Transparent Failover for an HA Firewall

https://campus.barracuda.com/doc/41115837/

An HA system can be used for load balancing to exploit all features that are available through the Barracuda NG Firewall architecture. Use transparent failover to synchronize the forward packet sessions (inbound and outbound TCP, UDP, ICMP-Echo, and OTHER-IP-Protocols) of the Firewall server between the two HA partners. Transparent failover is enabled by default and activated per rule.

For transparent failover, both HA partners must have identical network configurations, except for the NICs, which may differ. The assignment of the interfaces must be identical. For example, if the ISP is connected on eth0 and the DMZ is on eth1, the same interface must be used on the partner unit to connect to the ISP and DMZ.

Unsynchronized Components

Certain components are not HA-synced. These are listed in the table below:

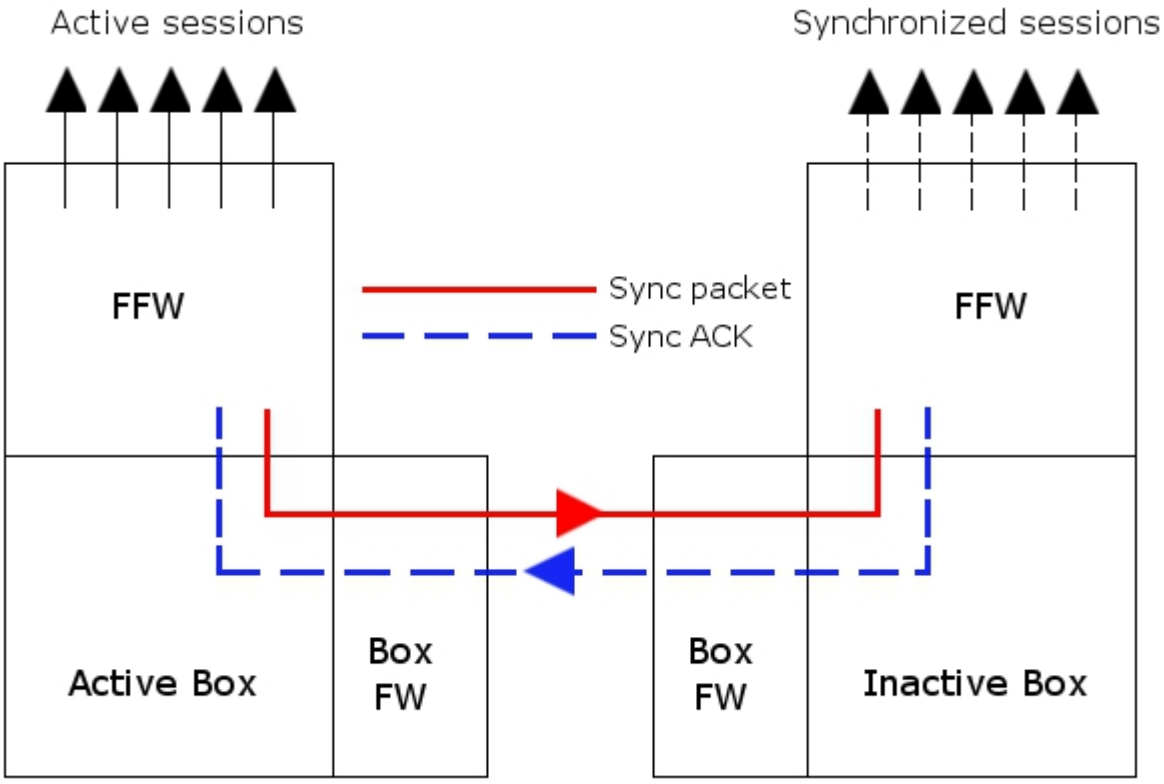
Module or Component	Sub Components
Firewall	• Local sessions • Stream sessions • WANOPT sessions • SSL decryption sessions • Sessions using a box IP address as dynamic bind IP address • Sessions using a box IP address as redirection target • Sessions for which HA synchronization was disabled in the **Advanced Rule Settings**
VPN Service	• IPSec tunnels
Access Control Service	All
Eventing	All
Logging	All
Box Statistics	All
Home Directories *(Admins)*	All
SMS Messages	All

Synchronizing Procedure

Synchronization can be carried out via dedicated HA uplink or, alternatively, via the LAN connection.

Synchronization traffic is transmitted by AES-encrypted UDP packets, so-called sync packets, on port 689. The AES keys are created by using the BOX RSA Keys and renewed every 60 seconds.

Only a small amount of synchronization traffic is necessary for synchronizing via LAN connection. Sync traffic is kept at a minimum by synchronizing only sessions and not each packet. Due to the characteristics of the TCP protocol (SYN, SYN-ACK, ...), only existing established TCP connections are synchronized. When the synchronization takes place during the TCP handshake, the handshake must be repeated.



The synchronizing procedure takes place immediately (if possible). If synchronization packets are lost, up to 70 sessions per second are synchronized.

Depending on the system availability, the behavior differs:

- **If the partner unit is inactive/rebooted -** Sometimes it may happen that the backup unit is not available and, therefore, does not respond to the sync packets (for example, for maintenance reasons). In this case, the active unit stops synchronizing. As soon as the partner unit reappears, the active unit checks whether the other one was rebooted or has an obsolete session state and resynchronizes all necessary sessions.
- **If the active unit reboots without a takeover -** The **Firmware Restart** button was clicked. The *acpf* and sockets are gone, but the unit is not rebooted physically. In this case, the partner unit recognizes that its session state is obsolete and removes all synchronized sessions.

Takeover Procedure

When the HA unit on which the firewall runs does not respond to the heartbeat (Control UDP 801), takeover is initiated after a delay of 10 to 15 seconds. This delay is necessary because of potentially low network performance.

During this time, no service is available.

When the unit stays inactive, the synchronized sessions on the second unit are activated and all connections are available again. Again, the TCP protocol must be mentioned separately. The backup unit does not have the current TCP sequence numbers. In case of a takeover, the sequence number is not checked for correctness. As soon as the connection has traffic, the sequence number is known to the former backup unit, and the sequence number check is performable again. The missing sequence number on the backup unit also results from the fact that TCP connections that were taken over but have since had no traffic cannot be reset in a clean way. Terminating the session via the **Terminate Session** button removes the connection but does not send a TCP Reset (TCP-RST) signal.

Configuration

In each firewall rule, you can edit a **Transparent Failover active/inactive** setting that defines whether sessions that are affected by this rule must be synchronized. For more information, see Advanced Firewall Rule Settings.

Monitoring

To view the status of sessions, go to the **Firewall** > **Status** page.

Figures