مصدر المحتوى الإضافي الآمن - NAR مع عملاء AAA للمستخدمين ومجموعات المستخدمين

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
قيود الوصول إلى الشبكة
حول قيود الوصول إلى الشبكة
إضافة NAR مشترك
تحرير NAR مشترك
حذف خط اتصال مشترك
تعيين قيود الوصول إلى الشبكة لمستخدم
تعيين قيود الوصول إلى الشبكة لمجموعة مستخدمين
معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين تقييدات الوصول إلى الشبكة (NAR) في الإصدار x.4 من Cisco لخادم التحكم في الوصول الآمن (ACS) باستخدام عملاء AAA (بما في ذلك الموجهات و PIX و ASA ووحدات التحكم اللاسلكية) للمستخدمين ومجموعات المستخدمين.

المتطلبات الأساسية

المتطلبات

يتم إنشاء هذا المستند بافتراض تكوين عملاء Cisco Secure ACS و AAA والعمل بشكل صحيح.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ACS 3.0 الآمن من Cisco والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

قيود الوصول إلى الشبكة

يصف هذا القسم قوائم التحكم في الوصول للإنترنت، ويقدم تعليمات تفصيلية لتكوين قوائم التحكم في الوصول للإنترنت المشتركة وإدارتها.

يحتوي هذا القسم على الموضوعات التالية:

- حول قيود الوصول إلى الشبكة
- إضافة NAR مشترك
- تحرير NAR مشترك
- حذف خط اتصال مشترك

حول قيود الوصول إلى الشبكة

NAR هو تعريف، تضعه في ACS، للشروط الإضافية التي يجب عليك استيفاؤها قبل أن يتمكن المستخدم من الوصول إلى الشبكة. يطبق ACS هذه الشروط باستخدام معلومات من سمات يرسلها عملاء AAA. على الرغم من أنه يمكنك إعداد قوائم التحكم في الوصول (NARs) بعدة طرق، فإنها تستند جميعها إلى معلومات السمة المطابقة التي يرسلها عميل AAA. لذلك، يجب أن تفهم تنسيق ومحتوى السمات التي يرسلها عملاء AAA إذا كنت تريد إستخدام قوائم التحكم في الوصول (NARs) الفعالة.

عندما تقوم بإنشاء وحدة مكافحة الحرائق، يمكنك إختيار إذا ما كان المرشح يعمل بشكل إيجابي أو سلبي. هذا يعني أنك في قائمة التحكم في الوصول للبنية الأساسية (NAR) تحدد ما إذا كنت تسمح بالوصول إلى الشبكة أو ترفضه بناء على المعلومات المرسلة من عملاء AAA عند مقارنتها بالمعلومات المخزنة في قائمة التحكم في الوصول للبنية الأساسية (NAR). ومع ذلك، إذا لم تواجه وحدة التحكم في الشبكة (NAR) معلومات كافية لتشغيلها، فإنها تقوم بالإعدادات الافتراضية لرفض الوصول. يوضح هذا الجدول هذه الشروط:

	مستند إلى IP	**غير مستند إلى IP**	**معلومات غير كافية**
تصريح	تم منح حق الوصول	تم رفض الوصول	تم رفض الوصول
تنكر	تم رفض الوصول	تم منح حق الوصول	تم رفض الوصول

يدعم ACS نوعين من مرشحات NAR:

- **عوامل تصفية قائمة على بروتوكول IP — تعمل** عوامل تصفية NAR المستندة إلى بروتوكول IP على الحد من الوصول بناء على عناوين IP الخاصة بعميل المستخدم النهائي وعميل AAA. راجع قسم حول عوامل تصفية NAR المستندة إلى IP للحصول على مزيد من المعلومات.
- **عوامل تصفية غير قائمة على IP — تعمل** عوامل تصفية NAR غير المستندة إلى IP على الحد من الوصول بناء على مقارنة سلسلة بسيطة لقيمة تم إرسالها من عميل AAA. يمكن أن تكون القيمة رقم تعريف سطر الاتصال (CLI) أو رقم خدمة التعرف على الرقم المطلوب (DNIS) أو عنوان MAC أو قيمة أخرى تنشأ من العميل. لتشغيل هذا النوع من NAR، يجب أن تتطابق القيمة الواردة في وصف NAR تماما مع ما يتم إرساله من العميل، والذي يتضمن أي تنسيق يتم إستخدامه. على سبيل المثال، رقم الهاتف (217) 555-4534 لا يطابق 217-555-4534. راجع قسم حول عوامل تصفية NAR غير المستندة إلى IP للحصول على مزيد من المعلومات.

يمكنك تحديد NAR لمستخدم معين أو مجموعة مستخدمين معينين وتطبيقه على. راجع تعيين قيود الوصول إلى الشبكة لمستخدم أو تعيين قيود الوصول إلى الشبكة لأقسام مجموعة مستخدمين للحصول على مزيد من المعلومات. ومع ذلك، في قسم مكونات ملف التعريف المشترك من ACS، يمكنك إنشاء وتسمية خط اتصال مشترك بدون

الاستشهاد مباشرة بأي مستخدم أو مجموعة مستخدمين. أنت تعطي ال NAR مشترك اسم أن يستطيع كنت مرجع في آخر جزء من ال ACS موقع قارن. ثم، عندما تقوم بإعداد مستخدمين أو مجموعات مستخدمين، يمكنك تحديد لا شيء، واحد، أو قيود مشتركة متعددة ليتم تطبيقها. عندما تحدد تطبيق قوائم التحكم بالوصول المشتركة المتعددة لمستخدم أو مجموعة مستخدمين، فإنك تختار أحد معيارين للوصول:

- يجب أن تسمح كافة عوامل التصفية المحددة.
- يجب أن يسمح أي عامل تصفية محدد.

يجب أن تفهم ترتيب الأسبقية المرتبط بالأنواع المختلفة من قوائم التحكم في الوصول للإنترنت. هذا هو ترتيب ترشيح NAR:

1. NAR المشتركة على مستوى المستخدم
2. وحدة نار مشتركة على مستوى المجموعة
3. NAR غير المشتركة على مستوى المستخدم
4. وحدة نار غير مشتركة على مستوى المجموعة

يجب أن تفهم أيضا أن **منع الوصول على أي مستوى له الأسبقية على الإعدادات على مستوى آخر التي لا تمنع الوصول**. هذا هو الاستثناء الوحيد في ACS لقاعدة أن إعدادات مستوى المستخدم تتجاوز إعدادات مستوى المجموعة. على سبيل المثال، قد لا يكون لدى مستخدم معين أي قيود NAR على مستوى المستخدم تنطبق. ومع ذلك، إذا كان ذلك المستخدم ينتمي إلى مجموعة مقيدة بواسطة NAR مشتركة أو غير مشتركة، يتم رفض الوصول إلى المستخدم.

يتم الاحتفاظ بقوائم التحكم في الشبكة (NAR) المشتركة في قاعدة البيانات الداخلية ل ACS. يمكنك إستخدام ميزات النسخ الاحتياطي والاستعادة ل ACS لإجراء نسخ إحتياطي لها واستعادتها. يمكنك أيضا نسخ شبكات NAR المشتركة، مع التكوينات الأخرى، إلى ACS الثانوية.

حول عوامل تصفية NAR المستندة إلى IP

بالنسبة لعوامل تصفية NAR المستندة إلى IP، يستخدم ACS السمات كما هو موضح، والتي تعتمد على بروتوكول AAA الخاص بطلب المصادقة:

- **إذا كنت تستخدم TACACS+**— يتم إستخدام حقل `rem_addr` من نص حزمة TACACS+ بدء التشغيل.**ملاحظة:** عند إعادة توجيه طلب مصادقة بواسطة وكيل إلى ACS، يتم تطبيق أي من قوائم التحكم في الوصول لطلبات TACACS+ على عنوان IP الخاص بخادم AAA لإعادة التوجيه، وليس على عنوان IP الخاص بعميل AAA الأصلي.
- **إذا كنت تستخدم RADIUS IETF**— فيجب إستخدام (31).**ملاحظة:** تعمل عوامل تصفية NAR المستندة إلى IP فقط إذا تلقت ACS سمة 31 (RADIUS Call-Station-ID). يجب أن يحتوي معرف 31 (Call-Station) على عنوان IP صالح. وإذا لم تفعل ذلك، فإنها سوف تقع ضمن قواعد DNIS.

لا تدعم عملاء AAA التي لا توفر معلومات كافية عن عنوان IP (على سبيل المثال، بعض أنواع جدار الحماية) وظائف NAR الكاملة.

تتضمن السمات الأخرى للقيود **المستندة إلى IP**، لكل بروتوكول، حقول NAR كما هو موضح:

- **إذا كنت تستخدم TACACS+**— تستخدم حقول NAR في ACS القيم التالية:**عميل AAA**— يتم أخذ عنوان NAS-IP من عنوان المصدر في المقبس بين ACS وعميل TACACS+.**المنفذ**— يتم أخذ حقل المنفذ من نص حزمة TACACS+ بدء التشغيل.

حول عوامل تصفية NAR غير المستندة إلى IP

عامل تصفية NAR غير المستند إلى IP (أي عامل تصفية NAR القائم على DNIS/CLI) عبارة عن قائمة بمواقع الاتصال أو نقاط الوصول المسموح بها أو المرفوضة التي يمكنك إستخدامها لتقييد عميل AAA عندما لا يكون لديك اتصال يستند إلى IP. تستخدم ميزة NAR غير المستندة إلى IP بشكل عام رقم CLI ورقم DNIS.

ومع ذلك، عند إدخال عنوان IP بدلا من واجهة سطر الأوامر، يمكنك إستخدام عامل التصفية غير المستند إلى IP؛ حتى عندما لا يستخدم عميل AAA إصدار برنامج Cisco IOS®الذي يدعم CLI أو DNIS. في إستثناء آخر لإدخال واجهة سطر أوامر (CLI)، يمكنك إدخال عنوان MAC للسماح بالوصول أو رفضه. على سبيل المثال، عند إستخدام عميل Cisco Aironet AAA. وبالمثل، يمكنك إدخال عنوان MAC لنقطة الوصول Cisco Aironet AP بدلا من DNIS. يجب أن يتطابق تنسيق ما تقوم بتحديده في مربع CLI- CLI أو عنوان IP أو عنوان MAC- مع تنسيق ما تتلقاه من عميل AAA. يمكنك تحديد هذا التنسيق من سجل محاسبة RADIUS الخاص بك.

تتضمن سمات القيود المستندة إلى DNIS/CLI، لكل بروتوكول، حقول NAR كما هو موضح:

- **إذا كنت تستخدم TACACS+**- تستخدم حقول NAR المدرجة هذه القيم:**عميل AAA**— يتم أخذ `NAS-IP` من عنوان المصدر في المقبس بين ACS وعميل TACACS+.**المنفذ**— يتم إستخدام حقل في نص حزمة بدء TACACS+.**CLI**— يتم إستخدام حقل `rem-addr` في نص حزمة بدء TACACS+.**DNIS**— يتم إستخدام حقل `rem-addr` المأخوذ من نص حزمة بدء TACACS+. في الحالات التي تبدأ فيها بيانات rem-addr بالمائلة (/)، يحتوي حقل DNIS على بيانات rem-addr بدون المائلة (/).**ملاحظة:** عند إعادة توجيه طلب مصادقة بواسطة وكيل إلى ACS، يتم تطبيق أي من قوائم التحكم في الوصول لطلبات TACACS+ على عنوان IP الخاص بخادم AAA لإعادة التوجيه، وليس على عنوان IP الخاص بعميل AAA الأصلي.
- **إذا كنت تستخدم RADIUS**- فإن حقول NAR المدرجة تستخدم القيم التالية:**عميل AAA**— `NAS-IP` (السمة 4) أو، في حالة عدم وجود عنوان NAS-IP، يتم إستخدام `NAS` (سمة RADIUS 32).**المنفذ**— يتم إستخدام `NAS-Port` (السمة 5) أو، إذا لم يكن منفذ NAS موجودا، `NAS-port-ID` (السمة 87).**CLI**— يتم إستخدام (السمة 31).**DNIS**— يتم إستخدام المستدعي (السمة 30).

عندما تحدد NAR، يمكنك إستخدام علامة نجمية (*) كحرف بدل لأي قيمة، أو كجزء من أي قيمة لإنشاء نطاق. يجب استيفاء كافة القيم أو الشروط الواردة في وصف NAR لتقييد الوصول من قبل NAR. هذا يعني أن القيم تحتوي على قيمة منطقية و.

إضافة NAR مشترك

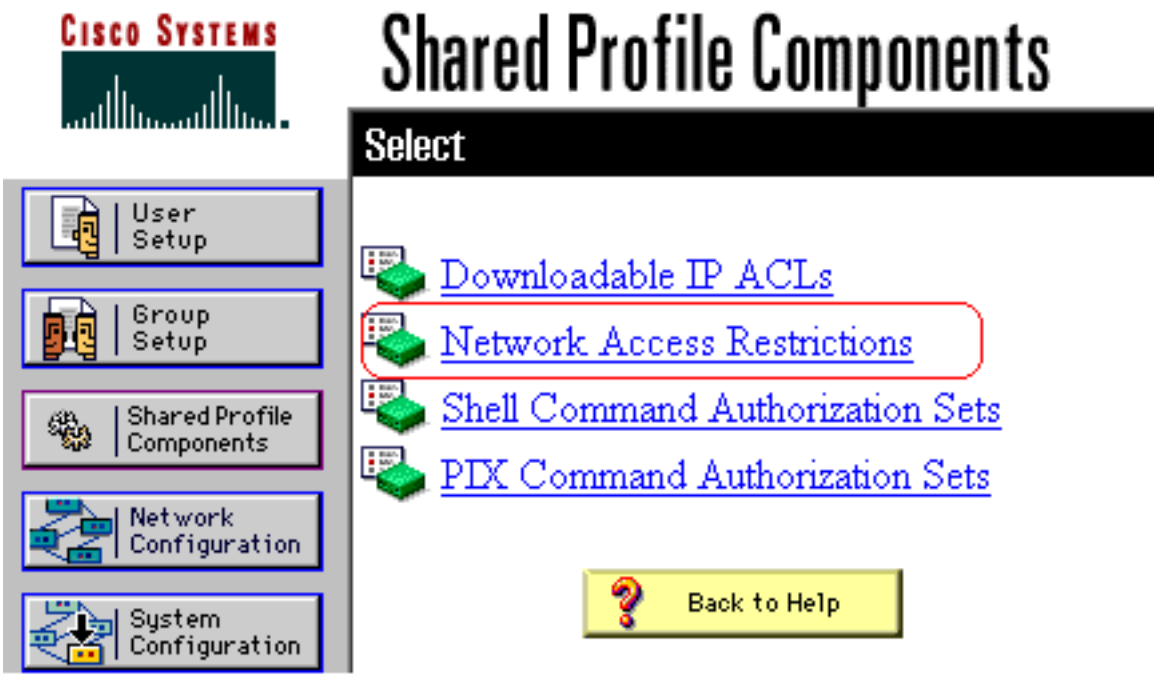
يمكنك إنشاء NAR مشترك يحتوي على العديد من قيود الوصول. على الرغم من أن واجهة ويب ل ACS لا تفرض حدودا على عدد قيود الوصول في NAR مشترك أو على طول كل قيد وصول، إلا أنه يجب عليك التقيد بهذه الحدود:

- لا يمكن أن تتجاوز مجموعة الحقول لكل عنصر بند 1024 حرفا.
- لا يمكن أن يحتوي NAR المشترك على أكثر من 16 كيلوبايت من الأحرف. يعتمد عدد عناصر البنود المدعومة على طول كل عنصر بند. على سبيل المثال، إذا قمت بإنشاء خط اتصال يستند إلى واجهة سطر الأوامر (CLI)/(DNIS حيث تكون أسماء عملاء AAA هي 10 حروف، وتكون أرقام المنافذ هي 5 حروف، وتكون إدخالات واجهة سطر الأوامر (15 (CLI حرفا، وتكون إدخالات DNIS هي 20 حرفا، فيمكنك إضافة 450 عنصرا من عناصر السطر قبل أن تصل إلى حد 16 كيلوبايت.

ملاحظة: قبل أن تقوم بتعريف NAR، تأكد من أنك قمت بتحديد العناصر التي تنوي إستخدامها في NAR. لذلك، يجب أن تكون قد حددت جميع NAF و NDGs، وعرفت جميع عملاء AAA المعنيين، قبل أن تجعلهم جزءا من تعريف NAR. راجع قسم حول قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.

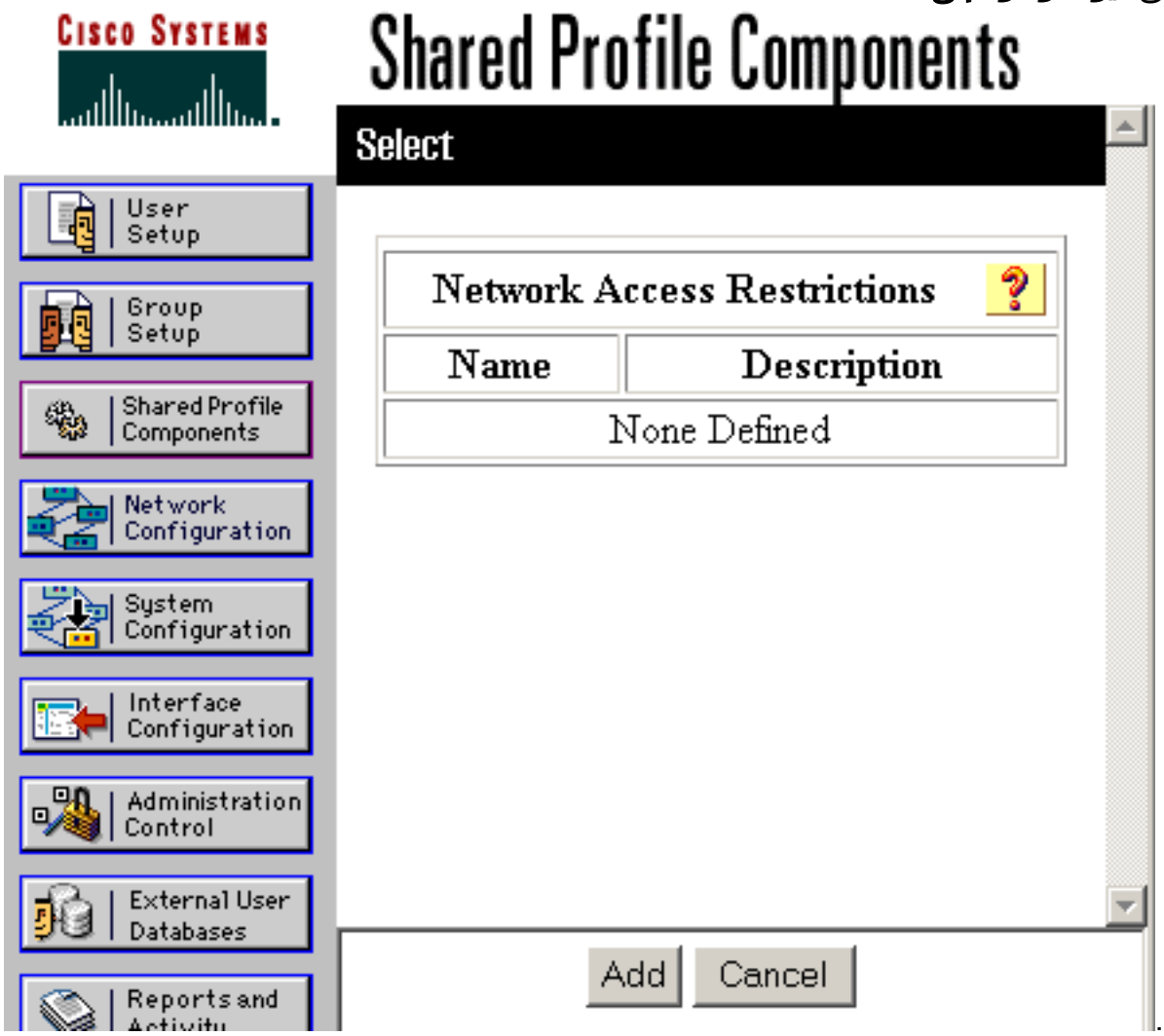
أتمت هذا steps in order to أضفت مشترك نار:

1. في شريط التنقل، انقر على **مكونات ملف التخصيص المشترك**.تظهر نافذة مكونات التوصيف



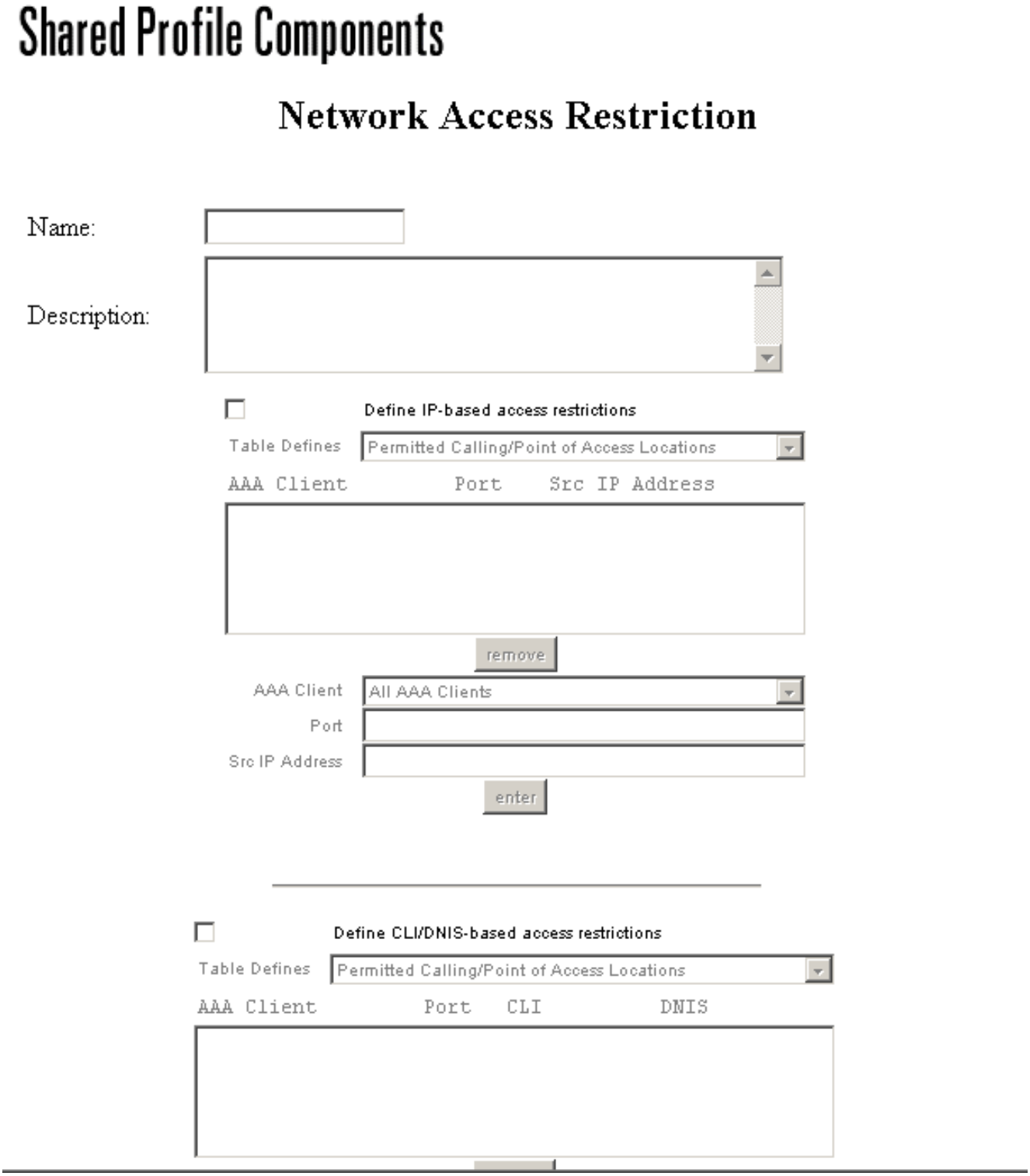
المشترك.

2. انقر على **قيود الوصول إلى**



الشبكة.

3. انقر فوق **إضافة (Add)**.يظهر إطار "تقييد الوصول إلى الشبكة".



4. في مربع الاسم، قم بإدخال اسم ل NAR المشترك الجديد.**ملاحظة:** يمكن أن يحتوي الاسم على ما يصل إلى 31 حرفا. غير مسموح بالمسافات البادئة والزائدة. لا يمكن أن تحتوي الأسماء على هذه الأحرف: قوس يسار ([)، قوس يمين (])، فاصلة (،)، أو شرطة (/).
5. في مربع الوصف، أدخل وصفا ل NAR المشترك الجديد. يمكن أن يصل الوصف إلى 30،000 حرف.
6. إذا كنت ترغب في السماح بالوصول أو رفضه استنادا إلى عنونة IP:حدد خانة الاختيار **تعريف أوصاف الوصول المستندة إلى IP**.لتحديد ما إذا كنت تقوم بإدراج العناوين المسموح بها أو المرفوضة، حدد القيمة القابلة للتطبيق من قائمة تعريف الجدول.قم بتحديد المعلومات القابلة للتطبيق أو إدخالها في كل من هذه المربعات:**عميل AAA**— حدد **جميع عملاء AAA**، أو اسم NDG، أو NAF، أو عميل AAA الفردي، الذي يتم السماح بالوصول إليه أو رفضه.**المنفذ**—أدخل رقم المنفذ الذي تريد السماح بالوصول إليه أو رفضه. يمكنك إستخدام العلامة النجمية (*) كحرف بدل للسماح بالوصول إلى جميع المنافذ على عميل AAA المحدد أو رفضه.**عنوان IP** ل **SRC**—أدخل عنوان IP للتصفية عند تنفيذ قيود الوصول. يمكنك إستخدام العلامة النجمية (*) كحرف بدل لتحديد جميع عناوين IP.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات عنوان IP

للمنفذ و Src 1024. على الرغم من أن ACS يقبل أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR ولا يمكن ل ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**.تظهر معلومات عميل AAA والمنفذ والعنوان كعنصر سطر في الجدول.كرر الخطوات C و D لإدخال عناصر بنود إضافية مستندة إلى IP.

7. إذا كنت ترغب في السماح بالوصول أو رفضه استنادا إلى موقع الاتصال أو القيم بخلاف عناوين IP:حدد خانة الاختيار **تعريف تقييدات الوصول المستندة إلى CLI/DNIS**.لتحديد ما إذا كنت تسرد المواقع المسموح بها أو المرفوضة من قائمة تعريف الجدول، حدد القيمة القابلة للتطبيق.لتحديد العملاء الذين ينطبق عليهم هذا NAR، حدد إحدى القيم التالية من قائمة عملاء AAA:اسم المديرية الوطنية للتنميةاسم عميل AAA المعينجميع عملاء AAA**تلميح:** يتم سرد فقط NDGs التي قمت بتكوينها بالفعل.دخلت in order to عينت المعلومة على أي هذا NAR أن مرشح، قيمة في هذا صندوق، حسب الانطباق:**تلميح:** يمكنك إدخال علامة نجمية (*) كحرف بدل لتحديد **الكل** كقيمة.**المنفذ**—أدخل عدد المنافذ التي سيتم التصفية عليها.**CLI**—أدخل رقم واجهة سطر الأوامر الذي سيتم التصفية عليه. يمكنك أيضا إستخدام هذا المربع لتقييد الوصول بناء على قيم أخرى غير CLIs، مثل عنوان IP أو عنوان MAC. راجع قسم حول قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.**DNIS**—أدخل الرقم الذي تم طلبه عليه للتصفية.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات المنفذ و CLI و DNIS 1024. على الرغم من أن ACS يقبل أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR ولا يمكن ل ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**.تظهر المعلومات التي تحدد عنصر سطر NAR في الجدول.كرر الخطوات من c إلى e لإدخال عناصر إضافية لسطر NAR غير المستندة إلى IP.انقر فوق **إرسال** لحفظ تعريف NAR المشترك.يحفظ ACS NAR المشترك ويسرد في جدول **تقييدات الوصول إلى الشبكة**.

تحرير NAR مشترك

أتمت هذا steps in order to حررت مشترك NAR:

1. في شريط التنقل، انقر على **مكونات ملف التخصيص المشترك**.تظهر نافذة مكونات التوصيف المشترك.
2. انقر على **قيود الوصول إلى الشبكة**.يظهر جدول تقييدات الوصول إلى الشبكة.
3. في عمود "الاسم"، انقر فوق NAR المشترك الذي تريد تحريره.يظهر إطار "تقييد الوصول إلى الشبكة" ويعرض معلومات عن NAR المحدد.
4. قم بتحرير اسم أو وصف NAR، حسب ما هو منطبق. يمكن أن يصل الوصف إلى 30،000 حرف.
5. لتحرير عنصر بند في جدول قيود الوصول المستندة إلى IP:انقر نقرا مزدوجا فوق عنصر السطر الذي تريد تحريره.تتم إزالة المعلومات الخاصة بعنصر البند من الجدول وتتم كتابتها إلى المربعات الموجودة تحت الجدول.قم بتحرير المعلومات، حسب الحاجة.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات عنوان IP للمنفذ و Src 1024. على الرغم من أن ACS يمكنه قبول أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR هذا ويتعذر على ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**.تتم كتابة المعلومات المحررة لعنصر البند هذا إلى جدول قيود الوصول المستندة إلى IP.
6. لإزالة عنصر سطر من جدول قيود الوصول المستندة إلى IP:حدد عنصر البند.تحت الجدول، انقر فوق **إزالة**.تمت إزالة عنصر البند من جدول قيود الوصول المستندة إلى IP.
7. لتحرير عنصر سطر في جدول تقييدات الوصول إلى CLI/DNIS:انقر نقرا مزدوجا فوق عنصر السطر الذي تريد تحريره.تتم إزالة المعلومات الخاصة بعنصر البند من الجدول وتتم كتابتها إلى المربعات الموجودة تحت الجدول.قم بتحرير المعلومات، حسب الحاجة.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات المنفذ و CLI و DNIS 1024. على الرغم من أن ACS يمكنه قبول أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR هذا ويتعذر على ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**تتم كتابة المعلومات المحررة لعنصر السطر هذا إلى جدول تقييدات الوصول إلى CLI/DNIS.
8. لإزالة عنصر سطر من جدول تقييدات الوصول إلى CLI/DNIS:حدد عنصر البند.تحت الجدول، انقر فوق **إزالة**.تتم إزالة عنصر البند من جدول تقييدات الوصول إلى CLI/DNIS.
9. انقر فوق **إرسال** لحفظ التغييرات التي قمت بها.يقوم ACS بإعادة إدخال عامل التصفية باستخدام المعلومات الجديدة، والتي تدخل حيز التنفيذ على الفور.

حذف خط اتصال مشترك

ملاحظة: تأكد من إزالة اقتران NAR المشترك لأي مستخدم أو مجموعة قبل حذف NAR.

أتمت هذا steps in order to محات مشترك NAR:

1. في شريط التنقل، انقر على **مكونات ملف التخصيص المشترك**.تظهر نافذة مكونات التوصيف المشترك.
2. انقر على **قيود الوصول إلى الشبكة**.
3. انقر فوق اسم NAR المشترك الذي تريد حذفه.يظهر إطار "تقييد الوصول إلى الشبكة" ويعرض معلومات عن NAR المحدد.
4. في أسفل النافذة، انقر على **حذف**.تحذرك الشاشة من أنك على وشك حذف NAR مشترك.
5. طقطقة **ok** in order to أكدت أن أنت تريد أن يمحو ال NAR مشترك.يتم حذف NAR المشترك المحدد.

تعيين قيود الوصول إلى الشبكة لمستخدم

تستخدم جدول تقييدات الوصول إلى الشبكة في منطقة الإعدادات المتقدمة من إعداد المستخدم لضبط قوائم التحكم في الوصول إلى الشبكة بثلاث طرق:

- تطبيق قوائم التحكم في الوصول للإنترنت المشتركة الموجودة بالاسم.
- تحديد قيود الوصول المستندة إلى IP للسماح بوصول المستخدم إلى عميل AAA محدد أو إلى منافذ محددة على عميل AAA أو رفضه عند إنشاء اتصال IP.
- قم بتحديد قيود الوصول المستندة إلى واجهة سطر الأوامر (CLI)/DNIS للسماح بوصول المستخدم أو رفضه استنادا إلى CLI/DNIS التي يتم إستخدامها.**ملاحظة:** يمكنك أيضا إستخدام منطقة قيود الوصول المستندة إلى CLI/DNIS لتحديد قيم أخرى. راجع قسم قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.

في العادة، تقوم بتعريف قوائم التحكم في الوصول (المشتركة) من خلال قسم المكونات المشتركة بحيث يمكنك تطبيق هذه القيود على أكثر من مجموعة أو مستخدم واحد. راجع قسم إضافة NAR مشترك للحصول على مزيد من المعلومات. يجب أن تكون قد حددت خانة الاختيار **تقييدات الوصول إلى الشبكة على مستوى المستخدم** في صفحة الخيارات المتقدمة في قسم تكوين الواجهة لهذه المجموعة من الخيارات التي ستظهر في واجهة الويب.

مهما، أنت يستطيع أيضا استعملت ACS أن يعين وطبق NAR لمستخدم وحيد من ضمن قسم إعداد المستخدم. يجب تمكين إعداد **تقييدات الوصول إلى الشبكة على مستوى المستخدم** في صفحة الخيارات المتقدمة في قسم تكوين الواجهة لخيارات عامل التصفية المستند إلى IP لمستخدم واحد وخيارات عامل تصفية مستند إلى CLI/DNIS لمستخدم واحد لكي تظهر في واجهة الويب.

ملاحظة: عند إعادة توجيه طلب مصادقة بواسطة وكيل إلى ACS، يتم تطبيق أي طلبات NARs لنظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) على عنوان IP الخاص بخادم AAA لإعادة التوجيه، وليس على عنوان IP الخاص بعميل AAA الأصلي.

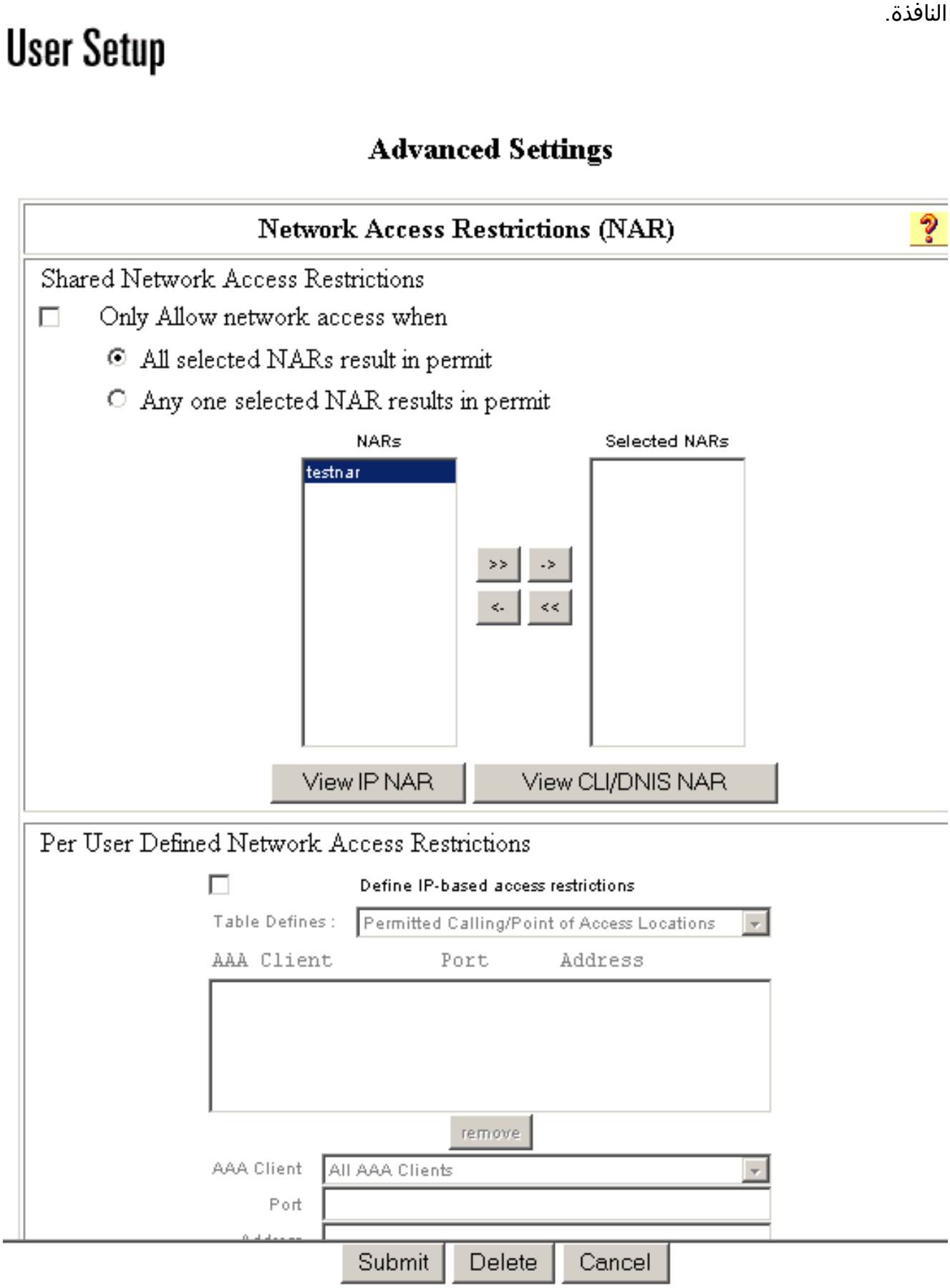
عندما تقوم بإنشاء قيود وصول على أساس كل مستخدم، فإن ACS لا يفرض حدودا على عدد قيود الوصول ولا يفرض حدا على طول كل قيد وصول. ولكن هناك حدود صارمة:

- لا يمكن أن يتجاوز طول مجموعة الحقول لكل عنصر بند 1024 حرفا.
- لا يمكن أن يحتوي NAR المشترك على أكثر من 16 كيلوبايت من الأحرف. يعتمد عدد عناصر البنود المدعومة على طول كل عنصر بند. على سبيل المثال، إذا قمت بإنشاء خط اتصال يستند إلى واجهة سطر الأوامر (CLI)/DNIS حيث تكون أسماء عملاء AAA هي 10 حروف، وتكون أرقام المنافذ هي 5 حروف، وتكون إدخالات واجهة سطر الأوامر (CLI) 15 حرفا، وتكون إدخالات DNIS هي 20 حرفا، فيمكنك إضافة 450 عنصرا من عناصر السطر قبل أن تصل إلى حد 16 كيلوبايت.

أتمت هذا steps in order to ثبتت NARs لمستخدم:

1. قم بتنفيذ الخطوات من 1 إلى 3 من إضافة حساب مستخدم أساسي.يظهر إطار تحرير إعداد المستخدم. يظهر اسم المستخدم الذي تضيفه أو تحرره في أعلى

النافذة.



2. لتطبيق NAR مشترك تم تكوينه مسبقا لهذا المستخدم:**ملاحظة:** لتطبيق NAR مشترك، يجب أن تكون قد انتهيت من تكوينه تحت قيود الوصول إلى الشبكة في قسم مكونات ملف التعريف المشترك. راجع قسم إضافة NAR مشترك للحصول على مزيد من المعلومات.حدد خانة الاختيار **السماح فقط بوصول الشبكة**.لتحديد ما إذا كان يجب تطبيق واحد أو كل قوائم التحكم بالوصول المشتركة على المستخدم للسماح له بالوصول، حدد واحد، حسب ما يكون منطبقا:ينتج عن كافة أرقام الأسعار غير القابلة للتحويل (NARS) المحددة تصريح.وينتج عن أي

وحدة منتقاة للنار تصريح بذلك.حدد اسم NAR مشترك في قائمة NARs، ثم انقر —> (زر السهم الأيمن) لنقل الاسم إلى قائمة NARs المحددة.**تلميح:** لعرض تفاصيل الخادم الخاصة بشبكات NARs المشتركة التي حددتها لتطبيقها، يمكنك النقر فوق **عرض IP NAR** أو **عرض CLID/DNIS NAR**، حسب الاقتضاء.

3. in order to عينت وطبقت NAR، ل هذا مستعمل خاص، أن يسمح أو ينكر هذا مستعمل منفذ استنادا إلى عنوان، أو عنوان IP ومنفذ:**ملاحظة:** يجب تحديد معظم قوائم التحكم في الوصول للإنترنت من خلال قسم المكونات المشتركة حتى يمكنك تطبيقها على أكثر من مجموعة أو مستخدم واحد. راجع قسم إضافة NAR مشترك للحصول على مزيد من المعلومات.في الجدول "قيود الوصول إلى الشبكة"، وتحت "قيود الوصول إلى الشبكة المحددة لكل مستخدم"، حدد خانة الاختيار **تعريف تقييدات الوصول المستندة إلى IP**.لتحديد ما إذا كانت القائمة التالية تحدد عناوين IP المسموح بها أو المرفوضة، من قائمة تعريف الجدول، أختر واحد:**مواقع الاتصال/ نقطة الوصول المسموح بهامواقع الاتصال/نقطة الوصول المرفوضة**حدد أو أدخل المعلومات في هذه المربعات:**عميل AAA**—حدد **جميع عملاء AAA**، أو اسم مجموعة أجهزة الشبكة (NDG)، أو اسم عميل AAA الفردي، الذي يجب السماح بالوصول إليه أو رفضه.**المنفذ**—أدخل عدد المنفذ الذي تريد السماح بالوصول إليه أو رفضه. يمكنك إستخدام العلامة النجمية (*) كحرف بدل للسماح بالوصول إلى جميع المنافذ على عميل AAA المحدد أو رفضه.**العنوان**—أدخل عنوان IP أو العناوين التي سيتم إستخدامها عند تنفيذ تقييدات الوصول. يمكنك إستخدام العلامة النجمية (*) كحرف بدل.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات عنوان IP للمنفذ و Src 1024. على الرغم من أن ACS يقبل أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR ولا يمكن ل ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**.تظهر معلومات عميل AAA والمنفذ والعنوان المحددة في الجدول الموجود أعلى قائمة عملاء AAA.
4. للسماح بوصول المستخدم هذا أو رفضه استنادا إلى موقع الاستدعاء أو القيم بخلاف عنوان IP المنشأ:حدد خانة الاختيار **تعريف تقييدات الوصول المستندة إلى CLI/DNIS**.لتحديد ما إذا كانت القائمة التالية تحدد القيم المسموح بها أو المرفوضة، من قائمة تعريف الجدول، أختر واحد:**مواقع الاتصال/ نقطة الوصول المسموح بهامواقع الاتصال/نقطة الوصول المرفوضة**أكمل المربعات كما هو موضح:**ملاحظة:** يجب إدخال إدخال في كل مربع. يمكنك إستخدام العلامة النجمية (*) كحرف بدل لكل قيمة أو جزء منها. يجب أن يتطابق التنسيق الذي تستخدمه مع تنسيق السلسلة التي تتلقاها من عميل AAA الخاص بك. يمكنك تحديد هذا التنسيق من سجل محاسبة RADIUS الخاص بك.**عميل AAA**—حدد **جميع عملاء AAA**، أو اسم NDG، أو اسم عميل AAA الفردي، الذي يجب السماح بالوصول إليه أو رفضه.**المنفذ**—أدخل عدد المنفذ الذي تريد السماح بالوصول إليه أو رفضه. يمكنك إستخدام العلامة النجمية (*) كحرف بدل للسماح بالوصول إلى جميع المنافذ أو رفضه.**CLI**—أدخل رقم واجهة سطر الأوامر الذي يتم السماح بالوصول إليه أو رفضه. يمكنك إستخدام العلامة النجمية (*) كحرف بدل للسماح بالوصول أو رفضه بناء على جزء من الرقم.**تلميح:** أستخدم إدخال CLI إذا كنت تريد تقييد الوصول بناء على قيم أخرى مثل عنوان MAC لعميل Cisco Aironet. راجع قسم حول قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.**DNIS**—أدخل رقم DNIS الذي تسمح بالوصول أو رفضه. أستخدم هذا الإدخال لتقييد الوصول بناء على الرقم الذي سيطلبه المستخدم. يمكنك إستخدام العلامة النجمية (*) كحرف بدل للسماح بالوصول أو رفضه بناء على جزء من الرقم.**تلميح:** أستخدم تحديد DNIS إذا كنت تريد تقييد الوصول بناء على قيم أخرى مثل عنوان MAC لنقطة الوصول Cisco Aironet AP. راجع قسم حول قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.**ملاحظة:** يجب ألا يتجاوز العدد الإجمالي للأحرف في قائمة عملاء AAA ومربعات **المنفذ** و**CLI** و**DNIS** 1024. على الرغم من أن ACS يقبل أكثر من 1024 حرف عند إضافة NAR، إلا أنه لا يمكنك تحرير NAR ولا يمكن ل ACS تطبيقه على المستخدمين بدقة.طقطقة **يدخل**.تظهر المعلومات التي تحدد عميل AAA والمنفذ و CLI و DNIS في الجدول أعلى قائمة عملاء AAA.
5. إذا انتهيت من تكوين خيارات حساب المستخدم، انقر فوق **إرسال** لتسجيل الخيارات.

تعيين قيود الوصول إلى الشبكة لمجموعة مستخدمين

يمكنك إستخدام الجدول "تقييدات الوصول إلى الشبكة" في "إعداد المجموعة" لتطبيق قوائم التحكم في الوصول إلى الشبكة بثلاث طرق مختلفة:

- تطبيق قوائم التحكم في الوصول للإنترنت المشتركة الموجودة بالاسم.
- قم بتحديد قيود الوصول للمجموعة المستندة إلى IP للسماح بالوصول إلى عميل AAA محدد أو المنافذ المحددة

على عميل AAA أو رفضها عند إنشاء اتصال IP.

- قم بتعريف قوائم التحكم في الوصول (NARs) الخاصة بالمجموعة المستندة إلى واجهة سطر الأوامر (CLI)/DNIS) للسماح بالوصول إلى رقم واجهة سطر الأوامر (CLI) أو رقم DNIS المستخدم أو رفضه.**ملاحظة:** يمكنك أيضا إستخدام منطقة قيود الوصول المستندة إلى CLI/DNIS لتحديد قيم أخرى. راجع قسم حول قيود الوصول إلى الشبكة للحصول على مزيد من المعلومات.

في العادة، تقوم بتعريف قوائم التحكم في الوصول (المشتركة) من خلال قسم المكونات المشتركة بحيث يمكن تطبيق هذه القيود على أكثر من مجموعة واحدة أو مستخدم واحد. راجع قسم إضافة NAR مشترك للحصول على مزيد من المعلومات. يجب عليك التحقق من خانة الاختيار **تقييد الوصول إلى الشبكة المشتركة على مستوى المجموعة** في صفحة **الخيارات المتقدمة** في قسم تكوين الواجهة حتى تظهر هذه الخيارات في واجهة ويب ل ACS.

مهما، أنت يستطيع أيضا استعملت ACS أن يعين وطبق NAR لمجموعة منفردة من ضمن قسم **إعداد المجموعة**. يجب عليك التحقق من إعداد **تقييد الوصول إلى الشبكة على مستوى المجموعة** ضمن صفحة الخيارات المتقدمة في قسم تكوين الواجهة لخيارات التصفية المستندة إلى IP الخاصة بالمجموعة الفردية وخيارات التصفية المستندة إلى CLI/DNIS الخاصة بالمجموعة المفردة لكي تظهر في واجهة ويب ACS.

ملاحظة: عند إعادة توجيه طلب مصادقة بواسطة وكيل إلى خادم ACS، يتم تطبيق أي من قوائم التحكم في الوصول لطلبات RADIUS على عنوان IP الخاص بخادم AAA لإعادة التوجيه، وليس على عنوان IP الخاص بعميل AAA الأصلي.

أتمت هذا steps in order to ثبتت NARs لمجموعة مستعمل:

1. في شريط التنقل، انقر فوق **إعداد المجموعة**.يظهر إطار تحديد إعداد المجموعة.
2. من قائمة المجموعة، حدد مجموعة، ثم انقر **تحرير الإعدادات**.يظهر اسم المجموعة في أعلى نافذة إعدادات المجموعة.

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).