

# عم ASA لى جع Thin-Client SSL VPN (WebVPN) ASDM نيوكت لاثم

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [تكوين SSL ل VPN قليل السمك باستخدام ASDM](#)
- [الخطوة 1. تمكين WebVPN على ASA](#)
- [الخطوة 2. تكوين خصائص إعادة توجيه المنفذ](#)
- [الخطوة 3. إنشاء نهج مجموعة وربطه بقائمة إعادة توجيه المنافذ](#)
- [الخطوة 4. إنشاء مجموعة نفق وربطها بنهج المجموعة](#)
- [الخطوة 5. إنشاء مستخدم وإضافة هذا المستخدم إلى نهج المجموعة](#)
- [تكوين SSL ل VPN قليل السمك باستخدام CLI](#)
- [التحقق من الصحة](#)
- [الإجراء](#)
- [الأوامر](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [هل اكتملت عملية مصادقة SSL؟](#)
- [هل يعمل Thin-Client SSL VPN؟](#)
- [الأوامر](#)
- [معلومات ذات صلة](#)

## المقدمة

تسمح تقنية SSL VPN للعميل قليل السمك بالوصول الآمن لبعض التطبيقات التي تحتوي على منافذ ثابتة، مثل Telnet(23 و SSH(22 و POP3(110 و IMAP4(143 و SMTP(25). يمكنك استخدام شبكة VPN الخاصة ب Thin-Client SSL تطبيق يقوده المستخدم أو تطبيق قائم على السياسات أو كليهما. وهذا يعني أنه يمكنك تكوين الوصول على مستخدم حسب المستخدم أو يمكنك إنشاء نهج مجموعة حيث تقوم بإضافة مستخدم واحد أو أكثر.

- **SSL VPN (WebVPN) بدون عملاء**—يوفر عميل بعيد يتطلب مستعرض ويب يدعم SSL للوصول إلى خوادم الويب HTTP أو HTTPS على شبكة منطقة محلية (LAN) للشركات. بالإضافة إلى ذلك، توفر الشبكة الخاصة الظاهرية (VPN) الخاصة بروتوكول نظام ملفات الإنترنت العام (CIFS) وصولاً إلى إستعراض ملفات Windows. يعد Outlook Web Access (OWA) مثالا للوصول إلى HTTP. ارجع إلى [SSL VPN \(WebVPN\)](#)
- **Thin-Client SSL VPN (إعادة توجيه المنفذ)**—يوفر عميلا عن بعد يقوم بتنزيل تطبيق صغير قائم على Java

ويسمح بالوصول الآمن لتطبيقات بروتوكول التحكم في الإرسال (TCP) التي تستخدم أرقام منافذ ثابتة. يعد بروتوكول مكتب البريد (POP3) وبروتوكول نقل البريد البسيط (SMTP) وبروتوكول الوصول إلى رسائل الإنترنت (IMAP) وبروتوكول طبقة الأمان (SSH) وبروتوكول Telnet أمثلة للوصول الآمن. نظرا لتغيير الملفات الموجودة على الجهاز المحلي، يجب أن يكون لدى المستخدمين امتيازات إدارية محلية لاستخدام هذه الطريقة. لا تعمل هذه الطريقة لـ SSL VPN مع التطبيقات التي تستخدم تعيينات المنافذ الديناميكية، مثل بعض تطبيقات بروتوكول نقل الملفات (FTP). ملاحظة: بروتوكول مخطط بيانات المستخدم (UDP) غير مدعوم.

• **عمل SSL VPN (وضع النفق)**- يقوم بتنزيل عميل صغير إلى محطة العمل البعيدة ويسمح بالوصول الآمن الكامل إلى الموارد على شبكة شركة داخلية. يمكنك تنزيل (SVC) SSL VPN Client (SVC) بشكل دائم إلى محطة عمل بعيدة، أو يمكنك إزالة العميل بمجرد إغلاق جلسة العمل الآمنة. ارجع إلى [SSL VPN Client \(SVC\)](#) على [ASA مع مثال تكوين ASDM](#) لمعرفة المزيد حول عمل SSL VPN.

يوضح هذا المستند تكوين بسيطاً لشبكة VPN الخاصة بـ SSL Thin-Client على جهاز الأمان القابل للتكيف (ASA). يسمح التكوين للمستخدم بوضع برنامج Telnet بشكل آمن على موجه موجود داخل ASA. يتم دعم التكوين في هذا المستند لـ ASA الإصدار x.7 والإصدارات الأحدث.

## [المتطلبات الأساسية](#)

### [المتطلبات](#)

قبل أن تحاول إجراء هذا التكوين، تأكد من استيفاء متطلبات محطات العملاء البعيدة التالية:

- مستعرض ويب تم تمكين SSL عليه
  - Sun Java JRE الإصدار 1.4 أو إصدار أحدث
  - تم تمكين ملفات تعريف الارتباط
  - تم تعطيل المحصرات المنبثقة
  - الامتيازات الإدارية المحلية (غير مطلوبة ولكن مقترحة بشدة)
- ملاحظة: يتوفر أحدث إصدار من Sun Java JRE كتحميل مجاني من [موقع Java على الويب](#).

### [المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

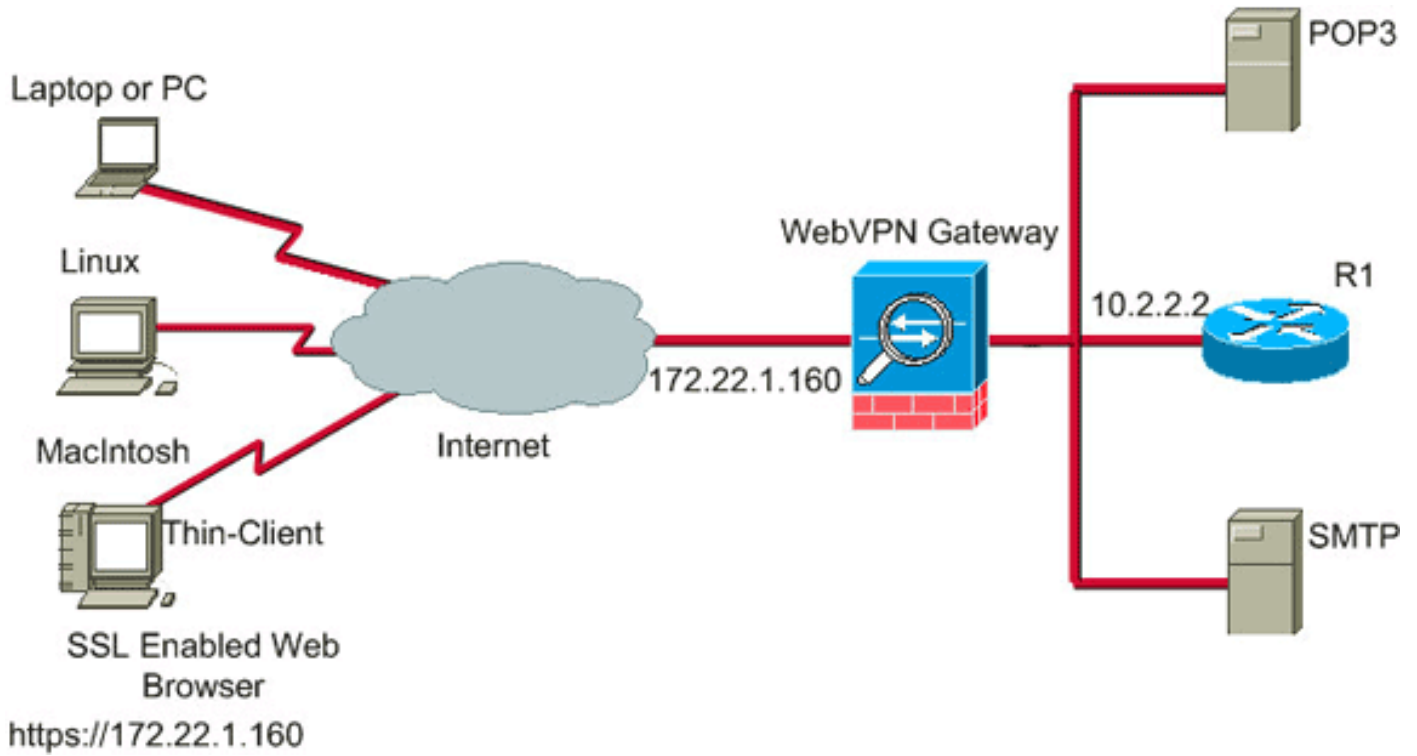
- جهاز الأمان القابل للتكيف طراز 5510 من Cisco
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1) [ملاحظة](#): ارجع إلى [السماح بوصول HTTPS إلى ASDM](#)
- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance، الإصدار (1)7.2
- العميل البعيد 2 (SP) (Microsoft Windows XP Professional)

تم تطوير المعلومات الواردة في هذا المستند في بيئة معملية. تمت إعادة تعيين جميع الأجهزة المستخدمة في هذا المستند إلى التكوين الافتراضي الخاص بها. إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر. تم تحديد جميع عناوين IP المستخدمة في هذا التكوين من عناوين RFC 1918 في بيئة معملية؛ وعناوين IP هذه ليست قابلة للتوجيه على الإنترنت وهي لأغراض الاختبار فقط.

### [الرسم التخطيطي للشبكة](#)

يستخدم هذا المستند تكوين الشبكة الموضح في هذا القسم.

عندما يقوم عميل بعيد ببدء جلسة عمل باستخدام ASA، يقوم العميل بتنزيل برنامج Java صغير إلى محطة العمل. يتم تقديم قائمة بالموارد التي تم تكوينها مسبقاً للعميل.



## الاصطلاحات

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

## معلومات أساسية

لبدء جلسة، يفتح العميل البعيد مستعرض SSL إلى الواجهة الخارجية ل ASA. بعد إنشاء الجلسة، يمكن للمستخدم استخدام المعلومات التي تم تكوينها على ASA لاستدعاء أي وصول إلى Telnet أو التطبيق. يمثل ASA الاتصال الآمن ويسمح للمستخدم بالوصول إلى الجهاز.

**ملاحظة:** قوائم الوصول الواردة غير ضرورية لهذه الاتصالات لأن هيئة المعايير الإعلانية على علم بما يشكل جلسة قانونية.

## تكوين VPN ل SSL قليل السمك باستخدام ASDM

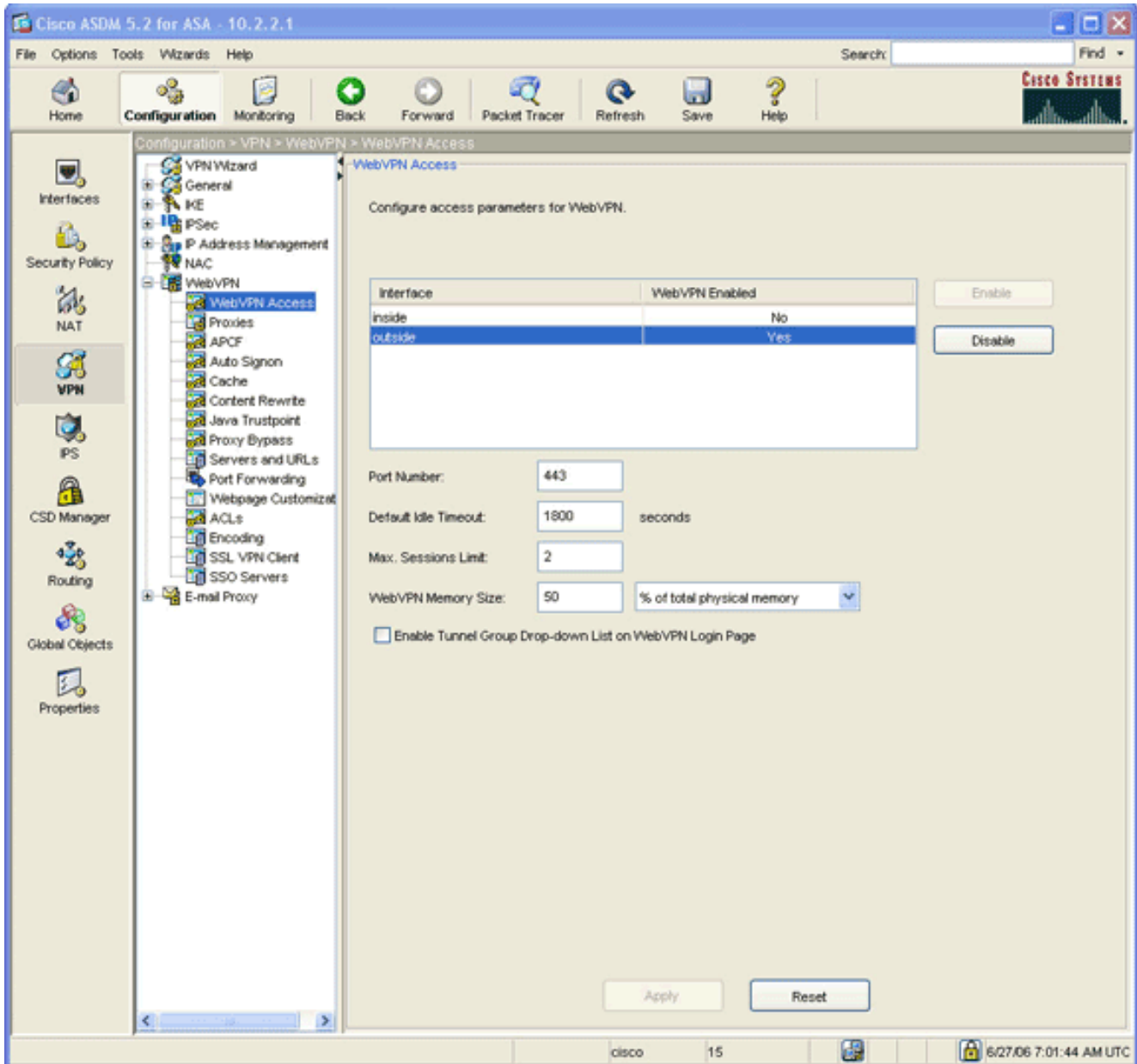
أتمت in order to شكلت Thin-Client SSL VPN على ال ASA، هذا steps:

1. [تمكين WebVPN على ASA](#)
2. [تكوين خصائص إعادة توجيه المنفذ](#)
3. [إنشاء سياسة مجموعة وربطها بقائمة إعادة توجيه المنافذ](#) (التي تم إنشاؤها في الخطوة 2)
4. [إنشاء مجموعة نفق وربطها بنهج المجموعة](#) (الذي تم إنشاؤه في الخطوة 3)
5. [إنشاء مستخدم وإضافة هذا المستخدم إلى نهج المجموعة](#) (تم إنشاؤه في الخطوة 3)

### الخطوة 1. تمكين WebVPN على ASA

أتمت in order to مكنت WebVPN على ال ASA، هذا steps:

1. ضمن تطبيق ASDM، انقر فوق تكوين، ثم انقر فوق VPN.
2. قم بتوسيع WebVPN، واختر وصول



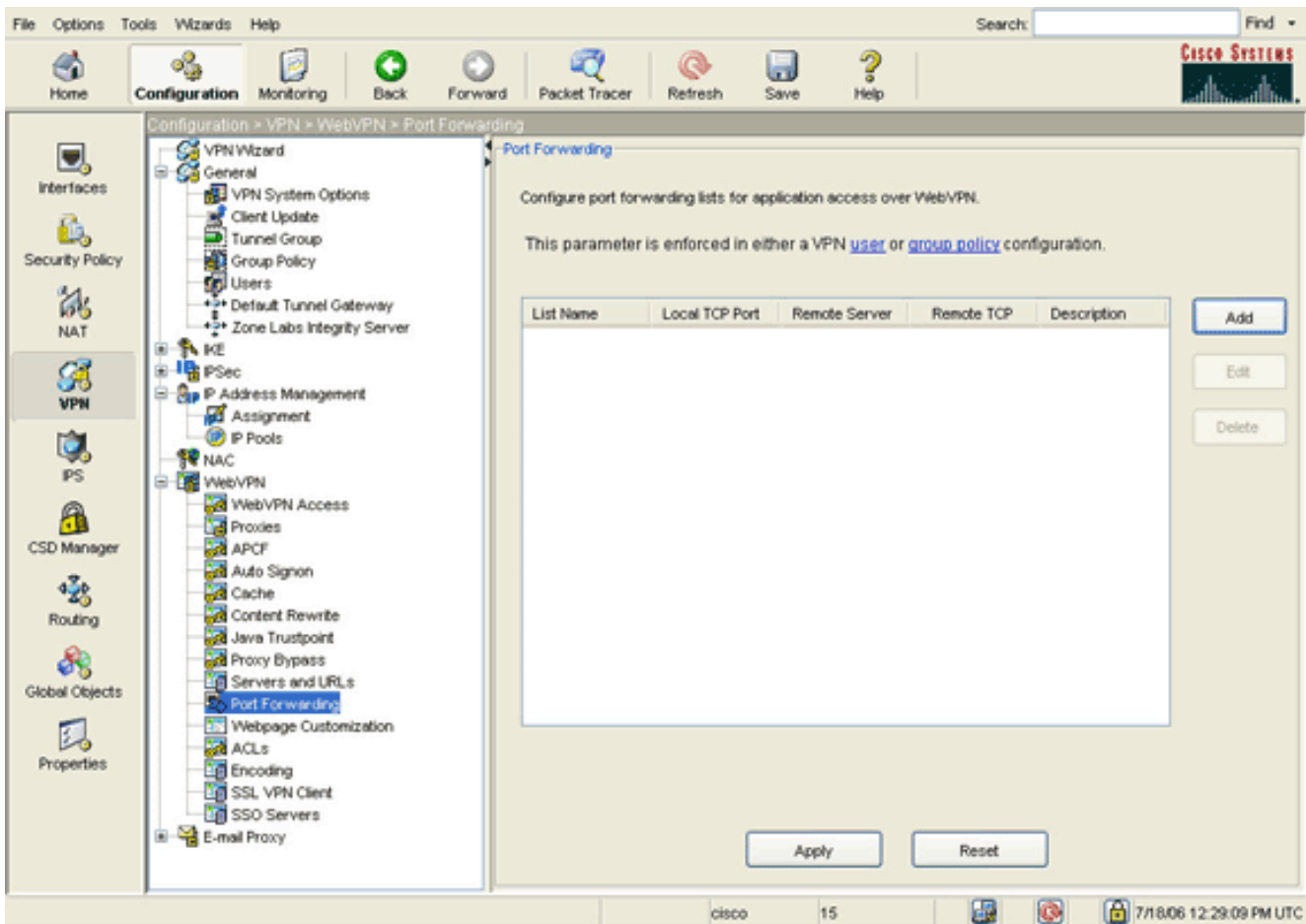
3. ركزت القارن، وطققة يمكن.

4. انقر فوق تطبيق، ثم انقر فوق حفظ، ثم انقر فوق نعم لقبول التغييرات.

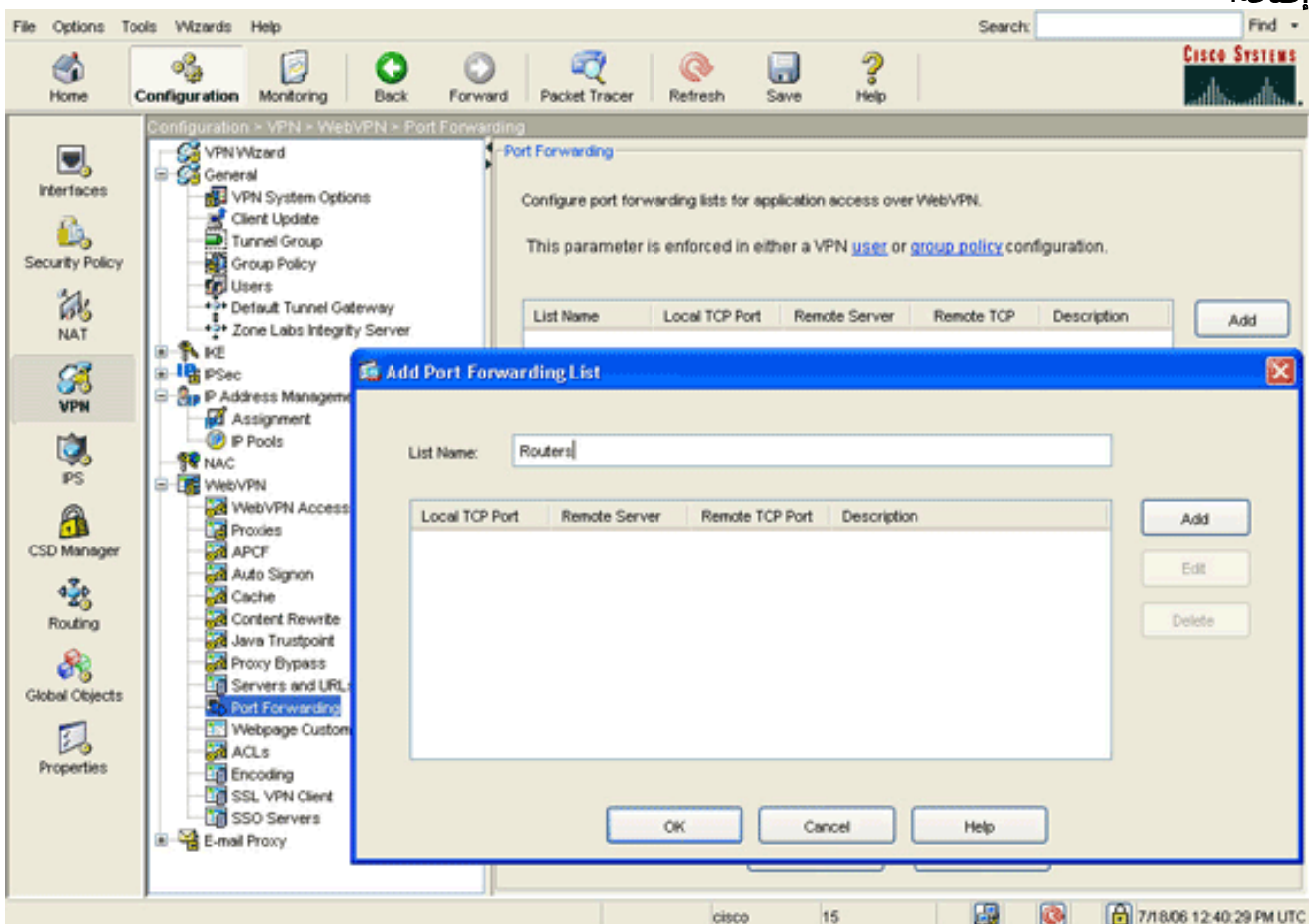
## الخطوة 2. تكوين خصائص إعادة توجيه المنفذ

أتمت in order to شكلت ميناء forwarding صفة، هذا steps:

1. قم بتوسيع WebVPN، واختر إعادة توجيه المنفذ.



2. انقر فوق الزر إضافة.



3. في شاشة قائمة إعادة توجيه المنافذ الإضافية، أدخل اسم قائمة، ثم انقر فوق إضافة. يظهر مربع الحوار إضافة إدخال إعادة توجيه

The screenshot shows a dialog box titled "Add Port Forwarding Entry". It has a close button (X) in the top right corner. The dialog contains the following fields and values:

- Local TCP Port: 3044
- Remote Server: 10.2.2.2
- Remote TCP Port: 23
- Description: Telnet to R1

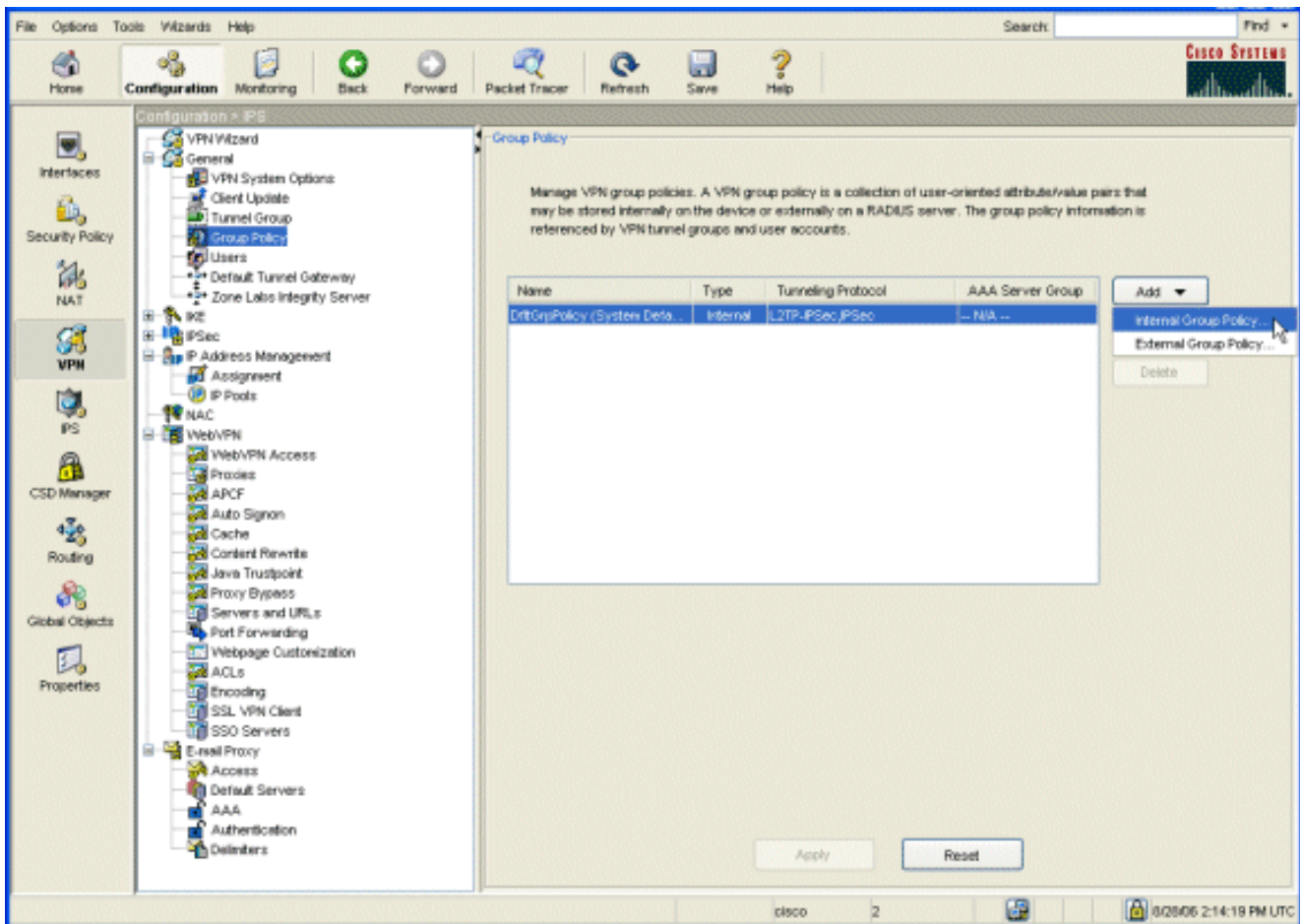
At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a mouse cursor.

4. في شاشة إضافة إدخال إعادة توجيه المنفذ، أدخل الخيارات التالية: في حقل منفذ TCP المحلي، أدخل رقم منفذ أو قبل القيمة الافتراضية. يمكن أن تكون القيمة التي أدخلتها أي رقم من 1024 إلى 65535. في حقل "الخدم البعيد"، أدخل عنوان IP. يستخدم هذا المثال عنوان الوجه. دخلت في البعيد TCP ميناء مجال، رقم أيسر. يستعمل هذا مثال ميناء 23. دخلت في الوصف مجال، وصف، وطققة ok.
5. انقر فوق موافق، ثم انقر فوق تطبيق.
6. انقر فوق حفظ، ثم انقر فوق نعم لقبول التغييرات.

### الخطوة 3. إنشاء نهج مجموعة وربطه بقائمة إعادة توجيه المنافذ

لإنشاء سياسة مجموعة وربطها بقائمة إعادة توجيه المنافذ، أكمل الخطوات التالية:

1. قم بتوسيع عام، واختر نهج المجموعة.



2. انقر فوق إضافة، واختر نهج المجموعة الداخلي. يظهر مربع الحوار إضافة نهج مجموعة داخلي.

**Add Internal Group Policy**

Name:

General | IPSec | Client Configuration | Client Firewall | Hardware Client | NAC | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols:  Inherit  IPSec  WebVPN  L2TP over IPSec

Filter:  Inherit  Manage...

**Connection Settings**

Access Hours:  Inherit  Manage...

Simultaneous Logins:  Inherit

Maximum Connect Time:  Inherit  Unlimited  minutes

Idle Timeout:  Inherit  Unlimited  minutes

**Servers**

DNS Servers:  Inherit Primary:  Secondary:

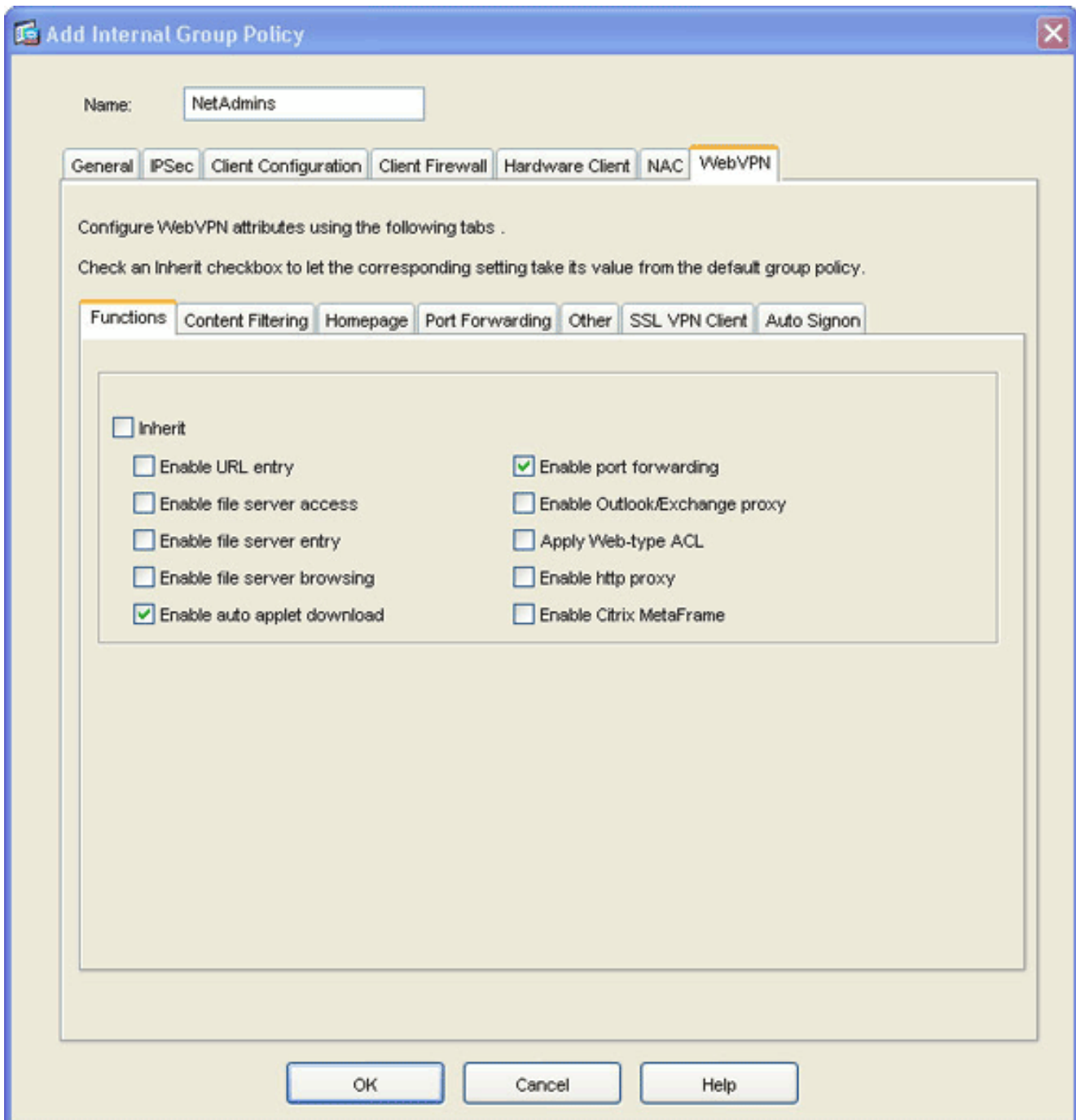
WINS Servers:  Inherit Primary:  Secondary:

DHCP Scope:  Inherit

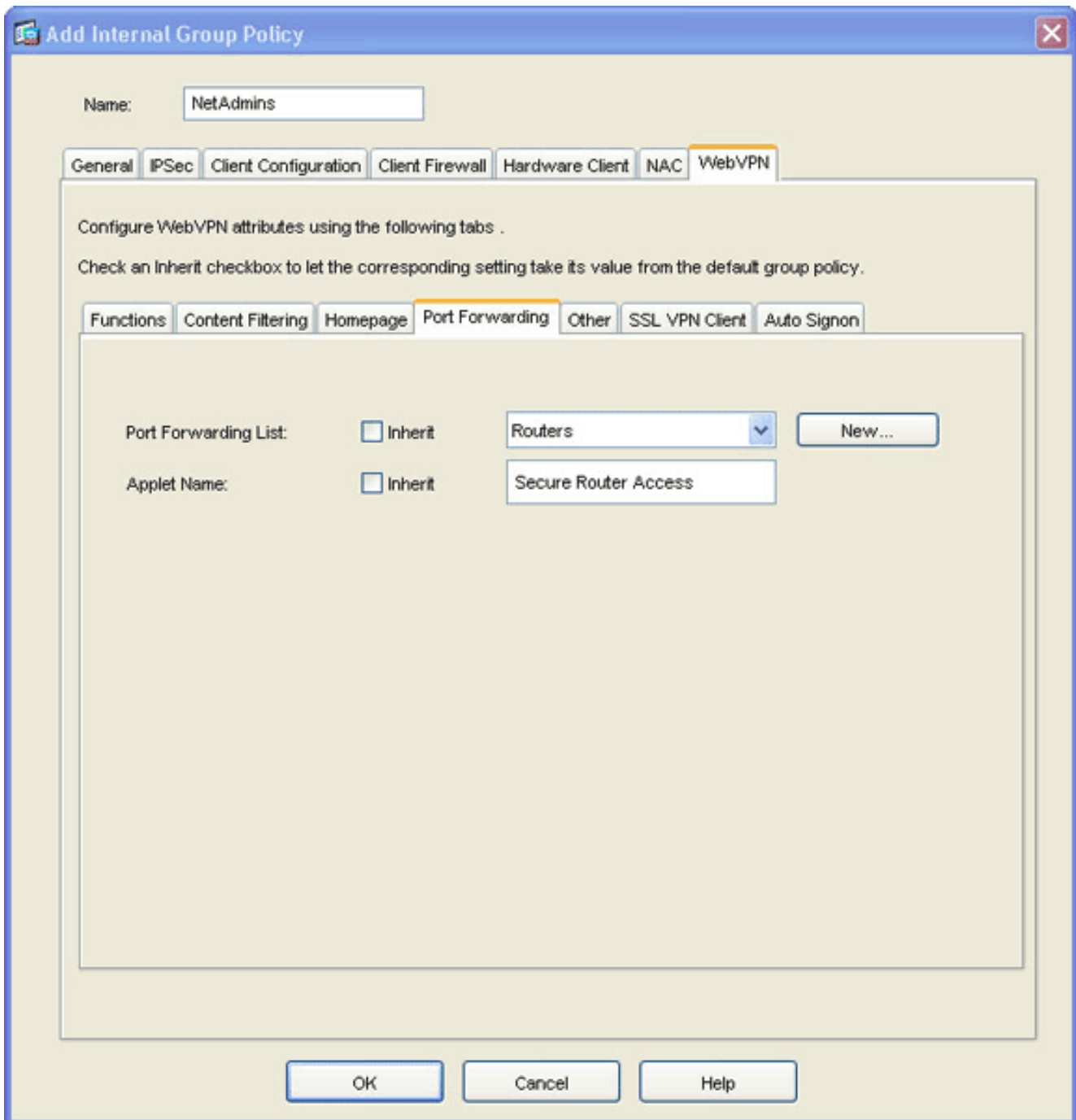
OK Cancel Help

3. أدخل اسما أو وافق على اسم المجموعة الافتراضي.
4. قم بإلغاء تحديد خانة الاختيار **Inherit** Tunneling Protocols، وحدد خانة الاختيار **WebVPN**.
5. انقر علامة التبويب **WebVPN** الموجودة في أعلى الشاشة، ثم انقر فوق علامة التبويب **وظائف**.
6. قم بإلغاء تحديد خانة الاختيار **وراثه**، وحدد خانة الاختيار **تمكين تنزيل التطبيق التلقائي وتمكين إعادة توجيه المنافذ** كما هو موضح في هذه الصورة:





7. أيضا ضمن علامة التبويب WebVPN، انقر فوق علامة التبويب إعادة توجيه المنفذ، وقم بإلغاء تحديد خانة الاختيار توريث لقائمة إعادة توجيه المنافذ.



8. انقر فوق السهم المنسدل لقائمة إعادة توجيه المنافذ، واختر قائمة إعادة توجيه المنافذ التي قمت بإنشائها في [الخطوة 2](#).
9. قم بإلغاء تحديد خانة الاختيار توريث اسم التطبيق، و قم بتغيير الاسم في حقل النص. يعرض العميل اسم التطبيق عند الاتصال.
10. انقر فوق موافق، ثم انقر فوق تطبيق.
11. انقر فوق حفظ، ثم انقر فوق نعم لقبول التغييرات.

#### [الخطوة 4. إنشاء مجموعة نفق وربطها بنهج المجموعة](#)

يمكنك تحرير مجموعة النفق *DefaultWebVPNGroup* الافتراضية أو إنشاء مجموعة نفق جديدة.

لإنشاء مجموعة نفق جديدة، أكمل الخطوات التالية:

1. قم بتوسيع عامة، واختر مجموعة النفق.

File Options Tools Wizards Help Search: Find

Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help

Configuration > VPN > General > Tunnel Group

VPN Wizard  
 General  
 VPN System Options  
 Client Update  
**Tunnel Group**  
 Group Policy  
 Users  
 Default Tunnel Gateway  
 Zone Labs Integrity Server  
 IKE  
 PSec  
 IP Address Management  
 Assignment  
 IP Pools  
 NAC  
 WebVPN  
 WebVPN Access  
 Proxies  
 APCF  
 Auto Signon  
 Cache  
 Content Rewrite  
 Java Trustpoint  
 Proxy Bypass  
 Servers and URLs  
 Port Forwarding  
 Webpage Customization  
 ACLs  
 Encoding  
 SSL VPN Client  
 SSO Servers  
 E-mail Proxy

**Tunnel Group**

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPsec or WebVPN connection.

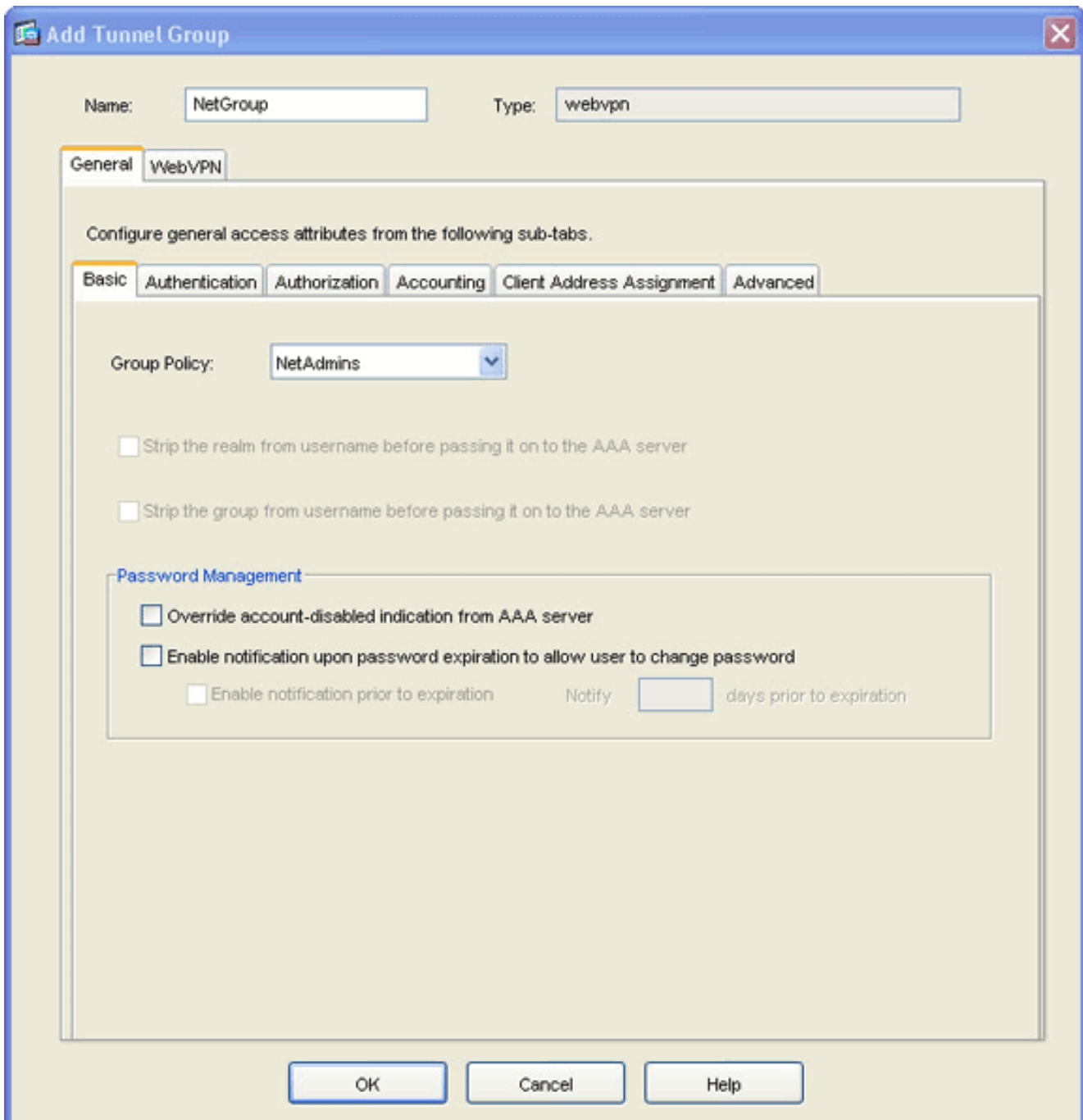
Name	Type	Group Policy
DefaultWEBVPNGroup	webvpn	DfltGrpPolicy
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Group Delimiter: -- None --

Apply Reset

Configuration changes saved successfully. cisco 15 7/18/06 1:26:59 PM UTC

2. انقر فوق إضافة، واختر وصول WebVPN. يظهر مربع الحوار إضافة مجموعة نفق.



3. أدخل اسما في حقل "الاسم".

4. انقر فوق السهم المنسدل لنهج المجموعة، واختر نهج المجموعة الذي أنشأته في [الخطوة 3](#).

5. انقر فوق موافق، ثم انقر فوق تطبيق.

6. انقر فوق حفظ، ثم انقر فوق نعم لقبول التغييرات. يتم الآن ربط مجموعة النفق ونهج المجموعة وخصائص إعادة توجيه المنفذ.

### [الخطوة 5. إنشاء مستخدم وإضافة هذا المستخدم إلى نهج المجموعة](#)

لإنشاء مستخدم وإضافة ذلك المستخدم إلى نهج المجموعة، أكمل الخطوات التالية:

1. قم بتوسيع عامة، واختر المستخدمين.

File Options Tools Wizards Help Search Find

Home Configuration Monitoring Back Forward Packet Tracer Refresh Save Help

Configuration > VPN > General > Users

Users

Create entries in the ASA local user database. Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

User Name	Privilege Level (Role)	VPN Group Policy	VPN Group Lock
enable_15	15	N/A	N/A
cisco	15	DfltGrpPolicy	-- Inherit Group Polic...
admin1	15	DfltGrpPolicy	-- Inherit Group Polic...
sales1	4	SalesGroupPolicy	-- Inherit Group Polic...

Buttons: Add, Edit, Delete, Apply, Reset

2. انقر فوق الزر إضافة. يظهر مربع الحوار إضافة حساب مستخدم.

Add User Account

Identity VPN Policy WebVPN

Username: user1

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

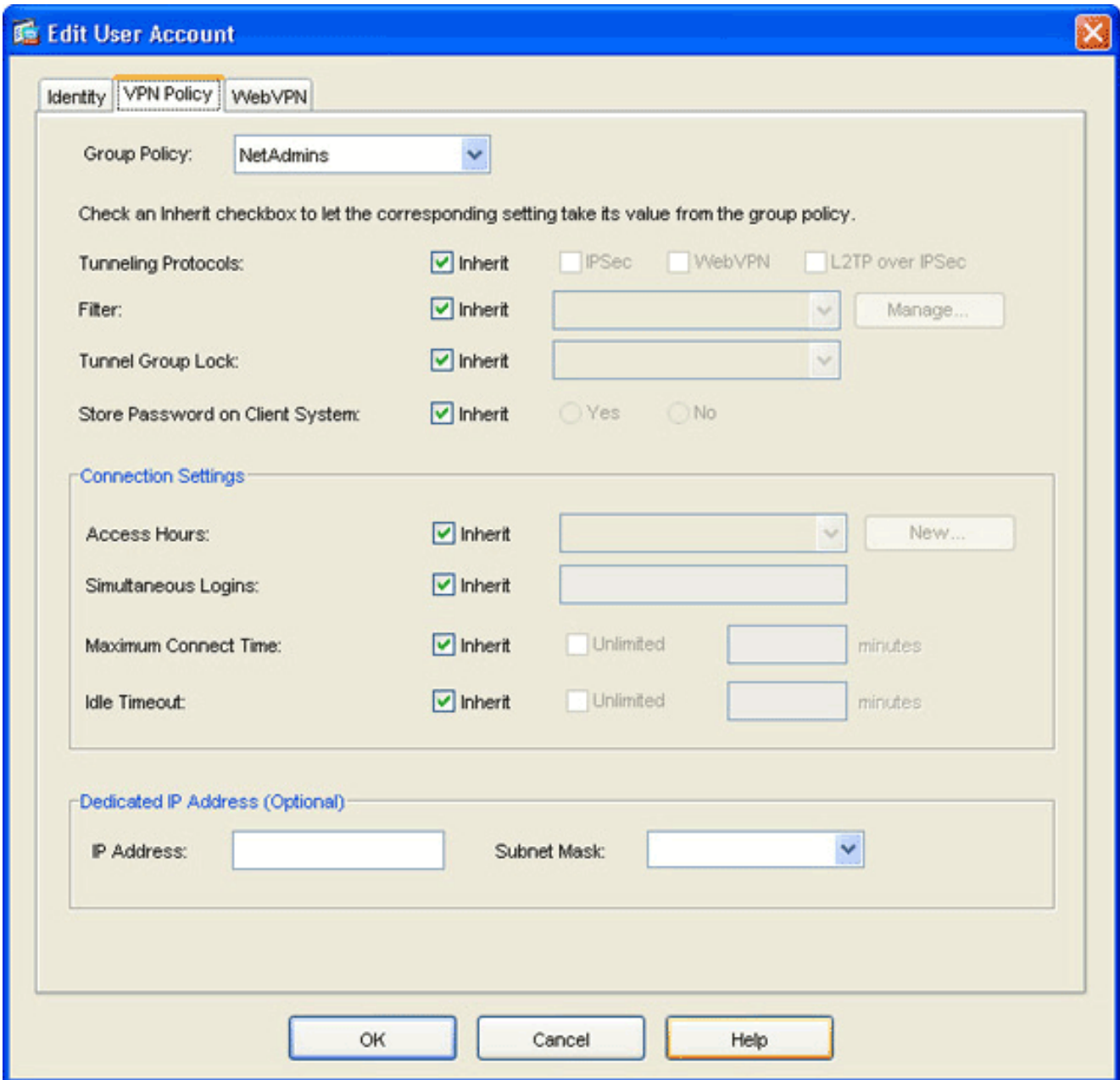
User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

OK Cancel Help

3. أدخل قيم لمعلومات اسم المستخدم وكلمة المرور والامتياز، ثم انقر فوق علامة التبويب سياسة .VPN



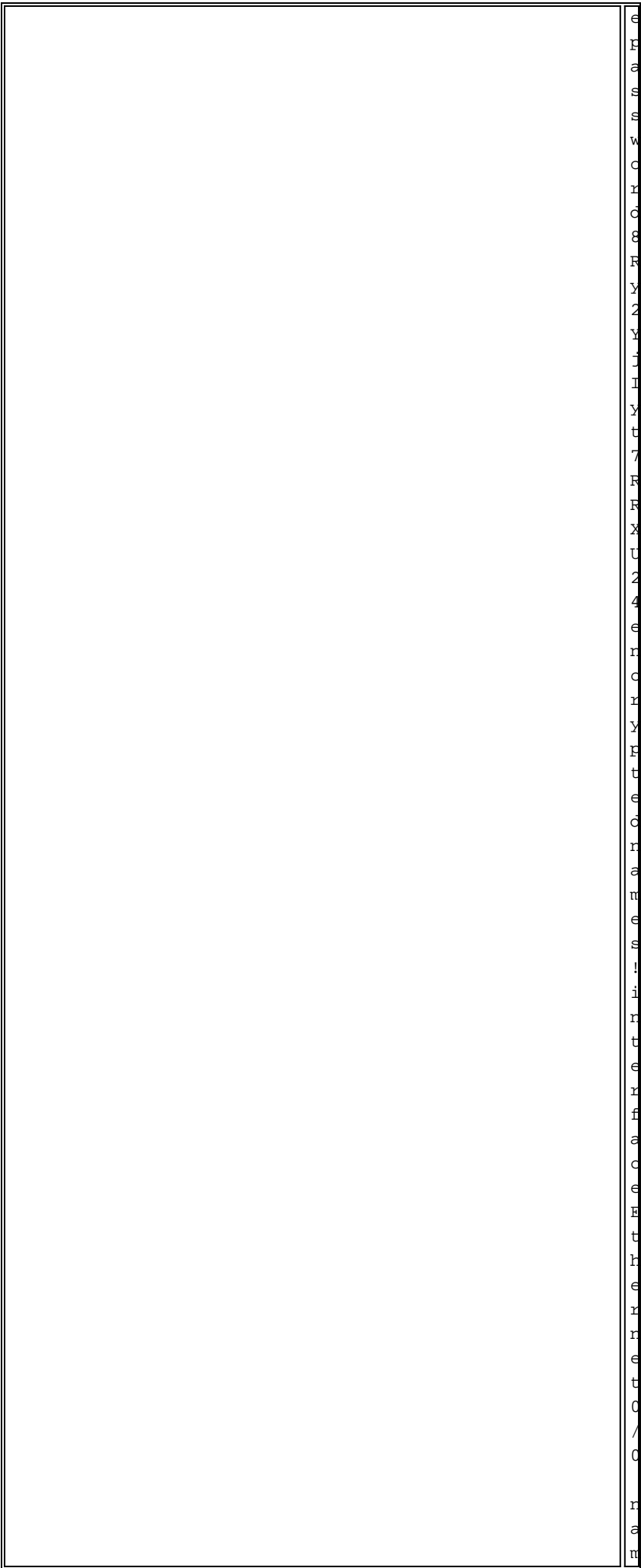
4. انقر فوق السهم المنسدل لـ **نهج المجموعة**، واختر نهج المجموعة الذي أنشأته في [الخطوة 3](#). يرث هذا المستخدم خصائص WebVPN ونهج نهج المجموعة المحددة.
5. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.
6. انقر فوق **حفظ**، ثم نعم لقبول التغييرات.

## تكوين VPN لـ SSL قليل السمك باستخدام CLI

	A S A
	A S A V E r s

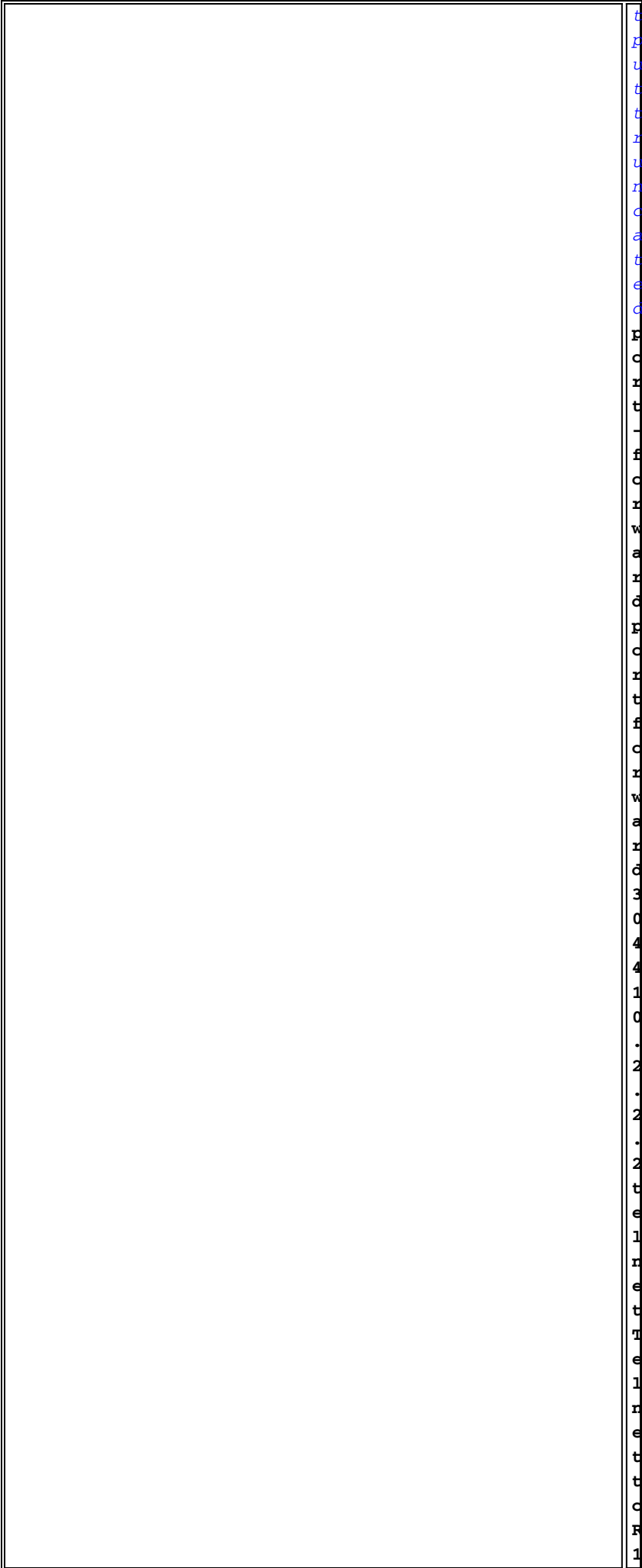
i	Contents
7	Introduction
2	Chapter 1
1	Chapter 2
1	Chapter 3
1	Chapter 4
1	Chapter 5
1	Chapter 6
1	Chapter 7
1	Chapter 8
1	Chapter 9
1	Chapter 10
1	Chapter 11
1	Chapter 12
1	Chapter 13
1	Chapter 14
1	Chapter 15
1	Chapter 16
1	Chapter 17
1	Chapter 18
1	Chapter 19
1	Chapter 20
1	Chapter 21
1	Chapter 22
1	Chapter 23
1	Chapter 24
1	Chapter 25
1	Chapter 26
1	Chapter 27
1	Chapter 28
1	Chapter 29
1	Chapter 30
1	Chapter 31
1	Chapter 32
1	Chapter 33
1	Chapter 34
1	Chapter 35
1	Chapter 36
1	Chapter 37
1	Chapter 38
1	Chapter 39
1	Chapter 40
1	Chapter 41
1	Chapter 42
1	Chapter 43
1	Chapter 44
1	Chapter 45
1	Chapter 46
1	Chapter 47
1	Chapter 48
1	Chapter 49
1	Chapter 50
1	Chapter 51
1	Chapter 52
1	Chapter 53
1	Chapter 54
1	Chapter 55
1	Chapter 56
1	Chapter 57
1	Chapter 58
1	Chapter 59
1	Chapter 60
1	Chapter 61
1	Chapter 62
1	Chapter 63
1	Chapter 64
1	Chapter 65
1	Chapter 66
1	Chapter 67
1	Chapter 68
1	Chapter 69
1	Chapter 70
1	Chapter 71
1	Chapter 72
1	Chapter 73
1	Chapter 74
1	Chapter 75
1	Chapter 76
1	Chapter 77
1	Chapter 78
1	Chapter 79
1	Chapter 80
1	Chapter 81
1	Chapter 82
1	Chapter 83
1	Chapter 84
1	Chapter 85
1	Chapter 86
1	Chapter 87
1	Chapter 88
1	Chapter 89
1	Chapter 90
1	Chapter 91
1	Chapter 92
1	Chapter 93
1	Chapter 94
1	Chapter 95
1	Chapter 96
1	Chapter 97
1	Chapter 98
1	Chapter 99
1	Chapter 100



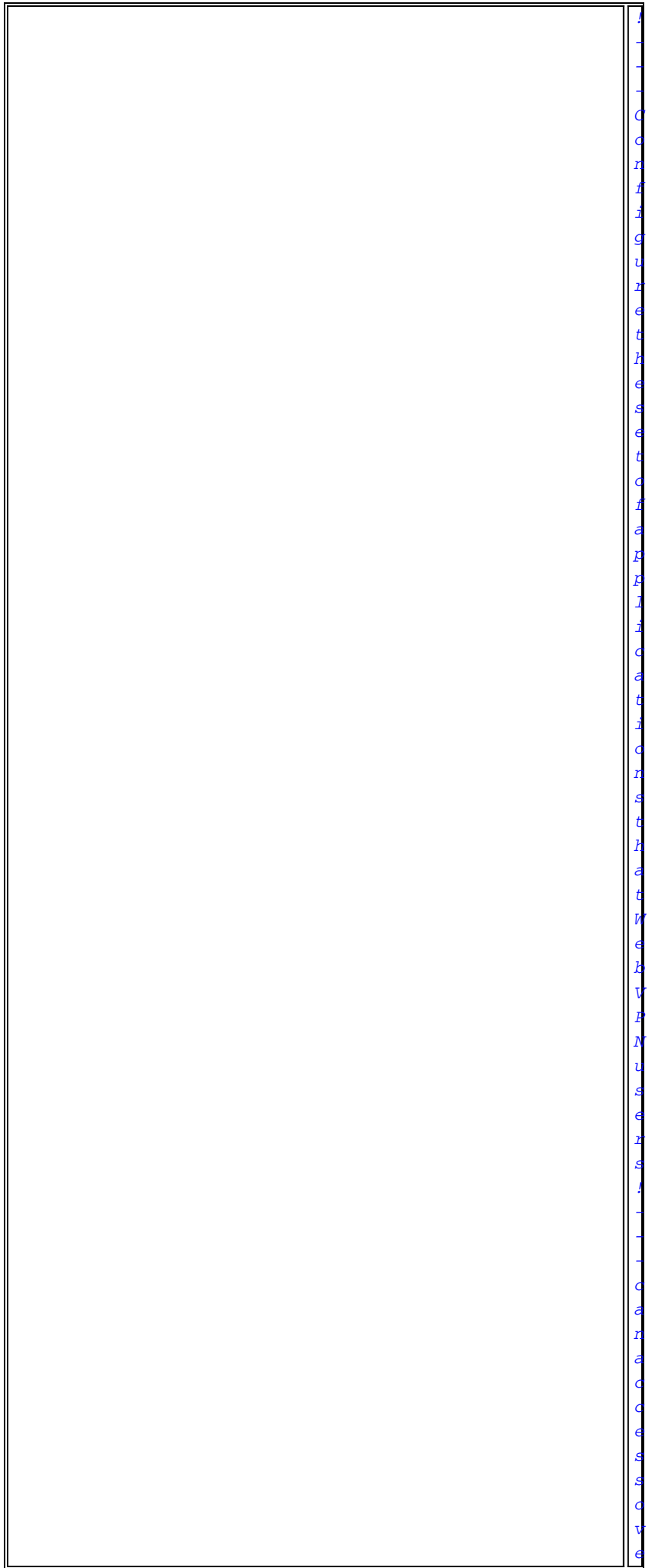


6  
H  
a  
s  
s  
w  
o  
r  
d  
8  
F  
Y  
2  
Y  
J  
I  
Y  
t  
7  
F  
F  
X  
U  
2  
4  
e  
r  
o  
r  
y  
F  
t  
e  
o  
r  
a  
m  
e  
s  
!  
i  
r  
t  
e  
r  
f  
a  
c  
e  
E  
t  
h  
e  
r  
e  
t  
c  
/

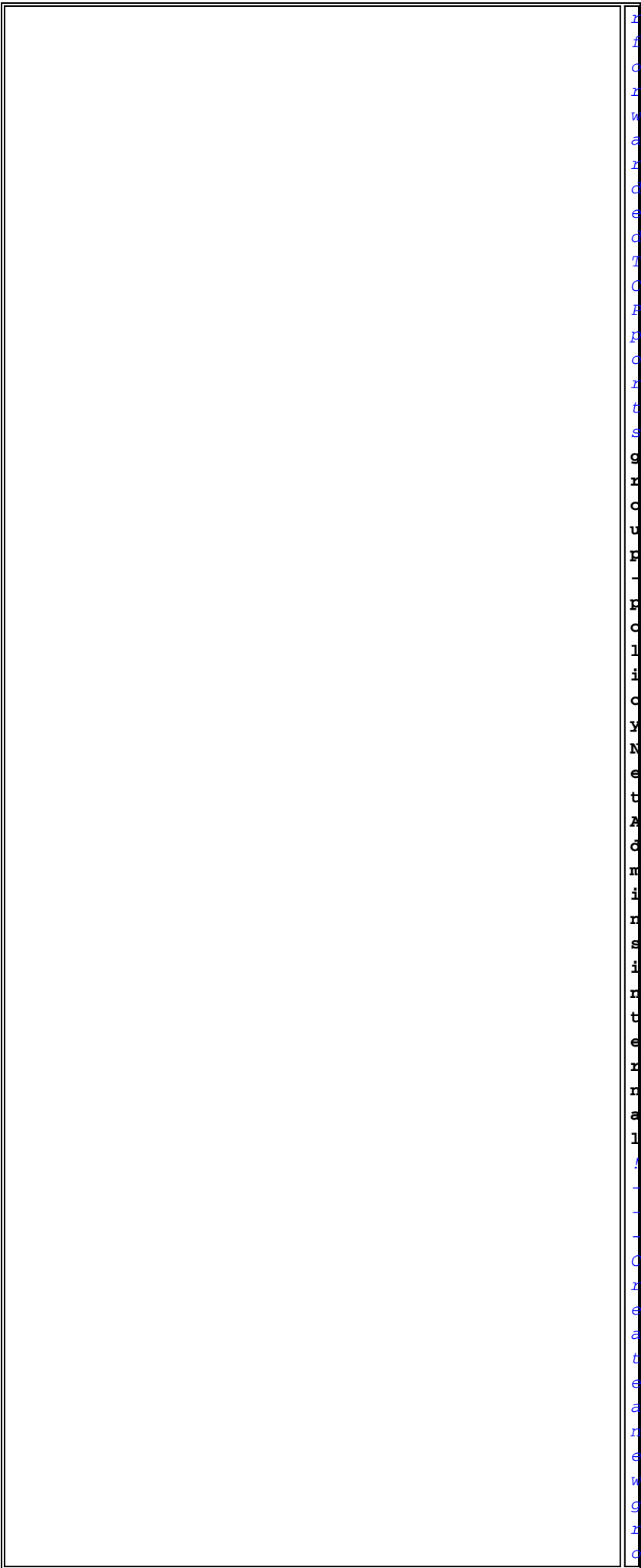
	6
	i
	f
	i
	r
	s
	i
	o
	e
	s
	e
	c
	u
	r
	i
	t
	y
	l
	e
	v
	e
	l
	l
	l
	c
	c
	i
	f
	a
	c
	o
	r
	e
	s
	s
	l
	c
	.
	l
	.
	l
	.
	l
	.
	l
	.
	2
	5
	5
	.
	2
	5
	5
	.
	2
	5
	5
	.
	c
	.
	l
	l
	l
	c
	l



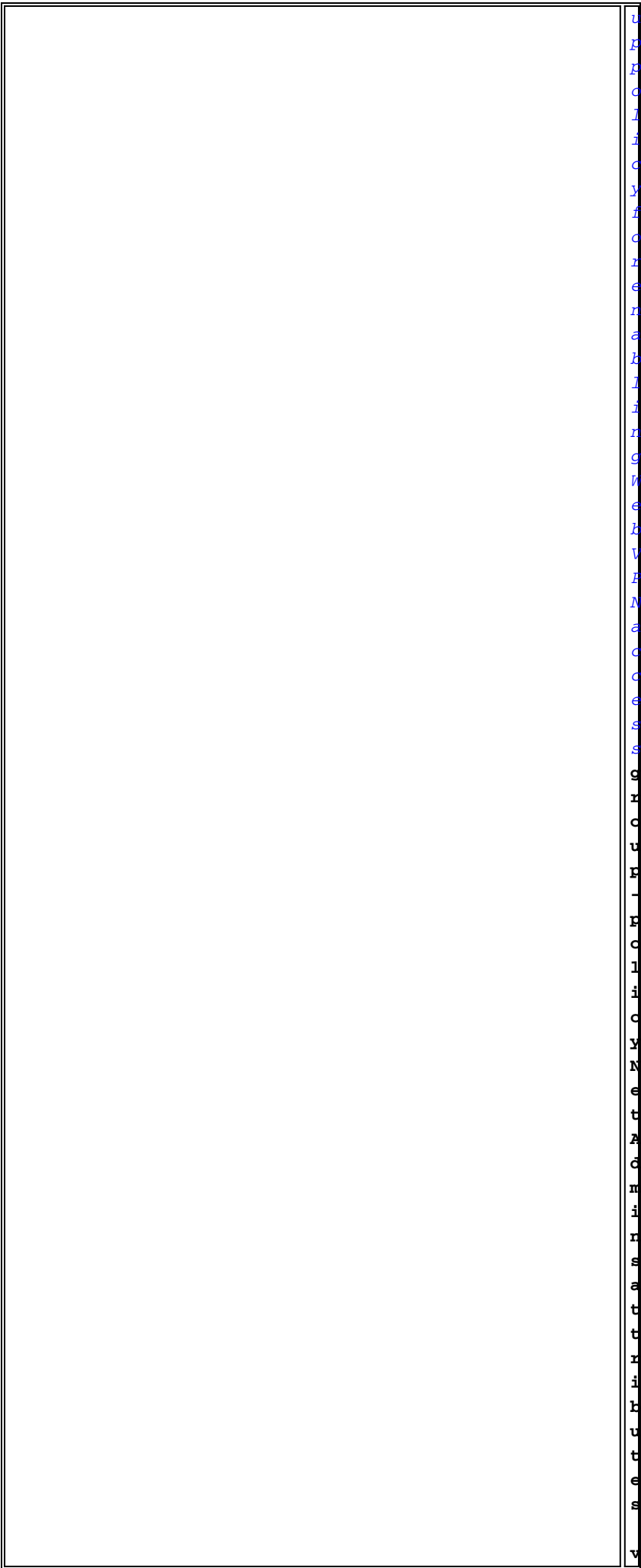
U  
t  
t  
U  
U  
O  
a  
t  
e  
C  
F  
C  
H  
t  
l  
F  
O  
H  
w  
a  
H  
G  
F  
C  
H  
t  
F  
C  
H  
v  
a  
H  
C  
E  
C  
A  
A  
1  
O  
. . .  
2  
. . .  
2  
. . .  
2  
t  
e  
l  
r  
e  
t  
F  
e  
l  
r  
e  
t  
C  
F  
l



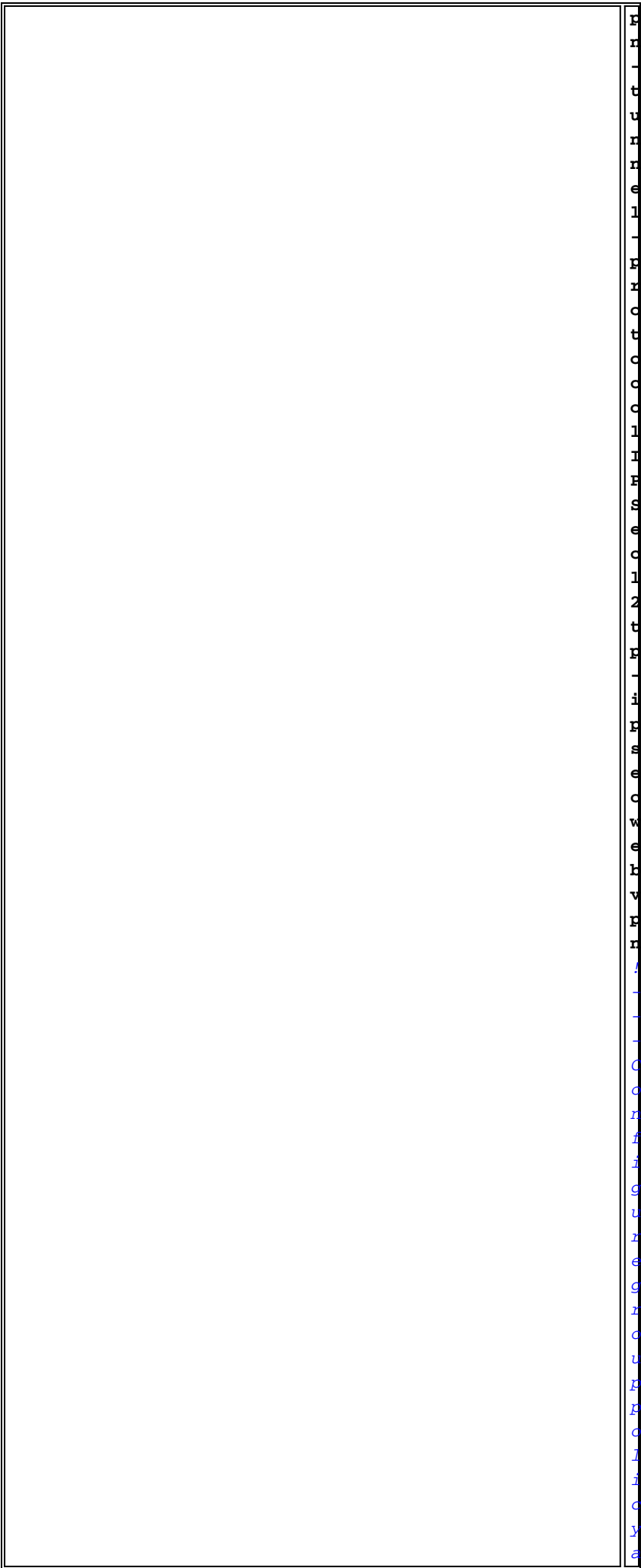
1  
1  
1  
1  
C  
o  
n  
f  
i  
g  
u  
r  
e  
t  
h  
e  
s  
s  
e  
t  
o  
f  
f  
a  
c  
t  
o  
r  
s  
a  
n  
d  
i  
n  
f  
l  
u  
e  
n  
c  
e  
s  
a  
t  
t  
r  
i  
b  
u  
t  
i  
n  
g  
t  
o  
t  
h  
e  
o  
u  
t  
c  
o  
m  
e  
s  
o  
f  
t  
h  
e  
m  
o  
d  
e  
l.  
W  
e  
h  
a  
v  
e  
v  
e  
r  
y  
o  
n  
e  
o  
f  
t  
h  
e  
s  
e  
f  
a  
c  
t  
o  
r  
s  
a  
n  
d  
i  
n  
f  
l  
u  
e  
n  
c  
e  
s  
i  
n  
o  
r  
d  
e  
r  
o  
f  
i  
m  
p  
o  
r  
t  
a  
n  
c  
e  
a  
n  
d  
i  
n  
t  
e  
r  
a  
c  
t  
i  
o  
n  
a  
m  
o  
u  
n  
t  
s.  
C  
o  
n  
f  
i  
d  
e  
n  
t  
i  
f  
y  
i  
n  
g  
t  
h  
e  
i  
m  
p  
o  
r  
t  
a  
n  
t  
f  
a  
c  
t  
o  
r  
s  
a  
n  
d  
i  
n  
f  
l  
u  
e  
n  
c  
e  
s  
a  
n  
d  
i  
n  
t  
e  
r  
a  
c  
t  
i  
o  
n  
a  
m  
o  
u  
n  
t  
s  
i  
s  
a  
c  
c  
e  
s  
s  
o  
f  
t  
h  
e  
o  
u  
t  
c  
o  
m  
e  
s  
o  
f  
t  
h  
e  
m  
o  
d  
e  
l.  
W  
e  
h  
a  
v  
e  
v  
e  
r  
y  
o  
n  
e  
o  
f  
t  
h  
e  
s  
e  
f  
a  
c  
t  
o  
r  
s  
a  
n  
d  
i  
n  
f  
l  
u  
e  
n  
c  
e  
s  
i  
n  
o  
r  
d  
e  
r  
o  
f  
i  
m  
p  
o  
r  
t  
a  
n  
c  
e  
a  
n  
d  
i  
n  
t  
e  
r  
a  
c  
t  
i  
o  
n  
a  
m  
o  
u  
n  
t  
s.

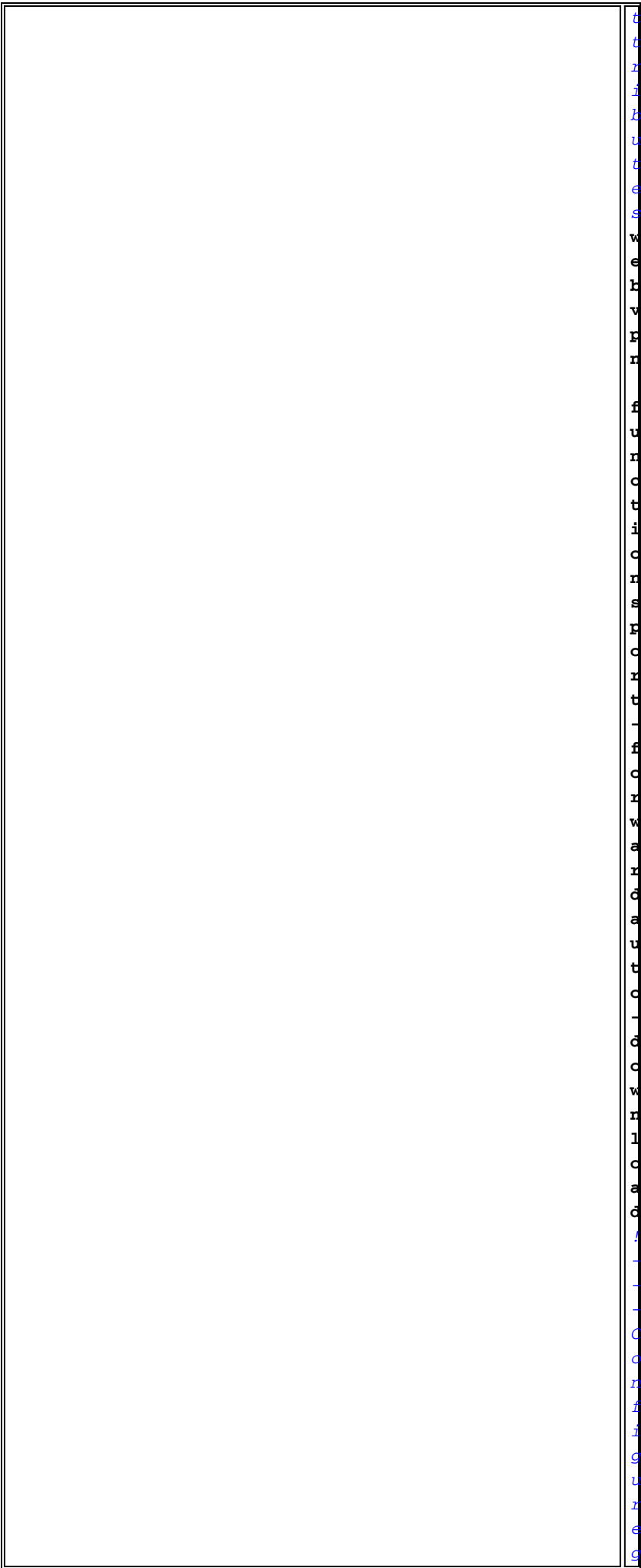


H  
H  
C  
H  
W  
a  
H  
C  
e  
C  
T  
C  
F  
H  
C  
H  
t  
s  
S  
S  
H  
C  
U  
H  
H  
C  
L  
i  
C  
Y  
M  
e  
t  
A  
C  
H  
i  
H  
S  
i  
H  
t  
e  
H  
H  
a  
l  
H  
H  
C  
H  
e  
a  
t  
e  
a  
H  
e  
W  
C  
H  
C



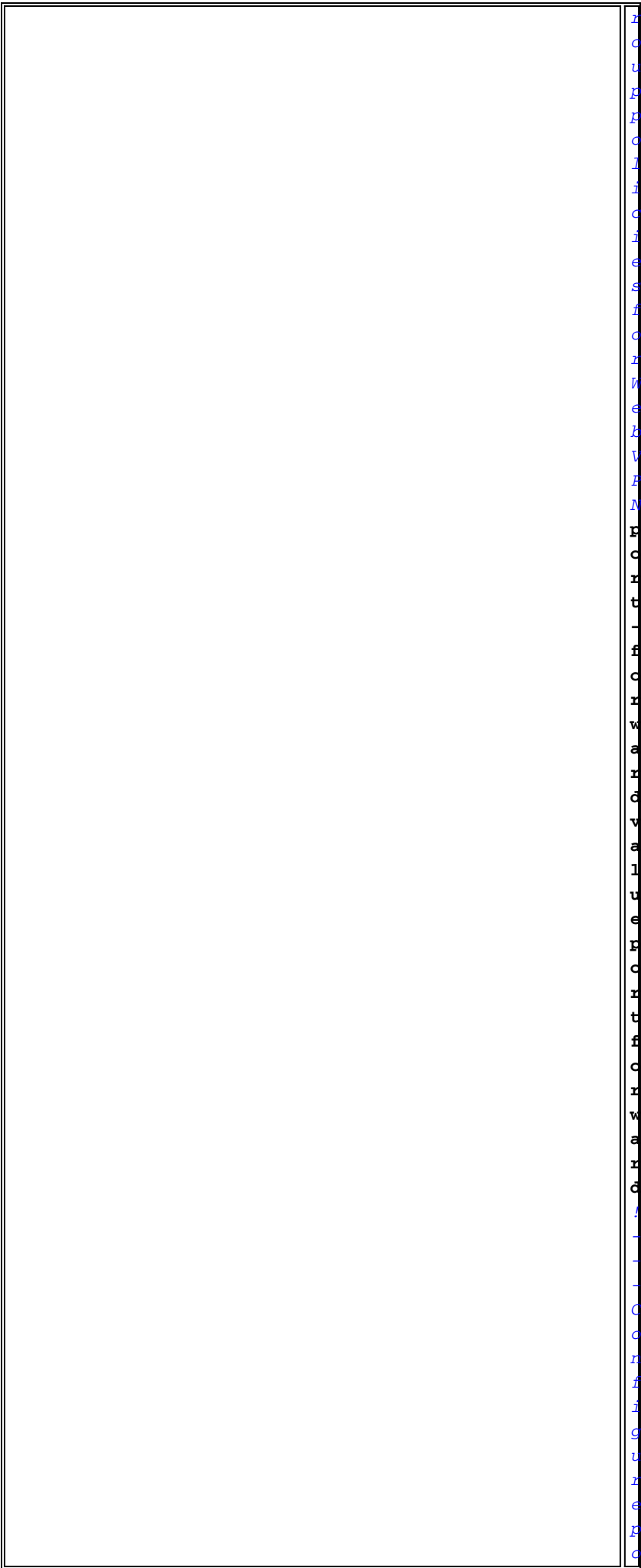
U  
F  
F  
C  
L  
i  
C  
Y  
f  
C  
r  
e  
n  
a  
b  
L  
i  
n  
G  
W  
e  
k  
V  
F  
N  
a  
C  
C  
e  
s  
s  
S  
G  
H  
C  
U  
F  
L  
F  
C  
L  
i  
C  
Y  
M  
e  
t  
A  
C  
H  
i  
r  
s  
a  
t  
t  
r  
i  
F  
U  
t  
e  
S  
V



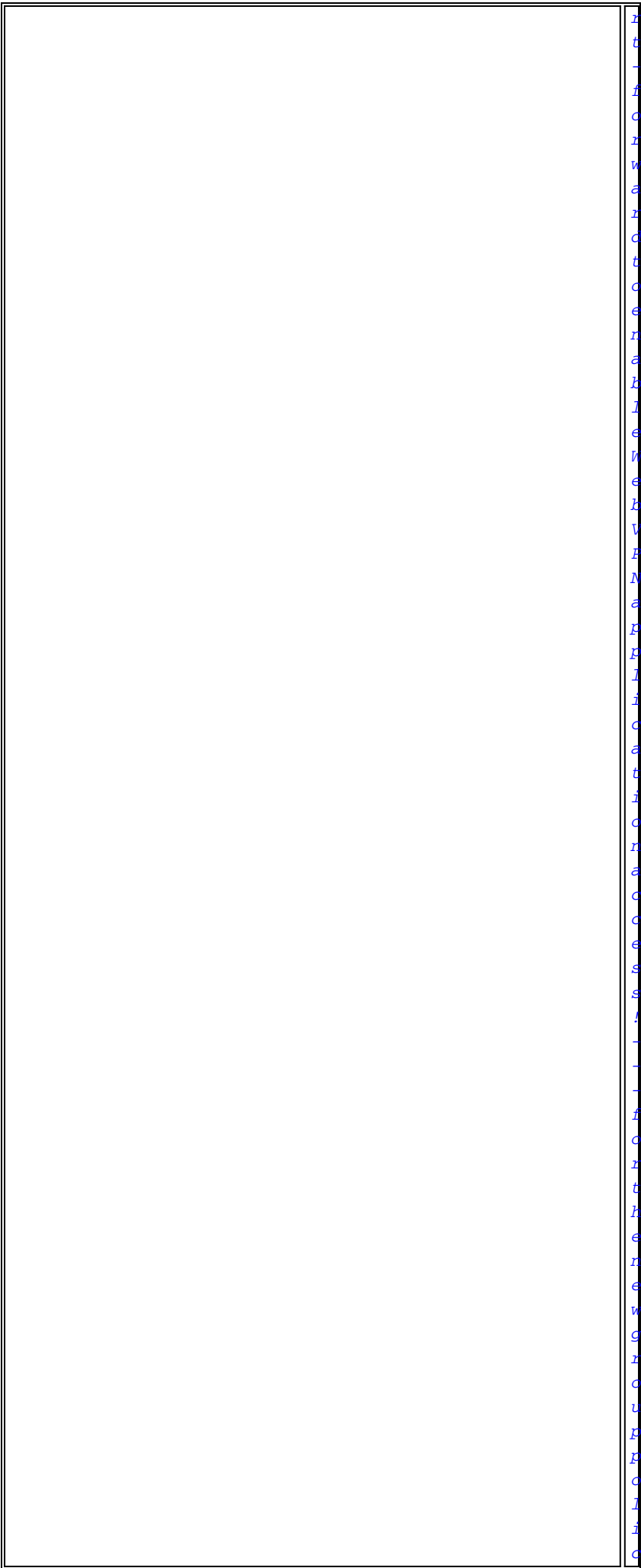


t  
b  
i  
b  
u  
t  
e  
s  
w  
e  
h  
v  
f  
n  
f  
u  
n  
o  
t  
i  
o  
n  
s  
f  
o  
r  
t  
h  
e  
c  
o  
o  
p  
e  
r  
a  
t  
i  
o  
n  
o  
f  
t  
h  
e  
u  
n  
i  
t  
e  
d  
n  
a  
t  
i  
o  
n  
s

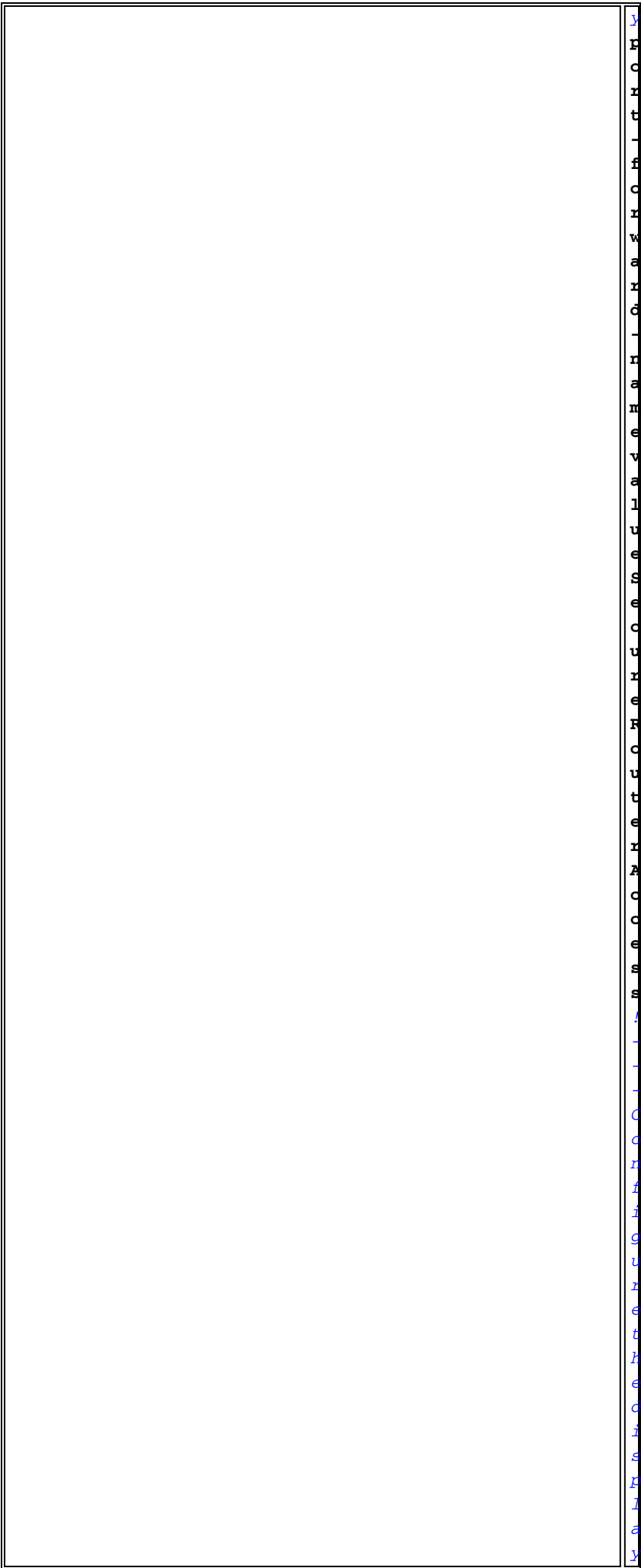




H  
C  
U  
F  
H  
C  
L  
i  
C  
i  
e  
S  
f  
C  
H  
W  
e  
k  
V  
F  
N  
H  
C  
H  
t  
l  
f  
C  
H  
v  
a  
H  
C  
v  
a  
l  
U  
e  
H  
C  
H  
t  
f  
C  
H  
v  
a  
H  
C  
N  
l  
l  
C  
H  
f  
H  
G  
U  
H  
e  
H  
C

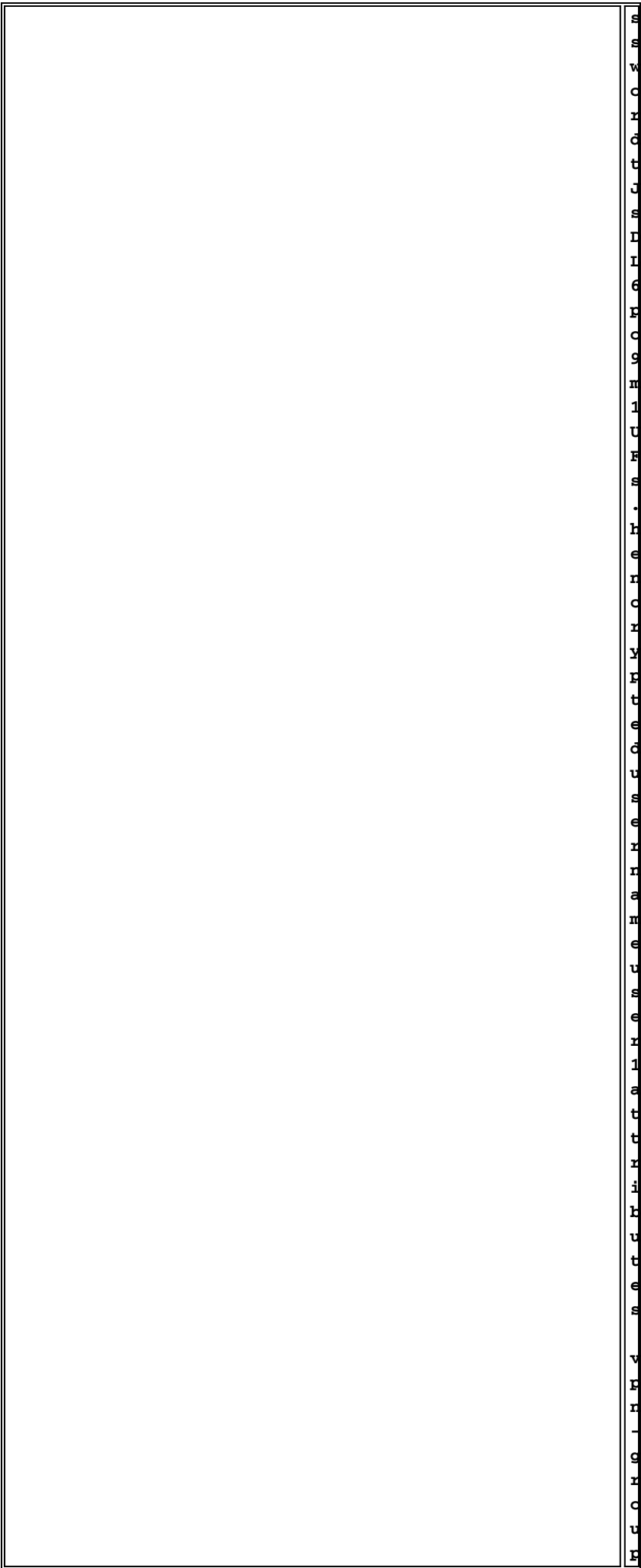


h  
t  
-  
f  
o  
r  
w  
a  
r  
d  
t  
o  
e  
n  
a  
b  
l  
e  
w  
e  
b  
v  
i  
d  
e  
o  
a  
n  
d  
i  
n  
t  
e  
r  
v  
i  
e  
w  
s  
a  
n  
d  
p  
o  
d  
c  
a  
s  
t  
s  
a  
n  
d  
m  
o  
r  
e  
i  
n  
f  
o  
r  
m  
a  
t  
i  
o  
n  
v  
i  
s  
i  
t  
h  
t  
t  
p  
:  
//  
w  
w  
w  
.  
h  
o  
m  
e  
b  
i  
n  
g  
r  
o  
u  
p  
.  
c  
o  
m

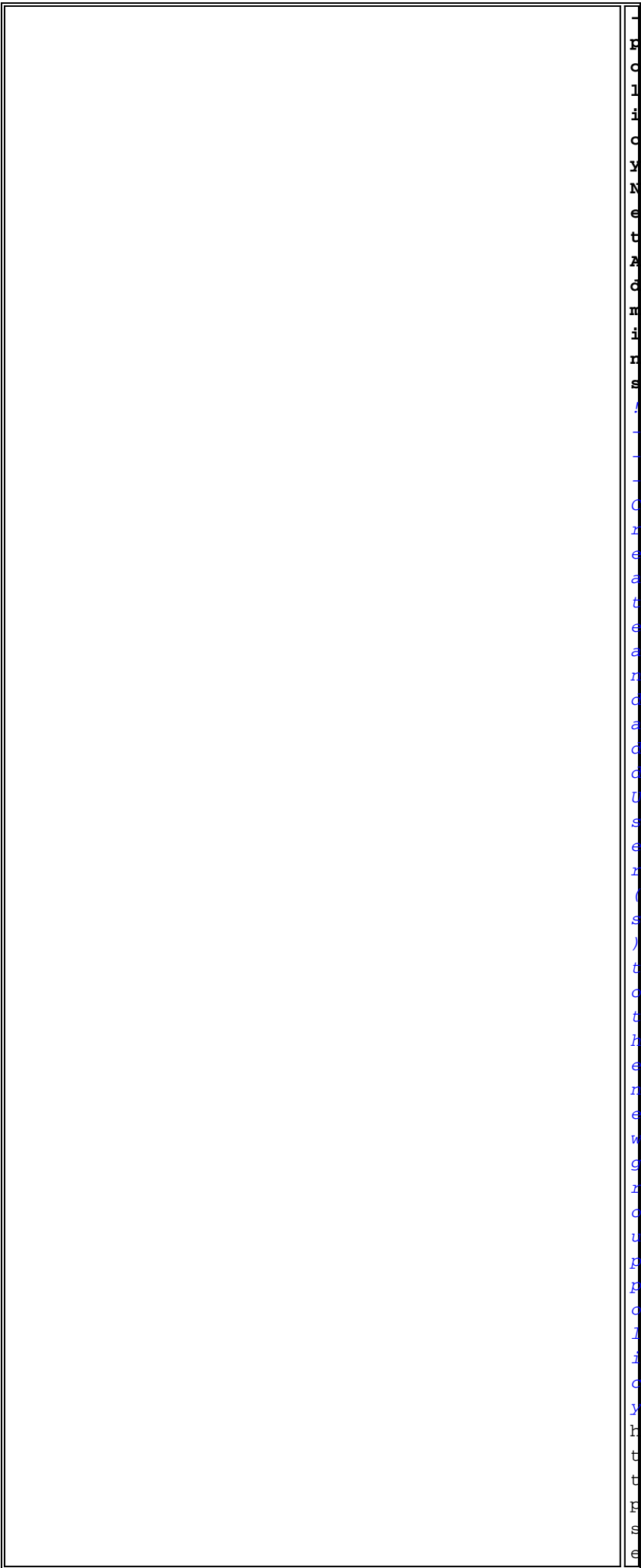


Y  
K  
O  
R  
t  
-  
f  
O  
R  
W  
a  
R  
C  
-  
H  
a  
H  
e  
v  
a  
l  
u  
e  
S  
C  
U  
H  
e  
F  
C  
U  
t  
e  
H  
M  
C  
C  
e  
S  
S  
N  
-  
I  
-  
C  
H  
H  
G  
U  
H  
e  
t  
H  
e  
C  
H  
S  
H  
I  
a  
Y

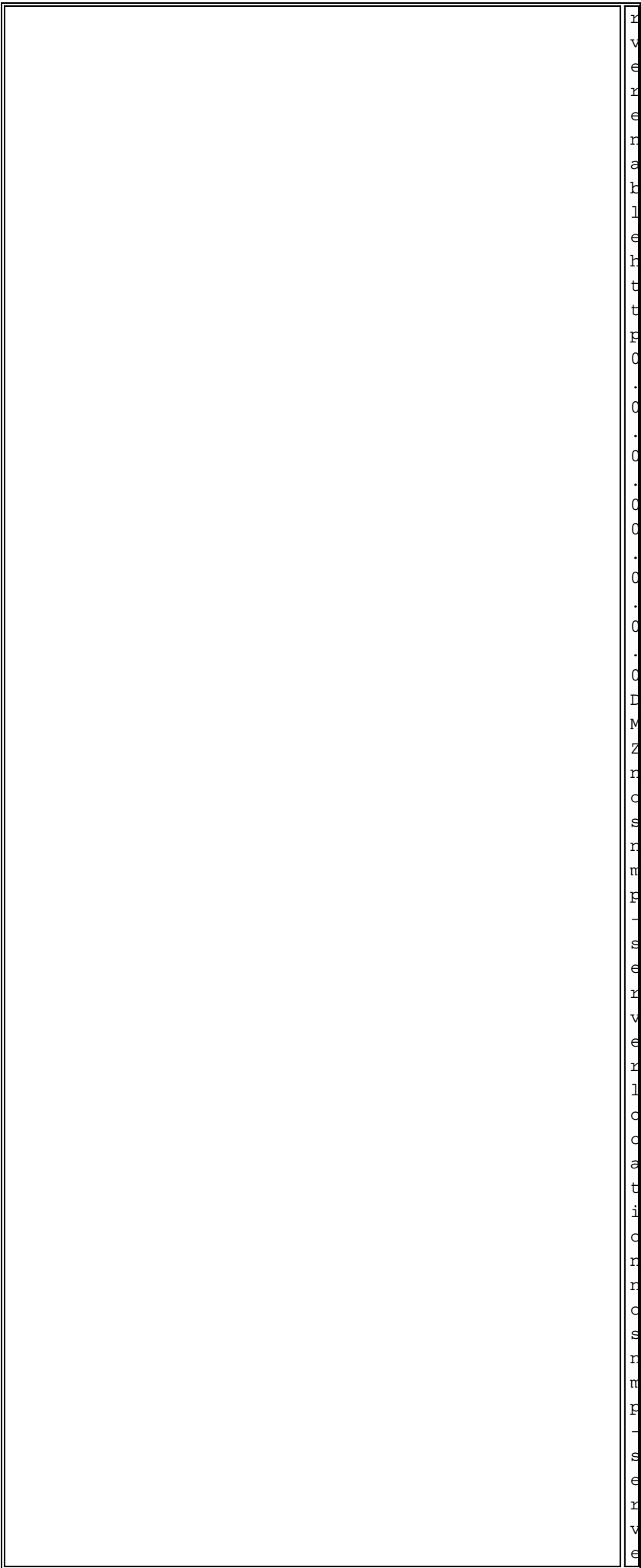
	n
	a
	m
	e
	t
	h
	a
	t
	i
	d
	e
	n
	t
	i
	f
	i
	e
	s
	s
	T
	O
	F
	F
	C
	n
	t
	!
	-
	-
	f
	C
	n
	w
	a
	n
	C
	i
	n
	G
	t
	C
	e
	n
	C
	U
	s
	e
	n
	s
	U
	s
	e
	H
	r
	a
	H
	e
	U
	s
	e
	H
	1
	F
	a



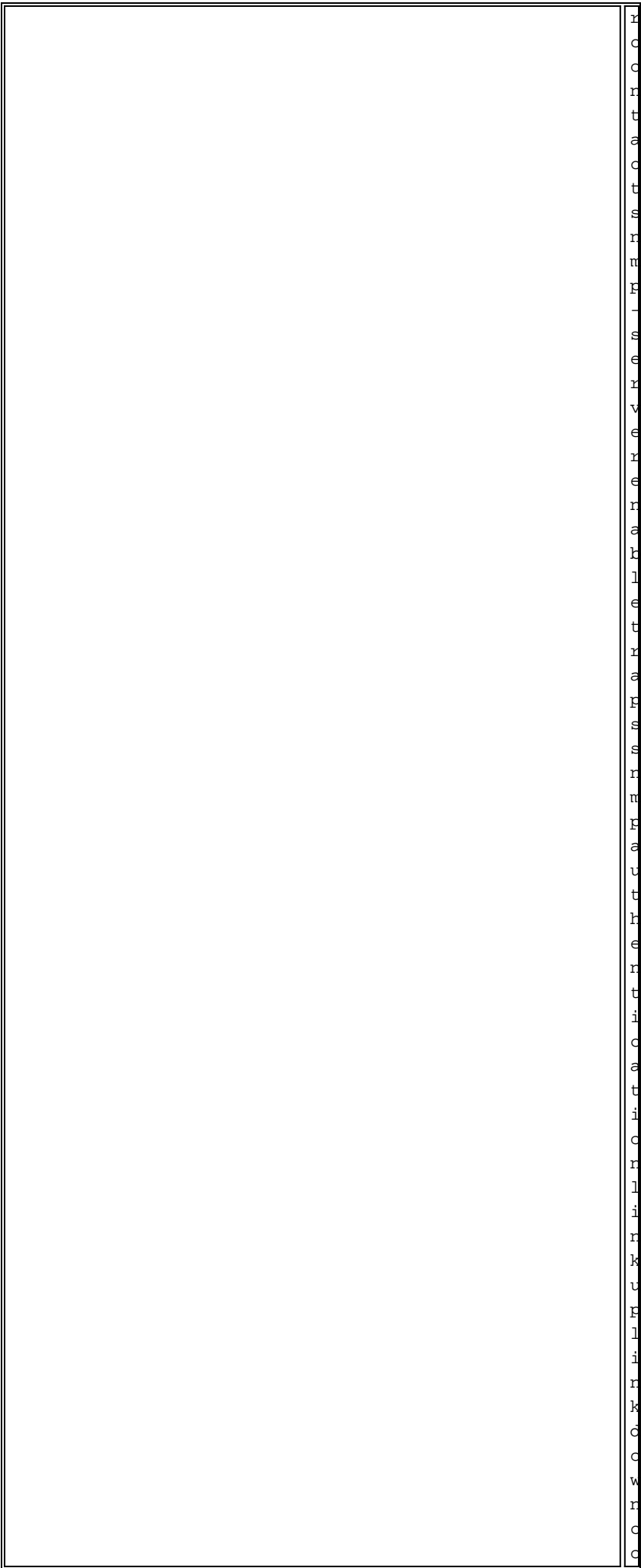
S  
S  
W  
O  
R  
O  
t  
J  
S  
I  
I  
6  
K  
O  
S  
H  
1  
U  
F  
S  
.  
H  
e  
H  
O  
H  
Y  
H  
t  
e  
C  
U  
S  
e  
H  
H  
a  
H  
e  
U  
S  
e  
H  
1  
a  
t  
t  
H  
i  
H  
U  
t  
e  
S  
v  
H  
H  
L  
G  
H  
C  
U  
T



1  
F  
C  
L  
i  
C  
V  
N  
e  
t  
A  
C  
m  
i  
n  
s  
:  
-  
-  
O  
r  
e  
a  
t  
e  
a  
r  
C  
a  
C  
U  
s  
e  
r  
(  
s  
)  
t  
C  
t  
H  
e  
r  
e  
w  
G  
r  
C  
U  
F  
F  
C  
I  
C  
V  
r  
t  
t  
r  
s  
e



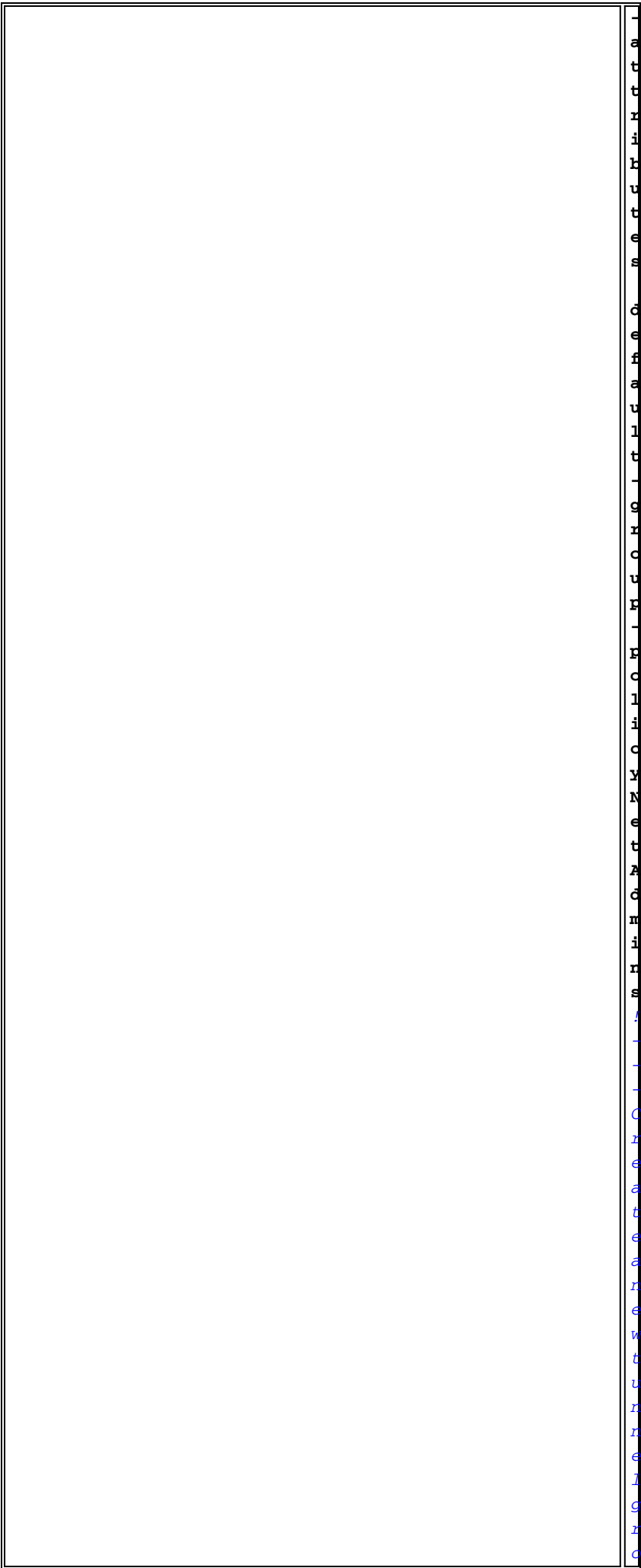
REVISED



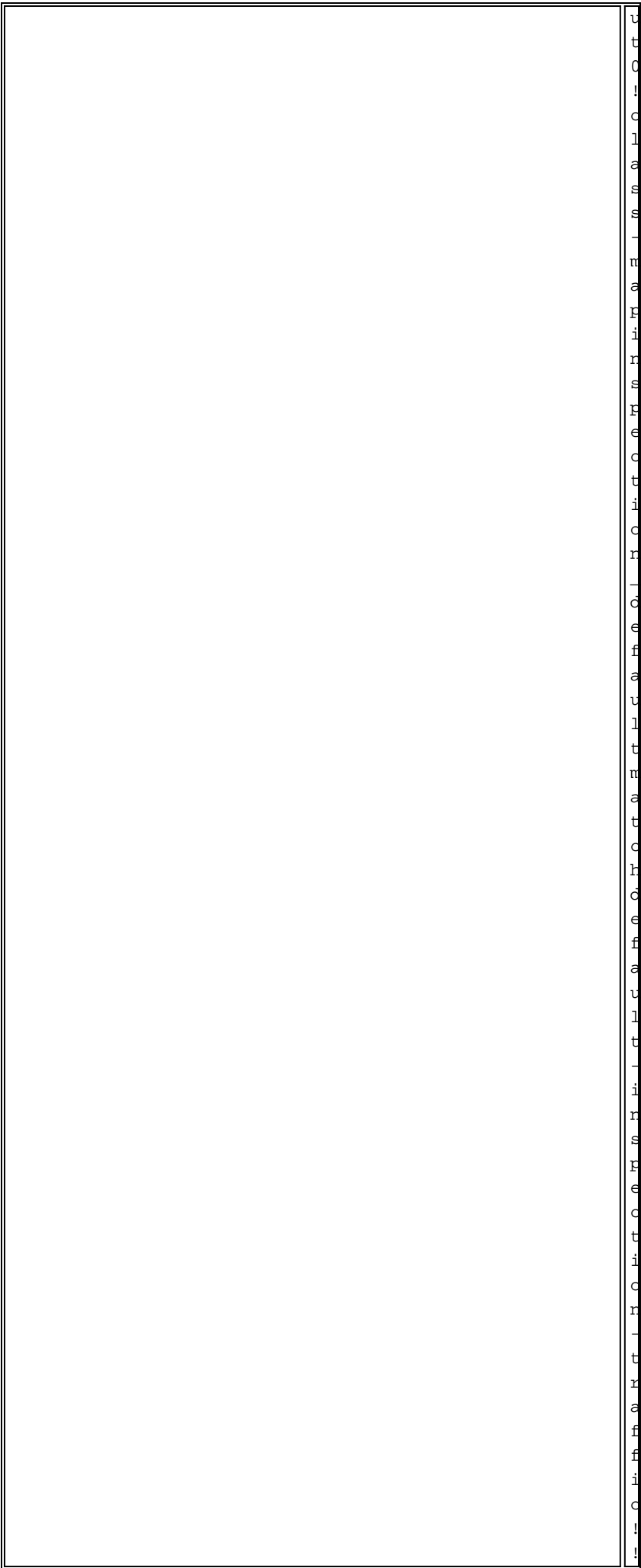
r  
o  
c  
k  
t  
a  
c  
t  
s  
n  
m  
f  
l  
s  
e  
r  
v  
e  
r  
e  
n  
a  
b  
l  
e  
t  
r  
a  
s  
s  
n  
m  
f  
a  
u  
t  
h  
e  
r  
t  
i  
o  
a  
t  
i  
o  
n  
l  
i  
n  
k  
u  
f  
l  
i  
r  
k  
o  
c  
w  
r  
o  
c



	l
	o
	s
	t
	a
	r
	t
	t
	u
	n
	n
	e
	l
	l
	g
	n
	c
	u
	n
	n
	e
	t
	G
	n
	c
	u
	n
	t
	y
	n
	e
	v
	e
	H
	v
	n
	t
	u
	n
	n
	e
	l
	l
	g
	n
	c
	u
	n
	n
	e
	t
	G
	n
	c
	u
	n
	g
	e
	n
	e
	r
	a
	l



	U
	F
	a
	n
	d
	L
	i
	n
	k
	i
	t
	t
	c
	t
	H
	e
	S
	G
	H
	c
	U
	F
	F
	c
	L
	i
	c
	Y
	t
	e
	l
	r
	e
	t
	t
	i
	n
	e
	c
	U
	t
	E
	s
	s
	R
	t
	i
	n
	e
	c
	U
	t
	E
	c
	O
	R
	s
	c
	L
	e
	t
	i
	n
	e
	c

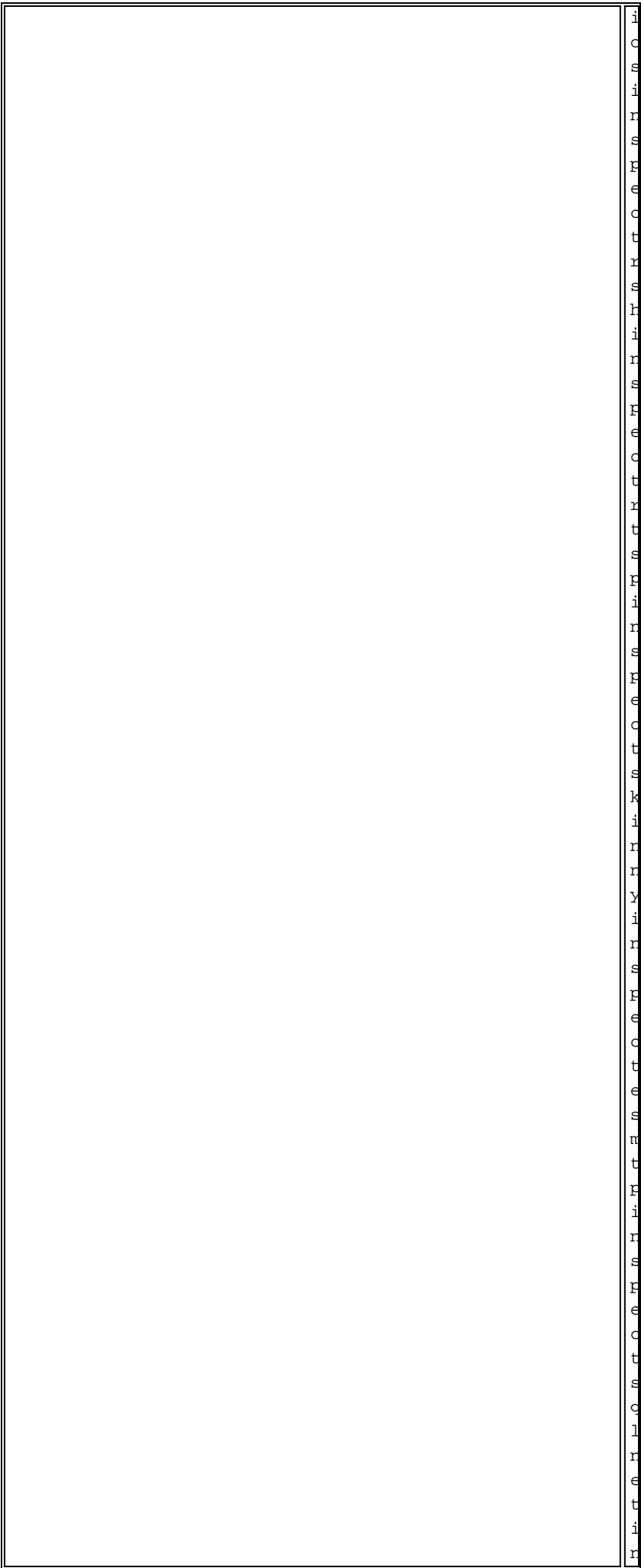


U  
t  
O  
!  
o  
l  
a  
s  
s  
-  
n  
a  
n  
i  
n  
s  
n  
e  
o  
t  
i  
o  
n  
-  
o  
e  
f  
a  
u  
l  
t  
n  
a  
t  
o  
r  
o  
e  
f  
a  
u  
l  
t  
-  
i  
n  
s  
n  
e  
o  
t  
i  
o  
n  
-  
t  
r  
a  
s  
f  
i  
o  
!

R  
o  
l  
l  
i  
n  
c  
o  
u  
n  
c  
i  
l  
l  
y  
-  
m  
a  
j  
o  
r  
i  
t  
y  
v  
o  
t  
e  
s  
r  
e  
q  
u  
i  
r  
e  
d  
t  
o  
c  
o  
n  
s  
e  
n  
s  
e  
t  
t  
e  
r  
a  
n  
d  
c  
o  
n  
f  
i  
r  
m  
l  
y  
a  
n  
d  
t  
h  
e  
c  
o  
n  
s  
e  
n  
s  
e  
t  
t  
e  
r  
i  
n  
g  
s  
a  
n  
d  
t  
h  
e  
t  
e  
r  
m  
i  
n  
a  
t  
i  
o  
n  
s  
s  
h  
a  
l  
l  
b  
e  
c  
o  
n  
f  
i  
r  
m  
l  
y  
a  
n  
d  
t  
h  
e  
c  
o  
n  
s  
e  
n  
s  
e  
t  
t  
e  
r  
i  
n  
g  
s

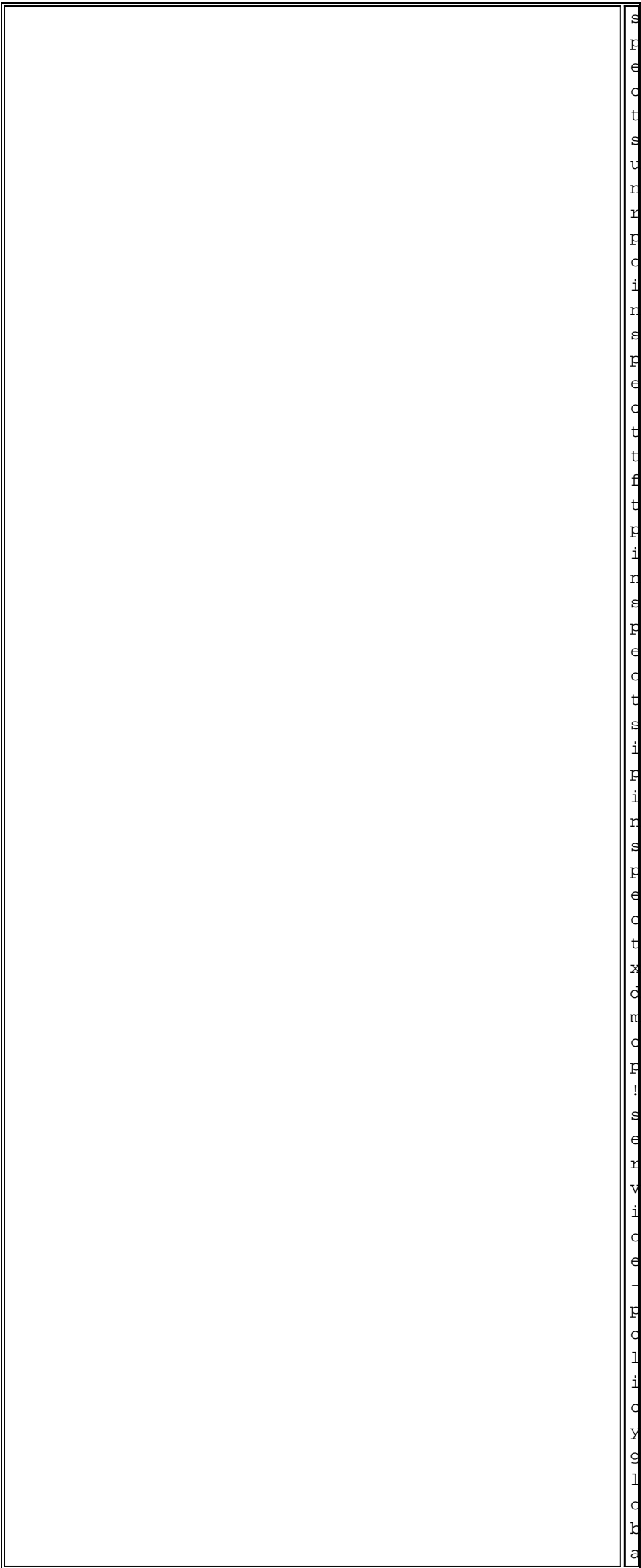
	x
	i
	n
	u
	n
	5
	1
	2
	F
	c
	l
	i
	c
	y
	l
	m
	a
	F
	g
	l
	c
	k
	a
	l
	l
	F
	c
	l
	i
	c
	y
	c
	l
	a
	s
	s
	s
	i
	r
	s
	F
	e
	c
	t
	t
	i
	c
	r
	l
	c
	e
	f
	a
	u
	l
	t
	t
	i
	r
	s
	F
	e
	c
	c
	t
	c
	r
	s

	R
	r
	e
	s
	s
	e
	t
	t
	l
	o
	r
	s
	l
	m
	a
	f
	i
	r
	s
	f
	e
	c
	t
	t
	f
	t
	f
	r
	i
	r
	s
	f
	e
	c
	t
	t
	r
	3
	2
	3
	r
	2
	2
	5
	i
	r
	s
	f
	e
	c
	t
	r
	3
	2
	3
	r
	a
	s
	i
	r
	s
	f
	e
	c
	t
	t
	r
	e
	t
	r

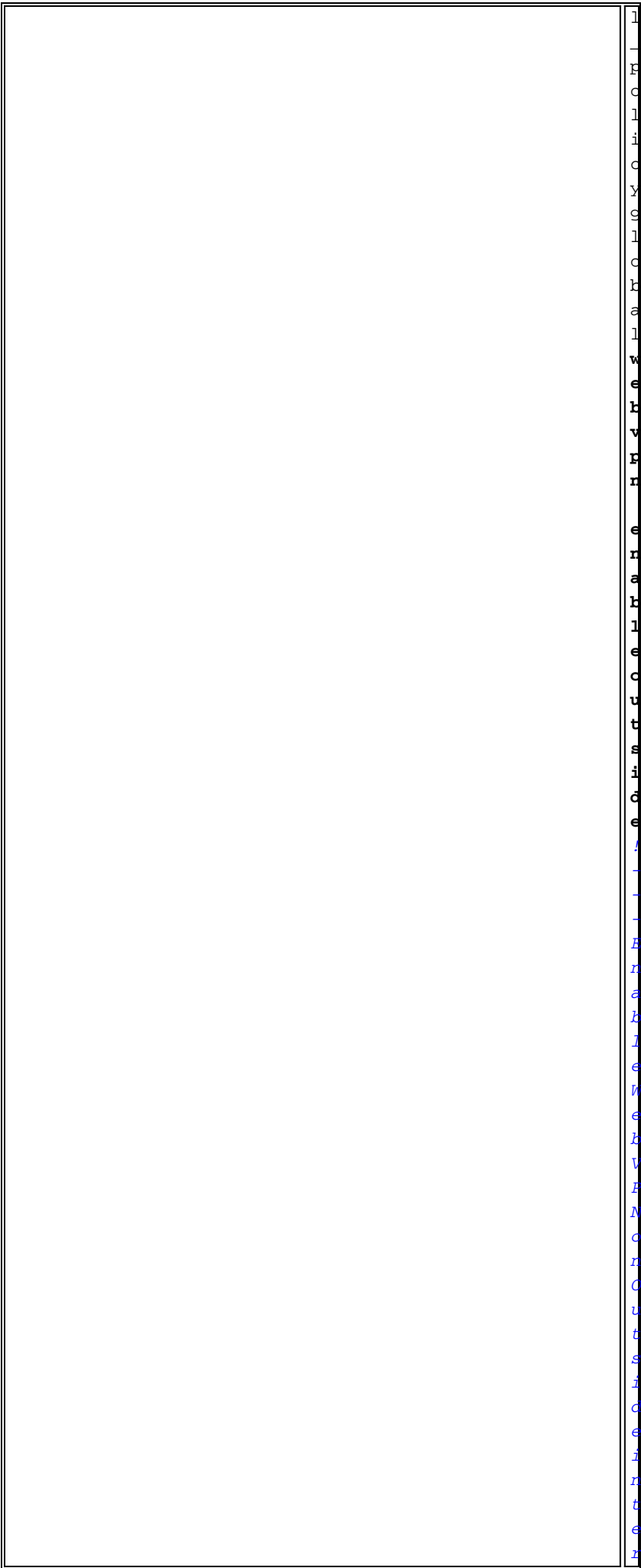


i  
o  
s  
i  
n  
s  
e  
o  
t  
r  
s  
h  
i  
n  
s  
e  
o  
t  
r  
t  
s  
f  
i  
n  
s  
e  
o  
t  
s  
k  
i  
n  
r  
y  
i  
n  
s  
e  
o  
t  
e  
s  
n  
t  
f  
i  
n  
s  
e  
o  
t  
s  
c  
l  
r  
e  
t  
i  
r

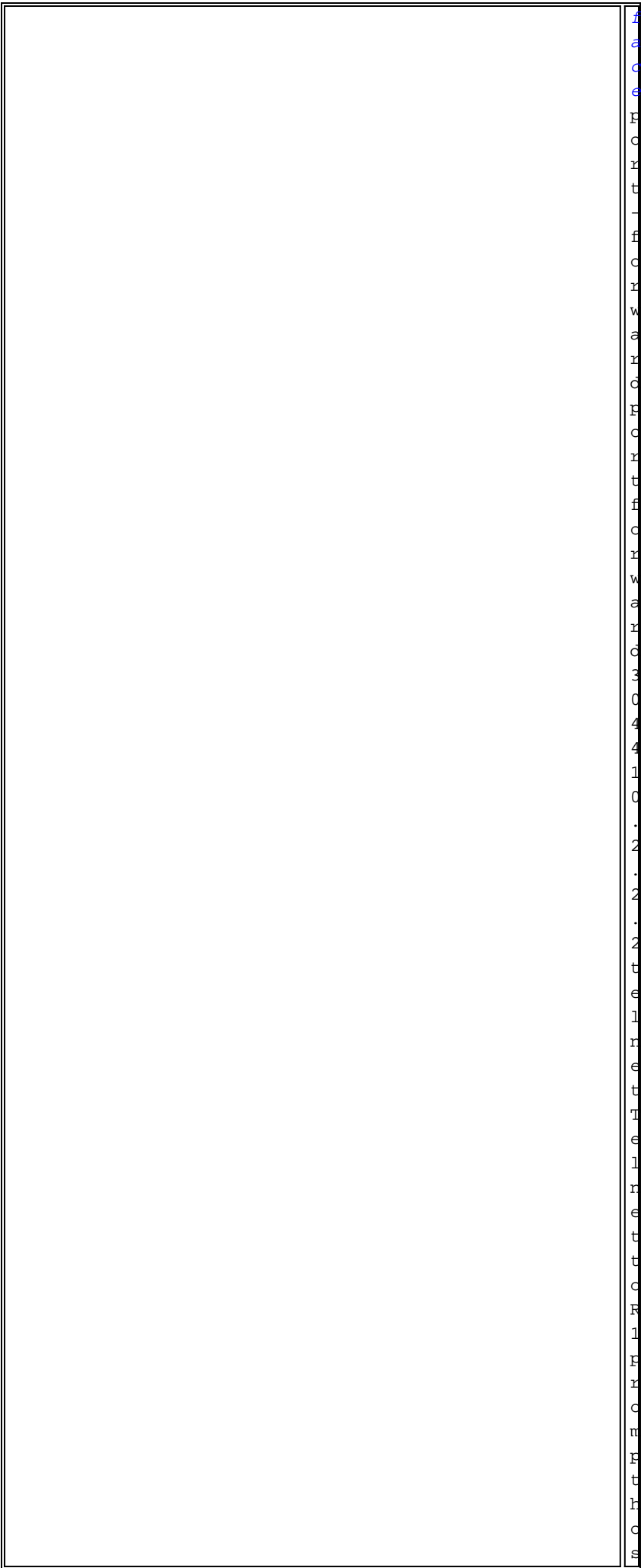




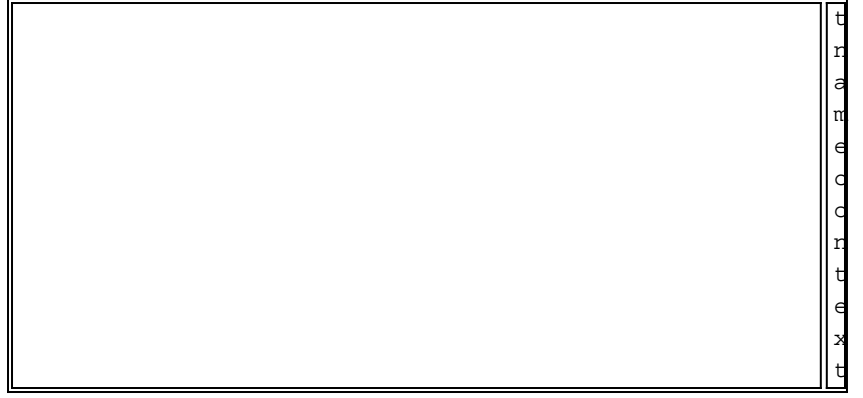
S  
R  
e  
o  
t  
s  
J  
n  
R  
o  
i  
n  
s  
R  
e  
o  
t  
t  
t  
f  
t  
R  
i  
n  
s  
R  
e  
o  
t  
s  
i  
R  
i  
n  
s  
R  
e  
o  
t  
x  
o  
n  
o  
R  
!  
s  
e  
R  
v  
i  
o  
e  
-  
R  
o  
l  
i  
o  
y  
s  
l  
o  
R  
a



l
l
k
c
l
i
c
y
g
l
c
k
a
l
w
e
k
v
k
n
n
e
n
a
k
l
e
c
u
t
s
i
c
e
n
l
l
B
n
a
k
k
e
W
e
k
V
F
N
c
n
c
u
t
s
k
c
e
k
n
t
e
n



h  
a  
c  
e  
r  
c  
r  
t  
i  
f  
c  
r  
w  
a  
r  
c  
r  
c  
r  
w  
a  
r  
c  
3  
c  
4  
4  
1  
c  
.  
2  
.  
2  
.  
2  
t  
e  
l  
r  
e  
t  
T  
e  
l  
r  
e  
t  
t  
c  
F  
l  
F  
r  
c  
n  
F  
t  
r  
c  
s



## التحقق من الصحة

أستخدم هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

## الإجراء

يوضح هذا الإجراء كيفية تحديد صلاحية التكوين وكيفية إختبار التكوين.

1. من محطة عمل عميلة، أدخل `https://:خارج_IP_ASA` ؛ حيث يكون `outside_IPAddress` هو عنوان SSL URL ل ASA. بمجرد قبول الشهادة الرقمية، ومصادقة المستخدم، تظهر صفحة ويب خدمة WebVPN.

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `https://172.22.1.160/+webvpn+/portal.html`. The page content includes the Cisco Systems logo and the heading 'WebVPN Service'. Below this, there is a section titled 'SECURE ROUTER ACCESS' with a 'Start Application Client' button. A modal dialog box is overlaid on the page, containing the following text:

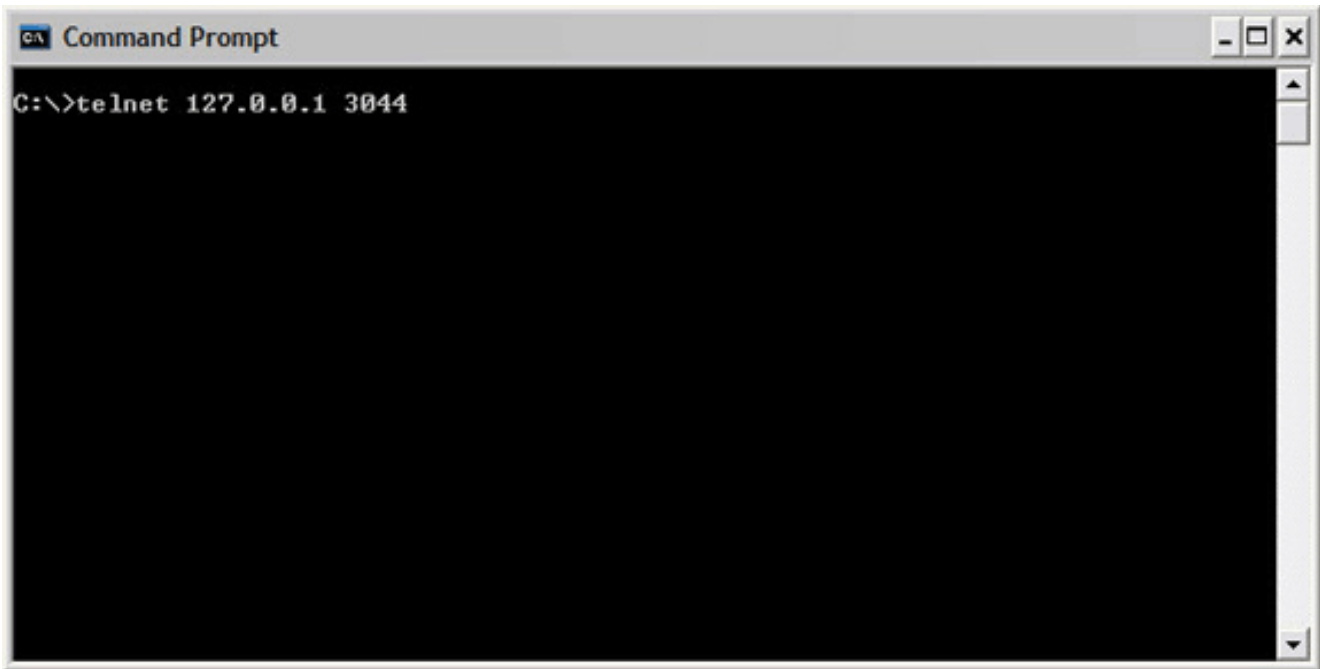
Close this window when you finish using Application Access.  
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. [Click here for details.](#)

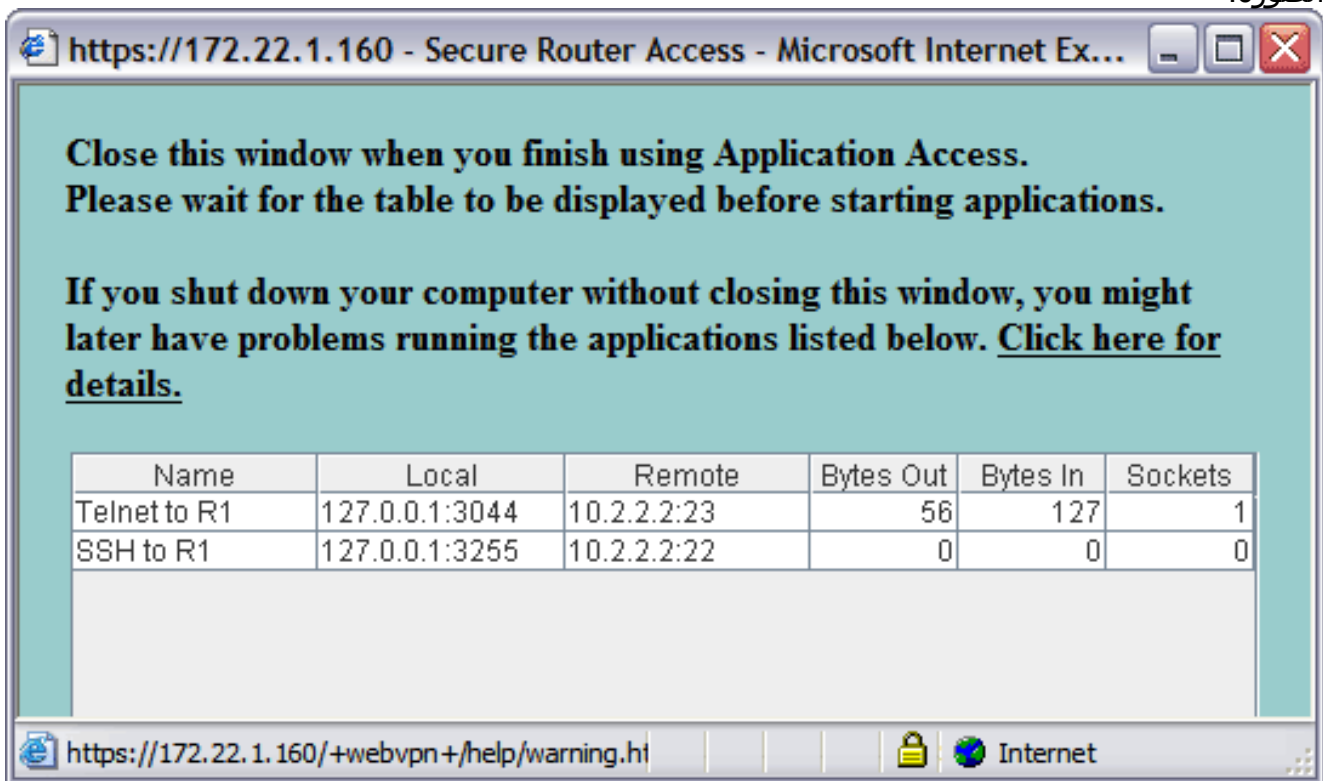
Name	Local	Remote	Bytes Out	Bytes In	Sockets
Telnet to R1	127.0.0.1:3044	10.2.2.2:23	0	0	0
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0

The dialog box also shows a 'Done' button at the bottom left and a status bar at the bottom right indicating 'Internet' access.

- تظهر معلومات العنوان والمنفذ المطلوبة للوصول إلى التطبيق في العمود المحلي. لا تعرض الأعمدة "بايت خارج" و"بايت في" أي نشاط نظرا لعدم إستدعاء التطبيق في هذا الوقت.
2. أستخدم مطالبة DOS أو تطبيق Telnet آخر لبدء جلسة عمل Telnet.
3. في موجه الأمر، أدخل `Telnet 127.0.0.1 3044`. ملاحظة: يقدم هذا الأمر مثالا لكيفية الحصول على الوصول إلى المنفذ المحلي المعروض في صورة صفحة ويب لخدمة WebVPN في هذا المستند. لا يتضمن الأمر علامة نقطتين (:). اكتب الأمر كما هو موضح في هذا المستند. يتلقى ال ASA الأمر على ال يأمن جلسة، ولأنه يخزن خريطة من المعلومة، ال ASA يعرف فورا أن يفتح الآمن telnet جلسة إلى ال يخطط أداة.



بمجرد إدخال اسم المستخدم وكلمة المرور، يكتمل الوصول إلى الجهاز.  
4. للتحقق من الوصول إلى الجهاز، تحقق من وجود "وحدات البايت" و"وحدات البايت" في الأعمدة كما هو موضح في هذه الصورة:



## الأوامر

يتم إقران العديد من أوامر العرض مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات ومعلومات أخرى. للحصول على معلومات تفصيلية حول أوامر العرض، ارجع إلى [التحقق من تكوين WebVPN](#).

ملاحظة: الإنتاج مترجم بساند أداة (يسجل زبون فقط) (OIT) مؤكد عرض أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر show .

## استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

### هل اكتملت عملية مصافحة SSL؟

بمجرد الاتصال ب ASA، تحقق مما إذا كان سجل الوقت الفعلي يظهر اكتمال تأكيد اتصال SSL.

Severity	Date	Time	Syslog	Source IP	Destination IP	Description
2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3102 to 216.239.53.1
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1029 on i
2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172.22.1.203/3101 to 64.101.176.170/1029 on i
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1029 on i
2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3100 to 216.239.53.1
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.1
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.1
6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3097
6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previous sessi
6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3097 for TLSv
6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3711 for outside:172.22.1.203/3097 (172.2
6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.
6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP connection 3710 for outside:172.22.1.203/3096 to NP Id
6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3096
6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3096 for TLSv
6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3710 for outside:172.22.1.203/3096 (172.2
3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
3	Jun 27 2006	11:40:16	305005	171.68.222.149		No translation group found for udp src inside:10.2.2.4/1830 dst outside:
2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.1
2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.1

### هل يعمل SSL VPN Thin-Client؟

للتحقق من عمل SSL VPN Thin-Client، أكمل الخطوات التالية:

1. طقطقت **monitore**، وبعد ذلك طقطقت **VPN**.
2. مددت **VPN إحصاء**، وطقطقة جلسة. يجب أن تظهر جلسة عمل SSL VPN الخاصة بالعمل الدقيق في قائمة جلسات العمل. تأكد من التصفية بواسطة WebVPN كما هو موضح في هذه الصورة:

The screenshot shows the Cisco ASDM 5.2 for ASA - 10.2.2.1 interface. The main window is titled "Monitoring > VPN > VPN Statistics > Sessions". The left sidebar shows a tree view with "VPN" selected. The main content area displays a summary table for various VPN types and a detailed table for WebVPN sessions.

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	22

Filter By: WebVPN -- All Sessions -- Filter

Username	Group Policy	Protocol	Login Time
IP Address	Tunnel Group	Encryption	Duration
user1	NetAdmins	WebVPN	11:41:23 UTC Tue Jun 27 2006
172.22.1.203	DefaultWEBVPNGroup	3DES	0h:01m:06s

Logout Sessions Refresh

Last Updated: 6/27/06 2:13:00 PM

## الأوامر

تقترن العديد من أوامر تصحيح الأخطاء ب WebVPN. للحصول على معلومات تفصيلية حول هذه الأوامر، ارجع إلى [إستخدام أوامر تصحيح الأخطاء ل WebVPN](#).

ملاحظة: يمكن أن يؤثر إستخدام أوامر تصحيح الأخطاء سلبا على جهاز Cisco الخاص بك. قبل إستخدام أوامر debug، ارجع إلى [معلومات مهمة عن أوامر تصحيح الأخطاء](#).

## معلومات ذات صلة

- [ClientWithout SSL VPN \(WebVPN\) على مثال تكوين ASA](#)
- [SSL VPN Client \(SVC\) على ASA مع مثال تكوين ASDM](#)
- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [ASA مع WebVPN وتسجيل دخول أحادي باستخدام مثال تكوين ASDM و NTLMv1](#)
- [الدعم التقني والمستندات - Cisco Systems](#)



ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا