EITS
Enterprise IT Security

RELEASE DATE:	CONTACT:
March 25, 2021	Jason Punda
	Principle Architect
RELEASE METHOD:	Enterprise IT Security
Social Media and Website	info@eits.com

Improve Firewall Performance with a Health Check

It’s the reason dogs chase cars: they’re flashy, attention-grabbing and you just have to have it. The IT crowd sometimes get that mentality with security tools – it’s a common observation among EITS’ Security Engineers and Architects that folks do this instead of looking inward at their existing infrastructure. But when it comes to security products such as firewalls, shouldn’t you have the latest and greatest? Even though it might sound like a good plan of action to invest in buying the hot product – especially when it’s the buzzword on social media and on vendor lips – it can be an expensive tradeoff.

There is a common notion in the security world that the only thing more expensive than paying for the security to prevent an incident is paying for the cost of cleaning up after one. Gartner reports that spending for IT security in 2019 – increased by 8.7% over 2018, versus a general IT spending hike of only 3.4%. We in the IT world certainly expected that the trend would continue in 2020 with spending up 20% from the previous year; of course, that prediction was made in the halcyon days before the coronavirus pandemic. As you may expect, spending on IT security took a dive in the last year. Instead we saw some of that outlay shift to facilitate work-from-home Zoom licenses, VPNs, and new laptops. General IT spending outside of security is predicted to be flat or to actually fall. And while working through a VPN doesn’t necessarily add vulnerability, if employees are on their home PCs attached to the corporate network, they can present new threats. The need to invest in security is obviously not going to change, so it is critical to be strategic about where and how the money gets spent. CISOs can’t afford to treat the security budget like a kid spending their allowance because it’s burning a hole in their pocket.

Why perform a security assessment? The 2015 IRS breach

For businesses that take a deeper look at security, it seems to coincide with getting audited. These audits come in all shapes and sizes, such as PCI compliance for folks that process credit cards, IRS audits for government organizations that handle taxpayer data, and HIPAA compliance for anyone handling patient medical data. These kinds of audits do serve a purpose, of course, but they tend to be long on findings and short on actionable data. Far too often, an audit ends and the security team gets stuck with a stack of findings that they then need to review, classify, rank, and attempt to remediate – all while still performing their normal job functions. What typically happens is that either the audit gets filed away for some nebulous future remediation plan, or a single facet of the red team findings becomes the remediation focus. This one component may, in fact, get resolved, but at the cost of only minimally increasing the organization's overall level of security.

When the IRS was breached in 2015 to the tune of 700,000 user accounts, bogus tax returns were filed, and the "refunds" were electronically funneled into hackers' bank accounts. The focus of the post-incident activity was placed on the unencrypted data, but access was achieved using valid credentials! The bad actors relied on compromising knowledge-based authentication (KBA) questions. Much of the personally identifiable information (PII) that could challenge the KBA questions for the accounts was easily found online. This particular attack could have been virtually eliminated with a security assessment and moving toward measures such as validating users' access using a form of token or authenticator-based multi-factor authentication to validate both something the user knew (their username and password) and something they had at the time of access (the token or authenticator code), as well using multi-tiered lockout rules.

What's more, what was needed at the IRS and elsewhere was not another audit by a generalist, but instead a deeper dive into the subject of concern by engineers that are experts on the matter. This allows such engineers – subject matter experts (SMEs) – to then apply that calculated eye to the issue and help security-minded organizations make practical changes to increase their security level, ace their next audit, and increase their overall operational stability, all without needing to buy new product.

Performing a security assessment allows companies to see if there are improvements to their security posture without having to go out and buy new "toys." It's a common trend I see in most of the organizations I step into, across all business types and sizes: Money was spent to procure a best-of-breed solution, time was invested in getting it set up, and some measure of time later the changes performed have all been operational in nature. Security is always a moving target, with standards and best practices changing frequently; organizations that do not adjust and adapt to the changes are usually left behind by them and leave themselves open for exploitation by adversaries. Just ask the IRS.

You've invested your money and time into your existing IT security platforms, so before replacing them it's best to re-evaluate how they are deployed and used to see if they are being used to their fullest potential. There are a few ways to accomplish this, of course, but for me and my EITS team members, this usually comes in the form of a security assessment and a health check of some kind. Anything that can be hardened and made compliant can then have a health check performed against it. For example, in our modern security environment, the most obvious icon of network security is the firewall, and the firewall is often the place where you can make the most impact in the shortest amount of time by performing a health check. The exact process you would go through is going to vary somewhat depending on the make and model of the firewall, of course, but the concepts and areas to evaluate are going to stay the same – in the same way that a Ford Focus and a Jeep Cherokee are different vehicles produced by two unrelated companies, and yet can be mechanically serviced in much the same way.

What does Firewall Health Check evaluate and what do we do with the findings?

So, we have our firewall that we are going to be performing a health check on. What does that really mean? Well, first we always start by talking to the engineers who are doing the daily care and feeding to try and capture as much environmental knowledge as possible. All of us were customers at one time – senior architects and engineers – so we look at what we would want if we were the customer. We want to know how the firewall fits into the network, how it gets used, what it physically cables to – really any background knowledge that we can get from those closest to them on a daily basis. Doing this gives us the level of detail we need to intelligently look into the configuration and saves us from tripping ourselves up when we start putting together recommendations for remediation. For example, a border firewall that isn't doing any form of URL filtering of user traffic would normally be an issue we'd want to focus on; however, if we take our time to learn about the environment we are checking, we might find that the customer is actually using zScaler and is doing URL filtering, but not on the device we are dialed in on. It also helps us to understand what the potential impact of the remediation efforts we are going to be suggesting could be, which is a big part of how we close out these health checks.

With the knowledge dump completed and environmental knowledge gained, it's time to roll up our sleeves and get into the nitty-gritty of the work: deep diving into the firewall configurations and applying that calculated eye. To compile a full list of things here that we would want to check for would be rather exhausting and would also vary depending on the make of the firewall and where in the network it is deployed, but some things are always going require evaluation:

- Is the firewall under support?
- Is it running a current OEM-suggested version of firmware?
- Is it application aware and, if it is, are the rules built out to control traffic based on applications instead of ports?
- What percent of traffic being processed is encrypted and is any of it being decrypted?
- How do administrators authenticate and are their changes being logged and audited?
- Are proper cryptography standards being applied where in use, such as in VPN connections and for administrator access to the system?
- Is High Availability (HA) properly configured?
- Are there features that are included or have been purchased but aren't being used?

Once we've completed the evaluation, it's time to sit down and build our report. Once again, the goal here is to provide actionable data, not just a laundry list of findings. So, while we do list everything we've discovered in the report, the real focus is on what we believe the priorities should be. We evaluate and create a list of the 10 most important things we found in our health check, and then turn around and rank them based on how critical the impact is, what the risk is, and what the level of effort is. This gives the security team a quick "hit list" to tackle and enables them to make an intelligent decision on which items to resolve, in which order, since we don't treat all issues the same.

For example, if we look at a High Availability pair of firewalls, a common issue we'll find is that HA will be configured to trigger in the event that the active firewall fails completely (due to something like a full power outage) but won't be set to fail over in the event it simply stops processing traffic because of a downstream issue (such as a switch failure). This is a critical issue – or will be the moment the environment goes down because the firewalls didn't fail over – but the fix is typically going to be low on the risk level, and the level of effort might be as little as 15 minutes of configuration and testing. Compare that to enabling SSL decryption, for example, which is also a critical issue, but one that is going to have a high level of both risk and effort. So the final task completed as part of the EITS health check is to work with the customer to plan out how to remediate the issues that have been uncovered. This could involve the customer having us do it for them, or it could be a matter of us simply providing guidance and acting as a sounding board for them to handle it internally.

Either way, the goal should always be that the end security posture will be much higher when we finish than it was when we started. Security assessments should be done for more than just compliance, and choosing professionals who can assess the best approach for your individual setup is important. In addition to changes implemented to improve firewall best practice adherence, we also often uncover opportunities for them to be used in new ways that will solve other problems customers were already facing and simultaneously harden their security and save even more money – all for a fraction of the price of chasing after that new, shiny tool.