Return to the VPLS Blog

Blog Post

An Engineer's Perspective on Managed Firewalls

Published
Mar 4, 2021

Written by
John Headley

Filed under
Cybersecurity, Firewall, Fortinet

Most of the articles you'll read today on the pros and cons of MSP-managed firewalls focus on these two buzzwords: CapEx and OpEx.

Choosing upfront or recurring expenses is certainly an important decision for the business, but as an engineer who installs both managed and non-managed firewalls for our customers, I wanted to share some technical aspects of the decision that should be considered as well.

Are Your Employees Trained?

Organizations that want to migrate to or install a new non-managed firewall should consider if their employee(s) that will be managing this firewall will know how to use it, and this extends beyond simply making a new policy or blocking a website. To make the most of the new firewall, and to ensure the business is protected, the firewall admins should know how to:

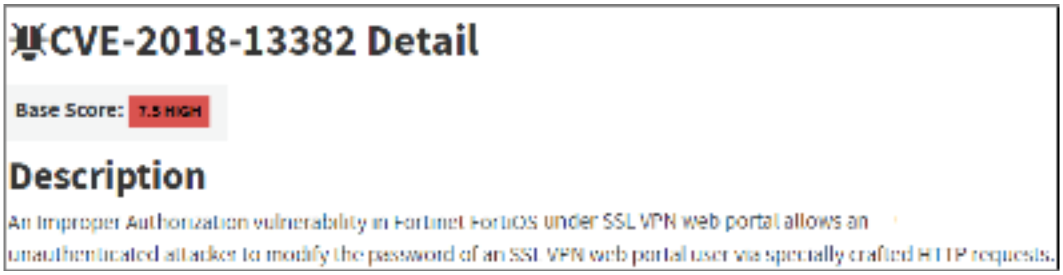
- Ensure any changes are made with configuration and security best practices
- Utilize advanced features of the firewall, such as single sign-on
- Incorporate and use other security devices and software to improve network security, visibility, and management (for example, devices in the Fortinet Security Fabric)
- Troubleshoot all components when an issue arises for quick issue resolution

If this list looks like a tall order for your employees now, then how long will it take them to get up to speed? The Fortinet NSE4 certification, for example, is 5 days of training material, not including engineer practice time. Do your employees have this time to dedicate to learning how to use the FortiGate?

Vulnerability Mitigation and Patching

After investing the time to learn how to use the firewall, will your admins have the time to be able to stay on top of firewall patches and vulnerabilities?

Firewall vendors regularly release updated firmware versions. These updates can include bug fixes, new features, vulnerability mitigations, and can sometimes even introduce new bugs of their own. Your admins will need to adopt a process to keep an eye out for these updates and vulnerability announcements and assess the security risk for your business.



CVE-2018-13382 Detail

Base Score: 7.5 HIGH

Description

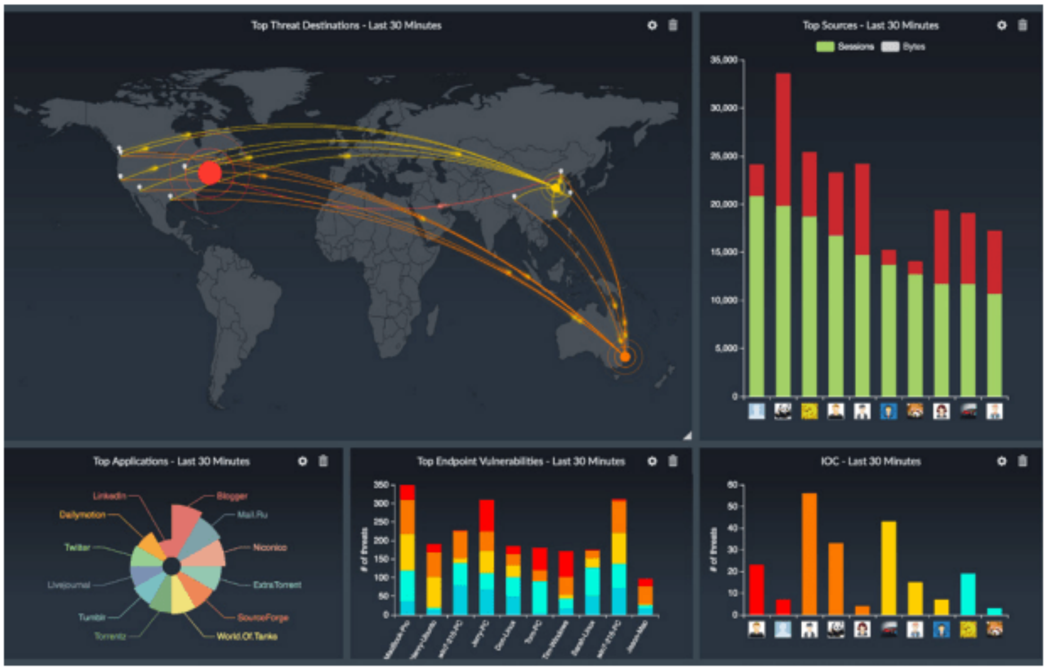
An Improper Authorization vulnerability in Fortinet FortiOS under SSL VPN web portal allows an unauthenticated attacker to modify the password of an SSL VPN web portal user via specially crafted HTTP requests.

Not if, but when the time comes that a firmware upgrade is necessary, your staff should perform their due diligence to ensure the new firmware is fully tested in a lab environment before being rolled out to production to avoid any surprises.

24x7 Monitoring and Incident Response

A “set it and forget it” approach to a firewall does not work in today’s cybersecurity

A "set it and forget it" approach to a firewall does not work in today's cybersecurity landscape. If your organization is going to manage the firewall yourselves, then your employees should be performing many of the same functions as a security operations center (SOC), including continuous monitoring and incident response. Can these admins monitor the firewall logs for indicators of comprise (IOC) and indicators of attack (IOA) and perform incident response 24×7?



If 24×7 is out of the question and you settle for 8×5 monitoring and incident response, your employees still only have so much time in a day. Will adding these responsibilities stretch them too thin and/or compromise the quality of work?

MSP-Managed Firewalls - An Easy Button

Organizations who do not have staff with enough time to dedicate to security, or those lacking staff with necessary security expertise, will find handling all the responsibilities that come with a firewall to be challenging. In this situation, outsourcing these responsibilities to an MSP/MSSP really is an easy button, allowing your business to focus on what it does best instead of trying to quickly master cybersecurity.

If you would like to discuss how VPLS can take ownership and manage the complexities of your firewall, which is such an important cybersecurity investment for your business, then please reach out to us; we'd love to help.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

‹ PREVIOUS
Eliminating Firewall Blind Spots with SSL Decrypti...

NEXT ›
VPLS Acquires New York Data Center and Strengt...

If you enjoyed this article, you'll probably like:

BLOG POST
5 Reasons SOC-as-a-Service
Will Give You Peace of Mind
If you're not sure if outsourcing your SOC is worth it, here are some SOC-as-a-Service features that provide peace of mind.
READ NOW

5 Reasons SOC-as-a-Service Features Help You

March 29, 2022

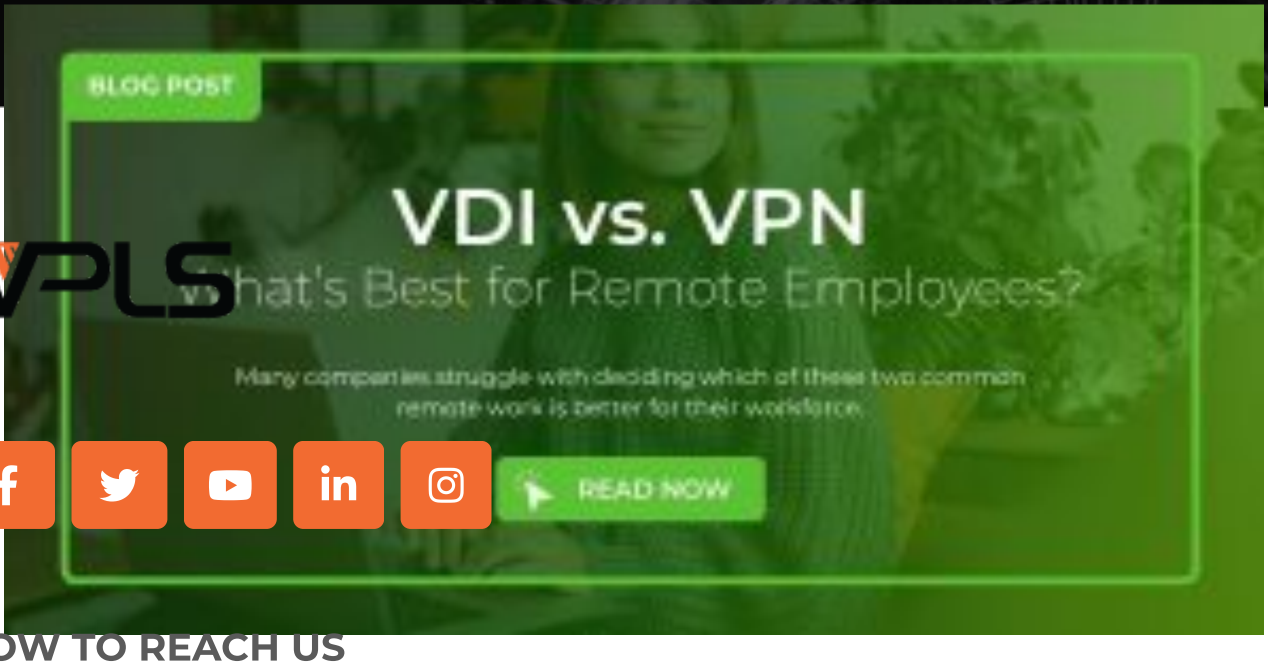
Read More »

BLOG POST
What is SOC-as-a-Service?
SOC-as-a-Service (SOCaaS) functions as an extension of a company's IT department and helps take the guesswork out of cybersecurity.
READ NOW

What Is SOC-as-a-Service?

March 28, 2022

Read More »


BLOG POST
VDI vs. VPN
What's Best for Remote Employees?
Many companies struggle with deciding which of these two common remote work is better for their workforce.
READ NOW

VDI vs. VPN: What’s Best for Remote Employees?

February 14, 2022

Read More »

HOW TO REACH US

Corporate Headquarters
600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service
+1 (888) 365-2656

support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector