Fortinet School Administration Lab

Emma Matsuda

Advanced Cisco Cybersecurity

**Purpose**

The purpose of this lab is to configure our Fortinet firewall so that we can apply it to an imaginary school district. We were told to list out websites and applications that we would block as school administrators and to physically configure the firewall. My group and I decided to look at what categories of filtering existed on the Fortinet firewall first, and then decided if we want specific websites to be blocked.

**Background Info**

FortiOS is Fortinet’s operating system and is the foundation of the Fortinet Security Fabric. The Security Fabri is the industry’s highest-performing and most expansive cybersecurity platform, built on a common management and security framework. It ties all of the Fabric’s security and networking components together in order to ensure seamless integration, enabling the convergence of networking and security functions to deliver a consistent user experience and resilient security posture across all manner environments.

|  |  |
| --- | --- |
| Web filtering feature | Content |
| Content Filtering | * allow administrators to block or allow access to websites based on categories such as adult content, gambling, social media, and more. * Customizable URL filters enable specific websites to be blocked or allowed. * Real-time updates from FortiGuard Labs ensure that the latest malicious sites are included in the blocked list. |
| Safe Search Enforcement | * Can be enforced for major search engines, ensuring that inappropriate content is filtered out of search results. |
| SSL Inspection | * can inspect encrypted traffic to enforce web filtering policies even on HTTPS sites, providing deeper security. |
| User and Group Policies | * can be applied to specific users or groups, offering flexibility and granular control over web access. |

|  |  |
| --- | --- |
| DNS filtering feature | Content |
| DNS-Based Threat Protection | * offer DNS filtering to block access to malicious domains. This helps prevent phishing attacks, malware distribution, and command-and-control communications. |
| Domain Categorization | * can be filtered based on domain categories, providing another layer of control over internet usage |

|  |  |
| --- | --- |
| Application filtering feature | Content |
| Application Control | * can identify and control applications using deep packet inspection. This allows administrators to block or restrict access to specific applications, such as social media apps, streaming services, or file-sharing applications. |
| Granular Policies | * can be highly granular, specifying actions for different behaviors within an application. For example, allowing general use of a collaboration tool while blocking file uploads. |
| Visibility and Reporting | * provides detailed visibility into application usage across the network. This includes real-time monitoring and historical reports, aiding in security audits and compliance. |

**Lab Summary**

1. Start up the Fortinet firewall, connecting the Fortinet port to the computer
2. Enable DHCP and set up the computer accordingly to configure settings on the web GUI
3. Access the web GUI
4. Create and configure security profiles
5. Put the policies into place

**Lab Commands**

No new commands were introduced during this lab, since everything was done in the Fortinet web GUI.

**Network Diagram/Topology**

There are no diagrams/topologies for this lab, since all of the configurations were made in the web GUI – in which they were all for simple configurations to the firewall itself.

**Configurations** – screenshots of the process

|  |  |
| --- | --- |
| 1. Console your computer into Port 1 of the Fortinet firewall |  |
| 1. Enable DHCP on computer.   (or set the IP to 192.168.1.1 255.255.255.0) |  |
| A close up of a message  Description automatically generated | 1. Enter <https://192.168.1.99> to access the Web GUI for the firewall. |
| A screenshot of a login screen  Description automatically generated | 1. Enter the username “admin” and keep the password blank to login. |
| A screenshot of a computer screen  Description automatically generated | 1. Change the password to anything you’d like. Keep the old password blank, since there was none assigned at default. We set ours to “Admin123” |
| A screenshot of a computer  Description automatically generated | 1. Then, the next screen will be the FortiGate Setup. 2. This process would allow the user to specify hostname, register with FortiCare, change Password, Upgrade Firmware, and complete the Dashboard Setup. |
| A screenshot of a computer error message  Description automatically generated | 1. Specify the hostname – we named our firewall “fortigate-40f16” because the device 40f is the version of the model, and our FortiGate was numbered 16. |
| A screenshot of a computer screen  Description automatically generated | 1. Register with FortiCare – we skipped this step initially to get our administrator to sign in for us, but this step is something we can come back to later. 2. FortiCare only for remote management |
| A screenshot of a computer  Description automatically generated | 1. Choose the optimal option for the dashboard – this will give a set of the popular, most used defaults dashboards and FortiView monitors. |
| A screenshot of a computer  Description automatically generated | 1. Once successfully logged in, the default dashboard should show up. |
|  | 1. Under Security Profile, click on AntiVirus. |
|  | 1. Configure the name and the Inspected Protocols, and the APT Protection Options. |
|  | 1. Look through the Inspected Protocols, AP Protection Options, and the Virus Outbreak Prevention to configure the necessary filtering. |
|  | 1. After configured, click “OK” and the AntiVirus filter should appear in the menu. |
|  | 1. Under Security Profile, click on Web Filter. |
|  | 1. Configure the name and the FortiGuard Category Based Filter. |
|  |  |
|  | 1. After configured, click “OK” and the Web filter should appear in the menu. |
|  | 1. Under Security Profile, click on DNS Filter. |
|  | 1. Configure the name and FortiGuard Category Based Filter, like the web filtering. |
|  | 1. Configure the Static Domain Filters, and the other Options that are available. |
|  | 1. After configured, click “OK” and the DNS filter should appear in the menu. |
|  | 1. Under Security Profile, click on Application Control. |
|  | 1. Configure the name and the Categories of applications, choosing the appropriate categories for schools. |
|  | 1. Select the option for Network Protocol Enforcement, then look at the Application and Filter Overrides, and then the other options available. |
|  | 1. After configured, click “OK” and the Application filter should appear in the menu. |
|  | 1. Check if the filtering is working with a website that should be blocked – we tried it with Facebook. |

**Problems**

We didn’t have many problems for this lab, but the one that was not much of a technical difficulty was:

* We lost internet connection one day because of the switch that we were using – although we don’t know what exactly caused the switch to lose internet (we think it could possibly be a physical wiring issue), we put the wires into a different switch and gained internet access. Our Fortinet GUI was accessible again.

**Conclusion**

In this lab, we were instructed to configure antivirus, website, DNS, and application filtering for an imaginary school district as an imaginary school administrator. We created firewall policies to put these filters into use and to block the inappropriate/potentially dangerous websites, applications, and viruses. Through this lab, we learned how to configure a Fortinet firewall in a real-life situation and apply our basic skills into a more complex scenario.

