Secure ACS - NAR avec clients AAA pour utilisateurs et groupes d'utilisateurs

Contenu

Introduction

Ce document décrit comment configurer les restrictions d’accès au réseau (NAR) dans la version 4.x du Cisco Secure Access Control Server (ACS) avec des clients AAA (y compris les routeurs, le PIX, l’ASA et les contrôleurs sans fil) pour des utilisateurs et des groupes d’utilisateurs.

Conditions préalables

Conditions requises

Ce document est créé en supposant que les clients Cisco Secure ACS et AAA sont configurés et fonctionnent correctement.

Components Used

Les informations de ce document sont basées sur Cisco Secure ACS 3.0 et versions ultérieures.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Restrictions d'accès au réseau

Cette section décrit les NAR et fournit des instructions détaillées pour configurer et gérer les NAR partagés.

Cette section contient ces sujets :

À propos des restrictions d'accès au réseau

Une NAR est une définition, que vous définissez dans ACS, des conditions supplémentaires que vous devez respecter avant qu'un utilisateur puisse accéder au réseau. ACS applique ces conditions en utilisant les informations des attributs que vos clients AAA envoient. Bien que vous puissiez configurer les NAR de plusieurs manières, toutes sont basées sur les informations d'attribut correspondantes qu'un client AAA envoie. Par conséquent, vous devez comprendre le format et le contenu des attributs que vos clients AAA envoient si vous voulez utiliser des NAR efficaces.

Lorsque vous configurez un NAR, vous pouvez choisir si le filtre fonctionne de manière positive ou négative. C'est-à-dire que dans la NAR, vous indiquez si vous voulez autoriser ou refuser l'accès au réseau, en fonction des informations envoyées par les clients AAA par rapport aux informations stockées dans la NAR. Cependant, si une NAR ne rencontre pas suffisamment d'informations pour fonctionner, elle refuse par défaut l'accès. Ce tableau présente les conditions suivantes :

	Basé sur IP	Non basé sur IP	Informations insuffisantes
Autoriser	Accès accordé	Accès refusé	Accès refusé
Refuser	Accès refusé	Accès accordé	Accès refusé

ACS prend en charge deux types de filtres NAR :

- **Filtres IP** - Les filtres NAR IP limitent l'accès en fonction des adresses IP du client utilisateur final et du client AAA. Reportez-vous à la section À propos des filtres NAR basés sur IP pour plus d'informations.
- **Filtres non basés sur IP** - Les filtres NAR non basés sur IP limitent l'accès en fonction d'une simple comparaison de chaînes d'une valeur envoyée par le client AAA. La valeur peut être le numéro d'identification de ligne appelante (CLI), le numéro DNIS (Dialed Number Identification Service), l'adresse MAC ou une autre valeur provenant du client. Pour que ce type de NAR fonctionne, la valeur de la description NAR doit correspondre exactement à ce qui est envoyé par le client, qui inclut le format utilisé. Par exemple, le numéro de téléphone

(217) 555-4534 ne correspond pas au 217-555-4534. Reportez-vous à la section À propos des filtres NAR non basés sur IP pour plus d'informations.

Vous pouvez définir une NAR pour un utilisateur ou un groupe d'utilisateurs spécifique et l'appliquer à un utilisateur ou à un groupe d'utilisateurs spécifique. Reportez-vous aux sections Définir des restrictions d'accès réseau pour un utilisateur ou Définir des restrictions d'accès réseau pour un groupe d'utilisateurs pour plus d'informations. Cependant, dans la section Composants de profil partagé d'ACS, vous pouvez créer et nommer une NAR partagée sans citer directement un utilisateur ou un groupe d'utilisateurs. Vous attribuez au NAR partagé un nom qui peut être référencé dans d'autres parties de l'interface Web ACS. Ensuite, lorsque vous configurez des utilisateurs ou des groupes d'utilisateurs, vous pouvez sélectionner aucune, une ou plusieurs restrictions partagées à appliquer. Lorsque vous spécifiez l'application de plusieurs NAR partagés à un utilisateur ou à un groupe d'utilisateurs, vous choisissez l'un des deux critères d'accès suivants :

- Tous les filtres sélectionnés doivent être autorisés.
- Tout filtre sélectionné doit être autorisé.

Vous devez comprendre l'ordre de priorité associé aux différents types de NAR. Voici l'ordre du filtrage NAR :

1. NAR partagé au niveau de l'utilisateur
2. NAR partagé au niveau du groupe
3. NAR non partagé au niveau de l'utilisateur
4. NAR non partagé au niveau du groupe

Vous devez également comprendre que **le refus d'accès à n'importe quel niveau prime sur les paramètres d'un autre niveau qui ne refusent pas l'accès**. Il s'agit de la seule exception dans ACS à la règle selon laquelle les paramètres de niveau utilisateur remplacent les paramètres de niveau groupe. Par exemple, un utilisateur particulier peut ne pas avoir de restrictions NAR au niveau de l'utilisateur qui s'appliquent. Cependant, si cet utilisateur appartient à un groupe restreint par un NAR partagé ou non partagé, l'accès est refusé à l'utilisateur.

Les NAR partagés sont conservés dans la base de données interne ACS. Vous pouvez utiliser les fonctions de sauvegarde et de restauration ACS pour les sauvegarder et les restaurer. Vous pouvez également répliquer les NAR partagés, ainsi que d'autres configurations, vers des ACS secondaires.

À propos des filtres NAR basés sur IP

Pour les filtres NAR basés sur IP, ACS utilise les attributs comme indiqué, qui dépendent du protocole AAA de la demande d'authentification :

- **Si vous utilisez TACACS+** : le champ `rem_addr` du corps du paquet de début TACACS+ est utilisé.**Remarque :** Lorsqu'une demande d'authentification est transmise par proxy à un ACS, toutes les NAR pour les requêtes TACACS+ sont appliquées à l'adresse IP du serveur AAA de transfert et non à l'adresse IP du client AAA d'origine.
- **Si vous utilisez RADIUS IETF** : l'`ID de la station appelante` (attribut 31) doit être utilisé.**Remarque :** les filtres NAR basés sur IP ne fonctionnent que si ACS reçoit l'attribut Radius Calling-Station-Id (31). L'ID de la station appelante (31) doit contenir une adresse IP valide. Si ce n'est pas le cas, il relèvera des règles du DNIS.

Les clients AAA qui ne fournissent pas suffisamment d'informations d'adresse IP (par exemple, certains types de pare-feu) ne prennent pas en charge la fonctionnalité NAR complète.

Les autres attributs des restrictions **IP**, par protocole, incluent les champs NAR comme indiqué :

- **Si vous utilisez TACACS+**—les champs NAR dans ACS utilisent ces valeurs :**Client AAA** - L'adresse IP NAS provient de l'adresse source dans le socket entre ACS et le client TACACS+.**Port** : le champ du port est extrait du corps du paquet de début TACACS+.

À propos des filtres NAR non basés sur IP

Un filtre NAR non basé sur IP (c'est-à-dire un filtre NAR basé sur DNIS/CLI) est une liste d'emplacements d'appel ou de point d'accès autorisés ou refusés que vous pouvez utiliser pour restreindre un client AAA lorsque vous n'avez pas de connexion IP établie. La fonction NAR non basée sur IP utilise généralement le numéro CLI et le numéro DNIS.

Cependant, lorsque vous saisissez une adresse IP à la place de l'interface de ligne de commande, vous pouvez utiliser le filtre non basé sur IP ; même lorsque le client AAA n'utilise pas de version du logiciel Cisco IOS® prenant en charge CLI ou DNIS. Dans une autre exception à la saisie d'une CLI, vous pouvez saisir une adresse MAC pour autoriser ou refuser l'accès. Par exemple, lorsque vous utilisez un client AAA Cisco Aironet. De même, vous pouvez saisir l'adresse MAC de l'AP Cisco Aironet à la place du DNIS. Le format de ce que vous spécifiez dans la zone CLI (CLI, IP address ou MAC address) doit correspondre au format de ce que vous recevez de votre client AAA. Vous pouvez déterminer ce format à partir de votre journal de comptabilité RADIUS.

Les attributs des restrictions basées sur DNIS/CLI, par protocole, incluent les champs NAR comme indiqué :

- **Si vous utilisez TACACS+**—Les champs NAR répertoriés utilisent ces valeurs :**Client AAA** - L'`adresse IP NAS` provient de l'adresse source dans le socket entre ACS et le client TACACS+.**Port** : le champ `port` du corps du paquet de début TACACS+ est utilisé.**CLI** - Le champ `rem-addr` du corps du paquet de début TACACS+ est utilisé.**DNIS** - Le champ `rem-addr` du corps du paquet de début TACACS+ est utilisé. Dans les cas où les données rem-addr commencent par la barre oblique (/), le champ DNIS contient les données rem-addr sans barre oblique (/).**Remarque :** Lorsqu'une demande d'authentification est transmise par proxy à un ACS, toutes les NAR pour les requêtes TACACS+ sont appliquées à l'adresse IP du serveur AAA de transfert et non à l'adresse IP du client AAA d'origine.
- **Si vous utilisez RADIUS** : les champs NAR répertoriés utilisent ces valeurs :**Client AAA** - L'`adresse IP NAS` (attribut 4) ou, si l'adresse IP NAS n'existe pas, `identificateur NAS` (attribut RADIUS 32) est utilisé.**Port** : le `port NAS` (attribut 5) ou, si le port NAS n'existe pas, l'`ID de port NAS` (attribut 87) est utilisé.**CLI** - L'`ID de la station appelante` (attribut 31) est utilisé.**DNIS** : `appelé-station-ID` (attribut 30) est utilisé.

Lorsque vous spécifiez un NAR, vous pouvez utiliser un astérisque (*) comme caractère générique pour n'importe quelle valeur, ou comme élément d'une valeur quelconque pour établir une plage. Toutes les valeurs ou conditions d'une description NAR doivent être remplies pour que la NAR puisse restreindre l'accès. Cela signifie que les valeurs contiennent un ET booléen.

Ajouter une NAR partagée

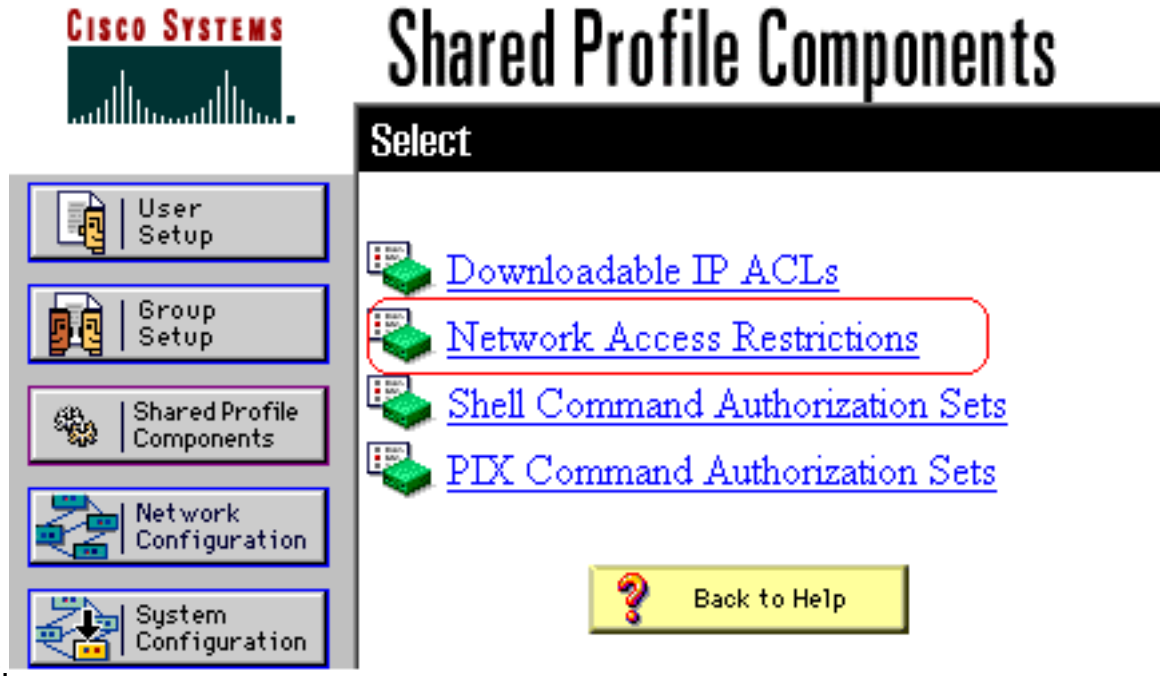
Vous pouvez créer une NAR partagée qui contient de nombreuses restrictions d'accès. Bien que l'interface Web ACS n'applique pas de limites au nombre de restrictions d'accès dans un NAR partagé ou à la longueur de chaque restriction d'accès, vous devez respecter ces limites :

- La combinaison de champs pour chaque élément de ligne ne peut pas dépasser 1 024 caractères.
- La NAR partagée ne peut pas comporter plus de 16 Ko de caractères. Le nombre d'éléments de ligne pris en charge dépend de la longueur de chaque élément de ligne. Par exemple, si vous créez un NAR basé sur CLI/DNIS où les noms des clients AAA sont 10 caractères, les numéros de port sont 5 caractères, les entrées CLI sont 15 caractères et les entrées DNIS sont 20 caractères, vous pouvez ajouter 450 éléments de ligne avant d'atteindre la limite de 16 Ko.

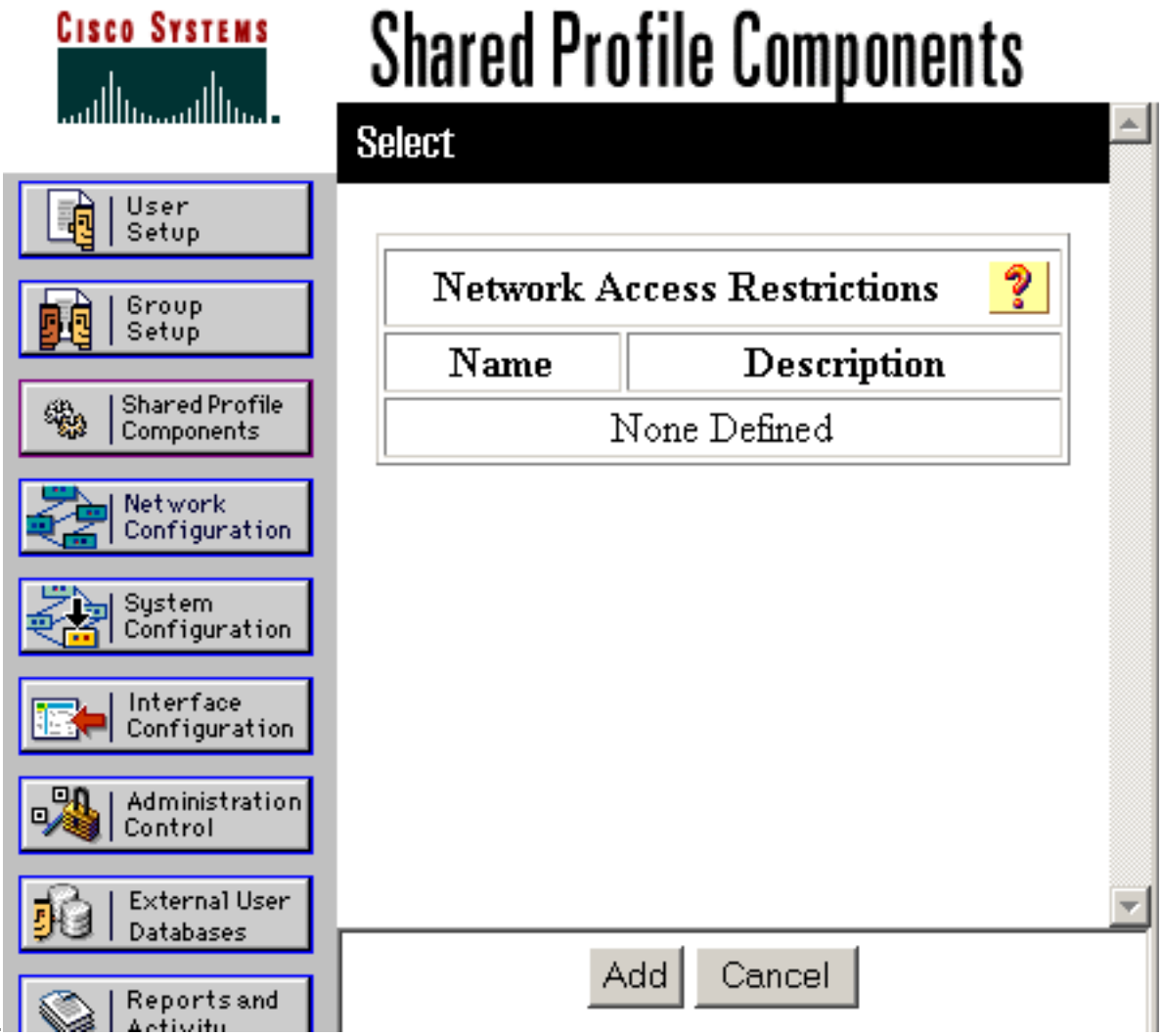
Remarque : avant de définir un NAR, assurez-vous d'avoir défini les éléments que vous avez l'intention d'utiliser dans ce NAR. Par conséquent, vous devez avoir spécifié tous les NAF et NDG et défini tous les clients AAA pertinents avant de les intégrer à la définition NAR. Pour plus d'informations, reportez-vous à la section À propos des restrictions d'accès au réseau.

Complétez ces étapes afin d'ajouter une NAR partagée :

1. Dans la barre de navigation, cliquez sur **Composants de profil partagé**.La fenêtre Composants du profil partagé s'affiche.

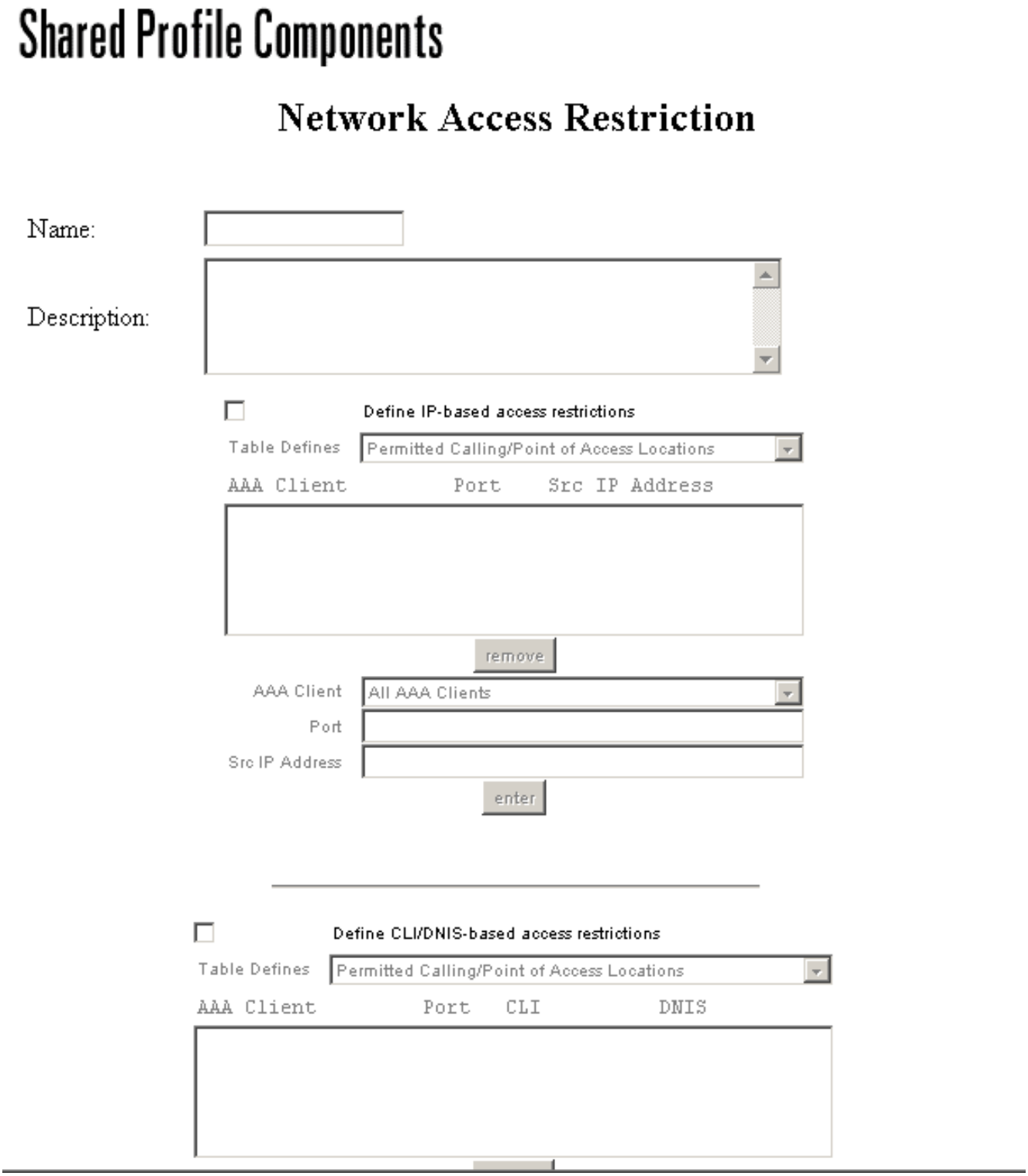


2. Cliquez sur **Restrictions d'accès au**



réseau.

3. Cliquez sur **Add**.La fenêtre Restriction d'accès au réseau s'affiche.



4. Dans la zone Nom, saisissez un nom pour le nouveau NAR partagé.**Remarque :** Le nom peut contenir jusqu'à 31 caractères. Les espaces de début et de fin ne sont pas autorisés. Les noms ne peuvent pas contenir les caractères suivants : crochet gauche ([), crochet droit (]), virgule (,) ou barre oblique (/).
5. Dans la zone Description, saisissez une description du nouveau NAR partagé. La description peut comporter jusqu'à 30 000 caractères.
6. Si vous voulez autoriser ou refuser l'accès en fonction de l'adressage IP :Cochez la case **Définir les descriptions d'accès basées sur IP**.Afin de spécifier si vous listez des adresses autorisées ou refusées, dans la liste Définitions de table, sélectionnez la valeur applicable.Sélectionnez ou saisissez les informations applicables dans chacune de ces zones :**Client AAA** : sélectionnez **Tous les clients AAA**, ou le nom du NDG, ou du NAF, ou du client AAA individuel auquel l'accès est autorisé ou refusé.**Port** : saisissez le numéro du port

auquel vous souhaitez autoriser ou refuser l'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour autoriser ou refuser l'accès à tous les ports du client AAA sélectionné.**Src IP Address** : saisissez l'adresse IP à filtrer lors de l'exécution des restrictions d'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour spécifier toutes les adresses IP.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et les zones Port et Src IP Address ne doivent pas dépasser 1024. Bien qu'ACS accepte plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier la NAR et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée**.Les informations relatives au client, au port et à l'adresse AAA apparaissent comme un élément de ligne dans le tableau.Répétez les étapes c et d afin d'entrer des éléments de ligne supplémentaires basés sur IP.

7. Si vous voulez autoriser ou refuser l'accès en fonction de l'emplacement d'appel ou de valeurs autres que les adresses IP :Cochez la case **Définir les restrictions d'accès basées sur CLI/DNIS**.Afin de spécifier si vous listez des emplacements autorisés ou refusés dans la liste Définitions de table, sélectionnez la valeur applicable.Afin de spécifier les clients auxquels cette NAR s'applique, sélectionnez l'une de ces valeurs dans la liste des clients AAA :Nom du NDGNom du client AAA particulierTous les clients AAA**Conseil :** seuls les NDG que vous avez déjà configurés sont répertoriés.Afin de spécifier les informations sur lesquelles ce NAR doit filtrer, entrez des valeurs dans ces zones, le cas échéant :**Conseil :** Vous pouvez saisir un astérisque (*) comme caractère générique pour spécifier **tout** comme valeur.**Port** : saisissez le numéro du port sur lequel filtrer.**CLI** : saisissez le numéro CLI sur lequel filtrer. Vous pouvez également utiliser cette zone pour restreindre l'accès en fonction de valeurs autres que les CLI, telles qu'une adresse IP ou MAC. Pour plus d'informations, reportez-vous à la section À propos des restrictions d'accès au réseau.**DNIS** : saisissez le numéro composé à partir duquel filtrer.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et dans les zones Port, CLI et DNIS ne doit pas dépasser 1024. Bien qu'ACS accepte plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier la NAR et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée**.Les informations qui spécifient l'élément de ligne NAR apparaissent dans le tableau.Répétez les étapes c à e afin d'entrer d'autres éléments de ligne NAR non basés sur IP.Cliquez sur **Submit** afin d'enregistrer la définition NAR partagée.ACS enregistre la NAR partagée et la répertorie dans la table **Restrictions d'accès au réseau**.

Modifier un NAR partagé

Complétez ces étapes afin de modifier une NAR partagée :

1. Dans la barre de navigation, cliquez sur **Composants de profil partagé**.La fenêtre Composants du profil partagé s'affiche.
2. Cliquez sur **Restrictions d'accès au réseau**.Le tableau Restrictions d'accès au réseau s'affiche.
3. Dans la colonne Nom, cliquez sur la NAR partagée à modifier.La fenêtre Restriction d'accès au réseau s'affiche et affiche des informations pour la NAR sélectionnée.
4. Modifiez le nom ou la description de la NAR, le cas échéant. La description peut comporter jusqu'à 30 000 caractères.
5. Afin de modifier un élément de ligne dans le tableau des restrictions d'accès basées sur IP :Double-cliquez sur l'élément de ligne à modifier.Les informations relatives à l'élément de ligne sont supprimées du tableau et écrites dans les zones situées sous le tableau.Modifiez

les informations si nécessaire.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et dans les zones Port et Src IP Address ne doit pas dépasser 1024. Bien qu'ACS puisse accepter plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier une NAR de ce type et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée**.Les informations modifiées pour cet élément de ligne sont écrites dans le tableau des restrictions d'accès basées sur IP.

6. Afin de supprimer un élément de ligne de la table de restrictions d'accès IP :Sélectionnez l'élément de ligne.Sous le tableau, cliquez sur **Supprimer**.L'élément de ligne est supprimé de la table de restrictions d'accès IP.
7. Afin de modifier un élément de ligne dans le tableau des restrictions d'accès CLI/DNIS :Double-cliquez sur l'élément de ligne à modifier.Les informations relatives à l'élément de ligne sont supprimées du tableau et écrites dans les zones situées sous le tableau.Modifiez les informations si nécessaire.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et dans les zones Port, CLI et DNIS ne doit pas dépasser 1024. Bien qu'ACS puisse accepter plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier une NAR de ce type et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée.**Les informations modifiées pour cet élément de ligne sont écrites dans le tableau des restrictions d'accès CLI/DNIS.
8. Afin de supprimer un élément de ligne de la table de restrictions d'accès CLI/DNIS :Sélectionnez l'élément de ligne.Sous le tableau, cliquez sur **Supprimer**.L'élément de ligne est supprimé du tableau des restrictions d'accès CLI/DNIS.
9. Cliquez sur **Submit** afin d'enregistrer les modifications que vous avez apportées.ACS réintroduit le filtre avec les nouvelles informations, qui prennent effet immédiatement.

Supprimer un NAR partagé

Remarque : assurez-vous de supprimer l'association d'une NAR partagée à un utilisateur ou à un groupe avant de supprimer cette NAR.

Complétez ces étapes afin de supprimer une NAR partagée :

1. Dans la barre de navigation, cliquez sur **Composants de profil partagé**.La fenêtre Composants du profil partagé s'affiche.
2. Cliquez sur **Restrictions d'accès au réseau**.
3. Cliquez sur le nom de la NAR partagée à supprimer.La fenêtre Restriction d'accès au réseau s'affiche et affiche des informations pour la NAR sélectionnée.
4. En bas de la fenêtre, cliquez sur **Supprimer**.Une boîte de dialogue vous avertit que vous êtes sur le point de supprimer une NAR partagée.
5. Cliquez sur **OK** afin de confirmer que vous voulez supprimer la NAR partagée.La NAR partagée sélectionnée est supprimée.

Définir des restrictions d'accès réseau pour un utilisateur

Vous utilisez le tableau Restrictions d'accès au réseau dans la zone Paramètres avancés du programme d'installation de l'utilisateur pour définir les NAR de trois manières :

- Appliquez les NAR partagés existants par nom.
- Définissez des restrictions d'accès basées sur IP pour autoriser ou refuser l'accès utilisateur à

un client AAA spécifié ou à des ports spécifiés sur un client AAA lorsqu'une connexion IP a été établie.
- Définissez des restrictions d'accès basées sur CLI/DNIS pour autoriser ou refuser l'accès utilisateur en fonction de CLI/DNIS utilisé.**Remarque :** Vous pouvez également utiliser la zone de restrictions d'accès basée sur CLI/DNIS pour spécifier d'autres valeurs. Reportez-vous à la section Restrictions d'accès au réseau pour plus d'informations.

En règle générale, vous définissez des NAR (partagés) à partir de la section Composants partagés afin de pouvoir appliquer ces restrictions à plusieurs groupes ou utilisateurs. Pour plus d'informations, reportez-vous à la section Ajouter une NAR partagée. Vous devez avoir coché la case **Restrictions d'accès réseau au niveau de l'utilisateur** sur la page Options avancées de la section Configuration de l'interface pour que ce jeu d'options apparaisse dans l'interface Web.

Cependant, vous pouvez également utiliser ACS pour définir et appliquer une NAR pour un utilisateur unique à partir de la section User Setup. Vous devez avoir activé le paramètre **User-Level Network Access Restrictions** sur la page Options avancées de la section Configuration d'interface pour les options de filtre IP utilisateur unique et les options de filtre CLI/DNIS utilisateur unique pour apparaître dans l'interface Web.

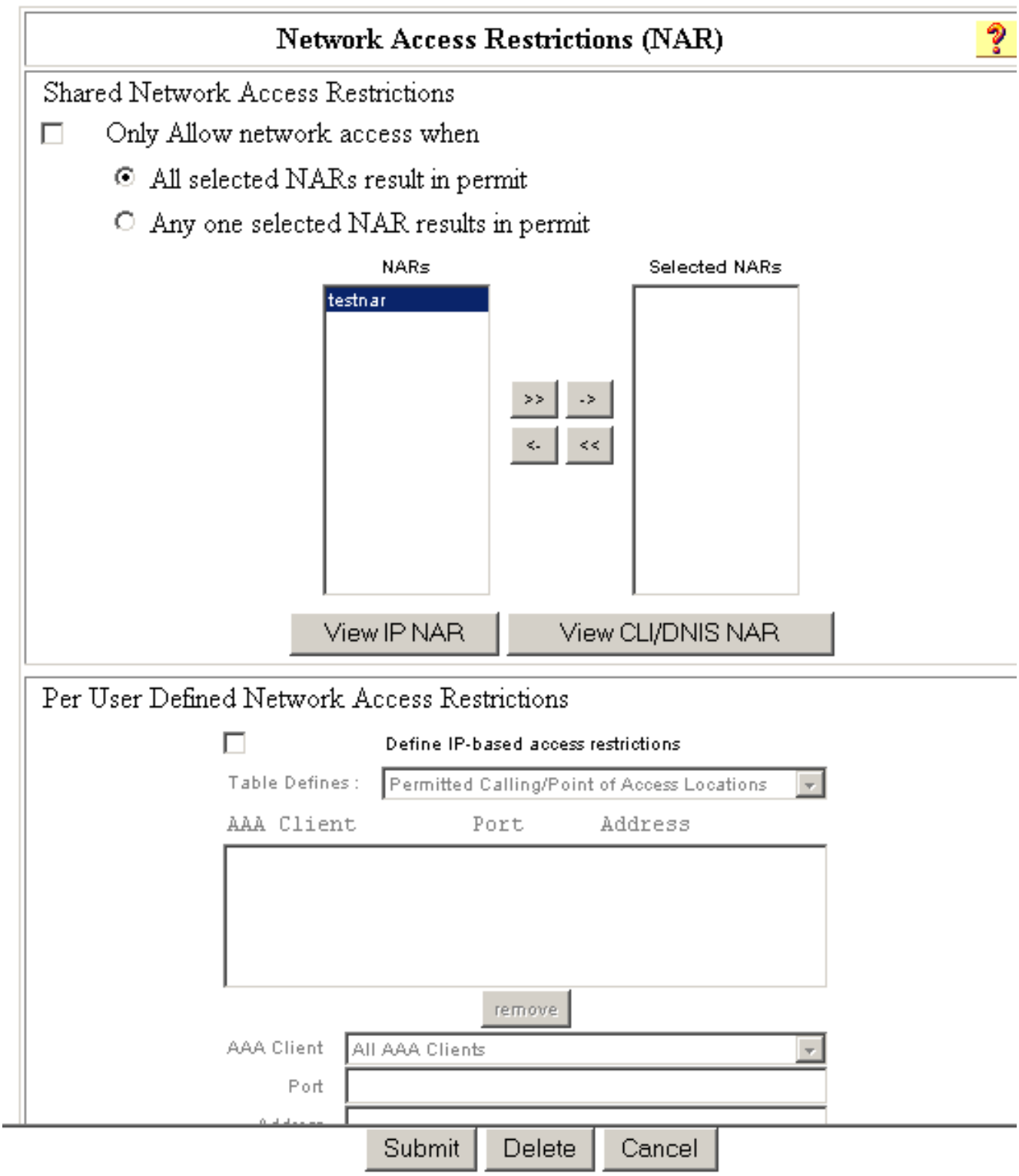
Remarque : Lorsqu'une demande d'authentification est transmise par proxy à un ACS, toutes les NAR pour les requêtes TACACS+ (Terminal Access Controller Access Control System) sont appliquées à l'adresse IP du serveur AAA de transfert, et non à l'adresse IP du client AAA d'origine.

Lorsque vous créez des restrictions d'accès par utilisateur, ACS n'applique pas de limites au nombre de restrictions d'accès et n'applique pas de limite à la longueur de chaque restriction d'accès. Mais il y a des limites strictes :

- La combinaison de champs pour chaque élément de ligne ne peut pas dépasser 1 024 caractères.
- La NAR partagée ne peut pas comporter plus de 16 Ko de caractères. Le nombre d'éléments de ligne pris en charge dépend de la longueur de chaque élément de ligne. Par exemple, si vous créez un NAR basé sur CLI/DNIS où les noms des clients AAA sont 10 caractères, les numéros de port sont 5 caractères, les entrées CLI sont 15 caractères et les entrées DNIS sont 20 caractères, vous pouvez ajouter 450 éléments de ligne avant d'atteindre la limite de 16 Ko.

Complétez ces étapes afin de définir des NAR pour un utilisateur :

1. Effectuez les étapes 1 à 3 de l'ajout d'un compte d'utilisateur de base.La fenêtre User Setup Edit s'ouvre. Le nom d'utilisateur que vous ajoutez ou modifiez apparaît en haut de la fenêtre.



2. Afin d'appliquer une NAR partagée précédemment configurée à cet utilisateur :**Remarque :** Pour appliquer un NAR partagé, vous devez l'avoir configuré sous Restrictions d'accès au réseau dans la section Composants de profil partagé. Pour plus d'informations, reportez-vous à la section Ajouter une NAR partagée.Cochez la case **Autoriser uniquement l'accès au réseau lorsque**.Afin de spécifier si une ou toutes les NAR partagées doivent demander l'accès autorisé à l'utilisateur, sélectionnez-en une, selon le cas :Tous les NARS sélectionnés

ont pour résultat l'autorisation.N'importe quelle NAR sélectionnée obtient la valeur permit.Sélectionnez un nom NAR partagé dans la liste NAR, puis cliquez sur —> (bouton flèche droite) pour déplacer le nom dans la liste Selected NARs.**Conseil :** afin d'afficher les détails du serveur des NAR partagés que vous avez sélectionnés pour appliquer, vous pouvez cliquer sur **View IP NAR** ou **View CLID/DNIS NAR**, selon le cas.

3. Afin de définir et d'appliquer une NAR, pour cet utilisateur particulier, qui autorise ou refuse cet accès utilisateur en fonction de l'adresse IP, de l'adresse IP et du port :**Remarque :** Vous devez définir la plupart des NAR dans la section Composants partagés afin de pouvoir les appliquer à plusieurs groupes ou utilisateurs. Pour plus d'informations, reportez-vous à la section Ajouter une NAR partagée.Dans le tableau Restrictions d'accès au réseau, sous Restrictions d'accès réseau définies par l'utilisateur, cochez la case **Définir des restrictions d'accès basées sur IP**.Afin de spécifier si la liste suivante spécifie les adresses IP autorisées ou refusées, dans la liste Définitions de tableau, sélectionnez une adresse :**Emplacements d'appel/point d'accès autorisésEmplacements d'appel/point d'accès refusés**Sélectionnez ou saisissez les informations dans les zones suivantes :**Client AAA** : sélectionnez **Tous les clients AAA**, ou le nom d'un groupe de périphériques réseau (NDG), ou le nom du client AAA individuel auquel autoriser ou refuser l'accès.**Port** : saisissez le numéro du port auquel autoriser ou refuser l'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour autoriser ou refuser l'accès à tous les ports du client AAA sélectionné.**Address** : saisissez la ou les adresses IP à utiliser lors de l'exécution des restrictions d'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et les zones Port et Src IP Address ne doivent pas dépasser 1024. Bien qu'ACS accepte plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier la NAR et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée**.Les informations de client, de port et d'adresse AAA spécifiées apparaissent dans le tableau situé au-dessus de la liste des clients AAA.
4. Afin d'autoriser ou de refuser cet accès utilisateur en fonction de l'emplacement d'appel ou de valeurs autres qu'une adresse IP établie :Cochez la case **Définir les restrictions d'accès basées sur CLI/DNIS**.Afin de spécifier si la liste suivante spécifie des valeurs autorisées ou refusées, dans la liste Définitions de table, sélectionnez une valeur :**Emplacements d'appel/point d'accès autorisésEmplacements d'appel/point d'accès refusés**Remplissez les cases comme indiqué :**Remarque :** Vous devez entrer une entrée dans chaque case. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour tout ou partie d'une valeur. Le format que vous utilisez doit correspondre au format de la chaîne que vous recevez de votre client AAA. Vous pouvez déterminer ce format à partir de votre journal de comptabilité RADIUS.**Client AAA** : sélectionnez **Tous les clients AAA**, ou le nom du NDG, ou le nom du client AAA individuel auquel autoriser ou refuser l'accès.**PORT** : saisissez le numéro du port auquel autoriser ou refuser l'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour autoriser ou refuser l'accès à tous les ports.**CLI** : saisissez le numéro CLI auquel autoriser ou refuser l'accès. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour autoriser ou refuser l'accès en fonction d'une partie du numéro.**Conseil :** utilisez l'entrée CLI si vous souhaitez restreindre l'accès en fonction d'autres valeurs telles qu'une adresse MAC du client Cisco Aironet. Pour plus d'informations, reportez-vous à la section À propos des restrictions d'accès au réseau.**DNIS** : saisissez le numéro DNIS auquel autoriser ou refuser l'accès. Utilisez cette entrée pour restreindre l'accès en fonction du numéro vers lequel l'utilisateur doit composer. Vous pouvez utiliser l'astérisque (*) comme caractère générique pour autoriser ou refuser l'accès en fonction d'une partie du numéro.**Conseil :** utilisez la sélection DNIS si vous souhaitez restreindre l'accès en fonction

d'autres valeurs telles qu'une adresse MAC AP Cisco Aironet. Pour plus d'informations, reportez-vous à la section À propos des restrictions d'accès au réseau.**Remarque :** Le nombre total de caractères dans la liste des clients AAA et dans les zones **Port**, **CLI** et **DNIS** ne doit pas dépasser 1024. Bien qu'ACS accepte plus de 1 024 caractères lorsque vous ajoutez une NAR, vous ne pouvez pas modifier la NAR et ACS ne peut pas l'appliquer avec précision aux utilisateurs.Cliquez sur **Entrée**.Les informations qui spécifient le client AAA, le port, l'interface de ligne de commande et DNIS apparaissent dans le tableau au-dessus de la liste des clients AAA.

5. Si vous avez terminé de configurer les options de compte utilisateur, cliquez sur **Soumettre** afin d'enregistrer les options.

Définir des restrictions d'accès réseau pour un groupe d'utilisateurs

Vous utilisez le tableau Restrictions d'accès au réseau de la configuration du groupe pour appliquer les NAR de trois manières différentes :

- Appliquez les NAR partagés existants par nom.
- Définissez des restrictions d'accès de groupe basées sur IP pour autoriser ou refuser l'accès à un client AAA spécifié ou à des ports spécifiés sur un client AAA lorsqu'une connexion IP a été établie.
- Définissez les NAR de groupe basés sur CLI/DNIS pour autoriser ou refuser l'accès à l'un ou aux deux numéros CLI ou DNIS utilisés.**Remarque :** Vous pouvez également utiliser la zone de restrictions d'accès basée sur CLI/DNIS pour spécifier d'autres valeurs. Pour plus d'informations, reportez-vous à la section À propos des restrictions d'accès au réseau.

En règle générale, vous définissez des NAR (partagés) à partir de la section Composants partagés afin que ces restrictions puissent s'appliquer à plusieurs groupes ou utilisateurs. Pour plus d'informations, reportez-vous à la section Ajouter une NAR partagée. Vous devez cocher la case **Restriction d'accès réseau partagé de niveau groupe** sur la page **Options avancées** de la section Configuration de l'interface pour que ces options apparaissent dans l'interface Web ACS.

Cependant, vous pouvez également utiliser ACS pour définir et appliquer une NAR pour un groupe unique à partir de la section **Configuration du groupe**. Vous devez vérifier le paramètre **Restriction d'accès réseau au niveau du groupe** sous la page Options avancées de la section Configuration de l'interface pour les options de filtre IP à groupe unique et les options de filtre CLI/DNIS à groupe unique pour apparaître dans l'interface Web ACS.

Remarque : Lorsqu'une demande d'authentification est transmise par proxy à un serveur ACS, toutes les NAR pour les requêtes RADIUS sont appliquées à l'adresse IP du serveur AAA de transfert et non à l'adresse IP du client AAA d'origine.

Complétez ces étapes afin de définir des NAR pour un groupe d'utilisateurs :

1. Dans la barre de navigation, cliquez sur **Configuration du groupe**.La fenêtre Sélection de la configuration du groupe s'ouvre.
2. Dans la liste Groupe, sélectionnez un groupe, puis cliquez sur **Modifier les paramètres**.Le nom du groupe apparaît en haut de la fenêtre Paramètres du groupe.