# ASA versie 9.2.1 VPN-houding met ISEconfiguratievoorbeeld

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram en verkeersstroom **Configuraties** ASA ISE Periodieke herbeoordeling Verifiëren Problemen oplossen Debugs op de ISE Debug-informatie op de ASA Debugs voor de Agent NAC Agent-poortfout Gerelateerde informatie

## Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) versie 9.2.1 moet configureren om VPN-gebruikers tegen de Cisco Identity Services Engine (ISE) te positioneren zonder dat ze een Inline Positie Node (IPN) nodig hebben.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA CLI-configuratie en Secure Socket Layer (SSL) VPN-configuratie
- Basiskennis van de configuratie van VPN voor externe toegang op de ASA
- Basiskennis van ISE en posterijen

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco ASA-softwareversies 9.2.1 en hoger
- Microsoft Windows versie 7 met Cisco AnyConnect Secure Mobility Client versie 3.1
- Cisco ISE-versie 1.2 met Patch 5 of hoger

## Achtergrondinformatie

Cisco ASA versie 9.2.1 ondersteunt RADIUS-wijziging van autorisatie (CoA) (RFC 5176). Dit maakt het mogelijk VPN-gebruikers tegen Cisco ISE te positioneren zonder dat ze een IPN nodig hebben. Nadat een VPN-gebruiker zich heeft aangemeld, leidt de ASA het webverkeer naar de ISE om, waar de gebruiker is voorzien van een Network Admission Control (NAC) Agent of Web Agent. De agent voert specifieke controles uit op de gebruikersmachine om de naleving ervan te bepalen aan de hand van een geconfigureerde reeks postuur regels, zoals het besturingssysteem, patches, AntiVirus, Service, Application of Register-regels.

De resultaten van de posterisatievalidering worden vervolgens naar de ISE gestuurd. Als de machine als klacht wordt beschouwd, dan kan de ISE een RADIUS CoA naar de ASA sturen met de nieuwe reeks vergunningsbeleid. Na een succesvolle posterievalidatie en CoA krijgt de gebruiker toegang tot de interne bronnen.

## Configureren

Netwerkdiagram en verkeersstroom



Hier is de verkeersstroom, zoals wordt geïllustreerd in het netwerkdiagram:

- 1. De externe gebruiker gebruikt Cisco AnyConnect voor VPN-toegang tot de ASA.
- 2. ASA stuurt een RADIUS-toegangsaanvraag voor die gebruiker naar de ISE.
- 3. Dat verzoek raakt het beleid genaamd **ASA92-postuur** op de ISE. Hierdoor wordt het **ASA92postieve** autorisatieprofiel geretourneerd. De ISE stuurt een RADIUS access-acceptatie met twee Cisco Attribute-Value-paren:

**url-redirect-acl=redirect** - dit is de naam van de Toegangscontrolelijst (ACL) die lokaal op ASA wordt bepaald, die beslist welk verkeer moet worden omgeleid.

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp - dit is de URL waarnaar de externe gebruiker moet worden doorgestuurd.Tip: de Domain Name System (DNS)-servers die aan de VPN-clients zijn toegewezen, moeten de FQDN-naam (FFully Qualified Domain Name) kunnen oplossen die in de doorverwijzing-URL wordt teruggestuurd. Als de VPN-filters zijn geconfigureerd om de toegang op tunnelgroepsniveau te beperken, zorg er dan voor dat de clientpool toegang heeft tot de ISE-server op de geconfigureerde poort (TCP 8443 in dit voorbeeld).

4. ASA verzendt een RADIUS-accounting-aanvangspakket en ontvangt een antwoord. Dit is nodig om alle details met betrekking tot de sessie naar de ISE te kunnen sturen. Deze details omvatten Session\_id, extern IP-adres van de VPN-client en het IP-adres van de ASA. De ISE gebruikt de sessie\_id om die sessie te identificeren. ASA stuurt ook periodieke tussentijdse accountinformatie, waarbij het belangrijkste kenmerk het framed-IP-adres met het IP is dat door de ASA aan de client is toegewezen (10.10.10.10 in dit voorbeeld).

- 5. Wanneer het verkeer van de VPN-gebruiker overeenkomt met de lokaal gedefinieerde ACL (omleiden), wordt het omgeleid naar **https://ise2.test-cisco.com:8443**. Afhankelijk van de configuratie, de ISE-bepalingen van de NAC Agent of de Web Agent.
- 6. Nadat de agent op de clientmachine is geïnstalleerd, worden automatisch specifieke controles uitgevoerd. In dit voorbeeld wordt gezocht naar het bestand c:\test.txt. Het stuurt ook een posterieverslag naar de ISE, die meerdere uitwisselingen kan omvatten met het gebruik van SWISS protocol en poorten TCP/UDP 8905 om toegang te krijgen tot de ISE.
- 7. Wanneer de ISE het posteringsrapport van de agent ontvangt, verwerkt zij de autorisatieregels opnieuw. Ditmaal is het resultaat van de postuur bekend en er wordt een andere regel geraakt. Er wordt een RADIUS CoA-pakket verzonden:

Als de gebruiker compatibel is, wordt een Downloadbare ACL (DACL)-naam die volledige toegang toestaat verzonden (AuthZ-regel ASA92-conform).

Als de gebruiker niet-compatibel is, wordt een DACL-naam die beperkte toegang toestaat verzonden (AuthZ-regel ASA92-niet-compatibel).**Opmerking**: de RADIUS CoA wordt altijd bevestigd; dat wil zeggen, de ASA stuurt een antwoord naar de ISE om te bevestigen.

- 8. ASA verwijdert de omleiding. Als de DACL's niet zijn gecacheed, moet het een Accessrequest verzenden om ze van de ISE te downloaden. De specifieke DACL is gekoppeld aan de VPN-sessie.
- 9. De volgende keer dat de VPN-gebruiker probeert toegang te krijgen tot de webpagina, heeft deze toegang tot alle bronnen die zijn toegestaan door de DACL die op de ASA is geïnstalleerd.

Indien de gebruiker niet voldoet, wordt slechts beperkte toegang verleend. **Opmerking**: dit stroommodel verschilt van de meeste scenario's die RADIUS CoA gebruiken. Voor bekabelde/draadloze 802.1x-verificaties bevat RADIUS CoA geen kenmerken. Het activeert alleen de tweede verificatie waarbij alle eigenschappen, zoals DACL, zijn gekoppeld. Voor de ASA VPN-houding is er geen tweede verificatie. Alle eigenschappen worden teruggegeven in de RADIUS CoA. De VPN-sessie is actief en het is niet mogelijk om de meeste VPN-gebruikersinstellingen te wijzigen.

### Configuraties

Gebruik deze sectie om de ASA en de ISE te configureren.

#### ASA

Hier is de basis-ASA configuratie voor Cisco AnyConnect-toegang:

ip local pool **POOL 10.10.10.10.10.10.100** mask 255.255.255.0

```
security-level 0
ip address xxxx 255.255.25.0
Т
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.111.10 255.255.255.0
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
key cisco
webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable
```

Zorg voor ASA-integratie met de ISE-houding ervoor dat u:

- Configureer de AAA-server (Verificatie, autorisatie en accounting) voor dynamische autorisatie om CoA te accepteren.
- Configureer de accounting als een tunnelgroep om VPN-sessiedetails naar de ISE te sturen.
- Configureer de tussentijdse accounting die het aan de gebruiker toegewezen IP-adres verstuurt en update periodiek de sessiestatus op ISE
- Configureer de omleiding van ACL, die bepaalt of DNS en ISE-verkeer zijn toegestaan. Al het andere HTTP-verkeer wordt naar de ISE omgeleid voor postuur.
   Hier is het configuratievoorbeeld:

```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
aaa-server ISE protocol radius
authorize-only
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
key cisco
tunnel-group RA general-attributes
address-pool POOL
```

```
authentication-server-group ISE
accounting-server-group ISE
default-group-policy GP-SSL
```

#### ISE

Voltooi de volgende stappen om de ISE te configureren:

1. Navigeren naar **Beheer > Netwerkbronnen > Netwerkapparaten** en de ASA als netwerkapparaat toevoegen:

alada	
cisco Identity Services Engine	
🔆 System 🦉 Identity Management 📑 I	Network Resources 🛛 🛃 Web Portal Management 🛛 🔂 Feed Service
Network Devices Network Device Groups Ext	ternal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices	Network Devices List > New Network Device Network Devices * Name ASA Description * IP Address: 192.168.111.10 / 32 Model Name * Software Version * * Network Device Group Location All Locations * Device Type All Device Types * Set To Default Set To Default Set To Default Set To Default
	Enable Authentication Settings Protocol RADIUS
	* Shared Secret Show

2. Navigeer naar **Beleid > Resultaten > Autorisatie > Downloadbare ACL** en configureer de DACL zodat deze volledige toegang mogelijk maakt. De standaard ACL-configuratie maakt al het IP-verkeer op de ISE mogelijk:

cisco Identity Services Engine	Administration   ▼
Authentication 🥥 Authorization 🔀 Dictionaries Conditions Results	Profiling 👩 Posture 😡 Client Provisioning 📄 Security Group Access
Results	Downloadable ACL List> PERMIT_ALL_TRAFFIC Downloadable ACL * Name PERMIT_ALL_TRAFFIC Description Allow all Traffic * DACL Content 1 permit ip any any 2 3 4 5 6 7 8 9 10 • Check DACL Syntax

- 3. Configureer een soortgelijke ACL die beperkte toegang biedt (voor niet-conforme gebruikers).
- 4. Navigeer naar Beleid > Resultaten > Autorisatie > Autorisatieprofielen en configureer het autorisatieprofiel ASA92-postuur, dat gebruikers omleidt naar postuur. Controleer het aanvinkvakje Web Redirection, selecteer Client Provisioning in de vervolgkeuzelijst en zorg ervoor dat redirect wordt weergegeven in het ACL-veld (dat ACL lokaal is gedefinieerd op de ASA):

cisco Identity Services Engine	Administration
Authentication Authorization Conditions Conditions Results	Nome Operations   Policy   Administration      Profiling Posture   Client Provisioning Security Group Access     Authorization Profiles > ASA92-posture   Authorization Profile   *Name   ASA92-posture   Description   *Access Type   ACCESS_ACCEPT   Service Template     Voice Domain Permission   Web Redirection (CWA, DRW, MDM, NSP, CPP)
	Client Provisioning (Posture)  ACL redirect Static IP/Host name

5. Configureer het autorisatieprofiel met de naam **ASA92-conform**, dat alleen DACL met de naam **PERMIT\_ALL\_TRAFFIC** moet retourneren die volledige toegang biedt voor de compatibele gebruikers:

cisco Identity Services Engine	Administration   ▼
Authentication Solutions Results	Profiling 💽 Posture 🔊 Client Provisioning 📄 Security Group Access
Results	Authorization Profiles > ASA92-compliant Authorization Profile *Name ASA92-compliant Description *Access Type ACCESS_ACCEPT  Service Template
<ul> <li>Posture</li> <li>Client Provisioning</li> <li>Security Group Access</li> </ul>	Common Tasks DACL Name PERMIT_ALL_TRAFFIC

- 6. Configureer een soortgelijk autorisatieprofiel met de naam **ASA92-nonconforme** controller, die de DACL met beperkte toegang moet retourneren (voor niet-conforme gebruikers).
- 7. Navigeer naar **Beleid > autorisatie** en configureer de autorisatieregels:

Maak een regel die volledige toegang verleent als de positieresultaten compatibel zijn. Het resultaat is het **autorisatiebeleid ASA92-conform**.

Maak een regel die beperkte toegang verleent als de positieresultaten niet conform zijn. Het resultaat is het **autorisatiebeleid ASA92-non-conforme**.

Zorg ervoor dat als geen van de vorige twee regels wordt geraakt, de standaardregel de **ASA92-houding** retourneert, die een omleiding op de ASA dwingt.

	ASA92 complaint	if	Session:PostureStatus EQUALS Compliant	then	ASA92-compliant
	ASA92 non complaint	if	Session:PostureStatus EQUALS NonCompliant	then	ASA92-noncompliant
<b>~</b>	ASA92 redirect	if	Radius:NAS-IP-Address EQUALS 192.168.111.10	then	ASA92-posture

 De standaardverificatieregels controleren de gebruikersnaam in het interne identiteitsarchief. Als dit moet worden gewijzigd (controle in de Active Directory (AD), bijvoorbeeld), navigeer dan naar Beleid > Verificatie en breng de wijziging aan:

cisco	Identity Services Engine		🟠 Home	Operations   🔻	Policy   🔻	Administration	¥	
🔔 Au	thentication 🧕 Authorizati	on 🔀 Profiling	Post	ture 👩 Clien	t Provisioning	🚊 Security	Group Access	🐥 Pol
Auther	ntication Policy							
Define the Policy Typ	e Authentication Policy by selection e O Simple I Rule-Base	ng the protocols that ad	ISE should us	e to communicate	with the netwo	ork devices, and th	e identity sources	s that it sh
	MAB	: If Wired_MAB ( Wireless_MA	DR NB			Allow Protocols	Default Network	Access
		Use Interna				Allow Protocole	Dofault Notwork	Accore
	Default	Wireless_80	2.1X Il Users			Allow Protocols .	Deladit Network	ALLESS
E	Default Rule (If no match)	: Allow Protocols :	Default Netwo	ork Access	a	nd use : Internal (	Users	

9. Navigeer naar Policy > Client Provisioning en configureer de provisioningregels. Dit zijn de regels die bepalen welk soort agent moet worden geleverd. In dit voorbeeld, bestaat slechts één eenvoudige regel, en de ISE selecteert de NAC Agent voor alle Microsoft Windowssystemen:

cisco Identity S	ervices Engine	🙆 Home	Operations   • Policy   • Ad	ministration   🔻	
🛓 Authentication	Authorization	🔀 Profiling 🛛 🕅 Postu	re 🔄 Client Provisioning	🚞 Security Group Access	🐥 Policy Elements
Client Provisionin Define the Client Provisi For Agent Configuration: For Native Supplicant Co	ng Policy oning Policy to determine version of agent, agent p nfiguration: wizard profile	e what users will receive upor profile, agent compliance mo e and/or wizard. Drag and dro	login and user session initiation: Jule, and/or agent customization pa p rules to change the order.	ickage.	
Rule N	lame	Identity Groups	Operating Systems	Other Conditions	Results
ASA92-p	osture	If Any and	Windows All and	Condition(s)	then NACAgent 4.9.0.1013

Wanneer de agenten niet op de ISE zijn, is het mogelijk om ze te downloaden:

CAgent 4.9 🗢 🔄		Done
Agent Configuration		
Agent:	NACAgent 4.9.0.1013	📀 🗹 Is Upgrade Mandatory
Profile:	Choose a Profile	Agents
Compliance Module:	Choose a Compliance Module	
Agent Customization Package:	Choose a Customization Package	⟨ <b>→</b> ▼ <b>■</b> •
Native Supplicant Co Config Wizard: Choose a Wizard Profile: Choose a	nfiguration Config Wizard 📀 Wizard Profile 📀	<ul> <li>Clear Control Download Resource</li> <li>NACAgent 4.9.0.52</li> <li>NACAgent 4.9.0.1009</li> <li>NACAgent 4.9.0.1013</li> </ul>
		WebAgent 4.9.0.24
		WebAgent 4.9.0.31
		WebAgent 4.9.0.1005

- 10. Indien nodig kunt u naar **Beheer > Systeem > Instellingen > Proxy** navigeren en de proxy voor de ISE configureren (voor toegang tot internet).
- 11. Configureer de houdingsregels, die de clientconfiguratie verifiëren. U kunt regels configureren die het volgende controleren:

bestanden - existentie, versie, datum

register - sleutel, waarde, bestaan

toepassing - procesnaam, actief, niet actief

service - servicenaam, actief, niet actief

**antivirus** - meer dan 100 leveranciers ondersteund, versie, wanneer definities worden bijgewerkt

**antispyware** - meer dan 100 leveranciers ondersteund, versie, wanneer definities worden bijgewerkt

samengestelde voorwaarde - mengsel van alle

aangepaste woordenboekvoorwaarden - gebruik van de meeste ISE-woordenboeken

12. In dit voorbeeld wordt alleen een eenvoudige bestaanscontrole van bestanden uitgevoerd. Als het bestand c:\test.txt op de clientmachine staat, is het compatibel en krijgt u volledige toegang. Navigeer naar Beleid > Voorwaarden > Bestandsvoorwaarden en configureer de bestandsvoorwaarde:

cisco Identity Services Engine	Administration ▼ Policy ▼ Administration ▼	
🛓 Authentication 🛛 🧔 Authorization 🔀	Profiling 💽 Posture 🔂 Client Provisioning 🚊 Security Group Access	🔒 Policy Elements
Dictionaries Conditions Results		
Posture	File Conditions List > file_condition File Condition * Name file_condition Description * File Path ABSOLUTE_PATH • * File Type FileExistence • * File Operator Exists • * Operating System Windows All Save Reset	

13. Navigeren naar Beleid > Resultaten > Houding > Vereisten en een vereiste creëren. Aan dit vereiste moet worden voldaan wanneer aan de vorige voorwaarde is voldaan. Als dit niet het geval is, worden herstelmaatregelen uitgevoerd. Er zijn vele soorten remediërende acties beschikbaar, maar in dit voorbeeld wordt de eenvoudigste gebruikt: een specifiek bericht wordt weergegeven.

cisco Identity Services Engine	☆ Home Operations   ▼ Policy   ▼	Administration   💌		L
Authentication S Authorization K Dictionaries Conditions Results	Profiling 🔀 Posture 🕞 Client Provisionin	g 📑 Security Group Access	Policy Elements	
Results	Requirements Name	Operating Systems	Conditions	Remediation Actions
Authentication     Authentication	file_requirement	for Windows All m	et if file_condition else	Message Text Only
Profiling     Postare     Remediation Actions	Any_Av_Installation_Win	for Windows All m	etif ANY_av_win_inst else	AnyA/DefRemediation/VI
Requirements     Glent Provisioning     Security Group Access	Any_AS_Installation_Win Any_AS_Definition_Win	for Windows All m	et if ANY_as_win_inst else	Message Text Only AnyASDefRemediationWi
	Any_AV_Installation_Mat	for Mac OSX m	et if ANY_av_mac_inst else	n Message Text Only
	Any_AV_Definition_Mac	for Mac OSX m	etif ANY_av_mac_def else	AnyAVDelRemediationMa c Message Text Only
	Any_AS_Definition_Mac	for Mac OSX m	etif ANY_as_mac_def else	Message Text Only

**Opmerking**: in een normaal scenario kan de actie Bestandsherstel worden gebruikt (de ISE biedt het downloadbare bestand).

14. Navigeer naar Beleid > Houding en gebruik de vereiste die u gecreëerd hebt in de vorige stap (genaamd file\_requirements) in de postuur regels. De enige posture regel vereist dat alle Microsoft Windows systemen voldoen aan de file\_requirements. Als aan deze eis wordt voldaan, is het station conform; als er niet aan wordt voldaan, is het station niet conform.

cisco Identity Services Engine	🟠 Home Operations	▼ Policy ▼ Administra	tion   <del>+</del>		
🛓 Authentication 👩 Authorization 📈	Profiling 🔀 Posture 🛃 🤅	Client Provisioning 🛛 🚊 Se	curity Group Access 🛛 🐴	Policy Elements	
Posture Policy Define the Posture Policy by configuring rules based of	n operating system and/or other cor	ditions.			
•					
Status Rule Name	Identity Groups	Operating Systems	Other Conditions	Requireme	ents
posture	If Any :	and Windows All		then file_requirer	ment

#### Periodieke herbeoordeling

Standaard is postuur een eenmalige gebeurtenis. Soms is het echter nodig om periodiek de gebruikersnaleving te controleren en de toegang tot de bronnen aan te passen op basis van de resultaten. Deze informatie wordt via het SWISS-protocol (NAC Agent) of gecodeerd binnen de toepassing (Web Agent).

Voltooi de volgende stappen om te controleren of de gebruiker voldoet aan de eisen:

1. Navigeren naar **Beheer > Instellingen > Houding > Herbeoordelingen** en globaal opnieuw beoordelen (per configuratie van identiteitsgroep):



2. Maak een postuur voorwaarde die aansluit bij alle herbeoordelingen:

cisco Identity Services Engine	Mome Operations   ▼ Policy   ▼ Administration   ▼	
🛓 Authentication 🛛 🧕 Authorization	🎸 Profiling 👩 Posture 🛛 Client Provisioning 🚊 Security Group Access 🛛 🔒 Policy Eler	ments
Dictionaries Conditions Results		
Posture	Dictionary Conditions List > New Dictionary Condition Dictionary Simple Condition * Name reassesment Description	
te Application Condition	* Attribute * Operator * Value	
Service Condition	Session:Agent-Request-Type 📀 Equals 👻 Periodic Reassessmen	ntį
Compound Condition	Submit Cancel	
AV Compound Condition		
AS Compound Condition		
📔 Dictionary Simple Condition		
E Dictionary Compound Condition		

3. Maak een soortgelijke voorwaarde die alleen overeenkomt met de eerste beoordelingen:

cisco Identity Services Engine	
🚨 Authentication 🛛 👩 Authorization	Profiling 👩 Posture 👦 Client Provisioning 📄 Security Group Access 🔥 Policy Elements
Dictionaries Conditions Results	
Posture    Posture     P	Dictionary Conditions List > New Dictionary Condition Dictionary Simple Condition *Name initial Description
Registry Condition     Application Condition	*Attribute *Operator *Value
Service Condition	Session:Agent-Request-Type 📀 Equals 👻 Initial
E Compound Condition	Submit Cancel
E AV Compound Condition	
AS Compound Condition	
E Dictionary Simple Condition	
E Dictionary Compound Condition	

Deze beide condities kunnen worden gebruikt in de postuur regels. De eerste regel komt alleen overeen met de eerste beoordelingen en de tweede met alle volgende beoordelingen:

cisco Identity Se	rvices Engine	1	🏠 Home Opera	ations   🔻	Policy   + Ac	dministration   💌		
🛓 Authentication	🧕 Authorization 🔀	Profiling	Posture	Clien	t Provisioning	🚊 Security Group Access	🐥 Policy Elements	
sture Policy								
fine the Posture Policy	by configuring rules based	on operatin	g system and/or oth	ier conditio	ins.			
Status Rule N	lame		Identity Groups		Operating System	other Conditions		Requirements
osture posture	_initial	r	Any	and	Windows All	initial	then	file_requirement
🗹 posture	_reassessment	ľ	Апу	and	Windows All	reassessment	then	file_requirement

## Verifiëren

Zorg ervoor dat deze stappen zoals beschreven zijn voltooid om te bevestigen dat uw configuratie

correct werkt:

- 1. De VPN-gebruiker maakt verbinding met de ASA.
- 2. De ASA verzendt een RADIUS-Verzoek en ontvangt een antwoord met de eigenschappen url-redirect en url-redirect-acl:



3. De ISE-logboeken geven aan dat de autorisatie overeenkomt met het postuur-profiel (de eerste logvermelding):

- <b>-</b>	ò	#ACSACL#-IP-P	ASA9-2		Compliant ise2
<b>1</b>	à	192.168.10.67	A5A9-2	ASA92-compliant	Compliant ise2
0	à	0 cisco 192.168.10.67			Compliant ise2
<b>1</b>	o l	cisco 192.168.10.67	ASA9-2	ASA92-posture User Iden	itity Gro Pending ise2

4. De ASA voegt een doorverwijzing toe aan de VPN-sessie:

```
aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10
```

 De status van de VPN-sessie op de ASA toont aan dat de houding vereist is en omleidt het HTTP-verkeer:

```
ASA# show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username
           : cisco
                                                : 9
                                    Index
                                    Public IP
Assigned IP : 10.10.10.10
                                                : 10.147.24.61
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
           : AnyConnect Essentials
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
            : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Hashing
Bytes Tx
            : 16077
                                    Bytes Rx
                                               : 19497
Pkts Tx : 43
                                                : 225
                                    Pkts Rx
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
Group Policy : GP-SSL
                                    Tunnel Group : RA
```

Login Time : 14:55:50 CET Mon Dec 23 2013

: 0h:01m:34s

Inactivity : 0h:00m:00s

Duration

VLAN Mapping : N/A VLAN : none Audt Sess ID : c0a8700a0000900052b840e6 Security Grp : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 9.1 Public IP : 10.147.24.61 Encryption : none Hashing : none TCP Src Port : 50025 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 779 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 9.2 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Hashing : SHA1 TCP Src Port : 50044 Auth Mode : userPassword Idle TO Left : 28 Minutes Encryption : RC4 Encapsulation: TLSv1.0 TCP Dst Port : 443 Idle Time Out: 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 172 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 9.3 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Encryption: AES128Hashing: SHA1Encapsulation: DTLSv1.0UDP Src Port: 63296UDP Dst Port : 443Auth Mode: userPasswordIdle Time Out: 30 MinutesIdle TO Left: 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5669 Bytes Rx : 18546 Pkts Tx : 35 Pkts Rx : 222 Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?
sessionId=c0a8700a0000900052b840e6&action=cpp
Redirect ACL : redirect

 De client die het HTTP-verkeer initieert dat overeenkomt met de omgeleide ACL, wordt omgeleid naar de ISE:

```
aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for 10.10.10.10
```

7. De client wordt omgeleid naar de ISE voor postuur:

🗲 🔒 https://ise2.test-cisco.com:0443/authA	CppSetup.action?session=c0a0700a0000600052b0366c&cs=Windows T (4) 🏫 🔻 C 📲 - AVC Secure Search 📃 👂	
CISCO Client Prov	visioning Portal	
Cisco Identity Ser Engine Network	rvices Determining prior Cisco Agent installation on device28 second(s Coordinate Cisco Agent installation on device28 second(s	s).
Notice	Do you want to Continue? The connection to this website is untrusted. Website: https://ise2.test-cisco.com:8443	
	Note: The certificate is not valid and cannot be used to verify the identity of this website. This application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute. Please contact the Publisher for more information. More information Continue Continue	

8. De NAC Agent is geïnstalleerd. Nadat de NAC Agent is geïnstalleerd, downloadt het de postuur regels via SWISS protocol en voert controles uit om naleving te bepalen. Het verslag van de standplaats wordt vervolgens naar de ISE gestuurd.



9. De ISE ontvangt het positierapport, herevalueert de autorisatieregels en (indien nodig) wijzigt de autorisatiestatus en stuurt een CvA. Dit kan worden geverifieerd in de **ise-psc.log**:

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
:::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
:::- Posture CoA is triggered for endpoint [null] with session
[c0a8700a0000900052b840e6]
```

10. De ISE verstuurt een RADIUS CoA die de **sessie\_id** en de DACL-naam bevat die volledige toegang mogelijk maakt:

No.	Source	Destination	Protocol Le	ngth Info						
	7 10.48.66.74	192.168.111.10	RADIUS	231 CoA-Request(43) (id=	11, l=189)					
;	8 192.168.111.10	10.48.66.74	RADIUS	62 CoA-ACK(44) (id=11,	l=20)					
4										
▶ Fi	rame 7: 231 bytes on w	wire (1848 bits), 2	31 bytes ca	ptured (1848 bits)						
▶ E1	thernet II, Src: Vmwa	re_c0:00:03 (00:50:	56:c0:00:03	), Dst: Vmware_e8:ef:25 (6	00:0c:29:e8:ef:25)					
▶ Ir	Internet Protocol Version 4, Src: 10.48.66.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)									
U:	ser Datagram Protocol,	, Src Port: 44354 (	44354), Dst	Port: mps-raft (1700)						
⇒ Rá	adius Protocol									
	Code: CoA-Request (43)									
	Packet identifier: 0xb (11)									
	Length: 189									
	Authenticator: d20817	c6ca828ce7db4ee54f	l5177b8d							
	[The response to this	; request is in fran	<u>ne 81</u>							
~	Attribute Value Pairs	i i								
	▷ AVP: l=6 t=NAS-IP	Address(4): 10.147.	24.61							
	▷ AVP: l=15 t=Callin	g-Station-Id(31): 1	92.168.10.6	7						
	▷ AVP: l=6 t=Event-T	imestamp(55): Dec 1	8, 2013 15:	32:10.00000000 CET						
	▶ AVP: l=18 t=Messag	e•Authenticator(80)	: 1ee29f1d8	3e5f3aa4934d60aa617ebeb						
	▼ AVP: l=75 t=Vendor	<ul> <li>Specific(26) v=cis</li> </ul>	coSystems(9	)						
	▹ VSA: l=69 t=Cisco	AVPair(1): ACS:Cis	coSecure-Det	fined-ACL=#ACSACL#-IP-PERM	IIT_ALL_TRAFFIC-51ef7db1					
	▼ AVP: l=49 t=Vendor	-Specific(26) v=cis	coSystems(9	)						
	▶ VSA: l=43 t=Cisco	AVPair(1): audit-se	ession-id=c	a8700a0000d00052b1b1bc						

Dit wordt weerspiegeld in de ISE-logboeken:

De eerste logboekingang is voor de aanvankelijke authentificatie die het houdingsprofiel (met omleiding) terugkeert.

De tweede logboekvermelding wordt ingevuld nadat het conforme SWISS-rapport is ontvangen.

Het derde logbestand wordt ingevuld wanneer de CoA wordt verzonden, samen met de bevestiging (beschreven als Dynamic Authorisation Succeeded).

De laatste logingang wordt gemaakt wanneer de ASA DACL downloadt.

. 🗹	O.	#ACSACL#-IP-P	ASA9-2		Compliant	ise2
- <u>-</u>	- Q	192.168.10.67	A5A9-2	ASA92-compliant	Compliant	ise2
	à	0 cisco 192.168.10.67			Compliant	ise2
<ul> <li>Image: Construction</li> </ul>	O.	cisco 192.168.10.67	ASA9-2	ASA92-posture Use	r Identity Gro Pending	ise2

11. Debugs op de ASA tonen aan dat de CoA wordt ontvangen en de redirect wordt verwijderd. ASA downloadt indien nodig DACL's:

AS/	\# F	Rece	eive	ed I	RAD_	_C07	A_RE	QUE	IST								
RAI	RADIUS packet decode (CoA-Request)																
Rad	Radius: Value (String) =																
41	43	53	3a	43	69	73	63	6f	53	65	63	75	72	65	2d		ACS:CiscoSecure-
44	65	66	69	6e	65	64	2d	41	43	4c	3d	23	41	43	53		Defined-ACL=#ACS
41	43	4c	23	2d	49	50	2d	50	45	52	4d	49	54	5f	41		ACL#-IP-PERMIT_A
4c	4c	5f	54	52	41	46	46	49	43	2d	35	31	65	66	37		LL_TRAFFIC-51ef7
64	62	31															db1

Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6

Got AV-Pair with value ACS:CiscoSecure-Defined-ACL= #ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-51ef7db1

aaa\_url\_redirect: Deleted url redirect for 10.10.10.10 12. Na de VPN-sessie heeft Cisco de DACL (volledige toegang) toegepast voor de gebruiker:

#### ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed Username : cisco Index : 9 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Essentials License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 94042 Bytes Rx : 37079 : 169 Pkts Tx : 382 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GP-SSL Tunnel Group : RA Login Time : 14:55:50 CET Mon Dec 23 2013 Duration : 0h:05m:30s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : c0a8700a0000900052b840e6 Security Grp : 0 AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID. ...Public IP: 10.147.24.61Encryption: none Tunnel ID : 9.1 Hashing : none TCP Src Port : 50025 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes Client OS : win Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 779 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: : 9.2 Tunnel ID Assigned IP : 10.10.10.10Public IP : 10.147.24.61Encryption : RC4Hashing : SHA1Encapsulation: TLSv1.0TCP Src Port : 50044TCP Dst Port : 443Auth Mode : userPassword Auth Mode : userPassword TCP Dst Port : 443 Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 172 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-51ef7db1 DTLS-Tunnel: Tunnel ID : 9.3 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61

Encryption :	AES128	Hashing	:	SHA1
Encapsulation:	DTLSv1.0	UDP Src Port	:	63296
UDP Dst Port :	443	Auth Mode	:	userPassword
Idle Time Out:	30 Minutes	Idle TO Left	:	29 Minutes
Client OS :	Windows			
Client Type :	DTLS VPN Client			
Client Ver :	Cisco AnyConnect VPN Ag	gent for Windo	ws	3.1.02040
Bytes Tx :	83634	Bytes Rx	:	36128
Pkts Tx :	161	Pkts Rx	:	379
Pkts Tx Drop :	0	Pkts Rx Drop	:	0
Filter Name :	#ACSACL#-IP-PERMIT_ALL_	TRAFFIC-51ef7	db	<b>1</b>

**Opmerking**: de ASA verwijdert altijd de omleidingsregels, zelfs wanneer de CoA geen DACL heeft aangesloten.

## Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

### Debugs op de ISE

Blader naar **Beheer > Vastlegging > Configuratie debug log** om debugs in te schakelen. Cisco raadt u aan tijdelijke debugs in te schakelen voor:

- ZWITSERSE
- Non-stop doorsturen (NSF)
- NSF-sessie
- Voorziening
- houding

Voer deze opdracht in de CLI in om de debugs-bestanden te bekijken:

ise2/admin# show logging application ise-psc.log tail count 100 Ga naar Operations > Rapporten > ISE-rapporten > Endpoints en gebruikers > Posture Details Assessment om de posture rapporten te bekijken:

alada									and 1 representation	I Legent   Peribeck D
CISCO Identity Services Engine	🔔 Home Oper	ntions   +	Policy	• Admini	stration   +					Satup Ar
😰 Authentications 📑 Reports 🔯 Dec	🔮 Authentications 📑 Reports 🔯 Endpoint/Protection Genetice 💊 Troubleshoot									
Report Selector	Posture Detail Asses	sment								🔶 Favorite 🛛 🚇 Export 🛛 💾
Favorites										Generated at 2013-12-
ISE Reports	From 12/23/2013 12:00:0	0 AM to 12	23/29/13	32:56:58 PM						Page << 1 >> Page 167
<ul> <li>Auth Services Stelue</li> </ul>	Logged At	51stus	Detail	PRA.	Identity	Endpoint ID	P Address	Endpoint 05	Agent	Metoage
6 reports	2013-12-23 15:21:34.9	-	.0	continue	cisco	08:08:27:CD/E8:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RAE A	Received a posture report from an endpoint
Diployment Status     Trivports	2013-12-23 15:08:58.3		.a	continue	cisco	08/08/27/CD/68/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
+ Endpoints and Users	2013-12-23 14:59:34.3	-	.0	continue	cisco	08:01:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO NAC A	Received a posture report from an endpoint
Client Provisianing	2013-12-23 14:55:28.6	•	.0	N/A	cisco	08-08-27-CD-E8-A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
Current Active Sessions	2013-12-23 14:44:45.0	۰	.0	N/A	cisco	08:08:27:CD/E8:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO NAC A	Received a posture report from an endpoint
Guest Activity	2013-12-23 13:34:30.3	۰	.0	NA	cisco	08/08/27/7F/SF/6	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A	Received a posture report from an endpoint
Guest Accounting	2013-12-23 13:27:10.3	۰	.0	NA	cisco	08:00:27:79:57:6	10.147.24.92	Windows 7 Ultimate 64-bit	CISCO NAC A	Received a posture report from an endpoint
discacturing										
Guest Spotsor Happing										
Guest Sponsor Summary										
Endpoint Protection Service Audit										
Mobile Device Hanagement										
Posture Detail Assessment Posture Totay *										

Op de pagina Posture More Detail Assessment is er een beleidsnaam met een vereiste naam die wordt weergegeven, samen met de resultaten:

Posture More Detail As	sessment						
Time Range: From 12/23/2 Generated At: 2013-12-23 1	From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM 2013-12-23 15:57:31 248						
Client Details							
Username:	cisco						
Mac Address:	08:00:2	27:CD:E8:A2					
IP address:	10.147	.24.92					
Session ID:	c0a870	0a0000b00052b	846c0				
Client Operating System	: Window	/s 7 Enterprise 64	l-bit				
Client NAC Agent:	Cisc o N	AC Agent for Win	dows 4.9.0	0.1013			
PRA Enforcement:	1						
CoA:	Receive	ed a posture repor	t from an	endpoint			
PRA Grace Time:							
PRA Interval:	240						
PRA Action:	continu	ie					
User Agreement Status:	NotEna	bled					
System Name:	MGARC	ARZ-WS01					
System Domain:	cisco.c	om					
System User:	mgarca	arz					
User Domain:	CI SC O						
AV Installed:	McAfee	VirusScan Enterp	orise;8.8.0	.975;7227;10	/13/2013;McAfee	AV,Cisco Security Agent;6.0.2.130;;;CiscoAV	1
AS Installed:	Window	/s Defender;6.1.7	600.1638	5;1.95.191.0;	11/19/2010;Micro	osoftAS	
Posture Report							
Posture Status:	Compli	ant					
Logged At:	2013-1	2-23 15:21:34.90	)2				
			-				
Posture Policy Details							
Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions	
posture_initial	file_require	Mandatory		file_conditio	n		

### Debug-informatie op de ASA

U kunt deze debugs op de ASA inschakelen:

- debug aaa url-redirect
- debug aaa-autorisatie
- debug radius dynamisch-autorisatie
- debug radius decode
- debug radius gebruiker cisco

### Debugs voor de Agent

Voor de NAC Agent is het mogelijk de debugs te verzamelen met de Cisco Log Packager, die gestart is vanuit de GUI of met de CLI: **CAAgentLogPackager.app**.

🛨 Cisco Log Pa	ckager v	1.7.0.11									
cisco.	<ul> <li>Cisco Log Packager</li> </ul>										
	Cisco Log Packager collects information for product support requests. The information is stored in a ZIP archive that can be protected by a password.										
Protect dat	a with fo	blowing password:									
Collect Da	ta	Show Log	Locate Report File	Cancel	Exit						

Tip: u kunt de resultaten decoderen met de TAC-tool (Technical Assistance Center).

Om de logbestanden voor de Web Agent op te halen, navigeer naar deze locaties:

- C: > Document en instellingen > <user> > Lokale instellingen > Temperatuur > webagent.log (gedecodeerd met het TAC-gereedschap)
- C: > Document en instellingen > <user> > Lokale instellingen > Temperatuur > webagentsetup.log

**Opmerking**: Als de logbestanden niet op deze locaties staan, moet u de variabele **TEMP Environment** controleren.

### NAC Agent-poortfout

Als de houding mislukt, krijgt de gebruiker de reden:

cisco Client	Provisioning Portal	
Information	Cisco NAC Agent	About
	Temporary Network Access	00:03:30 left
	Security Compliance Summary Scan Result Requirement Name Mandatory file_requirement Hide Details	
	System Check Complete	

De gebruiker kan dan herstelacties uitvoeren als deze zijn geconfigureerd:



## Gerelateerde informatie

- Gebruikersautorisatie voor een externe server voor security applicatie configureren
- Configuratiehandleiding voor Cisco ASA Series VPN CLI, 9.1
- <u>Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2</u>
- Technische ondersteuning en documentatie Cisco Systems

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.