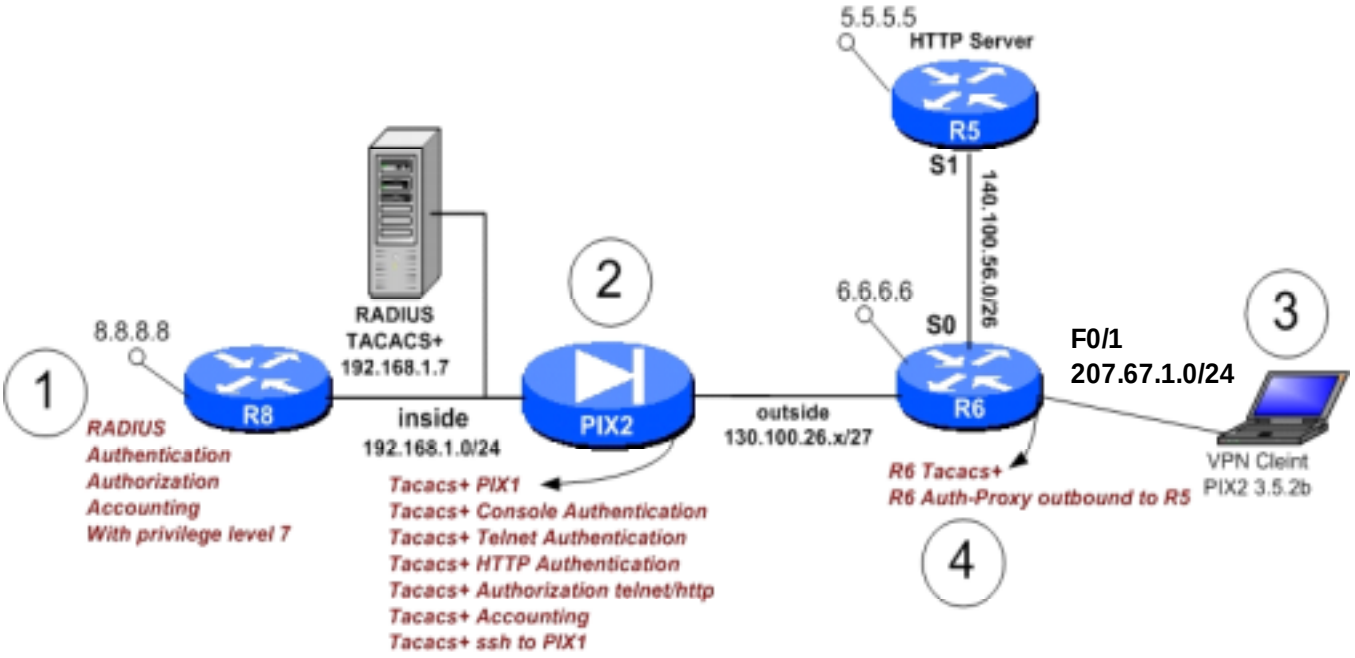
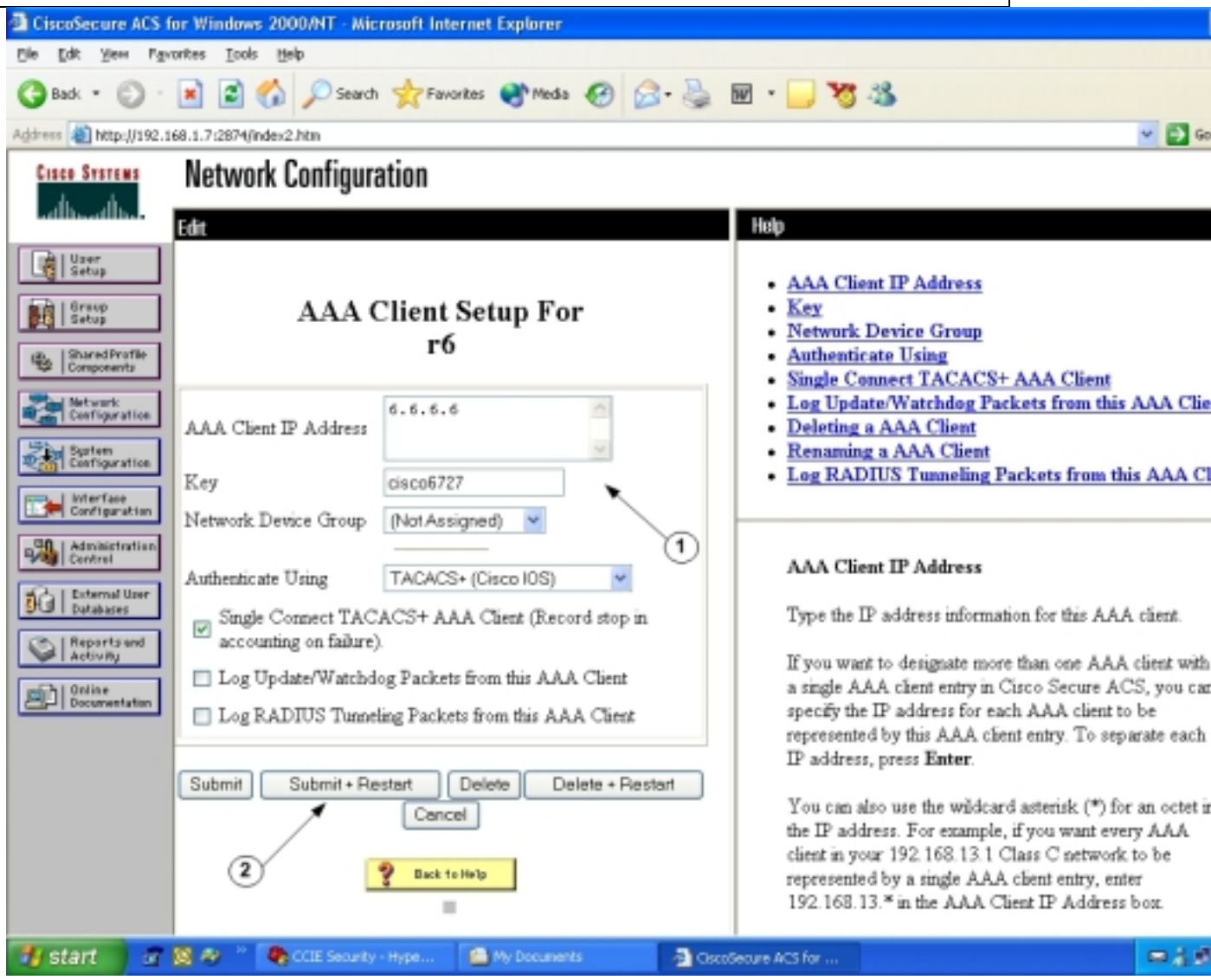
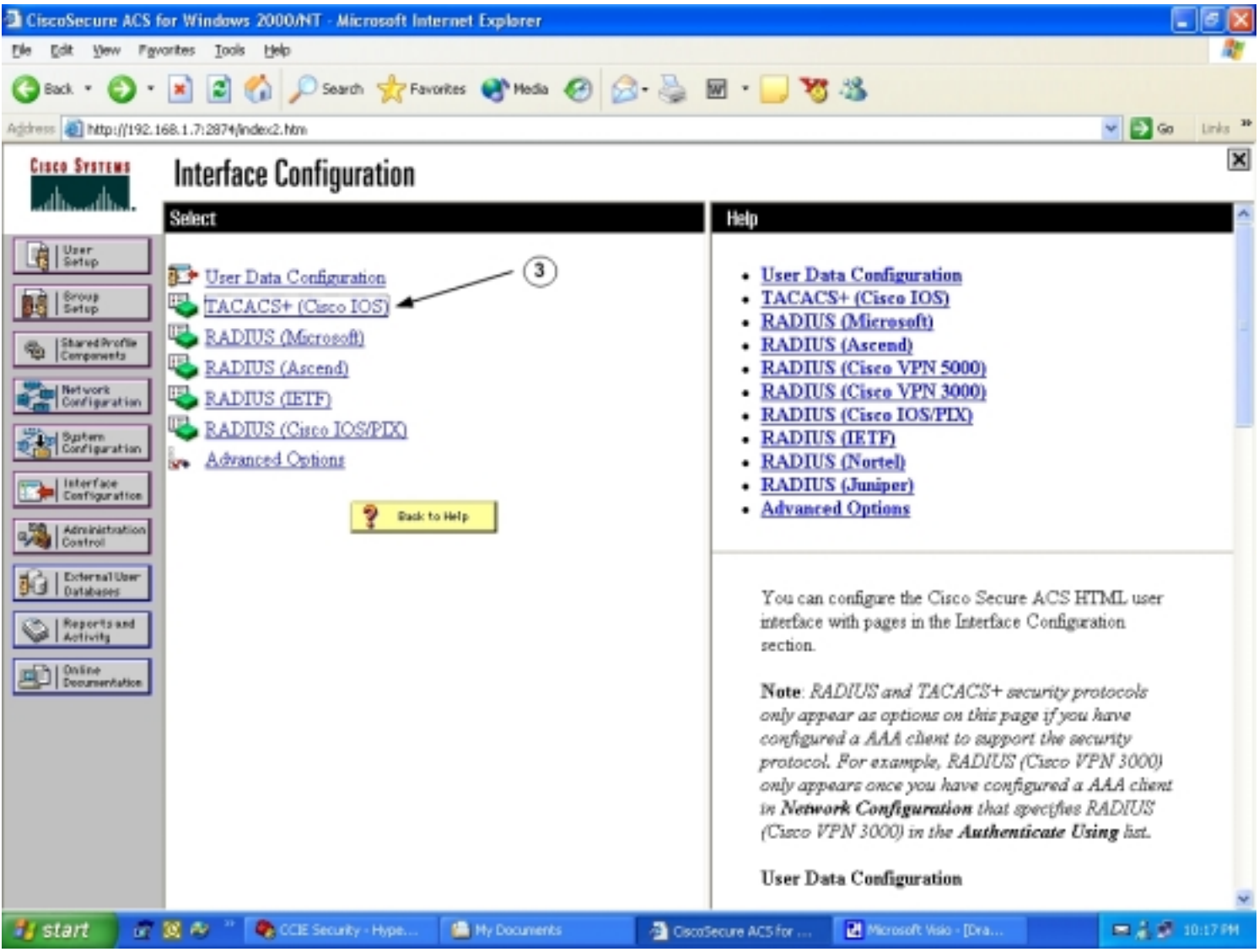


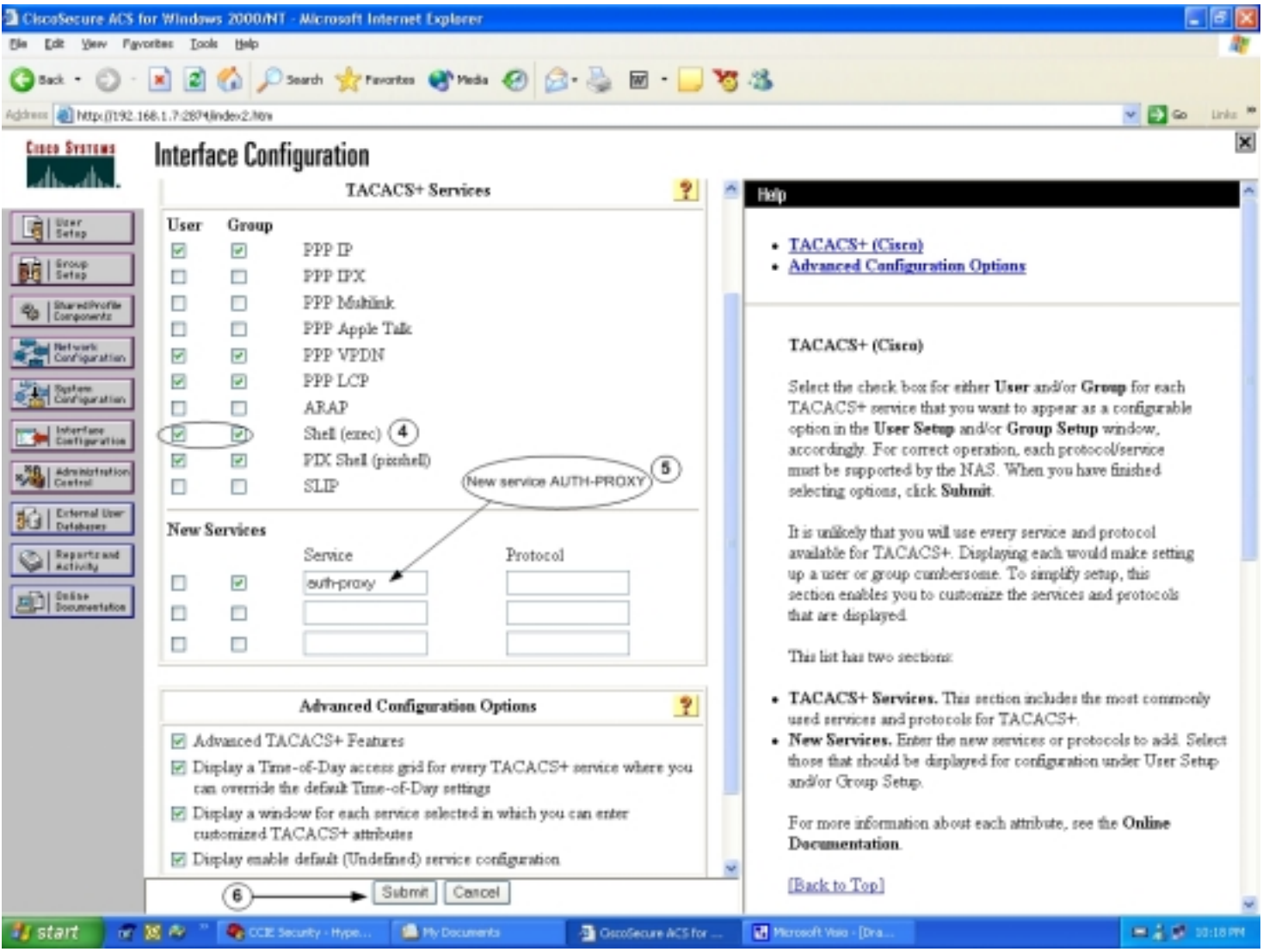
Figure 1 Section 5 Authentication Proxy with TACACS+

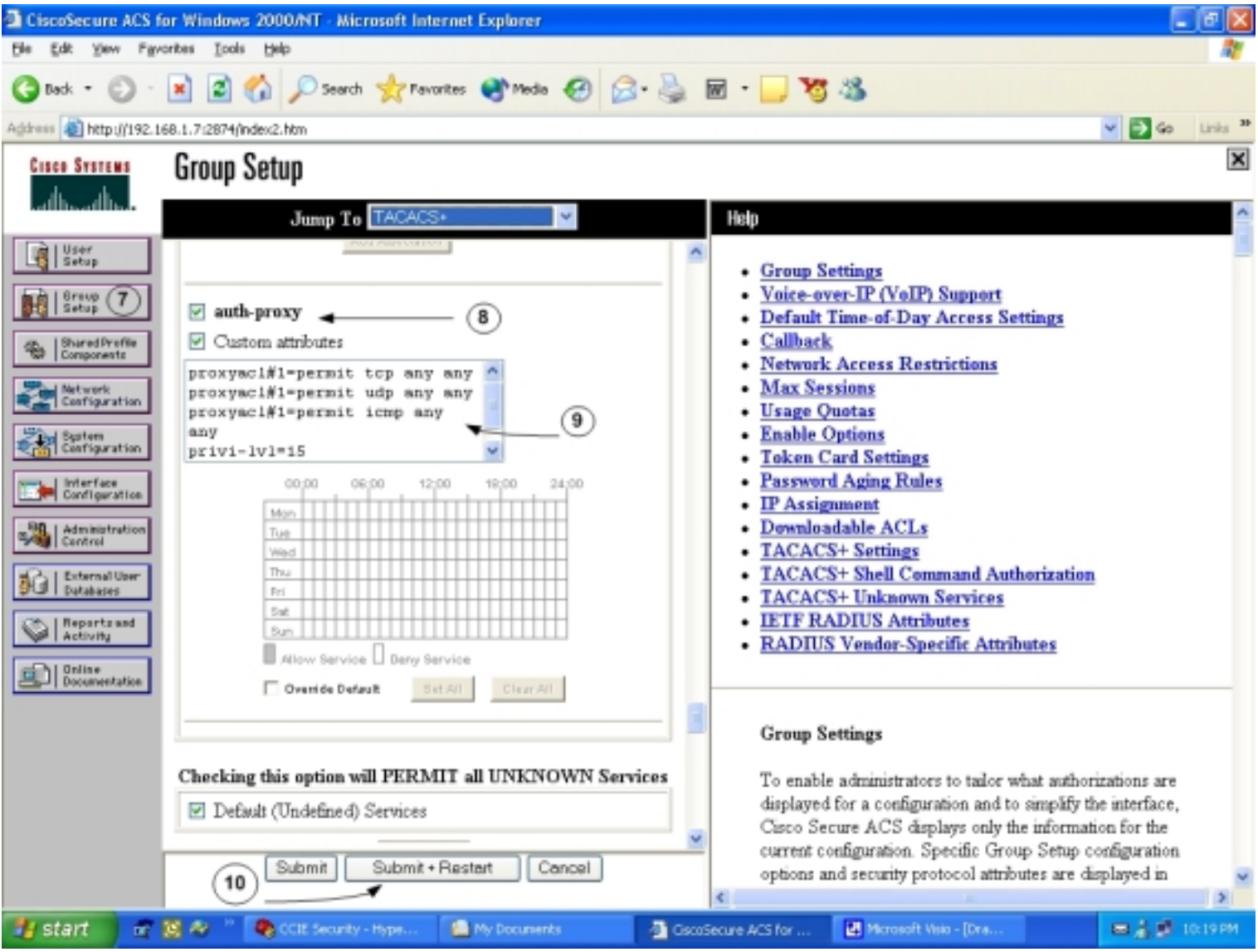
```
hostname RR6
!
aaa new-model
!
aaa authentication login default group tacacs+
aaa authentication login no_login enable local line none
aaa authentication enable default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa authorization configuration default group tacacs+
aaa accounting exec default start-stop group tacacs+
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
ip dhcp pool VPN_Client
   network 207.67.1.0 255.255.255.0
   default-router 207.67.1.1
!
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 5
ip auth-proxy name auth http
ip auth-proxy auth-proxy-audit
!
interface Loopback6
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/0
 ip address 130.100.26.6 255.255.255.224
 ip auth-proxy auth
!
```

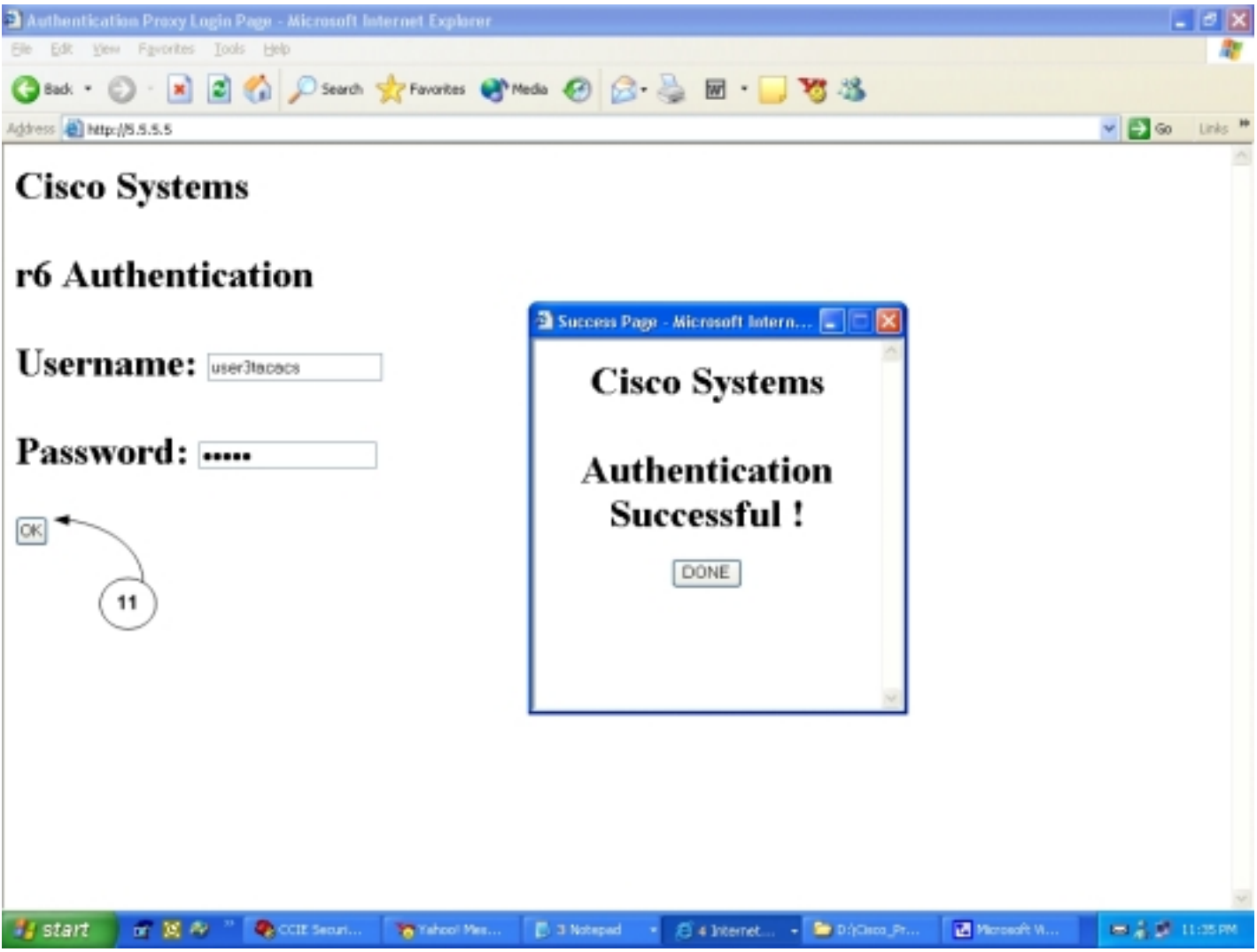
```
interface Serial0/0
 ip address 140.100.56.6 255.255.255.192
 ip ospf network point-to-point
!
interface FastEthernet0/1
 ip address 207.67.1.1 255.255.255.0
 ip auth-proxy auth
!

ip classless
ip tacacs source-interface Loopback6

ip http server
ip http authentication aaa
!
tacacs-server host 130.100.26.7 key cisco6727
tacacs-server key cisco6727


!
R6#
```




CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:2874/index2.htm
Go Links
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Select
User Data Configuration
TACACS+ (Cisco IOS)
RADIUS (Microsoft)
RADIUS (Ascend)
RADIUS (IETF)
RADIUS (Cisco IOS/PIX)
Advanced Options
3
Back to Help
Help
User Data Configuration
TACACS+ (Cisco IOS)
RADIUS (Microsoft)
RADIUS (Ascend)
RADIUS (Cisco VPN 5000)
RADIUS (Cisco VPN 3000)
RADIUS (Cisco IOS/PIX)
RADIUS (IETF)
RADIUS (Nortel)
RADIUS (Juniper)
Advanced Options
You can configure the Cisco Secure ACS HTML user interface with pages in the Interface Configuration section.
Note: RADIUS and TACACS+ security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000) in the Authenticate Using list.
User Data Configuration
start
CCIE Security - Hype...
My Documents
CiscoSecure ACS for ...
Microsoft Visio - [Dra...
10:17 PM


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
Interface Configuration
TACACS+ Services
User
Group
PPP IP
PPP IPX
PPP Multilink
PPP Apple Talk
PPP VPDN
PPP LCP
ARAP
Shell (exec)
PIX Shell (pixshell)
SLIP
New service AUTH-PROXY
New Services
Service
Protocol
auth-proxy
Advanced Configuration Options
Advanced TACACS+ Features
Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings
Display a window for each service selected in which you can enter customized TACACS+ attributes
Display enable default (Undefined) service configuration
Submit
Cancel
Help
TACACS+ (Cisco)
Advanced Configuration Options
TACACS+ (Cisco)
Select the check box for either User and/or Group for each TACACS+ service that you want to appear as a configurable option in the User Setup and/or Group Setup window, accordingly. For correct operation, each protocol/service must be supported by the NAS. When you have finished selecting options, click Submit.
It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, this section enables you to customize the services and protocols that are displayed.
This list has two sections:
TACACS+ Services. This section includes the most commonly used services and protocols for TACACS+.
New Services. Enter the new services or protocols to add. Select those that should be displayed for configuration under User Setup and/or Group Setup.
For more information about each attribute, see the Online Documentation.
[Back to Top]


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.7:2874/index2.htm
Cisco Systems
Group Setup
Jump To TACACS+
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
7
auth-proxy
8
Custom attributes
proxyacl#1=permit tcp any any
proxyacl#1=permit udp any any
proxyacl#1=permit icmp any
any
privi-lvl=15
9
00:00 06:00 12:00 18:00 24:00
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Allow Service
Deny Service
Override Default
Set All
Clear All
Checking this option will PERMIT all UNKNOWN Services
Default (Undefined) Services
10
Submit
Submit + Restart
Cancel
Help
Group Settings
Voice-over-IP (VoIP) Support
Default Time-of-Day Access Settings
Callback
Network Access Restrictions
Max Sessions
Usage Quotas
Enable Options
Token Card Settings
Password Aging Rules
IP Assignment
Downloadable ACLs
TACACS+ Settings
TACACS+ Shell Command Authorization
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Group Settings
To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Cisco Secure ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in
start
CCIE Security - Hype...
My Documents
CiscoSecure ACS for ...
Microsoft Visio - [Dra...
10:19 PM



To verify Auth-Proxy enable the HTTP server on R5

```
hostname R5
!
ip http server
ip http authentication local
```

Successful Debug

```
R6#show debugging
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

HTTP:
  HTTP transactions debugging is on
  HTTP EZSetup debugging is on
  HTTP URL debugging is on
  HTTP Authentication debugging is on
  HTTP Server Side Includes debugging is on
```

```
Feb 28 16:37:32: %SEC-6-IPACCESSLOGS: list 10 permitted
130.100.26.2 1 packet
Feb 28 16:37:59: timetag 392144
Feb 28 16:37:59: uname user3tacacs
```

```
Feb 28 16:37:59: HTTP: Authentication for url '/' '/' level
15  privless '/'
Feb 28 16:37:59: HTTP: Authentication proxy_username =
'user3tacacs' priv-level = 15 auth-type = aaa
Feb 28 16:37:59: AAA: parse name=FastEthernet0/0 idb type=-1
tty=-1
Feb 28 16:37:59: AAA: name=FastEthernet0/0 flags=0x15
type=12 shelf=0 slot=0 adapter=0 port=0 channel=0
Feb 28 16:37:59: AAA: parse name=<no string> idb type=-1
tty=-1
Feb 28 16:37:59: AAA/MEMORY: create_user (0x830BD600)
user='NULL' ruser='NULL' ds0=0 port='FastEthernet0/0
' rem_addr='130.100.26.2' authen_type=ASCII service=LOGIN
priv=0 initial_task_id='0'
Feb 28 16:37:59: AAA/AUTHEN/START (2185388406):
port='FastEthernet0/0' list='default' action=LOGIN service
=LOGIN
Feb 28 16:37:59: AAA/AUTHEN/START (2185388406): found list
default
Feb 28 16:37:59: AAA/AUTHEN/START (2185388406):
Method=tacacs+ (tacacs+)
Feb 28 16:37:59: TAC+: send AUTHEN/START packet ver=192
id=2185388406
Feb 28 16:37:59: TAC+: ver=192 id=2185388406 received AUTHEN
status = GETUSER
Feb 28 16:37:59: AAA/AUTHEN(2185388406): Status=GETUSER
Feb 28 16:37:59: AAA/AUTHEN/CONT (2185388406):
continue_login (user='(undef)')
Feb 28 16:37:59: AAA/AUTHEN(2185388406): Status=GETUSER
Feb 28 16:37:59: AAA/AUTHEN(2185388406): Method=tacacs+
(tacacs+)
Feb 28 16:37:59: TAC+: send AUTHEN/CONT packet id=2185388406
Feb 28 16:38:00: TAC+: ver=192 id=2185388406 received AUTHEN
status = GETPASS
Feb 28 16:38:00: AAA/AUTHEN(2185388406): Status=GETPASS
Feb 28 16:38:00: AAA/AUTHEN/CONT (2185388406):
continue_login (user='user3tacacs')
Feb 28 16:38:00: AAA/AUTHEN(2185388406): Status=GETPASS
Feb 28 16:38:00: AAA/AUTHEN(2185388406): Method=tacacs+
(tacacs+)
Feb 28 16:38:00: TAC+: send AUTHEN/CONT packet id=2185388406
Feb 28 16:38:00: TAC+: ver=192 id=2185388406 received AUTHEN
status = PASS
Feb 28 16:38:00: AAA/AUTHEN(2185388406): Status=PASS
Feb 28 16:38:00: FastEthernet0/0
AAA/AUTHOR/HTTP(3715440567): Port='FastEthernet0/0'
list='default' servic
e=AUTH-PROXY
Feb 28 16:38:00: AAA/AUTHOR/HTTP:
FastEthernet0/0(3715440567) user='user3tacacs'
Feb 28 16:38:00: FastEthernet0/0
AAA/AUTHOR/HTTP(3715440567): send AV service=auth-proxy
Feb 28 16:38:00: FastEthernet0/0
AAA/AUTHOR/HTTP(3715440567): send AV cmd*
Feb 28 16:38:00: FastEthernet0/0
AAA/AUTHOR/HTTP(3715440567): found list "default"
Feb 28 16:38:00: FastEthernet0/0
AAA/AUTHOR/HTTP(3715440567): Method=tacacs+ (tacacs+)
```

```
Feb 28 16:38:00: AAA/AUTHOR/TAC+: (3715440567):
user=user3tacacs
Feb 28 16:38:00: AAA/AUTHOR/TAC+: (3715440567): send AV
service=auth-proxy
Feb 28 16:38:00: AAA/AUTHOR/TAC+: (3715440567): send AV cmd*
Feb 28 16:38:00: TAC+: (3715440567): received author
response status = PASS_ADD
Feb 28 16:38:00: AAA/AUTHOR (3715440567): Post authorization
status = PASS_ADD

R6#
Feb 28 17:34:57: AAA/MEMORY: free_user (0x830C092C)
user='user3tacacs' ruser='NULL' port='FastEthernet0/0'
 rem_addr='130.100.26.2' authen_type=ASCII service=LOGIN
priv=0
Feb 28 17:35:15: AAA/AUTHOR (00000000): Method list
id=FFFFFFFF not configured. Skip author
Feb 28 17:35:15: AAA/AUTHOR/CONFIG: 'aaa author
configuration' not set. Download abort.
Feb 28 17:35:39: HTTP: parsed uri '/'
Feb 28 17:35:39: HTTP: processing URL '/' from host
130.100.26.2
Feb 28 17:35:39: HTTP: client version 1.1
Feb 28 17:35:39: HTTP: parsed extension Accept
Feb 28 17:35:39: HTTP: parsed extension Accept-Language
Feb 28 17:35:39: HTTP: parsed extension Accept-Encoding
Feb 28 17:35:39: HTTP: parsed extension User-Agent
Feb 28 17:35:39: HTTP: parsed extension Host
Feb 28 17:35:39: HTTP: parsed extension Connection
Feb 28 17:35:39: HTTP: parsed extension Authorization
Feb 28 17:35:39: HTTP: parsed authorization type Basic
Feb 28 17:36:08: HTTP: parsed uri '/'
Feb 28 17:36:08: HTTP: processing URL '/' from host
130.100.26.2
Feb 28 17:36:08: HTTP: client version 1.1
Feb 28 17:36:08: HTTP: parsed extension Accept
Feb 28 17:36:08: HTTP: parsed extension Referer
Feb 28 17:36:08: HTTP: parsed extension Accept-Language
Feb 28 17:36:08: HTTP: parsed extension Content-Type
Feb 28 17:36:08: HTTP: parsed extension Accept-Encoding
Feb 28 17:36:08: HTTP: parsed extension User-Agent
Feb 28 17:36:08: HTTP: parsed extension Host
Feb 28 17:36:08: HTTP: parsed extension Content-Length
Feb 28 17:36:08: HTTP: Content-length 55
Feb 28 17:36:08: HTTP: parsed extension Connection
Feb 28 17:36:08: HTTP: parsed extension Cache-Control
Feb 28 17:36:08: HTTP: parsed extension Authorization
Feb 28 17:36:08: HTTP: parsed authorization type Basic
Feb 28 17:36:08: HTTP: received POST '/' 4
Feb 28 17:36:08: HTTP: parsed variable 'au_pxytimetag'
Feb 28 17:36:08: HTTP: parsed value '1527380'
Feb 28 17:36:08: timetag 1527380
Feb 28 17:36:08: HTTP: parsed variable 'uname'
Feb 28 17:36:08: HTTP: parsed value 'user3tacacs'
Feb 28 17:36:08: uname user3tacacs
Feb 28 17:36:08: HTTP: parsed variable 'pwd'
Feb 28 17:36:08: HTTP: parsed value 'cisco'
Feb 28 17:36:08: HTTP: parsed variable 'ok'
```

```
Feb 28 17:36:08: HTTP: proxy done with post parsing
Feb 28 17:36:08: HTTP: Authentication for url '/' '/' level
15  privless '/'
Feb 28 17:36:08: HTTP: Authentication proxy_username =
'user3tacacs' priv-level = 15 auth-type = aaa
Feb 28 17:36:08: AAA: parse name=FastEthernet0/0 idb type=-1
tty=-1
Feb 28 17:36:08: AAA: name=FastEthernet0/0 flags=0x15
type=12 shelf=0 slot=0 adapter=0 port=0 channel=0
Feb 28 17:36:08: AAA: parse name=<no string> idb type=-1
tty=-1
Feb 28 17:36:08: AAA/MEMORY: create_user (0x830BE494)
user='NULL' ruser='NULL' ds0=0 port='FastEthernet0/0
' rem_addr='130.100.26.2' authen_type=ASCII service=LOGIN
priv=0 initial_task_id='0'
Feb 28 17:36:08: AAA/AUTHEN/START (3090194579):
port='FastEthernet0/0' list='default' action=LOGIN service
=LOGIN
Feb 28 17:36:08: AAA/AUTHEN/START (3090194579): found list
default
Feb 28 17:36:08: AAA/AUTHEN/START (3090194579):
Method=tacacs+ (tacacs+)
Feb 28 17:36:08: TAC+: send AUTHEN/START packet ver=192
id=3090194579
Feb 28 17:36:08: TAC+: ver=192 id=3090194579 received AUTHEN
status = GETUSER
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Status=GETUSER
Feb 28 17:36:08: AAA/AUTHEN/CONT (3090194579):
continue_login (user='(undef)')
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Status=GETUSER
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Method=tacacs+
(tacacs+)
Feb 28 17:36:08: TAC+: send AUTHEN/CONT packet id=3090194579
Feb 28 17:36:08: TAC+: ver=192 id=3090194579 received AUTHEN
status = GETPASS
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Status=GETPASS
Feb 28 17:36:08: AAA/AUTHEN/CONT (3090194579):
continue_login (user='user3tacacs')
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Status=GETPASS
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Method=tacacs+
(tacacs+)
Feb 28 17:36:08: TAC+: send AUTHEN/CONT packet id=3090194579
Feb 28 17:36:08: TAC+: ver=192 id=3090194579 received AUTHEN
status = PASS
Feb 28 17:36:08: AAA/AUTHEN(3090194579): Status=PASS
Feb 28 17:36:08: FastEthernet0/0
AAA/AUTHOR/HTTP(4207271648): Port='FastEthernet0/0'
list='default' servic
e=AUTH-PROXY
Feb 28 17:36:08: AAA/AUTHOR/HTTP:
FastEthernet0/0(4207271648) user='user3tacacs'
Feb 28 17:36:08: FastEthernet0/0
AAA/AUTHOR/HTTP(4207271648): send AV service=auth-proxy
Feb 28 17:36:08: FastEthernet0/0
AAA/AUTHOR/HTTP(4207271648): send AV cmd*
Feb 28 17:36:08: FastEthernet0/0
AAA/AUTHOR/HTTP(4207271648): found list "default"
```

```
Feb 28 17:36:08: FastEthernet0/0
AAA/AUTHOR/HTTP(4207271648): Method=tacacs+ (tacacs+)
Feb 28 17:36:08: AAA/AUTHOR/TAC+: (4207271648):
user=user3tacacs
Feb 28 17:36:08: AAA/AUTHOR/TAC+: (4207271648): send AV
service=auth-proxy
Feb 28 17:36:08: AAA/AUTHOR/TAC+: (4207271648): send AV cmd*
Feb 28 17:36:09: TAC+: (4207271648): received author
response status = PASS_ADD
Feb 28 17:36:09: AAA/AUTHOR (4207271648): Post authorization
status = PASS_ADD

Feb 28 16:52:07: %SYS-5-CONFIG_I: Configured from console by
console
Feb 28 16:52:14: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:14: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:29: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:29: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:29: AUTH-PROXY FUNC:
auth_proxy_if_marked_for_proxy
Feb 28 16:52:29: AUTH-PROXY FUNC: auth_proxy_get_idbsb
Feb 28 16:52:29: AUTH-PROXY FUNC:
auth_proxy_find_aprt_of_aprc_by_protocol
Feb 28 16:52:29: ip_old_accesscheck status = 0
Feb 28 16:52:29: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:29: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:29: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:29: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:30: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:30: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:30: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:30: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:30: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:30: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0
```

```
Feb 28 16:52:30: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:30: AUTH-PROXY auth_proxy_find_conn_info :
         find srcaddr - 130.100.26.2, dstaddr - 5.5.5.5
                 ip-srcaddr 130.100.26.2
                 pak-srcaddr 0.0.0.0

Feb 28 16:52:39: AUTH-PROXY FUNC: auth_proxy_fast_path
Feb 28 16:52:39: AUTH-PROXY FUNC: auth_proxy_fast_path


R6#show ip auth-proxy cache
Authentication Proxy Cache
 Client IP 130.100.26.2 Port 1065, timeout 5, state
HTTP_ESTAB
```