ASA versie 9.2.1 VPN-houding met ISE-configuratievoorbeeld

Inhoud

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

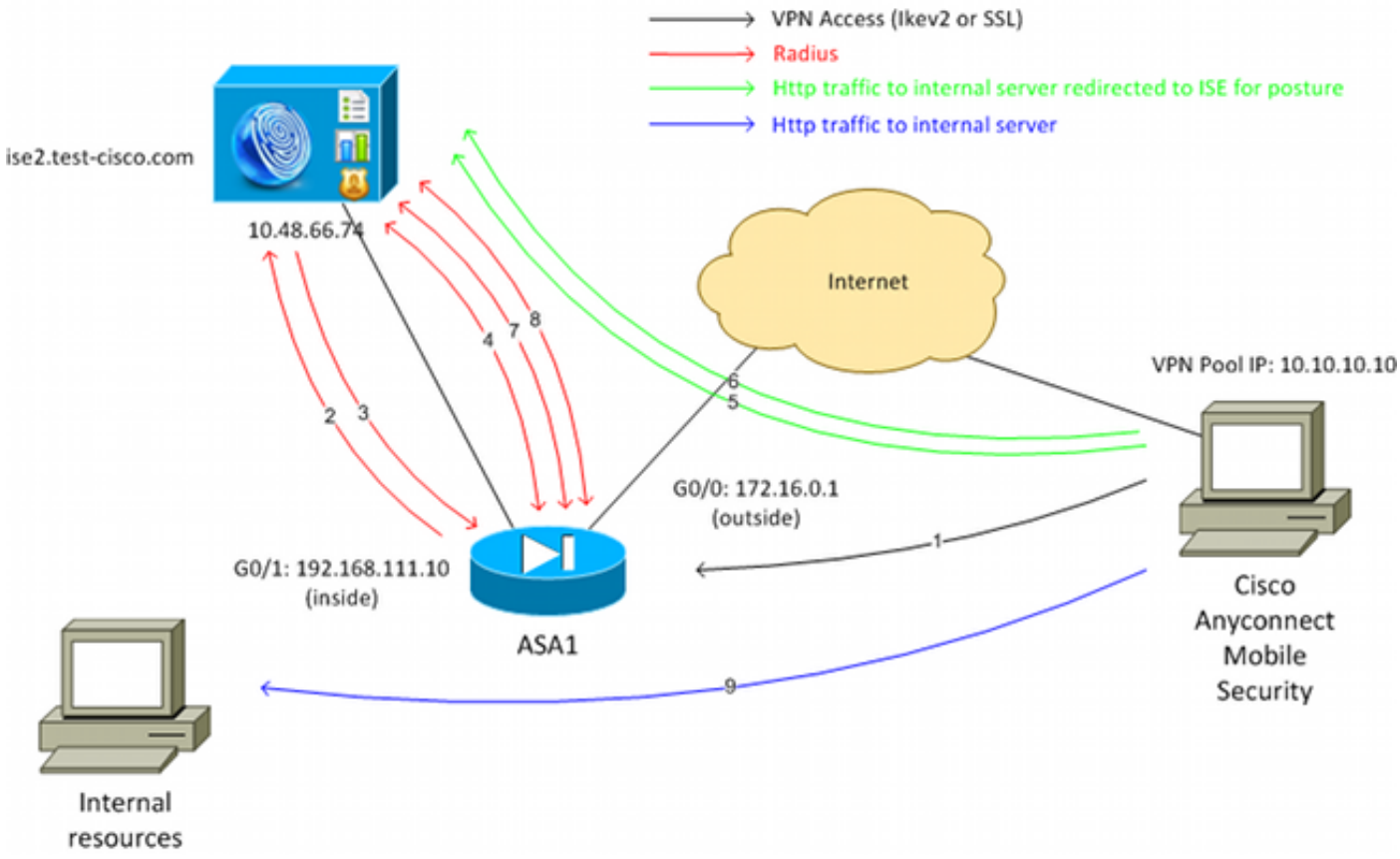
Achtergrondinformatie

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 **ASA92-postieve** 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 Access-request 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 10.10.10.10-10.10.10.100 mask 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
```

```
 security-level 0
 ip address xxxx 255.255.255.0
!
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:

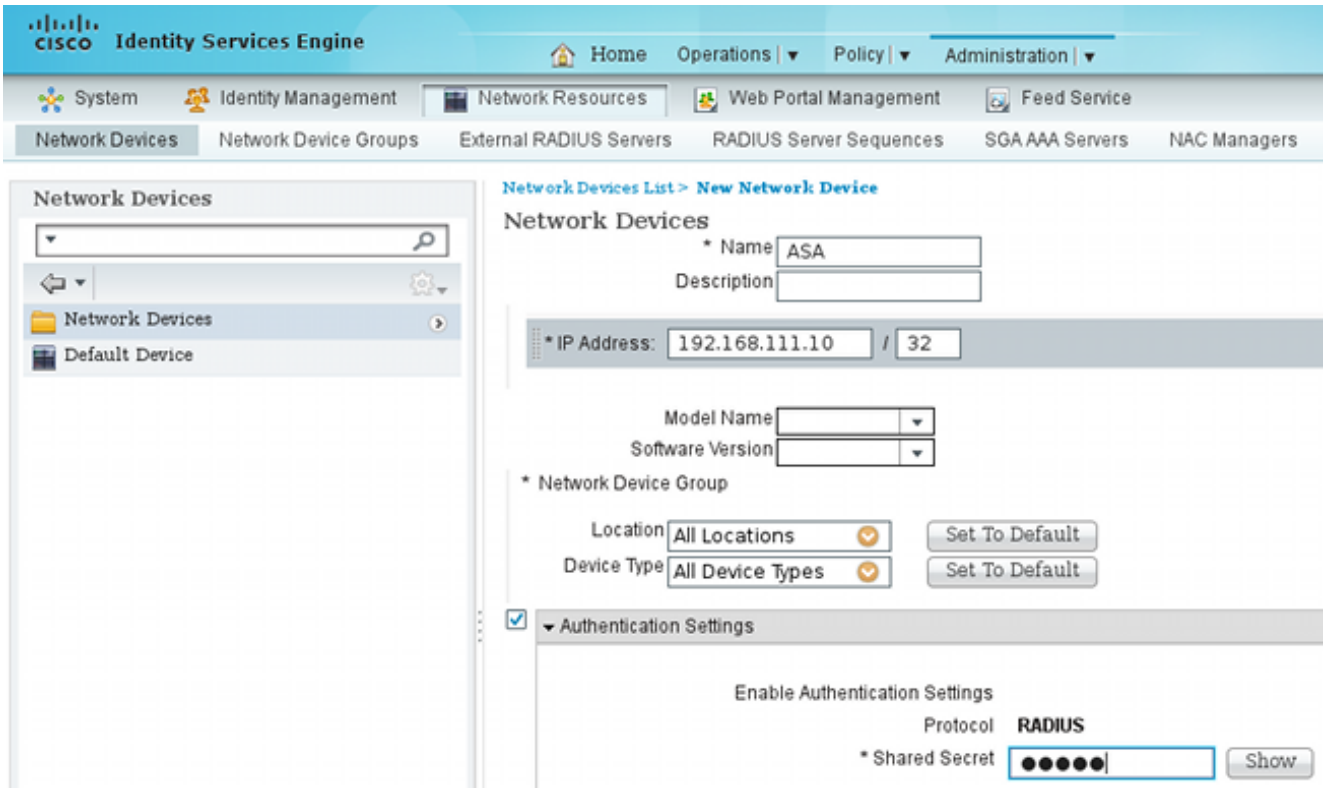
```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

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
```

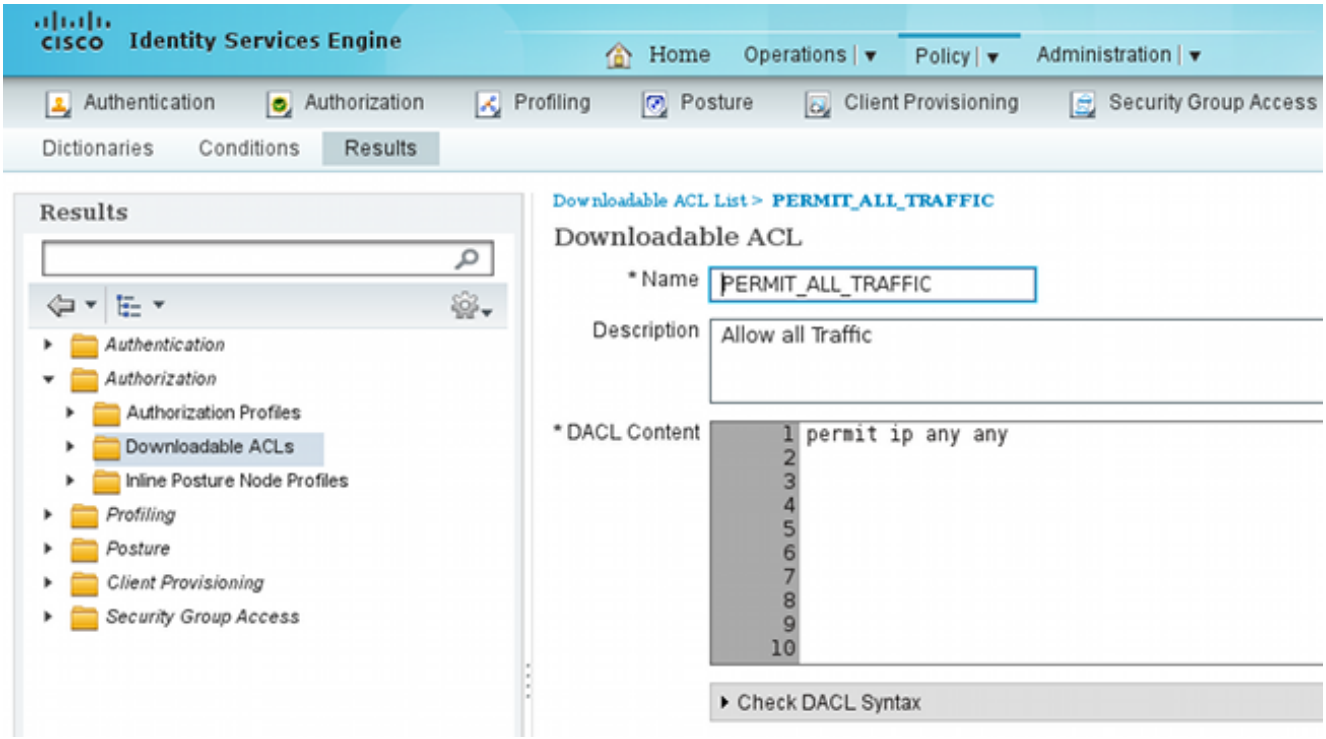
ISE

Voltooi de volgende stappen om de ISE te configureren:

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

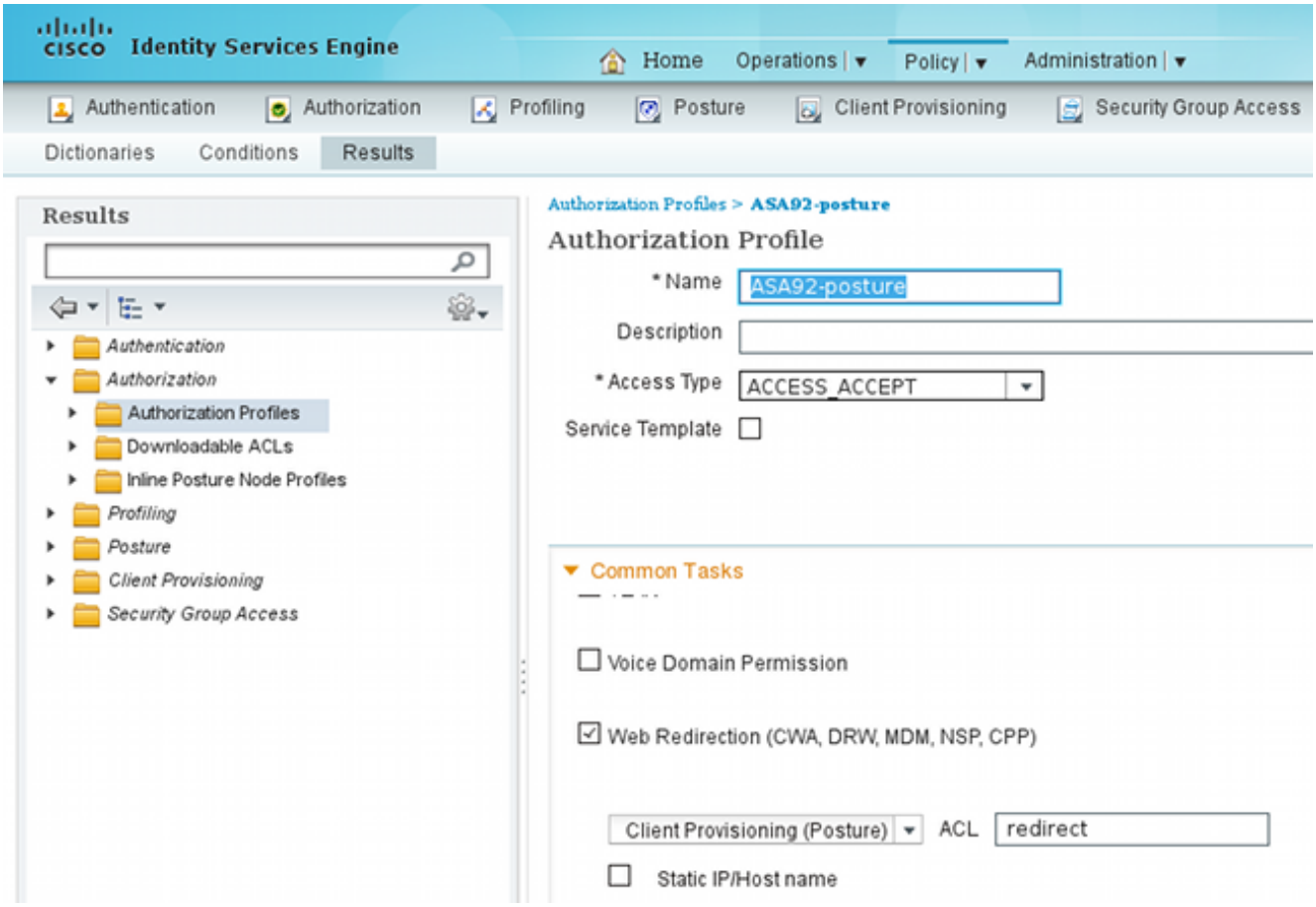


2. Navigeer naar **Beleid > Resultaten > Autorisatie > Downloadbare ACL** en configureer de DACL zodat deze volledige toegang mogelijk maakt. De standaard ACL-configuratie maakt al het IP-verkeer op de ISE mogelijk:

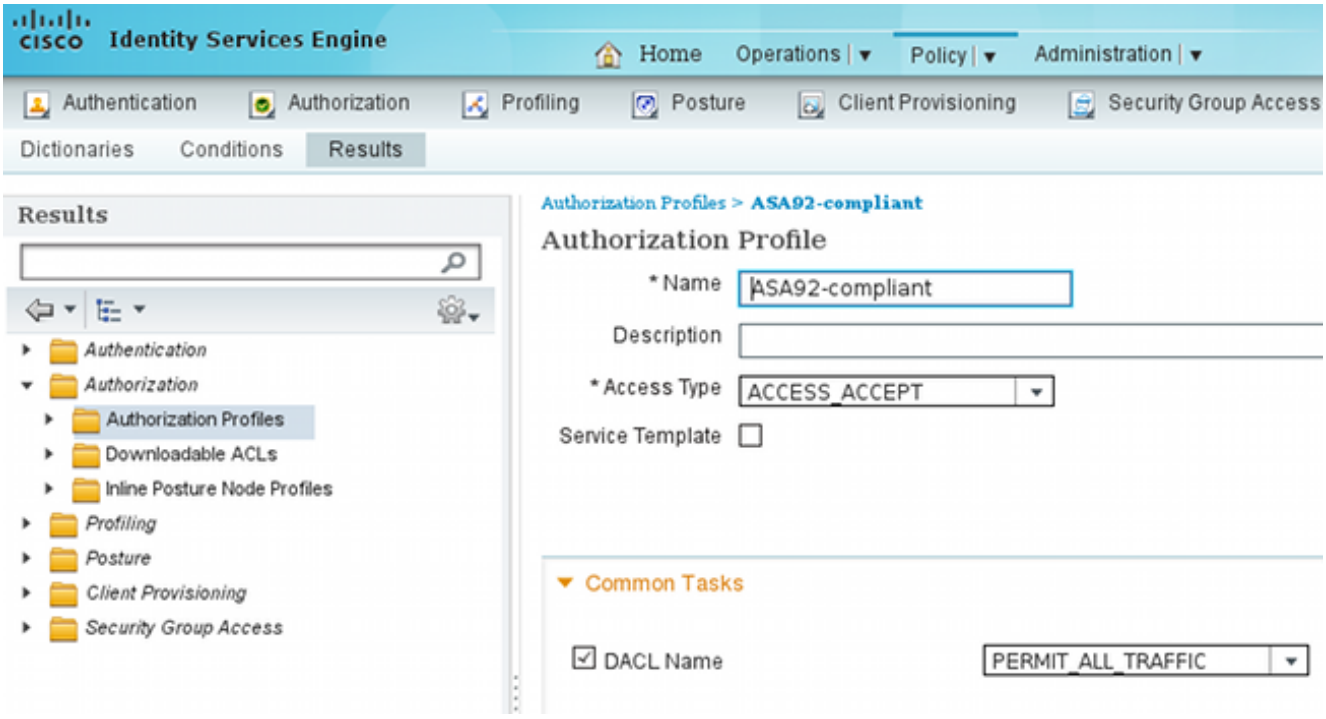


3. Configureer een soortgelijke ACL die beperkte toegang biedt (voor niet-conforme gebruikers).

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):



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:



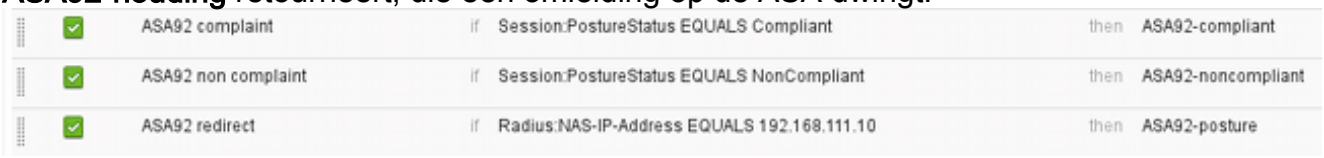
6. Configureer een soortgelijk autorisatieprofiel met de naam **ASA92-nonconforme** controller, die de DACL met beperkte toegang moet retourneren (voor niet-conforme gebruikers).

7. Navigeer naar **Beleid > autorisatie** en configureer de autorisatieregels:

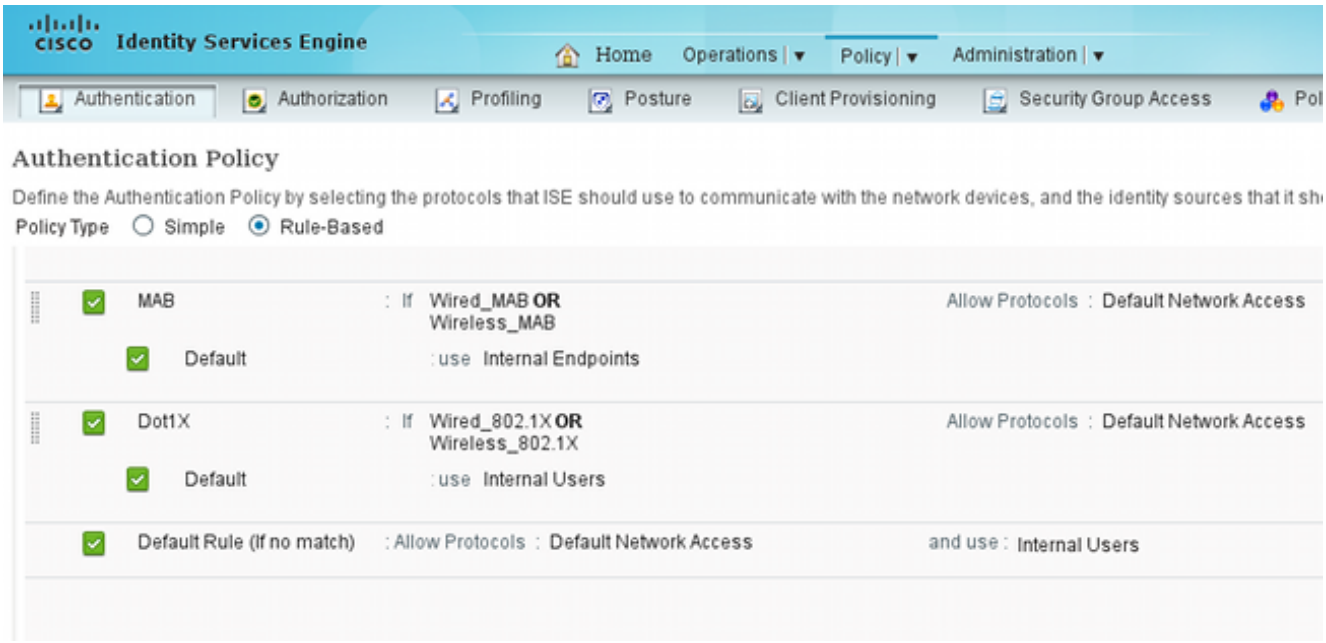
Maak een regel die volledige toegang verleent als de positieresultaten compatibel zijn. Het resultaat is het **autorisatiebeleid ASA92-conform**.

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

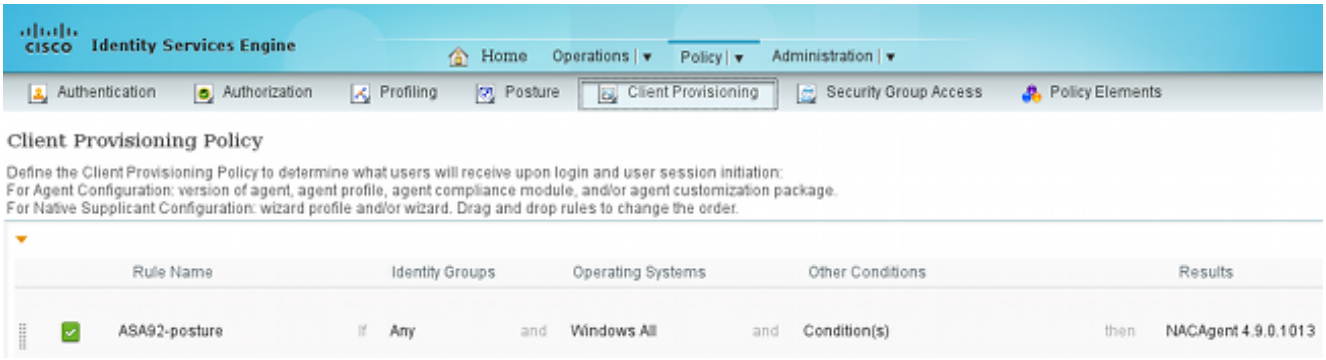
Zorg ervoor dat als geen van de vorige twee regels wordt geraakt, de standaardregel de **ASA92-houding** retourneert, die een omleiding op de ASA dwingt.



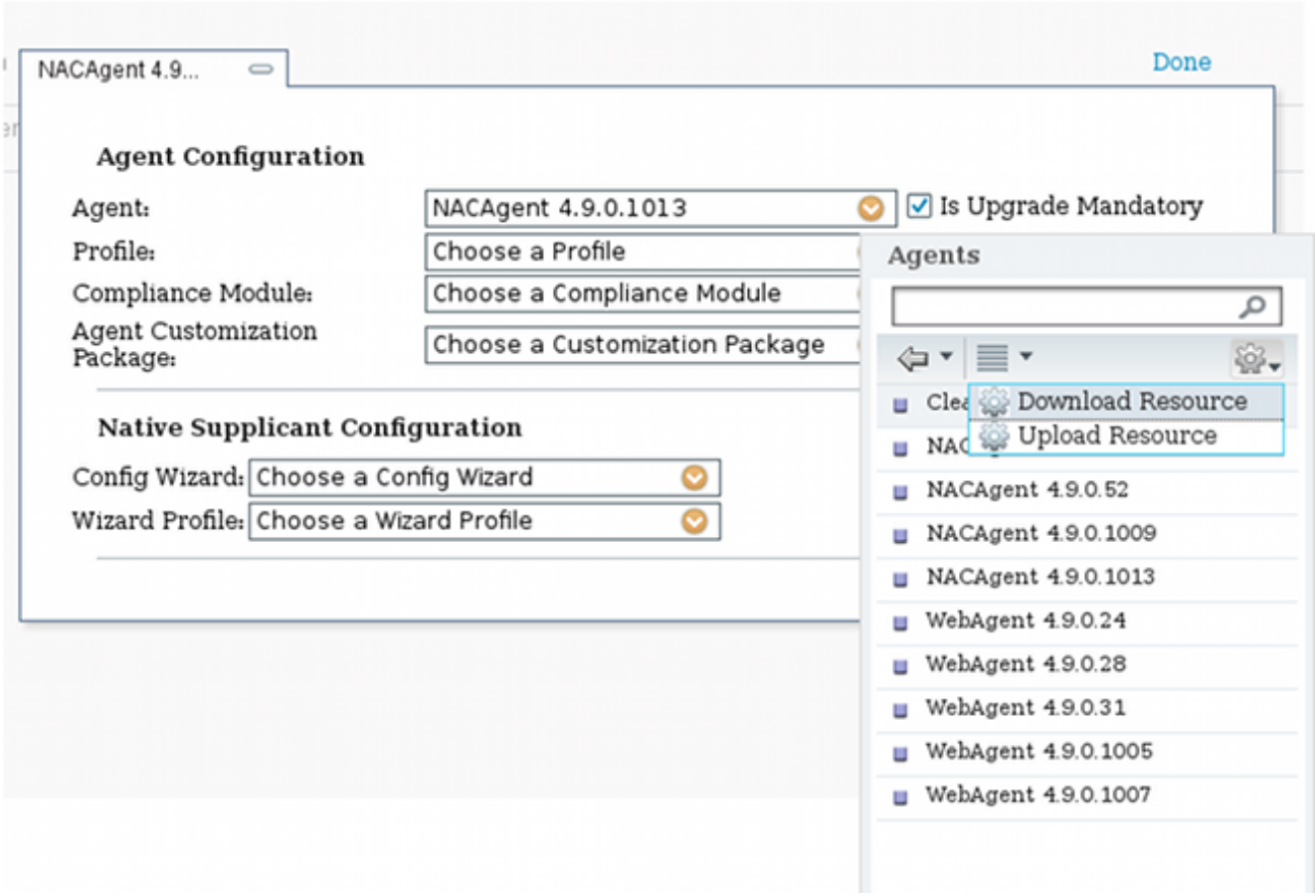
8. De standaardverificatieregels controleren de gebruikersnaam in het interne identiteitsarchief. Als dit moet worden gewijzigd (controle in de Active Directory (AD), bijvoorbeeld), navigeer dan naar **Beleid > Verificatie** en breng de wijziging aan:



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 Windows-systemen:



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



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

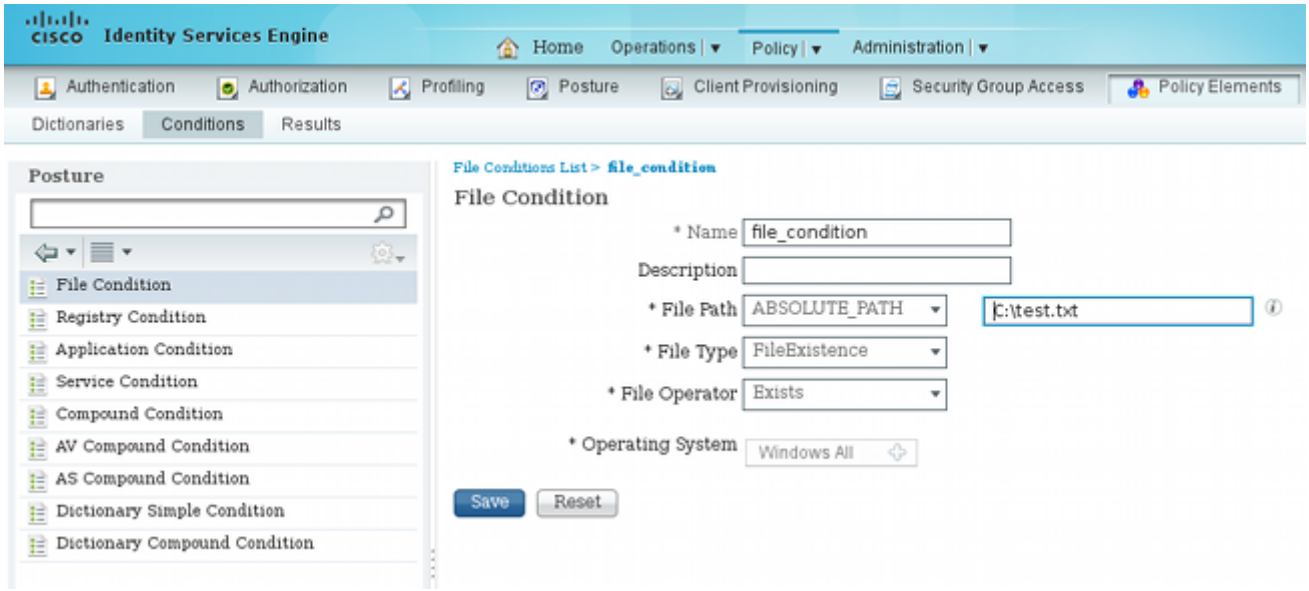
    antivirus - meer dan 100 leveranciers ondersteund, versie, wanneer definities worden bijgewerkt

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

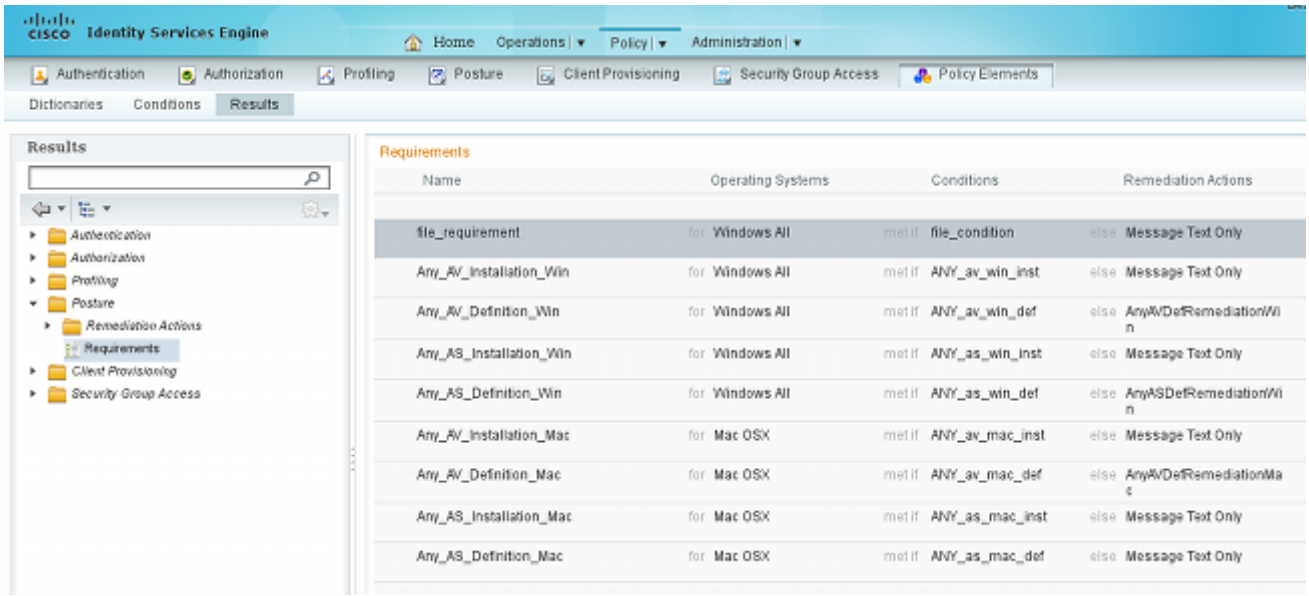
    samengestelde voorwaarde - mengsel van alle

    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:

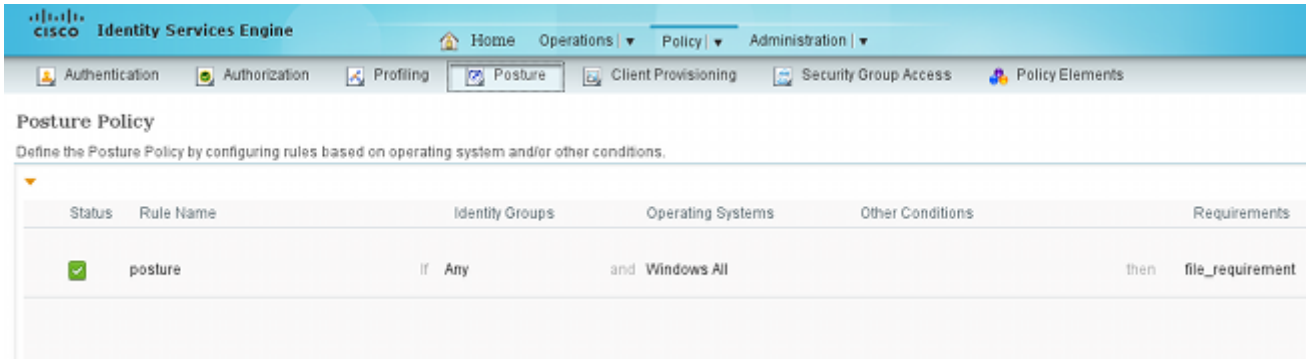


13. Navigeren naar **Beleid > Resultaten > Houding > Vereisten** en een vereiste creëren. Aan dit vereiste moet worden voldaan wanneer aan de vorige voorwaarde is voldaan. Als dit niet het geval is, worden herstelmaatregelen uitgevoerd. Er zijn vele soorten remediërende acties beschikbaar, maar in dit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



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.

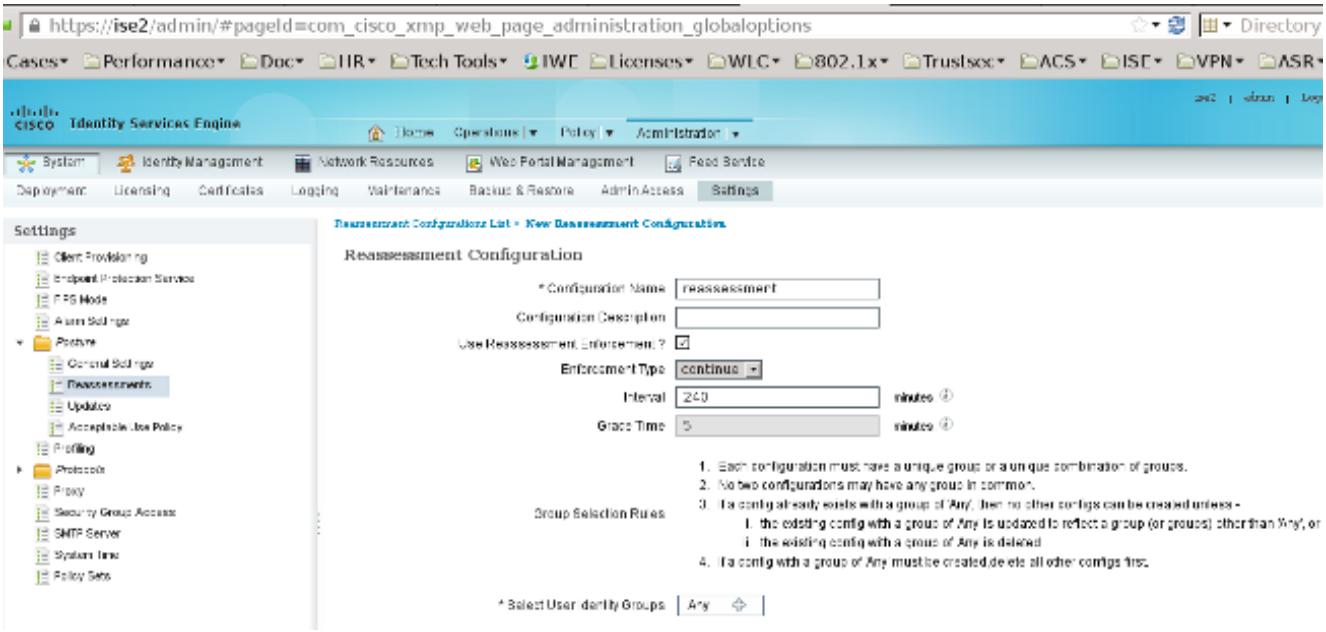


Periodieke herbeoordeling

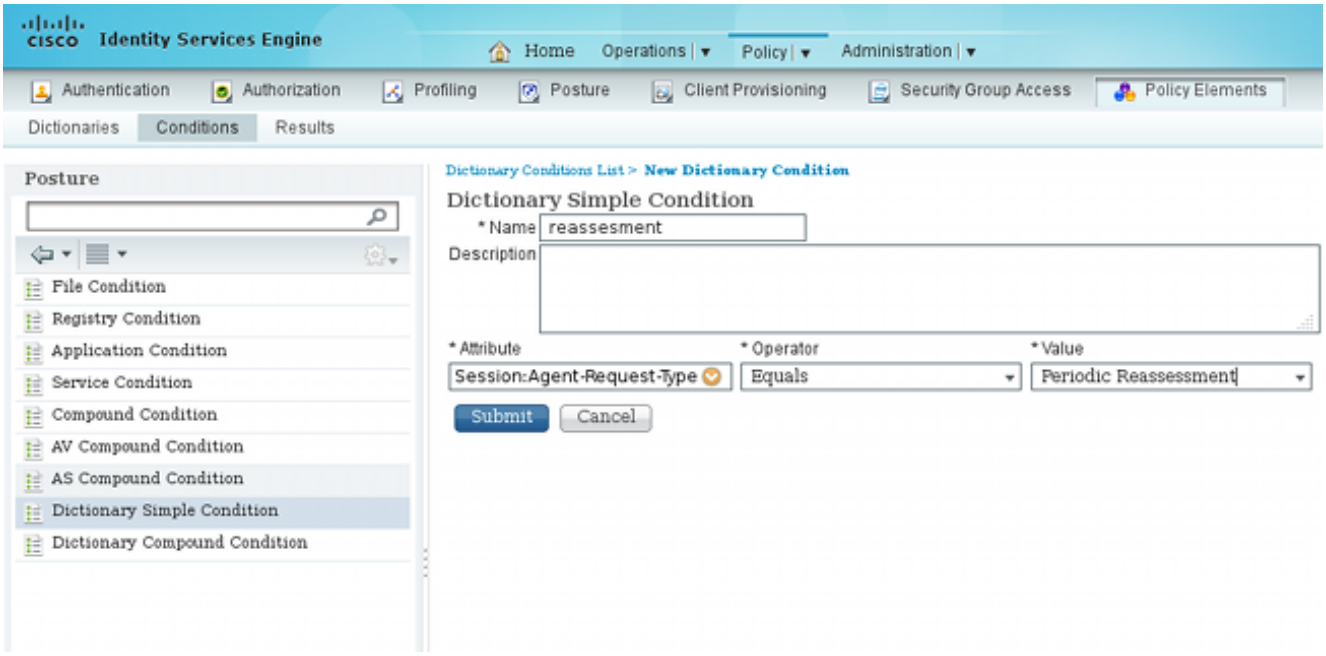
Standaard is postuur een eenmalige gebeurtenis. Soms is het echter nodig om periodiek de gebruikersnaleving te controleren en de toegang tot de bronnen aan te passen op basis van de resultaten. Deze informatie wordt via het SWISS-protocol (NAC Agent) of gecodeerd binnen de toepassing (Web Agent).

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

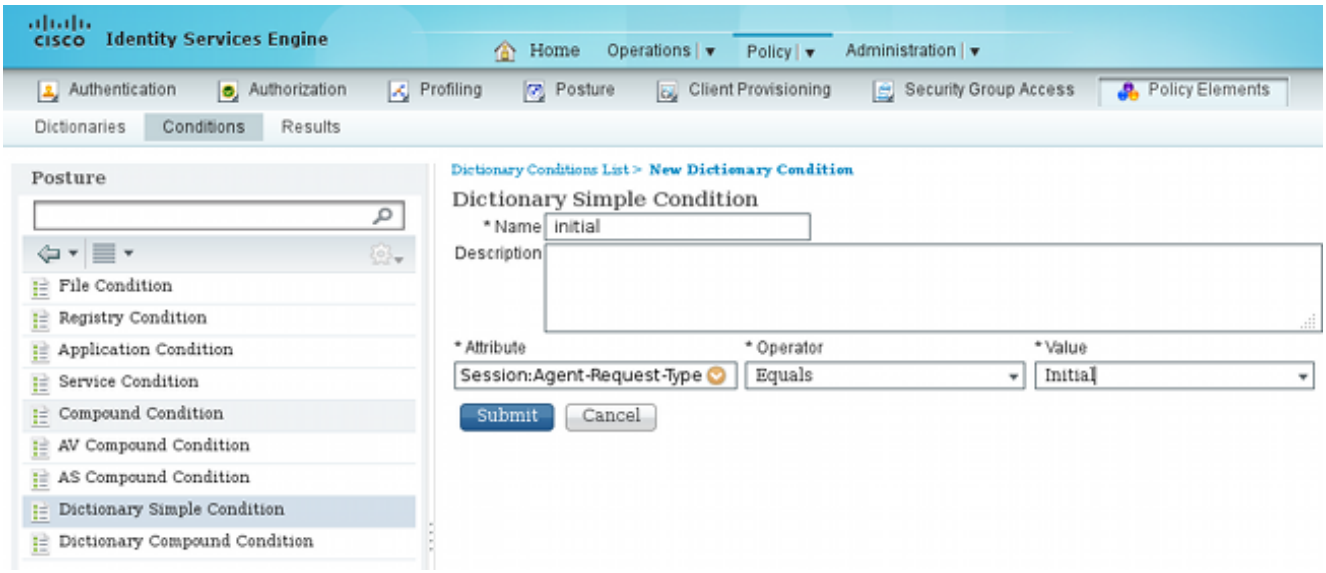
1. Navigeren naar **Beheer > Instellingen > Houding > Herbeoordelingen** en globaal opnieuw beoordelen (per configuratie van identiteitsgroep):



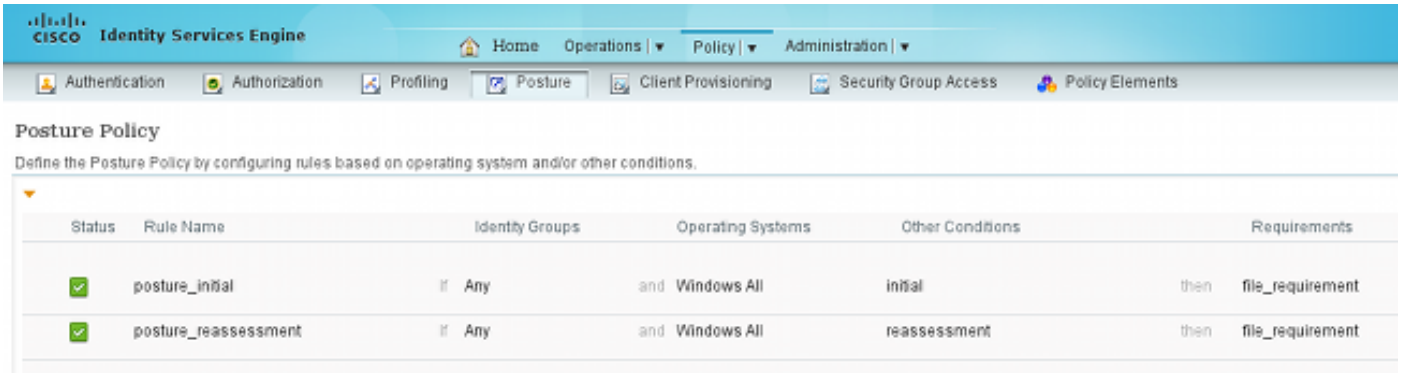
2. Maak een postuur voorwaarde die aansluit bij alle herbeoordelingen:



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



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:



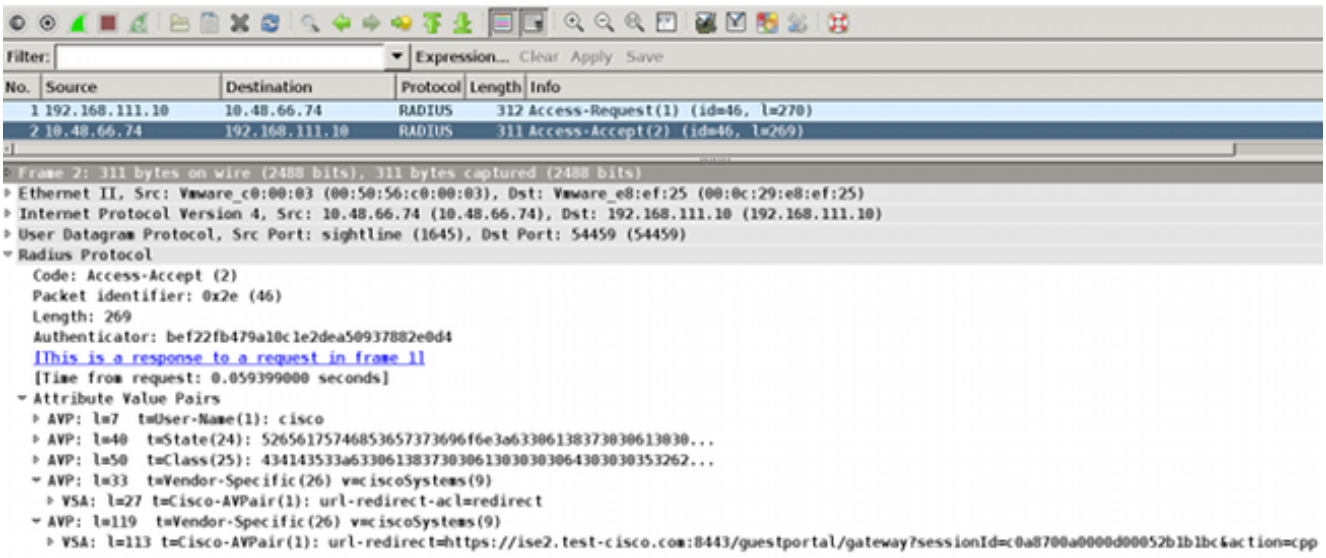
Verifiëren

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

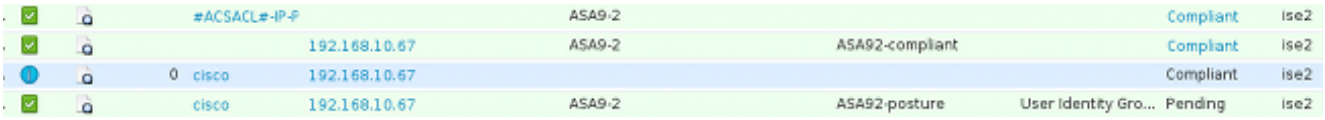
correct werkt:

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):



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
```

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

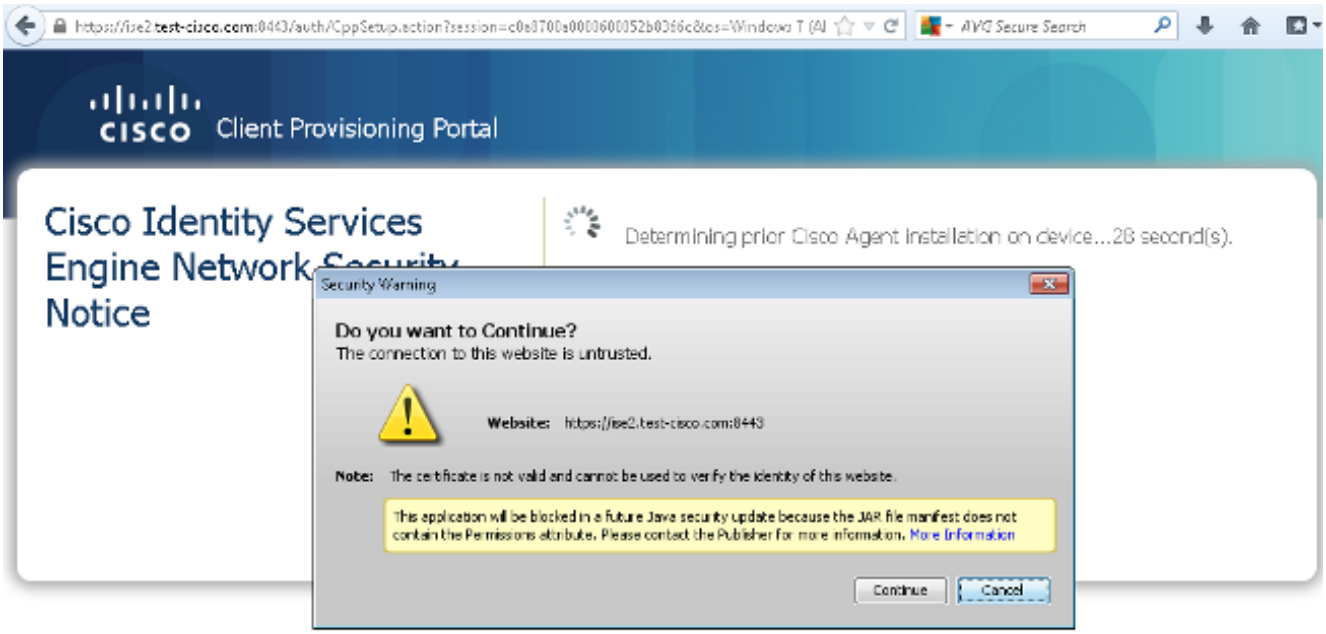
```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 9
Assigned IP  : 10.10.10.10            Public IP    : 10.147.24.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
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     : 16077                  Bytes Rx     : 19497
Pkts Tx      : 43                     Pkts Rx      : 225
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:01m:34s
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    : 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
 Encryption   : RC4                    Hashing      : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 50044
 TCP Dst Port : 443                    Auth Mode    : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 28 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   : 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 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
```

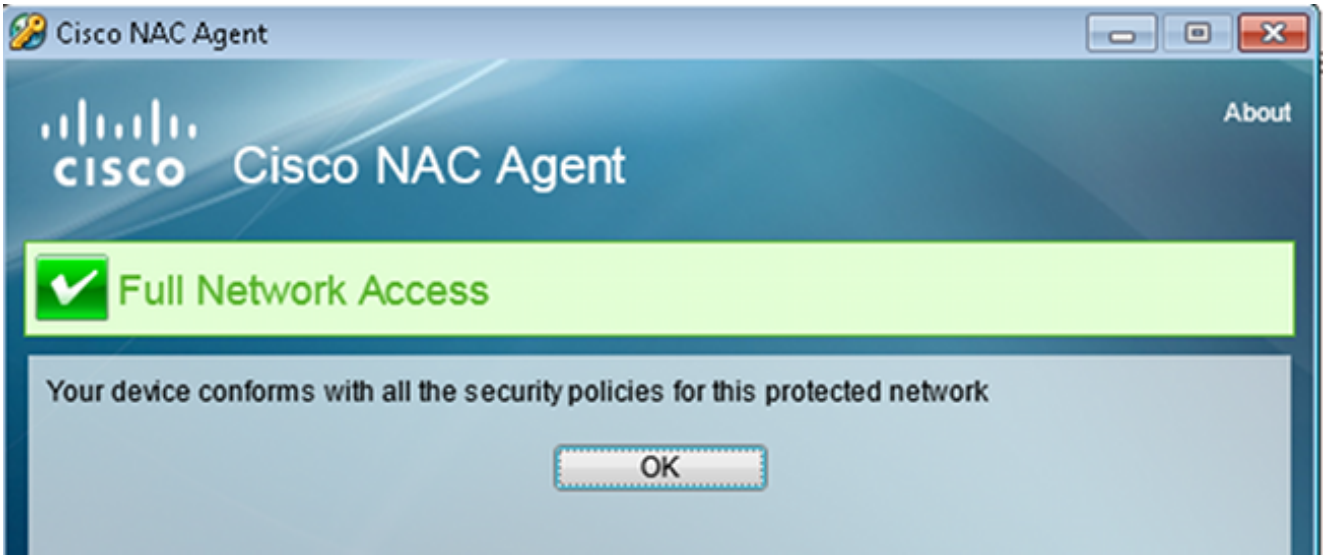
6. De client die het HTTP-verkeer initieert dat overeenkomt met de omgeleide ACL, wordt omgeleid naar de ISE:

```
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:



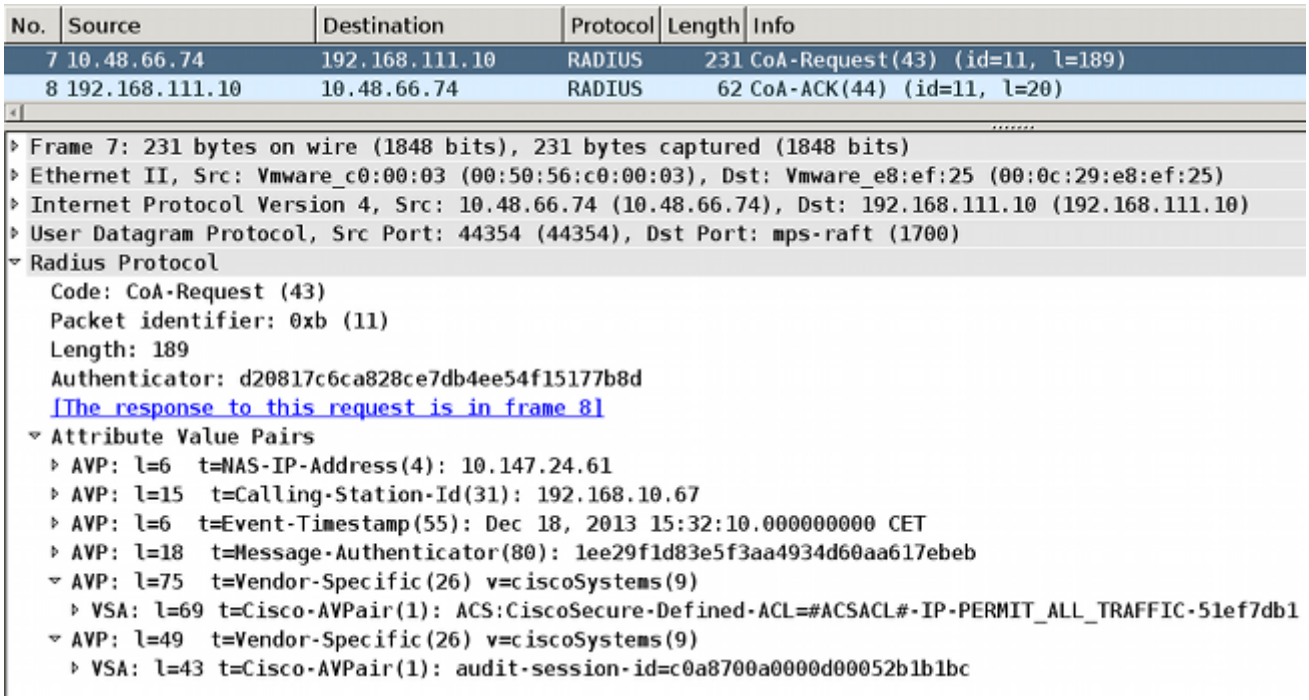
8. De NAC Agent is geïnstalleerd. Nadat de NAC Agent is geïnstalleerd, downloadt het de postuur regels via SWISS protocol en voert controles uit om naleving te bepalen. Het verslag van de standplaats wordt vervolgens naar de ISE gestuurd.



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  Length  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)

▸ Frame 7: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)
▸ Ethernet II, Src: Vmware_c0:00:03 (00:50:56:c0:00:03), Dst: Vmware_e8:ef:25 (00:0c:29:e8:ef:25)
▸ Internet Protocol Version 4, Src: 10.48.66.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)
▸ User Datagram Protocol, Src Port: 44354 (44354), Dst Port: mps-raft (1700)
▾ Radius Protocol
    Code: CoA-Request (43)
    Packet identifier: 0xb (11)
    Length: 189
    Authenticator: d20817c6ca828ce7db4ee54f15177b8d
    [The response to this request is in frame 8]
  ▾ Attribute Value Pairs
    ▸ AVP: l=6  t=NAS-IP-Address(4): 10.147.24.61
    ▸ AVP: l=15  t=Calling-Station-Id(31): 192.168.10.67
    ▸ AVP: l=6  t=Event-Timestamp(55): Dec 18, 2013 15:32:10.000000000 CET
    ▸ AVP: l=18  t=Message-Authenticator(80): 1ee29f1d83e5f3aa4934d60aa617ebeb
    ▾ AVP: l=75  t=Vendor-Specific(26) v=ciscoSystems(9)
      ▸ VSA: l=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
    ▾ AVP: l=49  t=Vendor-Specific(26) v=ciscoSystems(9)
      ▸ VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc
```

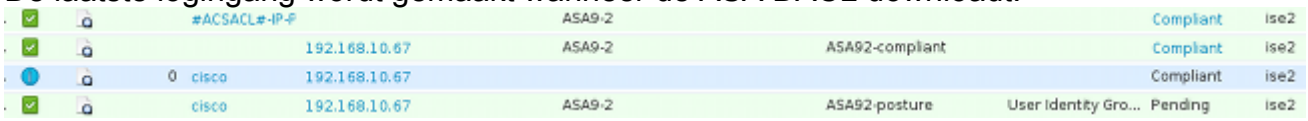
Dit wordt weerspiegeld in de ISE-logboeken:

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.



```
#ACSACL#-IP-P          ASA9-2                                  Compliant  ise2
192.168.10.67          ASA9-2          ASA92-compliant         Compliant  ise2
0 cisco    192.168.10.67                                       Compliant  ise2
cisco      192.168.10.67               ASA92-posture  User 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:

```
ASA# Received RAD_COA_REQUEST

RADIUS packet decode (CoA-Request)

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
License      : AnyConnect Essentials
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
Pkts Tx      : 169                    Pkts Rx      : 382
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    : 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 : 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:
 Tunnel ID    : 9.2
 Assigned IP  : 10.10.10.10            Public IP    : 10.147.24.61
 Encryption   : RC4                    Hashing      : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 50044
 TCP Dst Port : 443                    Auth Mode    : userPassword
 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 Agent for Windows 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-51ef7db1
```

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

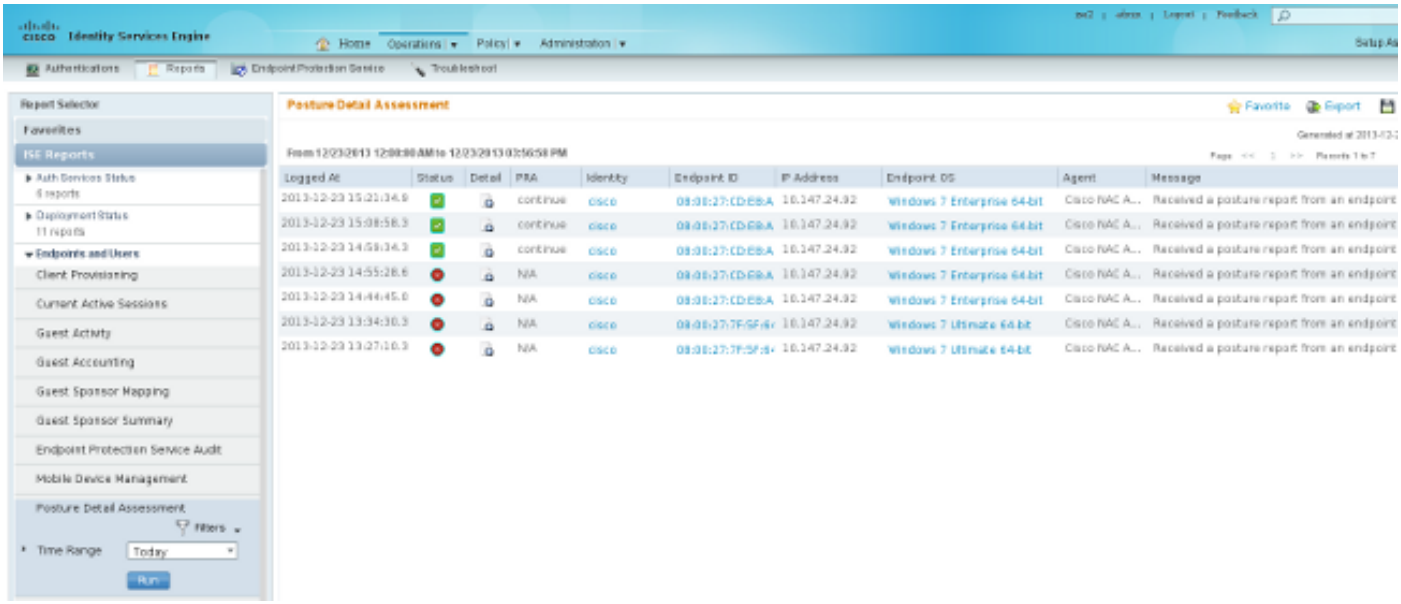
Blader naar **Beheer > Vastlegging > Configuratie debug log** om debugs in te schakelen. Cisco raadt u aan tijdelijke debugs in te schakelen voor:

- 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:



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 Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM
Generated At: 2013-12-23 15:57:31.248

Client Details

Username:	cisco
Mac Address:	08:00:27:CD:E8:A2
IP address:	10.147.24.92
Session ID:	c0a8700a0000b00052b846c0
Client Operating System:	Windows 7 Enterprise 64-bit
Client NAC Agent:	Cisco NAC Agent for Windows 4.9.0.1013
PRA Enforcement:	1
CoA:	Received a posture report from an endpoint
PRA Grace Time:	
PRA Interval:	240
PRA Action:	continue
User Agreement Status:	NotEnabled
System Name:	MGARCARZ-WS01
System Domain:	cisco.com
System User:	mgarcarz
User Domain:	CISCO
AV Installed:	McAfee VirusScan Enterprise;8.8.0.975;7227;10/13/2013;McAfeeAV,Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Windows Defender;6.1.7600.16385;1.95.191.0;11/19/2010;MicrosoftAS

Posture Report

Posture Status:	Compliant
Logged At:	2013-12-23 15:21:34.902

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require...	Mandatory		file_condition		

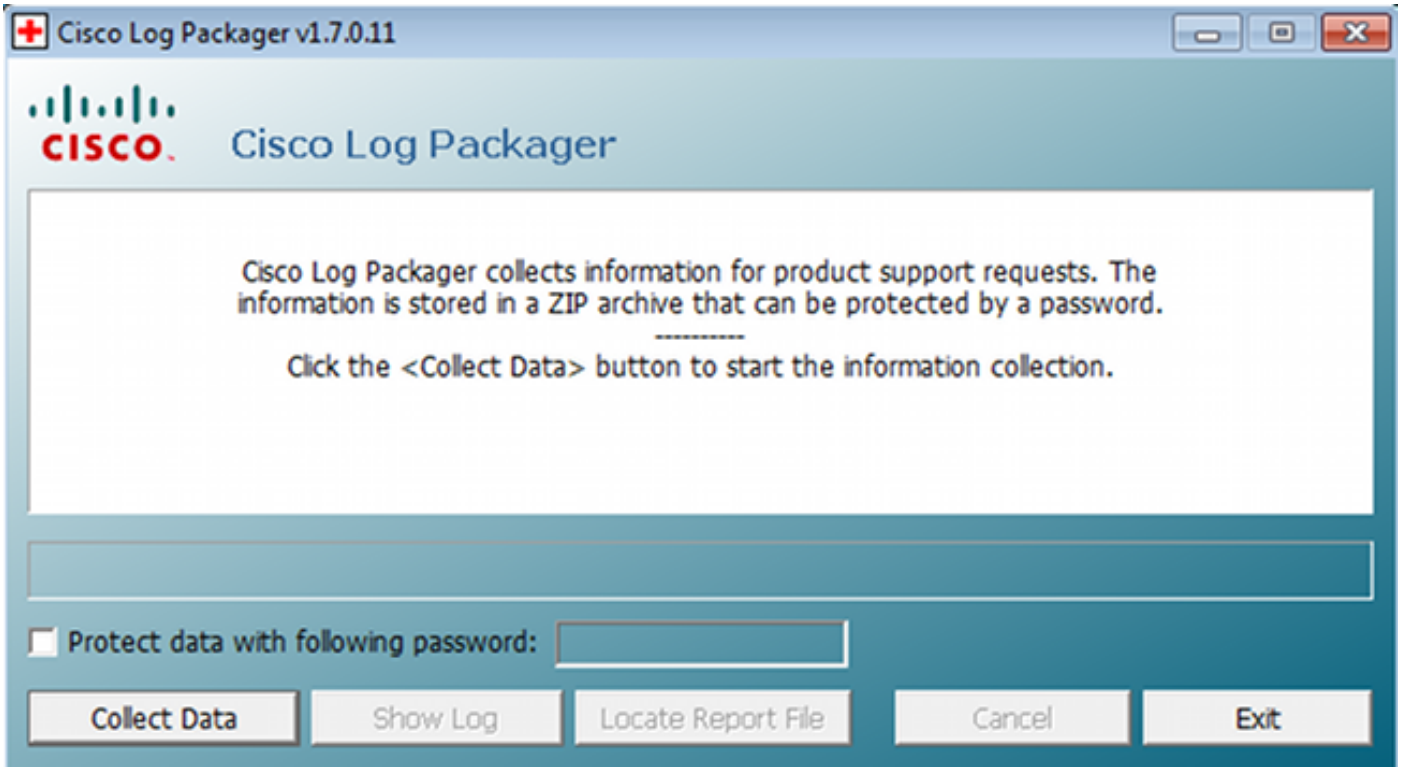
Debug-informatie op de ASA

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**.



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

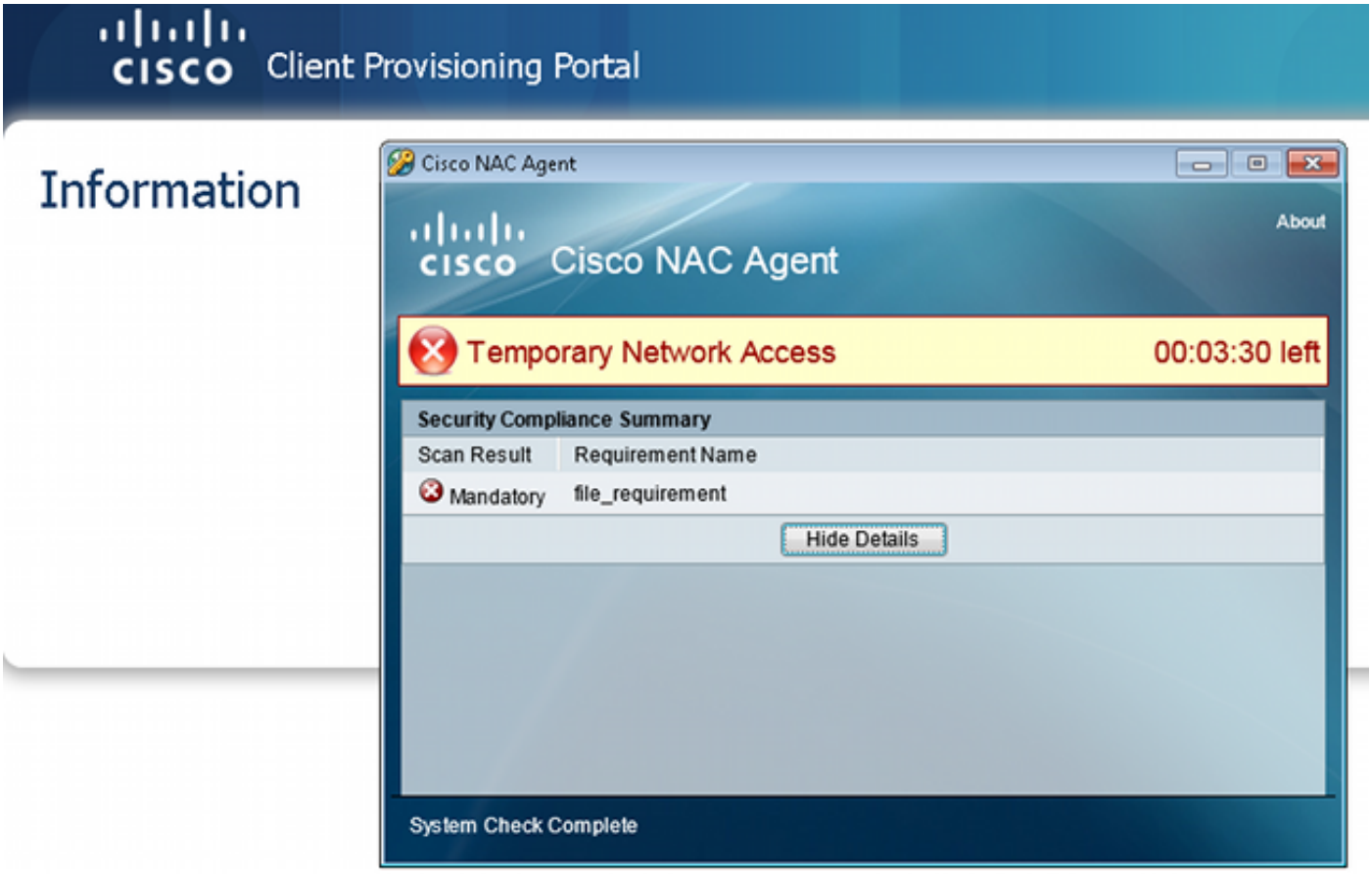
Om de logbestanden voor de Web Agent op te halen, navigeer naar deze locaties:

- **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**

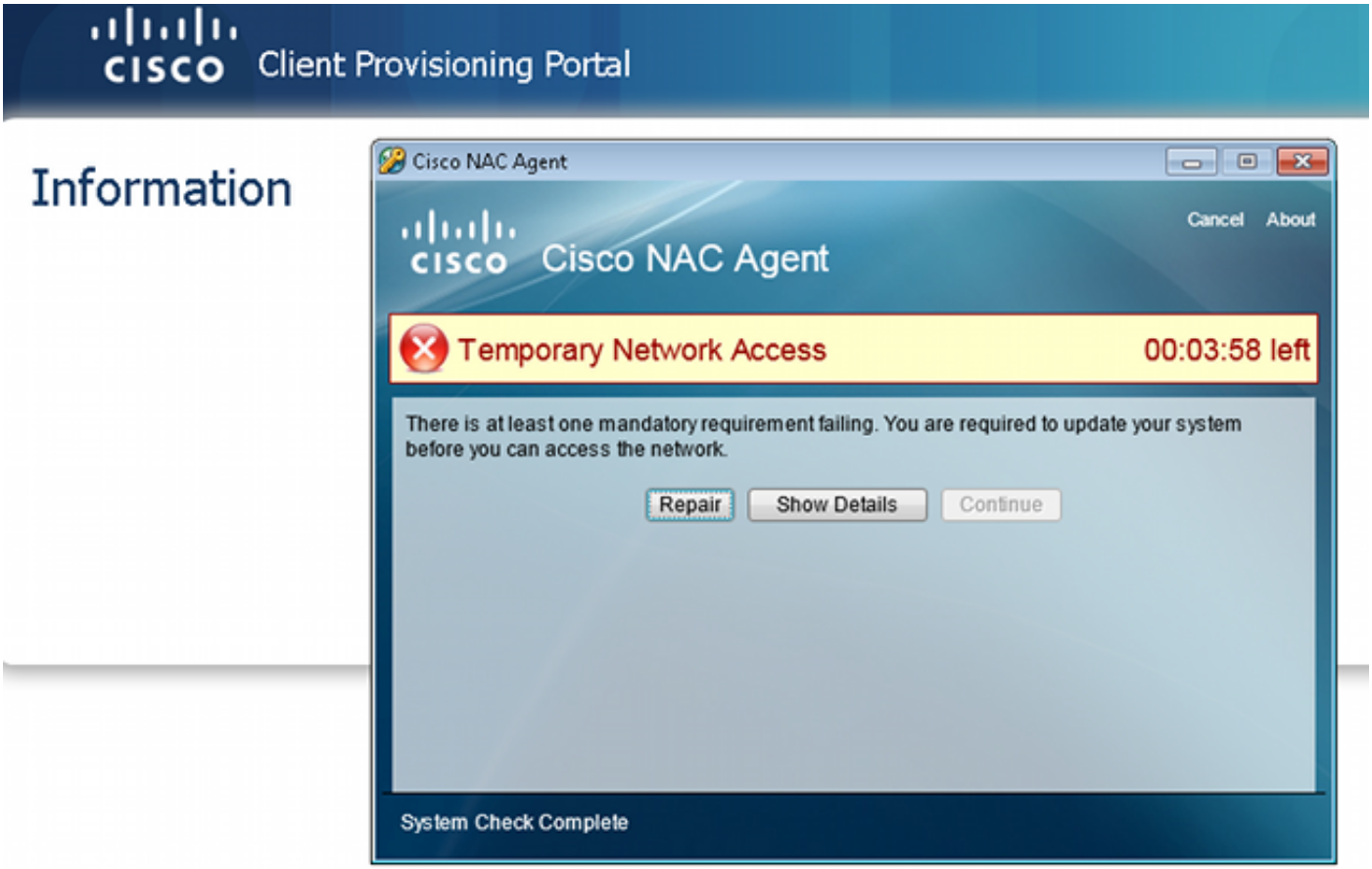
Opmerking: Als de logbestanden niet op deze locaties staan, moet u de variabele **TEMP Environment** controleren.

NAC Agent-poortfout

Als de houding mislukt, krijgt de gebruiker de reden:



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
- Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2
- 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.