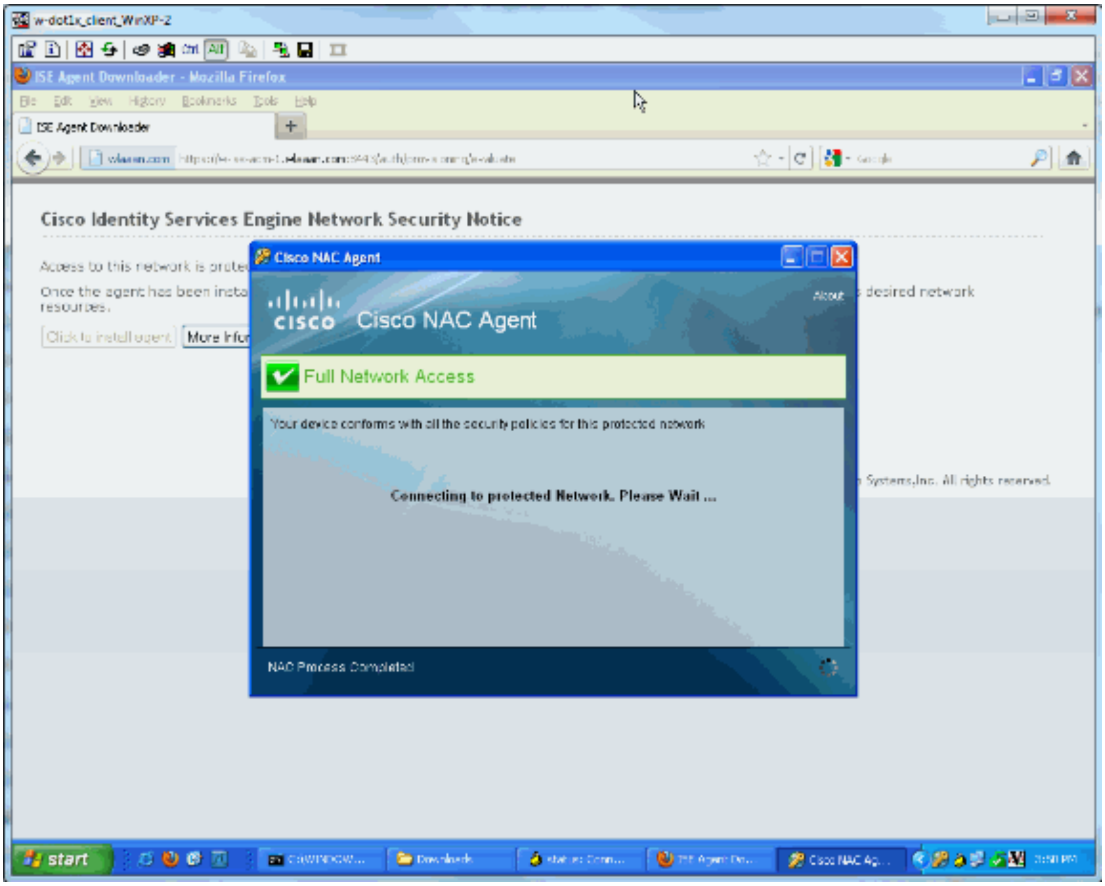
**And from the iPEP:**

```
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
```

**Once the agent is downloaded and installed:**

The agent should automatically detect the ISE and runs the posture assessment (assuming you have the posture rules defined already, which is another subject). In this example, the posture is successful, and this appears:



Cisco Identity Services Engine Network Security Notice

Access to this network is prote

Once the agent has been insta ... desired network resources.

Click to install agent More Infor

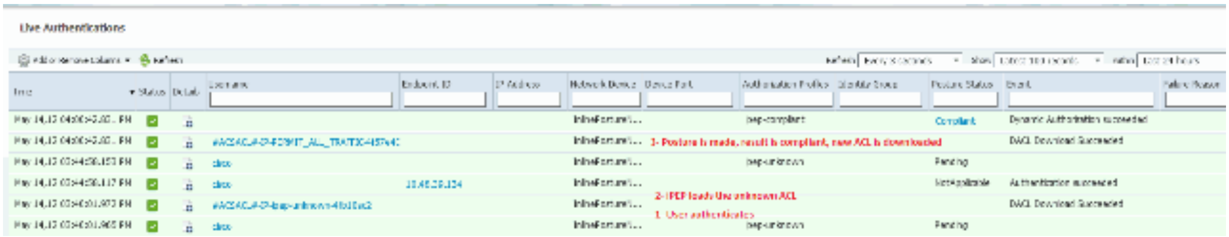
Full Network Access

Your device conforms with all the security policies for this protected network

Connecting to protected Network. Please Wait ...

NAC Process Completed

Systems,Inc. All rights reserved.



| Time | Status | Details | Username | Endpoint ID | IP Address | Network Device | Device Port | Authorization Profiles | Identity Group | Posture Status | Event | Failure Reason |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| May 14,12 04:00:03.0.. PM | ✓ | 🗎 | | | | InlinePosture#... | | pep-compliant | | Compliant | Dynamic Authorization succeeded | |
| May 14,12 04:00:03.0.. PM | ✓ | 🗎 | #ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e40 | | | InlinePosture#... | | | | | DACL Download Succeeded | |
| May 14,12 03:54:58.153 PM | ✓ | 🗎 | cisco | | | InlinePosture#... | | pep-unknown | | Pending | | |
| May 14,12 03:54:58.117 PM | ✓ | 🗎 | cisco | 10.48.28.124 | | InlinePosture#... | | | | NotApplicable | Authentication succeeded | |
| May 14,12 03:50:01.973 PM | ✓ | 🗎 | #ACSACL#-IP-ipep-unknown-4fb10ac2 | | | InlinePosture#... | | | | | DACL Download Succeeded | |
| May 14,12 03:50:01.965 PM | ✓ | 🗎 | cisco | | | InlinePosture#... | | pep-unknown | | Pending | | |

3- Posture is made, result is compliant, new ACL is downloaded

2- IPEP loads the unknown ACL

1- User authenticates

**Note:** There are two authentications in the screenshot above. However, because the iPEP box caches the ACLs, it is not downloaded every time.

**On the 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#
```

## Related Information

- **Technical Support & Documentation − Cisco Systems**