

Exemplo de postura de VPN na ASA versão 9.2.1 com configuração do ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de rede e fluxo de tráfego](#)

[Configurações](#)

[ASA](#)

[ISE](#)

[Reavaliação periódica](#)

[Verificar](#)

[Troubleshoot](#)

[Depurações no ISE](#)

[Depurações no ASA](#)

[Depurações para o agente](#)

[Falha de postura do agente NAC](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) Versão 9.2.1 para posicionar os usuários de VPN contra o Cisco Identity Services Engine (ISE) sem a necessidade de um Inline Posture Node (IPN).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração CLI do ASA e da configuração VPN SSL
- Conhecimento básico da configuração da VPN de acesso remoto no ASA
- Conhecimento básico de ISE e serviços de postura

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco ASA versões 9.2.1 e posteriores
- Microsoft Windows versão 7 com Cisco AnyConnect Secure Mobility Client versão 3.1
- Cisco ISE versão 1.2 com Patch 5 ou posterior

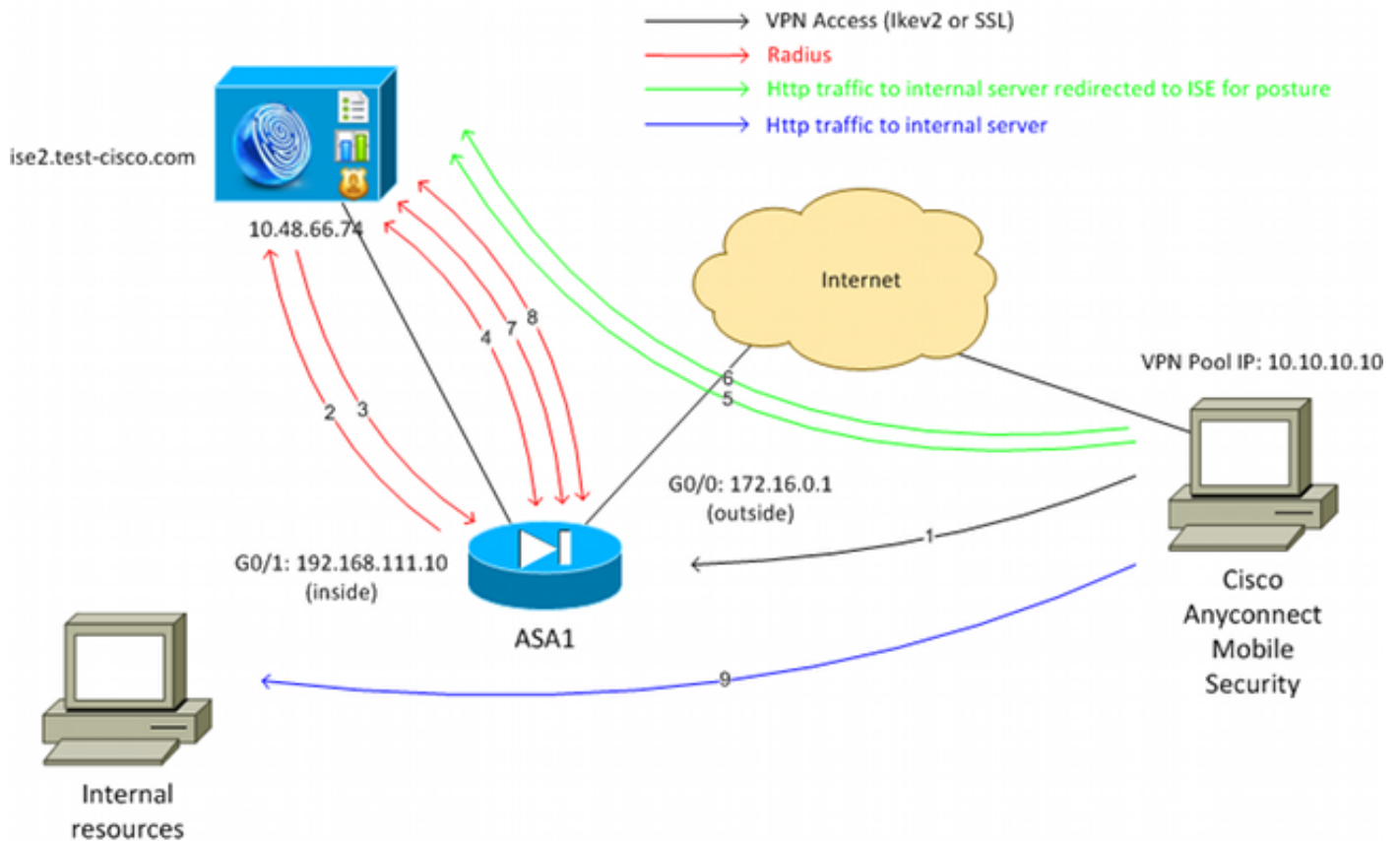
Informações de Apoio

O Cisco ASA versão 9.2.1 suporta RADIUS Change of Authorization (CoA) (RFC 5176). Isso permite a postura dos usuários de VPN em relação ao Cisco ISE sem a necessidade de um IPN. Depois que um usuário da VPN faz login, o ASA redireciona o tráfego da Web para o ISE, onde o usuário é provisionado com um Agente de Controle de Admissão na Rede (NAC - Network Admission Control) ou Agente da Web. O agente executa verificações específicas no computador do usuário para determinar sua conformidade com um conjunto configurado de regras de postura, como sistema operacional (SO), patches, antivírus, serviço, aplicativo ou regras de registro.

Os resultados da validação da postura são enviados ao ISE. Se a máquina for considerada reclamada, o ISE poderá enviar um RADIUS CoA para o ASA com o novo conjunto de políticas de autorização. Após a validação bem-sucedida da postura e do CoA, o usuário tem permissão para acessar os recursos internos.

Configurar

Diagrama de rede e fluxo de tráfego



Aqui está o fluxo de tráfego, como ilustrado no diagrama de rede:

1. O usuário remoto usa o Cisco Anyconnect para acesso VPN ao ASA.
2. O ASA envia uma solicitação de acesso RADIUS para esse usuário ao ISE.
3. Essa solicitação atinge a política chamada **postura do ASA92** no ISE. Como resultado, o perfil de autorização de postura do **ASA92** é retornado. O ISE envia um Access-Accept RADIUS com dois pares de Atributo-Valor da Cisco:

url-redirect-acl=redirect - esse é o nome da Lista de Controle de Acesso (ACL) definida localmente no ASA, que decide o tráfego que deve ser redirecionado.

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp - esta é a URL para a qual o usuário remoto deve ser redirecionado. **Dica:** os servidores DNS (Domain Name System) atribuídos aos clientes VPN devem ser capazes de resolver o FQDN (Fully Qualified Domain Name) retornado na URL de redirecionamento. Se os filtros VPN forem configurados para restringir o acesso no nível do grupo de túneis, certifique-se de que o pool de clientes seja capaz de acessar o servidor ISE na porta configurada (**TCP 8443** neste exemplo).

4. O ASA envia um pacote de início de solicitação de contabilização RADIUS e recebe uma resposta. Isso é necessário para enviar todos os detalhes referentes à sessão para o ISE. Esses detalhes incluem o `session_id`, o endereço IP externo do cliente VPN e o endereço IP do ASA. O ISE usa o `session_id` para identificar essa sessão. O ASA também envia informações periódicas sobre contas provisórias, onde o atributo mais importante é o Framed-IP-Address com o IP atribuído ao cliente pelo ASA (**10.10.10.10** neste exemplo).

5. Quando o tráfego do usuário da VPN corresponde à ACL definida localmente (redirecionamento), ele é redirecionado para <https://ise2.test-cisco.com:8443>. Dependendo da configuração, o ISE provisiona o NAC Agent ou o Web Agent.
6. Depois que o agente é instalado na máquina cliente, ele executa automaticamente verificações específicas. Neste exemplo, ele procura o arquivo `c:\test.txt`. Ele também envia um relatório de postura ao ISE, que pode incluir várias trocas com o uso do protocolo SWISS e portas TCP/UDP 8905 para acessar o ISE.
7. Quando o ISE recebe o relatório de postura do agente, ele processa as regras de autorização novamente. Desta vez, o resultado da postura é conhecido e outra regra é atingida. Ele envia um pacote RADIUS CoA:

Se o usuário for compatível, um nome de ACL para download (DACL) que permita acesso total será enviado (compatível com a regra AuthZ ASA92).

Se o usuário não for compatível, um nome de DACL que permita acesso limitado será enviado (regra de AuthZ ASA92 não compatível). **Observação:** o RADIUS CoA é sempre confirmado; isto é, o ASA envia uma resposta ao ISE para confirmar.

8. O ASA remove o redirecionamento. Se não tiver as DACLs em cache, ele deverá enviar uma solicitação de acesso para baixá-las do ISE. O DACL específico é anexado à sessão VPN.
9. Na próxima vez que o usuário VPN tentar acessar a página da Web, ele poderá acessar todos os recursos permitidos pelo DACL que está instalado no ASA.
Se o usuário não estiver em conformidade, somente o acesso limitado será concedido. **Observação:** este modelo de fluxo difere da maioria dos cenários que usam RADIUS CoA. Para autenticações 802.1x com/sem fio, RADIUS CoA não inclui nenhum atributo. Ele aciona apenas a segunda autenticação, na qual todos os atributos, como DACL, são anexados. Para a postura da VPN do ASA, não há uma segunda autenticação. Todos os atributos são retornados no RADIUS CoA. A sessão VPN está ativa e não é possível alterar a maioria das configurações de usuário da VPN.

Configurações

Use esta seção para configurar o ASA e o ISE.

ASA

Esta é a configuração básica do ASA para acesso ao Cisco AnyConnect:

```
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

```

Para integração do ASA com a postura do ISE, certifique-se de que você:

- Configure o servidor de Autenticação, Autorização e Tarifação (AAA) para autorização dinâmica para aceitar CoA.
- Configure a contabilidade como um grupo de túneis para enviar os detalhes da sessão VPN para o ISE.
- Configurar a contabilidade provisória que enviará o endereço IP atribuído ao usuário e atualizar periodicamente o status da sessão no ISE
- Configure a ACL de redirecionamento, que decide se o tráfego DNS e ISE são permitidos. Todo o tráfego HTTP restante é redirecionado ao ISE para postura.

Aqui está o exemplo de configuração:

```

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

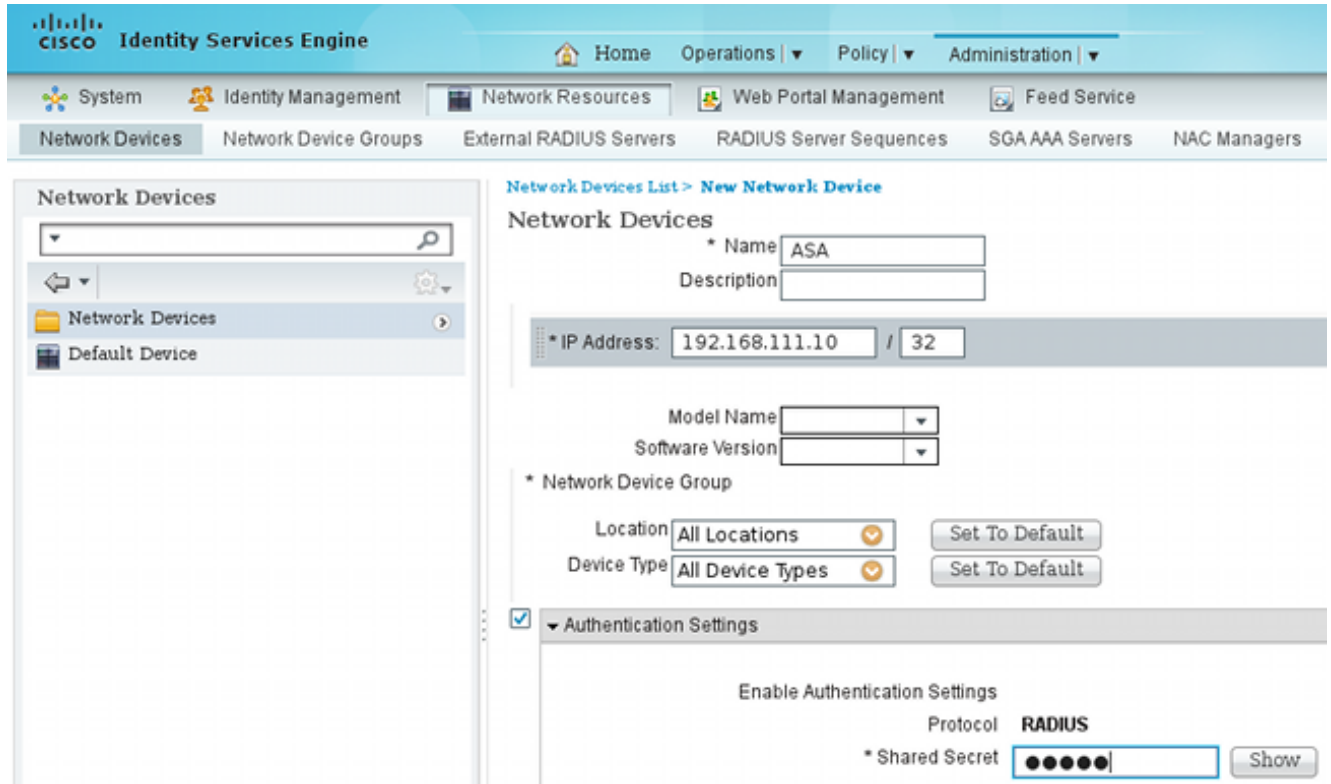
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE

```

ISE

Conclua estas etapas para configurar o ISE:

1. Navegue para **Administração > Recursos de rede > Dispositivos de rede** e adicione o ASA como um dispositivo de rede:



The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a new network device. The breadcrumb navigation path is **Network Devices List > New Network Device**. The main configuration area includes the following fields and options:

- Name:** ASA
- Description:** (empty)
- IP Address:** 192.168.111.10 / 32
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- Network Device Group:** (dropdown menu)
- Location:** All Locations (dropdown menu) with a **Set To Default** button.
- Device Type:** All Device Types (dropdown menu) with a **Set To Default** button.
- Authentication Settings:** (checked checkbox)
 - Enable Authentication Settings:** (checkbox)
 - Protocol:** RADIUS
 - * Shared Secret:** (masked with dots) with a **Show** button.

2. Navegue até **Policy > Results > Authorization > Downloadable ACL** e configure a DACL de modo que permita acesso total. A configuração ACL padrão permite todo o tráfego IP no ISE:

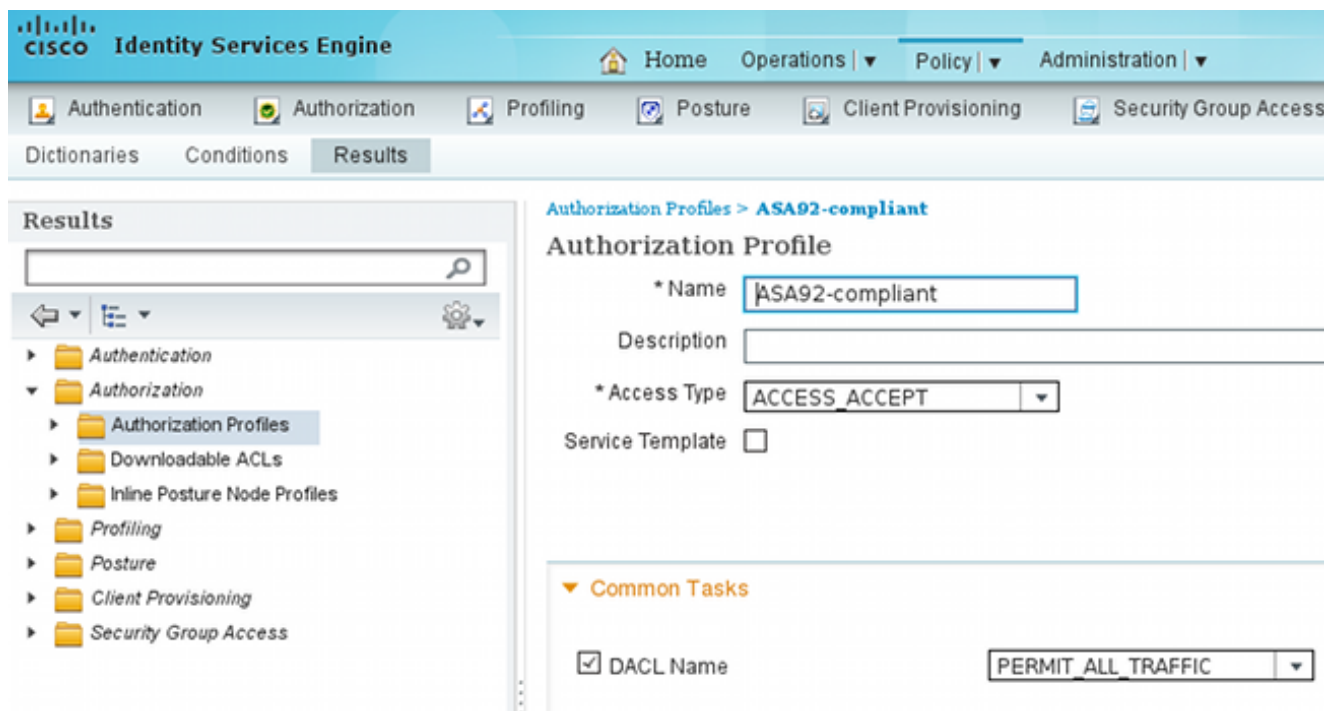
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below this, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The 'Results' tab is active, and the left sidebar shows a tree view of the configuration hierarchy, with 'Downloadable ACLs' selected. The main content area displays the configuration for a 'Downloadable ACL' named 'PERMIT_ALL_TRAFFIC'. The description is 'Allow all Traffic'. The DACL content is a single line: '1 permit ip any any'. There is a 'Check DACL Syntax' button at the bottom.

3. Configure uma ACL semelhante que forneça acesso limitado (para usuários não compatíveis).

4. Navegue para **Policy > Results > Authorization > Authorization Profiles** e configure o perfil de autorização chamado **ASA92-posture**, que redireciona os usuários para postura. Marque a caixa de seleção **Web Redirection**, selecione **Client Provisioning** na lista suspensa e verifique se **redirect** aparece no campo ACL (se a ACL está definida localmente no ASA):

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, and Administration. Below this, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The 'Results' tab is active, and the left sidebar shows a tree view of the configuration hierarchy, with 'Authorization Profiles' selected. The main content area displays the configuration for an 'Authorization Profile' named 'ASA92-posture'. The description is empty. The Access Type is set to 'ACCESS_ACCEPT'. The Service Template checkbox is unchecked. Under the 'Common Tasks' section, the 'Web Redirection (CWA, DRW, MDM, NSP, CPP)' checkbox is checked. At the bottom, the 'Client Provisioning (Posture)' dropdown is selected, and the ACL field contains the value 'redirect'. The 'Static IP/Host name' checkbox is unchecked.

5. Configure o perfil de autorização denominado **compatível com ASA92**, que deve retornar apenas o DACL denominado **PERMIT_ALL_TRAFFIC** que fornece acesso total para os usuários compatíveis:



6. Configure um perfil de autorização semelhante chamado **não compatível com ASA92**, que deve retornar o DACL com acesso limitado (para usuários não compatíveis).

7. Navegue para **Política > Autorização** e configure as Regras de Autorização:

Crie uma regra que permita acesso total se os resultados da postura forem compatíveis. O resultado é a política de autorização **compatível com ASA92**.

Crie uma regra que permita acesso limitado se os resultados da postura não forem compatíveis. O resultado é a política de autorização **não compatível com ASA92**.

Certifique-se de que se nenhuma das duas regras anteriores for atingida, a regra padrão retorna a **postura ASA92**, que força um redirecionamento no ASA.

<input checked="" type="checkbox"/>	ASA92 complaint	if Session:PostureStatus EQUALS Compliant	then ASA92-compliant
<input checked="" type="checkbox"/>	ASA92 non complaint	if Session:PostureStatus EQUALS NonCompliant	then ASA92-noncompliant
<input checked="" type="checkbox"/>	ASA92 redirect	if Radius:NAS-IP-Address EQUALS 192.168.111.10	then ASA92-posture

8. As regras de autenticação padrão verificam o nome de usuário no armazenamento de identidade interno. Se for necessário alterá-lo (marcado no Ative Directory (AD), por exemplo), navegue para **Política > Autenticação** e faça a alteração:

CISCO Identity Services Engine

Home Operations | Policy | Administration |

Authentication Authorization Profiling Posture Client Provisioning Security Group Access Pol

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Users	
<input checked="" type="checkbox"/>	Default Rule (if no match)	: Allow Protocols : Default Network Access and use : Internal Users	

9. Navegue até **Policy > Client Provisioning** e configure as regras de provisionamento. Essas são as regras que decidem o tipo de Agente que deve ser provisionado. Neste exemplo, existe apenas uma regra simples e o ISE seleciona o NAC Agent para todos os sistemas Microsoft Windows:

CISCO Identity Services Engine

Home Operations | Policy | Administration |

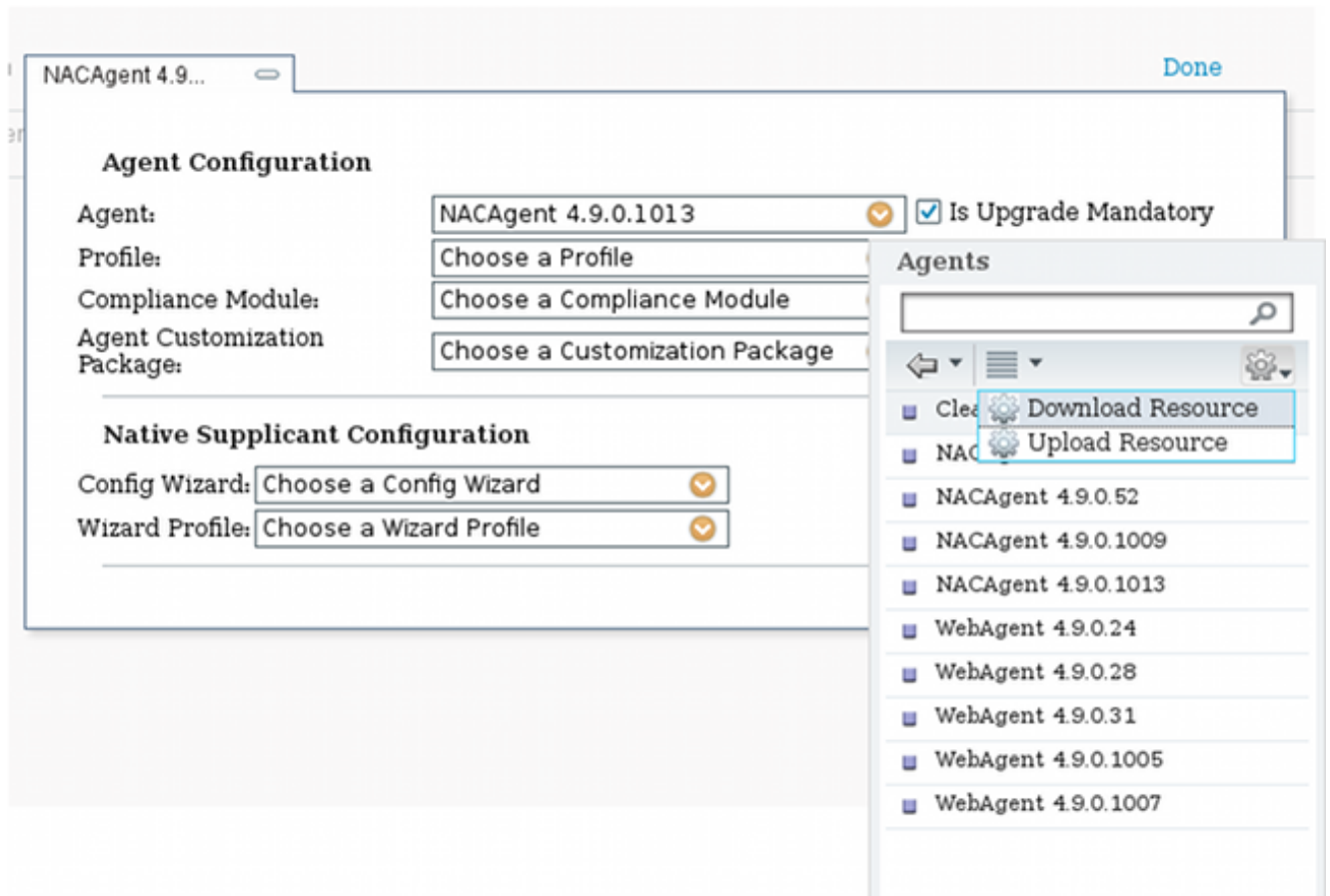
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation. For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> ASA92-posture	if Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1013

Quando os Agentes não estão no ISE, é possível baixá-los:



10. Se necessário, você pode navegar para **Administração > Sistema > Configurações > Proxy** e configurar o proxy para o ISE (para acessar a Internet).

11. Configure as regras de postura, que verificam a configuração do cliente. Você pode configurar regras que verificam:

arquivos - existência, versão, data

registro - chave, valor, existência

aplicativo - nome do processo, em execução, não em execução

service - nome do serviço, running, not running

antivírus - mais de 100 fornecedores suportados, versão, quando as definições são atualizadas

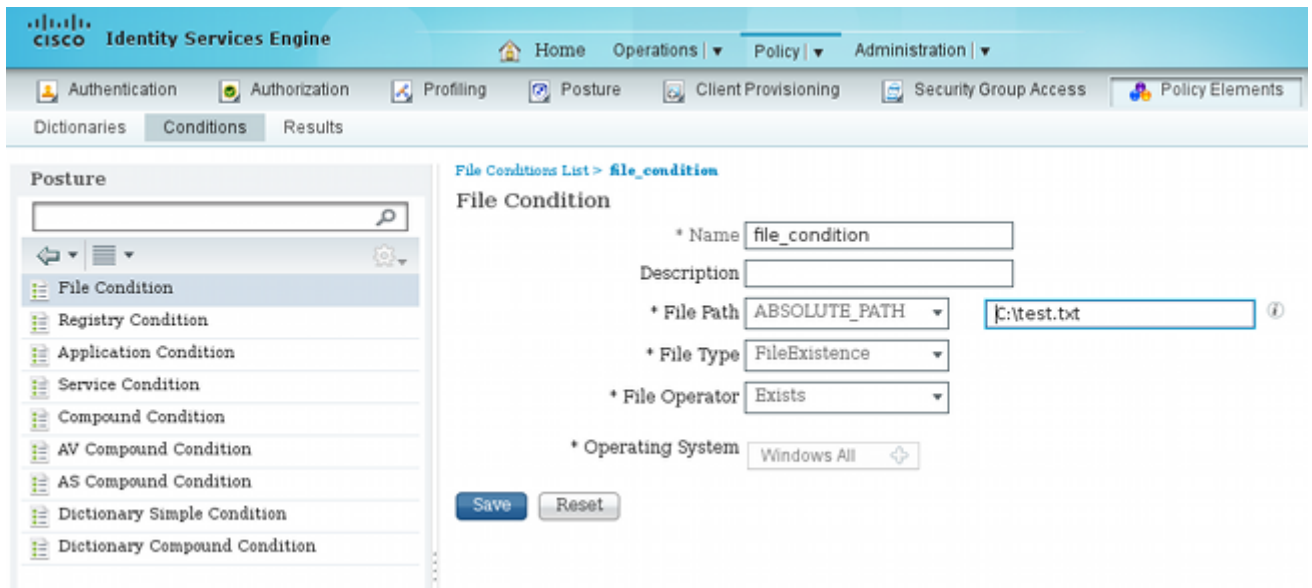
antispyware - mais de 100 fornecedores suportados, versão, quando as definições são atualizadas

estado composto - mistura de todos

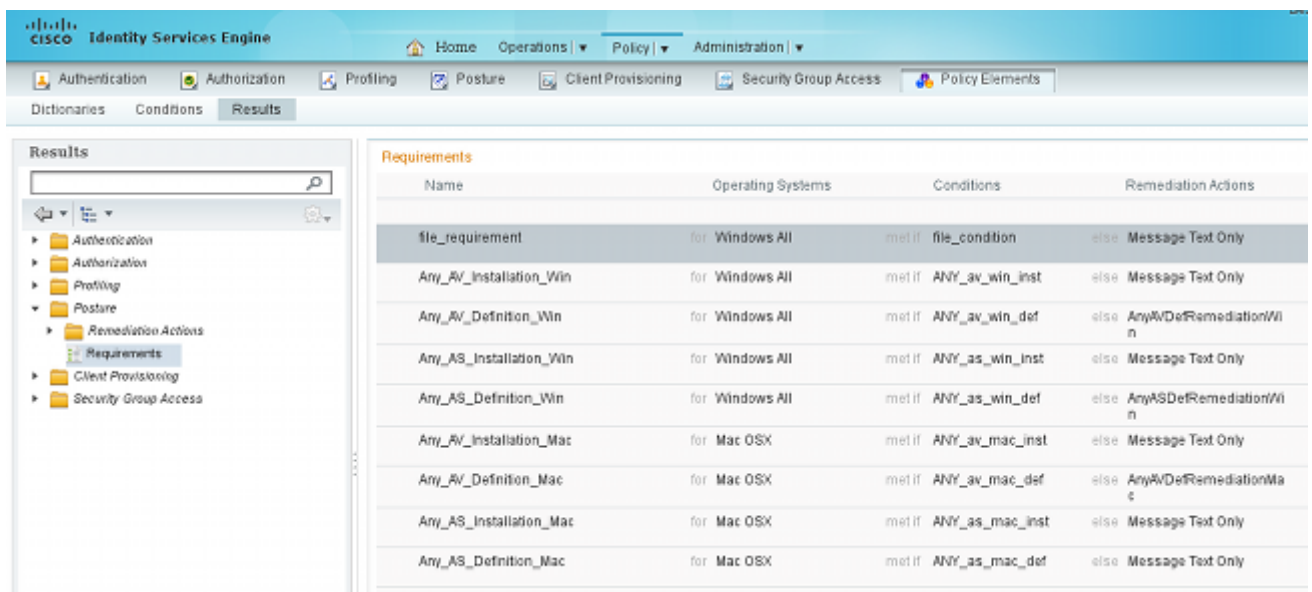
condições do dicionário personalizado - uso da maioria dos dicionários do ISE

12. Neste exemplo, somente uma verificação simples de existência de arquivo é executada. Se o arquivo `c:\test.txt` estiver presente na máquina cliente, ele é compatível e tem acesso total permitido. Navegue para **Política > Condições > Condições do arquivo** e configure a

condição do arquivo:

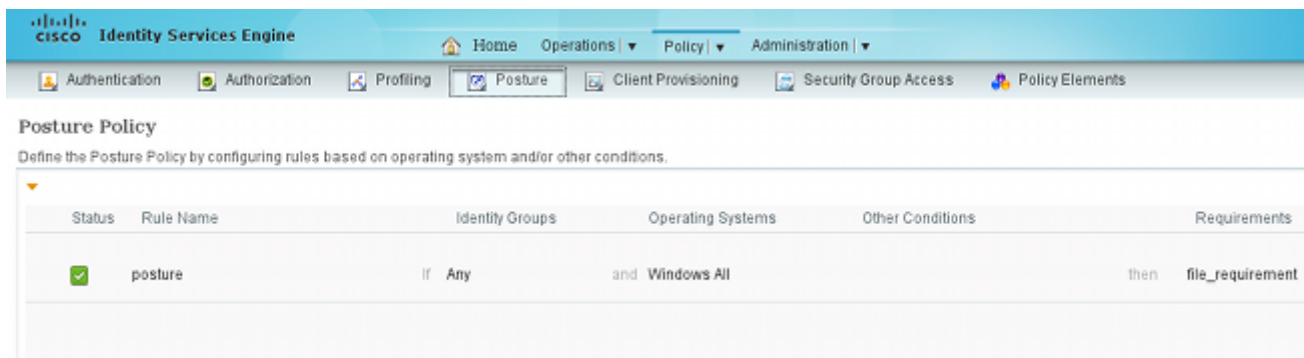


13. Navegue para **Política > Resultados > Postura > Requisitos** e crie um requisito. Este requisito deve ser cumprido quando a condição anterior for satisfeita. Se não for, a ação corretiva será executada. Pode haver muitos tipos de ações de remediação disponíveis, mas neste exemplo, o mais simples é usado: uma mensagem específica é exibida.



Observação: em um cenário normal, a ação de correção de arquivo pode ser usada (o ISE fornece o arquivo para download).

14. Navegue para **Política > Postura** e use o requisito que você criou na etapa anterior (chamado **file_requirement**) nas regras de postura. A única regra de postura requer que todos os sistemas Microsoft Windows atendam ao **file_requirement**. Se esse requisito for atendido, a estação está em conformidade; se não for atendida, a estação não está em conformidade.

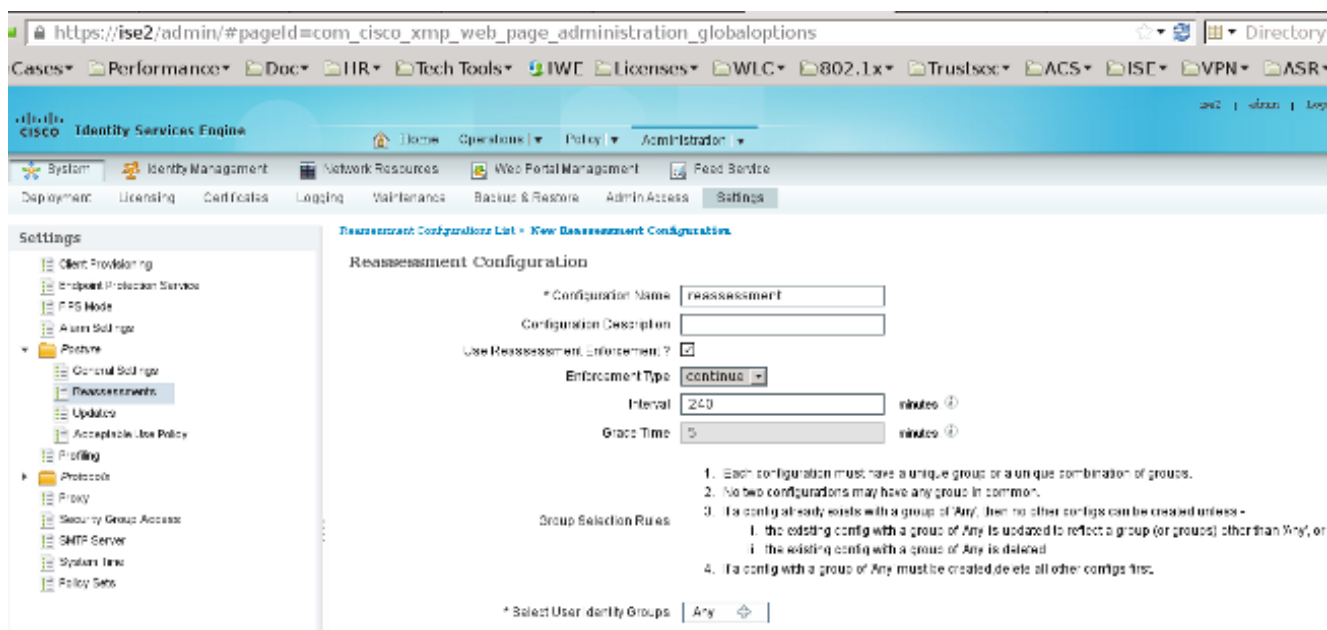


Reavaliação periódica

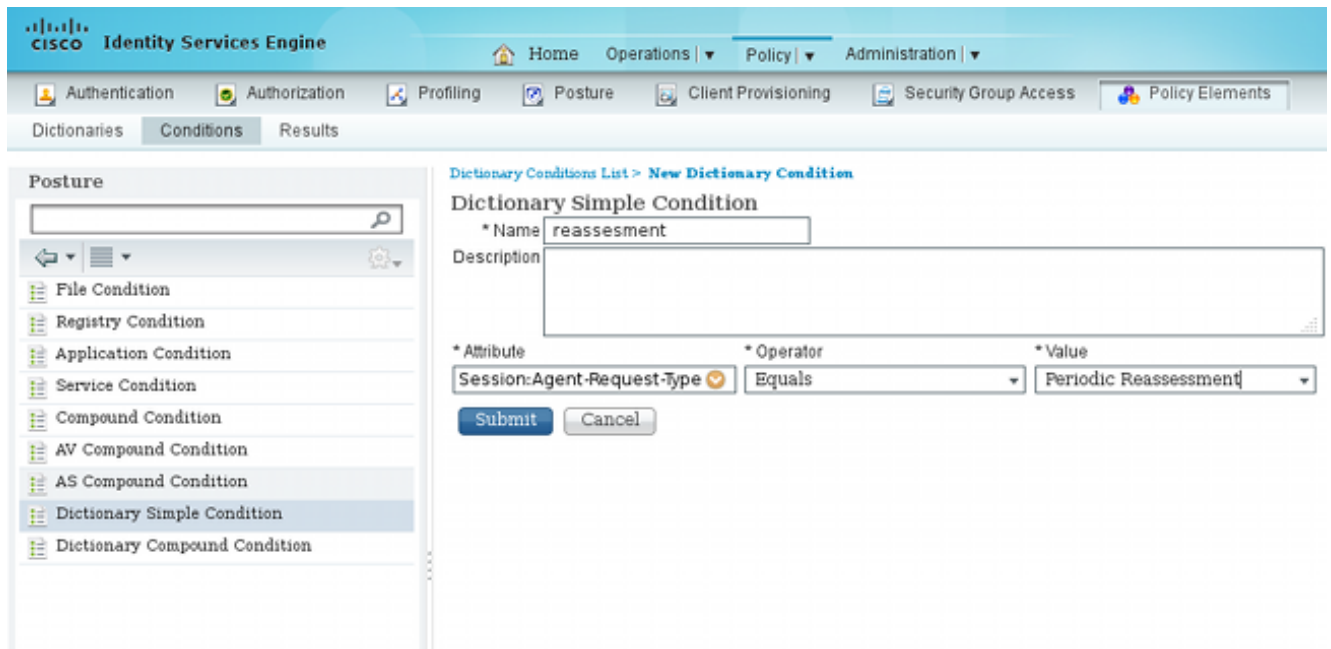
Por padrão, a postura é um evento único. No entanto, às vezes é necessário verificar periodicamente a conformidade do usuário e ajustar o acesso aos recursos com base nos resultados. Essas informações são enviadas por meio do protocolo SWISS (NAC Agent) ou codificadas no aplicativo (Web Agent).

Conclua estas etapas para verificar a conformidade do usuário:

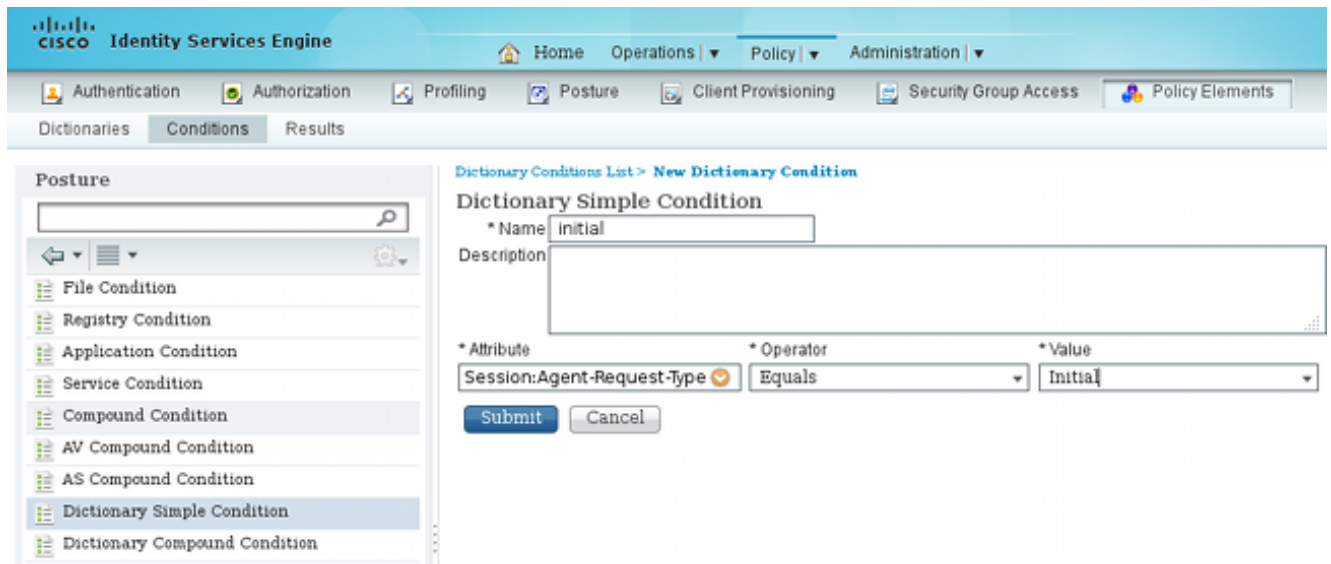
1. Navegue para **Administração > Configurações > Postura > Reavaliações** e habilite a reavaliação globalmente (por configuração de grupo de identidade):



2. Crie uma condição de postura que corresponda a todas as reavaliações:



3. Crie uma condição semelhante que corresponda somente às avaliações iniciais:



Ambas as condições podem ser usadas nas regras de postura. A primeira regra corresponde apenas às avaliações iniciais e a segunda corresponde a todas as avaliações subsequentes:

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

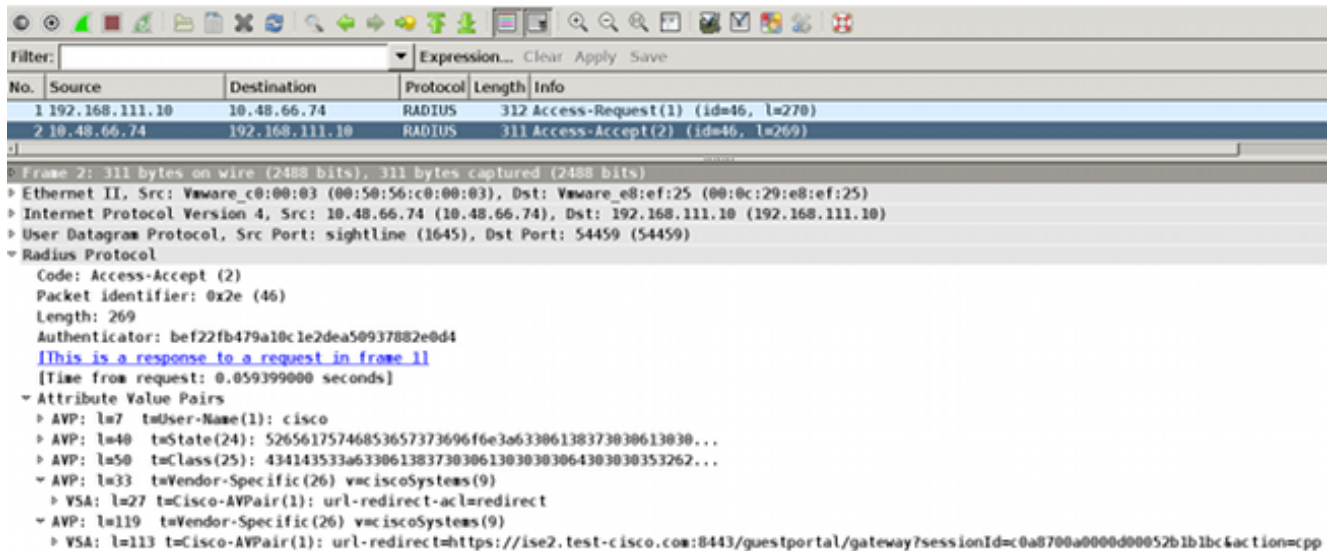
Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
✓	posture_initial	if Any	and Windows All	initial	then file_requirement
✓	posture_reassessment	if Any	and Windows All	reassessment	then file_requirement

Verificar

Para confirmar se sua configuração funciona corretamente, certifique-se de que estas etapas

sejam concluídas conforme descrito:

1. O usuário da VPN se conecta ao ASA.
2. O ASA envia uma solicitação RADIUS e recebe uma resposta com os atributos **url-redirect** e **url-redirect-acl**:



3. Os logs do ISE indicam que a autorização corresponde ao perfil de postura (a primeira entrada de log):

Check	Lock	Source	Destination	ASA	Profile	Status	Group
✓	🔒	#ACSACL#-IP-F		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	ASA9-2	ASA92-posture	Pending	User Identity Gro...

4. O ASA adiciona um redirecionamento à sessão VPN:

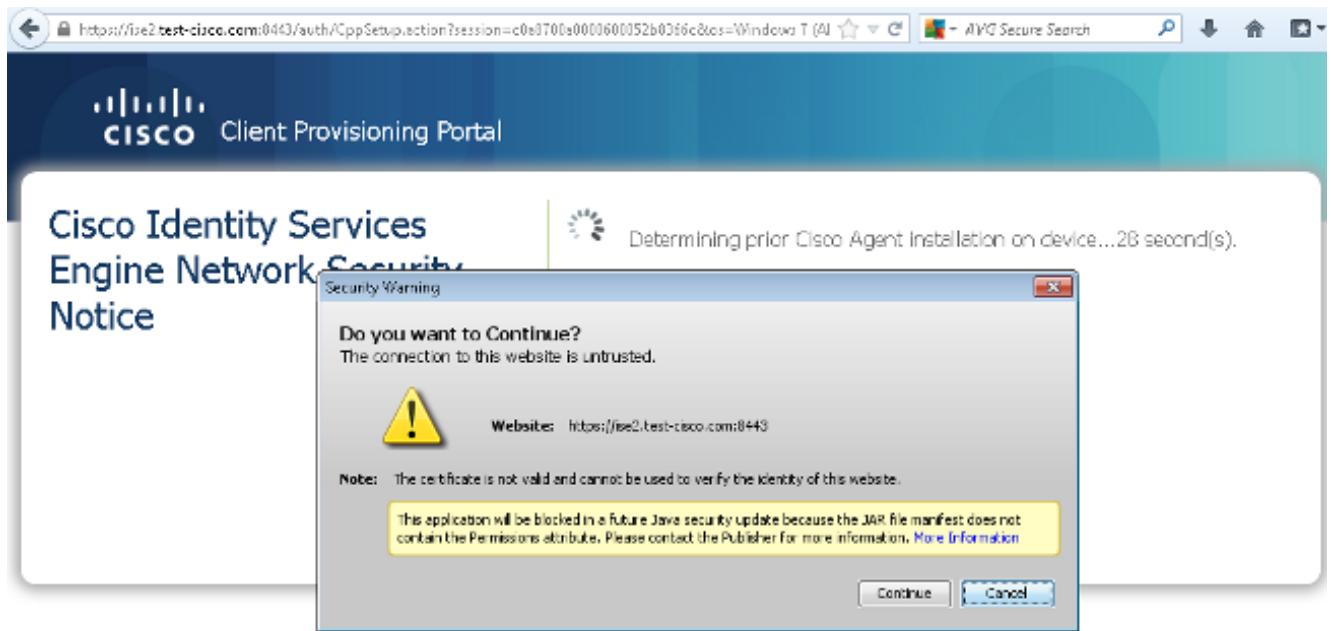
```
aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10
```

5. O status da sessão VPN no ASA mostra que a postura é necessária e redireciona o tráfego HTTP:

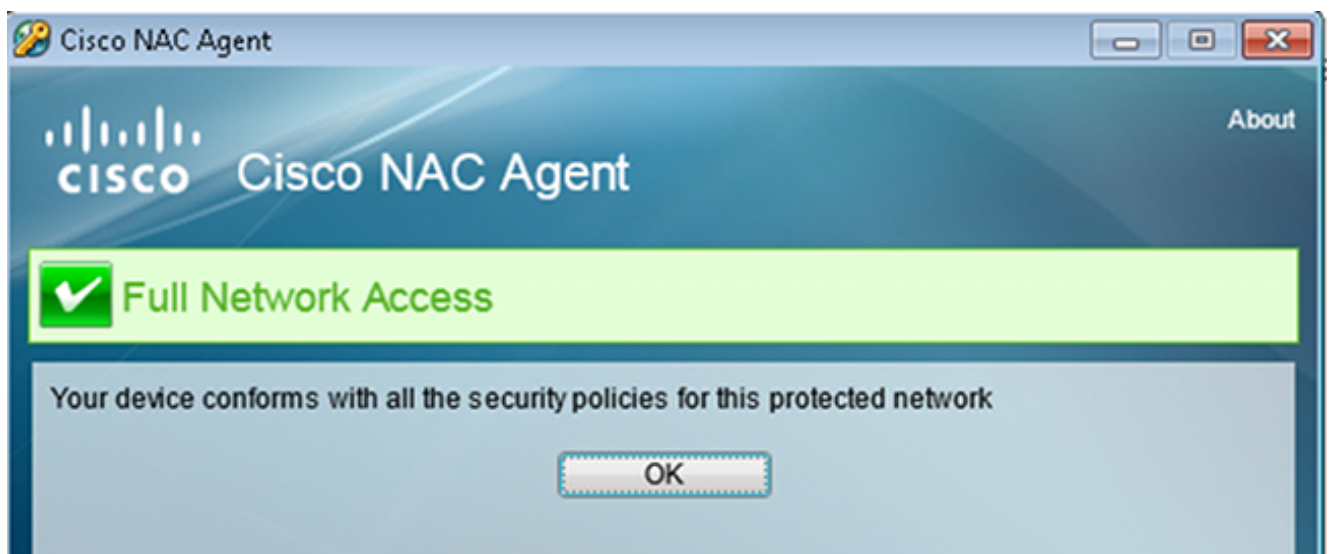
```
ASA# show vpn-sessiondb detail anyconnect
```

```
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
```

8. O NAC Agent está instalado. Depois que o NAC Agent é instalado, ele faz o download das regras de postura por meio do protocolo SWISS e executa verificações para determinar a conformidade. O relatório de postura é enviado ao ISE.



9. O ISE recebe o relatório de postura, reavalia as regras de autorização e (se necessário) altera o status de autorização e envia um CoA. Isso pode ser verificado no `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. O ISE envia um RADIUS CoA que inclui o **session_id** e o nome DACL que permite acesso total:

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)
v Radius Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xb (11)
  Length: 189
  Authenticator: d20817c6ca828ce7db4ee54f15177b8d
  [The response to this request is in frame 8]
v 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
  v 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
  v AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
    > VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc
  
```

Isso se reflete nos registros do ISE:

A primeira entrada de log é para a autenticação inicial que retorna o perfil de postura (com redirecionamento).

A segunda entrada de log é preenchida depois que o relatório SWISS compatível é recebido.

A terceira entrada de log é preenchida quando o CoA é enviado, junto com a confirmação (descrita como Dynamic Authorization Succeeded).

A entrada de log final é criada quando o ASA baixa o DACL.

✓	🔒	#ACSACL#-IP-F	ASA9-2	Compliant	ise2
✓	🔒	192.168.10.67	ASA9-2	ASA92-compliant	Compliant
🔄	🔒	0 cisco	192.168.10.67	Compliant	ise2
✓	🔒	cisco	192.168.10.67	ASA9-2	ASA92-posture
				User Identity Gro...	Pending
					ise2

11. As depurações no ASA mostram que o CoA foi recebido e o redirecionamento foi removido. O ASA faz o download das DACLs se necessário:

```
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. Após a sessão VPN, a Cisco aplica a DACL (acesso completo) para o usuário:

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
```

Observação: o ASA sempre remove as regras de redirecionamento, mesmo quando o CoA não tem nenhuma DACL anexada.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Depurações no ISE

Navegue para **Administration > Logging > Debug Log Configuration** para habilitar depurações. A Cisco recomenda que você habilite depurações temporárias para:

- SUÍÇO
- Encaminhamento ininterrupto (NSF)
- Sessão NSF
- Provisionar
- Postura

Insira este comando no CLI para exibir as depurações:

```
ise2/admin# show logging application ise-psc.log tail count 100
```

Navegue para **Operations > Reports > ISE Reports > Endpoints and Users > Posture Details Assessment** para exibir os relatórios de postura:

Posture Detail Assessment

From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 15:08:58.3	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:59:34.3	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:55:28.6	N/A		N/A	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:44:45.0	N/A		N/A	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:34:30.3	N/A		N/A	cisco	08:00:27:7F:5F:8*	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:27:10.3	N/A		N/A	cisco	08:00:27:7F:5F:8*	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

Na página Avaliação mais detalhada de postura, há um nome de política com um nome de requisito que é exibido, junto com os resultados:

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		

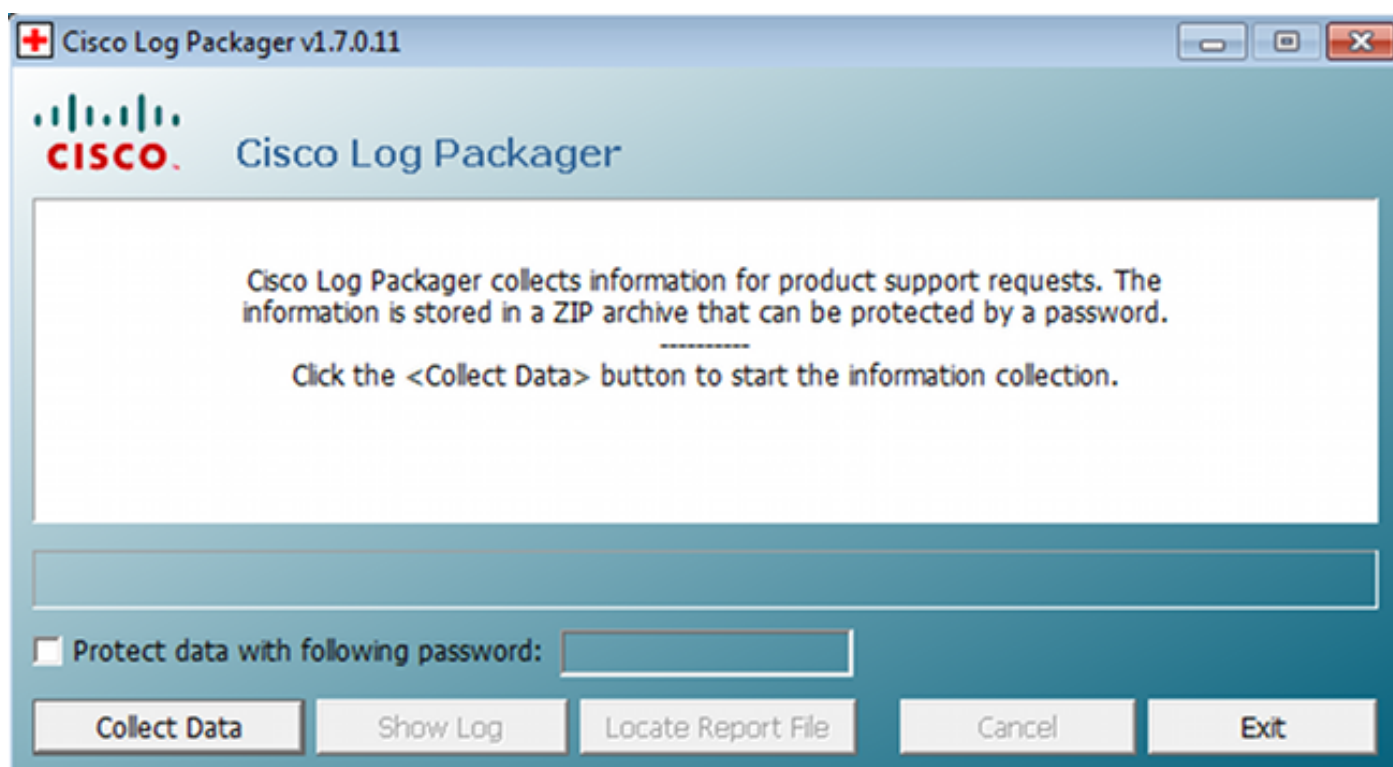
Depurações no ASA

Você pode habilitar estas depurações no ASA:

- debug aaa url-redirect
- debug aaa authorization
- debug radius dynamic-authorization
- debug radius decode
- debug radius user cisco

Depurações para o agente

Para o NAC Agent, é possível coletar as depurações com o Cisco Log Packager, que é iniciado na GUI ou com a CLI: **CCAAgentLogPackager.app**.



Dica: você pode decodificar os resultados com a ferramenta Technical Assistance Center (TAC).

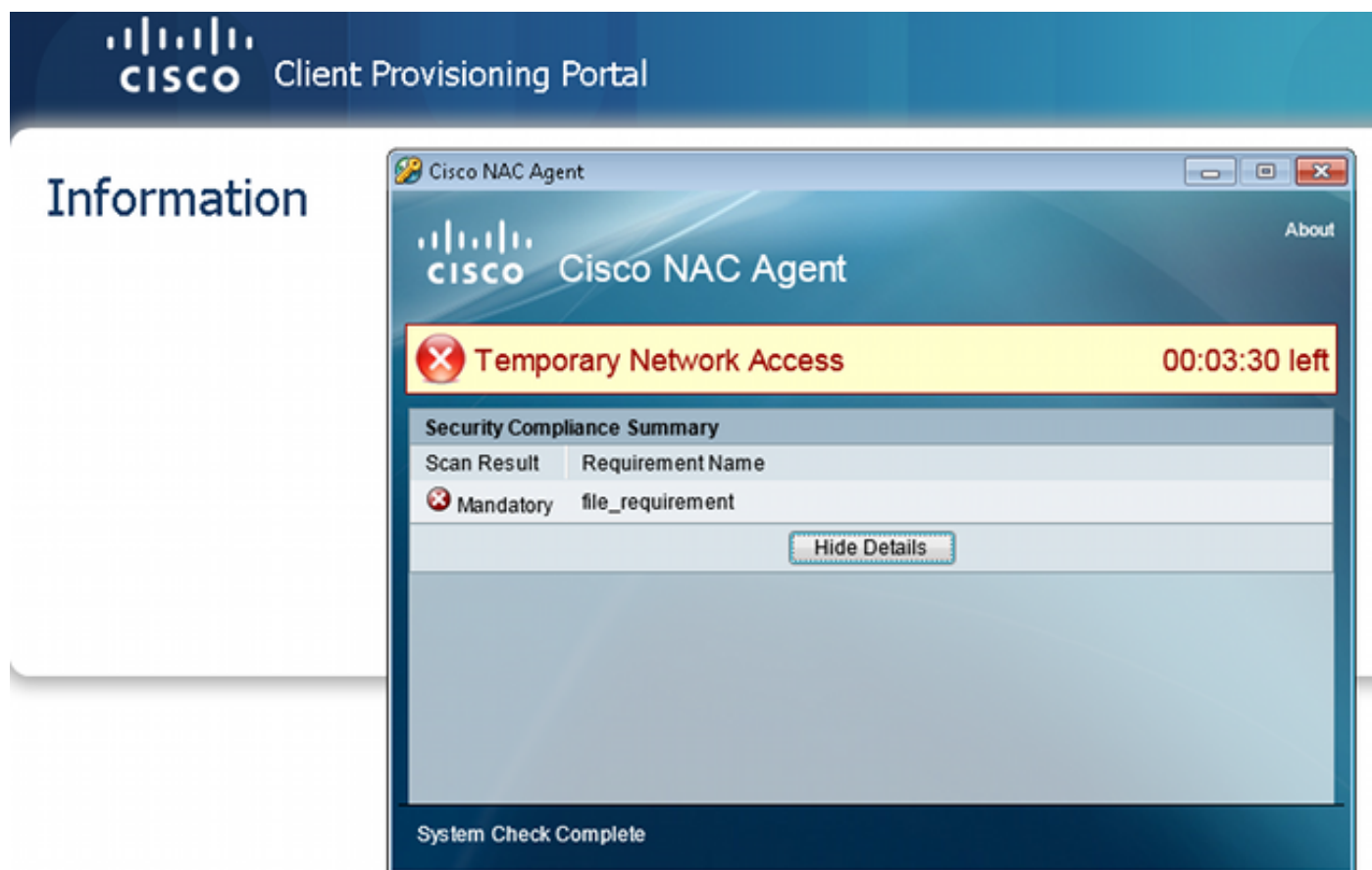
Para recuperar os logs do Agente da Web, navegue para estes locais:

- C: > Document and Settings > <user> > Local Settings > Temp > webagent.log (decodificado com a ferramenta TAC)
- C: > Document and Settings > <user> > Local Settings > Temp > webagentsetup.log

Observação: se os logs não estiverem nesses locais, verifique a variável **TEMP Environment**.

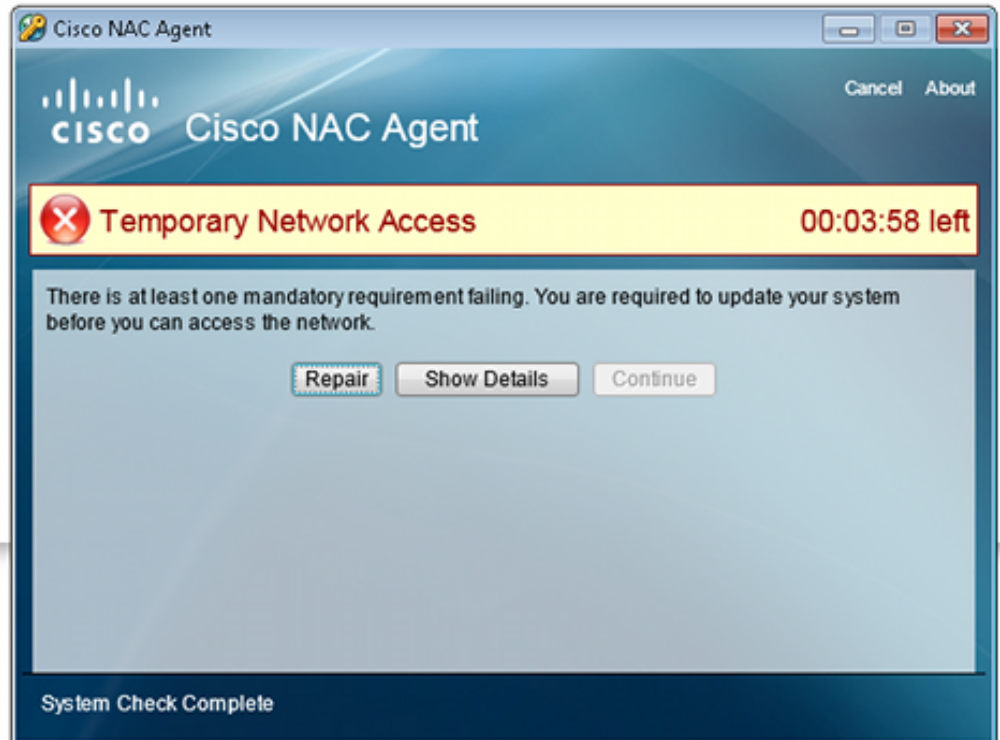
Falha de postura do agente NAC

Se a postura falhar, o usuário será apresentado com o motivo:



Em seguida, o usuário poderá executar ações corretivas se ele estiver configurado:

Information



Informações Relacionadas

- [Como configurar um servidor externo para autorização de usuário de dispositivo de segurança](#)
- [Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1](#)
- [Manual do usuário do Cisco Identity Services Engine, versão 1.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.