

عيرس ل VPN TCP غيرفت ليلحت

فادهال

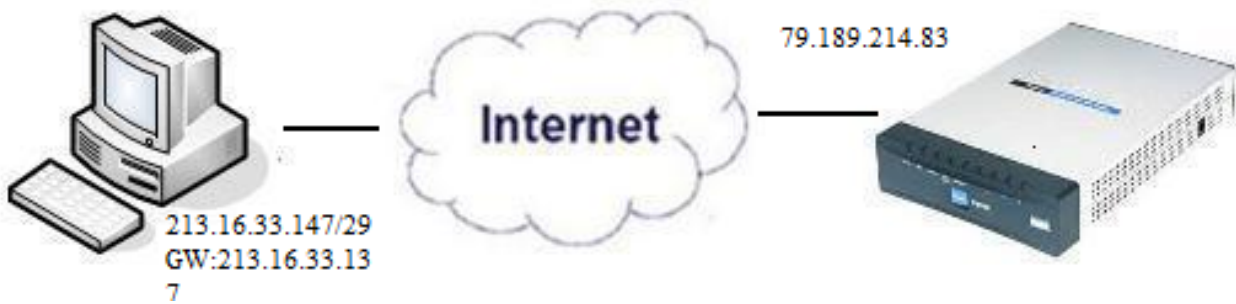
رورم ةكرح ةبقارمل Wireshark مادختساب مزحل طاقتل ةيفيك ةلاقملا هذه حضوت
يلع VPN جم انرب دادعال ةلهس ةقيرط QuickVPN دع ت QuickVPN دوجو دنع ليمعلا
نيطيسب رورم ةم لك و مدختسم مسا مادختساب لومحم رتوي بمك و اديعب رتوي بمك
[Wireshark](#). مدختسم ل زاهل ايلع انب تاكبش ل ايل نم ال لوصول ايل ك لذ دعاسيس
اهال صاوا عاطخال فاشكتسال ةكبش ل ايل مزحل طاقتل ال مدختسي مزحل sniffer وه

نيلع ال م عمل ةرفوتم ةلاقملا هذه ل ازت ال Cisco لبق نم ةم و دم QuickVPN دع ت مل
قوف رقنا QuickVPN ت مدختس ايل تاهجوم ل ايل ةمئاق ايل لوصول ل QuickVPN نوم دختسي
ويديفال ضرع كنكمي QuickVPN لوج تامولعمل نم ديزمل [Cisco Small Business QuickVPN](#).
ةلاقملا هذه ةيانه ايل

قيرب طتل ةلباق ل ةزهال

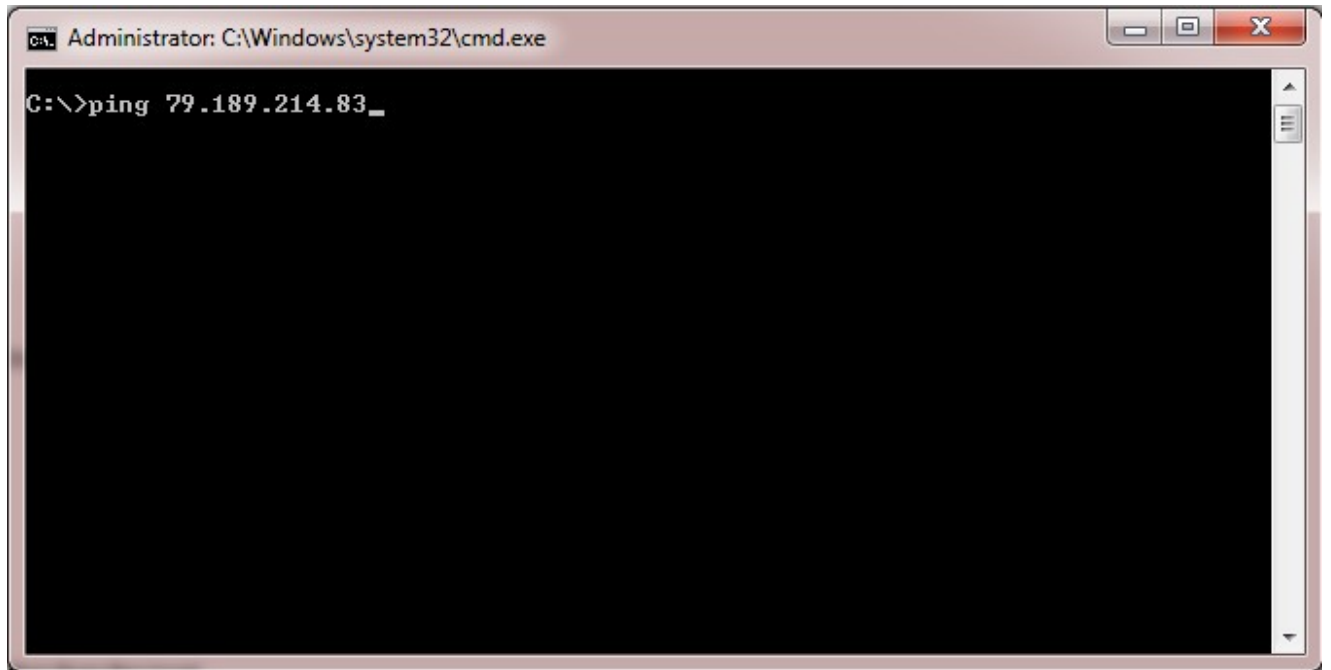
هالعال طابترال ايل ةدراول ةمئاق ل رظنا RV ةئف

QuickVPN ل TCP قارغ ايل لملع ليلحت



QuickVPN ليمعو Wireshark تيبثت مزلي، ةلاقملا هذه ايل ةدراول تاوطلخال عابتا لجا نم
رتوي بمك ل ايل

هجوم قيرب طتل ددحو cmd لخد ا. شحل طيرش ايل لقتنا، رتوي بمك ل ايل ل. 1 ةوطلخال
م، ةلال هذه ايل. هب لاصلتال لواحت ايل IP ناونعو ping رمال لخد ا. تارايل ل نم رماوالا
ping 79.189.214.83 لخد ا



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 output of the command is not visible.

ىلا مزحلا لاسرا اهلل الخ نم متي يتلا ةهجاو لا رتخاو Wireshark قي بطت حت فا 2. ةوطخل
طاقتل ال رورم ةكرحو تنرتن ال

مسا لقح يف في صوتل مسال خدا QuickVPN قي بطت لي غشت ادب 3. ةوطخل
في صوتل



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 عميل الـ VPN في عميل الـ QuickVPN 5. عوطل الـ



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 ل قح ي ف مداخل ناووع ل خدأ .6 ةوطخ لا



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 عب ال DNS مداخل مداخلتسا رايتخالالا ةناخ ددح (يرايتخا). 8 ةوطخال
يلحمل مداخلالا نم ال ددب دي عب ال



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 ققحتال مزلي ةيسيئر روم ةثالث كانه ، QuickVPN لاصتا ثدحي يكل

· لاصتال ةينام |

· (ءداهشال نم ققحتال) جهنال طيشنت

· ةكبشال نم ققحتال

رورم ةكرح يف (TLSv1) لقنل ةقبط نام مزح ةيؤر لىل الواجاتحن ، لاصتال نم ققحتلل تالوكوتورب يه هذه . اهل ةقباسال (SSL) ةنمآل لىصوتال ذخأم ةقبط عم طاقتلال ةكبشال ربع تالاصتال نامآل رفوت يتلل ريفشال

لوكوتوربو "تنترنال نام نارتقا" مزح مادختساب جهنال طيشنت نم ققحتال نكمي ةلآ ددحي وهو . اهطاقتال مت يتلل Wireshark رورم ةكرح يف (ISAKMP) حيتافمال ةرادا نم فيفختلاو ، حيتافمال ديوت تاي نقتو ، هتراداو هئاشن او (SA) نامآل نارتقا ةقداصم حيتافمال لدابتل IKE مدختسي هنإ . تاديدهتال ةدح

هل يدعتو هيلع ضوافتال او SA ءاشنال ةمزحل قيسنت ديدحت يف ISAKMP دعاسي لثم ةفلتخمال ةكبشال نام تامدخل ةبولطم ةعونتم تامولعم يلع يوتحي وهو . هفدحو لقنل ةقبط تامدخو ، عفدل لمح ني مضتو ، سألل ةقداصم كلذ يف امب ، IP ةقبط ةمدخ لدابتل تالومحل ISAKMP ددحي . ضوافتال رورم ةكرح ةيذلل ةيامل او ، قيبطتال او لقنل قسانتم لمع راطا تاقيسنتال هذه رفوت . ةقداصم لواحافمال ءاشنال تانايب ةيمزراوخو حيتافمال ءاشنال ةينقت نع لقنل سلكشب ةقداصم لواحافمال تانايب ةقداصم لىل آو ريفشال

ريغ قفاوتال او ةيرسال نم ققحتلل (ESP) ني مضتال نام ةلومح مادختسا متي ةكرح قفدتو ليغشتال ةءاعل ةداصم ل تامدخال تانايب لىل لىل ةقداصم لىل صتال اذه مدختسي . IPSec لوكوتورب يف اوضع ESP نوكي ، QuickVPN يف . دودحمل رورم ل ةقداصم لىل او ريفشال معددي وهو . اهتيرسو اهتال سو مزحل لىل لىل ريفوتل رايخل لىل صفنم لكشب

· ةقداصم نودب ريفشال لىل صوي ال : ةظالم

IP ةمزح ني مضت متي قفنل ءضوي يف نكلو IP سألل ةيامل ESP مادختسا متي ال ةيلخادل IP ةمزح لىل اهرىفوت متي و اهتفاضل متت . ديدج ةمزح سألل مادختساب لمالكال 50 مقرر لوكوتورب لىل مدختسيو IP قوف لمعي وهو . يلىل خادل سألل كلذ يف امب ةلمالكال

رارقال

QuickVPN و Wireshark مادختساب مزحل طاقتال ةيفيكل نألل 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 اذ ه Cisco ت مچرت
م ل اء ان ا ع مچ ي ف ن م دخت س م ل م عد و ت ح م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا 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 (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