

ةقداصملا ليك وذي فنت

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[كيفية تنفيذ وكيل المصادقة](#)

[ملفات تعريف الخادم](#)

[\(+Cisco Secure UNIX \(TACACS](#)

[\(+Cisco Secure Windows \(TACACS](#)

[ما يراه المستخدم](#)

[معلومات ذات صلة](#)

المقدمة

يتم استخدام وكيل المصادقة (وكيل المصادقة)، المتوفر في الإصدار T.12.0.5 من برنامج Cisco IOS® Software Firewall والإصدارات الأحدث، لمصادقة المستخدمين الواردين أو الصادرين، أو لكليهما. وعادة ما يتم حظر هؤلاء المستخدمين بواسطة قائمة وصول. ومع ذلك، باستخدام وكيل المصادقة، يحضر المستخدمون متصفح للانتقال من خلال جدار الحماية والمصادقة على خادم TACACS+ أو RADIUS. يقوم الخادم بتمرير إدخلات إضافية لقائمة الوصول إلى الموجه للسماح للمستخدمين بالمرور بعد المصادقة.

يعطي هذا وثيقة المستخدم نصائح عامة لتنفيذ وكيل المصادقة، ويزود بعض ملفات تعريف خادم Cisco الأمن لوكيل المصادقة، ويصف ما يراه المستخدم عندما يكون وكيل المصادقة قيد الاستخدام.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

كيفية تنفيذ وكيل المصادقة

أكمل الخطوات التالية:

1. تأكد من تدفق حركة المرور بشكل صحيح من خلال جدار الحماية قبل تكوين وكيل المصادقة.
2. لتقليل انقطاع الشبكة أثناء الاختبار، قم بتعديل قائمة الوصول الحالية لرفض الوصول إلى عميل اختبار واحد.
3. تأكد من أن عميل الاختبار الواحد لا يمكنه الوصول من خلال جدار الحماية ومن أنه يمكن للمضيفين الآخرين الوصول إليه.
4. قم بتشغيل تصحيح الأخطاء باستخدام `exec-timeout 0` ضمن منفذ وحدة التحكم أو الوحدات الطرفية للنوع الظاهري (VTYs)، أثناء إضافة أوامر وكيل المصادقة والاختبار.

ملفات تعريف الخادم

تم إجراء الاختبار باستخدام Cisco Secure UNIX و Windows. إذا كان RADIUS قيد الاستخدام، فيجب أن يدعم خادم RADIUS السمات الخاصة بالموارد (السمة 26). وفيما يلي أمثلة محددة على الخوادم:

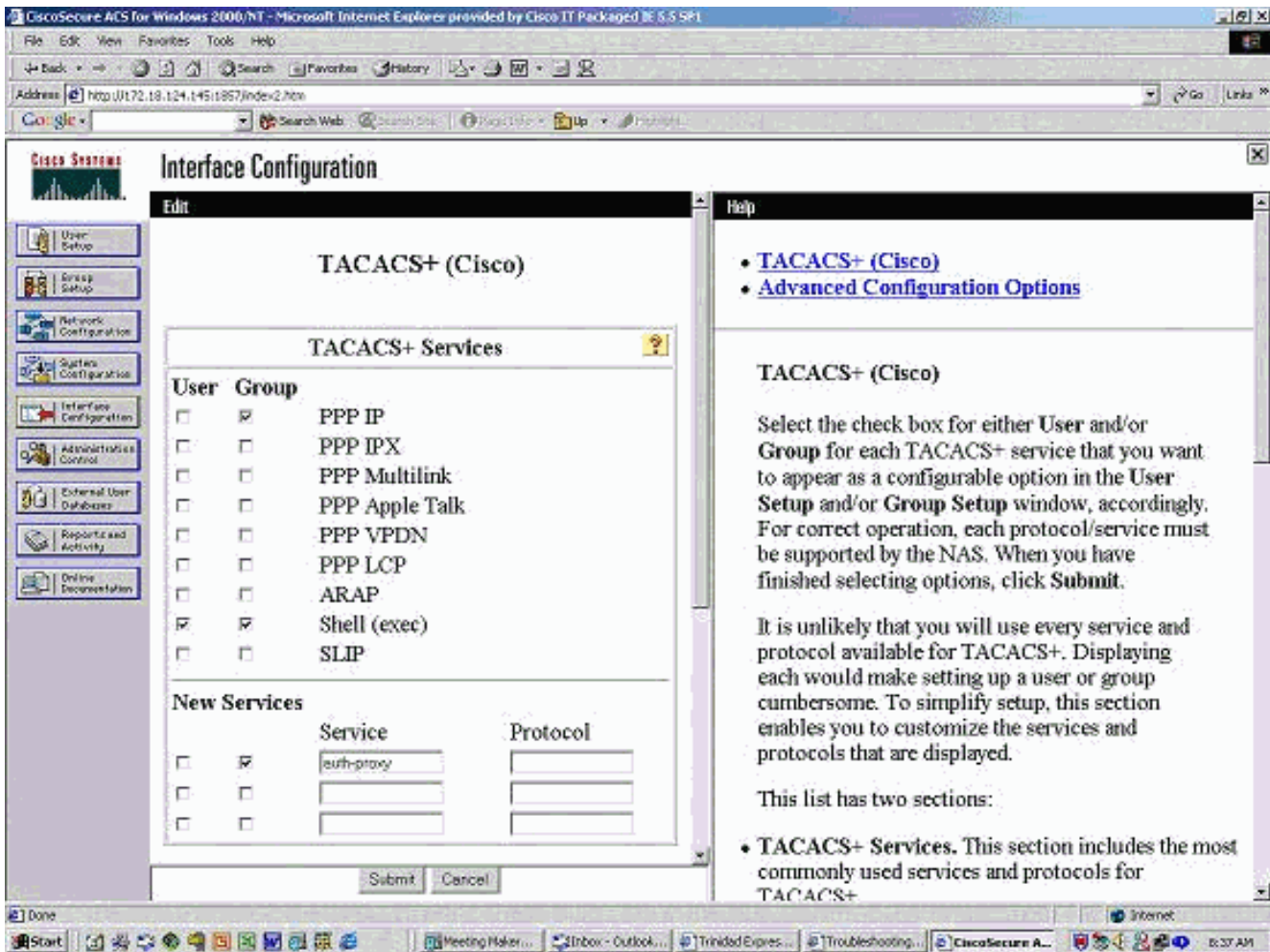
(+Cisco Secure UNIX (TACACS

```
ViewProfile -p 9900 -u proxyonly/. #
User Profile Information
}user = proxyonly
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
***** password = clear
} service=auth-proxy
set priv-lvl=15
"set proxyacl#1="permit icmp any any
"set proxyacl#2="permit tcp any any
"set proxyacl#3="permit udp any any
{
{
```

(+Cisco Secure Windows (TACACS

اتبع هذا الإجراء.

1. أدخل اسم المستخدم وكلمة المرور (قاعدة بيانات Cisco Secure أو Windows).
2. لتكوين الواجهة، حدد `+TACACS`.
3. تحت خدمات جديدة، حدد خيار المجموعة واكتب وكيل المصادقة في عمود الخدمة. ترك عمود البروتوكول فارغاً.



4. خيارات متقدمة - عرض نافذة لكل خدمة - سمات مخصصة.

5. في إعدادات المجموعة، تحقق من وكيل المصادقة وأدخل هذه المعلومات في النافذة:

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

(Cisco Secure UNIX (RADIUS

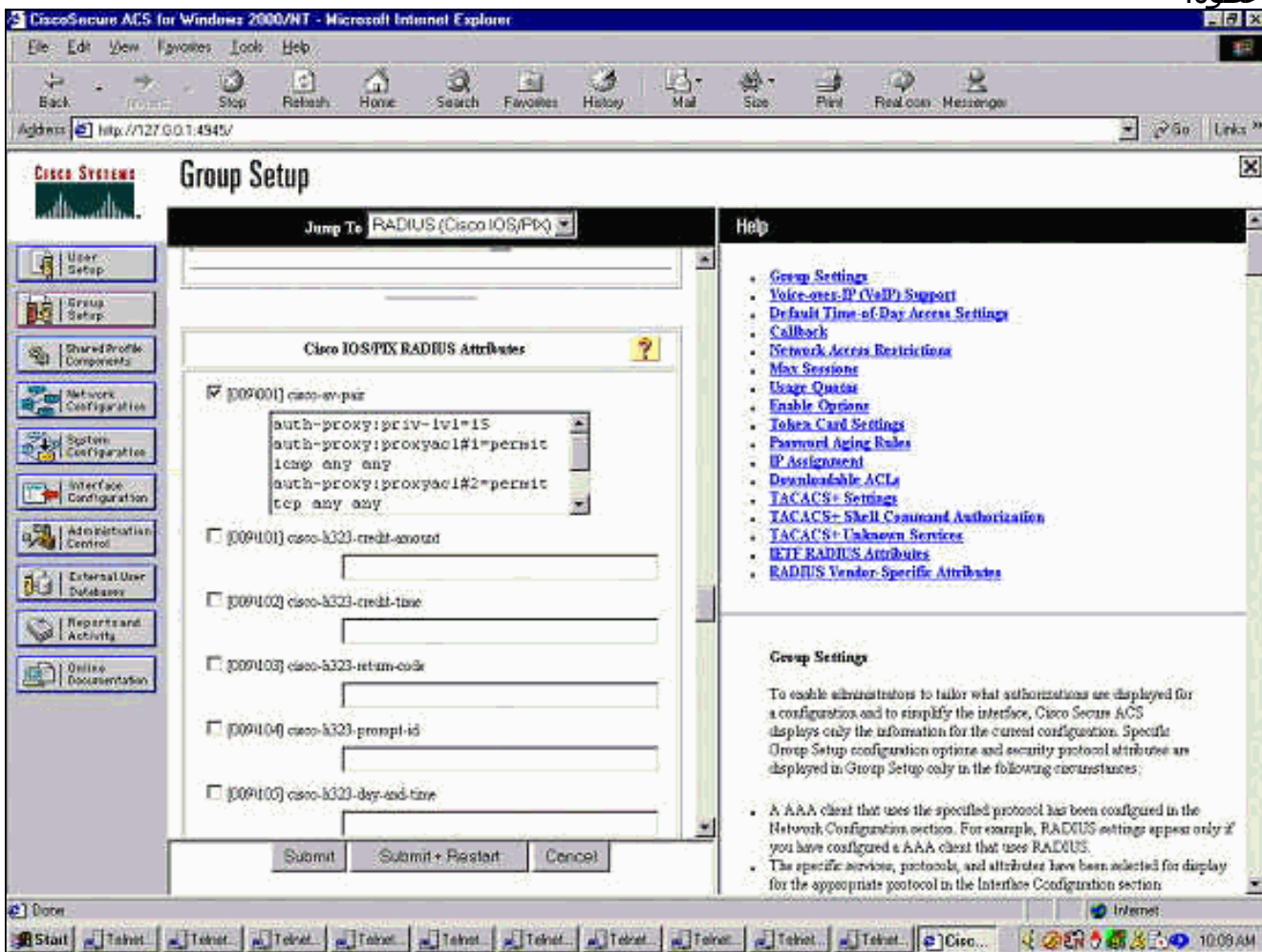
```
ViewProfile -p 9900 -u proxy/. #
User Profile Information
}user = proxy
profile_id = 58
profile_cycle = 1
} radius=Cisco
} =check_items
"proxy "=2
{
} =reply_attributes
"auth-proxy:priv-lvl=15 "=9,1
"auth-proxy:proxyacl#1=permit icmp any any "=9,1
"auth-proxy:proxyacl#2=permit tcp any any "=9,1
"auth-proxy:proxyacl#3=permit udp any any "=9,1
{
{
{
```

اتبع هذا الإجراء.

1. تكوين الشبكة المفتوحة. يجب أن يكون NAS هو Cisco RADIUS.
2. إن قارن تشكيل يتوفر RADIUS، فحصد VSA صندوق.
3. في إعدادات المستخدم، أدخل اسم المستخدم/كلمة المرور.
4. في إعدادات المجموعة، حدد الخيار ل [001/009] cisco-av-pair. في مربع النص أسفل التحديد، اكتب ما يلي:

```
auth-proxy:priv-1v1=15
auth-proxy:proxyacl#1=permit icmp any any
auth-proxy:proxyacl#2=permit tcp any any
auth-proxy:proxyacl#3=permit udp any any
```

هذا نافذة مثال من هذا خطوة.



ما يراه المستخدم

يحاول المستخدم إستعراض شيء ما على الجانب الآخر من جدار الحماية.

تظهر نافذة مع هذه الرسالة:

```
Cisco <hostname> Firewall
Authentication Proxy
```

:Username

:Password

إذا كان اسم المستخدم وكلمة المرور جيدين، فسيري المستخدم:

Cisco Systems

!Authentication Successful

إذا فشلت المصادقة، فإن الرسالة هي:

Cisco Systems

!Authentication Failed

معلومات ذات صلة

- [صفحة دعم جدار حماية IOS](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنل دن تسمل