

# عيرس ل VPN TCP غيرفت ليلحت

## فادهال

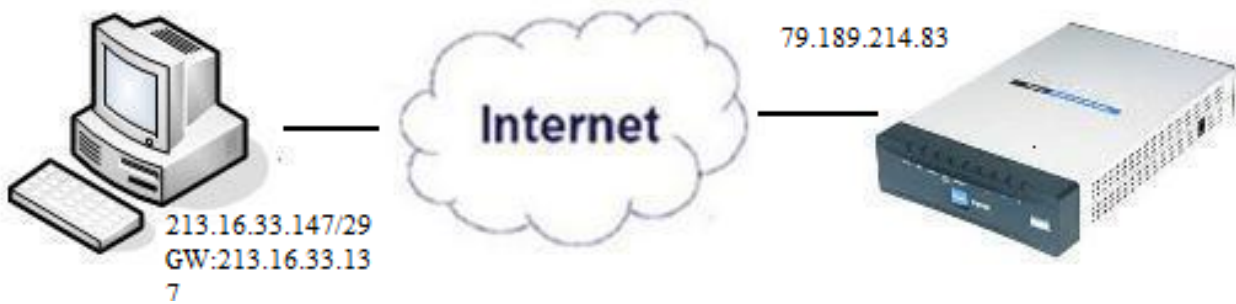
رورم ةكرح ةبقارمل Wireshark مادختساب مزحل طاقتل ةيفيك ةلاقملا هذه حضوت  
يلع VPN جم انرب دادعال ةلهس ةقيرط QuickVPN دعق. QuickVPN دوجو دنع ليمعلا  
نيطيسب رورم ةملاك و مدختسم مسا مادختساب لومحم رتويبمك و اديعب رتويبمك  
[Wireshark](#). مدختسملا زاهجال يلع انب تاكبشلا يلا نمالا لوصولا يف كلذ دعاسيس  
اهال صواو اعاطالا فاشكتسال ةكبشلا يف مزحل طاقتلال مدختسي مزحل sniffer وه

نيدلا عالمعلل ةرفوتم ةلاقملا هذه لازت ال Cisco لبق نم ةمومدم QuickVPN دعق مل  
قوف رقنا، QuickVPN تم دختسا يتلا تاهجوملاب ةمئاق يلع لوصولل QuickVPN نوم دختسي  
ويديفال ضرع كنكمي، QuickVPN لوح تامولعملال نم ديزمل [Cisco Small Business QuickVPN](#).  
ةلاقملا هذه ةيانه يف

## قيبطتلل ةلباقلا ةزهجال

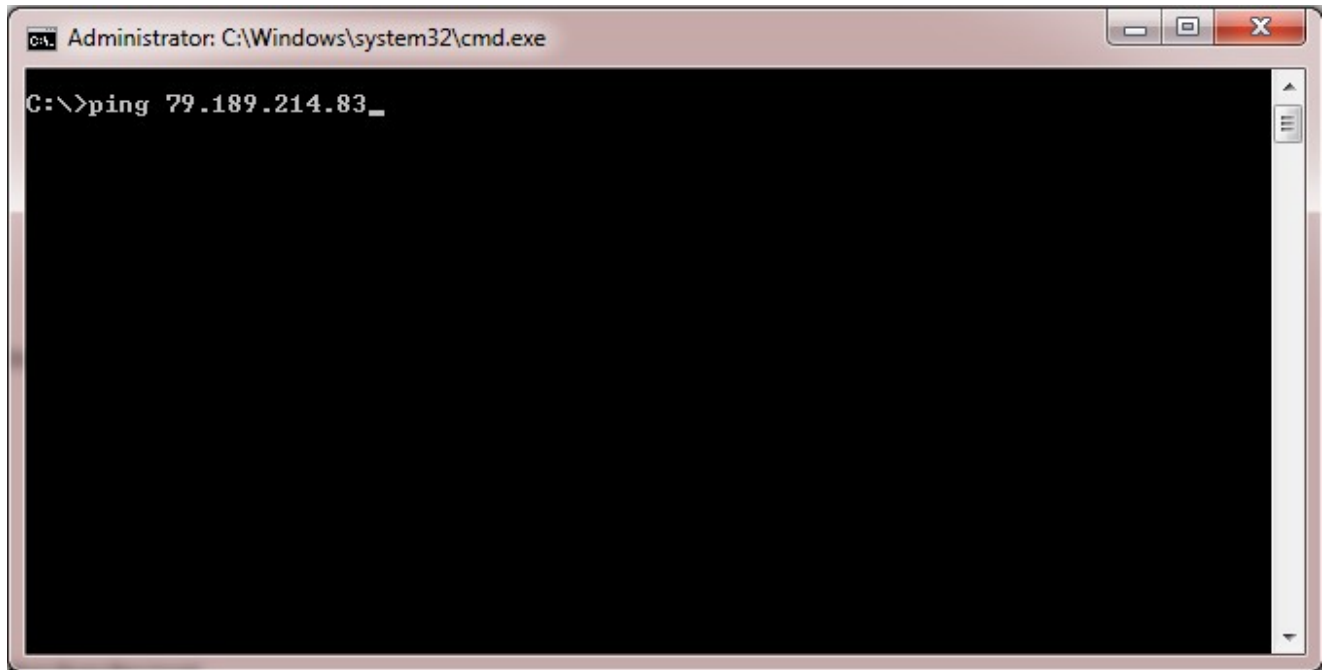
هالعا طابترالا يف ةدراولا ةمئاقلا رظنا) RV ةئف .

## QuickVPN ل TCP قارغا تاي لمع ليلحت



QuickVPN ليمعو Wireshark تيبتت مزلي، ةلاقملا هذه يف ةدراولا تاوطلخا عابتا لجا نم  
رتويبمكلا يلع

هجوم قيبطت ددحو cmd لخدا. شحبالا طيرش يلا لقتنا، رتويبمكلا يلع 1. ةوطلخا  
مت، ةلاجال هذه يف. هب لاصلتالا لواحت يذال IP ناونعو ping رمالا لخدا. تارايلخالا نم رماوالا  
ping 79.189.214.83 لخالدا



The image shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command prompt displays the command "C:\>ping 79.189.214.83\_" followed by a cursor. The rest of the window is black, indicating that the command has not yet been executed or the output is not visible.

ىلإ مزحلل لاسررا اهلل الخ نم متي يتللا ةهجاو لار تخاو Wireshark قيبطت حتفا 2. ةوطخلل  
طاقتللال رورم ةكرحو تنرتنللال

مسا لقح يف فيصوتلل مسا لخدأ. QuickVPN قيبطت ليغشت ادب 3. ةوطخلل  
فيصوتلل



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

\*\*\*\*\*

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

مدختسملا مسا ل قح ي ف مدختسملا مسا ل خدأ . 4 ةوطخلا



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

راجع ملء الكلا في ملء الكلا تلخد 5. ةوطخال



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

\*\*\*\*\*

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

مداخل ناووع لرح ي ف مداخل ناووع لخدأ. 6 ةوطخلا



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ةمئاق لدسنملا QuickVPN ل ءانملا يف QuickVPN ل ءانملا ترتخأ 7. ةوطخلا



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

XXXXXXXXXX

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :

443

60443

Auto

Connect

Save

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

DNS مداخل مداخلتسال دي عبال DNS مداخل مداخلتسال رايتخالالا ةناخ ددح (يرايتخا). 8 ةوطخال  
يلحمل مداخلالا نم ال دد دي عبال



Small Business

# QuickVPN Client

Profile Name :

Office

User Name :

admin

Password :

\*\*\*\*\*

Server Address :

79.189.214.83

Port For QuickVPN :

Auto

Use Remote DNS Server :



Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ليصوت ىل ع رقننا 9 ةوطخال

ةطقتللملا رورملا ةكرح فلم حتفا 10 ةوطخال



97	22.922202	79.189.214.86	213.16.33.141	TCP	https > nav-port [ACK] Seq=728 Ack=315 Win=5840 Len=0
98	22.953202	79.189.214.86	213.16.33.141	TLSv1	Change Cipher Spec, Encrypted Handshake Message
99	22.953514	213.16.33.141	79.189.214.86	TLSv1	Application Data, Application Data
100	23.047399	79.189.214.86	213.16.33.141	TCP	https > nav-port [ACK] Seq=779 Ack=589 Win=5840 Len=
115	26.839997	79.189.214.86	213.16.33.141	TLSv1	Application Data, Application Data
116	26.885516	79.189.214.86	213.16.33.141	TLSv1	Encrypted Alert
117	26.885548	213.16.33.141	79.189.214.86	TCP	nav-port > https [ACK] Seq=589 Ack=1187 Win=64350 Len=0
118	26.885644	213.16.33.141	79.189.214.86	TLSv1	Encrypted Alert
119	26.885751	213.16.33.141	79.189.214.86	TCP	nav-port > https [FIN, ACK] Seq=618 Ack=1187 Win=64350 Len=0
120	26.975742	79.189.214.86	213.16.33.141	TCP	https > nav-port [RST] Seq=1187 Win=0 Len=0
153	36.003017	213.16.33.141	79.189.214.86	ISAKMP	Identity Protection (Main Mode)
154	36.100454	79.189.214.86	213.16.33.141	ISAKMP	Identity Protection (Main Mode)
155	36.111330	213.16.33.141	79.189.214.86	ISAKMP	Identity Protection (Main Mode)
162	36.597760	79.189.214.86	213.16.33.141	ISAKMP	Identity Protection (Main Mode)
163	36.601730	213.16.33.141	79.189.214.86	ISAKMP	Identity Protection (Main Mode)
164	36.703206	79.189.214.86	213.16.33.141	ISAKMP	Identity Protection (Main Mode)
165	36.714256	213.16.33.141	79.189.214.86	ISAKMP	Quick Mode
166	37.279513	79.189.214.86	213.16.33.141	ISAKMP	Quick Mode
167	37.283580	213.16.33.141	79.189.214.86	ESP	ESP (SPI=0x8316d0a3)
168	37.283761	213.16.33.141	79.189.214.86	ISAKMP	Quick Mode
209	48.111271	213.16.33.141	79.189.214.86	ESP	ESP (SPI=0x8316d0a3)
216	48.233459	79.189.214.86	213.16.33.141	ESP	ESP (SPI=0x2b28e6ae)
224	51.775102	213.16.33.141	79.189.214.86	ISAKMP	Informational
225	51.783452	213.16.33.141	79.189.214.86	ISAKMP	Informational
227	51.834637	213.16.33.141	79.189.214.86	TCP	giga-pocket > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460
228	51.924897	79.189.214.86	213.16.33.141	TCP	https > giga-pocket [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
229	51.924934	213.16.33.141	79.189.214.86	TCP	giga-pocket > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
230	51.925230	213.16.33.141	79.189.214.86	SSLv2	Client Hello
231	52.016293	79.189.214.86	213.16.33.141	TCP	https > giga-pocket [ACK] Seq=1 Ack=125 Win=5840 Len=0
232	52.049811	79.189.214.86	213.16.33.141	TLSv1	Server Hello, Certificate, Server Hello Done
233	52.052284	213.16.33.141	79.189.214.86	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
237	52.181662	79.189.214.86	213.16.33.141	TCP	https > giga-pocket [ACK] Seq=728 Ack=315 Win=5840 Len=0
241	52.210977	79.189.214.86	213.16.33.141	TLSv1	Change Cipher Spec, Encrypted Handshake Message
242	52.211266	213.16.33.141	79.189.214.86	TLSv1	Application Data, Application Data
243	52.304238	79.189.214.86	213.16.33.141	TCP	https > giga-pocket [ACK] Seq=779 Ack=605 Win=5840 Len=0
244	52.407500	79.189.214.86	213.16.33.141	ISAKMP	Informational
245	52.412835	79.189.214.86	213.16.33.141	ISAKMP	Informational
255	56.043199	79.189.214.86	213.16.33.141	TLSv1	Application Data, Application Data
256	56.044568	79.189.214.86	213.16.33.141	TLSv1	Encrypted Alert
257	56.044596	213.16.33.141	79.189.214.86	TCP	giga-pocket > https [ACK] Seq=605 Ack=1091 Win=64446 Len=0
258	56.044668	213.16.33.141	79.189.214.86	TLSv1	Encrypted Alert
259	56.044774	213.16.33.141	79.189.214.86	TCP	giga-pocket > https [FIN, ACK] Seq=634 Ack=1091 Win=64446 Len=0

اهنم ققحتلا مزلي ةيسيئر رومأ ةثالث كانه ، QuickVPN لاصتا ثدحي يكل

· لاصتالا ةينام |

· (ةداهشلا نم ققحتلا) جهنلا طيشنت

· ةكبشلا نم ققحتلا

رورم ةكرح يف (TLSv1) لقنلا ةقبط نامأ مزح ةيؤر يلا الواجاتحن ، لاصتالا نم ققحتلل تالوكوتورب يه هذه . اهل ةقباسلا (SSL) ةنمألا ليصوتلا ذخأم ةقبط عم طاقتلالا . ةكبشلا ربع تالاصتالا نامألا رفوت يتللا ريفشتلا

لوكوتوربو "تنرتنالا نامأ نارثقا" ةمزح مادختساب جهنلا طيشنت نم ققحتلا نكمي ةيلا ددحي وهو . اهطاقتلا مت يتللا Wireshark رورم ةكرح يف (ISAKMP) حيتافملا ةرادا نم فيفختلاو ، حيتافملا ديوت تاي نقتو ، هتراداو هئاشناو (SA) نامألا نارثقا ةقداصم حيتافملا لدابتل IKE مدختسي هنإ . تاديدهتلا ةدح

هل يدعتو هيلع ضوافتلاو SA ءاشنالا ةمزحلا قيسنت ديدحت يف ISAKMP دعاسي لثم ةفلتخملا ةكبشلا نامأ تامدخل ةبولطم ةعونتم تامولعم يلع يوتحي وهو . هفدحو لقنلا ةقبط تامدخو ، عفدلا لمح ني مضتو ، سأللا ةقداصم كلذ يف امب ، IP ةقبط ةمدخ لدابتل تالومحلا ISAKMP ددحي . ضوافتلا رورم ةكرح ةيئاذلا ةيماحلا وأ ، قيبطتلا وأ لقنل قسانتم لمع راطا تاقيسي سنتلا هذه رفوت . ةقداصملاو حاتفملا ءاشنالا تانايب ةيمزراوخو حيتافملا ءاشنالا ةينقت نع لقنتم لكشب ةقداصملاو حيتافملا تانايب ةقداصملا ةيلاو ريفشتلا

ريغ قفاوتلاو ةيرسلا نم ققحتلل (ESP) ني مضتلا نامأ ةلومح مادختسا متي ةكرح قفدتو ليغشتلا ةداعلا ةداصملا تامدخلاو تانايبلا لصأ ةقداصملا لصتملا اذه مدختسي . IPSec لوكوتورب يف اوضع ESP نوكي ، QuickVPN يف . دودحملا رورملا ةقداصملاو ريفشتلا معددي وهو . اهتيرسو اهتالسو مزحلا ةلاصأ ريفوتل راخلا لصفنم لكشب

· ةقداصم نودب ريفشتلاب ي صوي ال : ةظحالم

IP ةمزح ني مضت متي قفنلا عضو يف نكلو IP سأللا ةيماحل ESP مادختسا متي ال ةيلا خادلا IP ةمزح يلا اهري فوت متي و اهتفاضلا متت . ديدج ةمزح سأللا مادختساب لمالكلا . 50 مقرر لوكوتوربلا مدختسيو IP قوف لمعي وهو . يلا خادلا سأللا كلذ يف امب ةلمالكلا

رارقلا

QuickVPN و Wireshark مادختساب مزحلا طاقتلا ةيفيكن نألا ماملعت دقل

...ةلاقملا هذهب قلعتي ويديف عطقم دهاش

[Cisco نمدىرخألا \(ةينقتلا تاتحادملا\) Tech Talks ضرعل انه رقتا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا 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 هذه ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا