# Comparar versões anteriores do ISE com o fluxo de postura do ISE no ISE 2.2

## Contents


[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Fluxo de postura antes do ISE 2.2](#)
[Fluxo de postura no ISE 2.2](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Configuração de provisionamento do cliente](#)
[Políticas e condições de postura](#)
[Configurar o Portal de Provisionamento de Cliente](#)
[Configurar perfis e políticas de autorização](#)
[Verificar](#)
[Troubleshoot](#)
[Informações gerais](#)
[Troubleshooting Problemas Comuns](#)
[Problemas relacionados ao SSO](#)
[Solucionar Problemas de Seleção de Política de Provisionamento de Cliente](#)
[Solucionar problemas de processos de postura](#)


## Introduction

Este documento descreve a comparação do fluxo de postura no ISE 2.2 com o fluxo de postura em versões do ISE anteriores à 2.2.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxo de postura no ISE
- Configuração de componentes de postura no ISE
- Configuração do Adaptive Security Appliance (ASA) para postura sobre redes virtuais privadas (VPN)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 2.2
- Cisco ASAv com software 9.6 (2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Este documento descreve uma nova funcionalidade no Identity Service Engine (ISE) 2.2 que permite que o ISE suporte um fluxo de postura sem qualquer tipo de suporte de redirecionamento em um dispositivo de acesso à rede (NAD) ou no ISE.

A postura é um componente essencial do Cisco ISE. A postura como componente pode ser representada por três elementos principais:

1. O ISE como um ponto de distribuição e decisão de configuração de política.
   Da perspectiva do administrador no ISE, você configura políticas de postura (que condições exatas devem ser atendidas para marcar um dispositivo como compatível com a empresa), políticas de provisionamento de clientes (que software de agente deve ser instalado em que tipo de dispositivo) e políticas de autorização (a que tipo de permissões devem ser atribuídas, dependendo do status da postura).
2. Um dispositivo de acesso à rede como um ponto de aplicação de política.
   No lado NAD, as restrições de autorização reais são aplicadas no momento da autenticação do usuário. O ISE como um ponto de política fornece parâmetros de autorização, como a ACL baixada (dACL)/VLAN/Redirect-URL/Redirect Access Control List (ACL).
   Tradicionalmente, para que a postura ocorra, os NADs são necessários para suportar o redirecionamento (para instruir o usuário ou o software do agente que o nó do ISE deve ser contatado) e a alteração de autorização (CoA) para reautenticar o usuário depois que o status da postura do endpoint for determinado.
3. Software do agente como um ponto de coleta de dados e interação com o usuário final.
   O Cisco ISE usa três tipos de software de agente: AnyConnect ISE Posture Module, NAC Agent e Web Agent. O agente recebe informações sobre requisitos de postura do ISE e fornece um relatório ao ISE sobre o status dos requisitos.

> **Observação**: este documento é baseado no módulo de postura do AnyConnect ISE, que é o único que suporta postura totalmente sem redirecionamento.

Na postura de fluxo anterior ao ISE 2.2, os NADs não são usados apenas para autenticar usuários e restringir o acesso, mas também para fornecer informações ao software do agente sobre um nó ISE específico que deve ser contatado. Como parte do processo de redirecionamento, as informações sobre o nó ISE são retornadas ao software do agente.

Historicamente, o suporte ao redirecionamento no NAD ou no ISE era um requisito essencial para

a implementação da postura. No ISE 2.2, o requisito de suporte ao redirecionamento é eliminado tanto para o processo inicial de provisionamento como para o processo de postura do cliente.

Provisionamento de cliente sem redirecionamento - No ISE 2.2, você pode acessar o Client Provisioning Portal (CPP) diretamente por meio do Fully Qualified Domain Name (FQDN) do portal. Isso é semelhante à maneira como você acessa o Portal do patrocinador ou o Portal do MyDevice.

Processo de postura sem redirecionamento - Durante a instalação do agente a partir do portal CPP, as informações sobre os servidores ISE são salvas no lado do cliente, o que torna a comunicação direta possível.

# Fluxo de postura antes do ISE 2.2

Esta imagem mostra uma explicação passo a passo do fluxo do módulo de postura do Anyconnect ISE anterior ao ISE 2.2:

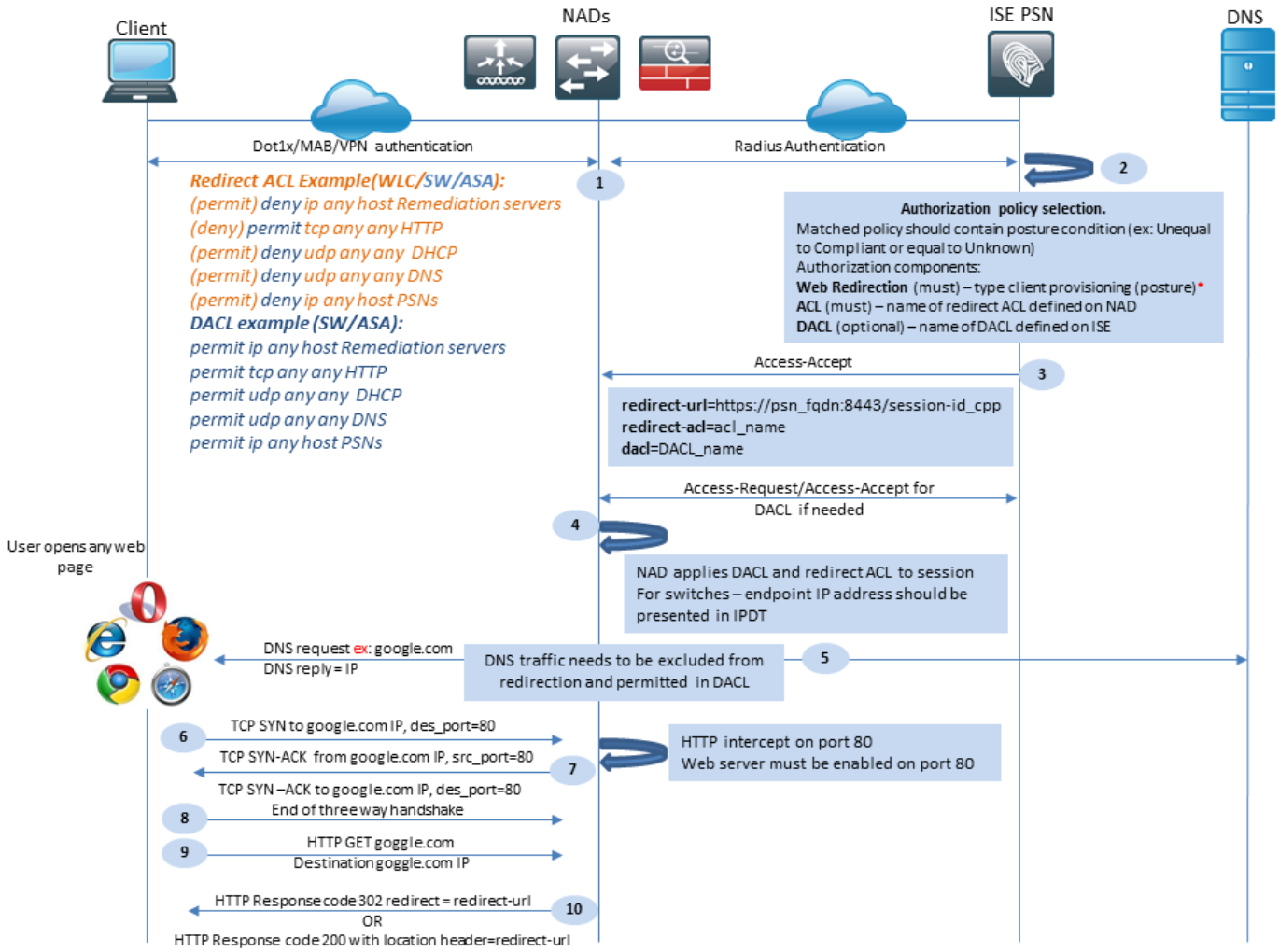


Figura 1-1

Etapa 1. A autenticação é a primeira etapa do fluxo, pode ser dot1x, MAB ou VPN.

Etapa 2. O ISE precisa escolher uma política de autenticação e autorização para o usuário. No cenário de postura, a política de autorização escolhida deve conter uma referência ao status da

postura, que inicialmente deve ser desconhecido ou não aplicável. Para cobrir estes dois casos, podem ser utilizadas condições com um estado de postura que permita uma conformidade desigual.

O perfil de autorização escolhido deve conter informações sobre o redirecionamento:

- Redirecionamento da Web - Para o caso de postura, o tipo de redirecionamento da Web deve ser especificado como provisionamento de cliente (postura).
- ACL- Esta seção precisa conter o nome da ACL que está configurado no lado NAD. Essa ACL é usada para instruir o NAD sobre qual tráfego deve ignorar o redirecionamento e qual deve ser realmente redirecionado.
- DACL- Pode ser usado em conjunto com redirect access-list, mas você deve ter em mente que diferentes plataformas processam DACL e Redirect ACLs em uma ordem diferente.

Por exemplo, o ASA sempre processa a DACL antes de redirecionar a ACL. Ao mesmo tempo, algumas plataformas de switch o processam da mesma forma que o ASA, e outras plataformas de switch processam primeiro a ACL de redirecionamento e verificam a ACL de DACL/Interface se o tráfego precisar ser descartado ou permitido.

> **Observação**: depois de ativar a opção de redirecionamento da Web no perfil de autorização, o portal de destino para redirecionamento deverá ser escolhido.

Etapa 3. O ISE retorna Access-Accept com atributos de autorização. A URL de redirecionamento nos atributos de autorização é gerada automaticamente pelo ISE. Ele contém estes componentes:

- FQDN do nó ISE no qual a autenticação ocorreu. Em alguns casos, o FQDN dinâmico pode ser substituído pela configuração do perfil de autorização (IP estático/nome do host/FQDN) na seção Redirecionamento da Web. Se o valor estático for usado, ele deverá apontar para o mesmo nó do ISE em que a autenticação foi processada. No caso do Balanceador de Carga (LB), esse FQDN pode apontar para LB VIP, mas apenas no caso de LB estar configurado para unir conexões Radius e SSL.
- Porta- O valor da porta é obtido da configuração do portal de destino.
- ID da sessão - Esse valor é obtido pelo ISE a partir da ID da sessão de auditoria do par Cisco AV apresentada em Solicitação de acesso. O valor em si é gerado dinamicamente pelo NAD.
- ID do portal - Identificador de um portal de destino no lado do ISE.

Etapa 4. O NAD aplica uma política de autorização à sessão. Além disso, se o DACL estiver configurado, seu conteúdo será solicitado antes da aplicação das políticas de autorização.

Considerações importantes:

- Todos os NADs- Device devem ter uma ACL configurada localmente com o mesmo nome daquela recebida em Access-Accept como redirect-acl.
- Switches - O endereço IP do cliente deve ser apresentado na saída de `show authentication session interface details` para aplicar com êxito o redirecionamento e as ACLs. O endereço IP do cliente é aprendido pelo recurso de rastreamento de dispositivo IP (IPDT).

Etapa 5. O cliente envia uma solicitação DNS para o FQDN que é inserido no navegador da Web. Nesse estágio, o tráfego DNS deve ignorar o redirecionamento e o endereço IP correto deve ser retornado pelo servidor DNS.

Etapa 6. O cliente envia TCP SYN para o endereço IP que é recebido na resposta DNS. O endereço IP origem no pacote é o IP do cliente e o endereço IP destino é o IP do recurso solicitado. A porta de destino é igual a 80, exceto nos casos em que um proxy HTTP direto é configurado no navegador da Web do cliente.

Etapa 7.NAD intercepta solicitações de clientes e prepara pacotes SYN-ACK com um IP de origem igual ao IP de recurso solicitado, o IP de destino igual ao IP de cliente e a porta de origem igual a 80.

Considerações importantes:

- Os NADs devem ter um servidor HTTP em execução na porta em que o cliente envia solicitações. Por padrão, é a porta 80.
- Se o cliente usar um servidor Web proxy HTTP direto, o servidor HTTP deverá ser executado na porta proxy no NAS. Este cenário está fora do escopo deste documento.
- Nos casos em que o NAD não tem um endereço IP local no cliente, a sub-rede SYN-ACK é enviada com a tabela de roteamento NAD (geralmente sobre a interface de gerenciamento). Neste cenário, o pacote é roteado pela infraestrutura de L3 e deve ser roteado de volta para o cliente por um dispositivo de upstream de L3. Se o dispositivo L3 for um firewall stateful, uma exceção adicional deverá ser dada para esse roteamento assimétrico.

Etapa 8. O cliente conclui o handshake triplo TCP com ACK.

Etapa 9. O HTTP GET para o recurso de destino é enviado por um cliente.

Etapa 10. O NAD retorna um URL de redirecionamento para o cliente com o código HTTP 302 (página movida), em alguns NADs, o redirecionamento pode ser retornado dentro da mensagem HTTP 200 OK no cabeçalho do local.

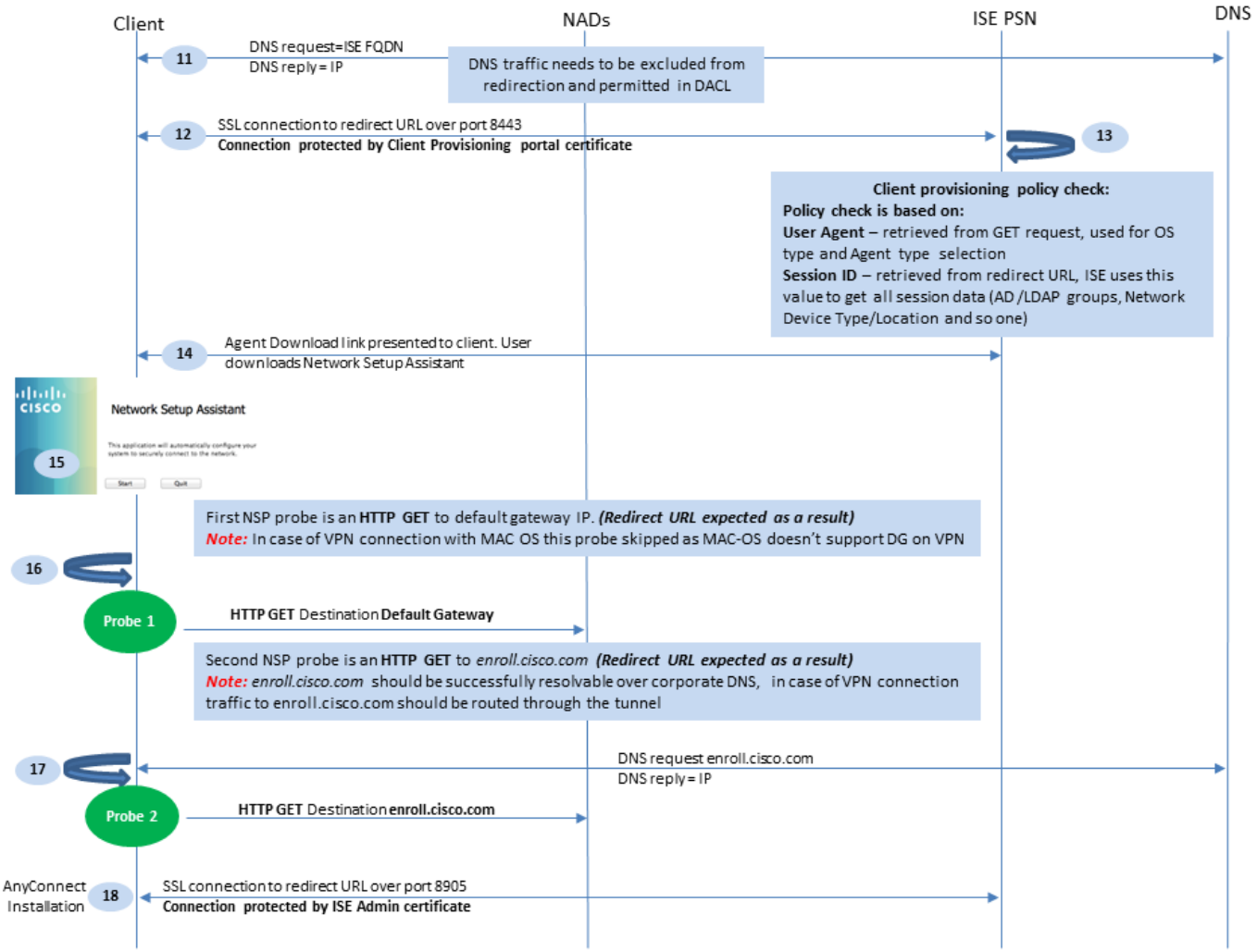


Figura 1-2

Etapa 11. O cliente envia uma solicitação DNS para o FQDN da URL de redirecionamento. O FQDN deve ser resolvível no lado do servidor DNS.

Etapa 12. A conexão SSL na porta recebida na URL de redirecionamento está estabelecida (padrão 8443). Esta conexão é protegida por um certificado de portal do lado do ISE. O Client Provisioning Portal (CPP) é apresentado ao usuário.

Etapa 13.Antes de fornecer uma opção de download para o cliente, o ISE deve selecionar a política de provisionamento do cliente de destino (CP). O Sistema Operacional (SO) do cliente detectado do agente de usuário do navegador e outras informações necessárias para a seleção de política CPP são recuperados da sessão de autenticação (como grupos AD/LDAP e assim por diante). O ISE conhece a sessão de destino a partir da ID da sessão apresentada na URL de redirecionamento.

Etapa 14. O link de download do Network Setup Assistant (NSA) é retornado ao cliente. O cliente faz o download do aplicativo.

**Observação**: normalmente, você pode ver a NSA como parte do fluxo de BYOD para Windows e Android, mas também esse aplicativo pode ser usado para instalar o Anyconnect ou seus componentes do ISE.

Etapa 15.O usuário executa o aplicativo NSA.

Etapa 16. O NSA envia a primeira sonda de descoberta - HTTP /auth/discovery para o gateway padrão. Como resultado, a NSA espera a URL de redirecionamento.

> **Observação**: para conexões via VPN em dispositivos MAC OS, esse teste é ignorado, pois o MAC OS não tem um gateway padrão no adaptador VPN.

Etapa 17.O NSA envia uma segunda sonda se a primeira falhar. A segunda sonda é um HTTP GET /auth/discovery para `enroll.cisco.com`. Este FQDN deve ser resolvível com êxito pelo servidor DNS. Em um cenário de VPN com um túnel dividido, o tráfego para `enroll.cisco.com` deve ser roteado através do túnel.

Etapa 18. Se qualquer uma das sondas for bem-sucedida, o NSA estabelece uma conexão SSL na porta 8905 com informações obtidas do redirect-url. Esta conexão é protegida pelo certificado de administrador do ISE. Dentro dessa conexão, a NSA faz o download do Anyconnect.

Considerações importantes:

- Antes da versão 2.2 do ISE, a comunicação SSL na porta 8905 é um requisito para postura.
- Para evitar avisos de certificado, os certificados do portal e do administrador devem ser confiáveis no lado do cliente.
- Em implantações de ISE com várias interfaces, as interfaces diferentes de G0 podem ser vinculadas ao FQDN de forma diferente do FQDN do sistema (com o uso de `ip host` CLI). Isso pode causar problemas com a validação do Nome da Entidade (SN)/Nome Alternativo da Entidade (SAN). Se o cliente for redirecionado para o FQDN da interface G1, por exemplo, o FQDN do sistema pode diferir do FQDN na URL de redirecionamento do certificado de comunicação 8905. Como solução para esse cenário, você pode adicionar FQDNs de interfaces adicionais nos campos SAN do certificado do administrador ou pode usar um curinga no certificado do administrador.

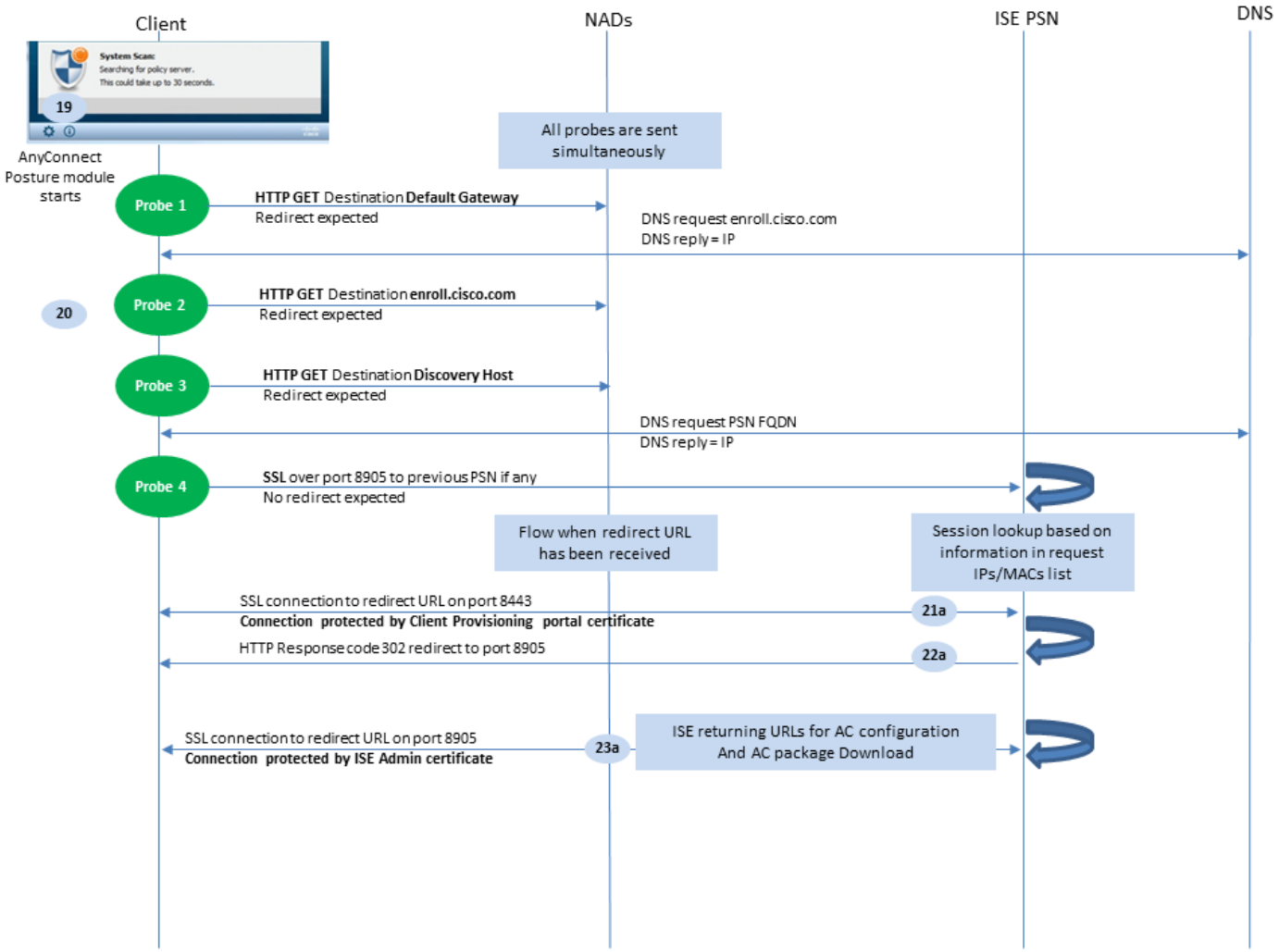


Figura 1-3

Etapa 19.O processo de postura do Anyconnect ISE é iniciado.

O módulo de postura do Anyconnect ISE inicia em qualquer uma destas situações:

- Após a instalação
- Após a alteração do valor do gateway padrão
- Após o evento de login do usuário do sistema
- Após o evento de alimentação do sistema

Etapa 20. Neste estágio, o módulo de postura do Anyconnect ISE inicia a detecção do servidor de política. Isso é realizado com uma série de testes que são enviados ao mesmo tempo pelo módulo de postura do Anyconnect ISE.

- Teste 1 - HTTP get /auth/discovery para o IP do gateway padrão. Lembre-se de que os dispositivos MAC OS não têm um gateway padrão no adaptador VPN. O resultado esperado para o teste é redirect-url.
- Sonda 2 - HTTP GET /auth/discovery para enroll.cisco.com. Este FQDN precisa ser resolvível com êxito pelo servidor DNS. Em um cenário de VPN com um túnel dividido, o tráfego para enroll.cisco.com deve ser roteado através do túnel. O resultado esperado para o teste é redirect-url.
- Teste 3 - HTTP get /auth/discovery para o host de descoberta. O valor do host de descoberta é retornado do ISE durante a instalação no perfil de postura de CA. O resultado esperado

para o teste é redirect-url.

- Sonda 4 - HTTP GET /auth/status sobre SSL na porta 8905 para PSN anteriormente conectado. Esta solicitação contém informações sobre IPs de clientes e lista de MACs para consulta de sessão no lado do ISE. Esse problema não é apresentado durante a primeira tentativa de postura. A conexão é protegida por um certificado de administrador ISE. Como resultado desse teste, o ISE pode retornar o ID da sessão de volta ao cliente se o nó onde o teste foi aterrado for o mesmo nó onde o usuário foi autenticado.

**Observação**: como resultado desse teste, a postura pode ser realizada com êxito mesmo sem o redirecionamento de trabalho em algumas circunstâncias. A postura bem-sucedida sem redirecionamento requer que a PSN atual que autenticou a sessão seja a mesma que a PSN conectada anteriormente com êxito. Lembre-se de que, antes do ISE 2.2, uma postura bem-sucedida sem redirecionamento é mais uma exceção do que uma regra.

As próximas etapas descrevem o processo de postura no caso em que a URL de redirecionamento é recebida (fluxo marcado com a letra a) como resultado de um dos testadores.

Etapa 21. O módulo de postura do AnyConnect ISE estabelece uma conexão com o portal de provisionamento do cliente com o uso de um URL recuperado durante a fase de descoberta. Nesse estágio, o ISE faz a validação da política de provisionamento do cliente mais uma vez com o uso das informações das sessões autenticadas.

Etapa 22.Se a política de provisionamento do cliente for detectada, o ISE retornará o redirecionamento para a porta 8905.

Etapa 23. O agente estabelece uma conexão com o ISE pela porta 8905. Durante essa conexão, o ISE retorna URLs para o perfil de postura, módulo de conformidade e atualizações do anyconnect.

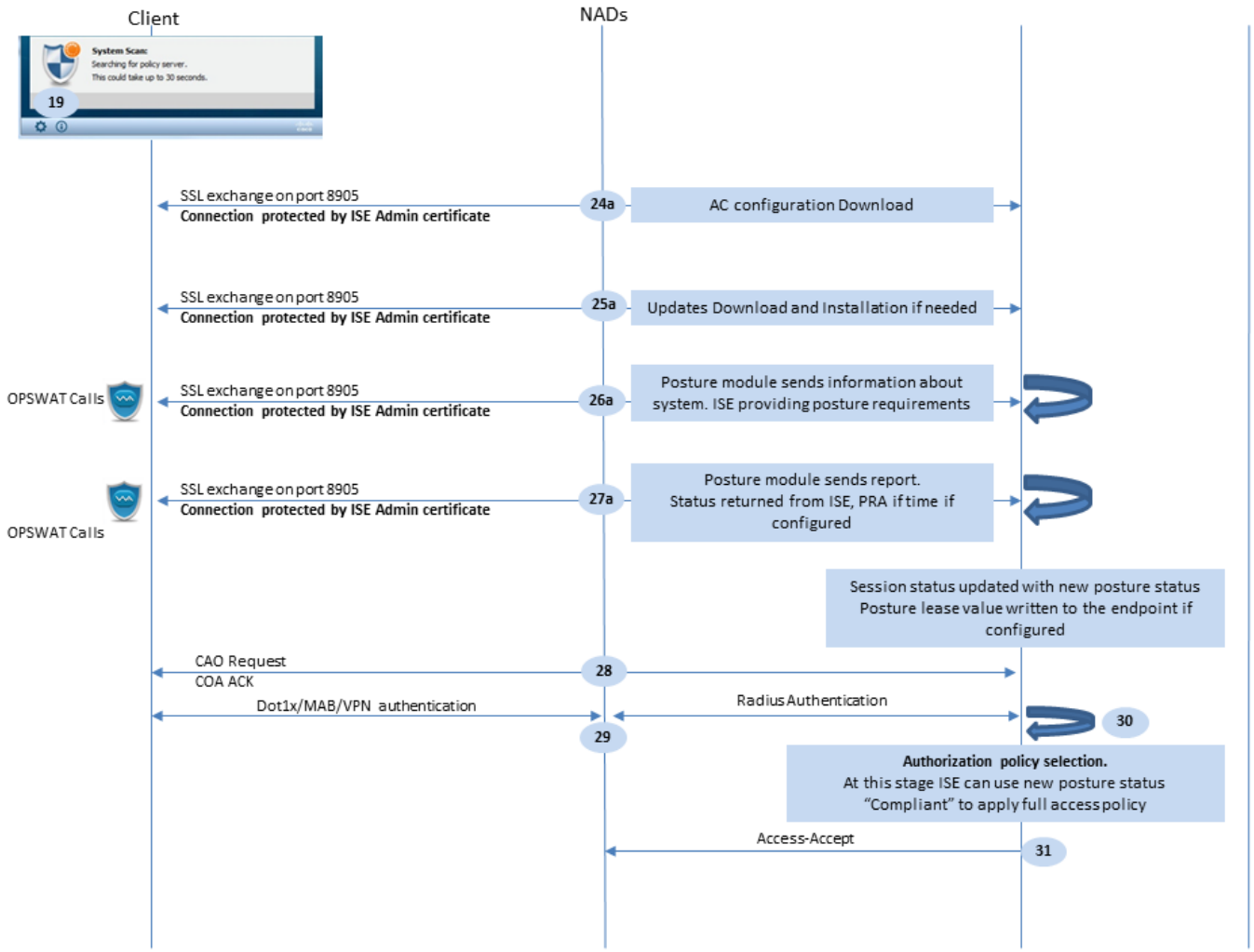


Figura 1-4

Etapa 24.Faça o download da configuração do módulo de postura do ISE AC a partir do ISE.

Etapa 25.Atualiza o download e a instalação, se necessário.

Etapa 26. O módulo de postura AC ISE coleta informações iniciais sobre o sistema (como versão do SO, produtos de segurança instalados e sua versão de definição). Neste estágio, o módulo de postura do ISE AC envolve a API OPSWAT para coletar informações sobre produtos de segurança. Os dados coletados são enviados ao ISE. Como resposta a essa solicitação, o ISE fornece uma lista de requisitos de postura. A lista de requisitos é selecionada como resultado do processamento da política de postura. Para corresponder à política correta, o ISE usa a versão do SO do dispositivo (presente na solicitação) e o valor de ID da sessão para selecionar outros atributos necessários (grupos AD/LDAP). O valor de ID da sessão também é enviado pelo cliente.

Etapa 27. Nesta etapa, o cliente envolve chamadas OPSWAT e outros mecanismos para verificar os requisitos de postura. O relatório final com a lista de requisitos e seu status são enviados ao ISE. O ISE precisa tomar a decisão final sobre o status de conformidade do endpoint. Se o ponto de extremidade estiver marcado como não compatível nesta etapa, um conjunto de ações de correção será retornado. Para o endpoint em conformidade, o ISE grava o status de conformidade na sessão e também coloca o último carimbo de data/hora de postura nos atributos do endpoint se o Posture Lease estiver configurado. O resultado da postura é enviado de volta ao endpoint. No caso de Reavaliação de postura (PRA), o tempo para PRA também é colocado pelo ISE nesse pacote.

Em um cenário não compatível, leve em conta estes pontos:

- Algumas ações de correção (como mensagens de texto de exibição, correção de links, correção de arquivos e outras) são executadas pelo próprio agente de postura.
- Outros tipos de remediação (como AV. AS, WSUS e SCCM) exigem a comunicação da API do OPSWAT entre o agente de postura e o produto de destino. Neste cenário, o agente de postura apenas envia uma solicitação de reparo ao produto. A correção em si é feita diretamente pelos produtos de segurança.

**Observação**: quando o produto de segurança tiver que se comunicar com recursos externos (servidores de Atualização Interna/Externa), você deve garantir que essa comunicação seja permitida em Redirect-ACL/DACL.

Etapa 28.O ISE envia uma solicitação COA ao NAD que deve disparar uma nova autenticação para o usuário. A NAD deve confirmar esta solicitação pelo COA ACK. Tenha em mente que, para os casos de VPN, o envio de COA é usado, portanto, nenhuma nova solicitação de autenticação é enviada. Em vez disso, o ASA remove parâmetros de autorização anteriores (URL de redirecionamento, ACL de redirecionamento e DACL) da sessão e aplica novos parâmetros da solicitação COA.

Etapa 29.Nova solicitação de autenticação para o usuário.

Considerações importantes:

- Normalmente para o Cisco NAD COA, a reautenticação é usada pelo ISE e isso instrui o NAD a iniciar uma nova solicitação de autenticação com o ID da sessão anterior.
- No lado do ISE, o mesmo valor de ID de sessão é uma indicação de que os atributos de sessão coletados anteriormente devem ser reutilizados (status de reclamação no nosso caso) e um novo perfil de autorização baseado nesses atributos deve ser atribuído.
- No caso de uma alteração de ID de sessão, essa conexão é tratada como nova e o processo de postura completa é reiniciado.
- A fim de evitar a repetição em cada alteração de id de sessão, um aluguel de postura pode ser usado. Neste cenário, as informações sobre o status da postura são armazenadas nos atributos do ponto final, que permanecem no ISE mesmo se a ID da sessãoé alterado.

Etapa 30. Uma nova política de autorização é selecionada no lado do ISE com base no status da postura.

Etapa 31. Access-Accept com novos atributos de autorização é enviado ao NAD.

O próximo fluxo descreve o cenário quando a URL de redirecionamento não é recuperada (marcada com a letra b) por qualquer sonda de postura e o PSN conectado anteriormente foi consultado pela última sonda. Todos os passos aqui são exatamente os mesmos do caso com o URL de redirecionamento, exceto a repetição que é retornada pela PSN como resultado da Sonda 4. Se esse teste foi aterrado no mesmo PSN que é um proprietário da sessão de autenticação atual, a reprodução conterá o valor de ID da sessão que será usado mais tarde pelo agente de postura para concluir o processo. Caso o headend conectado anteriormente não seja o mesmo que o proprietário da sessão atual, a pesquisa de sessão falha e uma resposta vazia é retornada ao módulo de postura do ISE AC. Como resultado final, a No Policy Server Detected é retornada ao usuário final.

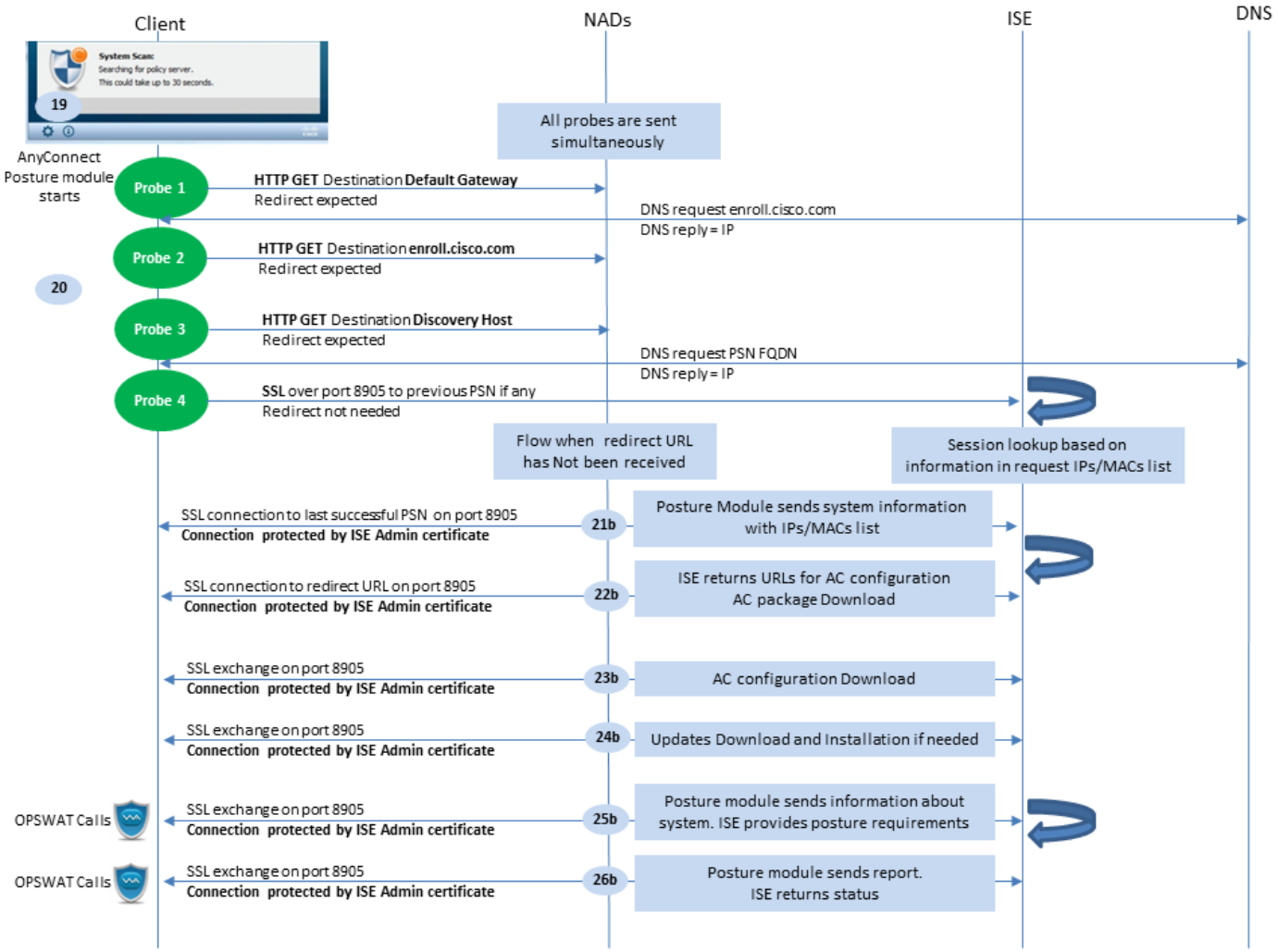


Figura 1-5

# Fluxo de postura no ISE 2.2

O ISE 2.2 oferece suporte a estilos antigos e novos simultaneamente. Esta é a explicação detalhada para o novo fluxo:

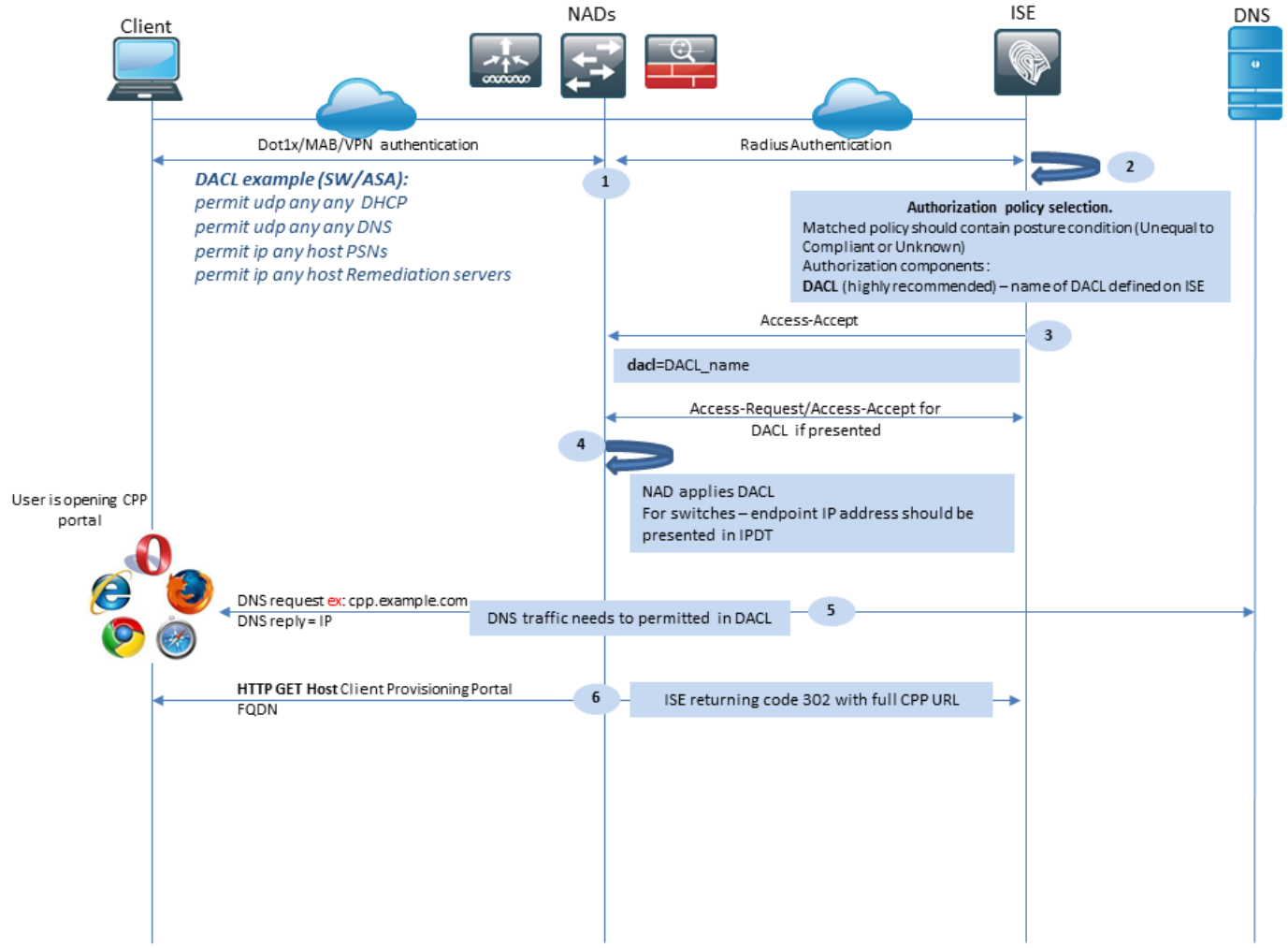


Figura 2-1

Etapa 1.A autenticação é a primeira etapa do fluxo. Pode ser dot1x, MAB ou VPN.

Etapa 2.O ISE deve escolher a política de autenticação e autorização para o usuário. Em postura, o cenário escolhido para a política de autorização deve conter uma referência ao status da postura, que inicialmente deve ser desconhecido ou não aplicável. Para cobrir estes dois casos, podem ser utilizadas condições com um estado de postura que permita uma conformidade desigual. Para uma postura sem redirecionamento, não há necessidade de usar qualquer configuração de Redirecionamento da Web no perfil de autorização. Você ainda pode considerar o uso de uma DACL ou de uma ACL de espaço aéreo para limitar o acesso do usuário no estágio em que o status da postura não está disponível.

Etapa 3.O ISE retorna Access-Accept com atributos de autorização.

Etapa 4. Se o nome da DACL for retornado em Access-Accept, o NAD iniciará o download do conteúdo da DACL e aplicará o perfil de autorização à sessão após sua obtenção.

Etapa 5. A nova abordagem pressupõe que o redirecionamento não é possível, portanto, o usuário deve inserir o FQDN do portal de provisionamento do cliente manualmente. O FQDN do portal CPP deve ser definido na configuração do portal no lado do ISE. Da perspectiva do servidor DNS, o registro A deve apontar para o servidor ISE com a função PSN habilitada.

Etapa 6. O cliente envia HTTP para chegar ao FQDN do portal de provisionamento do cliente, essa solicitação é analisada no lado do ISE e a URL completa do portal é retornada de volta ao

cliente.

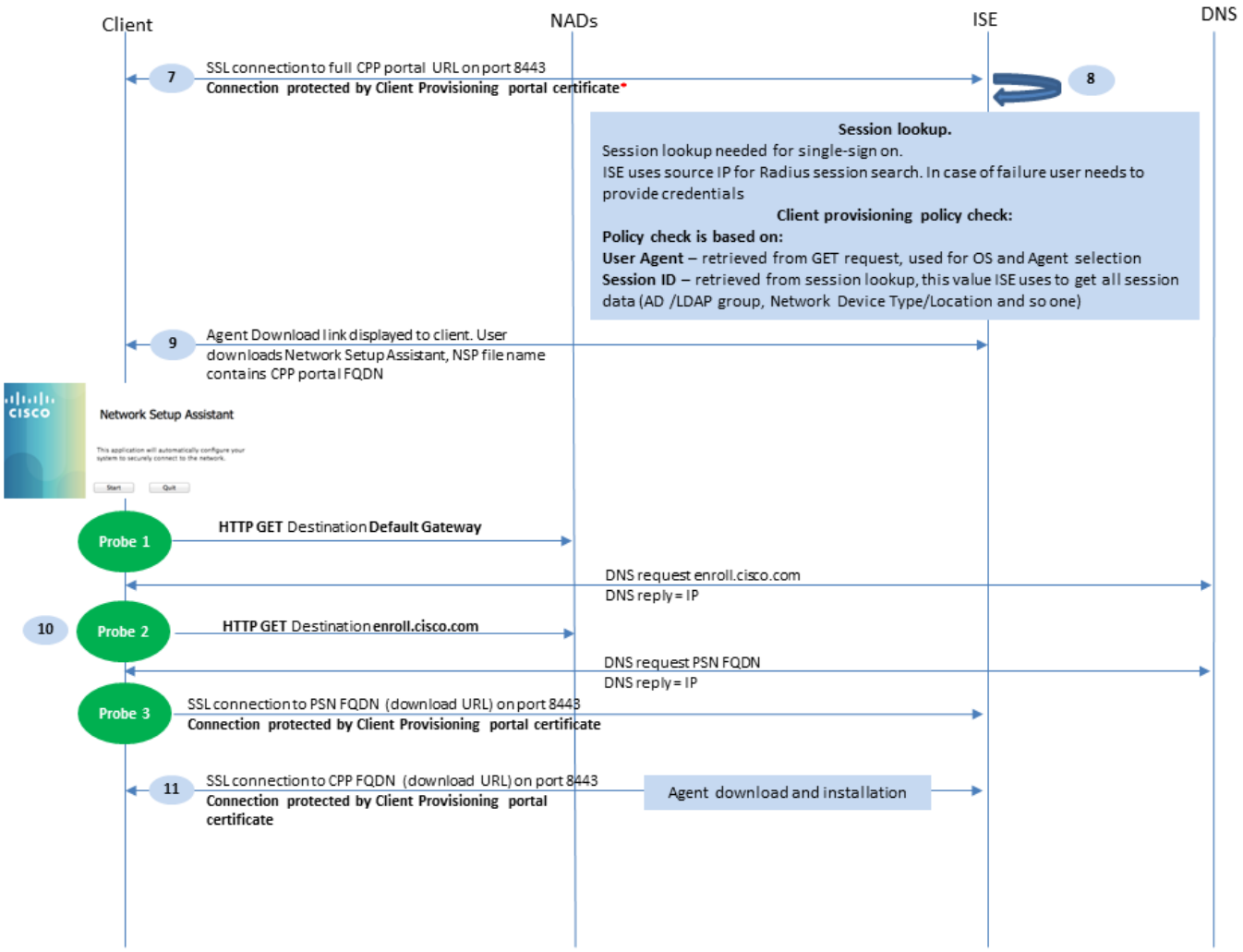


Figura 2-2

Etapa 7.A conexão SSL na porta recebida no URL de redirecionamento está estabelecida (padrão 8443). Esta conexão é protegida por um certificado de portal do lado do ISE. O Client Provisioning Portal (CPP) é apresentado ao usuário.

Etapa 8. Nesta etapa, dois eventos ocorrem no ISE:

- Logon único (SSO) - O ISE tenta pesquisar a autenticação bem-sucedida anterior. O ISE usa o endereço IP origem do pacote como um filtro de pesquisa para sessões de raio ao vivo.

**Observação**: a sessão é recuperada com base em uma correspondência entre o IP de origem no pacote e o endereço IP com quadro na sessão. O endereço IP enquadrado é normalmente recuperado pelo ISE a partir das atualizações de contabilização provisórias, portanto, é necessário ter a contabilização habilitada no lado NAD. Além disso, você deve lembrar que o SSO só é possível no nó que possui a sessão. Se, por exemplo, a sessão for autenticada no PSN 1, mas o próprio FQDN apontar para o PSN2, o mecanismo SSO falhará.

- Consulta da política de provisionamento do cliente - no caso de um SSO bem-sucedido, o ISE pode usar dados de sessão autenticada e agente de usuário do navegador do cliente. No

caso de um SSO malsucedido, o usuário deve fornecer as credenciais e, depois que as informações de autenticação do usuário forem recuperadas dos repositórios de Identidade interna e externa (grupos AD/LDAP/Interno), elas poderão ser usadas para verificação da política de provisionamento do cliente.

**Observação**: devido ao bug da Cisco ID CSCvd11574**, você pode ver um erro no momento da seleção da política de provisionamento do cliente para os casos não-SSO quando o usuário externo é membro de vários grupos AD/LDAP adicionados na configuração do armazenamento de identidade externo.** O defeito mencionado é fixo que começa no ISE 2.3 FCS e a correção requer o uso de CONTAINS em condição com o grupo AD em vez de EQUAL.

Etapa 9. Após a seleção da política de provisionamento do cliente, o ISE exibe a URL de download do agente para o usuário. Depois de clicar no NSA de download, o aplicativo é enviado para o usuário. O nome de arquivo NSA contém o FQDN do portal CPP.

Etapa 10. Nesta etapa, o NSA executa testes para estabelecer uma conexão com o ISE. Dois testes são clássicos, e o terceiro é projetado para permitir a descoberta do ISE em ambientes sem redirecionamento de url.

- O NSA envia a primeira sonda de descoberta - HTTP /auth/discovery para o gateway padrão. Como resultado, a NSA espera a URL de redirecionamento.
- O NSA enviará uma segunda sonda se a primeira falhar. A segunda sonda é um HTTP GET /auth/discovery para enroll.cisco.com. Este FQDN deve ser resolvível com êxito pelo servidor DNS. Em um cenário de VPN com um túnel dividido, o tráfego para enroll.cisco.com deve ser roteado através do túnel.
- O NSA envia a terceira sonda pela porta do portal CPP para o FQDN do portal de provisionamento do cliente. Essa solicitação contém informações sobre a ID de sessão do portal que permite que o ISE identifique quais recursos devem ser fornecidos.

Etapa 11. A NSA faz o download do Anyconnect e/ou de módulos específicos. O processo de download é feito pela porta do portal de provisionamento do cliente.

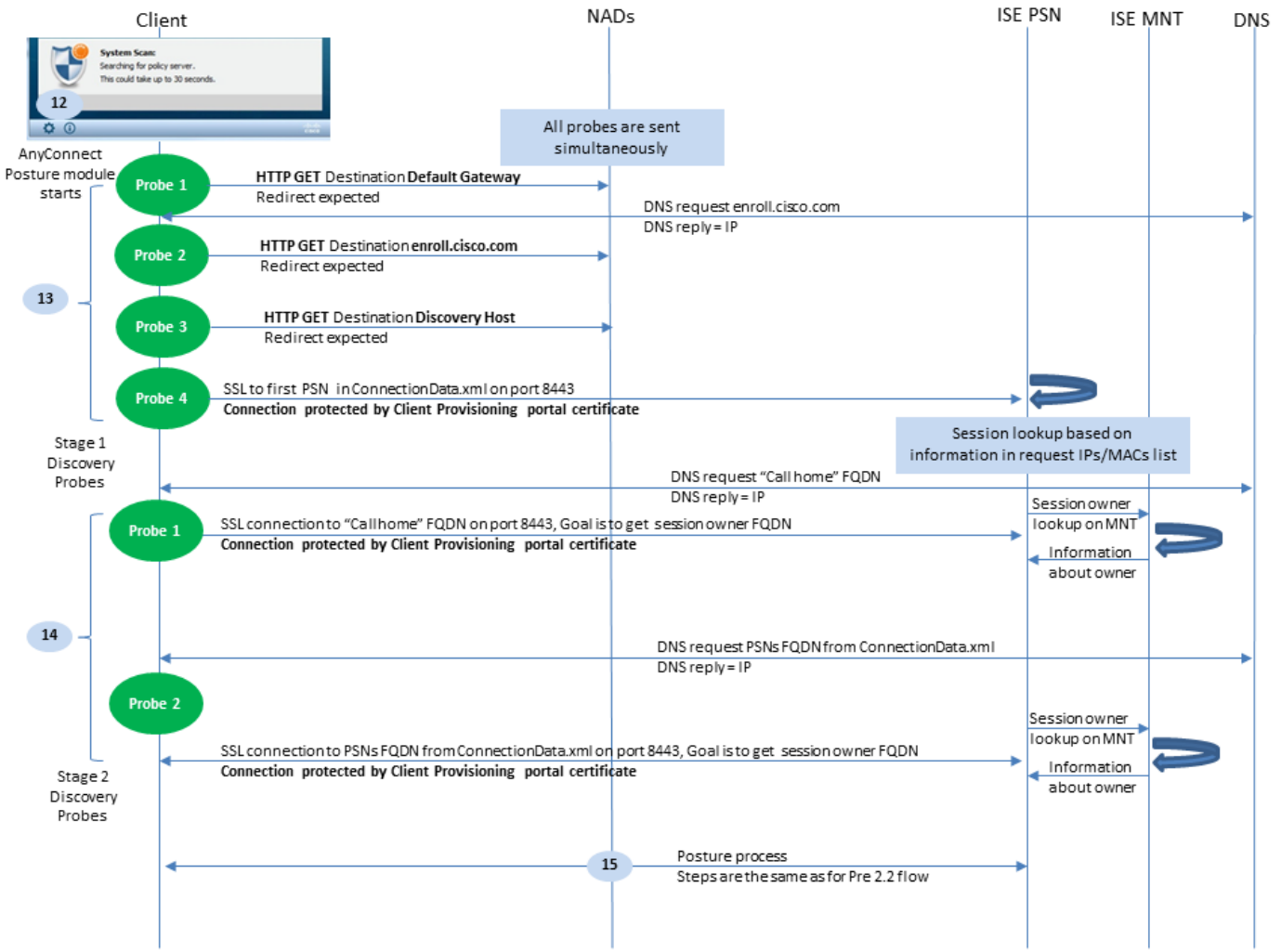


Figura 2-3

Etapa 12. No ISE 2.2, o processo de postura é dividido em duas etapas. O primeiro estágio contém um conjunto de testes de descoberta de postura tradicional para suportar compatibilidade retroativa com implantações que dependem do redirecionamento de url.

Etapa 13. O primeiro estágio contém todas as sondas tradicionais de descoberta de postura. Para obter mais detalhes sobre os testadores, reveja a Etapa 20. no fluxo de postura anterior ao ISE 2.2.

Etapa 14.O estágio dois contém dois testes de detecção que permitem que o módulo de postura do ISE AC estabeleça uma conexão com a PSN, onde a sessão é autenticada em ambientes onde o redirecionamento não é suportado. Durante o estágio dois, todos os testes são sequenciais.

- Sonda 1 - Durante a primeira sonda, o módulo de postura AC ISE tenta estabelecer com IP/FQDNs da 'Lista de Call Home'. Uma lista dos alvos da sonda deve ser configurada no perfil de postura AC no lado ISE. Você pode definir IPs/FQDNs separados por vírgulas, com dois-pontos você pode definir o número da porta para cada destino do Call Home. Essa porta deve ser igual à porta em que o portal de provisionamento do cliente é executado. No lado do cliente, as informações sobre os servidores do call home estão localizadas em ISEPostureCFG.xml, este arquivo pode ser encontrado na pasta - C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.
  Caso o destino do call home não seja o proprietário da sessão, uma pesquisa para o

proprietário é necessária nesse estágio. O módulo de postura AC ISE instrui o ISE a iniciar a pesquisa do proprietário com o uso de um URL de destino especial - /auth/ng-discovery requisição. Ele também contém a lista de IPs e MACs do cliente. Depois que essa mensagem é recebida pela sessão PSN, uma pesquisa é feita localmente pela primeira vez (essa pesquisa usa IPs e MACs da solicitação enviada pelo módulo de postura AC ISE). Se a sessão não for encontrada, o PSN iniciará uma consulta de nó MNT. Essa solicitação contém apenas a lista de MACs; como resultado, o FQDN do proprietário deve ser obtido do MNT. Depois disso, a PSN retorna o FQDN dos proprietários ao cliente. A próxima solicitação do cliente é enviada ao FQDN do proprietário da sessão com autenticação/status na URL e lista de IPs e MACs.

- Sonda 2 - Neste estágio, o módulo de postura AC ISE tenta FQDNs PSN localizados em ConnectionData.xml. Esse arquivo pode ser encontrado em C:\Users\ . O módulo de postura AC ISE cria esse arquivo após a primeira tentativa de postura. O arquivo contém uma lista de FQDNs de PSNs do ISE. O conteúdo da lista pode ser atualizado dinamicamente durante as próximas tentativas de conexão. O objetivo final desta sonda é obter o FQDN do proprietário da sessão atual. A implementação é idêntica à Sonda 1. com a única diferença na seleção do destino da sonda.
  O próprio arquivo está localizado na pasta do usuário atual, caso o dispositivo seja usado por vários usuários. Um usuário diferente não pode usar as informações deste arquivo. Isso pode levar os usuários ao problema do ovo e da galinha em ambientes sem redirecionamento quando os alvos do Call Home não são especificados.

Etapa 15. Depois que as informações sobre o proprietário da sessão são obtidas, todas as etapas subsequentes são idênticas ao fluxo anterior ao ISE 2.2.

# Configurar

Para este documento, o ASAv é usado como um dispositivo de acesso à rede. Todos os testes são realizados com postura sobre VPN. A configuração do ASA para postura sobre suporte VPN está fora do escopo do documento. Para obter mais detalhes, consulte Exemplo de Configuração de Postura de VPN com ISE do ASA Versão 9.2.1.

> **Observação**: para a implantação com usuários de VPN, a configuração recomendada é a postura baseada em redirecionamento. A configuração de callhomelist não é recomendada. Para todos os usuários não baseados em vpn, assegure-se de que a DACL seja aplicada de modo que eles não se comuniquem com a PSN onde a postura é configurada.

## Diagrama de Rede

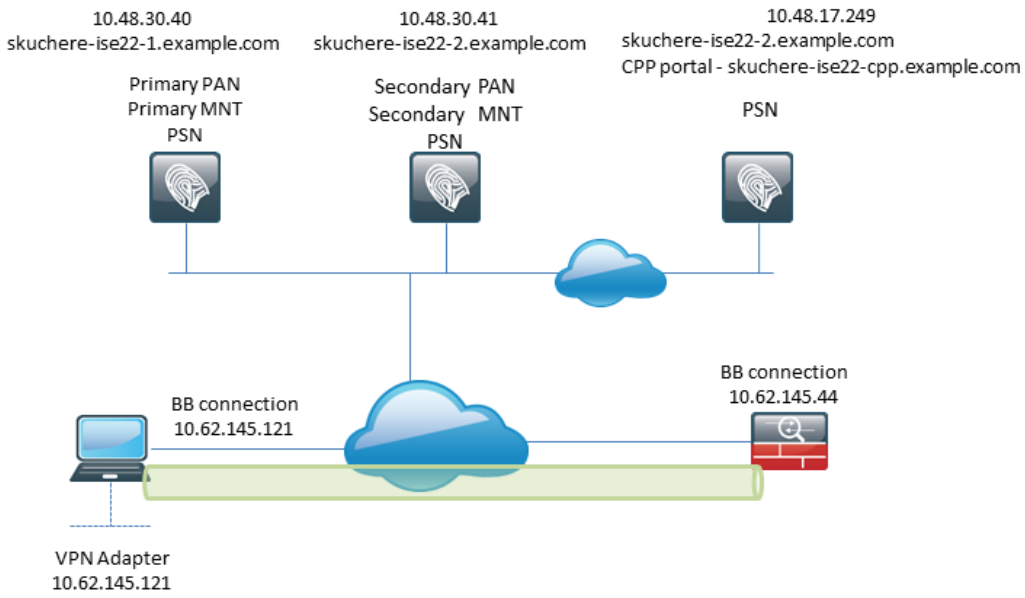


Figura 3-1

Essa topologia é usada em testes. Com o ASA, é possível simular facilmente o cenário quando o mecanismo SSO para o portal de provisionamento do cliente falha no lado PSN, devido ao recurso NAT. No caso de um fluxo de postura regular sobre VPN, o SSO deve funcionar bem, já que o NAT normalmente não é aplicado para IPs de VPN quando os usuários entram na rede corporativa.

## Configurações

### Configuração de provisionamento do cliente

Estas são as etapas para preparar a configuração do Anyconnect.

Etapa 1. Download do pacote do Anyconnect. O pacote do Anyconnect não está disponível para download direto do ISE, portanto, antes de começar, verifique se o AC está disponível em seu PC. Este link pode ser usado para download AC - https://www.cisco.com/site/us/en/products/security/secure-client/index.html. Neste documento, anyconnect-win-4.4.00243-webdeploy-k9.pkg pacote é usado.

Etapa 2. Para carregar o pacote AC no ISE, navegue até Policy > Policy Elements > Results > Client Provisioning > Resourcese clique em Add. Escolha Recursos do agente no disco local. Na nova janela, escolha Cisco Provided Packages, clique em browse e escolha o encapsulamento AC no seu PC.

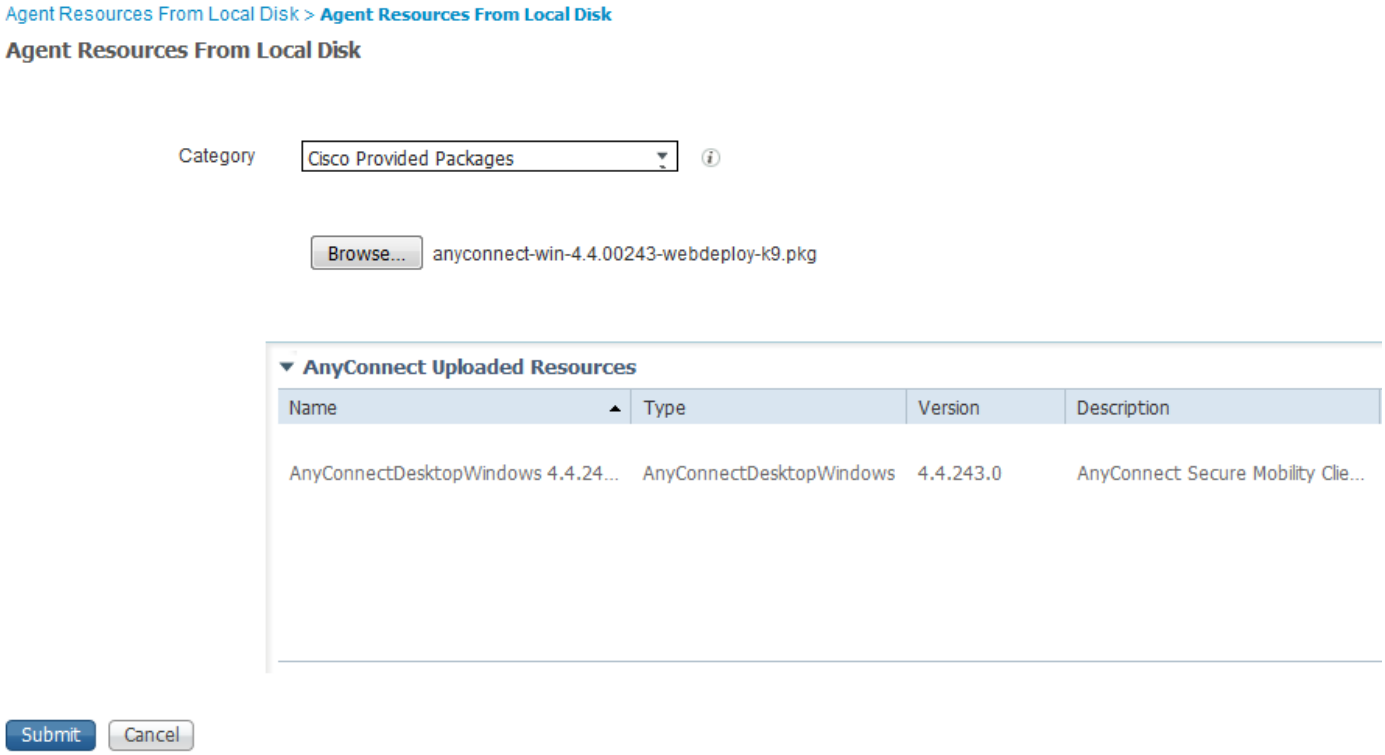


Figura 3-2

Clique em Submit para concluir a importação.

Etapa 3. O módulo de conformidade deve ser carregado no ISE. Na mesma página, clique em Add e escolha a opção Agent resources from Cisco site. Na lista de recursos, você deve verificar um módulo de conformidade. Para este documento, o AnyConnectComplianceModuleWindows 4.2.508.0 é usado o módulo de conformidade.

Etapa 4. Agora o perfil de postura AC deve ser criado. Clique em Add e escolha a opção NAC agent or Anyconnect posture profile.

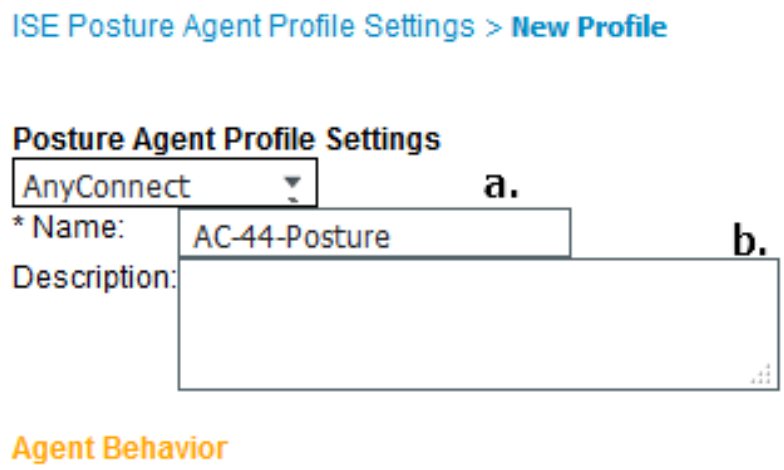


Figura 3-3

- Escolha o tipo de perfil. O AnyConnect deve ser usado para esse cenário.
- Especifique o nome do perfil. Navegue até a página Posture Protocol do perfil.

Posture Protocol

| Parameter | Value | Notes |
|---|---|---|
| PRA retransmission time | 120 secs | |
| Discovery host | | |
| * Server name rules | * a. | need to be blank by default to force admin to enter a value. "*" means agent will connect to all |
| Call Home List | skuchere-ise22-2.examp b. | List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal) |
| Back-off Timer | 30 secs | Enter value of back-off timer in seconds, the supported range is between 10s - 600s. |

Figura 3-4

- Especificar o Server Name Rules, este campo não pode estar vazio. O campo pode conter FQDN com caractere curinga que restringe a conexão do módulo de postura AC ISE a PSNs do namespace apropriado. Coloque uma estrela se for necessário permitir qualquer FQDN.
- Os nomes e IPs especificados aqui estão em uso durante o estágio 2 da descoberta de postura. Você pode separar nomes por vírgula, assim como números de porta podem ser adicionados após FQDN/IP com o uso dos dois-pontos. Caso a AC implantada fora da banda (não do portal de provisionamento do cliente ISE) com o uso do GPO ou qualquer outro sistema de provisionamento de software, a presença de endereços Call Home se torna essencial, pois essa é apenas uma prova que pode acessar o ISE PSN com êxito. Isso significa que, no caso de provisionamento de CA fora da banda, o administrador deve criar um perfil de postura do ISE de CA com o uso do editor de perfil de CA e provisionar esse arquivo junto com a instalação de CA.

**Observação**: lembre-se de que a presença de endereços Call home é essencial para PCs multiusuário. Revise a Etapa 14. em Fluxo de postura pós-ISE 2.2.

Etapa 5.Criar uma configuração de CA. Navegue até Policy > Policy Elements > Results > Client Provisioning > Resources, clicar Add, em seguida escolha AnyConnect Configuration.

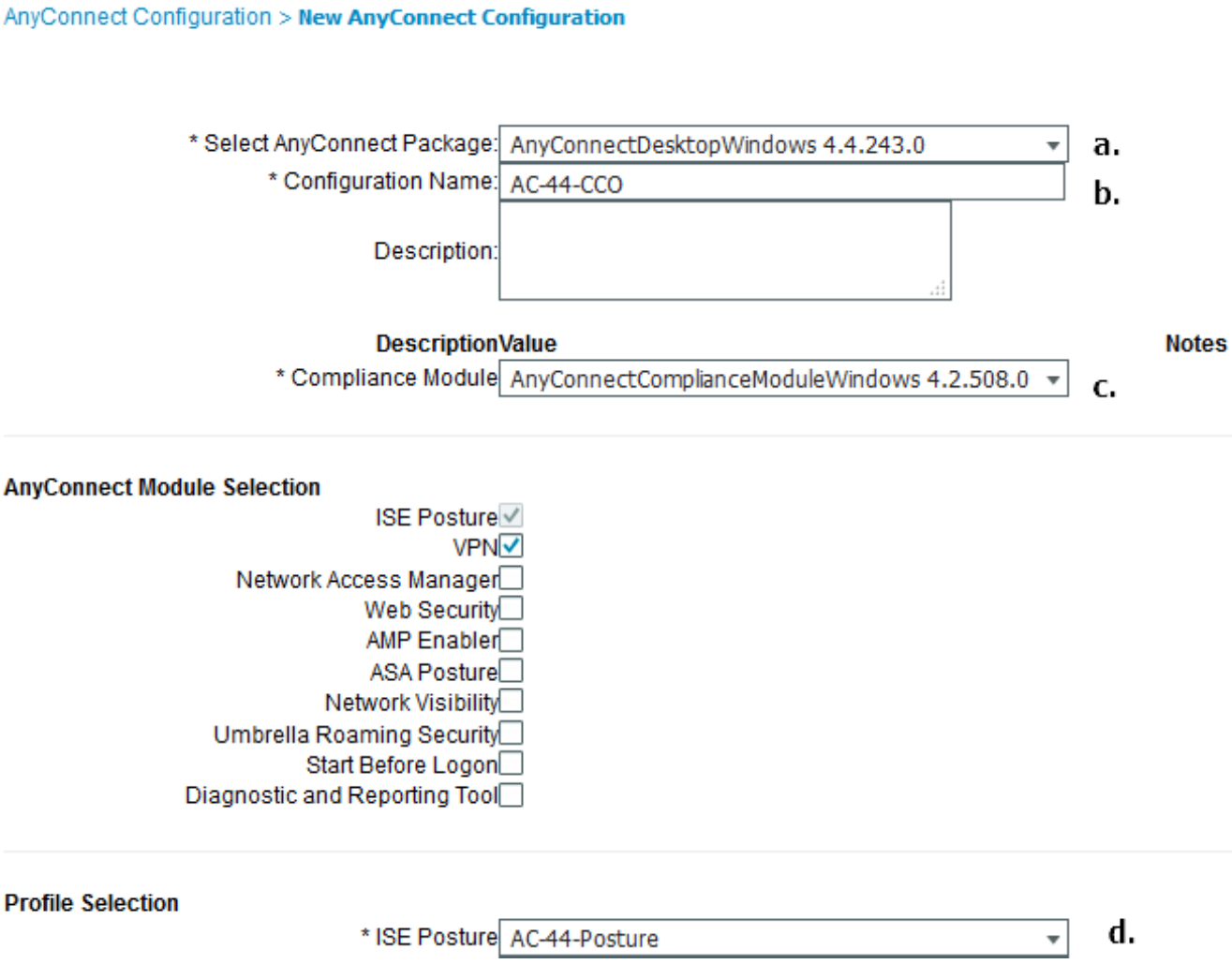


Figura 3-5

- Escolha o encapsulamento AC.
- Forneça o nome da configuração de CA.
- Escolha a versão do módulo de conformidade.
- Escolha o perfil de configuração de postura AC na lista suspensa.

Etapa 6. Configure a política de provisionamento do cliente. Navegue até Policy > Client Provisioning. No caso da configuração inicial, você pode preencher valores vazios na política apresentada com padrões. Se precisar adicionar uma política à configuração de postura existente, navegue até a política que pode ser reutilizada e escolha Duplicate Above or Duplicate Below . Também é possível criar uma política totalmente nova.

Este é um exemplo da política usada no documento.

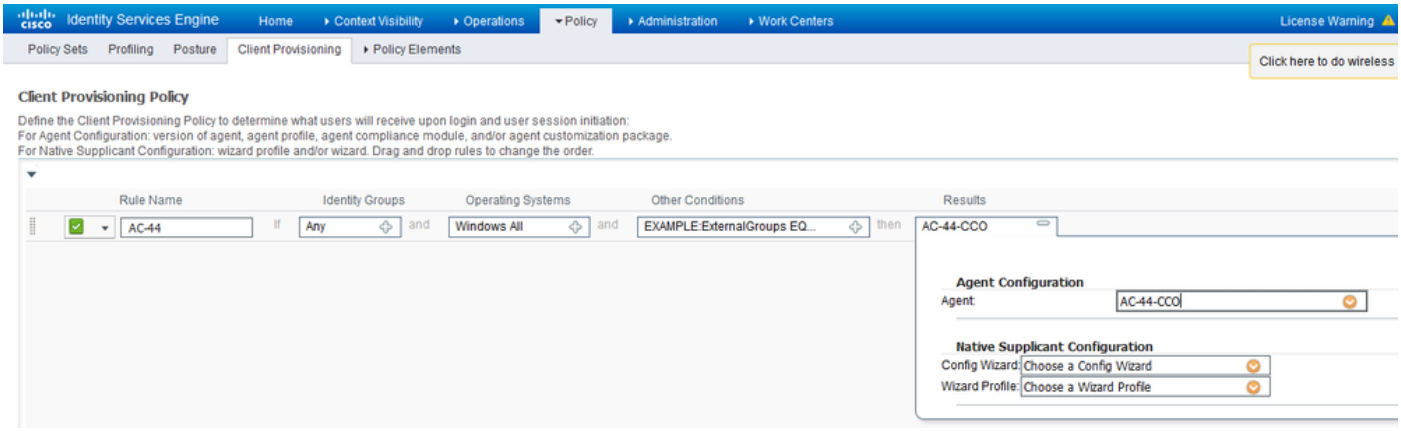


Figura 3-6

Escolha sua configuração AC na seção de resultados. Lembre-se de que, em caso de falha do SSO, o ISE pode ter apenas atributos do login ao portal. Esses atributos são limitados a informações que podem ser recuperadas sobre usuários de repositórios de identidades internos e externos. Neste documento, o grupo do AD é usado como uma condição na política de Provisionamento de clientes.

### Políticas e condições de postura

Uma simples verificação de postura é usada. O ISE é configurado para verificar o status do serviço do Windows Defender no lado do dispositivo final. Os cenários reais podem ser muito mais complicados, mas as etapas gerais de configuração são as mesmas.

Etapa 1. Criar condição de postura. As condições de postura estão localizadas em Policy > Policy Elements > Conditions > Posture. Escolha o tipo de condição de postura. Este é um exemplo de uma condição de serviço que deve verificar se o serviço Windows Defender está em execução.

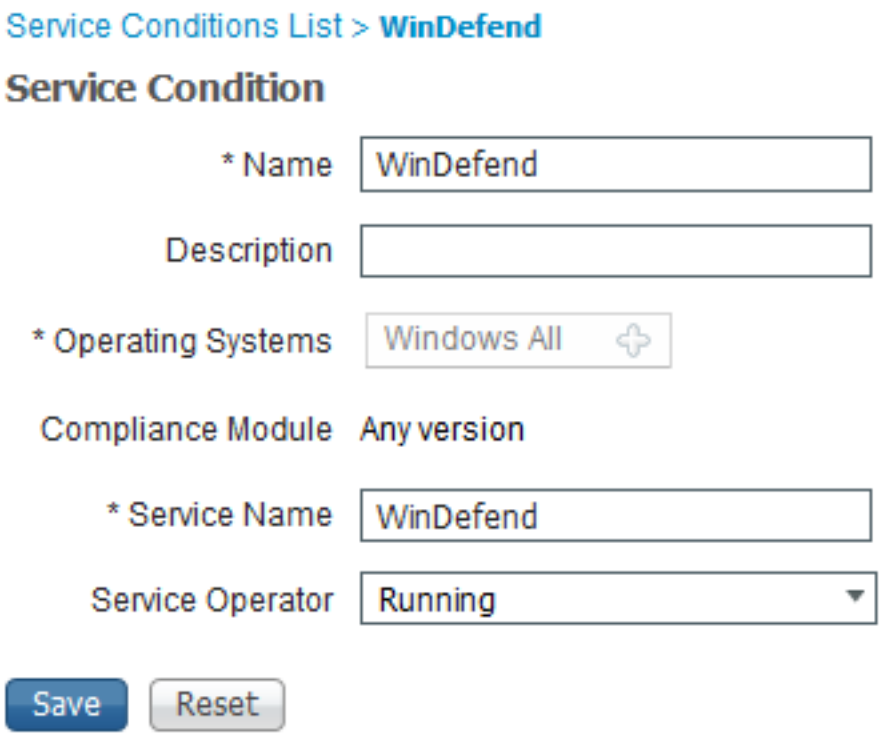


Figura 3-7

Etapa 2.Configuração dos requisitos de postura. Navegue até Policy > Policy Elements > Results > Posture > Requirements. Este é um exemplo de uma verificação do Windows Defender:

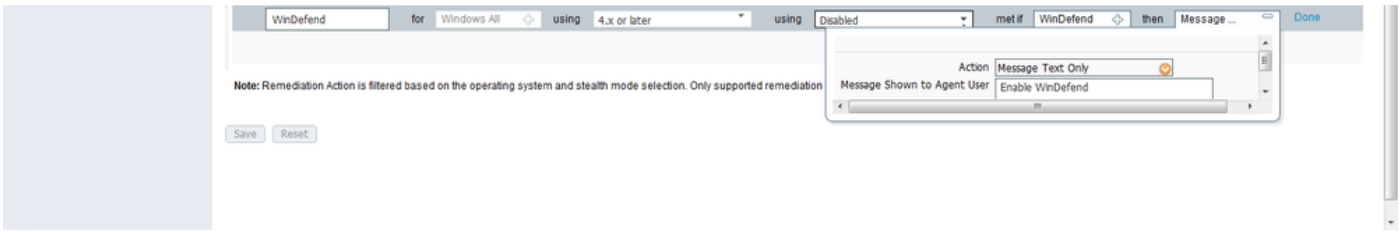


Figura 3-8

Escolha sua condição de postura no novo requisito e especifique uma ação corretiva.

Etapa 3. Configuração de política de postura. Navegue até Policy > Posture. Aqui, você pode encontrar um exemplo da política usada para este documento. A política tem o requisito do Windows Defender atribuído como obrigatório e contém apenas o nome do grupo AD externo como uma condição.

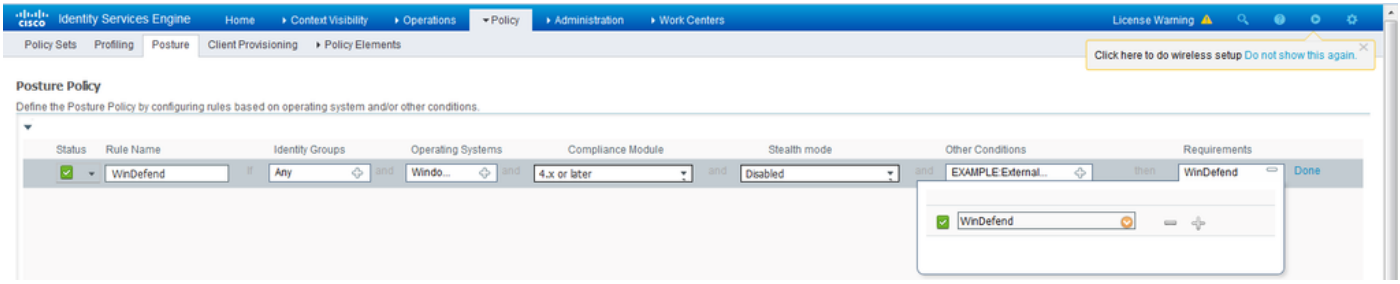


Figura 3-9

## Configurar o Portal de Provisionamento de Cliente

Para postura sem redirecionamento, a configuração do portal de provisionamento do cliente deve ser editada. Navegue até Administration > Device Portal Management > Client Provisioning.Você pode usar o portal padrão ou criar o seu próprio. O mesmo portal pode ser usado para ambas as posturas com e sem redirecionamento.

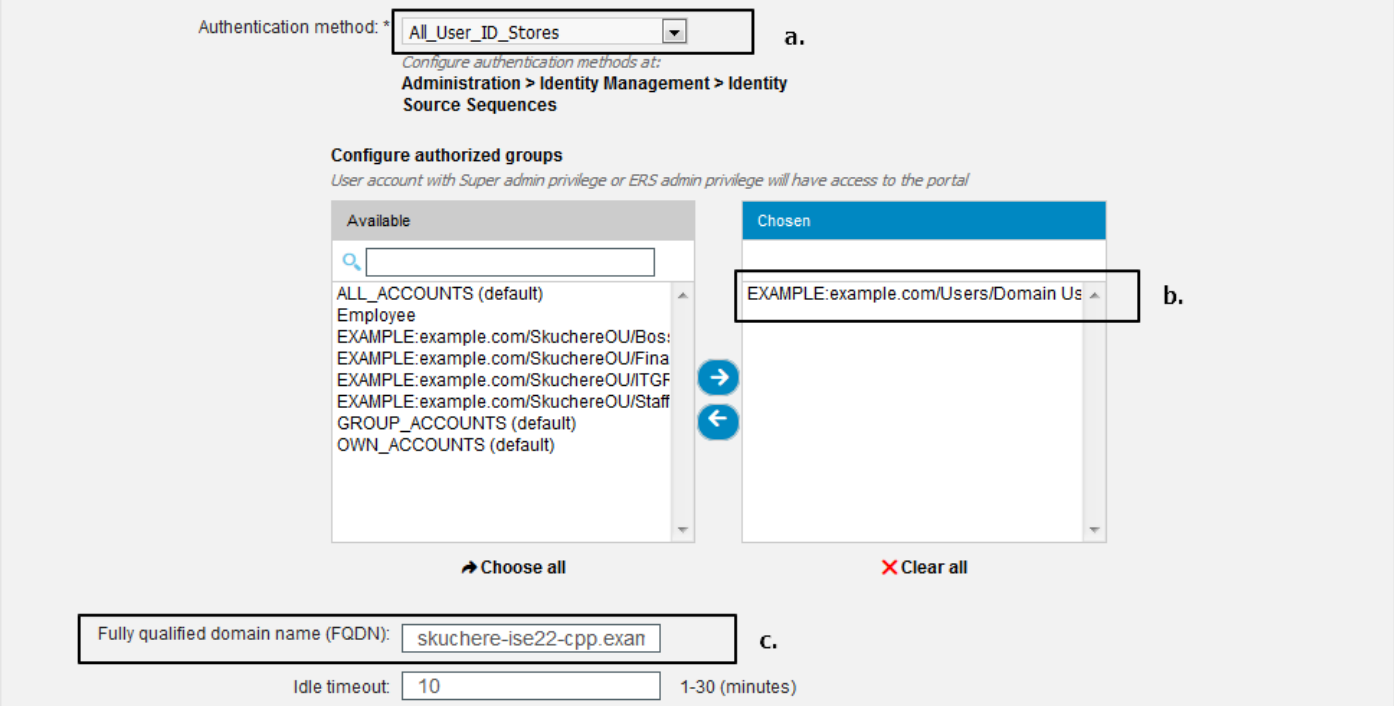


Figura 3-10

Essas configurações devem ser editadas na configuração do portal para o cenário de não redirecionamento:

- Em Autenticação, especifique a Sequência de Origem da Identidade que deverá ser usada se o SSO não puder localizar uma sessão para o usuário.
- De acordo com a lista Sequência de origem da identidade selecionada dos grupos disponíveis, será preenchido. Nesse ponto, você deve selecionar grupos autorizados a fazer login no portal.
- O FQDN do portal de provisionamento do cliente deve ser especificado para cenários em que o AC precisa ser implantado no portal de provisionamento do cliente. Esse FQDN deve ser resolvível para IPs ISE PSNs. Os usuários devem ser instruídos a especificar o FQDN no navegador da Web durante a primeira tentativa de conexão.

### Configurar perfis e políticas de autorização

O acesso inicial para clientes quando o status da postura não estiver disponível deve ser restrito. Isso pode ser obtido de várias maneiras:

- Atribuição de DACL - Durante a fase de acesso restrito, a DACL pode ser atribuída ao usuário para limitar o acesso. Essa abordagem pode ser usada para dispositivos de acesso à rede da Cisco.
- Atribuição de VLAN - Antes que os usuários de postura bem-sucedidos possam ser colocados em VLAN restrita, essa abordagem deve funcionar bem para praticamente qualquer fornecedor de NAD.
- Radius Filter-Id - Com esse atributo, a ACL definida localmente no NAD pode ser atribuída ao usuário com status de postura desconhecido. Como esse é um atributo RFC padrão, essa abordagem deve funcionar bem para todos os fornecedores de NAD.

Etapa 1. Configure a DACL. Como este exemplo é baseado no ASA, um NAD DACL pode ser

usado. Para cenários reais, você deve considerar VLAN ou ID de filtro como opções possíveis.

Para criar DACL, navegue até Policy > Policy Elements > Results > Authorization > Downloadable ACLse clique em Add.

Durante o estado de postura desconhecida, pelo menos estas permissões devem ser fornecidas:

- tráfego DNS
- tráfego DHCP
- Tráfego para ISE PSNs (portas 80 e 443) para uma possibilidade de abrir o FQDN amigável do portal. A porta na qual o portal CP está sendo executado é 8443 por padrão e a porta 8905 para compatibilidade com versões anteriores)
- Tráfego para servidores de remediação, se necessário

Este é um exemplo de DACL sem servidores de remediação:

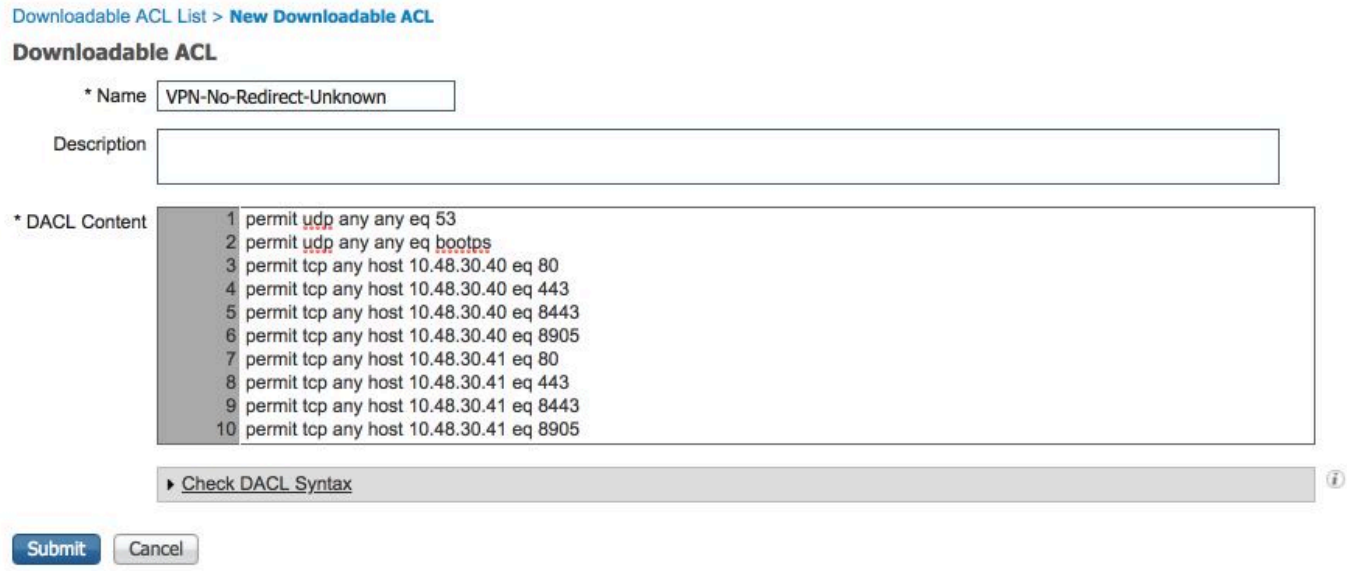


Figura 3-11

Etapa 2. Configure o perfil de autorização.

Como de costume, são necessários dois perfis de autorização para a postura. O primeiro deve conter qualquer tipo de restrição de acesso à rede (perfil com DACL usado neste exemplo). Esse perfil pode ser aplicado às autenticações para as quais o status de postura não é igual a compatível. O segundo perfil de autorização pode conter apenas permissão de acesso e pode ser aplicado a sessões com status de postura igual à conformidade.

Para criar um perfil de autorização, navegue até Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Exemplo do perfil de acesso restrito:

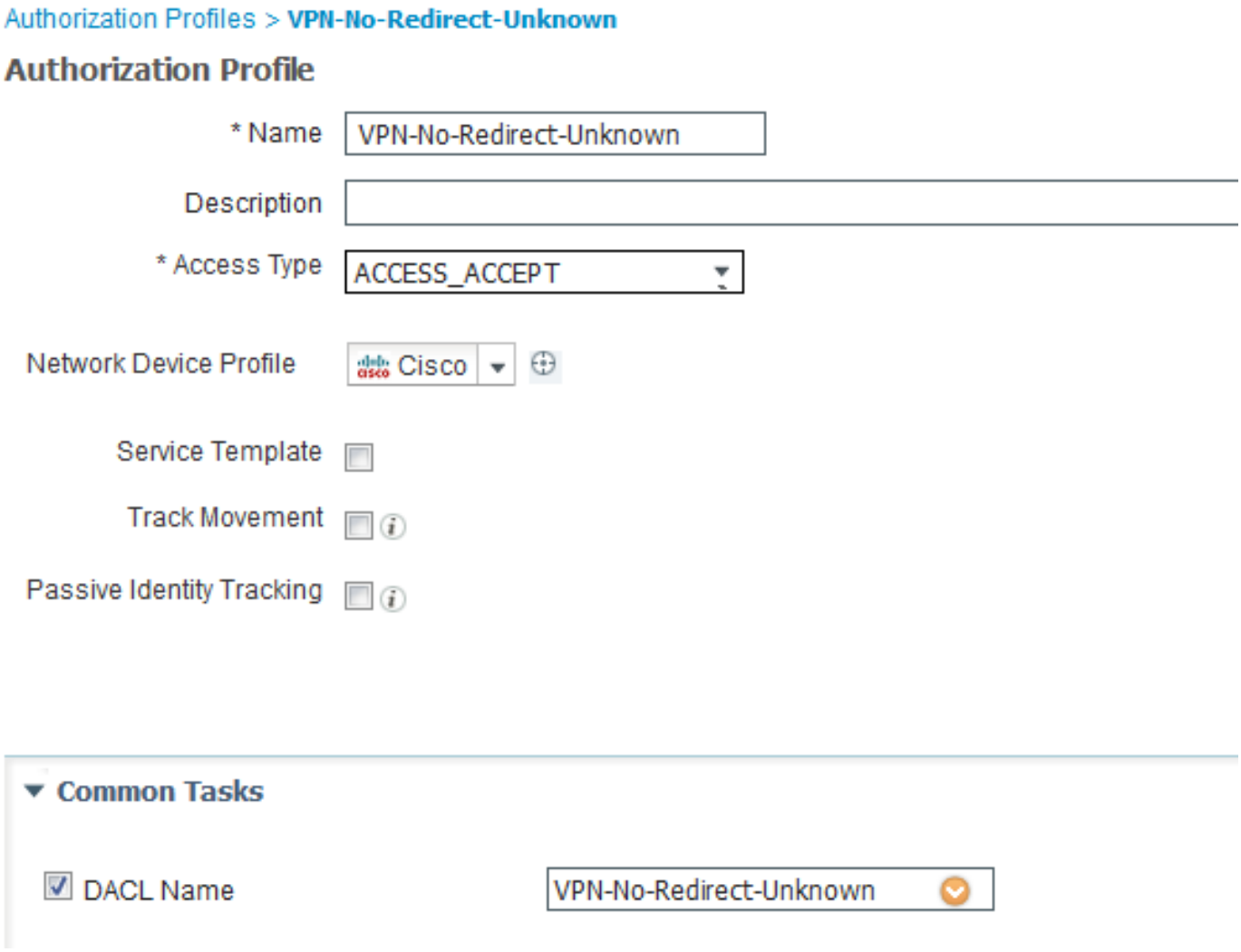


Figura 3-12

Neste exemplo, o perfil padrão do ISE PermitAccess é usado para a sessão após uma verificação de status de postura bem-sucedida.

Etapa 3. Configure a política de autorização. Durante essa etapa, duas políticas de autorização devem ser criadas. Uma é corresponder a solicitação de autenticação inicial com status de postura desconhecido e a segunda é atribuir acesso total após um processo de postura bem-sucedido.

Este é um exemplo de políticas de autorização simples para este caso:

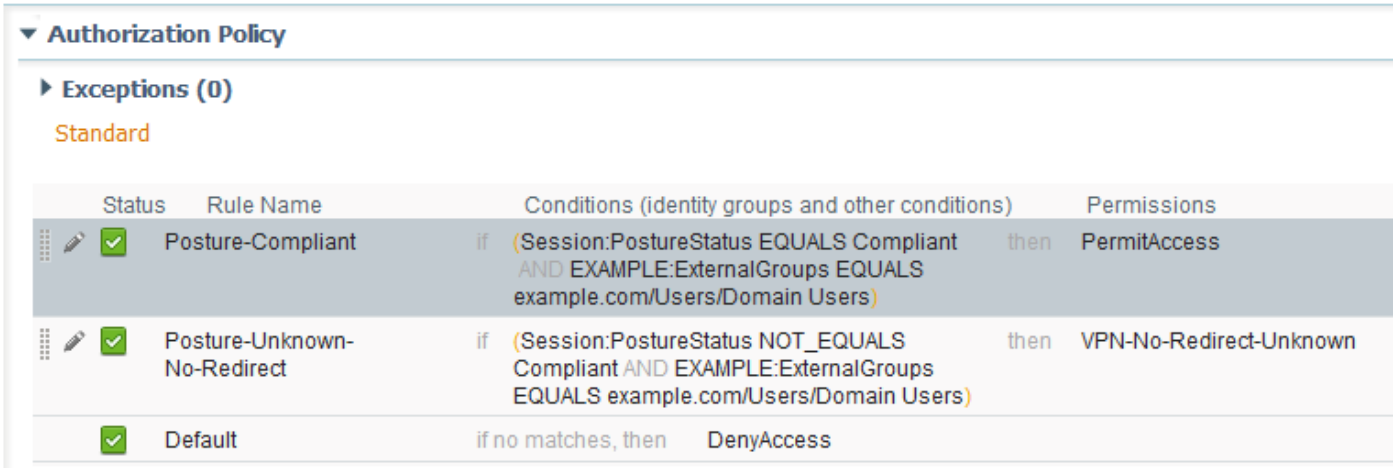


Figura 3-13

A configuração da política de Autenticação não faz parte deste documento, mas você deve ter em mente que, antes do processamento da política de autorização, a autenticação bem-sucedida deve ocorrer.

# Verificar

A verificação básica do caudal pode consistir em três etapas principais:

Etapa 1. Verificação do fluxo de autenticação.

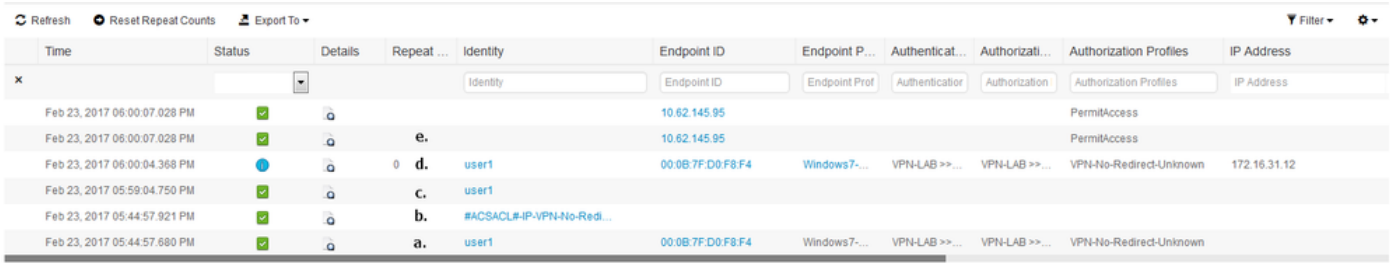


Figura 4-1

1. Autenticação inicial. Para esta etapa, você pode estar interessado na validação da qual o perfil de autorização foi aplicado. Se um perfil de autorização inesperado tiver sido aplicado, investigue um relatório de autenticação detalhado. Você pode abrir esse relatório clicando na lente de aumento na coluna Detalhes. Você pode comparar atributos em relatórios detalhados de autenticação com condições na política de autorização que você espera que correspondam.

2. Evento de download de DACL. Essa string é apresentada somente quando o perfil de autorização selecionado para a autenticação inicial contém um nome DACL.

3. Autenticação do portal - essa etapa no fluxo indica que o mecanismo SSO falhou ao localizar a sessão do usuário. Isso pode ocorrer por vários motivos:
   O NAD não está configurado para enviar mensagens de contabilização ou o endereço IP

com quadro não está presente nelasO FQDN do portal CPP foi resolvido para o IP do nó ISE diferente do nó em que a autenticação inicial foi processadaO cliente está localizado atrás do NAT

4. Alteração de dados da sessão. Neste exemplo específico, o estado da sessão mudou de Desconhecido para Compatível.

5. COA para o dispositivo de acesso à rede. Este COA deve ser bem-sucedido para enviar uma nova autenticação do lado NAD e novas atribuições de política de autorização no lado ISE. Se o COA falhar, você poderá abrir um relatório detalhado para investigar o motivo. Os problemas mais comuns com o COA podem ser: Tempo limite do COA - Nesse caso, o PSN que enviou a solicitação não está configurado como um cliente COA no lado NAD ou a solicitação COA foi descartada em algum lugar no caminho.ACK negativo de COA - Indica que o COA foi recebido pelo NAD, mas devido a algum motivo a operação do COA não pode ser confirmada. Para esse cenário, um relatório detalhado deve conter uma explicação mais detalhada.

Como o ASA é usado como um NAD para este exemplo, você não pode ver nenhuma solicitação de autenticação subsequente para o usuário. Isso acontece porque o ISE usa o push de COA para o ASA, o que evita a interrupção do serviço de VPN. Nesse cenário, o próprio COA contém novos parâmetros de autorização, portanto a reautenticação não é necessária.

Etapa 2.Verificação da seleção da política de provisionamento do cliente - Para isso, você pode executar um relatório no ISE que pode ajudá-lo a entender quais políticas de provisionamento do cliente foram aplicadas ao usuário.

Navegue até Operations > Reports Endpoint and Users > Client Provisioning e executar o relatório para a data necessária.

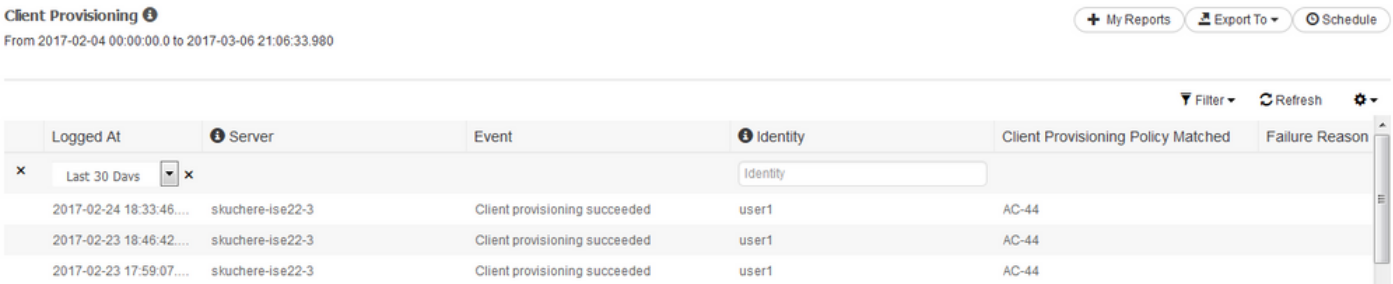


Figura 4-2

Com esse relatório, você pode verificar qual política de provisionamento de cliente foi selecionada. Além disso, em caso de falha, os motivos devem ser apresentados no Failure Reason coluna.

Etapa 3.Verificação do relatório de postura - Navegue até Operations > Reports Endpoint and Users > Posture Assessment by Endpoint.

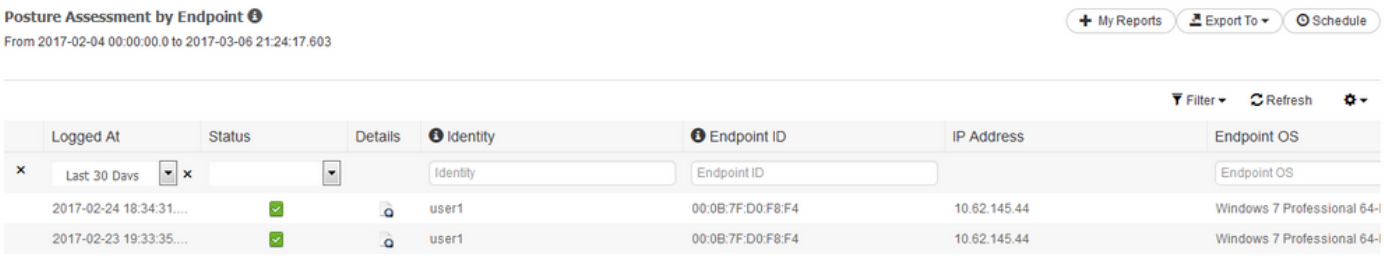


Figura 4-3

Você pode abrir um relatório detalhado aqui para cada evento específico para verificar, por exemplo, a qual ID de sessão este relatório pertence, quais requisitos de postura exatos foram selecionados pelo ISE para o endpoint e o status de cada requisito.

# Troubleshoot

## Informações gerais

Para a solução de problemas de processos de postura, esses componentes do ISE devem ser ativados para depuração nos nós do ISE onde o processo de postura pode ocorrer:

- client-webapp - O componente responsável pelo provisionamento do agente. Arquivos de log de destino guest.log e ise-psc.log.
- guestacess - O componente responsável pelo componente do portal de provisionamento do cliente e pela pesquisa do proprietário da sessão (quando a solicitação chega ao PSN incorreto). Arquivo de log de destino - guest.log.
- provisioning - O componente responsável pelo processamento da política de provisionamento do cliente. Arquivo de log de destino - guest.log.
- posture - Todos os eventos relacionados à postura. Arquivo de log de destino - ise-psc.log.

Para a solução de problemas do lado do cliente, você pode usar estes:

- acisensa.log -Em caso de falha de provisionamento do cliente no lado do cliente, esse arquivo é criado na mesma pasta para a qual o NSA foi baixado (faz downloads do diretório do Windows normalmente).
- AnyConnect_ISEPosture.txt - Esse arquivo pode ser encontrado no pacote DART no diretório Cisco AnyConnect ISE Posture Module. Todas as informações sobre a descoberta de PSN do ISE e as etapas gerais do fluxo de postura são registradas nesse arquivo.

## Troubleshooting Problemas Comuns

### Problemas relacionados ao SSO

No caso de um SSO bem-sucedido, você poderá ver essas mensagens no ise-psc.log, este conjunto de mensagens indica que a pesquisa de sessão foi concluída com êxito e que a autenticação no portal pode ser ignorada.

```
2016-11-09 15:07:35,951 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [10.62.145.121], mac Addrs [null]
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP
10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = 5
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType equal to 5 ( 5 is virtual
NAS_PORT_TYPE for VPN ). Found a VPN session null using ip address 10.62.145.121
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session c0a801010002600058232bb8
using ipAddr 10.62.145.121
```

Janela de texto 5-1

Você pode usar o endereço IP do ponto final como uma chave de pesquisa para encontrar essa informação.

Um pouco mais tarde, no log de convidado, você deve ver que a autenticação foi ignorada:

```
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
guestaccess.flowmanager.step.cp.CPInitStepExecutor -::- SessionInfo is not null and session
AUTH_STATUS = 1
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
com.cisco.ise.portalSessionManager.PortalSession -::- Putting data in PortalSession with key and
value: Radius.Session c0a801010002600058232bb8
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
com.cisco.ise.portalSessionManager.PortalSession -::- Putting data in PortalSession with key :
Radius.Session
2016-11-09 15:07:35,989 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
guestaccess.flowmanager.step.cp.CPInitStepExecutor -::- Login step will be skipped, as the
session =c0a801010002600058232bb8 already established for mac address null , clientIPAddress
10.62.145.121
2016-11-09 15:07:36,066 DEBUG [http-bio-10.48.30.40-8443-exec-12][]
cpm.guestaccess.flowmanager.processor.PortalFlowProcessor -::- After executeStepAction(INIT),
returned Enum: SKIP_LOGIN_PROCEED
```

Janela de texto 5-2

Caso a COS não funcione, a ise-psc log arquivo contém informações sobre falha de pesquisa de sessão:

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: null, MacAddr: null, ipAddr: 10.62.145.44
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [10.62.145.44], mac Addrs [null]
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP 10.62.145.44
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = null
```

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType == null or is not a virtual
NAS_PORT_TYPE ( 5 ).
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- No Radius session found
```

Janela de texto 5-3

No guest.log nesse caso, você deve ver a autenticação de usuário completa no portal:

```
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Find Next Step=LOGIN
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Step : LOGIN will be visible!
2017-02-23 17:59:00,779 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Returning next step =LOGIN
2017-02-23 17:59:00,780 INFO [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.flowmanager.step.StepExecutor -::- Radius Session ID is not set, assuming in
dry-run mode
```

Janela de texto 5-4

Em caso de falhas de autenticação no portal, você deve se concentrar na verificação da configuração do portal - Que armazenamento de identidade está em uso? Quais grupos estão autorizados a fazer login?

## Solucionar Problemas de Seleção de Política de Provisionamento de Cliente

Em caso de falhas nas políticas de provisionamento do cliente ou de processamento incorreto da política, você pode verificar o guest.log para obter mais detalhes:

```
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- In Client Prov : userAgent
=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0, radiusSessionID=null,
idGroupName=S-1-5-21-70538695-790656579-4293929702-513, userName=user1, isInUnitTestMode=false
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.common.utils.OSMapper -:user1:- UserAgent : Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:51.0) Gecko/20100101 Firefox/51.0
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
cpm.guestaccess.common.utils.OSMapper -:user1:- Client OS: Windows 7 (All)
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Retrieved OS=Windows 7 (All)
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Updating the idGroupName to
NAC Group:NAC:IdentityGroups:S-1-5-21-70538695-790656579-4293929702-513
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- User Agent/Radius Session is
empty or in UnitTestMode
2017-02-23 17:59:07,080 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- Calling
getMatchedPolicyWithNoRedirection for user=user1
2017-02-23 17:59:07,505 DEBUG [http-bio-10.48.17.249-8443-exec-2][]
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:user1:- CP Policy Status =SUCCESS,
needToDoVlan=false, CoaAction=NO_COA
```

Janela de texto 5-5

Na primeira string, você pode ver como as informações sobre a sessão são injetadas no mecanismo de seleção de política; no caso de nenhuma correspondência de política ou correspondência de política incorreta, você pode comparar atributos daqui com a configuração da política de provisionamento do cliente. A última string indica o status de seleção da política.

### Solucionar problemas de processos de postura

No lado do cliente, você deve estar interessado na investigação das sondas e seus resultados. Este é um exemplo de um teste de estágio 1 bem-sucedido:

```
****************************************

Date : 02/23/2017
Time : 17:59:57
Type : Unknown
Source : acise

Description : Function: Target::Probe
Thread Id: 0x4F8
File: SwiftHttpRunner.cpp
Line: 1415
Level: debug

PSN probe skuchere-ise22-cpp.example.com with path /auth/status, status is -1..

****************************************
```

Janela de texto 5-6

Nesse estágio, a PSN retorna às informações de CA sobre o proprietário da sessão. Você pode ver estas duas mensagens mais tarde:

```
****************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: Target::probeRecentConnectedHeadEnd
Thread Id: 0xBE4
File: SwiftHttpRunner.cpp
Line: 1674
Level: debug

Target skuchere-ise22-2.example.com, posture status is Unknown..

****************************************
```

Janela de texto 5-7

Os proprietários de sessão devolvem ao agente todas as informações necessárias:

```
****************************************

Date : 02/23/2017
Time : 17:59:58
Type : Unknown
Source : acise

Description : Function: SwiftHttpRunner::invokePosture
Thread Id: 0xFCC
File: SwiftHttpRunner.cpp
Line: 1339
Level: debug

MSG_NS_SWISS_NEW_SESSION, <?xml version="1.0" ?>
<root>
<IP></IP>
<FQDN>skuchere-ise22-2.example.com</FQDN>
<PostureDomain>posture_domain</PostureDomain>
<sessionId>c0a801010009e00058af0f7b</sessionId>
<configUri>/auth/anyconnect?uuid=106a93c0-9f71-471c-ac6c-a2f935d51a36</configUri>
<AcPackUri>/auth/provisioning/download/81d12d4b-ff58-41a3-84db-5d7c73d08304</AcPackUri>
<AcPackPort>8443</AcPackPort>
<AcPackVer>4.4.243.0</AcPackVer>
<PostureStatus>Unknown</PostureStatus>
<PosturePort>8443</PosturePort>
<PosturePath>/auth/perfigo_validate.jsp</PosturePath>
<PRAConfig>0</PRAConfig>
<StatusPath>/auth/status</StatusPath>
<BackupServers>skuchere-ise22-1.example.com,skuchere-ise22-3.example.com</BackupServers>
</root>
.

****************************************
```

Janela de texto 5-8

Do lado da PSN, você pode se concentrar nessas mensagens no guest.log quando você espera que a solicitação inicial que chega ao nó não seja proprietária da sessão:

```
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Got http request from 10.62.145.44 user
agent is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.48; AnyConnect Posture Agent v.4.4.00243)
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- mac_list from http request ==>
00:0B:7F:D0:F8:F4,00:0B:7F:D0:F8:F4
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- iplist from http request ==>
172.16.31.12,10.62.145.95
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Session id from http request -
req.getParameter(sessionId) ==> null
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently
being processed in the for loop ==> 172.16.31.12
2017-02-23 17:59:56,345 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently
being processed in the for loop ==> 10.62.145.95
2017-02-23 17:59:56,368 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Found Client IP null and corresponding mac
address null
```

```
2017-02-23 17:59:56,369 ERROR [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- Session Info is null
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Not able to find a session for input
values - sessionId : null, Mac addresses : [00:0B:7F:D0:F8:F4, 00:0B:7F:D0:F8:F4], client Ip :
[172.16.31.12, 10.62.145.95]
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- clientMac is null/ empty, will go over the
mac list to query MNT for active session
2017-02-23 17:59:56,369 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Performing MNT look up for macAddress ==>
00-0B-7F-D0-F8-F4
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Performed MNT lookup, found session 0 with
session id c0a801010009e00058af0f7b
2017-02-23 17:59:56,539 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- getting NIC name for skuchere-ise22-
cpp.example.com
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- local interface 0 addr 10.48.17.249 name
eth0
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- Nic name for local host: skuchere-ise22-
cpp.example.com is: eth0
2017-02-23 17:59:56,541 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- getting host FQDN or IP for host skuchere-
ise22-2 NIC name eth0
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- hostFQDNOrIP for host skuchere-ise22-2 nic
eth0 is skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- PDP with session of 00-0B-7F-D0-F8-F4 is
skuchere-ise22-2, FQDN/IP is: skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Redirecting the request to new URL:
https://skuchere-ise22-2.example.com:8443/auth/status
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cisco.cpm.client.posture.NextGenDiscoveryServlet -::- Session info is null. Sent an http
response to 10.62.145.44.
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PDP-WITH-SESSION value is
skuchere-ise22-2.example.com
2017-02-23 17:59:56,545 DEBUG [http-bio-10.48.17.249-8443-exec-10][]
cpm.client.provisioning.utils.ProvisioningUtil -::- header Location value is https://skuchere-
ise22-2.example.com:8443/auth/status
```

Janela de texto 5-9

Aqui você pode ver que o PSN primeiro tenta localizar uma sessão localmente e, após a falha, inicia uma solicitação ao MNT com o uso da lista de IPs e MACs para localizar o proprietário da sessão.

Um pouco mais tarde, você deverá ver uma solicitação do cliente na PSN correta:

```
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
null, IP addrs: [172.16.31.12, 10.62.145.95], mac Addrs [00:0B:7F:D0:F8:F4, 00:0B:7F:D0:F8:F4]
2017-02-23 17:59:56,790 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using IP 172.16.31.12
2017-02-23 17:59:56,791 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType = 5
```

```
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- nasPortType equal to 5 ( 5 is virtual
NAS_PORT_TYPE for VPN ). Found a VPN session null using ip address 172.16.31.12
2017-02-23 17:59:56,792 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session c0a801010009e00058af0f7b
using ipAddr 172.16.31.12
```

Janela de texto 5-10

Como próxima etapa, o PSN realiza a consulta da política de provisionamento do cliente para esta sessão:

```
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
com.cisco.cpm.swiss.SwissServer -::::- null or empty value for hostport obtained from
SwissServer : getHostNameBySession()
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: c0a801010009e00058af0f7b, MacAddr: 00-0b-7f-d0-f8-f4, ipAddr: 172.16.31.12
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
c0a801010009e00058af0f7b, IP addrs: [172.16.31.12], mac Addrs [00-0b-7f-d0-f8-f4]
2017-02-23 17:59:56,793 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session using sessionId
c0a801010009e00058af0f7b
2017-02-23 17:59:56,795 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -::::- User user1 belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-02-23 17:59:58,203 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
com.cisco.cpm.swiss.SwissServer -::::- null or empty value for hostport obtained from
SwissServer : getHPortNumberBySession()
2017-02-23 17:59:58,907 DEBUG [http-bio-10.48.30.41-8443-exec-10][]
cisco.cpm.posture.util.AgentUtil -::::- Increase MnT counter at
CP:ClientProvisioning.ProvisionedResource.AC-44-Posture
```

Janela de texto 5-11

Na próxima etapa, você pode ver o processo de seleção de requisitos de postura. No final da etapa, uma lista de requisitos é preparada e retornada ao agente:

```
2017-02-23 18:00:00,372 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:user1:::- About to query posture policy for user
user1 with endpoint mac 00-0b-7f-d0-f8-f4
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureManager -:user1:::- agentCMVersion=4.2.508.0,
agentType=AnyConnect Posture Agent, groupName=OESIS_V4_Agents -> found agent group with
displayName=4.x or later
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- User user1 belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-02-23 18:00:00,423 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- About to retrieve posture policy
resources for os 7 Professional, agent group 4.x or later and identity groups [NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation, NAC
Group:NAC:IdentityGroups:Any]
2017-02-23 18:00:00,432 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:WinDefend by agent group with FQN NAC
```

```
Group:NAC:AgentGroupRoot:ALL:OESIS_V4_Agents
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- The evaluation result by agent group for
resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend is Permit
2017-02-23 18:00:00,433 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:WinDefend by OS group with FQN NAC
Group:NAC:OsGroupRoot:ALL:WINDOWS_ALL:WINDOWS_7_ALL:WINDOWS_7_PROFESSIONAL_ALL
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- stealth mode is 0
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- The evaluation result by os group for
resourceId NAC Group:NAC:Posture:PosturePolicies:WinDefend is Permit
2017-02-23 18:00:00,438 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:WinDefend by Stealth mode NSF group with FQN NAC
Group:NAC:StealthModeStandard
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Procesing obligation with posture policy
resource with id NAC Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Found obligation id
urn:cisco:cepm:3.3:xacml:response-qualifier for posture policy resource with id NAC
Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Found obligation id PostureReqs for
posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:WinDefend
2017-02-23 18:00:00,439 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:user1:::- Posture policy resource id WinDefend has
following associated requirements []
2017-02-23 18:00:03,884 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- policy enforcemnt is 0
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- simple condition: [Name=WinDefend,
Descriptionnull, Service Name=WinDefend, Service Operator=Running, Operating Systems=[Windows
All], Service Type=Daemon, Exit code=0]
2017-02-23 18:00:03,904 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cpm.posture.runtime.agent.AgentXmlGenerator -:user1:::- check type is Service
2017-02-23 18:00:04,069 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:user1:::- NAC agent xml <?xml version="1.0"
encoding="UTF-8"?><cleanmachines>
<version>ISE: 2.2.0.470</version>
<encryption>0</encryption>
<package>
<id>10</id>
```

**WinDefend**

```
</package>
</cleanmachines>
```

Janela de texto 5-12

Mais tarde, você pode ver que o relatório de postura foi recebido pela PSN:

```
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- UDID is
8afb76ad11e60531de1d3e7d2345dbba5f11a96d for end point 00-0b-7f-d0-f8-f4
2017-02-23 18:00:04,231 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=report, userip=10.62.145.44, clientmac=00-0b-7f-d0-f8-f4, os=WINDOWS,
osVerison=1.2.1.6.1.48, architecture=9, provider=Device Filter, state=, userAgent=Mozilla/4.0
(compatible; WINDOWS; 1.2.1.6.1.48; AnyConnect Posture Agent v.4.4.00243),
session_id=c0a801010009e00058af0f7b
```

Janela de texto 5-13

No final do fluxo, o ISE marca o endpoint como compatível e inicia o COA:

```
2017-02-23 18:00:04,272 INFO [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureManager -:user1:::- Posture state is compliant for endpoint
with mac 00-0b-7f-d0-f8-f4
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- entering triggerPostureCoA for session
c0a801010009e00058af0f7b
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture CoA is scheduled for session id
[c0a801010009e00058af0f7b]
2017-02-23 18:00:04,272 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture status for session id
c0a801010009e00058af0f7b is Compliant
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Issue CoA on active session with sessionID
c0a801010009e00058af0f7b
2017-02-23 18:00:04,273 DEBUG [http-bio-10.48.30.41-8443-exec-8][]
cisco.cpm.posture.runtime.PostureCoA -:user1:::- Posture CoA is scheduled for session id
[c0a801010009e00058af0f7b]
```

Janela de texto 5-14

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.