Fail Open and Fail Closed Modes with the Barracuda WSA

https://campus.barracuda.com/doc/7761/

If connectivity from the Barracuda Web Security Agent (WSA) to a service host cannot be established (i.e. if either fallback to another Barracuda Web Security Service host, or connectivity to the Barracuda Web Security Gateway, was unsuccessful), the admin must configure the Barracuda WSA to either **Fail Open** or **Fail Closed** (see the **Fail Open** setting on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway). The Barracuda WSA then schedules another check for connectivity at a pre-configured time interval (see Note below). For Windows, configure this setting as described in Configuration Tool for Barracuda WSA Windows Client 4.x or Configuration Tool for Barracuda WSA Windows Client 5.0 and Above. For Mac OS, see Configuring Preferences for Barracuda WSA Macintosh Client.

Fail Open

In the **Fail Open** state, the Barracuda WSA is disabled, and the user can continue accessing the network, but without being filtered by the Barracuda WSA. As a consequence, policies configured on the host are not applied to the client until connectivity with the service host is established. The Barracuda WSA then schedules another connectivity check in the pre-configured time interval. Upon reconnection with the service host, the user's traffic resumes filtering by the Barracuda Web Security Gateway. While in **Fail Open** state, the Barracuda WSA icon displays a red exclamation mark. Hovering the mouse over the icon shows the message *Unable to reach Barracuda Web Security Gateway: Failing Open.*

Important: Because all traffic from the WSA is blocked when in Fail Closed state, Barracuda Networks recommends setting Fail Open to Yes on the ADVANCED > Remote Filtering page to prevent a Fail Closed state.

During connectivity checks, client browsing is temporarily interrupted. With the Barracuda WSA for WIndows, you can change the preconfigured time interval for connectivity checks from every 30 seconds to a longer interval by modifying two subkeys in the Windows registry. See Changing the Connectivity Check Interval below for instructions.

With the Barracuda WSA for Macintosh, you cannot change the pre-configured time interval for connectivity checks, but checks are conducted periodically ranging from 1x per 60 second interval to 1x per 5 minute interval.

Fail Closed

The Barracuda WSA is configured to remain active, but no external network access is possible until connectivity with the service host is re-established. The Barracuda WSA then schedules another connectivity check in the pre-configured time interval. Upon reconnection with the service host, the user's traffic resumes filtering by the Barracuda Web Security Gateway.

Important: Because all traffic from the WSA is blocked when in Fail Closed state, Barracuda Networks recommends setting Fail Open to *Yes* on the ADVANCED > Remote Filtering page to prevent a Fail Closed state.

While in **Fail Closed** state, the Barracuda WSA icon displays a red exclamation mark and the message *Unable to reach Barracuda Web Security Gateway: Failing Closed*.

Changing the Connectivity Check Interval

With the Barracuda WSA for windows, the administrator can override the default interval for connectivity checks between the client and the service host. This includes:
1) Shorten/lengthen the test request timeout – the time passing until WSA decides WSG is not reachable (this is by default 30 secs).
2) Shorten/lengthen the Retry time interval – the time in between two retries, once WSA is in FailOpen/ FailClosed mode.

To modify either or both of the settings above, there are two subkeys in the registry:

- Connection_RetryInterval (string value in ms)
- Connection_TimeOut (string value in ms)

If these keys are absent in the regsitry, the default values are used (30secs / 30 secs).

Important Notes on Fail Open/Closed Behavior

To prevent Fail Open/Closed behavior in the Barracuda WSA, Barracuda Networks recommends *not* setting **Send VIA Header** to **No** on the **ADVANCED > Proxy** page if an external host name is set as service host.