

RE: Spam: Zonealarm+Windows Firewall

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-02/msg00393.html>

- *From:* "evb" <swiver@xxxxxxx>
 - *Date:* Mon, 27 Feb 2006 11:41:59 -0700
-

I wanted to run an SSH server as a Windows service, but open a custom SSH port via port knocking only when access was needed.

To do this, I needed the SSH server to be running, but I also needed the port closed until I came a'knocking. When I needed SSH access, I could port knock, open the port, do my business, the port knock to close the port.

ZoneAlarm itself does not appear to allow this: that is, if SSH is running, the port is open and waiting for connections, or if the port is closed, then it's because the SSH service isn't bound to the port and therefore can't accept connections.

So I chose to run ZA plus the Windows firewall. Running both simultaneously allows SSH to bind to the port but still have the port closed for inbound connections (stealth mode).

So isn't that a good reason to have both?

Eric

:-----Original Message-----

:From: Jeff Britton, Monitored Security

:[\[mailto:jeff.britton@xxxxxxxxxxxxxxxxxxxxxxxx\]](mailto:jeff.britton@xxxxxxxxxxxxxxxxxxxxxxxx)

:Sent: Monday, February 27, 2006 8:43 AM

:To: barcajax@xxxxxxx

:Cc: security-basics@xxxxxxxxxxxxxxxxxxxx

:Subject: RE: Spam: Zonealarm+Windows Firewall

:

:I really don't see much value added by running both firewalls
:on the same host. In my experience, ZoneAlarm has done a
:great job monitoring both in and outbound traffic and should
:be sufficient (considering near-optimal management). Running
:a second firewall, such as the Windows Firewall, adds another
:layer of complexity, but not necessarily another layer of
:security. I just don't see it being efficient, from both a
:performance perspective, as well as from a security perspective.

:

:Jeff

RE: Spam: Zonealarm+Windows Firewall

:-----
:

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>
