ICSA labs
An Independent Division of Verizon Business

How to Select a Network Firewall

Table of Contents

Author

1. Brian Monkman

Introduction

You are in the market for a Network Firewall. To date you followed the steps outlined in the white paper entitled, "How to Select the Right Computer or Network Security Product." Having reached this point in your search now is the time to evaluate products on the shortlist.[1] The following sections outline some activities specific to choosing a Network Firewall that should be performed in advance of making a final product purchasing decision.

Vendor Product Evaluation

It's important to set aside time to evaluate the Network Firewall products on your shortlist and see how they integrate and behave in your environment. The handful of vendors with products on your shortlist will almost certainly be willing to loan one or more of their devices for evaluation. The length of time that vendors will permit you to evaluate their appliance or software may vary but, in general, you can figure on about 30-60 days.

Before the product can be deployed at your organization, the vendor will most likely want you to sign an NDA and/or an evaluation agreement. In the event that their product is not suitable for your network, the signed documents prohibit you from publishing or otherwise communicating anything uncomplimentary about the product's behavior or performance while it was under evaluation.

In terms of the evaluation agreement itself, the vendor helps tailor it to focus on what your organization wants to achieve. For your consideration, there is a high level list of pointers at the end of this paper to help complete your evaluation agreement.

With the evaluation agreement in place, ask the vendor to demonstrate their product for you. Hopefully, they will be able to demonstrate that the product performs as outlined in the evaluation agreement. If you need to test throughput in your network, request that the vendor measure this in your environment. Also, ask the vendor to install two Network Firewalls that match the way your network is configured.

Keep in mind that a Network Firewall is connected to another Network Firewall or to a remote client. In this whitepaper we are primarily focusing on gateway to gateway configuration. However, much of the same information applies in a gateway to remote client configuration.

Evaluate Products in Parallel Where Possible

Of course, the vendor won't remain at your organization throughout the evaluation. Before they leave, confirm that the vendor tailored the configuration on the deployed Network Firewall systems to fit your organization taking into consideration the services and applications that are run there. Once the vendor departs, leaving their device(s) at your organization, it is now up to you to complete the final steps of the evaluation. Ultimately, you will want to be as efficient as possible in evaluating the Network Firewall vendor products on your shortlist. To do so, you should consider practical ways to evaluate each product in parallel rather than one at a time. But how would you do that?

One potential test scenario comes to mind. Deploy the Network Firewalls into a test network segment. Using a three product shortlist scenario, deploy the three Network Firewalls into the same segment. These can be tested one at a time or in parallel depending on how you configure the gateways. The advantage of testing in parallel allows you to observe how each device behaves with similar traffic coming from each end.

When doing comparative testing make sure to use the exact same security policy for each gateway as you best can. In other words, configure the security policy to permit and deny the same mix of traffic. Doing so will make the comparison of the performance testing numbers more accurate.

[1] This white paper can be found on the ICSA Labs web site at:
https://www.icsalabs.com/sites/default/files/WP14354.How to select the right computer.pdf

During the evaluation be sure to document and review your experiences with the vendor so they can help you tweak and/or quickly resolve any issues you encounter. Pay attention to errors and log messages, and with the vendor's help, tune the configuration deployed on the devices to more precisely suit your environment paying particular attention to performance, the complexity of the configuration required to support your needs and how well the product supports your company's policy and approach to ongoing administration. Resolving issues during the evaluation period will give you some idea of the level of support that may be needed after purchasing the Network Firewall. You may also gain valuable insight into each product's ease of use as well as its level of configurability.

How Can You Get Your Hands Dirty?

Another potentially useful exercise is to run additional tests on the candidates in your test lab environment. There are many tools that generate traffic (e.g. IXIA, Spirent). Some free and some commercial tools are available to simulate traffic and to test performance. By integrating these tools you can determine your performance requirements and identify possible short-comings of the products. Keep in mind that performance should not be a measure of raw throughput, it should be considered from the point of view of the average mix and volume of your traffic and how the product responds to this. Remember that too many nonperformance tests can be exercised by sending simple ICMP messages (pings) through each Network Firewall to verify that the devices are working properly.

Because many of the traffic generation tools allow you to use your own packet captures, you may benefit from replaying that traffic through the Network Firewalls. Begin by capturing your own network traffic at the location or locations where the Network Firewall would most likely be deployed. This ensures that your subsequent testing reflects the kind of traffic that the Network Firewall will face when it is deployed.

If permitted by the evaluation agreement, ICSA Labs would encourage you to speak with both the vendor and a third-party test lab about your findings during the evaluation. Based on your findings, it may require the test lab to perform some additional testing of its own. Also, requests from enterprise organizations carry a lot of weight in terms of prompting vendors to have their products tested by independent third party test labs (in the event the product has not been tested by a third party).

You can construct any number of test scenarios to determine the behavior of the Network Firewall. Whatever scenarios you create, keep in mind that those products on your shortlist that are ICSA Labs Certified have already been tested in a multitude of different ways. Refer to the "ICSA Labs Network Firewalls Certification Testing Criteria"[2] to see what features/functions ICSA Labs tests.

Finally, if you do not have a dedicated test lab, or access to high-end test tools like IXIA or Spirent, contact the Network Firewall vendors whose products you are evaluating. Perhaps they can provide the equipment and environment for you to perform the evaluation.

Summary

Having studied trade journal reviews, industry analyst reports, and the results of independent, third-party testing it's time to evaluate the Network Firewall devices that made your organization's shortlist. The vendors on that list will allow you to evaluate one or more of their products for a month or two, typically after completing an NDA and evaluation agreement. You will work with each vendor to confirm that the evaluation agreement addresses your organization's needs. The vendor demonstrates the features and functions of their product including how it will meet all your business requirements. Then the vendor leaves the product with your organization. Using the rest of the evaluation time as

[2] The criteria can be found on the ICSA Labs web site at:
https://www.icsalabs.com/technology-program/firewalls/network-firewalls-document-library

efficiently as possible, observe what errors and log messages are triggered as your organization's traffic passes through the Network Firewalls on your shortlist. Adjust settings as needed, becoming as familiar as possible with each Network Firewall finalist. After all that, you should have enough information to decide which Network Firewall best fits your organization.

Some Items To Consider In Your Evaluation

1. Time to install
2. Time to configure for your environment
3. Ease of use
4. Integration with other network & security devices—many Network Firewalls are integrated with IPsec and Network IPS functionality.
5. Management and deployment
6. Fully integrated IPv6 support
7. High Availability
8. Reporting
9. Logging (is there enough for in-depth troubleshooting?)
10. Level and cost of vendor technical support
11. Availability and cost of vendor product training
12. Add or remove items to evaluate based on your business needs.

About ICSA Labs

ICSA Labs offers vendor-neutral testing and certification of security products and network connected devices to measure product compliance, reliability and performance to many of the world's top security vendors. The organization tests products in key technology categories such as anti-virus, anti-spyware, firewall, IPSec VPN, cryptography, network intrusion prevention, PC firewall, SSL-VPN, web application firewall, anti-spam and Wireless LAN. For more information about ICSA Labs, please visit: http://www.icsalabs.com.

Copyright