

عەدراوەلە ئەقداصلالىك و ئەقداصلە ACS و IPSec و VPN

تايىوتەملا

قەمدەملا

[قىسالا تابلەتەملا](#)

[تابلەتەملا](#)

[قەمدەختەسەملا تانوكەملا](#)

[تاجالەتصالا](#)

[نىوكەتلە](#)

[كېشىللە طەختەلە مەسىرلە](#)

[نىوكەتلە](#)

[نىوكەت VPN Client 4.8](#)

[Cisco نەممەلە ACS مادەختەسەپ TACACS+ مەداخ نىوكەت](#)

[قىطايىتحالاخسەنلە ۋەزىم نىوكەت](#)

[قەھىچەلە نەممە قەھىچەلە](#)

[اھالىص او عاطخالا فاشكەتسە](#)

[قەلصىتاذتامولۇم](#)

قەمدەملا

لۇصۇلوا وأ كېشىللە لۇخدەلە لېجىست ئىنالىم نىيمەختەسەملىل ئەقداصلالىك و ۋەزىم حىيتت اھقىبەت و مەبۇھە ئەصاللە لۇصۇلوا فيرىعت تافلم دادرتىسىم، HTTP، رېبۇت تەنرتىنالا ئىلە يف الە ئەطشىن مەختەسەملىا فيرىعت تافلم نوكتىلە TACACS+ و RADIUS. مەداخ نەممە ئاقلىت مەھىلە ئەقداصلالى نىيمەختەسەملىا نەممە ئەطشىن رورم ئەكەر دەچىرەتلىك.

10.17.17.17. ئىلە ھفادەتسا او 10.1.1.1 لىلع بىولە ضرۇتسەم ضرۇل نىوكەتلە اذە مىمىصىت مەت ئىلە لۇصۇللى 10.31.1.111 قىفنىلا ئىيەن ئەطقن لالخ نەممە لاقتنالل VPN لىمع نىوكەتلە ارظننى عەمجەت نەممە IP ناونۇع ئىلە رەت و يېبمكەلە لىصەحىي و IPSec قىفنى عاشىنە مەتى 10.17.17.x. 10.17.17.17. ئەطسەوب ئەقداصلالى بىلەت كەلذ دەعب مەتى. (عەضۇلە نىوكەت ذىفەنت مەتى ھەنأرەن POOL) مەداخ ئىلە انزەخم رورم ئەملەك و مەختەسەم مەسە مەختەسەملىا لەخدى نأ دەعب Cisco 3640. ۋەزىمە ئاق ئىلە مەداخلە نەممە اھرىرمەت مەت يەتلىلە لۇصۇلە ئەقىقە ئەفاضى مەتى، 10.14.14.3. يف TACACS+ 118. لۇصۇلە

قىسالا تابلەتەملا

تابلەتەملا

ئەيلاتلى تابلەتەملا ئەفەيىتسا نەممە دەكتىر، نىوكەتلە اذە ئەلواجم لېبىق:

- Cisco 3640. لۇصەن ئەل IPSec مادەختەسەپ قىفنى عاشىنەل Cisco VPN لىمع نىوكەت مەت
- "ئەلصىلا تاذتامولۇم" مەسىقى عەجار. ئەقداصلالى لېكۈلە TACACS+ مەداخ نىوكەت مەت تامولۇملا نەممە دېزم ئىلە

ةمدى تانوكمل

ةييلاتلا ئي داملا تانوكمل او جماربلا تارادصا ئىلإ دنتسملا اذه يف ئي داملا تامولعملاب دنتس.

- رادصا جمانربلا Cisco IOS؟ ماظن 12.4
 - Cisco 3640
 - يأ لمعي نأ بجي) 4.8 رادصا لىغشتلا ماظن Cisco VPN نم ئكبش ليمع (ثدحألا تارادصا او 4.x رادصا VPN ئكبشلي مع
- مت. T. 12.0.5.T. رادصا Cisco IOS Software، ip auth-proxy رمألا لاخدا مت: ئظحالم Cisco IOS، جمانربلا يف 12.4. رادصا جمانرب مادختساب نيوكتل اذه رابتخا.

ةصاخ ئي لمع ئي ب يف ئدوجوملا ئزهجألا نم دنتسملا اذه يف ئي داملا تامولعملاب عاشن ا مت تناك اذا. (يضاارتفا) حوسمم نيوكتب دنتسملا اذه يف ئمدى تانوكمل ئزهجألا عيمج تأدبل رمأ يأ لىمتحمل ريا ثأتلل كمهف نم دكأتاف، ئوشابم كتكمب بش.

تاجالطصا

[تاجيملت تاجالطصا](#) ئىلإ عجرا، تادنتسملا تاجالطصا لوح تامولعملاب ديزم ىلع لوصح لـ Cisco.

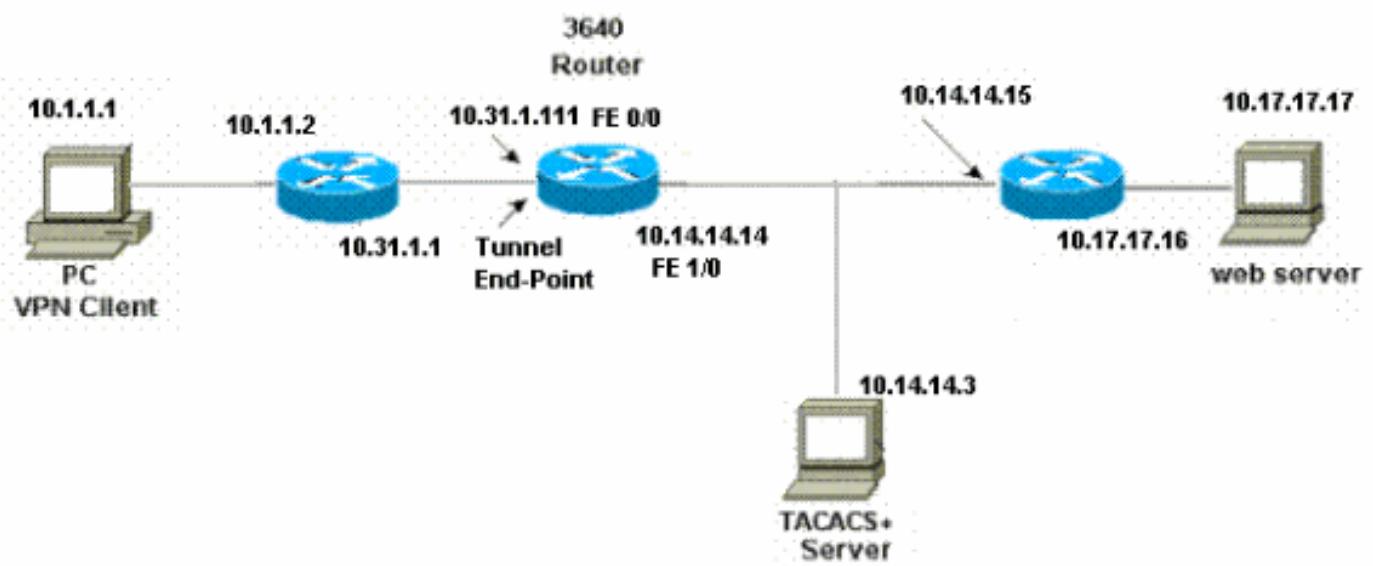
نيوكتل

دنتسملا اذه يف ئحضوملا تازيملا نيوكت تامولعم كل مدقق، مسقل اذه يف.

قادأ مديتسا، دنتسملا اذه يف ئمدى تانوكمل رمألا لوح ئيفاضا تامولعم ىلع روشعلل: ئظحالم (طقف نيوجسمل ئالمعلل) رمألا ثحب.

ئكبشلل يطيطرختلارا مسرا

ييلاتلا ئكبشلا دادعإ دنتسملا اذه مديتسى:



نيوكتل

چوہ 3640

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass
!--- Enable AAA. aaa new-model

!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
  server 10.14.14.3
!

!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode

aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHC$R/07uQ44E2JgVuCsOUWdG1
enable password ww
!
ip subnet-zero
!
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
^C
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
!--- Define ISAKMP policy. crypto isakmp policy 10
hash md5
authentication pre-share
group 2

!--- These commands define the group policy that !--- is
enforced for the users in the group RTPUSERS. !--- This
group name and the key should match what !--- is
configured on the VPN Client. The users from this !--- 
group are assigned IP addresses from the pool RTP-POOL.
crypto isakmp client configuration group RTPUSERS
key cisco123
pool RTP-POOL
!
!--- Define IPSec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
```

```

!
crypto dynamic-map RTP-DYNAMIC 10
  set transform-set RTP-TRANSFORM
!
!-- Define extended authentication (X-Auth) using the
local database. !-- This is to authenticate the users
before they can !-- use the IPSec tunnel to access the
resources. crypto map RTPCLIENT client authentication
list userauth

!-- Define authorization using the local database. !--
This is required to push the 'mode configurations' to
the VPN Client. crypto map RTPCLIENT isakmp
authorization list groupauth
crypto map RTPCLIENT client configuration address
initiate
crypto map RTPCLIENT client configuration address
respond
crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC
!
interface FastEthernet0/0
  ip address 10.31.1.111 255.255.255.0
  ip access-group 118 in
  no ip directed-broadcast

!-- Apply the authentication-proxy rule to the
interface. ip auth-proxy list_a
no ip route-cache
no ip mroute-cache
speed auto
half-duplex

!-- Apply the crypto-map to the interface. crypto map
RTPCLIENT
!
interface FastEthernet1/0
  ip address 10.14.14.14 255.255.255.0
  no ip directed-broadcast
  speed auto
  half-duplex
!
!-- Define the range of addresses in the pool. !-- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1

!-- Turn on the HTTP server and authentication. !--
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!-- The access-list 118 permits ISAKMP and IPSec
packets !-- to enable the Cisco VPN Client to establish
the IPSec tunnel. !-- The last line of the access-list
118 permits communication !-- between the TACACS+
server and the 3640 router to enable !-- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host

```

```

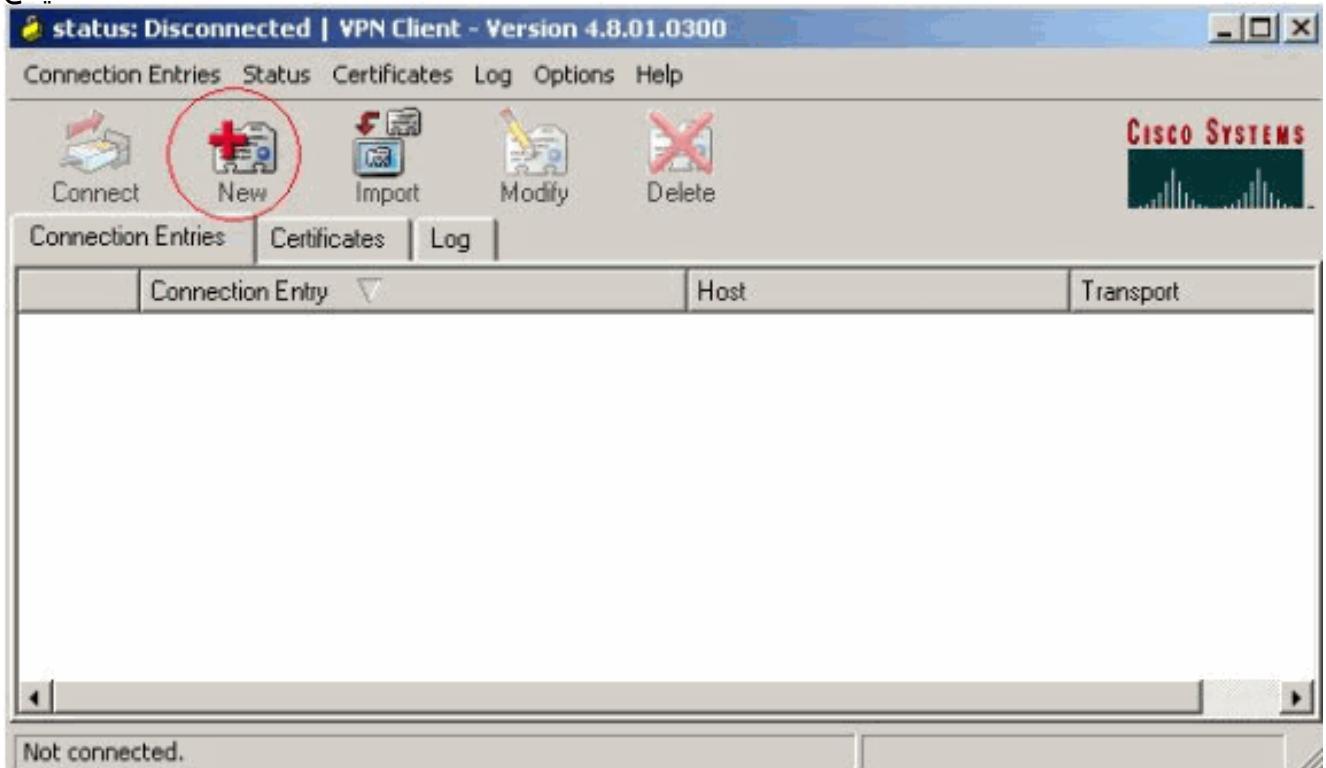
10.31.1.111
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
!
end

```

نويوكت VPN Client 4.8

نوبز VPN ل تلکش اذه تمتأ steps in order to 4.8:

1. نوبز > Cisco Systems VPN > جمانرب > ئادي ادب ترڅخا.
2. لاصتا ئاشندا "راطإلا لېغشتل دېدج ىلع رقنا دېدج".

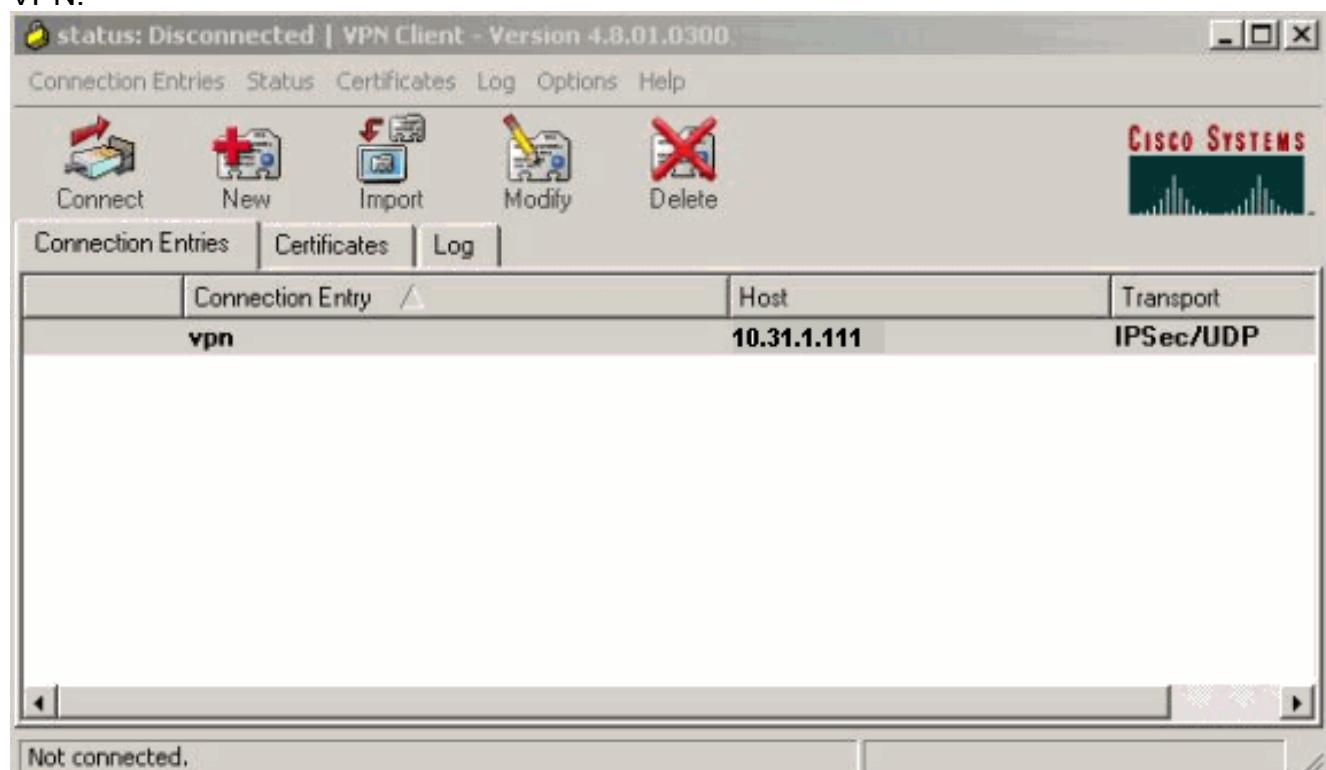


3. فيضملا عبزملا يف هجوملل يجراخلا IP ناونع لخدأ. فصو عم "لاصتا لاخدا" مسا لخدأ. ىلع رقنا او، رورملا ۋەملەك و VPN ۋەممەج مسا لخدأ مث



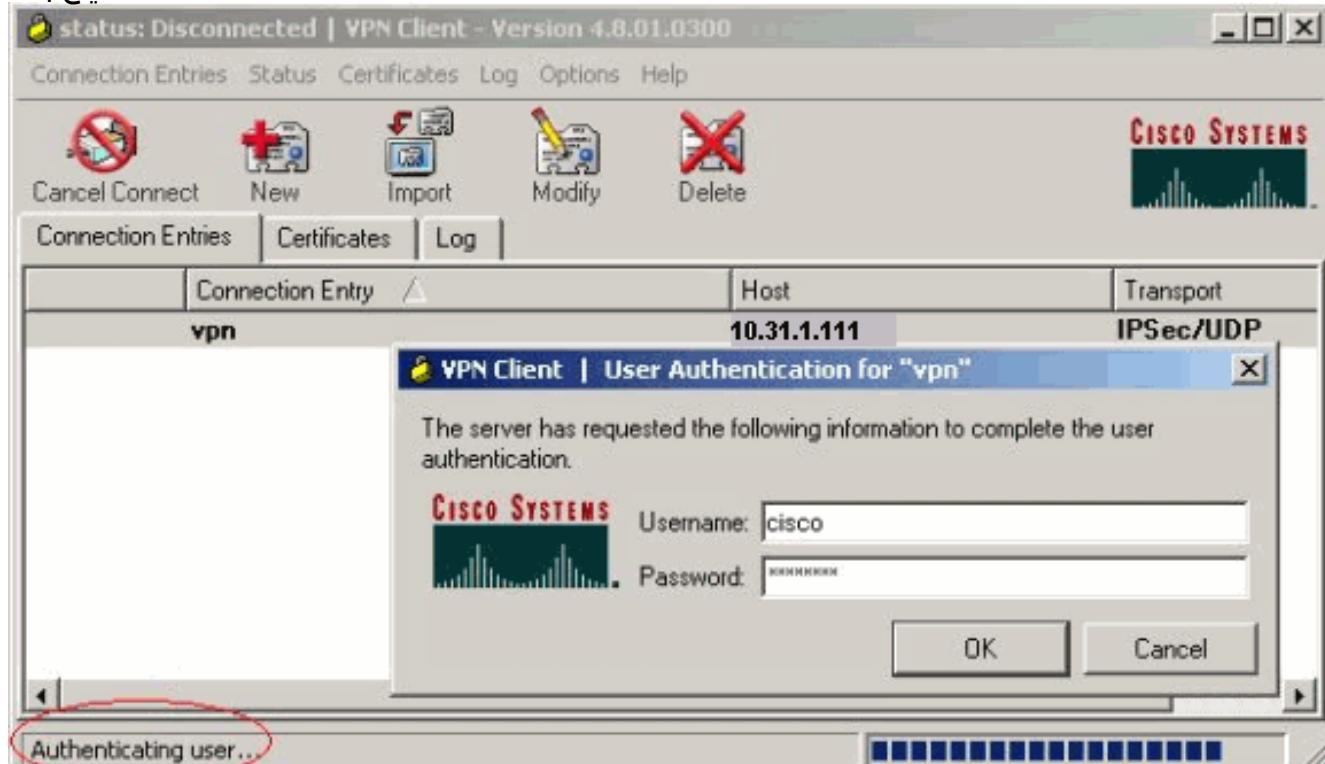
طفح.

4. يسیئرلا راطإلا نم لاصتالا قوف رقناو همادختسا ديرت يذلا لاصتالا ىلع رقنا
ةكبش لميعل VPN.

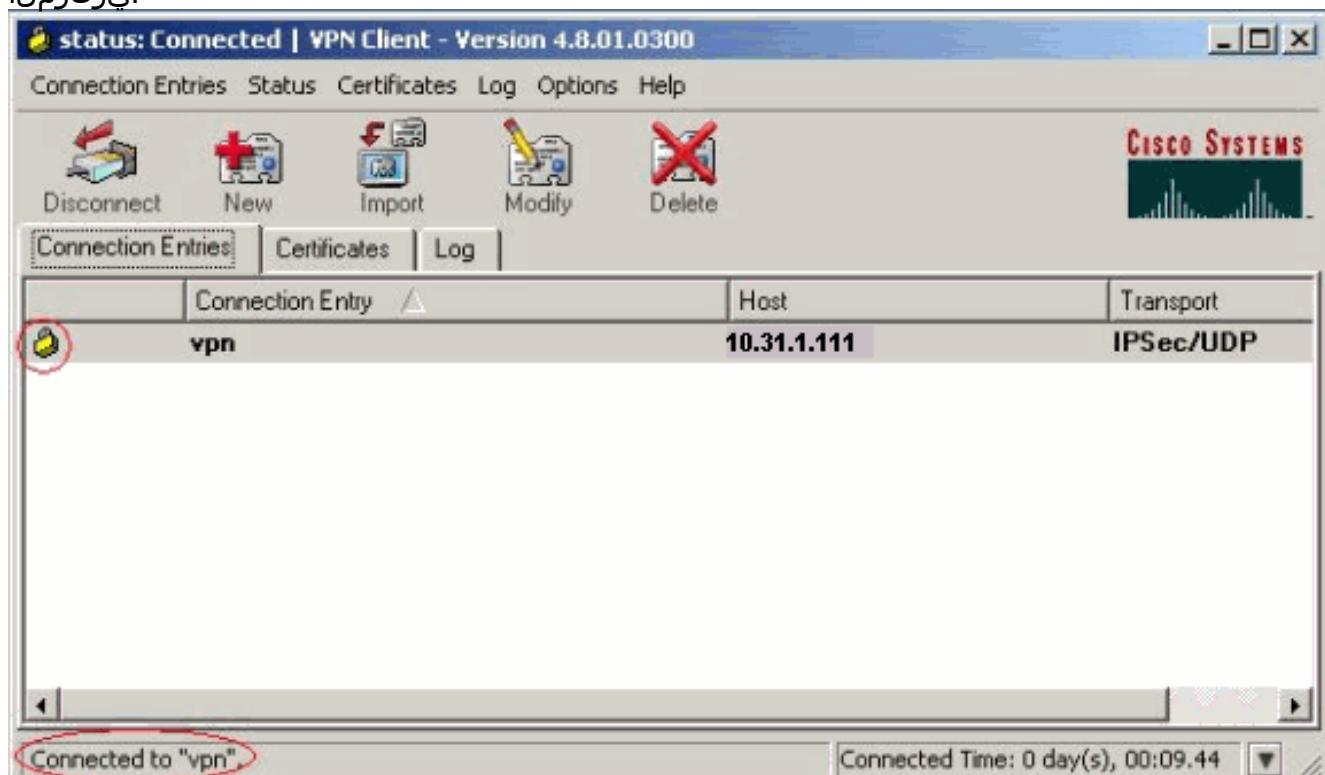


5. قف اوم قوف رقناو لاسرالل رورمل ا ةملکو مدخلتسمل ا مسا تامولعم لخدا ،ةبلاطمل ا دنع
ةكبش لاب لاصتالل

لاب عدي.



عقوملا يف هجوملاب VPN ڈڪ بش لي مع لاصتا متي
يزكرملما



ن姆 نمآلا ACS مادختس اب TACACS+ Cisco

ن姆 أي يف تسلکش TACACS+ cisco نم مأي اذه تم تأ

ن姆 ققحتل Cisco نم نمآلا يف اضالا وتحمل ردم عقوم ديدحتل هجوملا نيوكت بجي.

لاثمل ا ليبس ىلع مدختسملا دامتع ا تان اي:

3640(config)#

[aaa group server tacacs+ RTP](#)

```
3640(config)#
tacacs-server host 10.14.14.3 key cisco
```

2. جاحس ملل لخدم فيضي نأLuxم فيضي نقطق طوراسيلا لىع ليكشت ةكبش ترتبخأ. نيوكتل اقفو مدخلاتان اي بةداعاق رتبا. تايطعم ءداعاق لدان لىا اما يف ديدخت جوبل.

The screenshot shows the Cisco Network Configuration interface. On the left, there is a sidebar with various configuration options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled "Network Configuration" and "Select". Below this is a table titled "AAA Clients" with the following data:

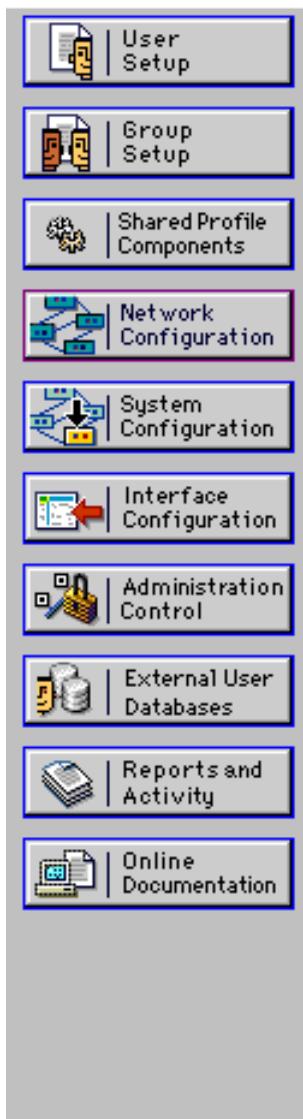
AAA Client Hostname	AAA Client IP Address	Authenticate Using
3640	10.14.14.14	TACACS+ (Cisco IOS)
PIX-A	172.16.1.85	RADIUS (Cisco IOS/PDG)
VPN3000	172.16.5.2	TACACS+ (Cisco IOS)
WLC	172.16.1.31	RADIUS (Cisco Aironet)
WLC Main	172.16.1.50	RADIUS (Cisco Aironet)

At the bottom of the table are "Add Entry" and "Search" buttons.

3. تنك اذا Cisco نم نمآل ACS مداخو 3640 هجوملا نيب ئقادصملل حاتفمل امادختسا مت يف TACACS+ (Cisco IOS) رتبا، ئقادصملل TACACS+ لوكوتورب ديدحت يف بغرت ئمئاقلا مادختساب ئقادصمل ا ئمئاق ئلدس نمل.

Network Configuration

Edit



Add AAA Client

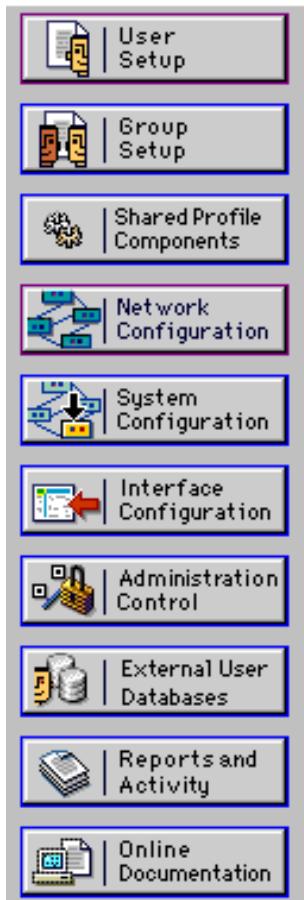
AAA Client Hostname	<input type="text" value="3640"/>
AAA Client IP Address	<input type="text" value="10.14.14.14"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="button" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

كـلـذ دـعـبـ ،ـتـايـطـعـمـ ـقـدـعـاـقـ نـمـأـيـ ciscoـ لـاـ يـفـ لـاجـمـ لـمـعـتـسـمـلـاـ يـفـ userـnـameـ لـاـ تـلـخـدـ
4ـ وـهـ مـدـخـتـسـمـلـاـ مـسـاـ ،ـلـاـثـمـلـاـ اـذـهـ يـفـ رـرـحـيـ /ـفـيـضـيـ ـقـقـطـقـ طـ
rtpuser.



User Setup

Select



User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			



5. كنكمي. rtpUserPass. ةملكلـا ،لـاثـم اـذـه يـفـ. مـدـخـتـسـمـلـا رـوـرـمـ ةـمـلـكـ لـخـدـأـ ،ـيـلـاتـلـا رـاطـإـلـا يـفـ
ـقـوـفـ رـقـنـاـ ،ـعـاهـتـنـالـا دـنـعـ. تـدـرـأـ اـذـإـ عـوـمـجـمـ ـىـلـا مـدـخـتـسـمـلـا بـاسـحـ نـيـيـعـتـ
ـلـاـسـرـاـ.



User Setup



Supplementary User Info

Real Name	rtpuser
Description	

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password	XXXXXXXXXX
Confirm Password	XXXXXXXXXX

Separate (CHAP/MS-CHAP/ARAP)

Password	
Confirm Password	

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is

ةي طايتحا خسنلا ئزيم نيوكت

مداخىللا هجوملا لشاف زواجت متيس، جاتم رىغ يس اسألا RADIUS مداخ حبصى امدنع يوناثلا RADIUS مداخ مادختسا يف هجوملا رمتسىس. يطايتحا خسنلل يلاتلا طشنلا يلاب مداخلا وه يسيئرلا مداخلا نوكى ام ۋداع. ارفوتمىس اسألا مداخلا ناك اذا ىتح دبألا يلى تانايىبللا ۋداعق مادختسا نكمى، احاتم يوناثلا مداخلا نكى مل اذا. لصفملما مداخ او ئادألا رمألا مادختساب ۋقاداصملل ئيلحملار [AAA authentication login default group rtp local](#).

ةحصلا نم ققحتلا

جي حص لكشب لممعي نيوكتلا نأ نم دكأتلل اهمادختسا كنكمى تامولعم مسقلما اذه رفوبي حفون 3640 هجومو يصخشلا رتوي بمكللا زاوج نيب IPSec قفن عاشناب مق.

Cisco 3640 ھجوم ضرعي . <http://10.17.17.17> ىلع ھيل ارش او رت و ي بمكلا ىلع ضرعتس م حتفا لسري . رورم ڈملک و مدخلتس م مسا کنم بـلـطـيـوـ، ـقـدـاـصـمـلـاـ لـيـكـوـرـيـثـيـوـ، ـهـذـهـ HTTP رورم ڈـکـرـحـ حاجـنـ ڈـلـاحـ یـفـ . ـقـدـاـصـمـلـلـ TACACS+ مـدـاخـ ىـلـاـ رورـمـلـاـ ڈـمـلـكـ مـدـخلـتسـ مـلـاـ مـسـاـ Cisco 3640 ىـلـعـ بـيـوـلـاـ مـدـاخـ ىـلـعـ بـيـوـلـاـ تـاحـفـصـ ڈـيـفـرـ ىـلـعـ اـرـدـاـقـ نـوـكـتـ نـأـ بـجـيـ ، ـقـدـاـصـمـلـاـ 10.17.17.17.

**يُتَلَوُ، (طَقْفٌ نَوْلِجْسِمْلَا عَالِمْعُلَا) جَارِخَالا مَجْرَتَمْ قَادْأا طَسْساَوْبُ ضَرْعَلَا رَمَاوَا ضَعْبُ مَعْدُ مَتْي
ضَرْعَلَا يَمْأُ جَارِخَالِيلِحَتْ ضَرْعُ كَلْ حَيْتَ**

- **show ip access lists** — عسومل او ئيسايقلا (ACL) لوصولاي مكحتلا مئاوق ضرعى لوصولاي ف مكحتلا مئاوق تالاخدا نممضتىي ئيامحللا رادج ھجوم ىلע اهنىوكت مت يتلا ئيكيمانيدلا (ACL) لوصولاي ف مكحتلا ۋەمىاق تالاخدا ۋەفااضا مەتت. (ئيكيمانيدلا (ACL) جانخىلا اذە ضرعى. اىل وۇقدىسي مىختىسىملا ناك اذا ام ىلى ادانتسا يىرۇد لىكشىب اهتلازاو ۋەقاداصملالىيکولىيغشتلىبىق 118 لوصولاي ۋەمىاق:

```
3640#show ip access-lists 118
Extended IP access list 118
 10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
 20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
 30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```

لبق نم حاجن ب ۋە دا صىملە لىكولى يېغىش دىپ 118 لۇصۇلما ئەمئاڭ جاڭىلا اذە ضرۇي مىدختىسىملا:

```
3640#show ip access-lists 118
Extended IP access list 118
 permit tcp host 10.20.20.26 any (7 matches)
 permit udp host 10.20.20.26 any (14 matches)
 permit icmp host 10.20.20.26 any
10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```

م دختسملا اذهل ٰددجملا تالاخدإلا يف لوصولا ٰقمئاق نم ىلولأا ٰثاثللا رطسألا لثممت م داخ نم اهلىزنت مت ي تتلاو TACACS+.

- **show ip auth-proxy cache** — قداص ملا ليك ونيوكت وأرق داص ملا ليك وتألاخدا اما ضرعى ، فيضم ملل IP ناونع درسل تقوف ملا نيزختلا ةركاذ ةيساسألا ةملكللا . هليغشت يراجلا مدخلتس ست يتلا تالاصتالا ئلاحو ، قداص ملا ليكول ئلهملا ئميقو ، رداص ملا ذفنم مقررو حجاجان مدخلتس ملا ئقداص نوكت ، ESTAB ئقداص ملا ليك و ئلاح تناك اذا . قداص ملا ليك و

```
3640#show ip auth-proxy cache
      Authentication Proxy Cache
      Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

اچالص اور عاطخآل افاسکتسا

ةفاضالاب، حيحصتلارو ققحتلارم اوأ **اھھالص او عاطخآلما فاشكتسأ** ۋە **قاداصملىكىو** ىلما عجرا يىخآلما اھھالص او عاطخآلما فاشكتسأ تامولعم ىلما.

اطفال حي حصن رماؤا يف قمهملات امولعملما عجار، عاطفالا حي حصن رماؤا رادصا لبـق: ظحالـم.

ةلص تاذ تامولعم

- QQ Cisco IOS
 - QQ Cisco IOS
 - QQ Cisco IOS
 - QQ Cisco IOS
 - QQ Cisco IOS

- [مِعْدَةٌ حُفَصٌ IPSec](#)
- [مِعْدَةٌ حُفَصٌ RADIUS](#)
- [تَاقِيَّلْعَتْلَا تَابِلْطَ \(RFCs\)](#)
- [مِعْدَةٌ حُفَصٌ TACACS/TACACS+](#)
- [TACACS+ قِيَادَةٌ وَيَفِ IOS](#)
- [يَنْفَلَا مِعْدَلَا - Cisco Systems](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).