Práticas recomendadas e considerações para implantação de postura do ISE

Contents

Introduction

Este documento descreve algumas configurações básicas que abordam vários casos de uso com postura baseada em redirecionamento. Nessas configurações, o cliente permanece compatível, mas o dispositivo de acesso à rede (NAD) limita o acesso porque está no estado de redirecionamento.

Restrições

As configurações neste documento funcionam para Cisco NADs, mas não necessariamente para NADs de terceiros.

Comportamento do cliente de postura

O cliente de postura acionará sondas nestes momentos:

- Login inicial
- Alteração de placa de interface de rede (NIC)/alteração de camada 3 (L3) (novo endereço IP, alteração de estado da NIC)

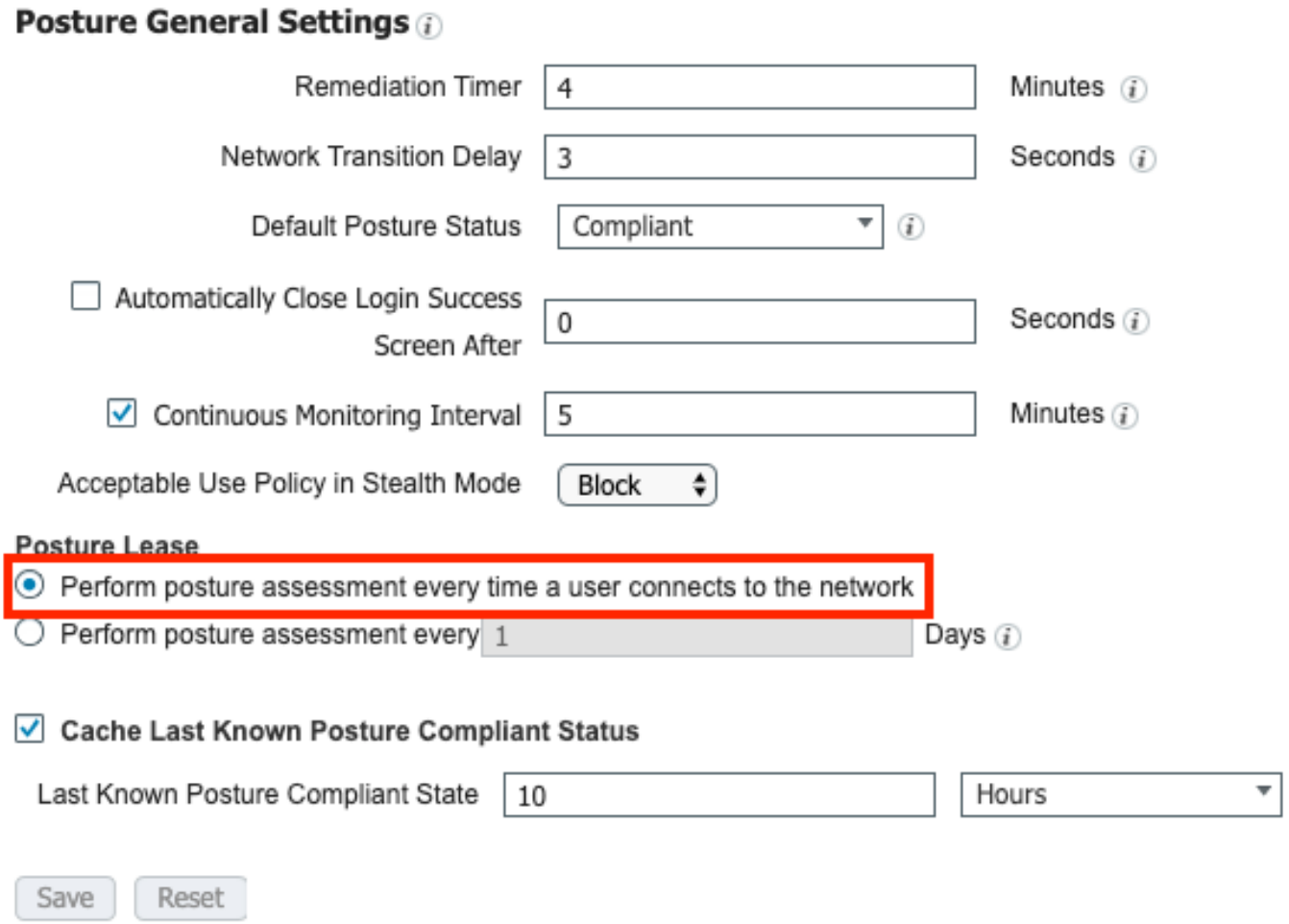
Casos de uso

Caso de uso 1 - A reautenticação do cliente força o NAD a gerar uma nova ID de sessão.

Nesse caso de uso, o cliente ainda é compatível, mas devido à reautenticação, o NAD está no estado de redirecionamento (URL de redirecionamento e lista de acesso).

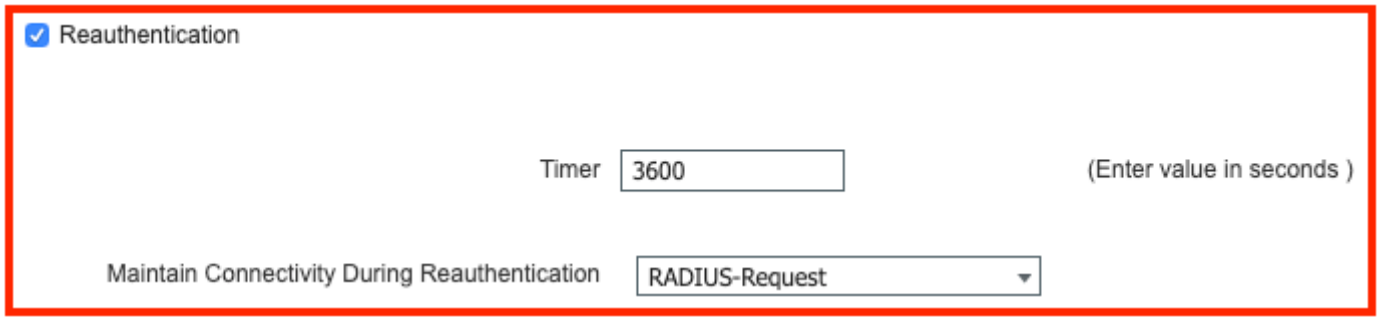
Por padrão, o Identity Services Engine (ISE) é configurado para executar uma avaliação de postura toda vez que se conecta à rede, mais especificamente para cada nova sessão.

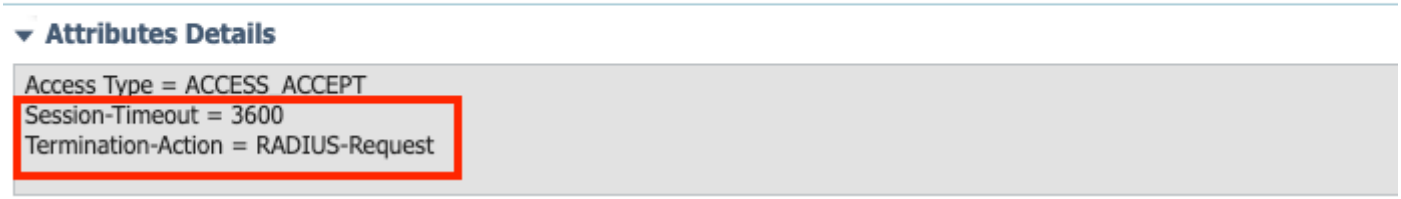
Essa configuração é configurada em Centros de trabalho > Postura > Configurações > Configurações gerais de postura.



Para impedir que o NAD gere uma nova ID de sessão na reautenticação, configure estes valores de reautenticação no perfil de autorização. O temporizador de reautenticação exibido não é uma recomendação padrão, os temporizadores de reautenticação devem ser considerados por implantação com base no tipo de conexão (sem fio/com fio), no design (quais são as regras de persistência no balanceador de carga) e assim por diante.

Política > Elementos de política > Resultados > Autorização > Perfis de autorização





Nos switches, você precisa configurar cada interface, ou modelo, para obter seu temporizador de reautenticação do ISE.

```
authentication timer reauthenticate server
```

> **Note**: Se houver um balanceador de carga, você precisará certificar-se de que a persistência esteja configurada de forma que as reautenticações sejam retornadas ao PSN (Policy Service, serviço de política original).

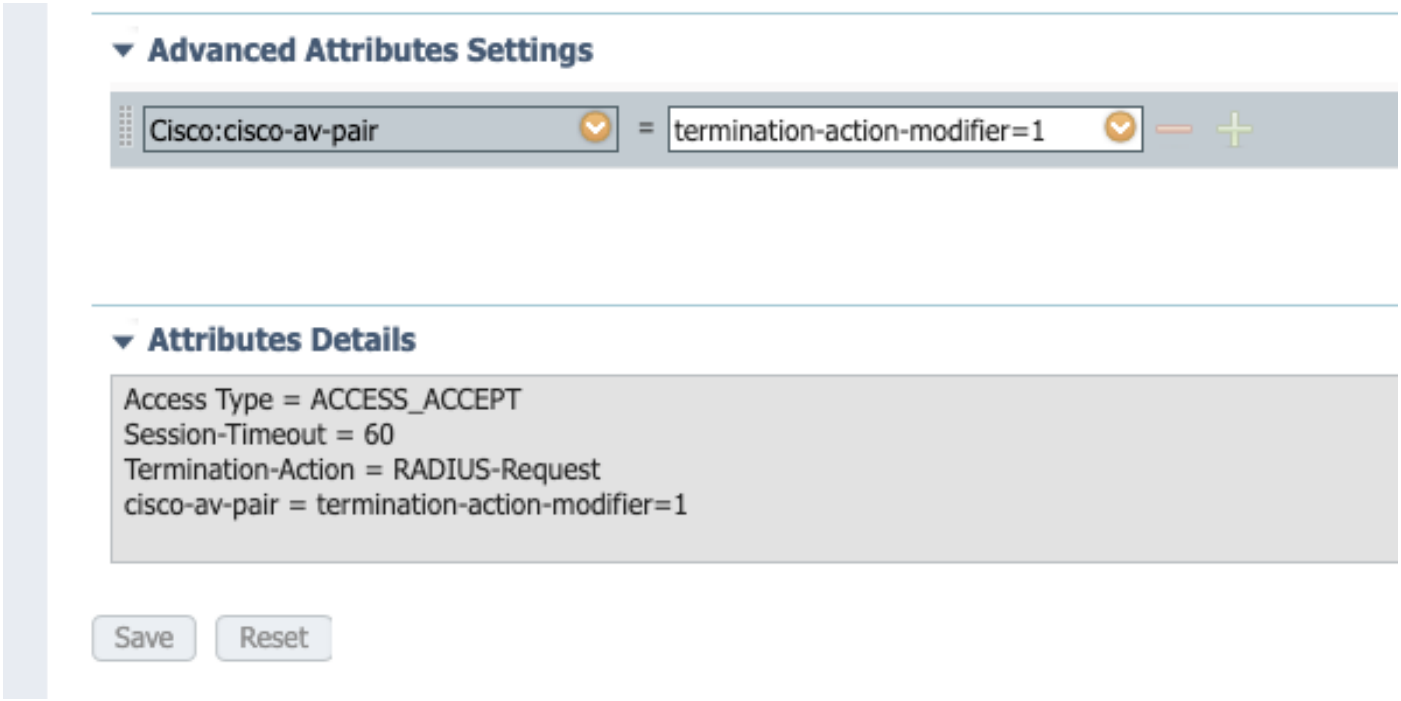
Caso de uso 2 - O switch está configurado com o pedido MAB DOT1X e a prioridade DOT1X MAB (com fio).

Nesse caso, as reautenticações serão encerradas, pois uma parada de contabilização para a sessão 802.1x será enviada quando o MAC Authentication Bypass (MAB) for tentado durante a reautenticação.

- A parada de contabilização enviada para o processo MAB quando ele falha na autenticação está correta, já que o nome de usuário do cliente muda do nome de usuário 802.1X para o nome de usuário MAB.
- Dot1x como o method-id na parada contábil também está correto, pois o método de autorização foi dot1x.
- Quando o método Dot1x é bem-sucedido, ele envia um início de contabilidade com method-id como dot1x. Aqui também, esse comportamento é o esperado.

Para resolver esse problema, configure o cisco-av-pair:terminação-action-modificfier = 1 no perfil authZ usado quando um endpoint é compatível. Este par de atributo-valor (AV) especifica que o NAD deve reutilizar o método escolhido na autenticação original, independentemente da ordem

configurada.



Caso de uso 3 - O roaming de clientes sem fio e as autenticações de APs diferentes estão indo para controladores diferentes.

Para essa situação, a rede sem fio precisará ser projetada para que os access points (APs) ao alcance de outros APs para roaming usem o mesmo controlador ativo. Um exemplo é o failover de switchover stateful (SSO) do Wireless LAN Controller (WLC). Para obter mais informações sobre SSO de alta disponibilidade (HA) para WLC, consulte Guia de implantação de alta disponibilidade (SSO).

Caso de uso 4 - Implantações com balanceadores de carga (Pré 2.6 Patch 6, 2.7 Patch P2 e 3.0).

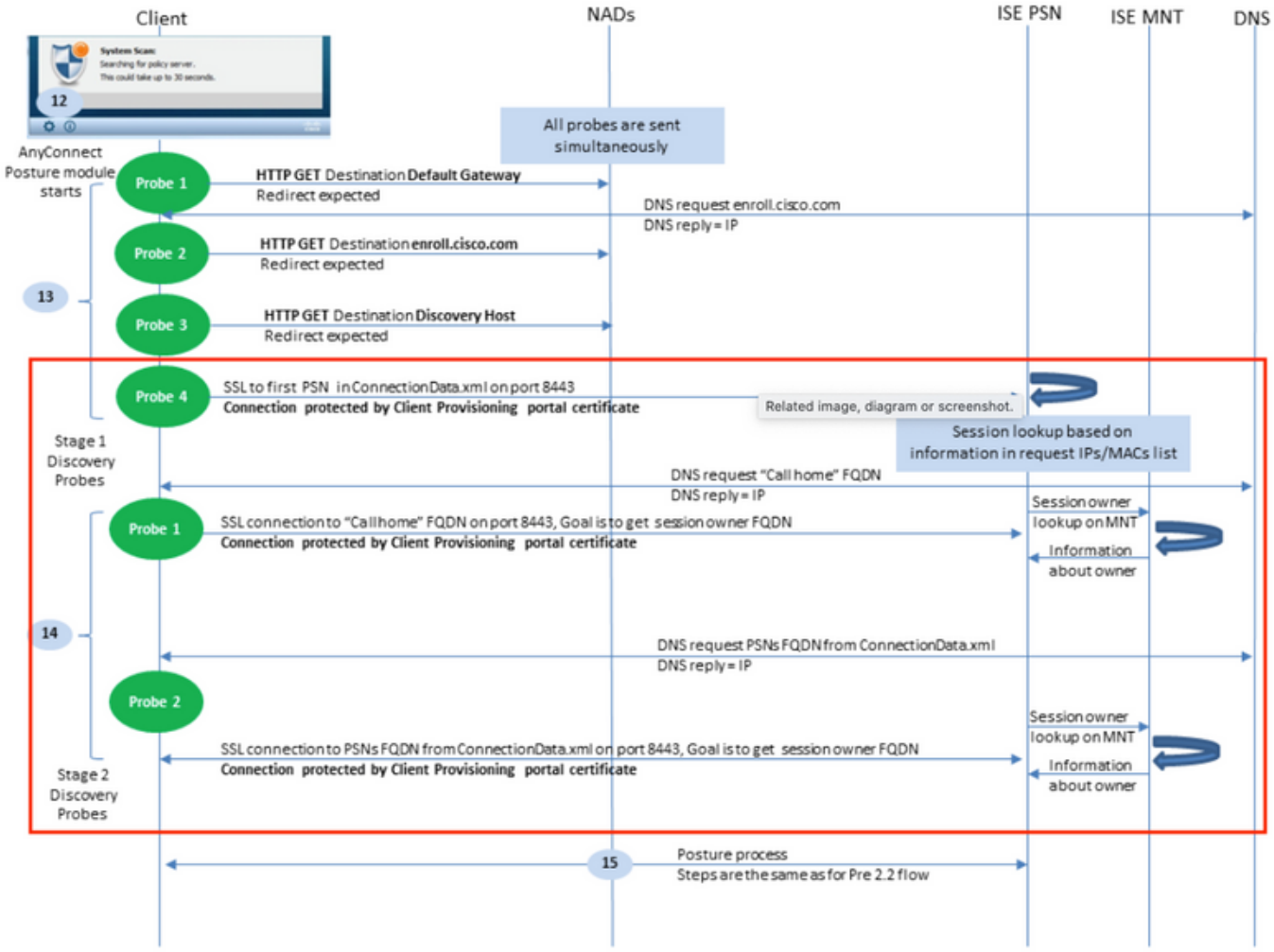
Em implantações com balanceadores de carga envolvidos, é importante certificar-se de que depois de fazer as alterações nos casos de uso anteriores, as sessões continuem indo para o mesmo PSN. Antes da versão/patches listados para esta etapa, o status da postura não é replicado entre os nós através da Distribuição de dados leve (anteriormente Diretório de sessão leve). Por causa disso, é possível que diferentes PSNs retornem resultados de status de postura diferentes.

Se a persistência não estiver configurada corretamente, as sessões que reautenticam poderão ir para uma PSN diferente daquela que foi originalmente usada. Se isso acontecer, o novo PSN poderá marcar o status de conformidade das sessões como desconhecido e passar o resultado authZ com a ACL/URL e limitar o acesso dos endpoints. Novamente, essa alteração no NAD não seria reconhecida pelo módulo de postura e as sondas não serão acionadas.

Para obter mais informações sobre como configurar balanceadores de carga, consulte o Guia de Implantação da Cisco e F5: Balanceamento de carga do ISE usando BIG-IP. Ele fornece uma visão geral de alto nível e configuração específica F5 de um projeto de práticas recomendadas para implantações de ISE em um ambiente com balanceamento de carga.

Caso de uso 5 - As sondas de descoberta da fase 2 são respondidas por um servidor diferente do cliente com o qual o cliente é autenticado (Patch 6 anterior à 2.6, 2.7 Patch 2 e 3.0).

Observe as sondas dentro da caixa vermelha neste diagrama.



Os PSNs armazenarão os dados da sessão por cinco dias, de modo que, às vezes, os dados da sessão para uma sessão "compatível" ainda permanecem na PSN original, mesmo que o cliente não se autentique mais com esse nó. Se as sondas incluídas na caixa vermelha forem respondidas por uma PSN diferente daquela que autentica atualmente a sessão E que a PSN é anteriormente proprietária e marcou essa compatibilidade de ponto final, é possível que haja uma incompatibilidade entre o status da postura do módulo de postura no ponto final e a PSN de autenticação atual.

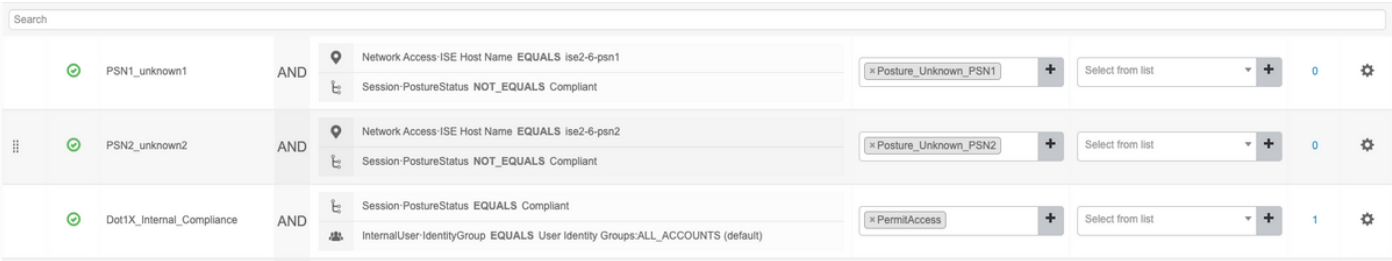
Aqui estão alguns cenários comuns em que essa incompatibilidade pode ocorrer:

- Não é recebida uma parada de contabilidade para um ponto final quando ele se desconecta da rede.
- O NAD falhou de um PSN para outro.
- Um balanceador de carga encaminha autenticações para PSNs diferentes para o mesmo endpoint.

Para proteger-se desse comportamento, o ISE pode ser configurado para permitir que somente as sondas de descoberta de um endpoint específico cheguem à PSN para a qual ele se autentica

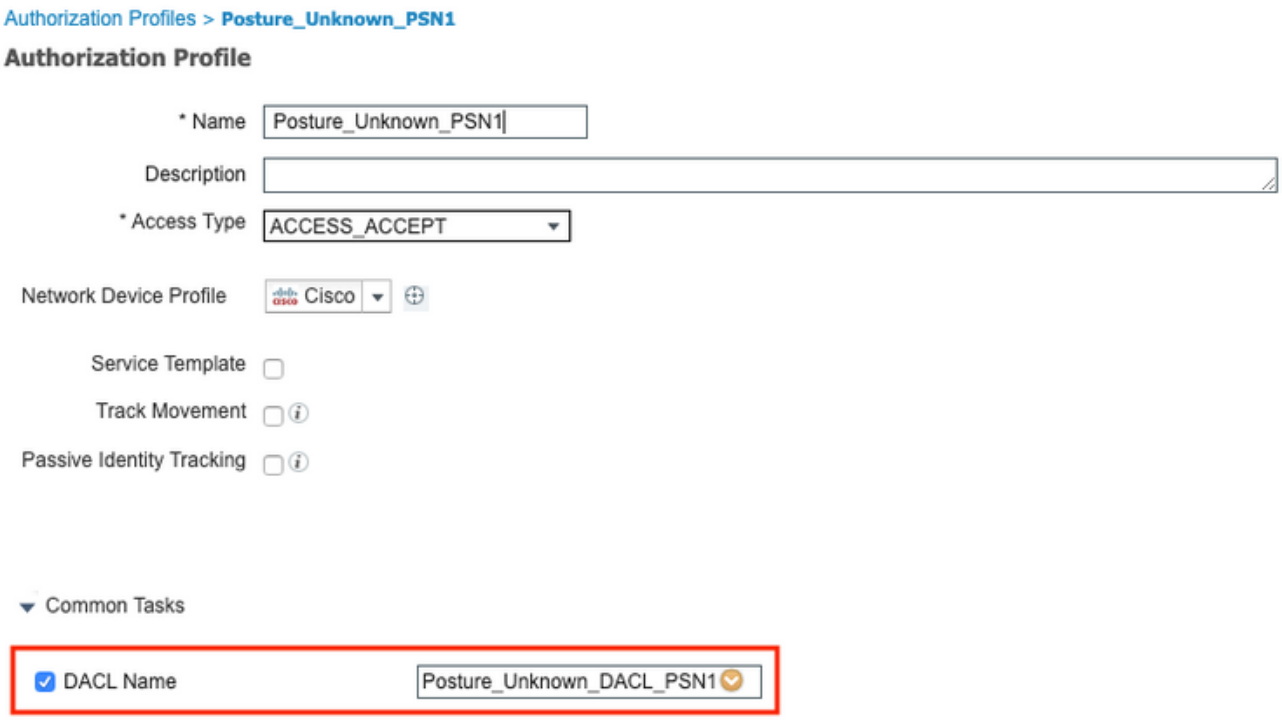
no momento. Para conseguir isso, configure uma política de autorização diferente para cada PSN em sua implantação. Nessas políticas, consulte um perfil authZ diferente que contenha uma Lista de Controle de Acesso (DACL - Access Control List) para Download, que permite sondas APENAS para a PSN especificada na condição authZ. Veja este exemplo:

Cada PSN terá uma regra para status de postura desconhecida:

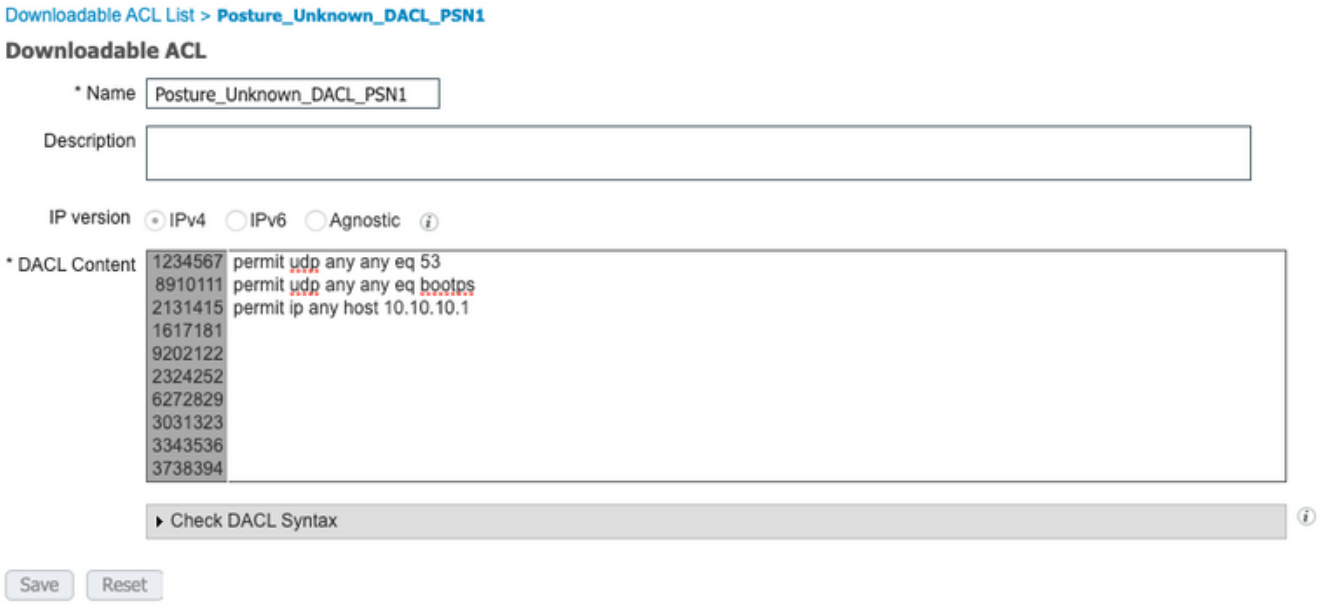


Cada perfil individual faz referência a um DACL diferente.

Note: Para redes sem fio, use ACLs Airespace.



Cada DACL permite somente acesso de prova à PSN que manipula a autenticação.



No exemplo anterior, 10.10.10.1 é o endereço IP do PSN 1. O DACL referenciado pode ser alterado para quaisquer serviços/IPs adicionais, conforme necessário, mas deve limitar o acesso somente ao PSN que lida com a autenticação.

Alteração de comportamento Pós 2.6 Patch 6, 2.7 Patch 2 e 3.0

O status de postura foi adicionado ao Diretório de Sessão RADIUS através da estrutura de Distribuição de Dados Leves. Cada vez que uma atualização de status de postura é recebida em qualquer PSN, ela será replicada para TODOS os PSNs na implantação. Depois que essa alteração estiver em vigor, as implicações de autenticações e/ou sondas que chegam a diferentes PSNs em diferentes autenticações serão removidas e qualquer PSN poderá responder a todos os endpoints, independentemente de onde eles estejam autenticados no momento.

Nos cinco casos de uso neste documento, considere estes comportamentos:

Caso de uso 1 - A reautenticação do cliente força o NAD a gerar uma nova ID de sessão. O cliente ainda é compatível, mas devido à reautenticação, o NAD está no estado de redirecionamento (redirecionar URL e lista de acesso).

- Esse comportamento não será alterado e essa configuração ainda deve ser implementada no ISE e nos NADs.

Caso de uso 2 - O switch está configurado com o pedido MAB DOT1X e a prioridade DOT1X MAB (com fio).

- Esse comportamento não será alterado e essa configuração ainda deve ser implementada no ISE e nos NADs.

Caso de uso 3 - O roaming de clientes sem fio e as autenticações de APs diferentes estão indo para controladores diferentes.

- Esse comportamento não será alterado e essa configuração ainda deve ser implementada no ISE e nos NADs.

Caso de uso 4 - Implantações com balanceadores de carga.

- As melhores práticas definidas no guia de balanceamento de carga ainda devem ser seguidas, mas caso as autenticações sejam encaminhadas para PSNs diferentes pelo balanceador de carga, o status correto da postura deve ser devolvido ao cliente.

Caso de uso 5 - As sondas de descoberta de estágio 2 são respondidas por um servidor diferente do cliente com o qual são autenticadas

- Este não deve ser um problema com o novo comportamento e o perfil de autorização por PSN não deve ser necessário.

Considerações ao manter a mesma ID de sessão

Quando você usa os métodos listados neste documento, um usuário que permanece conectado à rede pode potencialmente permanecer compatível por longos períodos. Mesmo que eles reautentiquem, sessionID não é alterado e, portanto, o ISE continuará a passar o resultado de AuthZ por sua regra correspondente ao status de conformidade.

Nesse caso, a reavaliação periódica precisa ser configurada para que a postura seja necessária para garantir que o endpoint permaneça em conformidade com as políticas corporativas em intervalos definidos.

Isso pode ser configurado em Centros de trabalho > Postura > Configurações > Configurações de avaliação.