

# IKE and DPD

Both IKE Keep-alive and Dead Peer Detection settings can show when a tunnel is disconnected. When they find the tunnel has disconnected, they start a new Phase 1 negotiation. If you select both IKE Keep-alive and Dead Peer Detection, the Phase 1 renegotiation that one starts can cause the other to identify the tunnel as disconnected and start a second Phase 1 negotiation. Each Phase 1 negotiation stops all tunnel traffic until the tunnel has been negotiated.

**To improve tunnel stability, select either IKE Keep-alive or Dead Peer Detection. Do not select both!**

Note the following about these settings:

The IKE Keep-alive setting is used only by WatchGuard devices. Do not use it if the remote endpoint is a third-party IPSec device!

When you enable IKE Keep-alive, the Firebox sends a message to the remote gateway device at a regular interval and waits for a response. Message interval determines how often a message is sent. Max failures is how many times the remote gateway device can fail to respond before the Firebox tries to renegotiate the Phase 1 connection.

Dead Peer Detection is an industry standard that is used by most IPSec devices. Select Dead Peer detection if both endpoint devices support it. When you enable Dead Peer Detection, the Firebox monitors tunnel traffic to identify whether a tunnel is active. If no traffic has been received from the remote peer for the amount of time entered for Traffic idle timeout, and a packet is waiting to be sent to the peer, the Firebox sends a query. If there is no response after the number of Max retries, the Firebox renegotiates the Phase 1 connection.

For more information about Dead Peer Detection, see <http://www.ietf.org/rfc/rfc3706.txt>.

About this IKE Keep-alive thing. Forget that this thing is called a "keepalive" and don't think about IKE keepalives as a way to keep anything alive.

(However, you don't want to confuse "IKE Keepalives" with the "VPN Keepalive" that the Edge can send; that's an entirely different beast.)

It's unfortunate that the industry decided to call this thing an "IKE keep-alive" because that's not at all what it's designed to do. It's not designed to "keep IKE alive" or to keep anything or anyone else alive. It's there to \*kill\* something, and it hopes that that something will resurrect itself.

The IKE keepalive is only there to detect whether the remote peer is still there. If the "keepalive" scheme detects that the remote peer is not there, then the Firebox kills its SAs.

So in reality the "IKE keepalives" should have been called "IKE killer" because that's the only action the Firebox will take as a result of sending IKE keepalives. If the remote peer responds to the "keepalives", absolutely nothing happens. If the remote peer fails to respond then the Firebox kills Phase 1 and Phase 2 SAs.

Further, if there no traffic is currently passing over the tunnel, then no traffic is *\*still\** passed over the tunnel when an "IKE keepalive" is sent.

In other words, the IKE keepalive is *\*not\** traffic that can help to keep the Tunnel up. It's just a small message that is Phase 1 traffic with an ISAKMP header.

Phase 1 traffic is not Tunnel traffic (we usually describe Tunnel traffic as Phase 2 traffic or IPSec traffic). Thus the keepalive does nothing for the health of the Tunnel.

Phase 2 traffic (traffic encapsulated in an IPSec header/trailer and tied to a Phase 2 Security Association via some SPI number) is Tunnel traffic.

So, a ping to a host on the other side (just what the Edge does when it sends its "VPN Keepalive") or log traffic going to a host on the other side is Phase 2 traffic and this indicates a healthy Tunnel.

All the same things can be said about DPD. DPD is simply a more intelligent way to do a test for liveliness than IKE Keepalives is. It's an RFC standard, unlike "IKE Keepalives". There is no RFC for IKE keepalives; our IKE Keepalive scheme is proprietary to our appliances, as is any other vendor's "IKE Keepalives".

If it's an RFC-compliant dead peer detection mechanism then it's called Dead Peer Detection. Which is a much better name for it, because it describes its sole purpose.

Like "IKE keepalives", DPD does nothing for the health of the tunnel; its only purpose is to kill the SAs when a dead peer is detected. Its goal is exactly the same as "IKE keepalives" - to force renegotiation when a dead peer is detected. At least DPD has a name that makes sense. "IKE keepalive" is a scheme for nothing more than detecting dead peers and it should never have been called "keepalive".