Cisco Secure ACS: Netzwerkzugriffsbeschränkungen mit AAA-Clients für Benutzer und Benutzergruppen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Network Access Restrictions (NAR) in Cisco Secure Access Control Server (ACS) 4.x mit AAA-Clients (einschließlich Router, PIX, ASA, Wireless Controller) für Benutzer und Benutzergruppen konfigurieren.

Voraussetzungen

Anforderungen

Dieses Dokument wird unter der Annahme erstellt, dass Cisco Secure ACS- und AAA-Clients konfiguriert und ordnungsgemäß funktionieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure ACS 3.0 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Netzwerkzugriffsbeschränkungen

Dieser Abschnitt beschreibt die NARs und enthält detaillierte Anweisungen zur Konfiguration und Verwaltung gemeinsam genutzter NARs.

Dieser Abschnitt behandelt folgende Themen:

Informationen zu Netzwerkzugriffsbeschränkungen

Ein NAR ist eine Definition zusätzlicher Bedingungen, die Sie in ACS festlegen müssen, bevor ein Benutzer auf das Netzwerk zugreifen kann. ACS wendet diese Bedingungen an, indem es Informationen aus Attributen verwendet, die von den AAA-Clients gesendet werden. NARs können zwar auf verschiedene Weise eingerichtet werden, aber alle basieren auf übereinstimmenden Attributinformationen, die ein AAA-Client sendet. Daher müssen Sie Format und Inhalt der Attribute verstehen, die Ihre AAA-Clients senden, wenn Sie effektive NARs verwenden möchten.

Beim Einrichten eines NAR können Sie auswählen, ob der Filter positiv oder negativ funktioniert. Das heißt, im NAR geben Sie an, ob der Netzwerkzugriff zugelassen oder verweigert werden soll, basierend auf Informationen, die von AAA-Clients im Vergleich zu den im NAR gespeicherten Informationen gesendet werden. Wenn ein NAR jedoch nicht auf ausreichende Informationen zum Betrieb stößt, wird standardmäßig der Zugriff verweigert. In dieser Tabelle sind folgende Bedingungen aufgeführt:

	IP-basiert	Nicht IP-basiert	Unzureichende Informationen
Zulassen	Zugriff gewährt	Zugriff verweigert	Zugriff verweigert
Ablehnen	Zugriff verweigert	Zugriff gewährt	Zugriff verweigert

ACS unterstützt zwei Arten von NAR-Filtern:

- **IP-basierte Filter** - IP-basierte NAR-Filter beschränken den Zugriff auf der Grundlage der IP-Adressen des Endbenutzer-Clients und des AAA-Clients. Weitere Informationen finden Sie im Abschnitt Info zu IP-basierten NAR-Filtern.
- **Nicht IP-basierte Filter** - Nicht IP-basierte NAR-Filter beschränken den Zugriff auf Basis eines einfachen Zeichenfolgenvergleichs eines vom AAA-Client gesendeten Werts. Der Wert kann die CLI-Nummer (Call Line Identification), die DNIS-Nummer (Dialed Number Identification Service), die MAC-Adresse oder ein anderer vom Client stammender Wert sein. Damit dieser

NAR-Typ funktioniert, muss der Wert in der NAR-Beschreibung exakt mit dem übereinstimmen, was vom Client gesendet wird. Dazu gehört auch das verwendete Format. Beispielsweise entspricht die Telefonnummer (217) 555-4534 nicht 217-555-4534. Weitere Informationen finden Sie im Abschnitt Informationen zu nicht IP-basierten NAR-Filtern.

Sie können einen NAR für einen bestimmten Benutzer oder eine bestimmte Benutzergruppe definieren und auf diesen anwenden. Weitere Informationen finden Sie in den Abschnitten Netzwerkzugriffsbeschränkungen für einen Benutzer festlegen oder Netzwerkzugriffsbeschränkungen für eine Benutzergruppe festlegen. Im Abschnitt "Komponenten des gemeinsam genutzten Profils" des ACS können Sie jedoch einen gemeinsam genutzten NAR erstellen und benennen, ohne direkt einen Benutzer oder eine Benutzergruppe aufzurufen. Sie geben dem freigegebenen NAR einen Namen, auf den in anderen Teilen der ACS-Webschnittstelle verwiesen werden kann. Wenn Sie dann Benutzer oder Benutzergruppen einrichten, können Sie keine, eine oder mehrere freigegebene Einschränkungen auswählen, die angewendet werden sollen. Wenn Sie die Anwendung mehrerer gemeinsam genutzter NARs auf einen Benutzer oder eine Benutzergruppe festlegen, wählen Sie eines von zwei Zugriffskriterien:

- Alle ausgewählten Filter müssen zugelassen werden.
- Jeder ausgewählte Filter muss zugelassen werden.

Sie müssen die Rangfolge verstehen, die sich auf die verschiedenen Typen von NARs bezieht. Die Reihenfolge für die NAR-Filterung ist wie folgt:

1. Gemeinsam genutzte NAR auf Benutzerebene
2. Gemeinsamer NAR auf Gruppenebene
3. Nicht gemeinsam genutzte NAR auf Benutzerebene
4. Nicht gemeinsam genutzter NAR auf Gruppenebene

Sie sollten auch verstehen, dass **die Verweigerung des Zugriffs auf jeder Ebene Vorrang vor Einstellungen auf einer anderen Ebene hat, die den Zugriff nicht verweigern**. Dies ist die einzige Ausnahme in ACS zur Regel, dass Einstellungen auf Benutzerebene Gruppeneinstellungen überschreiben. Beispielsweise gibt es für einen bestimmten Benutzer möglicherweise keine auf Benutzerebene geltenden NAR-Einschränkungen. Gehört dieser Benutzer jedoch zu einer Gruppe, die durch eine gemeinsam genutzte oder nicht gemeinsam genutzte NAR eingeschränkt ist, wird dem Benutzer der Zugriff verweigert.

Gemeinsame NARs werden in der internen ACS-Datenbank gespeichert. Sie können die Backup- und Wiederherstellungsfunktionen des ACS verwenden, um sie zu sichern und wiederherzustellen. Sie können die gemeinsam genutzten NARs zusammen mit anderen Konfigurationen auch auf sekundäre ACS replizieren.

Info zu IP-basierten NAR-Filtern

Für IP-basierte NAR-Filter verwendet ACS die angegebenen Attribute, die vom AAA-Protokoll der Authentifizierungsanfrage abhängen:

- **Wenn Sie TACACS+** verwenden, wird das Feld `rem_addr` aus dem TACACS+-Startpakettext verwendet.**Hinweis:** Wenn eine Authentifizierungsanfrage vom Proxy an einen ACS weitergeleitet wird, werden alle NARs für TACACS+-Anforderungen auf die IP-Adresse des weiterleitenden AAA-Servers angewendet, nicht auf die IP-Adresse des ursprünglichen AAA-Clients.
- **Wenn Sie RADIUS IETF verwenden**: Es muss die `Calling-Station-ID` (Attribut 31) verwendet werden.**Hinweis:** IP-basierte NAR-Filter funktionieren nur, wenn ACS das Radius Calling-

Station-Id (31)-Attribut empfängt. Die Calling-Station-ID (31) muss eine gültige IP-Adresse enthalten. Ist dies nicht der Fall, werden die DNIS-Regeln eingehalten.

AAA-Clients, die keine ausreichenden IP-Adressinformationen bereitstellen (z. B. einige Firewall-Typen), unterstützen nicht die vollständige NAR-Funktionalität.

Weitere Attribute für **IP-basierte** Einschränkungen umfassen laut Protokoll die NAR-Felder wie folgt:

- **Wenn Sie TACACS+** verwenden - Die NAR-Felder im ACS verwenden folgende Werte:**AAA-Client** - Die NAS-IP-Adresse wird von der Quelladresse im Socket zwischen ACS und dem TACACS+-Client übernommen.**Port** - Das Port-Feld wird aus dem TACACS+-Startpakettext übernommen.

Informationen zu nicht IP-basierten NAR-Filtern

Ein Nicht-IP-basierter NAR-Filter (d. h. ein DNIS/CLI-basierter NAR-Filter) ist eine Liste zulässiger oder abgelehnter Anrufe oder Zugriffspunkte, mit denen Sie einen AAA-Client einschränken können, wenn Sie keine etablierte IP-basierte Verbindung haben. Die nicht IP-basierte NAR-Funktion verwendet im Allgemeinen die CLI-Nummer und die DNIS-Nummer.

Wenn Sie jedoch anstelle der CLI eine IP-Adresse eingeben, können Sie den nicht IP-basierten Filter verwenden. auch wenn der AAA-Client keine Cisco IOS®-Softwareversion verwendet, die CLI oder DNIS unterstützt. In einer anderen Ausnahme zur Eingabe einer CLI können Sie eine MAC-Adresse eingeben, um den Zugriff zuzulassen oder zu verweigern. Wenn Sie beispielsweise einen Cisco Aironet AAA-Client verwenden. Ebenso können Sie anstelle des DNIS die Cisco Aironet AP MAC-Adresse eingeben. Das Format der im CLI-Feld angegebenen Daten - CLI, IP-Adresse oder MAC-Adresse - muss dem Format entsprechen, das Sie vom AAA-Client erhalten. Sie können dieses Format in Ihrem RADIUS-Accounting-Protokoll festlegen.

Attribute für DNIS/CLI-basierte Einschränkungen umfassen gemäß Protokoll die NAR-Felder wie folgt:

- **Wenn Sie TACACS+** verwenden - Die aufgeführten NAR-Felder verwenden folgende Werte:**AAA-Client** - Die `NAS-IP-Adresse` wird von der Quelladresse im Socket zwischen ACS und dem TACACS+-Client übernommen.**Port** - Das `Port`-Feld im TACACS+-Startpaket wird verwendet.**CLI** - Das `rem-addr`-Feld im TACACS+-Startpakettext wird verwendet.**DNIS** - Das `rem-addr`-Feld aus dem TACACS+-Startpaket wird verwendet. In Fällen, in denen die rem-addr-Daten mit dem Schrägstrich (/) beginnen, enthält das DNIS-Feld die rem-addr-Daten ohne Schrägstrich (/).**Hinweis:** Wenn eine Authentifizierungsanfrage vom Proxy an einen ACS weitergeleitet wird, werden alle NARs für TACACS+-Anforderungen auf die IP-Adresse des weiterleitenden AAA-Servers angewendet, nicht auf die IP-Adresse des ursprünglichen AAA-Clients.
- **Wenn Sie RADIUS verwenden** - Die aufgeführten NAR-Felder verwenden folgende Werte:**AAA-Client** - Die `NAS-IP-Adresse` (Attribut 4) oder, wenn die NAS-IP-Adresse nicht vorhanden ist, der `NAS-Identifier` (RADIUS-Attribut 32) wird verwendet.**Port** - Der `NAS-Port` (Attribut 5) oder, falls der NAS-Port nicht vorhanden ist, die `NAS-Port-ID` (Attribut 87) wird verwendet.**CLI**: Die `Calling-Station-ID` (Attribut 31) wird verwendet.**DNIS** - Die `genannte Station-ID` (Attribut 30) wird verwendet.

Wenn Sie ein NAR angeben, können Sie ein Sternchen (*) als Platzhalter für einen beliebigen Wert oder als Teil eines beliebigen Werts zum Festlegen eines Bereichs verwenden. Alle Werte

oder Bedingungen in einer NAR-Beschreibung müssen erfüllt sein, damit der NAR den Zugriff einschränken kann. Dies bedeutet, dass die Werte ein boolesches UND enthalten.

Hinzufügen eines gemeinsam genutzten NAR

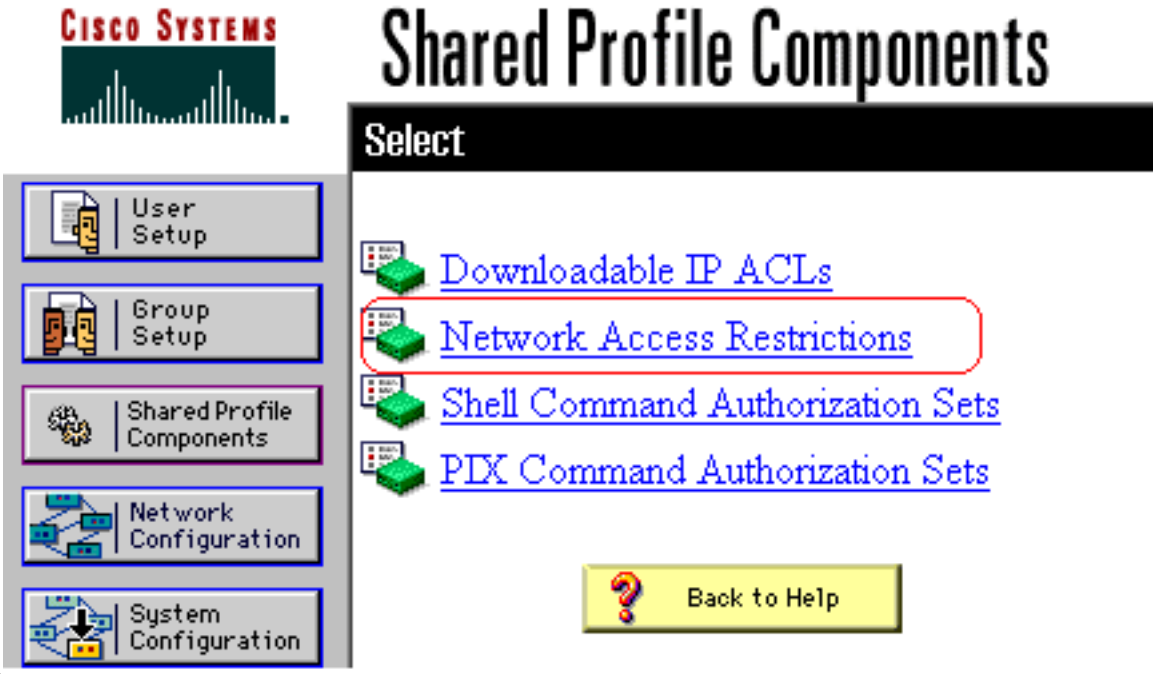
Sie können eine freigegebene NAR erstellen, die viele Zugriffsbeschränkungen enthält. Obwohl die ACS-Webschnittstelle keine Beschränkungen für die Anzahl der Zugriffsbeschränkungen in einem gemeinsamen NAR oder für die Länge jeder Zugriffsbeschränkung durchsetzt, müssen Sie die folgenden Beschränkungen einhalten:

- Die Feldkombination für jeden Posten darf 1024 Zeichen nicht überschreiten.
- Der freigegebene NAR darf nicht mehr als 16 KB Zeichen enthalten. Die Anzahl der unterstützten Posten hängt von der Länge der einzelnen Posten ab. Wenn Sie beispielsweise einen CLI/DNIS-basierten NAR erstellen, bei dem die AAA-Clientnamen 10 Zeichen enthalten, die Portnummern 5 Zeichen, die CLI-Einträge 15 Zeichen und die DNIS-Einträge 20 Zeichen enthalten, können Sie 450 Zeilen hinzufügen, bevor Sie den Grenzwert von 16 KB erreichen.

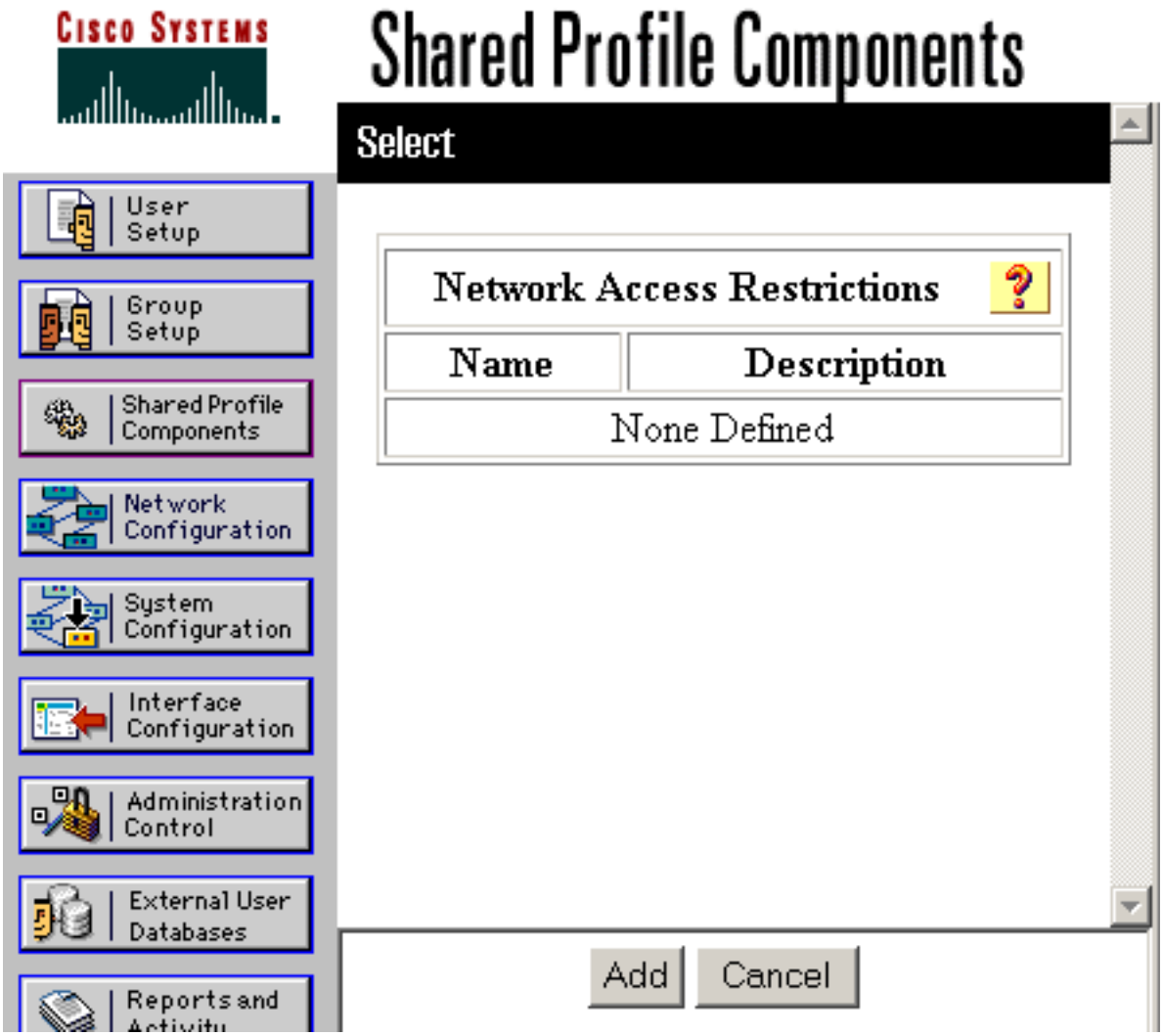
Hinweis: Bevor Sie einen NAR definieren, stellen Sie sicher, dass Sie die Elemente festgelegt haben, die Sie in diesem NAR verwenden möchten. Daher müssen Sie alle NAFs und NDGs angegeben und alle relevanten AAA-Clients definiert haben, bevor Sie sie in die NAR-Definition aufnehmen können. Weitere Informationen finden Sie im Abschnitt Informationen zu Netzwerkzugriffsbeschränkungen.

Gehen Sie wie folgt vor, um einen gemeinsamen NAR hinzuzufügen:

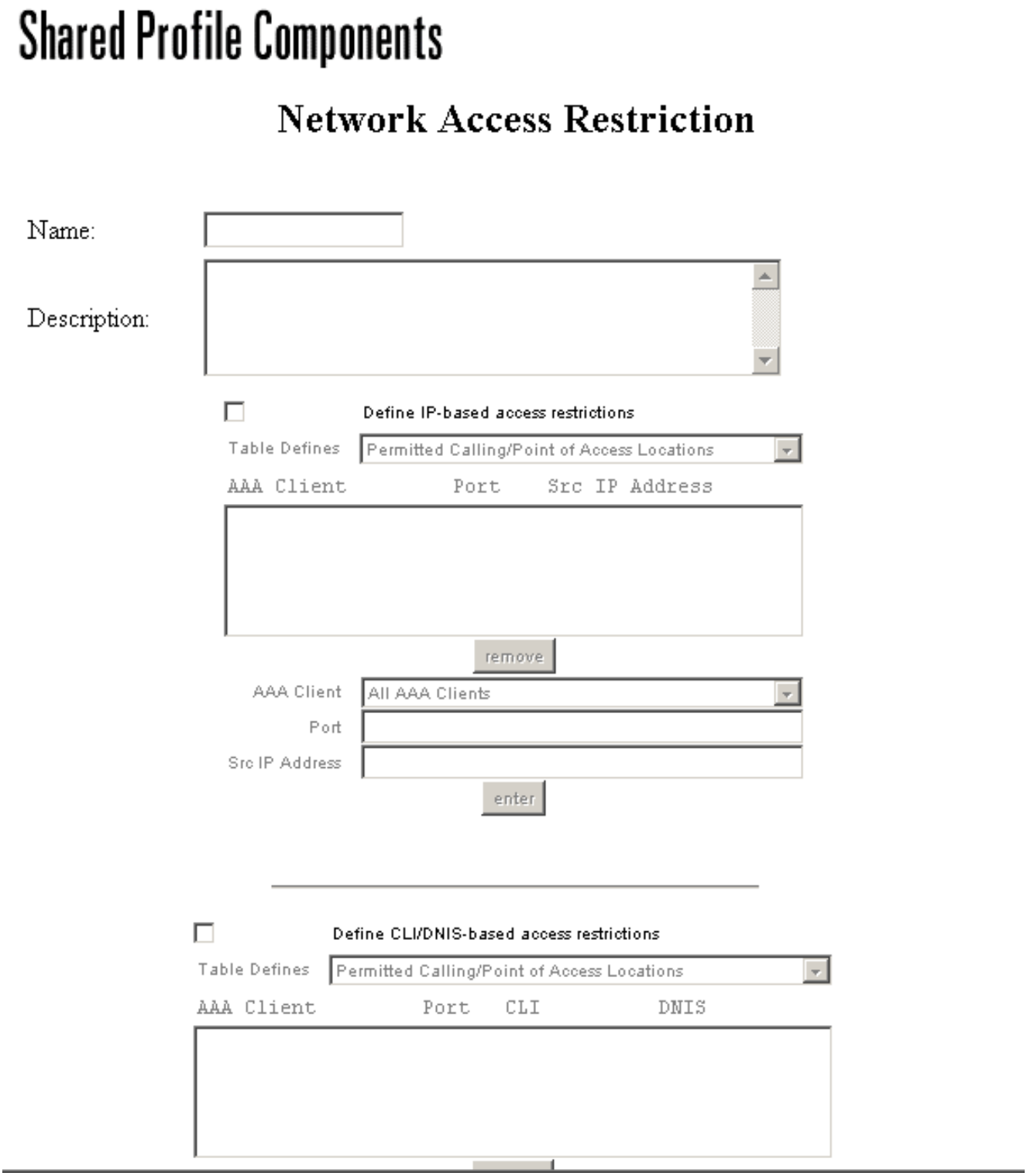
1. Klicken Sie in der Navigationsleiste auf **Komponenten freigegebener Profile**.Das Fenster Komponenten für freigegebene Profile wird angezeigt.



2. Klicken Sie auf **Netzwerkzugriffsbeschränkungen**.



3. Klicken Sie auf **Hinzufügen**.Das Fenster Netzwerkzugriffsbeschränkung wird angezeigt.



4. Geben Sie im Feld Name einen Namen für die neue freigegebene NAR ein.**Hinweis:** Der Name darf bis zu 31 Zeichen enthalten. Leads und nachfolgende Leerzeichen sind nicht zulässig. Namen dürfen keine der folgenden Zeichen enthalten: linke Halterung ([), rechte Halterung (]), Komma (,) oder Schrägstrich (/).
5. Geben Sie im Feld Description (Beschreibung) eine Beschreibung des neuen gemeinsam genutzten NAR ein. Die Beschreibung kann bis zu 30.000 Zeichen enthalten.
6. Wenn Sie den Zugriff basierend auf der IP-Adressierung zulassen oder verweigern möchten:Aktivieren Sie das Kontrollkästchen **IP-basierte Zugriffsbeschreibungen definieren**.Um anzugeben, ob Adressen aufgeführt werden sollen, die zugelassen oder abgelehnt werden, wählen Sie in der Liste Tabellendefinitionen den entsprechenden Wert aus.Wählen Sie in jedem der folgenden Felder die entsprechenden Informationen aus, oder geben Sie diese ein:**AAA-Client**: Wählen Sie **Alle AAA-Clients** oder den Namen des NDG,

des NAF oder des einzelnen AAA-Clients aus, auf den der Zugriff zugelassen oder verweigert wird.**Port** - Geben Sie die Nummer des Ports ein, zu dem Sie den Zugriff zulassen oder verweigern möchten. Sie können das Sternchen (*) als Platzhalter verwenden, um den Zugriff auf alle Ports des ausgewählten AAA-Clients zuzulassen oder zu verweigern.**Src IP Address (Src-IP-Adresse)**: Geben Sie die IP-Adresse ein, die beim Ausführen von Zugriffsbeschränkungen gefiltert werden soll. Sie können das Sternchen (*) als Platzhalter verwenden, um alle IP-Adressen anzugeben.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und in den Feldern Port und Src IP Address darf 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptiert, wenn Sie ein NAR hinzufügen, können Sie das NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**.Die Informationen zu AAA-Client, -Port und -Adresse werden in der Tabelle als Posten angezeigt.Wiederholen Sie die Schritte c und d, um weitere IP-basierte Posten einzugeben.

7. Wenn Sie den Zugriff basierend auf dem Anrufstandort oder anderen Werten als IP-Adressen zulassen oder verweigern möchten:Aktivieren Sie das Kontrollkästchen **CLI/DNIS-basierte Zugriffsbeschränkungen definieren**.Um anzugeben, ob Standorte aufgeführt werden, die in der Liste Tabellendefinitionen zugelassen oder abgelehnt sind, wählen Sie den entsprechenden Wert aus.Um die Clients anzugeben, auf die dieser NAR angewendet wird, wählen Sie einen der folgenden Werte aus der Liste der AAA-Clients aus:Name der NDGDer Name des bestimmten AAA-ClientsAlle AAA-Clients**Tipp:** Es sind nur NDGs aufgeführt, die Sie bereits konfiguriert haben.Um die Informationen anzugeben, für die dieser NAR filtern soll, geben Sie ggf. Werte in die folgenden Felder ein:**Tipp:** Sie können ein Sternchen (*) als Platzhalter eingeben, um **alle** als Wert anzugeben.**Port** - Geben Sie die Nummer des Ports ein, an den gefiltert werden soll.**CLI** - Geben Sie die CLI-Nummer ein, auf die gefiltert werden soll. Sie können dieses Feld auch verwenden, um den Zugriff auf der Grundlage anderer Werte als CLIs, z. B. einer IP-Adresse oder einer MAC-Adresse, zu beschränken. Weitere Informationen finden Sie im Abschnitt Informationen zu Netzwerkzugriffsbeschränkungen.**DNIS** (DNIS): Geben Sie die Nummer ein, zu der Sie sich einwählen, um zu filtern.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und in den Feldern Port, CLI und DNIS darf 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptiert, wenn Sie ein NAR hinzufügen, können Sie das NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**.Die Informationen, die das NAR-Zeilenelement angeben, werden in der Tabelle angezeigt.Wiederholen Sie die Schritte c bis e, um weitere nicht IP-basierte NAR-Posten einzugeben.Klicken Sie auf **Senden**, um die freigegebene NAR-Definition zu speichern.ACS speichert den freigegebenen NAR und listet ihn in der Tabelle **Netzwerkzugriffsbeschränkungen auf**.

Bearbeiten eines gemeinsam genutzten NAR

Gehen Sie wie folgt vor, um einen gemeinsamen NAR zu bearbeiten:

1. Klicken Sie in der Navigationsleiste auf **Komponenten freigegebener Profile**.Das Fenster Komponenten für freigegebene Profile wird angezeigt.
2. Klicken Sie auf **Netzwerkzugriffsbeschränkungen**.Die Tabelle mit den Netzwerkzugriffsbeschränkungen wird angezeigt.
3. Klicken Sie in der Spalte Name auf die freigegebene NAR, die Sie bearbeiten möchten.Das Fenster Network Access Restriction (Netzwerkzugriffsbeschränkung) wird angezeigt und

zeigt Informationen für den ausgewählten NAR an.
4. Bearbeiten Sie gegebenenfalls den Namen oder die Beschreibung des NAR. Die Beschreibung kann bis zu 30.000 Zeichen enthalten.
5. So bearbeiten Sie einen Posten in der IP-basierten Zugriffslizenz:Doppelklicken Sie auf den Posten, den Sie bearbeiten möchten.Die Informationen für den Posten werden aus der Tabelle entfernt und in die Felder unter der Tabelle geschrieben.Bearbeiten Sie die Informationen nach Bedarf.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und in den Feldern Port und Src IP Address darf 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptieren kann, wenn Sie ein NAR hinzufügen, können Sie ein solches NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**.Die bearbeiteten Informationen für diesen Posten werden in die IP-basierte Zugriffslizenz-Tabelle geschrieben.
6. So entfernen Sie einen Posten aus der IP-basierten Tabelle für Zugriffsbeschränkungen:Wählen Sie den Posten aus.Klicken Sie unter der Tabelle auf **Entfernen**.Der Posten wird aus der Tabelle mit IP-basierten Zugriffsbeschränkungen entfernt.
7. So bearbeiten Sie einen Posten in der CLI/DNIS-Zugriffslizenz-Tabelle:Doppelklicken Sie auf den Posten, den Sie bearbeiten möchten.Die Informationen für den Posten werden aus der Tabelle entfernt und in die Felder unter der Tabelle geschrieben.Bearbeiten Sie die Informationen nach Bedarf.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und in den Feldern Port, CLI und DNIS darf 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptieren kann, wenn Sie ein NAR hinzufügen, können Sie ein solches NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**Die bearbeiteten Informationen für diesen Posten werden in die Tabelle mit CLI/DNIS-Zugriffsbeschränkungen geschrieben.
8. So entfernen Sie einen Posten aus der CLI/DNIS-Zugriffslizenz:Wählen Sie den Posten aus.Klicken Sie unter der Tabelle auf **Entfernen**.Der Posten wird aus der Tabelle mit CLI/DNIS-Zugriffsbeschränkungen entfernt.
9. Klicken Sie auf **Senden**, um die vorgenommenen Änderungen zu speichern.ACS gibt den Filter mit den neuen Informationen wieder, die sofort wirksam werden.

Löschen eines gemeinsam genutzten NAR

Hinweis: Stellen Sie sicher, dass die Zuordnung eines gemeinsamen NAR zu einem beliebigen Benutzer oder einer Gruppe entfernt wird, bevor Sie diesen NAR löschen.

Gehen Sie wie folgt vor, um eine gemeinsam genutzte NAR zu löschen:

1. Klicken Sie in der Navigationsleiste auf **Komponenten freigegebener Profile**.Das Fenster Komponenten für freigegebene Profile wird angezeigt.
2. Klicken Sie auf **Netzwerkzugriffsbeschränkungen**.
3. Klicken Sie auf den Namen des freigegebenen NAR, den Sie löschen möchten.Das Fenster Network Access Restriction (Netzwerkzugriffsbeschränkung) wird angezeigt und zeigt Informationen für den ausgewählten NAR an.
4. Klicken Sie unten im Fenster auf **Löschen**.In einem Dialogfeld werden Sie darauf hingewiesen, dass Sie im Begriff sind, einen gemeinsam genutzten NAR zu löschen.
5. Klicken Sie auf **OK**, um zu bestätigen, dass Sie den freigegebenen NAR löschen möchten.Der ausgewählte gemeinsam genutzte NAR wird gelöscht.

Festlegen von Netzwerkzugriffsbeschränkungen für einen Benutzer

Sie können die Tabelle "Network Access Restrictions" (Netzwerkzugriffsbeschränkungen) im Bereich "Advanced Settings" (Erweiterte Einstellungen) des Benutzer-Setups verwenden, um die NARs auf drei Arten festzulegen:

- Anwenden vorhandener gemeinsam genutzter NARs nach Namen
- Definieren Sie IP-basierte Zugriffsbeschränkungen, um den Benutzerzugriff auf einen angegebenen AAA-Client oder auf bestimmte Ports eines AAA-Clients zuzulassen oder zu verweigern, wenn eine IP-Verbindung hergestellt wurde.
- Definieren Sie CLI/DNIS-basierte Zugriffsbeschränkungen, um den Benutzerzugriff basierend auf der verwendeten CLI/DNIS zuzulassen oder zu verweigern.**Hinweis:** Sie können auch den Bereich CLI/DNIS-basierte Zugriffsbeschränkungen verwenden, um andere Werte anzugeben. Weitere Informationen finden Sie im Abschnitt Netzwerkzugriffsbeschränkungen.

In der Regel definieren Sie im Abschnitt "Gemeinsame Komponenten" (Shared, Shared) NARs, sodass Sie diese Einschränkungen auf mehrere Gruppen oder Benutzer anwenden können. Weitere Informationen finden Sie im Abschnitt Hinzufügen eines gemeinsamen NAR. Sie müssen das Kontrollkästchen **Netzwerkzugriffsbeschränkungen auf Benutzerebene** auf der Seite Erweiterte Optionen im Abschnitt Schnittstellenkonfiguration aktiviert haben, damit dieser Satz von Optionen in der Webschnittstelle angezeigt werden kann.

Sie können jedoch auch ACS verwenden, um im Abschnitt User Setup (Benutzereinrichtung) einen NAR für einen einzelnen Benutzer zu definieren und anzuwenden. Sie müssen die Einstellung **Netzwerkzugriffsbeschränkungen auf Benutzerebene** auf der Seite Erweiterte Optionen im Abschnitt Schnittstellenkonfiguration für IP-basierte Filteroptionen für einen Benutzer und für die Anzeige in der Webschnittstelle CLI/DNIS-basierte Filteroptionen für einen Benutzer aktiviert haben.

Hinweis: Wenn ein Proxy eine Authentifizierungsanfrage an einen ACS weiterleitet, werden alle NARs für TACACS+-Anforderungen (Terminal Access Controller Access Control System) auf die IP-Adresse des weiterleitenden AAA-Servers angewendet, nicht auf die IP-Adresse des ursprünglichen AAA-Clients.

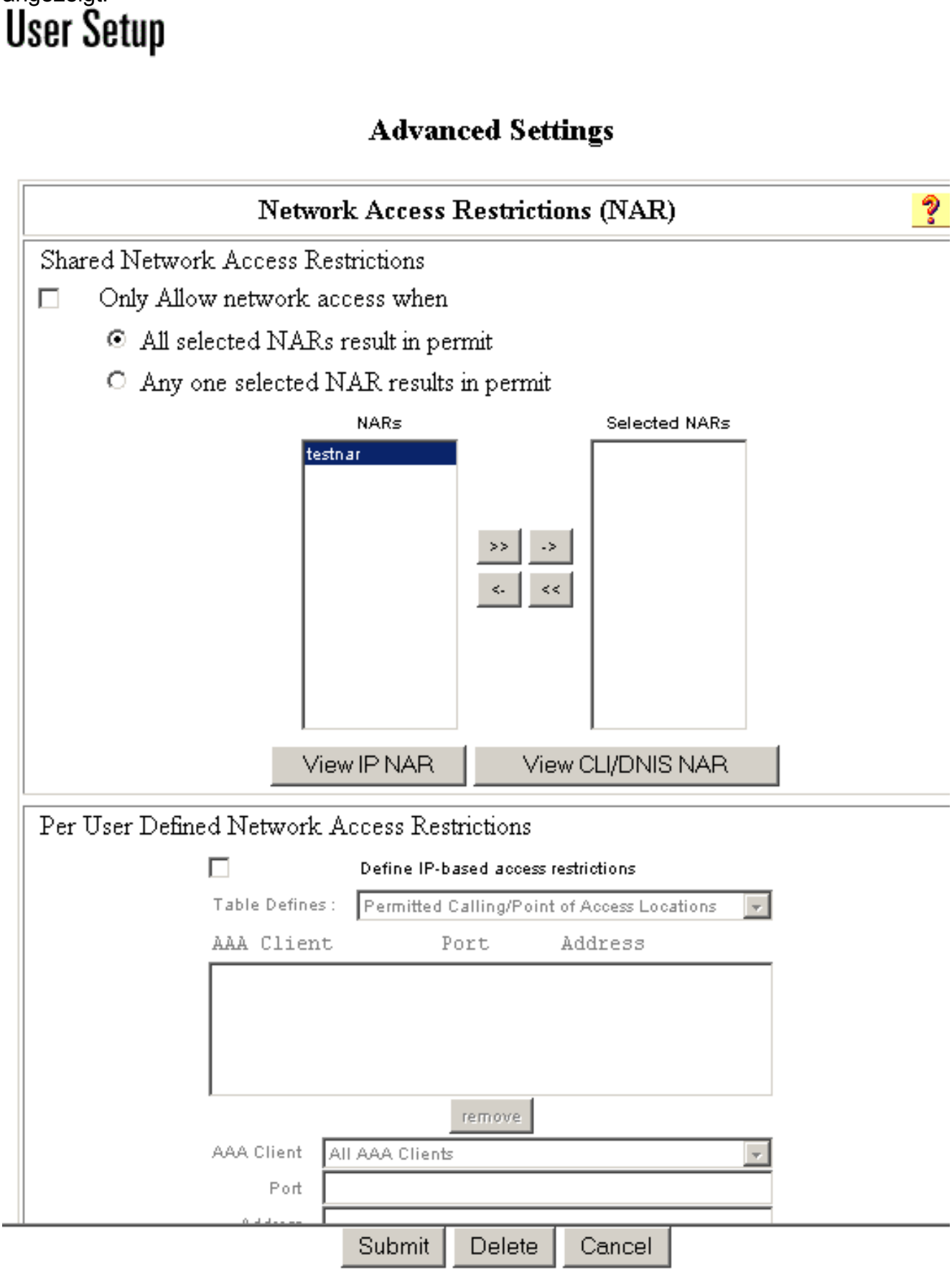
Wenn Sie Zugriffsbeschränkungen auf Benutzerbasis erstellen, setzt ACS keine Beschränkungen für die Anzahl der Zugriffsbeschränkungen durch und setzt keine Längenbeschränkung für jede Zugriffsbeschränkung durch. Es gibt jedoch strenge Grenzen:

- Die Feldkombination für jeden Posten darf 1024 Zeichen lang sein.
- Der freigegebene NAR darf nicht mehr als 16 KB Zeichen enthalten. Die Anzahl der unterstützten Posten hängt von der Länge der einzelnen Posten ab. Wenn Sie beispielsweise einen CLI/DNIS-basierten NAR erstellen, bei dem die AAA-Clientnamen 10 Zeichen enthalten, die Portnummern 5 Zeichen, die CLI-Einträge 15 Zeichen und die DNIS-Einträge 20 Zeichen enthalten, können Sie 450 Zeilen hinzufügen, bevor Sie den Grenzwert von 16 KB erreichen.

Gehen Sie wie folgt vor, um NARs für einen Benutzer festzulegen:

1. Führen Sie die Schritte 1 bis 3 durch, um ein einfaches Benutzerkonto hinzuzufügen.Das Fenster Bearbeiten der Benutzereinrichtung wird geöffnet. Der von Ihnen hinzugefügte oder bearbeitete Benutzername wird oben im Fenster

angezeigt.



2. So wenden Sie einen zuvor konfigurierten gemeinsamen NAR auf diesen Benutzer an:**Hinweis:** Um einen gemeinsam genutzten NAR anzuwenden, müssen Sie ihn im Abschnitt "Komponenten des gemeinsam genutzten Profils" unter "Netzwerkzugriffsbeschränkungen" konfiguriert haben. Weitere Informationen finden Sie im Abschnitt Hinzufügen eines gemeinsamen NAR.Aktivieren Sie das Kontrollkästchen **Nur**

Netzwerkzugriff bei aktiviertem Kontrollkästchen.Um festzulegen, ob eine oder alle gemeinsam genutzten NAR für den Benutzer eine Zugriffsberechtigung beantragen müssen, wählen Sie eine, falls zutreffend:Alle ausgewählten NARS resultieren in einer Genehmigung.Alle ausgewählten NARs sind zulässig.Wählen Sie in der Liste der NARs einen gemeinsamen NAR-Namen aus, und klicken Sie dann auf —> (Nach-rechts-Taste), um den Namen in die Liste der ausgewählten NARs zu verschieben.**Tipp:** Um die Serverdetails der freigegebenen NARs anzuzeigen, die Sie angewendet haben, können Sie auf **IP NAR anzeigen** oder **CLID/DNIS NAR** ggf. klicken.

3. Um einen NAR für diesen Benutzer zu definieren und anzuwenden, der diesen Benutzerzugriff basierend auf der IP-Adresse oder der IP-Adresse und dem Port zulässt oder verweigert:**Hinweis:** Sie sollten die meisten NARs im Abschnitt "Gemeinsame Komponenten" definieren, damit Sie sie auf mehrere Gruppen oder Benutzer anwenden können. Weitere Informationen finden Sie im Abschnitt Hinzufügen eines gemeinsamen NAR.Aktivieren Sie in der Tabelle Netzwerkzugriffsbeschränkungen unter Benutzerdefinierte Netzwerkzugriffsbeschränkungen das Kontrollkästchen **IP-basierte Zugriffsbeschränkungen definieren**.Um anzugeben, ob in der nachfolgenden Liste zulässige oder abgelehnte IP-Adressen angegeben sind, wählen Sie eine der folgenden Optionen aus der Liste Tabellendefinitionen:**Zulässige Anrufe/ZugangspunkteAbgelehnte Anrufe/Zugangspunkte**Wählen Sie die folgenden Felder aus, oder geben Sie diese ein:**AAA-Client**: Wählen Sie **Alle AAA-Clients**, den Namen einer Netzwerkgerätegruppe (NDG) oder den Namen des einzelnen AAA-Clients aus, auf den der Zugriff zugelassen oder verweigert werden soll.**Port** - Geben Sie die Nummer des Ports ein, zu dem der Zugriff zugelassen oder verweigert werden soll. Sie können das Sternchen (*) als Platzhalter verwenden, um den Zugriff auf alle Ports des ausgewählten AAA-Clients zuzulassen oder zu verweigern.**Adresse** - Geben Sie die IP-Adresse oder die IP-Adressen ein, die bei der Durchführung von Zugriffsbeschränkungen verwendet werden sollen. Sie können das Sternchen (*) als Platzhalter verwenden.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und die Felder für die Port- und SRC-IP-Adressen dürfen 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptiert, wenn Sie ein NAR hinzufügen, können Sie das NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**.Die angegebenen AAA-Client-, Port- und Adressinformationen werden in der Tabelle über der Liste der AAA-Clients angezeigt.
4. Um diesen Benutzerzugriff basierend auf dem Anrufstandort oder anderen Werten als einer festgelegten IP-Adresse zuzulassen oder zu verweigern, gehen Sie wie folgt vor:Aktivieren Sie das Kontrollkästchen **CLI/DNIS-basierte Zugriffsbeschränkungen definieren**.Um anzugeben, ob in der nachfolgenden Liste zulässige oder abgelehnte Werte angegeben werden, wählen Sie eine der folgenden Optionen aus der Liste Tabellendefinitionen:**Zulässige Anrufe/ZugangspunkteAbgelehnte Anrufe/Zugangspunkte**Füllen Sie die Felder wie gezeigt aus:**Hinweis:** Sie müssen in jedem Feld einen Eintrag erstellen. Sie können das Sternchen (*) als Platzhalter für den gesamten oder einen Teil eines Werts verwenden. Das Format, das Sie verwenden, muss dem Format der Zeichenfolge entsprechen, die Sie vom AAA-Client erhalten. Sie können dieses Format in Ihrem RADIUS-Accounting-Protokoll festlegen.**AAA-Client**: Wählen Sie **Alle AAA-Clients**, den Namen des NDG oder den Namen des einzelnen AAA-Clients aus, auf den der Zugriff zugelassen oder verweigert werden soll.**PORT** (PORT): Geben Sie die Nummer des Ports ein, zu dem der Zugriff zugelassen oder verweigert werden soll. Sie können das Sternchen (*) als Platzhalter verwenden, um den Zugriff auf alle Ports zuzulassen oder zu verweigern.**CLI** - Geben Sie die CLI-Nummer ein, der der Zugriff gestattet oder verweigert

werden soll. Sie können das Sternchen (*) als Platzhalter verwenden, um den Zugriff basierend auf einem Teil der Nummer zuzulassen oder zu verweigern.**Tipp:** Verwenden Sie den CLI-Eintrag, wenn Sie den Zugriff auf Basis anderer Werte wie einer MAC-Adresse des Cisco Aironet-Clients einschränken möchten. Weitere Informationen finden Sie im Abschnitt Informationen zu Netzwerkzugriffsbeschränkungen.**DNIS** - Geben Sie die DNIS-Nummer ein, der der Zugriff gestattet oder verweigert werden soll. Verwenden Sie diesen Eintrag, um den Zugriff basierend auf der Nummer zu beschränken, unter der der Benutzer wählen wird. Sie können das Sternchen (*) als Platzhalter verwenden, um den Zugriff basierend auf einem Teil der Nummer zuzulassen oder zu verweigern.**Tipp:** Verwenden Sie die DNIS-Auswahl, wenn Sie den Zugriff auf Basis anderer Werte wie einer Cisco Aironet AP MAC-Adresse einschränken möchten. Weitere Informationen finden Sie im Abschnitt Informationen zu Netzwerkzugriffsbeschränkungen.**Hinweis:** Die Gesamtzahl der Zeichen in der AAA-Client-Liste und den **Port-**, **CLI-** und **DNIS-**Feldern darf 1024 nicht überschreiten. Obwohl ACS mehr als 1024 Zeichen akzeptiert, wenn Sie ein NAR hinzufügen, können Sie das NAR nicht bearbeiten, und ACS kann es nicht korrekt auf Benutzer anwenden.Klicken Sie auf **Eingabe**.Die Informationen, die den AAA-Client, den Port, die CLI und den DNIS angeben, werden in der Tabelle über der Liste der AAA-Clients angezeigt.
5. Wenn Sie die Konfiguration der Benutzerkontenoptionen abgeschlossen haben, klicken Sie auf **Senden**, um die Optionen aufzuzeichnen.

Festlegen von Netzwerkzugriffsbeschränkungen für eine Benutzergruppe

Sie verwenden die Tabelle "Network Access Restrictions" (Netzwerkzugriffsbeschränkungen) im Gruppensetup, um NARs auf drei verschiedene Arten anzuwenden:

- Anwenden vorhandener gemeinsam genutzter NARs nach Namen
- Definieren Sie IP-basierte Zugriffsbeschränkungen für Gruppen, um den Zugriff auf einen angegebenen AAA-Client oder auf bestimmte Ports eines AAA-Clients zu erlauben oder zu verweigern, wenn eine IP-Verbindung hergestellt wurde.
- Definieren Sie CLI/DNIS-basierte Gruppen-NARs, um den Zugriff auf die CLI-Nummer oder die verwendete DNIS-Nummer zuzulassen oder zu verweigern.**Hinweis:** Sie können auch den Bereich CLI/DNIS-basierte Zugriffsbeschränkungen verwenden, um andere Werte anzugeben. Weitere Informationen finden Sie im Abschnitt Informationen zu Netzwerkzugriffsbeschränkungen.

In der Regel definieren Sie im Abschnitt "Gemeinsame Komponenten" (Shared, Shared) NARs, sodass diese Einschränkungen auf mehrere Gruppen oder Benutzer angewendet werden können. Weitere Informationen finden Sie im Abschnitt Hinzufügen eines gemeinsamen NAR. Sie müssen das Kontrollkästchen **Gruppenbasierte Zugriffsbeschränkung für freigegebene Netzwerke** auf der **Seite Erweiterte Optionen** im Abschnitt Schnittstellenkonfiguration aktivieren, damit diese Optionen in der ACS-Webschnittstelle angezeigt werden.

Sie können jedoch auch ACS verwenden, um im Abschnitt **Gruppeneinrichtung** eine NAR für eine Gruppe zu definieren und anzuwenden. Sie müssen die Einstellung für **Netzwerkzugriffsbeschränkungen auf Gruppenebene** auf der Seite Erweiterte Optionen im Abschnitt Schnittstellenkonfiguration für einzelne Gruppen-IP-basierte Filteroptionen und einzelne Gruppen-CLI/DNIS-basierte Filteroptionen überprüfen, um in der ACS-Webschnittstelle angezeigt zu werden.

Hinweis: Wenn eine Authentifizierungsanfrage vom Proxy an einen ACS-Server weitergeleitet wird, werden alle NARs für RADIUS-Anfragen auf die IP-Adresse des weiterleitenden AAA-Servers angewendet, nicht auf die IP-Adresse des ursprünglichen AAA-Clients.

Gehen Sie wie folgt vor, um NARs für eine Benutzergruppe festzulegen:

1. Klicken Sie in der Navigationsleiste auf **Gruppeneinrichtung**.Das Fenster "Gruppeneinrichtung auswählen" wird geöffnet.
2. Wählen Sie aus der Liste Gruppe eine Gruppe aus, und klicken Sie dann auf **Einstellungen bearbeiten**.Der Name der Gruppe wird oben im Fenster Gruppeneinstellungen angezeigt.