**Stunnel Install/Configure for Hosted Aleph**

**Firewall rules**:

1. In advance, ask the customer for the outgoing IP(s) of their self-check machines, or the servers where they plan to install stunnel.
2. Open a Salesforce case to Cloud Production and request that a firewall rule be added to allow traffic from the customer’s IP(s) to the Aleph server IP on port 6443.

**Install**:

1. Open a Salesforce case to Cloud Production and request that they install stunnel on this server and that they add stunnel stop/start scripts to the server. (Monitoring will be added later, at STP time.)

**Configuration**:

1. Log into the server as the aleph user.
2. Create a directory called stunnel under /exlibris/aleph
3. Navigate to the new directory.
4. Create a self-signed certificate for the Aleph server as follows:

openssl genrsa -out key.pem 2048

openssl req -new -x509 -nodes -key key.pem -out cert.pem -days 1095

NOTE: This is interactive. Most of the questions can be skipped, but you **must** enter the full hostname when prompted for the Common Name.

cat key.pem cert.pem >> stunnel.pem

1. Send the **stunnel.pem** file to customer, to be installed in the server where they will be configuring stunnel.
2. Create a file called **stunnel.conf** under /exlibris/aleph/stunnel with the following contents:

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; \* Global options \*

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* ;

; Debugging stuff (may useful for troubleshooting)

debug = 7

output = /exlibris/aleph/stunnel/stunnel.log

pid = /exlibris/aleph/stunnel/stunnel.pid

;Disable FIPS mode to allow non-approved protocols and algorithms

fips = no

;\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; \* Service defaults may also be specified in individual service sections \*

; \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

; Disable support for insecure SSLv2 protocol

options = NO\_SSLv2

[SIP2]

key = /exlibris/aleph/stunnel.pem

cert = /exlibris/aleph/stunnel.pem

client = no

accept = 6443

connect = 127.0.0.1:5331

TIMEOUTclose = 0

TIMEOUTconnect = 200

1. Start stunnel on the Aleph server using the following command:

stunnel /exlibris/aleph/stunnel/stunnel.conf

1. Tell the customer to make sure that their stunnel.conf file contains the following section (for the SIP2 service):

[SIP2]

key = stunnel.pem

cert = stunnel.pem

client = yes

accept = 127.0.0.1:5331

connect = **<Aleph server>**:6443

TIMEOUTclose = 0

TIMEOUTconnect = 200

(The key and cert parameters should point to the path of the stunnel.pem file they received from us.)

1. Customer should change their SIP machine’s server parameter from Aleph server to localhost
2. Open a Salesforce case to the 24x7 Hub and ask them to add stunnel monitoring to this server. If the customer has more than one SIP service set up, give the Hub a list of ports that need to be monitored.

**Support after STP**:

1. To stop services, run the following as Aleph:

kill `cat /exlibris/product/stunnel/stunnel.pid`

To make sure that the process has ended, enter the following:

ps -ef | grep stunnel

1. To start services, run the following as Aleph:

stunnel /exlibris/aleph/stunnel/stunnel.conf

To make sure that the process has started, enter the following:

ps -ef | grep stunnel

(You should see a few stunnel processes running.)