

Expressway SSL ريفش ت نيوكت صي صخت

تايتوحت حمل

[قم دق م ل](#)

[ةي س اس أ ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ةي س اس أ ت ا م و ل ع م](#)

[ر ي ف ش ت ل ا ة ل س ل س ص ح ف](#)

[ة م ز ل ا ط ا ق ت ل ا م ا د خ ت س ا ب T L S ة ح ف ا ص م ي ف ر ي ف ش ت ل ا ض و ا ف ت ص ح ف](#)

[ن ي و ك ت ل ا](#)

[د د ح م ر ي ف ش ت ل ي ط ع ت](#)

[ة م ا ع ة ي م ز ا و خ م ا د خ ت س ا ب ر ي ف ش ت ل ا ن م ة و م ح م ل ي ط ع ت](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

[ر ي ف ش ت ل ا ة ل س ل س ل ب ق ن م ا ه ب ح و م س م ل ا ر ي ف ش ت ل ا ة م ئ ا ق ص ح ف](#)

[ل ط ع م ر ي ف ش ت ل ي ع ض و ا ف ت ل ا ب T L S ل ا ص ت ا ر ا ب ت خ ا](#)

[ل ط ع م ر ي ف ش ت م ا د خ ت س ا ب T L S H a n d s h a k e ن م ة م ز ح ط ا ق ت ل ا ص ح ف](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

اهن ي و ك ت م ت ي ت ل ا ر ي ف ش ت ل ا ل س ا ل س ص ي ص خ ت ل ة م ز ا ل ل ا ت ا و ط خ ل ا د ن ت س م ل ا ا ذ ه ف ص ي
Expressway ل ع ا ق ب س م

ةي س اس أ ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ةي ل ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب C i s c o ي ص و ت

- Expressway ن م C i s c o و C i s c o V C S.
- T L S ل و ك و ت و ر ب .

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ةي ل ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- C i s c o E x p r e s s w a y ، ر ا د ص ا ل ا x 1 5 . 0 . 2 .

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت
ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج ا ل ا ع ي م ج ت ا د ب
ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ةيساسأ تامولعم

يتلاو، اقبس م اهنيوكت مت ريفش ل لسال س ي ضارت فالال ExpressWay نيوكت نم ضتي افيعض هرابتعا نكمي يذلا ريفش لال ضعب معد نيكمت يلع، قفاوتل بابسأل، لمعت لجال نم ريفش لال لسال س صيصخت نكمملا نم. ةسسؤملا نامأ تاسايس ضعب بجومب ةئيبل لكل ةدحمل تاسايس لال مئال تل اهطبض.

تالوكت ووربلال هذه نم لكل ةلقتسم ريفش لال لسال س نيوكت نكمملا نم، Expressway يف

- HTTPS
- LDAP
- يسكعلا ليكولا
- SIP
- SMTP
- ريفوت TMS
- امداخ فاشتك UC
- XMPP

[OpenSSL ريفش لال ةرادا ةحفص](#) يف فوصومل OpenSSL قيسنت ريفش لال لسال س عيطت eECDH:EDH:HIGH:- ةيسارت فالال ةلسل لسال عم X15.0.2 ي لال Expressway رادصا يتيأي اقبس م هنيوكت مت AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH ريفش لال > نامأل > ةناي ص تحت، بيولا ةرادا ةحفص نم. ءاوس دح يلع تالوكت ووربلال عي مجل ةني عم ةرفش ةلازا وأ ةفاضال، لوكت ووربل لكل ةني عم لال ريفش لال لسال س لي دعت كنكمي ةماع ةي م زراوخ م ادخت ساب تارفش م لال نم تاعومجم وأ

ريفش لال ةلسل لس صحت

عي مج يلع يوتحت ةمئاق جارخا كنكمي، <cipher string>" -v OpenSSL ciphers رمأل م ادخت ساب ايئوض ةرفش لال صحت فل اديفم نوكتي ام وهو، ةني عم ةلسل لس اهب حمست ي تال تارفش لال ةيسارت فالال Expressway ريفش لال لسل لس صحت دن ع جارخال لال م لال اذه حضوي:

```
<#root>
```

```
~ #
```

```
openssl ciphers -v "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH"
```

```
0x13,0x02 - TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD
0x13,0x01 - TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0xAD - ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0xAC - ECDHE-ECDSA-AES128-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
```

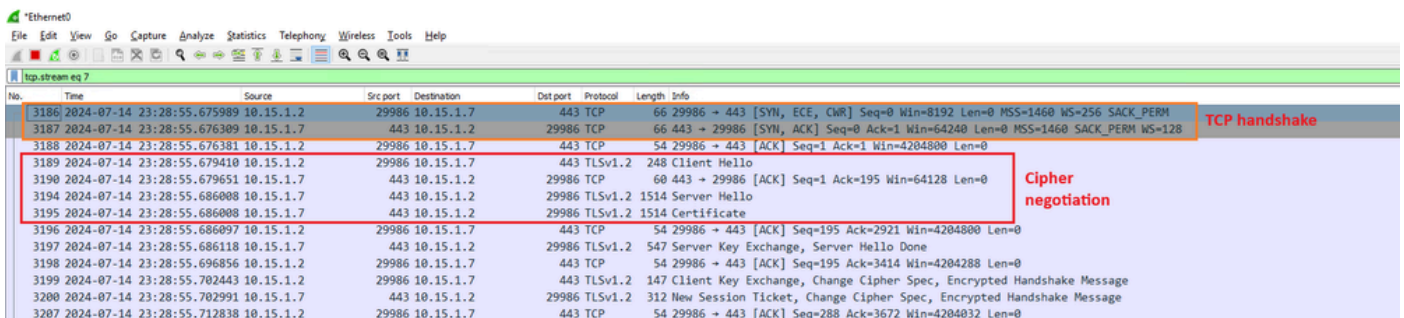
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
0xC0,0x09 - ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
0xC0,0x13 - ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0xA3 - DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
0x00,0x9F - DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xAA - DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0x9F - DHE-RSA-AES256-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0xA2 - DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
0x00,0x9E - DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9E - DHE-RSA-AES128-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x6B - DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x6A - DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
0x00,0x67 - DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x40 - DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
0x00,0x33 - DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0x32 - DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
0x00,0x9D - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x9D - AES256-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0x9C - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9C - AES128-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x3D - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x3C - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x2F - AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
~ #

تمرین طاق‌الت‌م‌ادخت‌س‌اب TLS ح‌ف‌اص‌م‌ ي‌ف‌ ر‌ي‌ف‌ش‌ت‌ل‌ا‌ ض‌و‌ا‌ف‌ت‌ ص‌ح‌ف

ر‌ي‌ف‌ش‌ت‌ل‌ا‌ ض‌و‌ا‌ف‌ت‌ ل‌ي‌ص‌ا‌ف‌ت‌ ص‌ح‌ف‌ ك‌ن‌ك‌م‌ي‌، ت‌م‌زح‌ ط‌ا‌ق‌ت‌ل‌ا‌ ي‌ف‌ TLS ض‌و‌ا‌ف‌ت‌ ط‌ا‌ق‌ت‌ل‌ا‌ ل‌ا‌ل‌خ‌ ن‌م‌ Wireshark م‌اد‌خ‌ت‌س‌اب

ت‌م‌ئ‌اق‌ ر‌ف‌و‌ي‌ ا‌م‌م‌، ل‌ي‌م‌ع‌ل‌ ز‌ا‌ه‌ ع‌ط‌س‌ا‌وب‌ ع‌ل‌س‌ر‌م‌ ClientHello ت‌م‌زح‌ TLS ح‌ف‌اص‌م‌ ت‌ي‌ل‌م‌ع‌ ن‌م‌ض‌ت‌ت‌ ا‌ه‌ن‌ي‌و‌ك‌ت‌ م‌ت‌ ي‌ت‌ل‌ا‌ ل‌ا‌ص‌ت‌ا‌ل‌ ل‌و‌ك‌و‌ت‌و‌ر‌ب‌ ع‌ر‌ف‌ش‌ ع‌ل‌س‌ل‌س‌ل‌ ا‌ق‌ف‌و‌ ا‌ه‌م‌ع‌د‌ي‌ ي‌ت‌ل‌ا‌ ت‌ا‌ر‌ف‌ش‌م‌ل‌ا‌ب‌ ع‌ط‌س‌ا‌وب‌ (ت‌د‌د‌ح‌م‌ل‌ا‌) ا‌ب‌ ح‌و‌م‌س‌م‌ل‌ا‌ ت‌ا‌ر‌ف‌ش‌ل‌ل‌ ع‌ص‌ا‌خ‌ل‌ ه‌ت‌م‌ئ‌اق‌ب‌ ا‌ه‌ن‌ر‌ا‌ق‌ي‌و‌، ت‌م‌ئ‌اق‌ل‌ م‌د‌ا‌خ‌ل‌ا‌ ع‌ج‌ا‌ر‌ي‌ ا‌ه‌م‌ا‌د‌خ‌ت‌س‌ا‌ب‌ م‌ت‌ي‌ل‌، ن‌ي‌م‌ا‌ظ‌ن‌ل‌ا‌ل‌ ا‌ك‌ ا‌ه‌م‌ع‌د‌ي‌ ع‌ر‌ف‌ش‌ ر‌ا‌ت‌خ‌ي‌و‌، (ه‌ب‌ ع‌ص‌ا‌خ‌ل‌ا‌ ر‌ي‌ف‌ش‌ت‌ل‌ا‌ ع‌ل‌س‌ل‌س‌ل‌ ر‌ا‌ت‌خ‌م‌ل‌ا‌ ر‌ي‌ف‌ش‌ت‌ل‌ا‌ ي‌ل‌ا‌ ر‌ي‌ش‌ت‌ ي‌ت‌ل‌a‌ ServerHello ت‌م‌زح‌ ع‌م‌ ب‌ي‌ج‌ت‌س‌ي‌ م‌ت‌. ع‌ر‌ف‌ش‌م‌ل‌ا‌ ع‌س‌ل‌ج‌ل‌ل‌ ر‌ي‌ف‌ش‌ت‌ل‌ا‌ ض‌و‌ا‌ف‌ت‌ ت‌ي‌ل‌ا‌ ن‌أ‌ ا‌ل‌، ع‌ح‌ف‌اص‌م‌ل‌l‌ 1.2 و TLS 1.3 ي‌ر‌ا‌و‌ح‌ ن‌ي‌ب‌ ت‌م‌ه‌م‌ ت‌ا‌ف‌ا‌ل‌ت‌خ‌ج‌و‌ت‌ ن‌ي‌ر‌ا‌د‌ص‌ا‌ل‌ا‌l‌ ا‌ك‌ ي‌ف‌ ه‌س‌ف‌ن‌ ا‌د‌ب‌م‌ل‌ا‌ ا‌ذ‌ه‌ م‌د‌خ‌ت‌س‌ت‌

443 ذ‌ف‌ن‌م‌ل‌ا‌ ي‌ل‌ع‌ Expressway و ب‌ي‌و‌ض‌ر‌ع‌ت‌س‌م‌ ن‌ي‌ب‌ TLS 1.3 ر‌ي‌ف‌ش‌ت‌ ض‌و‌ا‌ف‌ت‌ ي‌ل‌ع‌ ل‌ا‌ث‌م‌ ا‌ذ‌ه‌ Wireshark ي‌ف‌ ح‌ض‌و‌م‌ و‌ه‌ ا‌م‌ك‌



Wireshark ي‌ف‌ TLS ح‌ف‌اص‌م‌ ي‌ل‌ع‌ ل‌ا‌ث‌م‌

اهم عدي يتل تارفشال نم عمئاق عم ClientHello مزح ضرعت سمل لسري، الو:

The image shows a Wireshark capture of a network packet. The top pane displays a list of packets, with packet 275 highlighted in red. This packet is a TLSv1.3 Client Hello from source 10.15.1.2 to destination 10.15.1.7. The bottom pane shows the detailed structure of this packet, including the Transport Layer Security (TLS) record layer, Handshake Protocol, and a list of 16 cipher suites. The cipher suites list is also highlighted with a red box.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
270	2024-07-14 21:54:39.347430	10.15.1.2	26105	10.15.1.7	443	TCP	66	26105 → 443 [SYN, EC]
271	2024-07-14 21:54:39.347496	10.15.1.7	443	10.15.1.2	26105	TCP	66	443 → 26105 [SYN, AC]
272	2024-07-14 21:54:39.347736	10.15.1.2	26105	10.15.1.7	443	TCP	60	26105 → 443 [ACK] Seq
273	2024-07-14 21:54:39.348471	10.15.1.2	26105	10.15.1.7	443	TCP	1514	26105 → 443 [ACK] Seq
274	2024-07-14 21:54:39.348508	10.15.1.7	443	10.15.1.2	26105	TCP	54	443 → 26105 [ACK] Seq
275	2024-07-14 21:54:39.348533	10.15.1.2	26105	10.15.1.7	443	TLSv1.3	724	Client Hello
276	2024-07-14 21:54:39.348544	10.15.1.7	443	10.15.1.2	26105	TCP	54	443 → 26105 [ACK] Seq

> Frame 275: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits)
> Ethernet II, Src: VMware_b3:fe:d6 (00:50:56:b3:fe:d6), Dst: VMware_b3:5c:7a (00:50:56:b3:5c:7a)
> Internet Protocol Version 4, Src: 10.15.1.2, Dst: 10.15.1.7
> Transmission Control Protocol, Src Port: 26105, Dst Port: 443, Seq: 1461, Ack: 1, Len: 670
> [2 Reassembled TCP Segments (2130 bytes): #273(1460), #275(670)]
v Transport Layer Security
v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 2125
v Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 2121
Version: TLS 1.2 (0x0303)
Random: 7a61ba6edc3ff95c4b0672c7f1de5bf4542ced1f5eaa9147bef1cf2e54d83a50
Session ID Length: 32
Session ID: 98d41a8d7708e9b535baf26310bfea50fd668e69934585b95723670c44ae79f5
Cipher Suites Length: 32
v Cipher Suites (16 suites)
Cipher Suite: Reserved (GREASE) (0xaeaa)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03ab)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1

Wireshark يف ClientHello مزح يلع لاثم

لوكون و ربل اهن يوكت مت يتل هب ة صاخال ريفشال ة لسلس نم Expressway ققحتي ريفشيت دي دحت متي، لاثم اذه يف. لي مع لاه س فن مع دي ريفشيت نع شحب يو، HTTPS هب ة صاخال ServerHello مزح عم Expressway بيجت سي. ECDHE-RSA-AES256-GCM-SHA384. ة دحمل ة رفشال يل ريفشيت يتل:

eth0_diagnostic_logging_tcpdump00_exp-c1_2024-07-15_03_54_39.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 7

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
273	2024-07-14 21:54:39.348471	10.15.1.2	26105	10.15.1.7	443	TCP	1514	26105 → 443 [ACK] Seq=1 Ack=1 Win=4204800 Len=1460 [TCP segment of a reasse
274	2024-07-14 21:54:39.348508	10.15.1.7	443	10.15.1.2	26105	TCP	54	443 → 26105 [ACK] Seq=1 Ack=1461 Win=64128 Len=0
275	2024-07-14 21:54:39.348533	10.15.1.2	26105	10.15.1.7	443	TLSv1.3	724	Client Hello
276	2024-07-14 21:54:39.348544	10.15.1.7	443	10.15.1.2	26105	TCP	54	443 → 26105 [ACK] Seq=1 Ack=2131 Win=63488 Len=0
277	2024-07-14 21:54:39.349184	10.15.1.7	443	10.15.1.2	26105	TLSv1.3	314	Server Hello, Change Cipher Spec, Application Data, Application Data
278	2024-07-14 21:54:39.349635	10.15.1.2	26105	10.15.1.7	443	TLSv1.3	134	Change Cipher Spec, Application Data
279	2024-07-14 21:54:39.349976	10.15.1.7	443	10.15.1.2	26105	TLSv1.3	373	Application Data

> Frame 277: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)

> Ethernet II, Src: VMware_b3:5c:7a (00:50:56:b3:5c:7a), Dst: VMware_b3:fe:d6 (00:50:56:b3:fe:d6)

> Internet Protocol Version 4, Src: 10.15.1.7, Dst: 10.15.1.2

> Transmission Control Protocol, Src Port: 443, Dst Port: 26105, Seq: 1, Ack: 2131, Len: 260

Transport Layer Security

- TLV1.3 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 128
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 124
 - Version: TLS 1.2 (0x0303)
 - Random: ae5d8084b4032d2716e681a6d3052d4ea518faf7a87a8490234871ab4e603e5f
 - Session ID Length: 32
 - Session ID: 98d41a8d7708e9b535baf26310bfea50fd668e69934585b95723670c44ae79f5
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Compression Method: null (0)
 - Extensions Length: 52

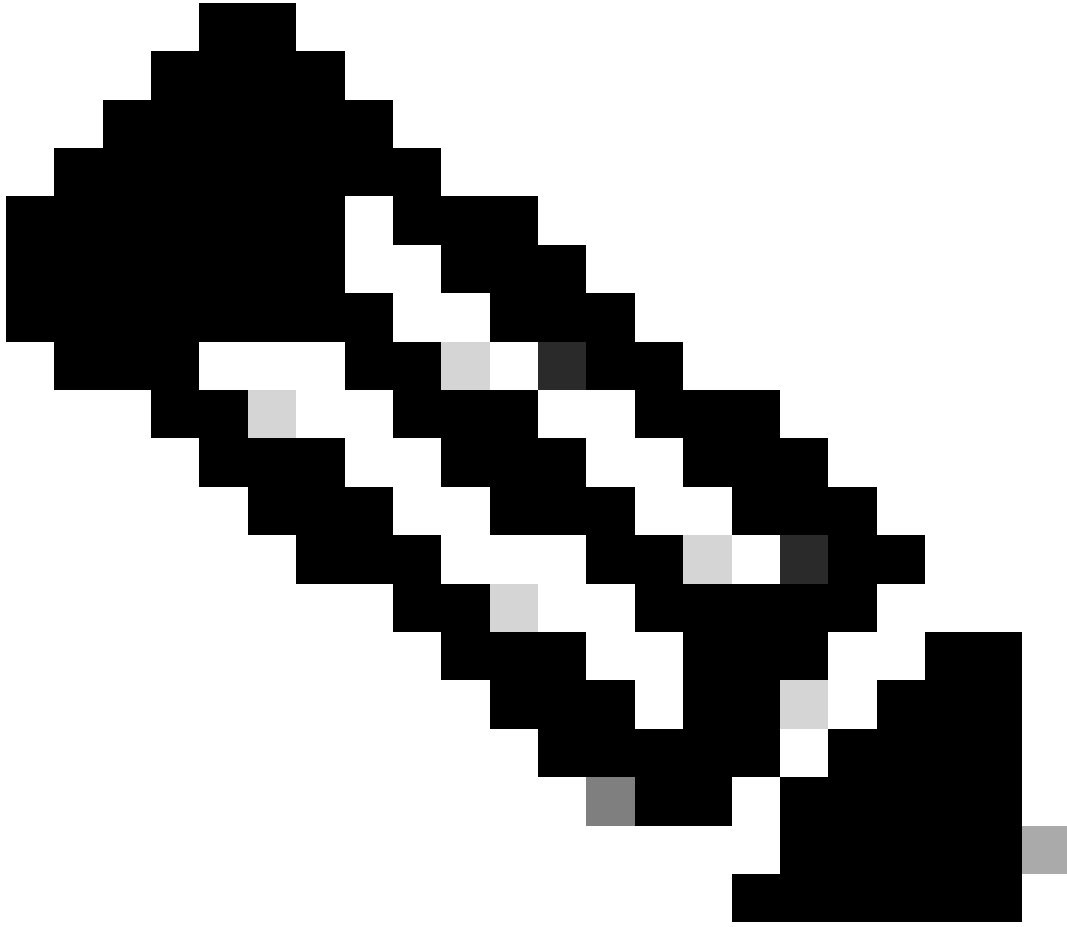
Wireshark ي ServerHello ةم زح يلع لاثم

نيوكتلا

يلع تاي لمع ءارجال ةصاخال فرحال نم ديدعل OpenSSL ريفشت ةلسلس قيسنت نمضتي كرتشم نوكم يف كرتشت يتلا ةرفشلا نم ةومجم وأ دحم ريفشت ةلازا لثم ةلسلسلا هذه يف ةمدختسمل فورحال نإف، ريفشلا ةلازا ةداع وه تاصيفشختلا هذه نم فدهلا نأ أمب يه ةلثمألا:

- لك وأ ضعيب حامسلا نكمي. ةمئاقلا نم ريفشختلا ةلازال مدختسمل، - فرحال يف اقحال رهظت يتلا تارايفخال ةطساوب ىرخأ ةرم هتلازا تمت يذلا ريفشختلا ةلسلسلا.
- حامسلا نكمي ال، همادختسا دنع. ةمئاقلا نم ريفشختلا ةلازال اضيأ مدختسمل، ! فرحال يف اقحال رهظت ىرخأ تارايفخ يأ ةطساوب ىرخأ ةرم اهتلازا تمت يتلا تارفشلاب ةلسلسلا.
- ةمئاقلا يف رصانعلا نيبلصافك لمعي يذلا: فرحال.

يلع لوصلل. لضفم! ،كلذ عمو، ةلسلسلا نم ريفشخت ةلازال امه نم الك مادختسا نكمي [OpenSSL تارفش قرادا ةحفص](#) عجار، ةصاخال فورحلاب ةلماك ةمئاق



روهظ ةداعإ نكمي ال"،! فرحلما ادختسا دنع هنا إلى OpenSSL عقوم ريشي: ةطحالما
نأ اذه ينعي ال". حيرص لكشب اهركذمت اذإ ىتح ةمئاقلا يف ةفوذحملما تارفشملما
طبخ ةرفشلما نم ريسفت قاطن إلى ريشي وه، ماظنلما نم ايئاهن فوذحملما ةرفشلما

ددحم ريفشت ليطعت

مساو،- وأ! ةمالعو، لصافلا: ةيضارتفالما ةلسلسلا قاحلاب مق، ددحم ريفشت ليطعتل
ةيمست قيسنت ريفشتلما مسا عيطي نأ بجي. اهليلطعت متيس يتلما ريفشتلما
ةجاحب تنك اذإ، لاثملا لابس ىلع. [OpenSSL ريفشت](#) ةرادا ةحفص يف رفوتملما، OpenSSL
لثم ريفشت ةلسلسل نيوكتب مقف، SIP تالاصتال AES128-SHA ريفشت ليطعت ىلإ
هذه:

<#root>

ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH

:!AES128-SHA

> نام أال > ةنايصالا إلإ ح ف ص تو ، Expressway في بيولا ةرادا ةح ف ص إلإ ل ق ت نا ، كل ذ د ع ب ر ق نا و ، بول ط م ل ا (ت ا ل و ك و ت و ر ب ل ا) ل و ك و ت و ر ب ل ل ة ص ص خ م ل ا ة ل س ل س ل ا ت ن ي ع و ، ر ي ف ش ت ل ا ، ل ا ث م ل ا ا ذ ه ي ف . م ا ط ن ل ل ا ل ي غ ش ت ة د ا ع إ م ز ل ي ، د ي د ج ل ا ن ي و ك ت ل ا ق ي ب ط ت م ت ي ي ك ل . ط ف ح ق و ف SIP TLS: ت ا ر ف ش ب ج و م ب SIP ل و ك و ت و ر ب إ ل ع ة ص ص خ م ل ا ة ل س ل س ل ا ن ي ي ع ت م ت ي

Status > System > Configuration > Applications > Users > Maintenance >

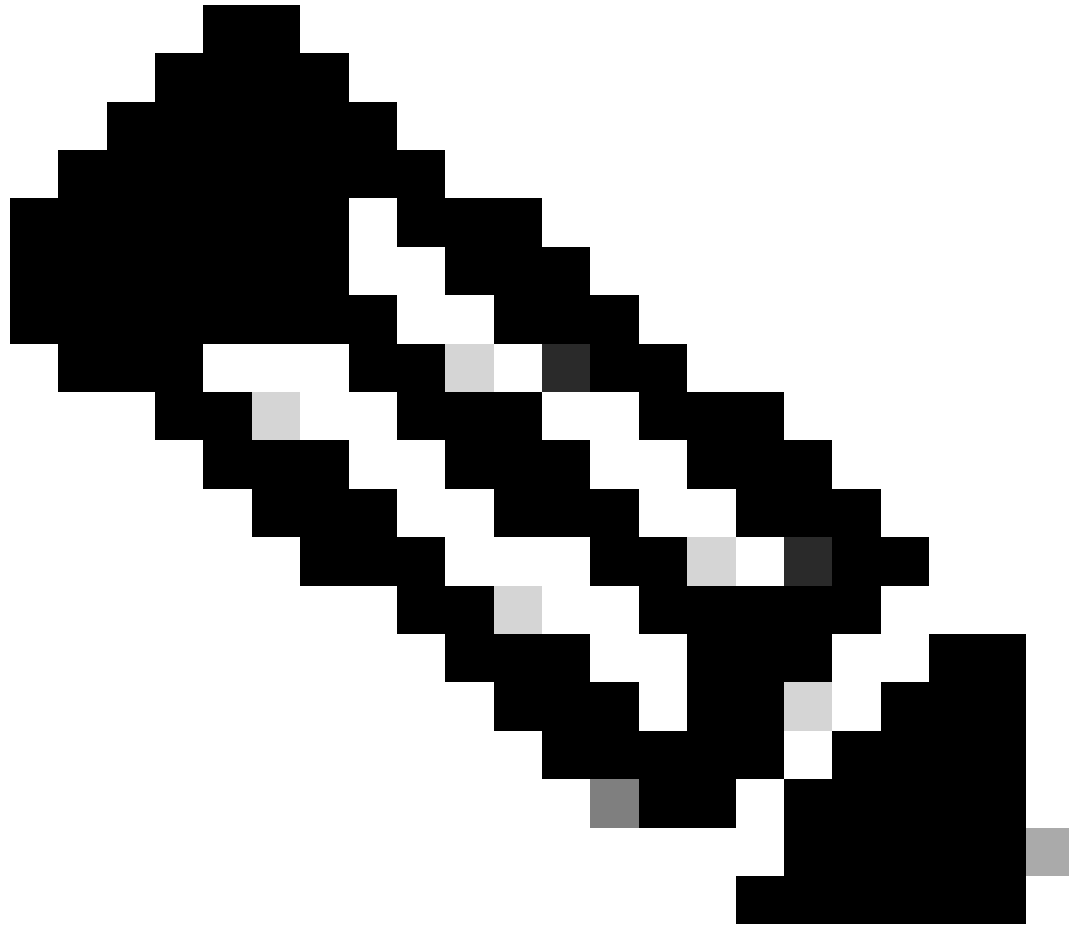
Ciphers

Configuration

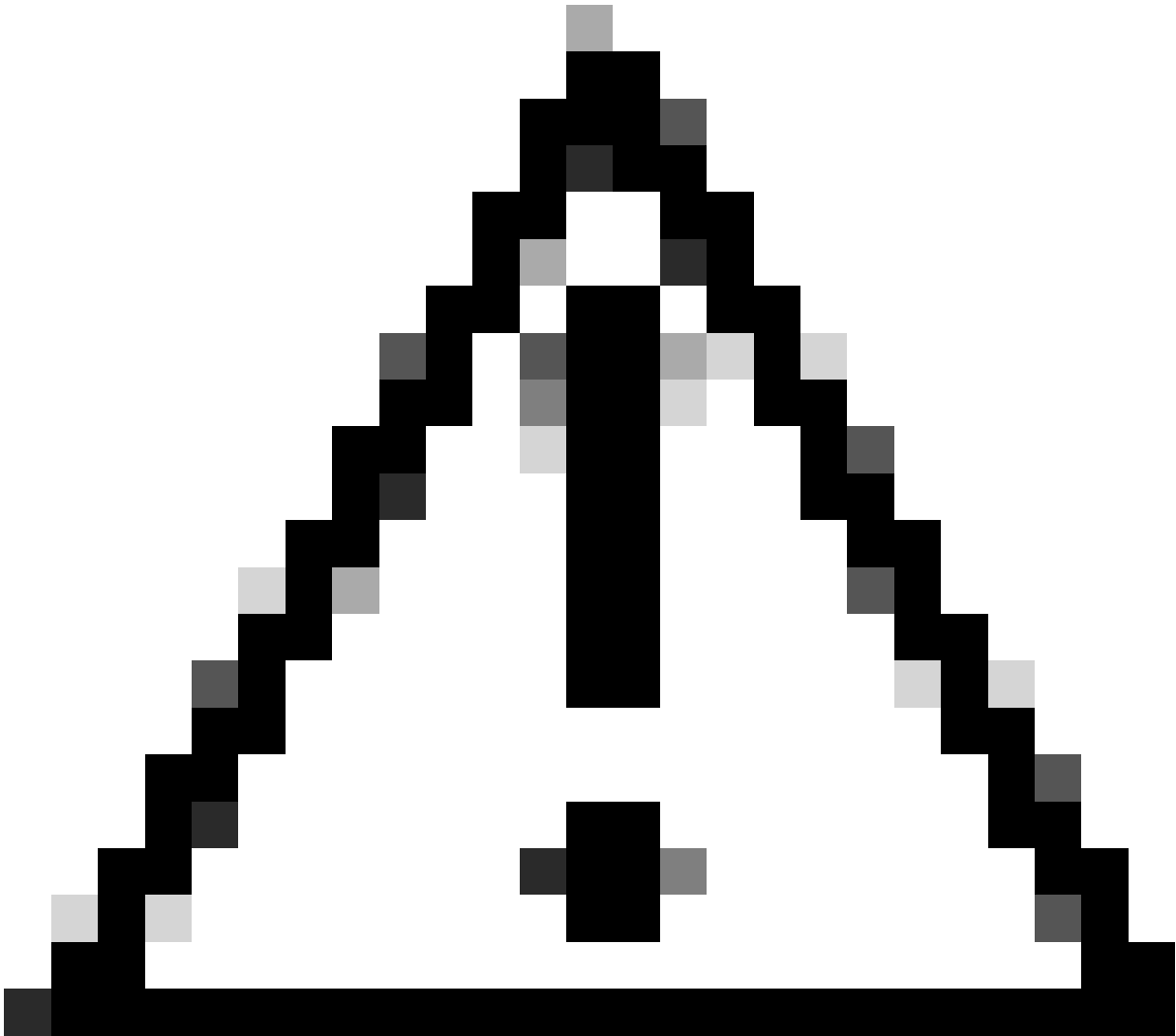
HTTPS ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
HTTPS minimum TLS version	TLS v1.2
LDAP TLS Ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
LDAP minimum TLS version	TLS v1.2
Reverse proxy TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
Reverse proxy minimum TLS version	TLS v1.2
SIP TLS ciphers	IMEDIUM:LOW:3DES:1MD5:IPSK:! !eNULL:! !eNULL:! !aDH:! !AES128-SHA
SIP minimum TLS version	TLS v1.2
SMTP TLS Ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
SMTP minimum TLS version	TLS v1.2
TMS Provisioning Ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
TMS Provisioning minimum TLS version	TLS v1.2
UC server discovery TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
UC server discovery minimum TLS version	TLS v1.2
XMPP TLS ciphers	EECDH:EDH:HIGH:-AES256+SHA:IMEDIUM:LOW:3DES:1MD5:IPSK:!
XMPP minimum TLS version	TLS v1.2

Save

Expressway Web Admin لخدم إ ل ع ر ي ف ش ت ل ا ت ا د ا د ع إ ة ح ف ص



يُساس ألام داخل اللى ع تاريخي غتلا ءارجاب مق، Expressway ءومجم ءلاح يف : ءطحال م
ءومجم لام اظن ءاضعأ يقاب لىل ءلام تم اءسن ءىءال نىوكتلا ءسن مءى . طقف



[رشن لیلید](#) ڤی دراولا هب ڤصوملا ةعومجملا لڤغشت ةداعا لسلست مدختسا: رڤذحت ڤساسالا مداخال لڤغشت ةداعا ڤأڤا. [اهتنا ڤڤو Cisco نم Expressway ةعومجم ؤاشنا](#) ةمئاق لاق و رڤظن لك عم لثم لڤاب مق مٲ، بڤولا ةهجا و ربع هڤلا لوصولا رظتنا و ؤمجتلا > ماظنلا نمض اهنڤوكت مٲ ڤتلا

ةماع ةڤمزر اوخ ماڤختسا ب رڤفشتلا نم ةعومجم لڤطعت

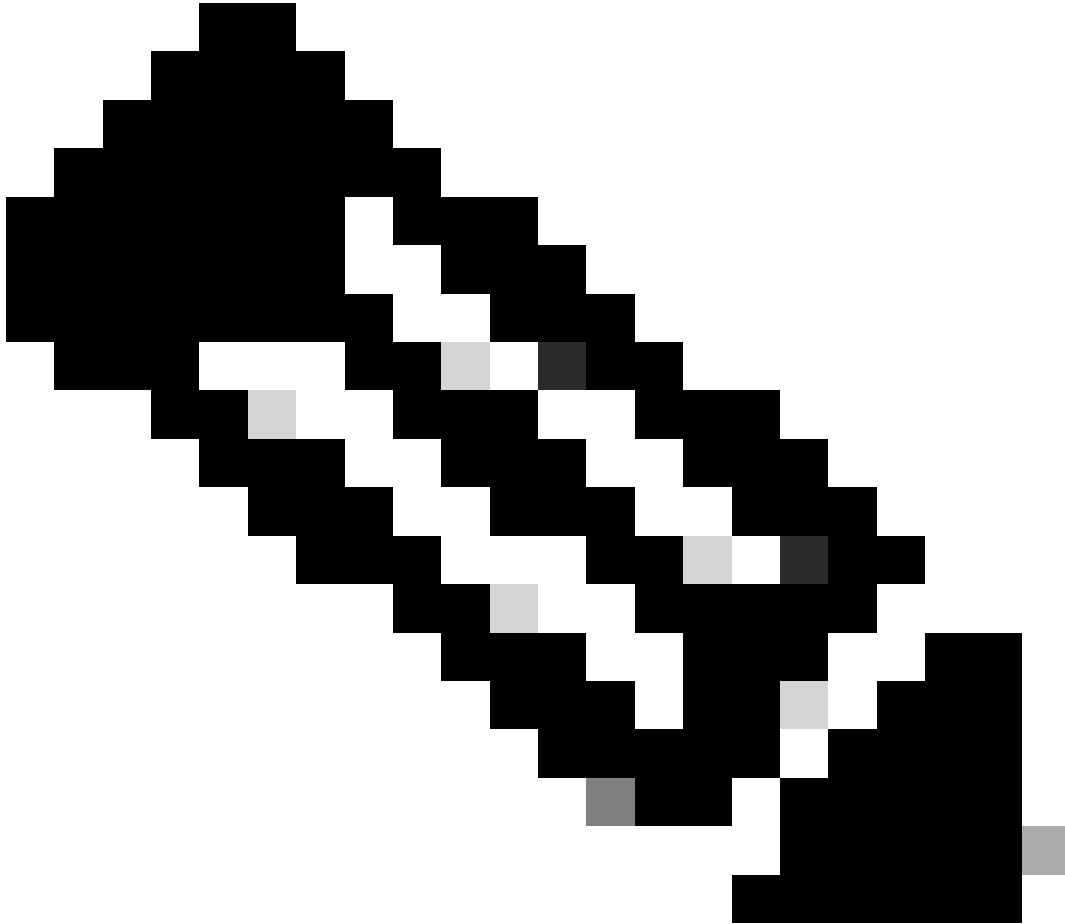
ةلسلسل قاح لڤ مق، ةكرتشم ةڤمزر اوخ ماڤختسا ب تارفشملا نم ةعومجم لڤطعتل ؤامسا رڤوتت. اه لڤطعت مٲس ڤتلا ةڤمزر اوخلا مسا و، - و!، لصالا: ةڤضارتفالا ؤاچب تنك اذا، لالم لڤبسلع. [OpenSSL رڤفشت](#) ةرادا ؤحفصل ڤم و ؤدملا ةڤمزر اوخلا رڤفشت ةلسلسل نڤوكت ب مق، DHE ةڤمزر اوخ مدختسا ڤي ذلا رڤفشتلا ؤمجم لڤطعت ڤلا هذله لثم:

```
<#root>
```

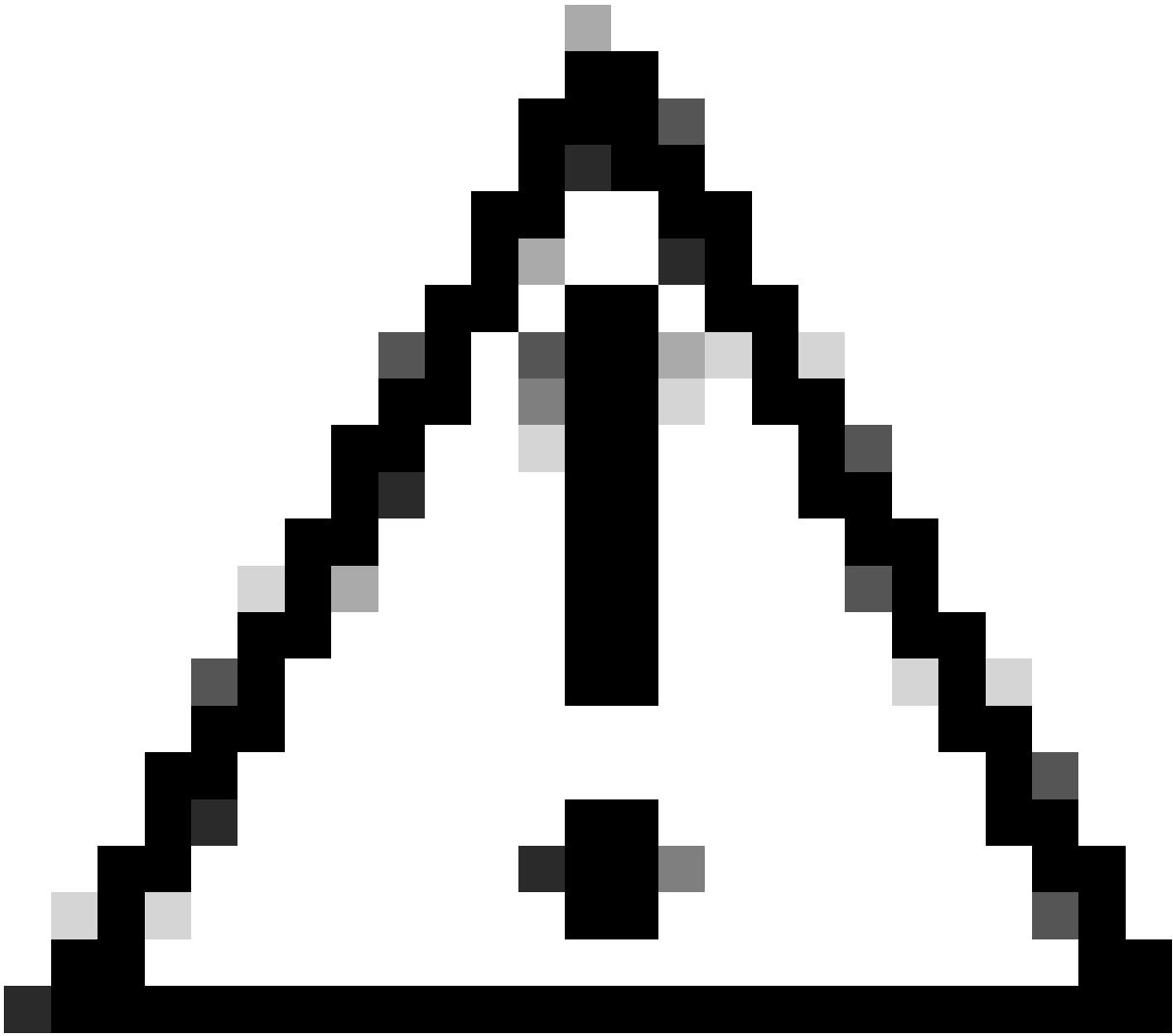
```
EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
```

```
:!DHE
```

تارفشلا > نامألا > ٲنايصللا ىلإ ءفصتو ، Expressway Web Admin ءففص ىلإ لقتنا
قوف رقناو ، ٲولطملا (تالوكوتورٲلا) لوكوتورٲلل ءصصءملا ءلسلسلا تنىعو
ماظنلا لىغشت ءءاعإ مزلى ، ءىءللا نىوكتلا قىٲٲت مئى كل . ظفء



ىساسألا مءاءلا ىلء ءارىىىءتلا ءارءاب مق ، Expressway ءومءم ءلاء ىف : ءظءالم
ءومءملا ماظن ءاضءأ ىقاب ىلإ الءامءم اءسن ءىءللا نىوكتلا ءسن مئى . طقف



[رشن لیلید](#) ېف دراوالا هب یصوملا ةعومجملا لیغشت ةداعا لسلسلست مدختسا: ریدخت
، یساسألا مداخال لیغشت ةداعاب ادبا. [اهتنا یصو Cisco نم Expressway ةعومجم ءاشنا](#)
ةمئاق لل اقو ریظن لك عم لثملاب مق مث ، بیولا ةهجاو ربع هیلا لوصولا رظتناو
عیمجتلا > ماظنلا نمض اهنیوكت مت یتلا

ةحصلال نم ققحتلا

ریفشتلا ةلسلس لبق نم اهب حومسمل ریشفتلا ةمئاق صحف

openssl ciphers -V "<cipher string>" رمألا مادختساب ةصصخملا ریشفتلا ةلسلس صحف كنكمی
تاریفتلا دعب اچردم دعی مل بوغرملا ریغ ریشفتلا نأ نم دكأتلل تاچرخملا عچار .
EECDH:EDH:HIGH:- ریشفت ةلسلس صحف متی ، لاثملا اذه یف
تاچرخم دكؤت . AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!PSKNULL:!aNULL:!aDH:!DHE.
DHE: ةیمزراوخ مدختسی یذلا ریشفتلا نم یأ حمست ال ةلسلسلا نأ رمألا

<#root>

```

~ # openssl ciphers -V "ECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH
:!DHE
"
0x13,0x02 - TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD
0x13,0x01 - TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0xAD - ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0xAC - ECDHE-ECDSA-AES128-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
0xC0,0x09 - ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
0xC0,0x13 - ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
0x00,0x9D - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x9D - AES256-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(256) Mac=AEAD
0x00,0x9C - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x9C - AES128-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(128) Mac=AEAD
0x00,0x3D - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
0x00,0x3C - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
0x00,0x2F - AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
~ #

```

لطمع ريفشت ىلع ضوافت لابس TLS لاصتا رابتخا

ريفشت مادختساب لاصتا ةلواحم ضفر نم ققحت لل openssl s_client رم ال مادختسا كنك مي رايخ مدختساو، كب صاخلا ذفنم لابل او Expressway ناو نع ديدحتل لاصتا رايخ مدختسا. لطمع انثا ليمع لاةطساوب اهن اشب ضوافت لامتيس يت لاةيدر فل ةرفش ل ديدحتل ريفشت ل TLS: ةحفاصم

```
openssl s_client -connect <address>:<port> -cipher <cipher> -no_tls1_3
```

هه ىلع تبثم Windows رتوي بمك نم Expressway ب TLS لاصتا ةلواحم متت، لاثم ل اذه يف ريفشت ىلع ضوافت لابل ال، ليمع لاهرابتع اب، يصخش ل رتوي بمك ل موق ي ال OpenSSL. DHE-RSA-AES256-CCM ةيمزراوخ مدختسي يذلاو، هه يف بوغرم ل ريفغ

```
<#root>
```

```
C:\Users\Administrator>
```

```
openssl s_client -connect exp.example.com:443 -cipher DHE-RSA-AES256-CCM -no_tls1_3
```

```
Connecting to 10.15.1.7
```

```
CONNECTED(0000154)
```

```
D0130000:error:0A000410:SSL routines:ssl3_read_bytes:
```

```
ssl/tls alert handshake failure
```

...\ssl\record\rec_layer_s3.c:865:

SSL alert number 40

no peer certificate available

No client certificate CA names sent

SSL handshake has read 7 bytes and written 118 bytes

Verification: OK

New, (NONE), Cipher is (NONE)

Secure Renegotiation IS NOT supported

No ALPN negotiated

SSL-Session:

Protocol : TLSv1.2

Cipher : 0000

Session-ID:

Session-ID-ctx:

Master-Key:

PSK identity: None

PSK identity hint: None

SRP username: None

Start Time: 1721019437

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

C:\Users\Administrator>

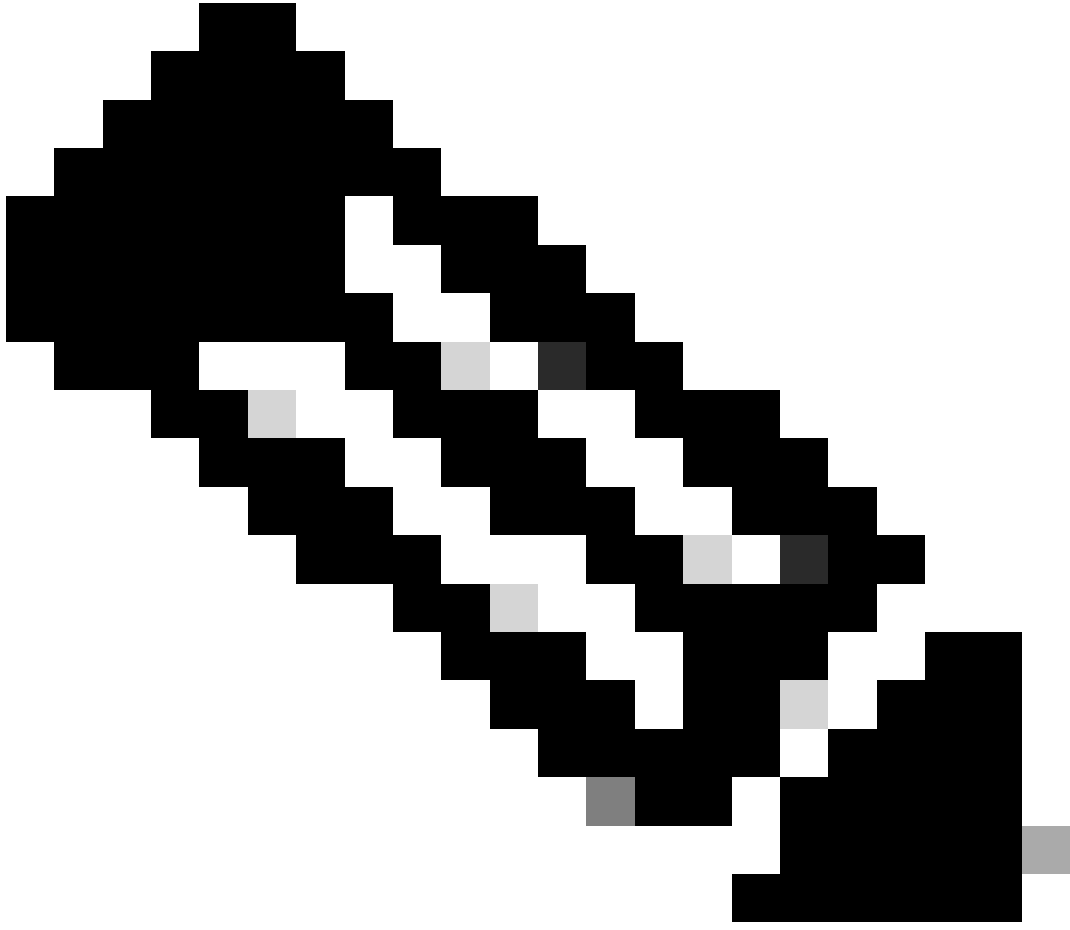
لاصتا ديكات لشف عم لاصتالا ةلواحم رمألا جارخا! ضرعي

"SSL/TLS":...\ssl\record\rec_layer_s3.c:865:SSL مقور 40، هي بنتل ارظن، Expressway ني وكتل ارظن،

EECDH:EDH:HIGH:- مادختسال

ةلسلس ريفشت AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK!eNULL:!aDH:!DHE

ةيمزراوخ مدختست يتل تارفشملا ل طعي يذلا، HTTPS تالاصتإ DHE.



مدختست يتلا تارابتخالال لمعت يكل رمألا لىل -no_tls1_3 راىخلا ريرمت مزلي :ةظحال م
ةرفش جارداپ ليمعلا موقى ،انمضتم نكي مل اذا .حضوم وه امك openssl s_client رمألا
ClientHello: ةمزح يف ائاقلت TLS 1.3

Urgent Pointer: 0

- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (247 bytes)
- Transport Layer Security
 - TLSv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 242
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 238
 - Version: TLS 1.2 (0x0303)
 - Random: 19ec4e8994cc334599cf889d4e45a812029589923c4cfcf2cef6b6fc47ec2840
 - Session ID Length: 32
 - Session ID: e0d17cb402229aa46cab70b6a637ce38d9b5a228c7b360cb43f49086ce88d5df
 - Cipher Suites Length: 10
 - Cipher Suites (5 suites)
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
 - Compression Methods Length: 1

Ciphers automatically inserted by the openssl s_client command

Cipher passed with the -cipher option

اي اقل اهتفاضل تم تارفش عم ClientHello مة زح

نم الدب اهنم ةدحاو راي تخ | نكم مي ، تارفش ل ك لت م عدي فده ل عي رس ل ا قير ط ل ا ناك اذ | ل ا ك دوق ي ن ا نكم مي ي ذل او ، حجان ل اص ت ال ا . ا ه ر اب ت خ | ل ا ج ا ت ح ت ي ت ل ا ة د ح م ل ا ة ر ف ش ل ا | ل ا ه ر ي ر م ت م ت ي ذل ا ل ط ع م ل ا ر ي ف ش ت ل ا م ا د خ ت س ا ب ا ن ك م م ن ا ك ل ا ص ت ال ا ن ا ب د ا ق ت ع ال ا | ل ا -cipher - راي خ ل ا م ا د خ ت س ا ب ر م ال ا

ل ط ع م ر ي ف ش ت م ا د خ ت س ا ب T L S ة ح ف ا ص م ن م ة م ز ح ط ا ق ت ل ا ص ح ف

ل اص ت ا ر ا ب ت خ | ا ر ج | ا ن ث ا ، Expressway ن م و ا ر ا ب ت خ ال ا ز ا ه ج ن م ، ة م ز ح ط ا ق ت ل ا ع ي م ج ت ك ن ك م ي ن م د ي ز م ل Wireshark م ا د خ ت س ا ب ه ص ح ف ذئ د ن ك ن ك م ي . ل ط ع م ل ا ر ي ف ش ت ل ا د ح ا م ا د خ ت س ا ب ة ح ف ا ص م ل ا ث ا د ح ا ل ل ي ل ح ت .

ل ي ل ع ط ق ف ض و ا ف ت ت ا ه ن ا ن م د ك ا ت . ر ا ب ت خ ال ا ز ا ه ج ة ط س ا و ب ه ل ا س ر ا م ت ي ذل ا ClientHello ن ع ث ح ب ا ة DHE م ي م ز ر ا و خ م ا د خ ت س ا ب ر ي ف ش ت ، ل ا ث م ل ا ا ذ ه ي ف ، ب و غ ر م ل ا ر ي غ ر ا ب ت خ ال ا ر ي ف ش ت

Wireshark interface showing a network capture on 'Ethernet0'. The packet list pane displays several packets, with packet 327 highlighted in blue. The packet details pane shows the structure of the Client Hello message.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
324	2024-07-14 23:00:32.459025	10.15.1.2	28872	10.15.1.7	443	TCP	66	28872 → 443 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
325	2024-07-14 23:00:32.459666	10.15.1.7	443	10.15.1.2	28872	TCP	66	443 → 28872 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
326	2024-07-14 23:00:32.459760	10.15.1.2	28872	10.15.1.7	443	TCP	54	28872 → 443 [ACK] Seq=1 Ack=1 Win=4204800 Len=0
327	2024-07-14 23:00:32.460733	10.15.1.2	28872	10.15.1.7	443	TLSv1.2	172	Client Hello
328	2024-07-14 23:00:32.461070	10.15.1.7	443	10.15.1.2	28872	TCP	60	443 → 28872 [ACK] Seq=1 Ack=119 Win=64128 Len=0
329	2024-07-14 23:00:32.461855	10.15.1.7	443	10.15.1.2	28872	TLSv1.2	61	Alert (Level: Fatal, Description: Handshake Failure)
330	2024-07-14 23:00:32.461855	10.15.1.7	443	10.15.1.2	28872	TCP	60	443 → 28872 [FIN, ACK] Seq=8 Ack=119 Win=64128 Len=0

Packet 327 details:

- Acknowledgment number (raw): 3235581935
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window: 16425
- [Calculated window size: 4204800]
- [Window size scaling factor: 256]
- Checksum: 0x16b7 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (118 bytes)
- Transport Layer Security
 - TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 113
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 109
 - Version: TLS 1.2 (0x0303)
 - Random: e5cb04a72ae567a0963c5a4a5901db3720fabcf5980aa2ef5a5ecc099254c1bf8
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - Cipher Suites (2 suites)
 - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc03f)
 - Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
 - Compression Methods Length: 1

Wireshark يف ClientHello ةمزمح لىل لاثم

:

اذه يف .لاصتالاض فر عم ،ةرطخ TLS هيبنت ةمزمح مادختساب Expressway ةباجتسا ديكأت اهنويوكت مت DHE ةرفش ةلسلس لكل DHE تارفش معدت ال Expressway نأل ارظن ،لاثملال 40 لشفال زمر لىل يوتحت ةلتاق TLS هيبنت ةمزمح عم بيچتست اهنإف ،HTTPS لوكوتوربل

Wireshark interface showing a network capture on 'Ethernet0'. The packet list pane shows several packets, with packet 329 highlighted in red. The packet details pane for packet 329 is expanded, showing the following information:

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
324	2024-07-14 23:00:32.459025	10.15.1.2	28872	10.15.1.7	443	TCP	66	28872 → 443 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
325	2024-07-14 23:00:32.459666	10.15.1.7	443	10.15.1.2	28872	TCP	66	443 → 28872 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
326	2024-07-14 23:00:32.459760	10.15.1.2	28872	10.15.1.7	443	TCP	54	28872 → 443 [ACK] Seq=1 Ack=1 Win=4204800 Len=0
327	2024-07-14 23:00:32.460733	10.15.1.2	28872	10.15.1.7	443	TLSv1.2	172	Client Hello
328	2024-07-14 23:00:32.461070	10.15.1.7	443	10.15.1.2	28872	TCP	60	443 → 28872 [ACK] Seq=1 Ack=119 Win=64128 Len=0
329	2024-07-14 23:00:32.461855	10.15.1.7	443	10.15.1.2	28872	TLSv1.2	61	Alert (Level: Fatal, Description: Handshake Failure)
330	2024-07-14 23:00:32.461855	10.15.1.7	443	10.15.1.2	28872	TCP	60	443 → 28872 [FIN, ACK] Seq=8 Ack=119 Win=64128 Len=0

The packet details pane for packet 329 shows the following structure:

- Frame 329: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface \Device\NPF_{122607A1-10A8-47F6-9069-936EB0CAAE1C}, id 0
- Ethernet II, Src: VMware_b3:5c:7a (00:50:56:b3:5c:7a), Dst: VMware_b3:fe:d6 (00:50:56:b3:fe:d6)
- Internet Protocol Version 4, Src: 10.15.1.7, Dst: 10.15.1.2
- Transmission Control Protocol, Src Port: 443, Dst Port: 28872, Seq: 1, Ack: 119, Len: 7
 - Source Port: 443
 - Destination Port: 28872
 - [Stream index: 2]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 7]
 - Sequence Number: 1 (relative sequence number)
 - Sequence Number (raw): 3235581935
 - [Next Sequence Number: 8 (relative sequence number)]
 - Acknowledgment Number: 119 (relative ack number)
 - Acknowledgment number (raw): 810929090
 - 0101 = Header Length: 20 bytes (5)
 - Flags: 0x018 (PSH, ACK)
 - Window: 501
 - [Calculated window size: 64128]
 - [Window size scaling factor: 128]
 - Checksum: 0x163f [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - [Timestamps]
 - [SEQ/ACK analysis]
 - TCP payload (7 bytes)
- Transport Layer Security
 - TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)
 - Content Type: Alert (21)
 - Version: TLS 1.2 (0x0303)
 - Length: 2
 - Alert Message
 - Level: Fatal (2)
 - Description: Handshake Failure (40)

Wireshark يي ةريطخ TLS هئي بنت ةمزح

ةلص تاذا تامول عم

- [OpenSSL تارفيش ةرادا](#)
- [Cisco Expressway \(X15.0\) لوؤسم لي ليد](#) - نامألا ةرادا :لص فال - ريفش تالا تا عومجمو TLS رادصل

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل