



Q&A from the TDS Webinar - *Defending Your Network and Data*

**Questions from businesses, with Answers by
Dr. Johannes Ullrich, SANS Internet Storm Center**

If we have servers in house that use IPv6, but are using an older IPv4 firewall appliance, do we need to update our perimeter security device (firewall) to control access to the IPv6 servers?

Yes. Also make sure that you have your host based firewall enabled to control IPv6.

How can you prevent MAC Spoofing?

MAC spoofing can not be prevented itself. However, some of the impact can be mitigated by controlling on the switch which MAC address can connect from what port.

How old is too old for a firewall?

I don't think there is a specific age at which a firewall "expires." It all depends on what you are doing. However, whenever the network that is protected by the firewall is upgraded (e.g. higher speed, significant new features like IPv6 or more servers, which will lead to more concurrent sessions) the firewall should be reviewed to verify if it is still adequate.

Why are e-mail services requiring that you drop all your system security to access their e-mail service?

You should not have to ☺. Work with your email provider to understand what specific security concerns there are. Again, you may not need to drop the security.

Do you recommend using cloud services for document back-ups?

Depends on the cloud service. Cloud services can provide reasonably priced remote storage to small businesses. However, realize that you are now at the mercy of whatever security the cloud service implements to protect your document. Most cloud services, for example, will state that they are not PCI compliant, as they do not provide sufficient controls to protect payment data like credit card numbers. Encrypted remote storage may be an option to mitigate these issues.

How do you verify the level of security in place?

This typically requires a full security assessment. As you may realize from the webinars so far, security is a multi-faceted problem. A security assessment

should look at your organization, identify critical data and verify that sufficient controls are in place to protect that data. A complete assessment would include a review of your network architecture, policies and controls. It may include a penetration test in which a security professional verifies that the controls are sufficient by trying to break into your network.

What are some hardening strategies for firewalls?

For most firewalls, you will find hardening guides from vendors or other organizations (for example, check cisecurity.org, or the SANS reading room at sans.org/rr). Typically, these guides are specific to a particular firewall as each firewall has its specific features. As a general guide, it is recommended to start with a “deny everything” policy, and then only allow specific traffic through the firewall.

Are software firewalls worth the effort?

Yes. Software firewalls can protect a host at a more granular level than a hardware firewall. For example, a software firewall is able to block certain applications from accessing the network. A hardware firewall will not be able to know what application sent a particular data packet.

How do you know if your hosting provider has a safe network?

You don't. There is no simple way to verify the security of your hosting provider's network. However, there are indications. For example hosting providers that offer overall better support or security features as part of the hosting package tend to have better security overall. In short: you get what you pay for.

What data is normally targeted by hackers and thieves?

Anything that can be turned into money. Credit card information, login credentials for online banking and identity information (social security numbers) are of course at the top of the list. But in some cases data has been stolen in order to blackmail individuals or trade secrets have been stolen in targeted attacks if a buyer was available. Customer lists and just e-mail address lists (for spam) are also stolen regularly.

Does your use of social media sites or online radio really affect your system's security?

The more traffic you allow in and out of your network, the harder it will be to protect your network. We will talk in the next webinar a bit about social networking sites. But while they are “just another website,” they are frequently used to distribute malware. Online radio frequently requires rather open firewall configurations in order to allow the access to the radio stream. The more relaxed firewall configuration could now be used by malware.

We have an email address on our website so prospective customers can request more information, but we get a lot of spam. How can we avoid the spam, but still make it easy to contact us?

A web-based form may be a decent alternative. The information from the form will then be sent to a “secret” e-mail address. Other than that, there is no great tool to get rid of spam. Various spam filters are able to filter out a large part of the spam but there is always a danger of missing a valid e-mail.

If I think my network has been breached, should I close everything off, or just focus on the area of the breach?

If you suspect an incident, it is important to keep a cool head and follow basic incident handling guidelines. First of all, identify the nature of the incident. Next, try to isolate the affected network segment. It may not be necessary to close everything off. All depends on the nature of the incident. For a bit more details, see this quick overview of incident handling:

<http://www.giac.org/resources/whitepaper/network/17.php>

Should hard drives be encrypted?

Hard drives should be encrypted if there is a risk of the drive being stolen. Encryption is usually of little use against a malware infection. The main use case for hard disk encryption is physical loss of the drive.

Does having a VPN open a hole in my network and add risk?

Yes. Like any feature added to the network, it will add risk. Someone is now able to remotely access your network. If the login credentials are stolen, or the VPN is badly configured, an outsider may use the VPN connection to access the network.

What can be done to protect against drive-by infections (e.g. infected ads on legitimate sites)?

Your best bet is anti-malware software. A hardened browser configuration (e.g. Firefox using the No-Script plugin) can help as well, but is not always easy to set up.