

Re: SBS 2008 and antivirus

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2009-01/msg01330.html>

- *From:* Steve Schwab <SteveSchwab@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Jan 2009 17:51:01 -0800
-

Thank you for the info. I'll follow the same procedure. So far I'm really impressed with this box (Edge 20e). I'll be installing more of these I'm sure. Including one for my own network. It's great that this stuff never even hits the exchange server. Do keep IMF running anyway?

"Leythos" wrote:

In article <399E1972-827B-4980-A6FB-4204687FDDF0@xxxxxxxxxxxx>, SteveSchwab@xxxxxxxxxxxxxxxxxxxxxxxx says...

Hope it's OK to barge in on this thread. Leythos, you recommended the UTM solution to me a while back. I've just installed a watchguard edge and it's working great. Can you recommend settings for email filtering? What do you do for "confirmed" "bulk" and "suspect". Do you deny, quarantine, or add subject tag? Have you seen many false positives?

I'm super impressed with Watchguard. It was easy to set up and it's obviously much better than the old Linksys wrt54 we were using before. Thanks for the recommendation.

During the first week we MARK (add subject) to all categories and email the user at 2AM (default setting) each list. At the end of the week we determine if any were mismarked and create exceptions for them.

After the 1 week period we "DELETE" "Confirmed" and "Bulk" and Quarantine "Suspect" spam – the Suspect spam is part of the nightly email status for each user, they can unquarantine as needed – so far we've not had more than 2 or 3 emails from thousands of accounts that had to release anything from quarantine.

As for false positives – the only time we get a "False" is when a customer forwards us something from one of their business partners that is a question about an attached email being spam/a threat – since we

Re: SBS 2008 and antivirus

don't white-list all of our customers, when they forward us a SPAM from someone they wanted white-listed our system detects it as spam.

I have seen no confirmed false positives, and I've seen no deleted emails that were improperly classified – we have hundreds of thousands of emails per week across many clients using this, I would think there would be at least a few complaints, but we're not hearing any since moving from GFI to WG UTM.

We also filter content out of SMTP sessions, blocking (removing) anything that could be malicious.

--

- Igitur qui desiderat pacem, praeparet bellum.
 - Calling an illegal alien an "undocumented worker" is like calling a drug dealer an "unlicensed pharmacist"
- spam999free@xxxxxxxxxxx (remove 999 for proper email address)