Configuring State Synchronization under FW-1

State Synchronization is the mechanism used by Firewall-1 to maintain identical state connection tables on a pair of redundant firewalls. If one of the firewalls fails, the other firewall should recognize this and maintain all valid connections transparently.

To configure state synchronization, you will require a dedicated interface on each firewall. These interfaces will be the "sync" interfaces and will be connected directly to each other via an Ethernet crossover cable running at 100MB full-duplex.

Procedure to be carried out on each firewall in the pair:

1) Create the file **'$FWDIR/conf/sync.conf'** on both firewalls.
2) In this file, put in the IP address of the sync interface of the **opposite** firewall.
3) Example:

If: Firewall A's sync port address = 10.10.10.1 then: On Firewall A, $FWDIR/conf/sync.conf = 10.10.10.2
If: Firewall B's sync port address = 10.10.10.2 then: On Firewall B, $FWDIR/conf/sync.conf = 10.10.10.1

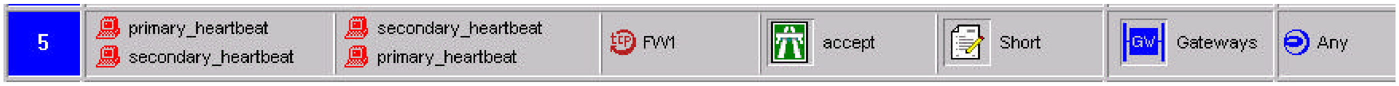
4) On each firewall, you will need to perform a "fw putkey" operation to authenticate the link between the sync interfaces:

```
$FWDIR/bin/fw putkey –n [my sync interface]  -p [password]  [opposite sync interface]

ex:  $FWDIR/bin/fw putkey –n  10.10.10.1  -p abc123  10.10.10.2          (on Firewall A)
ex:  $FWDIR/bin/fw putkey –n  10.10.10.2  -p abc123  10.10.10.1          (on Firewall B)
```

5) You can validate the key operation occurred by looking at the contents of the $FWDIR/conf/fwauth.keys This should relect the time/date of the putkey command you just performed on the sync interfaces.

6) Next, create a rule in the rulebase to allow the sync to occur between the firewall sync interfaces:



5	primary_heartbeat secondary_heartbeat	secondary_heartbeat primary_heartbeat	FW1	accept	Short	Gateways	Any

In the example above, the FW-1 object called **primary_heartbeat** contains Firewall A's sync interface address, and the FW-1 object **secondary_heartbeat** contains Firewall B's sync interface IP address.

6) At this point, stop and start your firewall using **$FWDIR/bin/fwstop** and **$FWDIR/bin/fwstart.**

Validating State Sync is working:

7) When FW-1 comes up, run the command "netstat –na" and look for a pair of connections from the state sync interfaces on port 256:

```
tcp 0 0 10.10.10.1.256 10.10.10.2.1056 ESTABLISHED
tcp 0 0 10.10.10.1.1054 10.10.10.2.256 ESTABLISHED
```

8) The final method to check proper sync between the firewalls is to compare the size of the connections table on each firewall using the command: **'fw tab -t connections -s'**

Each firewall will display a table like the one below:

```
HOST NAME ID #VALS
localhost connections 14 2143
```

9) The two **#VALS** numbers should be roughly equivalent on both firewalls. If there are differences, wait a few seconds and try the command again. ? Karim Ismail. karimi@ca.ibm.com, No Copying Permitted.