

SWG عقوم ىلإ لوصولا ءاطخأ فاشكتسا اهحالصإو

تايوتحمل

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[تانايبالا قفدت رطخ ببسب "403 أطح ببسب لوصولا ضفرمت"](#)

[Java يف ةلكشم ببسب "403 أطح لب لوصولا ضفر"](#)

[ةلأسملل ىوتسملل ىلإاع ىرذجلا ببسلا](#)

[؟ناملربلا ءاضعأ عم افاجب ةقلعتملا ةلكشملا يه ام](#)

[بارق](#)

[502 Bad؟ ةرابع يه ام](#)

[502 Bad Gateway ل ةعئاش لماع](#)

[ةمومدملا ريغ SWG ريفشت تاعومجم](#)

[بارق](#)

[لبىمعللا ةداهش ةقداصم بلط](#)

[لىكوللا ةطساوب اهتفاضلا تمت سوفر](#)

[بارق](#)

ةمدقملا

اهتيؤر مت يتللا بيولا عقوم ىلإ لوصولا ءاطخأ فاشكتسا ةيفيك دنتسملا اذه حضوي
اهحالصإو Umbrella Secure Web Gateway (SWG) لىك و مادختساب.

ةيساسأ تامولعم

امدنعو SWG لىك و ربع هيلإ لوصولا نكمي ال www.xyz.com بيولا عقوم نأ ضررت فن انعد
(ةروصلال ي Umbrella SWG دوجو نود) ةرشابم تنرتنإلا ىلإ لوصولا نومدختسملا لواحي
ةفلتخمللا أطحلا لئاسر عاونأو ةفلتخمللا ضارعالأ عجارن انعد .ديج لكشب لمعي اذه نإف
يه اعويش رثكالأ SWG ربع بيولا عقوم ىلإ لوصولا نكمي ال امدنع اهنع غالبالا مت يتللا
مت ،مداخلا ةداهش لاطبالا مت ،مداخلا ي ف ةلاسرا أطح ليحرت 502 ىلع رذعت ،ةئيس 502 ةرابع
تقول نارودلا دعب بيولا عقوم ةلهم ديدحت مت ،مداخلا ةرفش قباطت مدع ،403 لوصولا ضفر
هباش ام وأ ام .

قفدت رطخ ببسب "403 أطح ببسب لوصولا ضفرمت" تانايبالا

مكحتلا وأ SWG لىك و جورخب ةصاخلا IP تاقاطن رطحب مداخلا بناج وأ WebServer مداخ موقبي
هذه لجل SWG لخدملا IP تاقاطن ضعب رطحب Akamai WAF ماق ،لاثملا لىبس ىلع .اهي ف
رطخ ءاغلإ ىلع مهرا بجاو بيولا عقوم يلوؤسم ىلإ لوصولا وه طقف راخلا نوكي ،ةلكشملا

تالاجم الةراداةمئاق مادختساب SWG زواجتب مق ،نجل كلذىتح .انب ةصاخ ال IP تاقاطن نم عونل اذه عجرى ال ،راصتخابو .PAC و AnyConnect SWG تافل م رشن تايلمعل ةجراخل انه .ببول مداوخو لىكول مداوخ نب قفاوتل مدع لىل لب ،هسفن لىكول لىل لكاشم ال .جرخم ال IP ةلتك ببسب "403 لوصول اضفر" أطخل اديدت kb لىل لىل رىش نأ طبارل

ياماكأ مايقل ةلمتحم ال بابسأل اضعب يطغى يذل [طبارل](#) لىل امىف ،كلذىل ةفاضل باب ةجرم ال IP نىوانع رطحب .

Java يف ةلكشم ببسب "403 أطخل لوصول اضفر"

نامأ ةرابع أطخ - عونمم 403 وأ لوصول اضفر" ةرابع لاسراو ببول عقوم لىل لوصول نكمى ال .تافل ملل صحف دادعإ نىكمت عم SWG MPS لىكوربع بلطل لاسرا دنع "Umbrella ةباحس عقوم الانعضو اذا وأ .حاجنب ببول عقاوم لىمحت مئى ،تافل ملل صحف لىطعت ةلاح يف نكلو .حاجنب عقاوم لىمحت ،ببناج رىفش ك فى

ةلأسم لل ىوتسم ال ىلاع ىرذجل ببسب ال

؟نامل لربل ااضعأ عم افاجب ةقلعتم ال ةلكشم ال ىه ام

ةرم SSL وأ SNI هىبنتب قلعتى امىف TLS رىذحت عاجراب ىنعم ال ببول وأ عقوم ال مداوموقى لىسرى نأ دعب ثدحى اذه ،اساسأ .مداخل لب لاصلتال لىكول لواحى نأ دعب لىكول لىل ىرخأ هناف ،مىمصتال لالخم نم (وحنل اذه لىلعو Java لىل دمئعى يذل) MPS لىكول .ابحرم لىمعل لىلحت ءانثأ أطخ هناف لىل فصول لىل فى "فورعم رىغ مس" ب TLS تاهىبنتب ىل عم لماعتى [انه](#) لىل صافتال نم دىزم لىل روثعل م .ةلماعم ال ىهتنبو SNI

ىل وأ SWG عم ضراعت لىل نم دحاو اذه .MPS وأ SWG لىكول ةلكشم تسىل هذه ناب ملعل عاجرل رىذحتل اذه تاضرعتسم ال لهاجتت ام ةداع .بناج مداخل لىل misconfiguration ببسب لىكورخأ ىهتنبو حذاف أطخ هناف لىل SSL رىذحت عم لماعتى رخأ ىوتحم نامأ ةىفصت لماع وأ SWG نكلو أطخ نع غالب ال اضىل هنىكمى .نىمدختسم لل ةروطحم أطخ ةحفص 403 هنع جئنب امم ،ةسلجل وه امك ،403 عونمم أطخ وه هانبار ام نوكل ةلثمال مطعم عم نكلو ،502 ةحىحص رىغ ةرابع ةروصل هذه فى حضوم

403 Forbidden

Umbrella Cloud Security Gateway

15151734443924

ةقبط ةجلاعم ةىففى لىل مكحت ىل كللمى ال هناف ،تاقىبطلتال ققبط فى لمعى MPS نأ امب مداخل ةىلوؤسم نم .TLS لوكتورب فى اهجاتن مئى ىتال تاهىبنتل لىل ءانب ةكرلل TLS .[طابتال](#) اذه لىل عوجرل ىجرى .حىحص لكشب TLS تاداهش/ةياهن ةطقن نىوكت نامض

[ربتخم](#) نم ةلوهسب اهىل ةراش ال نكمى ،اهالصلو اهئاطخأ فاشكتسأ وأ ةلكشم ال لىلقتل [SSL](#).

[Java 7u25](#)

Client aborts on SNI unrecognized_name warning

RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1

[Java 8u161](#)

Client aborts on SNI unrecognized_name warning

RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1

[Java 11.0.3](#)

Client aborts on SNI unrecognized_name warning

RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1

[Java 12.0.1](#)

Client aborts on SNI unrecognized_name warning

RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1

15152060146964

هزواجت وأ HTTPS صحف فصتنم في SWG ليك ونودب بيول عقوم إلى لوصول متي امندن ع هيلع فرعتالم ريغ SNI مسا هيبننت لهاجتي ضرعتسمال نأل بيول عقوم لمعي، SWG نم بيول مداخل لاصلتالي في رمتسيو.

نأ نكمم فيفخت لصفأ وه ب صومال ليدبال لجال ناك، ةلاقمل هذه ةباتك تقوي في هذه ةللام اننكممي، ةديجال ليكول ةينب عمو، بيرقلا لبقستسمال في. كيلى محترقن ةقانأ رثكأ لكشبتالكشمال

رارق

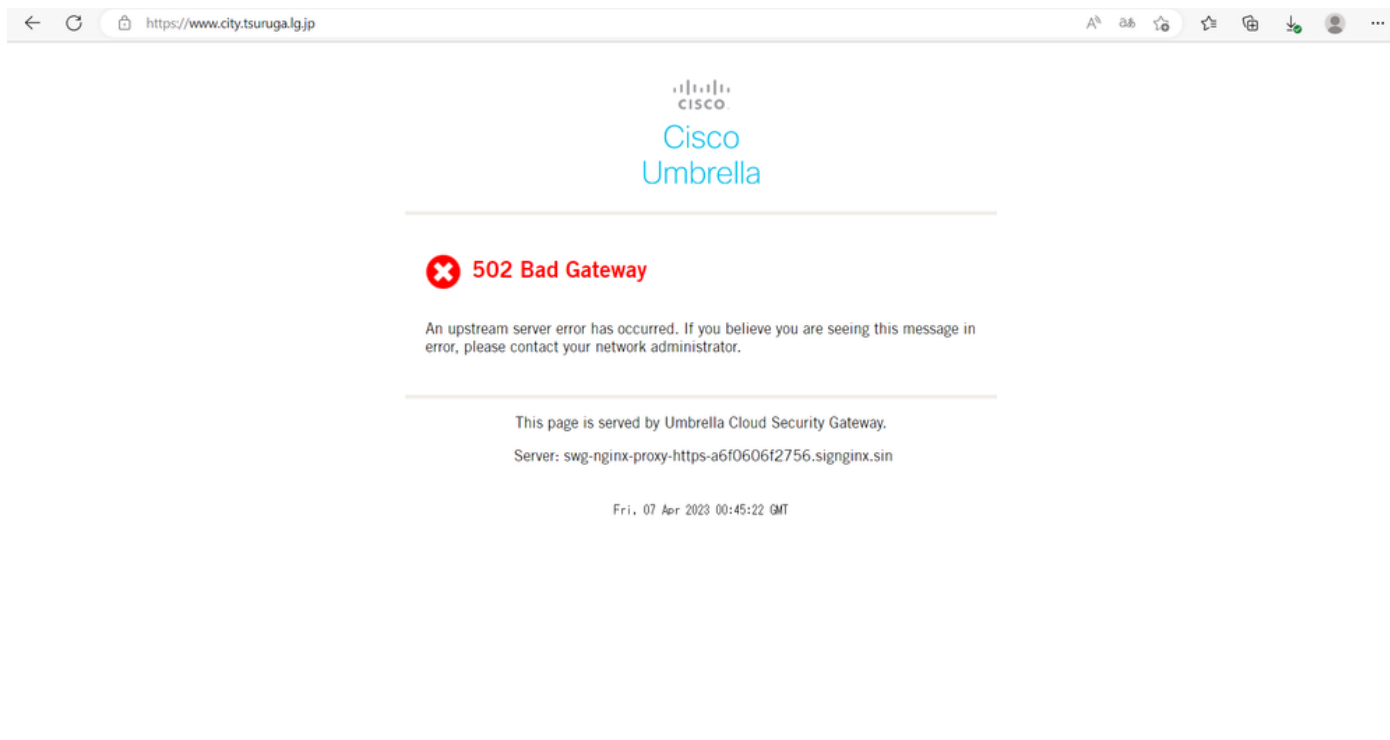
1. وأ - ةرثأتمال تالاجملل زيمرتال كف ليطعت.
2. (عقوملاب قثت تنك اذا) حامسال ةدعاق نارقإو ةهجال ةمئاق إلى لاجمل ةفاضإ.

502 Bad? ةرابع يه ام

ريغ ةباجتسإ ىقلتوليكو وأ ةباوبك لمعي ناك مداخل نأ 502 ةحيحص ريغ ةرابع أطخ ينعلي ليكو ربع بيول عقوم إلى لوصول مدختسمال لواحي امندن ع. مداخل مداخل مداخل نم ةحيحص لاصلتالا نم ناعفدت ثدحي، SWG.

(مداخل نم) ليكول لاصلتا → ليمعال أ)
(ليمحتلل) يفرطال بيول مداخل لاصلتا → ليكول ب)

مداخل لاصلتا ءاهنإل SWG (MPS، NGINX) ليكو ني ب 502 Bad ةرابع أطخ ثدحي.



502 Bad Gateway لةعئاش لماروع

موضوع دملاريغ SWG ريفش تاعومجم

رماً Curl نم لاثم

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

```
: - curl -v www.xyz.com:80
```

Mac/Linux:

```
- curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows:

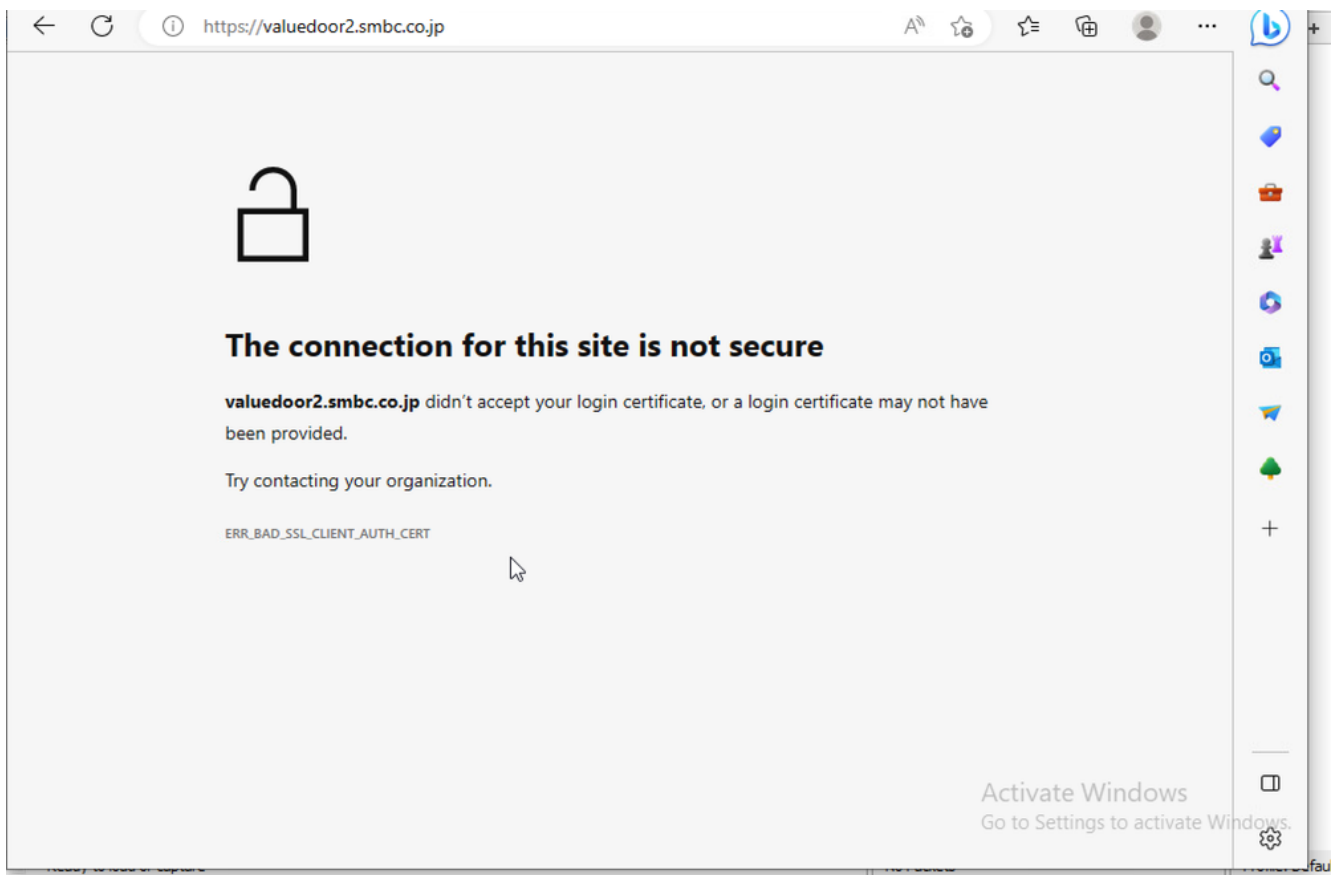
```
- curl -vvv -o null -k -L www.cnn.com
```

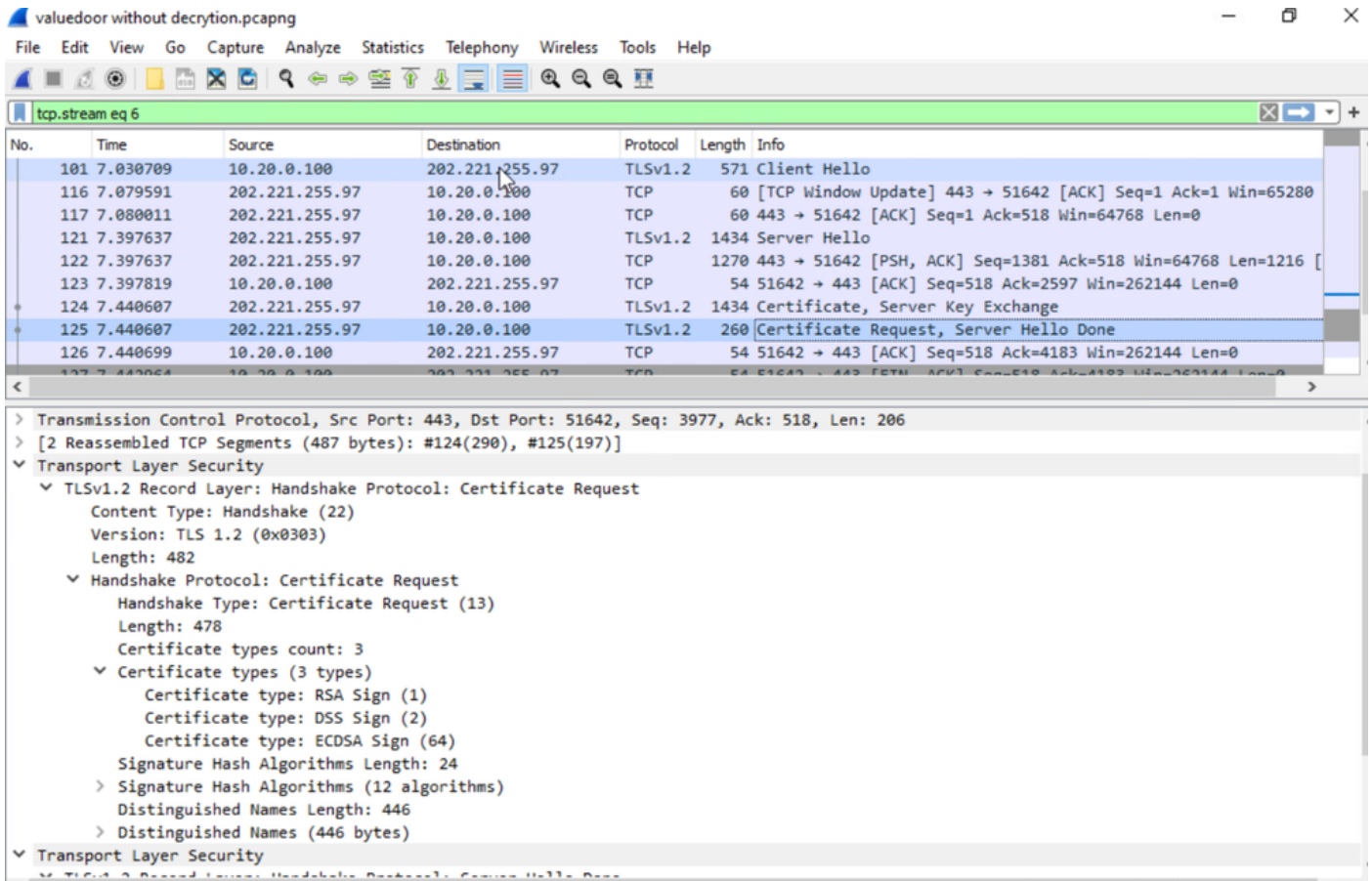
رارق

ك ف ةمئاق مادختساب لكاشم لل ريثم ل بيولا عقوقم ل صفال ي طخت ب مق ،ةلكشم ل حل
يئاقئنا ل ري فشت ل

ليمعل ةداهش ةقداصم بلط

ةقداصم تانايب ل قفدت بيو م داخ عقوقتي ،م داخ ل و SWG ليكو ني ب TLS ةحفاصم ءانثأ
نم تالاجم ل هذه زواجت ل اجاتحن ،ةم و عدم ريغ ليمعل ةداهش ةقداصم نأ امب . ليمعل ةداهش
يلع . طقف https صف زواجت ي فكي الو ،ةي ج راخ ل تالاجم ل ةرادا ةمئاق مادختساب ليكول
ل اثم ل لي بس : <https://valuedoor2.smbc.co.jp>.





15027192992276

ليكوللا ةطساوب اهتفاضل تامت سوؤر

X-Forward-For س أ ةفاضل ببسب 502 ةححص ريغ ةرابع أطخ نع غالبالب بيولا مداخ موقري لكاشم مطعم قييضي اننكمي HTTPS صحف نيكمت دنن SWG ليكو ةطساوب (XFF) اهالصلو ةلكشم ال فاشكتسأ قيرط نع ةلوهسب 502 اهددع غالبالب ةححص ال ريغ تارابع ال حسم ةلكشم داعبتس ال هنودب وأ تافللم ال صحفبو، هنودب وأ HTTPS صحف مادختساب ال MPS ليكو مادختساب تافللم ال.

```
vaishraj@VAISHRAJ-M-QJW4 ~ % curl https://www.monoprice.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 502
vaishraj@VAISHRAJ-M-QJW4 ~ % curl https://www.monoprice.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

مداخ ال مداخ ال مداخ ال مداخ ال نكمي ثيحب، HTTPS صحف ليغشت دنن XFF س أ مدختسن نحن مدختس ال عقوم رفوي يذل) لي م ال IP ال ادانتسا لثم ال فارغ ال عقوم ال وتحم ري فوت (لي لعل ال).

أطخ دجوي ال كلذل، ليكول ةطساوب سألل اذه ةفاضل متت ال، HTTPS صحف نيكم ت مدع دن ع بيوم داخ ل لأطخ ل اذه ببس عجري . SWG ليكولة كش م تسيل هذو . 502 ةحيحص ريغ ةراب ع يسايقل XFF سألر دامتعا مدعل حيحص ريغ لكشب هنيوكت مت يذل قفدت لل

رارق

كف مئاقق مادختساب ةنيعم (تالاجم) لاجمل HTTPS صحف زواجتب مق، ةلكشم لال حل ةيئاقق نال ريفش لل

- 517 تانايبل قفدت ةداهش لاطبل مت
- ةداهش لال TLS لوكوتورب ءاطخأ
- يلخادلل رابتخالل ايودي SWG DC ديدحت

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا