1 Einleitung

Dieses Dokument beschreibt eine Prüf-Installation eines Datafox Geräts an einem HTTPS-Proxy.

2 Generelle Funktionsprüfung HTTPS-Proxy

Als Proxyserver wird ein Squid-Server auf Ubuntu Linux 22.04 eingesetzt:

```
Squid Cache: Version 5.7
Service Name: squid
Ubuntu linux
configure options:  '--build=x86_64-linux-gnu' '--prefix=/usr' '--
includedir=${prefix}/include' '--mandir=${prefix}/share/man' '--infodir=${prefix}/share/info'
'--sysconfdir=/etc' '--localstatedir=/var' '--disable-option-checking' '--disable-silent-
rules' '--libdir=${prefix}/lib/x86_64-linux-gnu' '--runstatedir=/run' '--disable-maintainer-
mode' '--disable-dependency-tracking' 'BUILDCXXFLAGS=-g -O2 -ffile-prefix-map=/build/squid-
Apg30N/squid-5.7=. -flto=auto -ffat-lto-objects -flto=auto -ffat-lto-objects -fstack-
protector-strong -Wformat -Werror=format-security -Wdate-time -D_FORTIFY_SOURCE=2 -Wl,-
Bsymbolic-functions -flto=auto -ffat-lto-objects -flto=auto -Wl,-z,relro -Wl,-z,now '
'BUILDCXX=g++' '--with-build-environment=default' '--enable-build-info=Ubuntu linux' '--
datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--libexecdir=/usr/lib/squid' '--
mandir=/usr/share/man' '--enable-inline' '--disable-arch-native' '--enable-async-io=8' '--
enable-storeio=ufs,aufs,diskd,rock' '--enable-removal-policies=lru,heap' '--enable-delay-
pools' '--enable-cache-digests' '--enable-icap-client' '--enable-follow-x-forwarded-for' '--
enable-auth-basic=DB,fake,getpwnam,LDAP,NCSA,PAM,POP3,RADIUS,SASL,SMB' '--enable-auth-
digest=file,LDAP' '--enable-auth-negotiate=kerberos,wrapper' '--enable-auth-ntlm=fake,SMB_LM'
'--enable-external-acl-
helpers=file_userip,kerberos_ldap_group,LDAP_group,session,SQL_session,time_quota,unix_group,w
binfo_group' '--enable-security-cert-validators=fake' '--enable-storeid-rewrite-helpers=file'
'--enable-url-rewrite-helpers=fake' '--enable-eui' '--enable-esi' '--enable-icmp' '--enable-
zph-qos' '--enable-ecap' '--disable-translation' '--with-swapdir=/var/spool/squid' '--with-
logdir=/var/log/squid' '--with-pidfile=/run/squid.pid' '--with-filedescriptors=65536' '--with-
large-files' '--with-default-user=proxy' '--enable-linux-netfilter' '--with-systemd' '--with-
gnutls' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -ffile-prefix-map=/build/squid-
Apg30N/squid-5.7=. -flto=auto -ffat-lto-objects -flto=auto -ffat-lto-objects -fstack-
protector-strong -Wformat -Werror=format-security -Wall' 'LDFLAGS=-Wl,-Bsymbolic-functions -
flto=auto -ffat-lto-objects -flto=auto -Wl,-z,relro -Wl,-z,now ' 'CPPFLAGS=-Wdate-time -
D_FORTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -ffile-prefix-map=/build/squid-Apg30N/squid-5.7=. -
flto=auto -ffat-lto-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -
Werror=format-security'
```

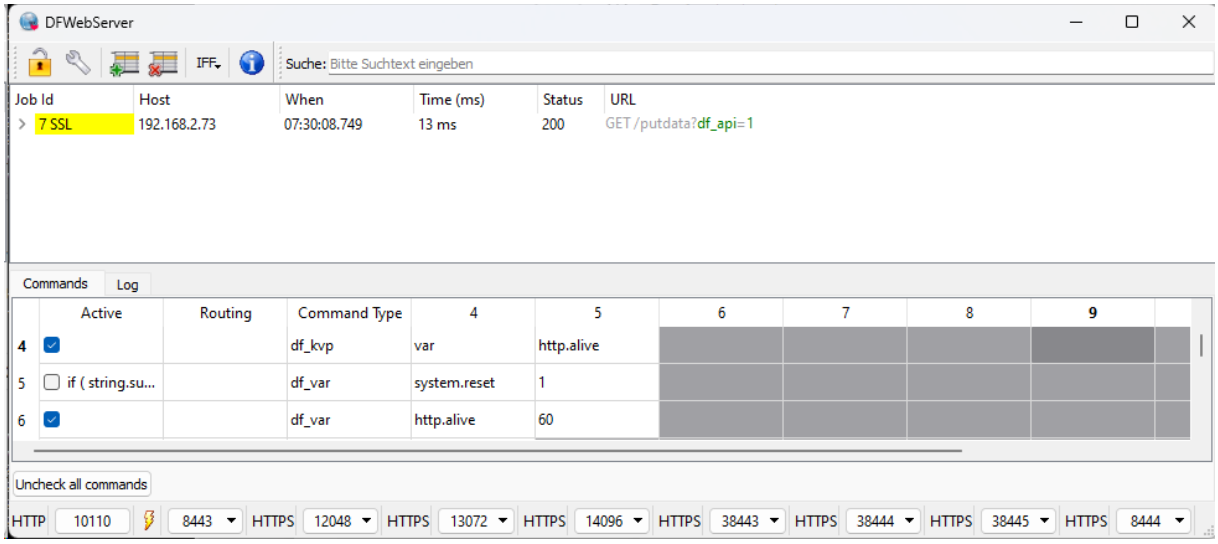
Dieser wird als 192.168.2.73:8443 betrieben und mit einem selbst-signiertem 2kBit RSA-Zertifikat ausgestattet.

Der zugehöriger Applikations-Webserver (ebenfalls mit 2bKit RSA-Zertifikat) ist unter 192.168.1.127:12048 erreichbar:

Per curl lässt sich ein Geräterequest von 192.168.1.127 über Proxy-Server an Webserver:

```
curl --insecure --proxy-insecure --proxy https://192.168.2.73:8443 -k
https://192.168.1.127:12048/putdata?df_api=1&df_table=abc
```

Die Anfrage wird durch den Webserver wie folgt entgegengenommen und protokolliert:

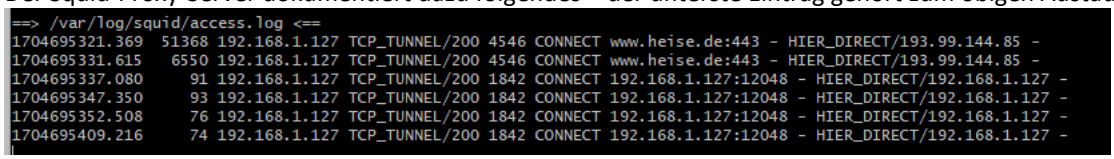


Als Antwort sendet der Webserver – gemäß Konfiguration:

```
df_api=1&df_kvp=var,http.alive&df_var=http.alive,60
```

Auf der Client-Seite (Curl-Aufruf und Response) stellt sich die Interaktion wie folgt dar:

Der Squid-Proxy-Server dokumentiert dazu folgendes – der unterste Eintrag gehört zum obigen Austausch:



3 Gerät

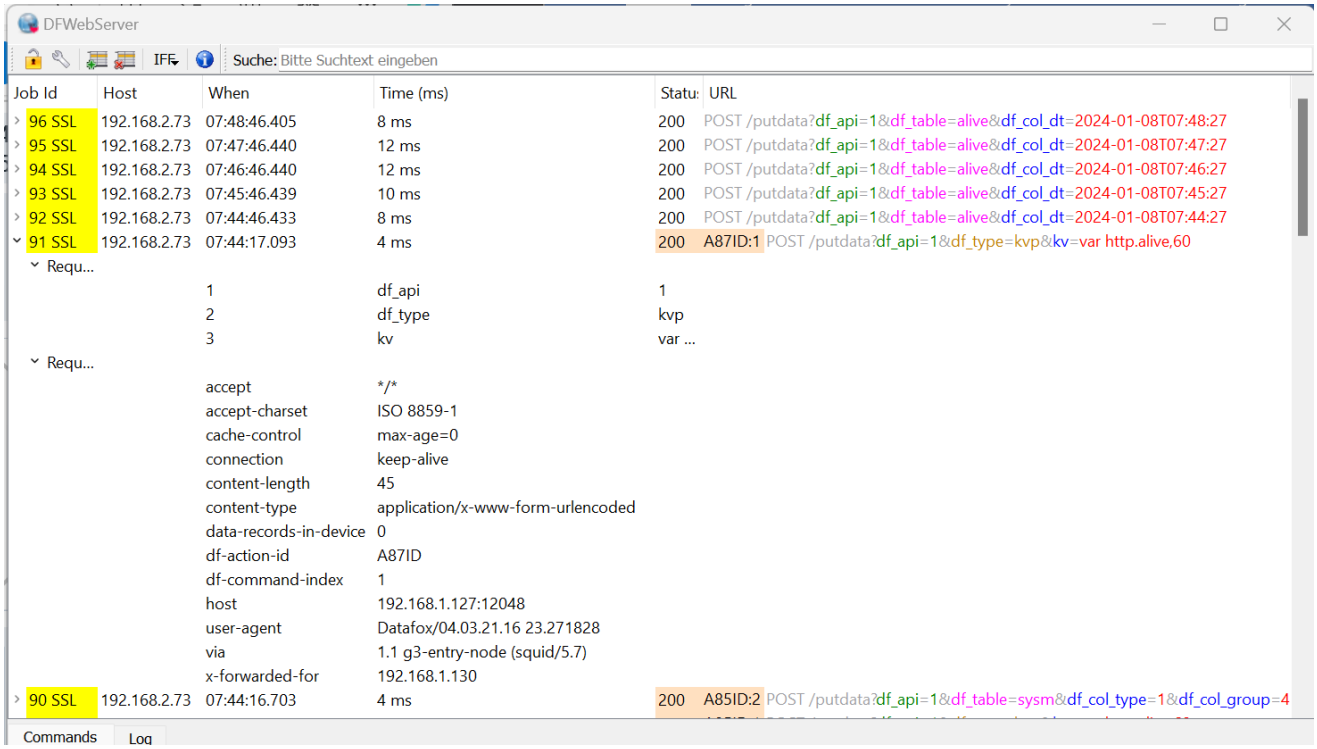
Konfiguration des Geräts:

Das Gerät kommuniziert mittels HTTPS (com.http = 2) über den Proxy-Server (com.http_mode[0].proxy.-Einstellungen 192.168.2.73:8443) mit dem Endpoint 192.168.1.127:12048.

Auf dem Gerät ist lediglich das Zertifikat des Proxy-Servers hinterlegt.

3.1 Requests auf dem Ziel-Webserver

Die Geräteanfragen werden vom Gerät über den Proxy-Server an den Web-Server weiterleitet. Anbei ein Request mit Header-Informationen in der Darstellung des Webservers:



Als “Host:”-Header ist der Ziel-Server hinterlegt, im “via:“-Header ist der Name des Proxy-Servers dokumentiert. Die IP-Adresse des Anfragenden ist ebenfalls die des Proxy-Servers.

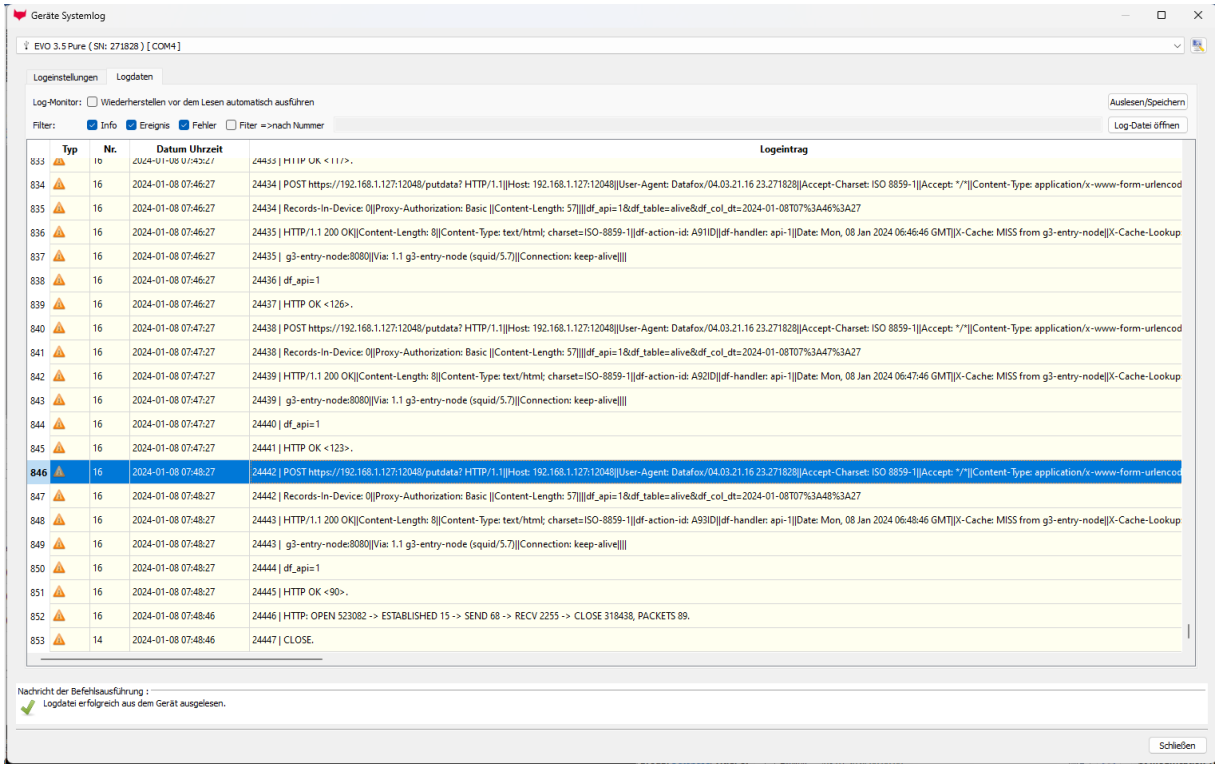
3.2 Log des Proxy-Servers

Der Proxy-Server protokolliert die eingehenden Requests wie folgt:

```
1704696252.489     74 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696252.886     72 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696253.197     75 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696253.686     73 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696253.985     79 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696254.429     84 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696254.885     77 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696255.277     89 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696255.594     83 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696255.957     67 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696256.241     77 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696256.521     73 192.168.1.130 TCP_MISS/200 366 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696256.901     75 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696257.186     81 192.168.1.130 TCP_MISS/200 345 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696257.573     88 192.168.1.130 TCP_MISS/200 248 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 -
1704696286.917     76 192.168.1.130 TCP_MISS/200 308 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696346.921     71 192.168.1.130 TCP_MISS/200 308 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
1704696406.926     82 192.168.1.130 TCP_MISS/200 308 POST https://192.168.1.127:12048/putdata? - HIER_DIRECT/192.168.1.127 text/html
```

3.3 Log des Geräts

Das Gerät protokolliert die ausgehenden Anfragen (blau hinterlegt) und die zugehörige Antwort wie folgt:


Geräte Systemlog
EVO 3.5 Pure (SN: 271828) [COM4]
Logeinstellungen
Logdaten
Log-Monitor:
Wiederherstellen vor dem Lesen automatisch ausführen
Auslesen/Speichern
Filter:
Info
Ereignis
Fehler
Filter =>nach Nummer
Log-Datei öffnen
Typ
Nr.
Datum Uhrzeit
Logeintrag
834 16 2024-01-08 07:46:27 24434 | POST https://192.168.1.127:12048/putdata? HTTP/1.1||Host: 192.168.1.127:12048||User-Agent: Datafox/04.03.21.16 23.271828||Accept-Charset: ISO 8859-1||Accept: */*||Content-Type: application/x-www-form-urlencod
835 16 2024-01-08 07:46:27 24434 | Records-In-Device: 0||Proxy-Authorization: Basic ||Content-Length: 57||||df_api=1&df_table=alive&df_col_dt=2024-01-08T07%3A46%3A27
836 16 2024-01-08 07:46:27 24435 | HTTP/1.1 200 OK||Content-Length: 8||Content-Type: text/html; charset=ISO-8859-1||df-action-id: A91ID||df-handler: api-1||Date: Mon, 08 Jan 2024 06:46:46 GMT||X-Cache: MISS from g3-entry-node||X-Cache-Lookup
837 16 2024-01-08 07:46:27 24435 | g3-entry-node:8080||Via: 1.1 g3-entry-node (squid/5.7)||Connection: keep-alive||||
838 16 2024-01-08 07:46:27 24436 | df_api=1
839 16 2024-01-08 07:46:27 24437 | HTTP OK <126>.
840 16 2024-01-08 07:47:27 24438 | POST https://192.168.1.127:12048/putdata? HTTP/1.1||Host: 192.168.1.127:12048||User-Agent: Datafox/04.03.21.16 23.271828||Accept-Charset: ISO 8859-1||Accept: */*||Content-Type: application/x-www-form-urlencod
841 16 2024-01-08 07:47:27 24438 | Records-In-Device: 0||Proxy-Authorization: Basic ||Content-Length: 57||||df_api=1&df_table=alive&df_col_dt=2024-01-08T07%3A47%3A27
842 16 2024-01-08 07:47:27 24439 | HTTP/1.1 200 OK||Content-Length: 8||Content-Type: text/html; charset=ISO-8859-1||df-action-id: A92ID||df-handler: api-1||Date: Mon, 08 Jan 2024 06:47:46 GMT||X-Cache: MISS from g3-entry-node||X-Cache-Lookup
843 16 2024-01-08 07:47:27 24439 | g3-entry-node:8080||Via: 1.1 g3-entry-node (squid/5.7)||Connection: keep-alive||||
844 16 2024-01-08 07:47:27 24440 | df_api=1
845 16 2024-01-08 07:47:27 24441 | HTTP OK <123>.
846 16 2024-01-08 07:48:27 24442 | POST https://192.168.1.127:12048/putdata? HTTP/1.1||Host: 192.168.1.127:12048||User-Agent: Datafox/04.03.21.16 23.271828||Accept-Charset: ISO 8859-1||Accept: */*||Content-Type: application/x-www-form-urlencod
847 16 2024-01-08 07:48:27 24442 | Records-In-Device: 0||Proxy-Authorization: Basic ||Content-Length: 57||||df_api=1&df_table=alive&df_col_dt=2024-01-08T07%3A48%3A27
848 16 2024-01-08 07:48:27 24443 | HTTP/1.1 200 OK||Content-Length: 8||Content-Type: text/html; charset=ISO-8859-1||df-action-id: A93ID||df-handler: api-1||Date: Mon, 08 Jan 2024 06:48:46 GMT||X-Cache: MISS from g3-entry-node||X-Cache-Lookup
849 16 2024-01-08 07:48:27 24443 | g3-entry-node:8080||Via: 1.1 g3-entry-node (squid/5.7)||Connection: keep-alive||||
850 16 2024-01-08 07:48:27 24444 | df_api=1
851 16 2024-01-08 07:48:27 24445 | HTTP OK <90>.
852 16 2024-01-08 07:48:46 24446 | HTTP: OPEN 523082 -> ESTABLISHED 15 -> SEND 68 -> RECV 2255 -> CLOSE 318438, PACKETS 89.
853 14 2024-01-08 07:48:46 24447 | CLOSE.
Nachricht der Befehlsausführung :
Logdatei erfolgreich aus dem Gerät ausgelesen.
Schließen