

Re: ZoneAlarm Pro, Sygate Personal Firewall, or built in xp firewall?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-05/21090.html>

From: CZ (CZ_at_no99spam.com)

Date: 05/21/04

Date: Fri, 21 May 2004 10:20:49 -0700

> *ICF is stateful, and ZA is stateless, so ICF can provide technology that ZA lacks*

What is the difference, please explain.

Lars:

A stateless firewall can only drop a packet per info in that single packet. A stateful firewall maintains a connection state table and can use additional info to drop packets.

Examples:

1) ACK scan (aka TCP ping):

Hackers can send an ACK packet to see if an address is active.

A stateless f/w cannot drop the packet because it cannot verify if it is part of an existing connection.

A stateful f/w can drop the packet per info in the connection state table.

2) Dynamic blocking of source address (SA) spoofing:

A stateless f/w cannot do it because it does not retain info from any packet, a stateful f/w can use its table to verify the SA.

The above is before mktg gets involved. LinkSys started claiming SPI (stateful packet inspection) as a feature of their routers several years ago, and then would not clarify what the phrase meant. Tests by knowledgeable people suggested the concept was not stateful.