CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 4, No. 2
October 2025
ISSN: 2832-1006

In this issue:

4. Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure
Reda M. Haddouch, University of Montana
Shawn F. Clouse, University of Montana
Ryan T. Wright, University of Virginia
Theresa M. Floyd, University of Montana
Victor C. Valgenti, University of Montana
Patricia Akello, University of Montana
Thomas P. Gallagher, University of Montana

36. PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings
Melissa Montes, University of Arizona
Shengjie Xu, University of Arizona

51. *Teaching Case:*
Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment
Stanley J. Mierzwa, Kean University
Christoper Eng, Kean University

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2025 ISCAP Board of Directors

Amy Connolly James Madison University President	Michael Smith Georgia Institute of Technology Vice President	Jeff Cummings Univ of NC Wilmington Past President
David Firth University of Montana Director	Mark Frydenberg Bentley University Director/Secretary	David Gomillion Texas A&M University Director
Leigh Mutchler James Madison University Director	RJ Podeschi Millikin University Director/Treasurer	Jeffry Babb West Texas A&M University Director/Curricular Matters
Eric Breimer Siena College Director/2024 Conf Chair	Tom Janicki Univ of NC Wilmington Director/Meeting Planner	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor

Copyright ©2025 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
Saint Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina Wilmington

Thomas Janicki
Publisher
University of North Carolina Wilmington

2025 Review Board

Shawn Clouse
University of Montana

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Zhouzhou Li
Southeast Missouri State University

Sushma Mishra
Robert Morris College

Samuel Sambasivam
Woodbury University

Kevin Slonka
Saint Francis University

Jeff Strain
Brigham Young University - Hawaii

Michael Smith
Georgia Tech

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Teaching Case

Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment

Stanley J. Mierzwa
smierzwa@kean.edu

Christopher Eng
engchr@kean.edu

Center for Cybersecurity
Kean University
Union, NJ 07083, USA

Abstract

As cybersecurity education in higher education continues to evolve, there is a growing emphasis on experiential learning and practical skill development aligned with real-world work roles. Programs designated as National Security Agency Centers of Academic Excellence increasingly require students to demonstrate advanced competencies across a range of cybersecurity domains. Among these, firewall technologies remain foundational to network and information security practices. This paper presents a classroom implementation project that integrates a commercially available virtual firewall into an introductory cybersecurity course. The goal was to provide students with an authentic, hands-on experience in configuring and managing firewall systems. The paper outlines the instructional design, tools used, and step-by-step implementation process, offering a replicable model for faculty interested in incorporating similar activities into their curriculum. Additionally, student feedback collected through a post-activity survey is analyzed to assess the effectiveness of the virtual firewall experience in enhancing learning outcomes. The results suggest that virtual firewalls can serve as a valuable pedagogical tool in cybersecurity education, bridging theoretical concepts with practical application.

Keywords: Pedagogy; Firewalls; Virtual Machines; Cybersecurity; Hands on Learning

Recommended Citation: Mierzwa, S.J., Eng, C., (2025). Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment *Cybersecurity Pedagogy and Practice Journal;* v4(n2) pp 51-66. DOI# https://doi.org/10.62273/BEOJ9082

©2025 ISCAP (Information Systems and Computing Academic Professionals)

Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment

Stanley J. Mierzwa and Christopher Eng

1. INTRODUCTION

This activity provided an opportunity to explore the feasibility and practical case study of using a virtual firewall configuration that was co-designed as a form of teaching pedagogy to provide a real-world connection between professional firewall devices and students. The design was created and pursued between a National Security Agency Center of Academic Excellence in Cyber Defense designated program and an industry provider of cybersecurity tools and technologies, including firewalls, endpoint security devices, intrusion detection, and artificial intelligence capabilities integration. One critical motivation for tackling this effort was to allow students in a cross-disciplinary undergraduate firewall course access to more hands-on experience in using a professional firewall. Additionally, a motivation was to include a student worker from the university's information technology department in the opportunity to partner with a faculty member on this activity. Finally, the inspiration also sought to document the solution in the event that other educators wished to explore the solution utilized.

Content is provided outlining the theoretical framework and model utilized as a guide in this activity, as well as background information on the said course that introduced a virtual machine firewall. Additionally, background information is provided on the technology and foundational settings utilized to make the solution available. Finally, a discussion is provided outlining the feedback assessed from students, activities to pursue going forward, and other implications.

2. THEORETICAL MODEL AND FRAMEWORK

As a theoretical guide to this effort, the instance-based learning theory was employed as a framework. Instance-based learning theory (IBLT) has been employed in previous cybersecurity research to explain situational awareness and provide models for acquiring real-world cybersecurity domain knowledge and experience (Veksler et al., 2018). Instance-based learning theory provides the theoretical background focused on the premise that every decision in a situation can be referenced back to an experience, known as the instance (Dutt et al., 2013). The theory provides a framework to follow in order to attempt to predict activities and timing based on threats through cybersecurity situational awareness (Gonzalez et al., 2003). In this activity, the ability to interface with virtual firewalls, given sequences and scenarios to follow, was approached and aligned with the IBLT by allowing the students to navigate the firewall in the same manner as professionals in the field. A train-the-trainer activity took place with a Fortinet engineer providing in-person instruction on the firewall solution, utilizing the materials that could be used for laboratory experiences (Fortinet, 2024). This action was meant to frame the purpose and reasons one would configure or reconfigure and program a virtual firewall, as well as create a reference point. As an example, a reference point outlined included the acquisition of a firewall, determining if any rules and configurations were to be migrated over to the new device, as well as the initial setup that was detailed for the students to pursue in a vendor-supplied laboratory exercise.

3. FIREWALLS SPECIFIC COURSE

Rapid Literature Review

In its most basic functionality, a firewall is a technological solution that is implemented to secure the perimeter of networks against unwanted breaches and cyber-attacks (Haghighi et al., 2024). In the field of information security, a firewall solution is often implemented by an expert who has experience in creating rules that allow or disallow specific types of network traffic. Network traffic can be filtered between operating zones by using a firewall. The detection and ability to block attacks via Intrusion Detection and Intrusion Prevention Systems (IDS/IPS) are often features built into a firewall device (Hassan, 2020).

Prior to introducing the use of virtual firewalls as part of a pedagogical strategy for a course, several steps were taken to conduct a rapid literature review. These steps included performing focused searches in several scholarly

©2025 ISCAP (Information Systems and Computing Academic Professionals)

databases and repositories. The result of this rapid literature review activity yielded a lack of such documented materials. The search criteria utilized within the demonstrated databases included performing a full-text search at any time and using the focused search terms of pedagogy with the Boolean AND operator and "virtual firewall." The goal of such a search was to quickly glean if other researchers and practitioners have put forth an effort to document the use of virtual firewall solutions, regardless of make, model, vendor, and strategies within the scholarly literature. The results are outlined in Table 1.

Using other novel techniques can be helpful in bringing forward a positive pedagogical method to instill knowledge and background on firewall technologies. Rozinaj et al. (2018) utilized the self-directed learning method with the use of virtual reality and the use of games to engage firewall technology knowledge users of the solution. Gampell et al. (2024) partnered with students, academics, and emergency management professionals to create a pedagogy that supported the use of a gaming platform that engaged students in learning about disaster critical adverse events risk reduction.

The role of firewalls extends to many different computing environments, including those that can be associated with the Internet of Things (IoT), which can be included in such areas as manufacturing. Previous research into the use of Palo Alto firewalls and their integration with IoT was approached as a form of pedagogy to understand such real-world scenarios (Sanchez et al., 2020). Many different firewall vendors provided solutions exist, and in the next section, an outline of the tasks that led to the product utilized in this pedagogical activity.

Database or Source	Search Term	Number of Entries
Google Scholar	"pedagogy" and "virtual firewall"	37
ACM Digital Library	"pedagogy" and "virtual firewall"	4
IEEE/IET Electronic Library	"pedagogy" and "virtual firewall"	0
EBSCOhost	"pedagogy" and "virtual firewall"	0
ABI/INFORM Global	"pedagogy" and "virtual firewall"	2
Homeland Security Digital Library	"pedagogy" and "virtual firewall"	0

Table 1: Academic Literature Rapid Scan

Course Details and Student Population

The cross-disciplinary course is titled Firewalls and Secure CPU (CJ3760). It is available to students pursuing a Bachelor of Science in Computer Science with a Cybersecurity option, a Bachelor of Science in Information Technology with a Cybersecurity option, and a Bachelor of Arts in Criminal Justice with a Cybersecurity concentration. Prerequisites to take CJ3760 include completion of an introductory cybersecurity course named Foundations in Cybersecurity (CJ2630). The prerequisite CJ2630 course includes theoretical content covering a broad set of topics, including an overview of cybersecurity, cybercrime, and the Internet, hacking, intellectual property, scams and fraud, online victimization of individuals, policing the Internet, cyber liberties, and the future of cybercrime and information security. The firewall course has traditionally been given from a theoretical perspective, with limited laboratory exercises, following the guidelines and curriculum outlined in a book published by Pearson. The course is given to students who have taken prerequisite information technology, computer science, or cybersecurity coursework but is considered an introduction to the concept, functionality, and implementation of firewalls to secure computing environments. The course is basically broken up into a 16-week program, with eight weeks focused on firewalls and eight weeks dedicated to securing computing environments, such as workstations, PCs, and other endpoints, via technical group policies and procedures. It is expected to have students from a variety of disciplines of computer science, information technology, and criminal justice. An example of several of the starting point laboratory exercises are presented in Appendix A and B.

4. METHODS

Partnering with a Firewall Vendor

A variety of professional vendor options, in the form of software and hardware, exist for computer networks, servers, workstations, routers, access points, and the like for an enterprise computing operation. A good number of options exist for firewall devices. The devices

can exist in hardware-based appliances with integrated hardware and software or the use of virtual software options to employ on one's hardware platform or virtual server configuration. In the case of this academic activity, to provide students with the ability to engage with a real-world vendor firewall, several vendors were contacted to inquire about the potential for an open educational resource or freely available options for students. An important aspect was to minimize the costs for students to operate firewalls in a laboratory environment. One vendor was rapid to the table with options, Fortinet. There could have been more vendor-based solutions and freely available options. However, Fortinet provided excellent input and guidance and was willing to visit the campus for a full day to both present and work on the established setup and configuration, and provide example labs that could be implemented.

The laboratory hardware components utilized for the firewalls course included the use of standard Windows 10 laptops, having the latest software and security updates, the freely available Oracle VM VirtualBox Manager (version 7.0.14 r161095), and the Fortinet FortiGate VM for VMWare. It was decided to use the available course laptops to minimize the solution requirement constraints since some students use Google Chromebooks, which would cause challenges for the installation and setup. The requirements to run VirtualBox include the use of either an Intel or AMD processor, ample RAM, depending on the operating system one wishes to run, and large enough disk space to host the virtual machine desired (Oracle VirtualBox, 2024). For the specific FortiGate VM used in the lab exercises, a base memory of 5 GB was enabled, along with 8 to 10 GB of disk space. For the virtual provisioning of the CPU, the setting of 4 Cores was configured. The exact image utilized for this case study was named FGT_VM64_HV-v7.4.2.F-build2571-FORTINET. The virtual image for the Fortinet FortiGate can be found by navigating and registering at the FortiGate Cloud web portal (https://www.forticloud.com). In the laboratory scenario utilized in this effort, the product image selected was the FortiGate product for Hyper-V to operate in a Windows Operating System environment.

The laptops are required to be connected to a wired or Wi-Fi network connection with Internet connectivity available in order to register the demonstration version of the virtual firewall. In order to permit the Fortinet FortiGate VM firewall to communicate with the local area network and the Internet, a vital adjustment was necessary. The network setting of the Oracle VM VirtualBox image mounted required the enabling of the network-bridged adapter setting. These settings can be seen in Figure 1.

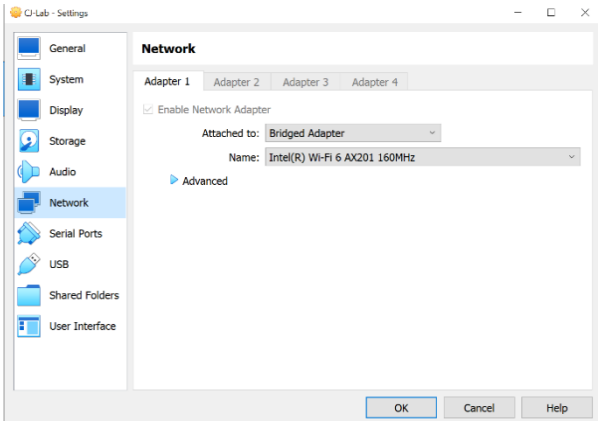


Figure 1: VirtualBox Bridged Adapter

Firewall Configuration and Settings

Upon starting up the Fortinet FortiGate firewall within the VirtualBox manager, the student is confronted with a pure command-line interface. Using a command line interface to configure a firewall provides students with a valuable and realistic knowledge and skills activity. By providing students a task to execute command line functions, they have the opportunity to recognize that firewalls can be configured by using a web interface as well as a traditional command line. A sample screen with the high-level configuration options made available by simply entering "?" is provided in Figure 2. Students were then asked to review all the high-level options available to them when using the command line interface.

```
FGVMEVRMOIQKX9BC login: admin
Password:
Welcome!

FGVMEVRMOIQKX9BC #
config       Configure object.
get          Get dynamic and system information.
show         Show configuration.
diagnose     Diagnose facility.
execute      Execute static commands.
alias        Execute alias commands.
exit         Exit the CLI.

FGVMEVRMOIQKX9BC #
```

Figure 2: Command Line Help Interface to Firewall Settings and Configuration

Initial Assignments and Lab Activities

In addition to providing the setup and installation instructions in order to get the virtual firewalls up and running, students were asked to follow and respond to prompts of growing complexity in navigating the firewall. Greater confidence in getting started with the configuration of a network perimeter defense device provides an

anchor or initiation step that helps one get oriented. Initial steps included logging into the command prompt interface, executing a ping to ensure proper connectivity existed, and proceeding through the steps to obtain the IP address assigned to the firewall. In addition, verifying the DNS settings and ensuring there is the ability to access public websites outside the laboratory environment was possible. The screen examples students would use with these successful steps can be found in Figures 3 and 4.

```
FGVMEVRMOIQKX9BC # execute ping www.yahoo.com
PING me-ycpi-cf-www.g06.yahoodns.net (69.147.92.11): 56 data bytes
64 bytes from 69.147.92.11: icmp_seq=0 ttl=51 time=11.7 ms
64 bytes from 69.147.92.11: icmp_seq=1 ttl=51 time=10.0 ms
64 bytes from 69.147.92.11: icmp_seq=2 ttl=51 time=26.4 ms
64 bytes from 69.147.92.11: icmp_seq=3 ttl=51 time=11.9 ms
64 bytes from 69.147.92.11: icmp_seq=4 ttl=51 time=10.4 ms

--- me-ycpi-cf-www.g06.yahoodns.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.0/14.0/26.4 ms
```

Figure 3: Executing a Command Line Connectivity Test

```
FGVMEVRMOIQKX9BC # diag ip addr list
IP=10.140.35.85->10.140.35.85/255.255.240.0 index=3 devname=port1
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=5 devname=root
IP=10.255.1.1->10.255.1.1/255.255.255.0 index=9 devname=fortilink
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=10 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=12 devname=vsys_fgfm

FGVMEVRMOIQKX9BC #
```

Figure 4: Obtaining IP Address from the Command Line

After struggling a lot with a command line interface, it was then time to provide students with the steps and procedures to access the graphical user interface, which is made available via an HTTPS page. The challenges with the command line interface included ensuring that commands were executed with proper syntax and with passing parameters. This was a new concept for some of the students who did not have a deep technical academic background, for example, those pursuing criminal justice degrees. Understanding the concept of getting started with a firewall configuration with a command line is a critical competency to develop since the practice can translate to other appliance devices, such as network switches. Students were instructed to utilize the private IP address obtained in an earlier lab to bring up the HTTPS interface in a browser. The login prompt provided in the browser, if successfully rendered, and the initial Fortinet FortiGate dashboard pages can be seen in Figures 5 and 6. The dashboard provided the students the opportunity to witness the web interface utilized to configure a firewall and monitor its activity.

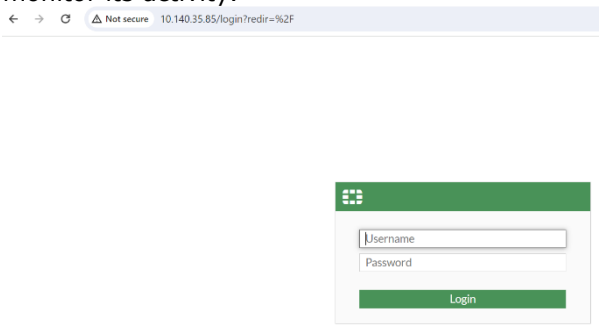


Figure 5: Firewall HTTPS Interface Login

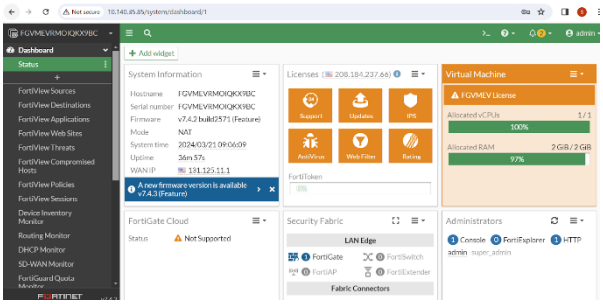


Figure 6: Virtual Firewall HTTPS Dashboard

5. RESULTS

The field of cybersecurity, including the technology and solutions that can be implemented, as well as the practices and procedures to consider, is vast. Providing students with more interactive and hands-on activities is beneficial in understanding the many building blocks required to secure an organization and computing environment. The pedagogy involved in instructing students on content related to firewalls will be beneficial in building more excellent competencies with the introduction of a "real-world" firewall device with which to engage. In addition to a critical theory, firewalls are a specific product set solution. They are still considered standard devices for implementation in any company, business, agency, or organization that connects to the public Internet. In fact, many organizations employ and have implemented many firewalls within their infrastructure in order to create separate networks with greater granular control. The use of a set of laboratory exercises to complement seeing a firewall first-hand can be beneficial to a recent cybersecurity graduate entering the field.

6. DISCUSSION AND IMPLICATIONS

The feedback survey results from students who utilized the firewall virtual machine configuration

outlined in this document found it to be meaningful. Every student in the course reported that this was their first time engaging, navigating, and configuring a firewall security appliance and device. All students (*N*=14) reported that the complement of using a virtual firewall device improved their understanding of how such devices can be used in businesses and organizations to protect the environment. Improving and enabling greater competency was reported as achieved. An open question was administered to obtain further suggestions for improvements in future classes. A common theme suggested was to engage even further with more laboratory time to allow for greater self-learning and optional laboratory assignments. The self-report web-based Google Forms surveys were administered to all the students in this introductory firewall course at the end of the course, as well as laboratory exercises.

7. CONCLUSION

Cybersecurity education at both undergraduate and graduate levels benefits from diverse pedagogical approaches that blend theory with practice. This paper demonstrated how integrating virtual machine firewalls into coursework can significantly enhance students' practical understanding of network security technologies. By moving beyond theoretical analysis, students engage directly with real-world tools, gaining hands-on experience that mirrors professional environments. This instructional design is particularly valuable for students at the introductory level, who may have limited exposure to firewall technologies. Providing access to authentic, interactive learning experiences helps bridge the gap between conceptual knowledge and applied skills—skills that are essential in nearly every organization with networked systems. Looking ahead, there is strong potential to further enrich the curriculum by revisiting the Foundations in Cybersecurity course. Enhancements could include expanded coverage of command-line interface tools and additional lab-based exercises that reinforce technical competencies. Such adjustments would not only deepen student engagement but also better prepare them for the evolving demands of cybersecurity roles in the workforce.

8. LIMITATIONS

Many firewall vendors exist, and even open-source firewalls could have been used in this pedagogy exercise and approach. Without the existence of a classroom full of physical firewalls, future exercises can be undertaken to evaluate other vendors or open-source firewalls that could be used to introduce students to these perimeter security devices and solutions. In addition, there is a limitation related to evaluating whether any cloud-based solutions exist that would eliminate the need to mount a virtual machine image on individual laptops. A limitation related to the theoretical framework or theory to follow as part of this activity is presented. Alternative theories that can be considered relevant to this pedagogy activity are available and could have been approached as part of this study paper. Finally, all students were polled at the end of the course to determine their feedback on using the virtual firewall solution. A limitation arose from not having a pre-course set of questions that asked students if they needed a more significant background in using a command-line interface prior to engaging with the virtual firewalls. The academic literature rapid scan in Table 1 could have also included the word "education" in addition to pedagogy, to possibly result in more found references.

9. ACKNOWLEDGEMENTS

Successful technical projects—especially those involving multiple components and collaborators—depend on the dedication of individuals who recognize the value of the work and contribute meaningfully to its success. We extend our sincere appreciation to Richard (Rik) Maerz, Cass Hill, and Troy Gallo of Fortinet for their generous support and collaboration in making open educational resources accessible to students. Their commitment to advancing cybersecurity education through practical tools and industry partnerships was instrumental in the implementation of this project. We also gratefully acknowledge Christopher Eng, a Kean University student and part-time staff member in the Office of Computer and Information Services, for his meticulous efforts in testing the virtual machine and firewall image. His work ensured compatibility with laboratory laptops and helped create a seamless experience for students engaging with the virtual firewall environment.
Finally, we would like to recognize the forward-thinking contributions of Michael Fagioli and Jessica Jones from the Kean Global and Online team. Their innovative vision helped shape the next iteration of the *Firewalls and Secure Computing Enterprise* course, which will feature enhanced instructional elements—including the integration of cybersecurity-themed Escape Rooms—to further engage students through immersive, experiential learning.

10. REFERENCES

Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2013). Cyber situation awareness: Modeling detection of cyber-attacks with instance-based learning theory. *Human Factors*, *55*(3), 605-618. https://doi.org/10.1177/0018720812464045

Fortinet. (2024). *Fast Track Workshops Experience the Fortinet Security Fabric in Action.* Retrieved August 14, 2024 from https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/Brochures/brochure-ftnt-fast-track.pdf

Gampell, A. V., Gaillard, J. C., Parsons, M., Le De, L., & Hinchliffe, G. (2024). Participatory Minecraft mapping: Fostering student's participation in disaster awareness, 48. https://doi.org/10.1016/j.entcom.2023.100605

Gonzalez, C., Lerch, J. F., & Lebiere, C. (2003). Instance-based learning in dynamic decision making. *Cognitive Science, 27*(4), 591-635. https://doi.org/10.1207/s15516709cog2704_2

Haghighi, M. S., Farivar, F., & Jolfaei, A. (2024). A machine-learning-based approach to build zero-false-positive IPSs for industrial IoT and CPS with a case study on power grid security, *IEEE Transactions on Industry Applications, 60*(1), 920-928. https://doi.org/10.1109/TIA.2020.3011397

Hassan, I. (2020). Teaching cybersecurity to computer science students utilizing terminal sessions recording software as a pedagogical tool. IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2020, pp. 1-8. https://doi.org/10.1109/FIE44824.2020.9274268

Oracle VirtualBox. (2024). VirtualBox End-user documentation. Retrieved August 22, 2024, from https://www.virtualbox.org/wiki/End-user_documentation

Rozinaj, G., Vančo, M., Vargic, R., Minárik, I., & Polakovič, A. (2018). Augmented/virtual reality as a tool of self-directed learning. *25th International Conference on Systems, Signals and Image Processing (IWSSIP)*, Maribor, Slovenia, 2018, 1-5. https://doi.org/10.1109/IWSSIP.2018.8439309

Sanchez, J., Mallorqui, S., Briones, A., Zaballos, A., & Corral, G. (2020). An integral pedagogical strategy for teaching and learning IoT cybersecurity. *Sensors, 20*(14), 1-35. https://doi.org/10.3390/s20143970

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in Psychology, 9*(691). https://doi.org/10.3389/fpsyg.2018.00691

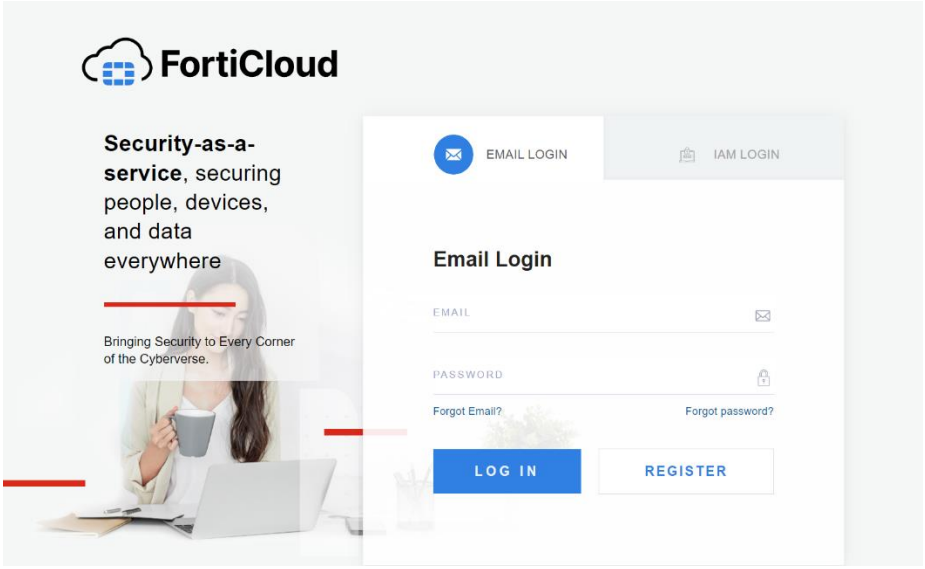
APPENDIX A

Fortinet Virtual Firewall Setup and Installation Steps

The steps below include the tasks that prepared the laboratory laptops to run the Oracle VirtualBox and virtual Fortinet firewall solution.

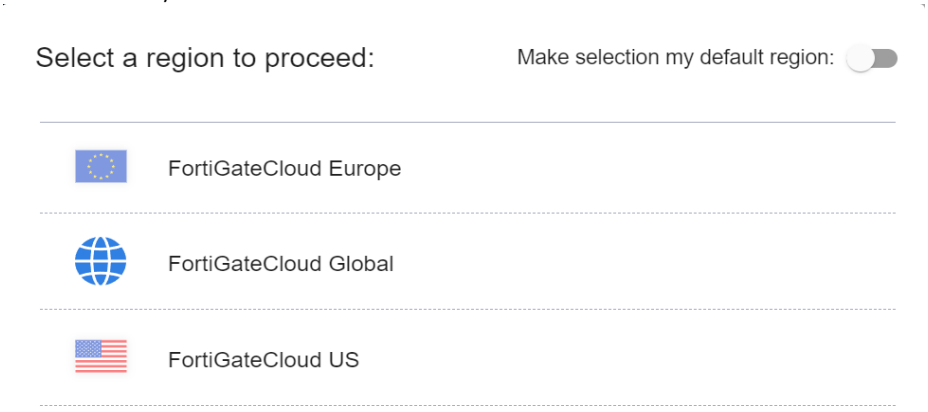
Download the Virtual Firewall Image

1. Navigate to the https://www.forticloud.com website.
2. From the FortiCloud website, click on the link to register and create a free account.



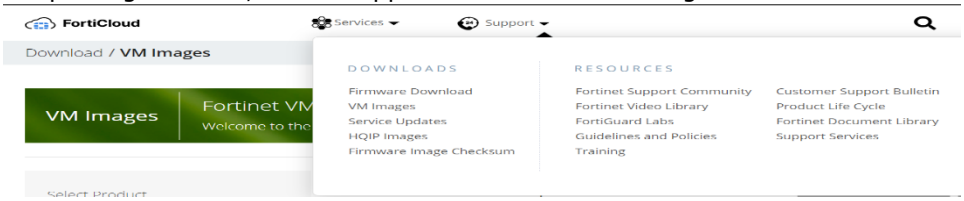
a.

3. After successfully logging into the FortiCloud website, select the appropriate region for your location. In our case, select FortiGateCloud US.



a.

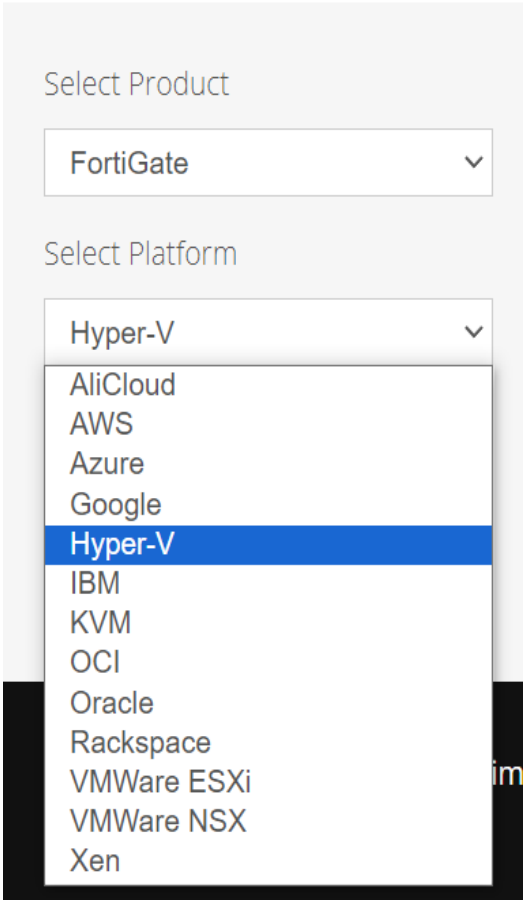
4. From the top navigation bar, select Support-Downloads-VM Images.



a.

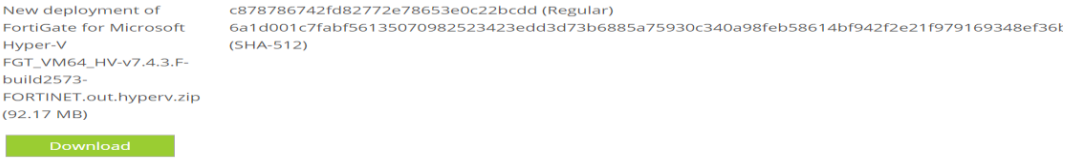
5. From the dropdown menu provided, select the product FortiGate and the Hyper-V platform.

a.



6. Select the FortiGate for Microsoft deployment.

a.



7. Click Download, and make note of the location where the FortiGate virtual firewall image was saved on the laptop hard drive.

Installation and Configuration of VirtualBox

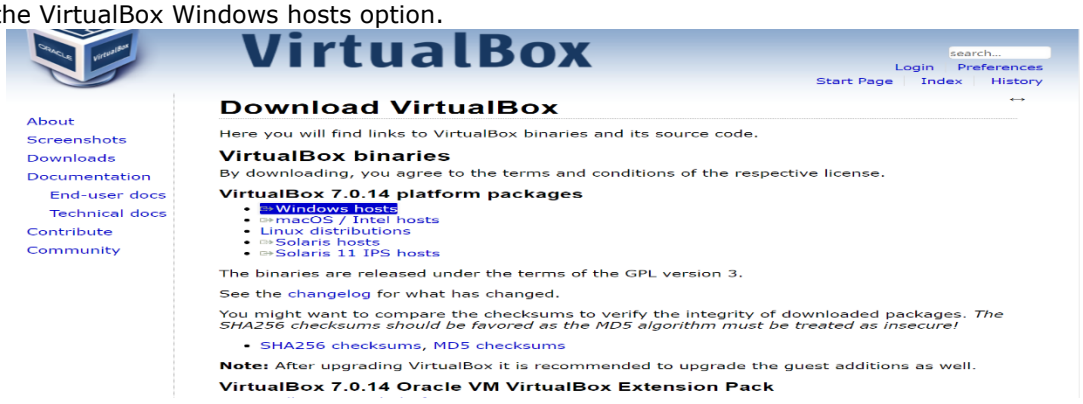
1. Navigate to the website https://virtualbox.org.

a.



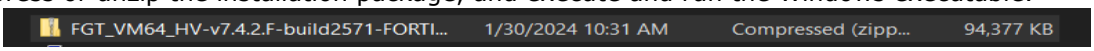
2. From the left navigation bar, click Downloads.
3. Select the VirtualBox Windows hosts option.

a.



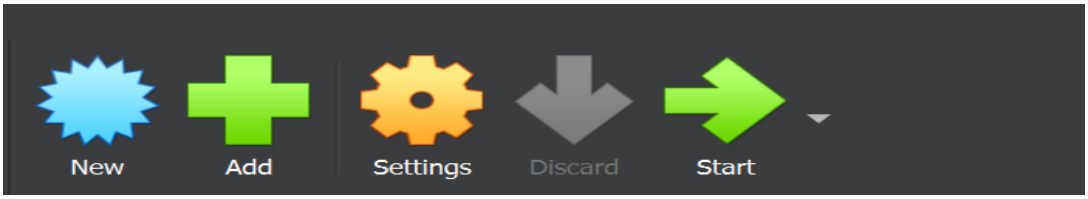
4. Uncompress or unzip the installation package, and execute and run the Windows executable.

a.



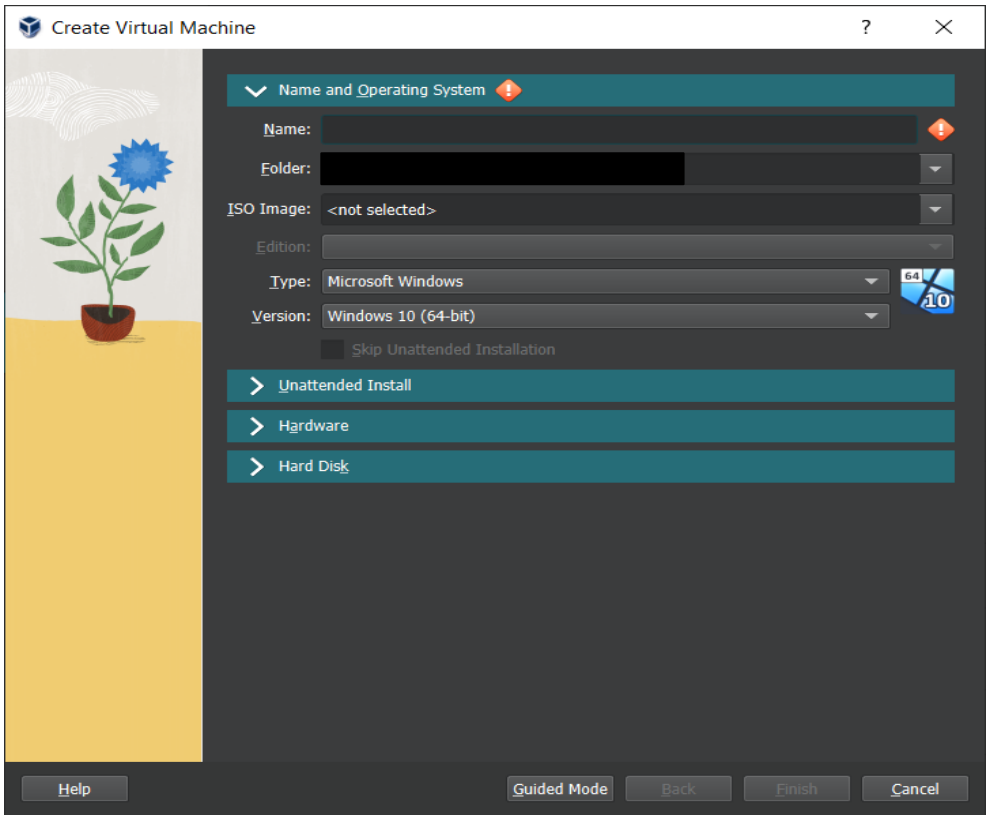
5. From the menu options available, click New to create a new virtual image for the Fortinet virtual firewall.

a.



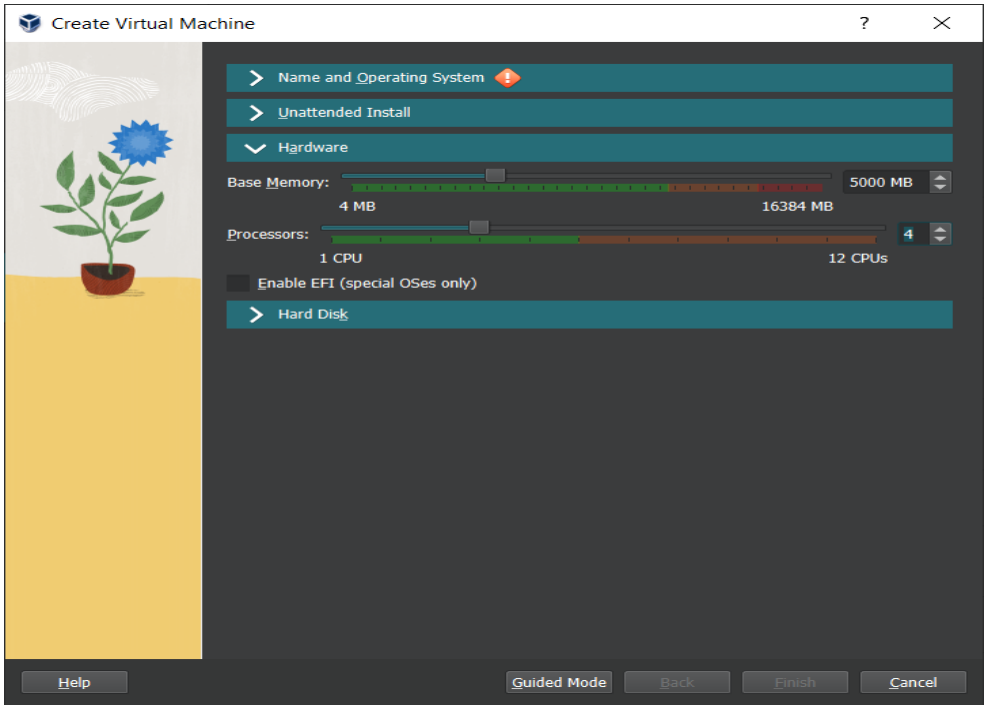
6. Name the virtual machine Fortinet Virtual Firewall

a.

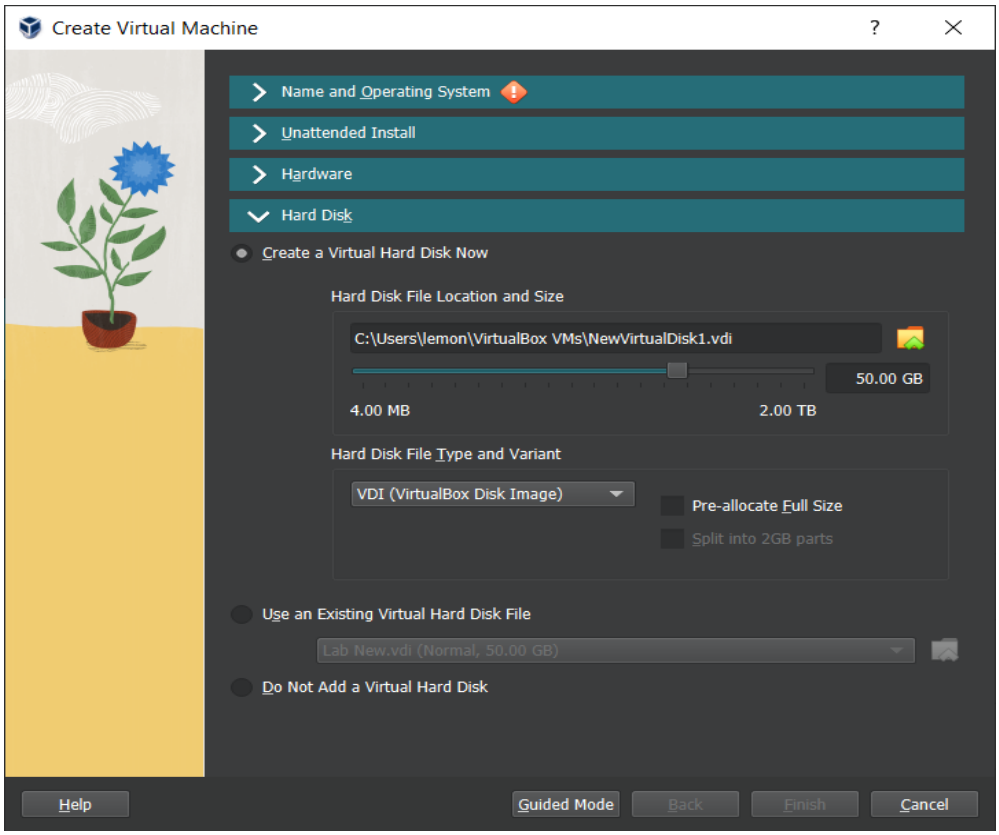


7. Proceed and step through the configuration steps, selecting the Base Memory of 5GB and 4 CPUs.

a.



8. Select the location to store the Virtual Hard Disk and allocate it with 50GB.

a. 

9. When presented with the File Explorer, click on the Virtual Hard Disks and select the downloaded FortiGate VHD image in Step 7 above.

APPENDIX A

Starting Virtual Machine – Fortinet Virtual Firewall – FortiOS

The steps and procedures below are utilized to configure the virtual Fortinet firewall on the Cyber Crime Lab laptops. The procedures are essential to ensure future lab experiments and demonstrations can be activated and work properly.

Command Line Interface

1. Boot the laptop.
2. Connect to the college Wi-Fi network in the cybercrime lab.
3. Ensure VirtualBox is configured with the Bridged Adapter setting enabled.
4. Login Using Command Line Interface (will be asked to change password).
    a. U: Admin
    b. P: password
5. Ping a site (to ensure connectivity routing outside the lab).
    a. Exec ping www.yahoo.com
    b. Verify connectivity
6. Obtain the IP address of the virtual firewall (use the command line).
    a. Diag IP Addr List
    b. Note Port1
    c. Obtain the IP Address for Port1

Web Interface

1. Open a web browser from the said laptop outside of the VirtualBox application.
2. Navigate to the IP address from Step 6 above.
3. Login – same credentials as Command Line Interface.
4. License
    a. Login to https://support.fortinet.com
    b. Set up account
    c. You must check your email – use @kean.edu email.
5. From the web interface – log in to apply the demo license.

APPENDIX B

Connecting to and Navigating the Virtual FortiGate GUI

In this exercise, you will have the opportunity to connect to the FortiGate GUI and explore the pre-configured Management interface.

Port1 on FGT-EDGE has been pre-configured to include the following settings, which are not part of the default FortiGate configuration:

• **IP/Netmask**: 192.168.0.101/255.255.255.0

• **Administrative Access**: HTTPS, HTTP, PING, FMG-Access, SSH, and Security Fabric Connection
A password was also set for the default **admin** account.

Tasks
1. Return to the **Lab Activity Tab**. Click **FGT-EDGE** in the sidebar menu under **Core**, and then click **HTTPS** to access the **FGT-EDGE** device.
2. Login using the default admin account by entering the following credentials:
Username: admin
Password: Fortinet1!
3. You have access to the FortiGate GUI.
4. Click **Network** > **Interfaces** and select **Management Network (port1)**. Click **Edit**. You can also double-click the interface. **Note:** Do not change any of the settings currently configured for port 1.
5. The pre-configured settings appear under **Address** and **Administrative Access**.
6. Click **Cancel** to exit without changing any settings.

Stop and Think
Security best practices recommend configuring management interfaces with the minimal level of administrative access required. The level of access is usually based on the role of the interface, accessibility to the interface, and the level of authority for users with access to that interface. Consider an organization that has the following infrastructure deployed:
• FortiGate management using FortiManager Cloud services
• FortiGate two-factor authentication via FortiToken Mobile
• Remote APs participating in the organization's Security Fabric

Set the System Time Background
In this exercise, you configure the system time on FGT-EDGE to AcmeCorp's local time zone, Eastern Standard Time.
Note: For the purpose of this lab, you must select Eastern Standard Time. Making changes to the time zone could disrupt the lab functionality.

Tasks
1. Click **System** > **Settings**.
2. Under **System Time**, select **(GMT-5:00) Eastern Time (US & Canada)**.
3. Set **Set Time** to **NTP**.
4. Set the **Select server** to **FortiGuard**.
5. Select **Apply**.

Create Firewall Addresses and an Address Group
Firewall addresses define sources and destinations of network traffic and are used when creating firewall policies. Address groups are used to group firewall addresses that require the same firewall policy.

In this exercise, you create three firewall addresses, one for each network. You also create a firewall group that contains the addresses for the Sales and Finance networks. By creating an address group that contains the addresses for both Sales and Finance, you can now configure FGT-EDGE to treat traffic from both of these networks in the same way.

Tasks
1. Click **Policy & Objects** > **Addresses** and then use the **Create New** drop-down menu to select **Address** and create an address for the Sales network.
2. Configure the following settings:
• **Name**: Sales
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.10.0/24
• **Interface**: **any**
3. Click **OK**.
4. Click **Create New** > **Address** to create an address for the Finance network.
5. Configure the following settings:
• **Name**: Finance
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.20.0/24
• **Interface**: **any**
6. Click **OK**.
7. Click **Create New** > **Address** to create an address for the DC network.
8. Configure the following settings:
• **Name**: DC
• **Type**: **Subnet**
• **IP/Netmask**: 172.16.100.0/24
• **Interface**: **any**
9. Click **OK**.
10. Use the **Create New** drop-down menu to click **Address Group**.
11. Configure the following settings:
• **Group name**: Sales and Finance
• **Type**: **Group**
• **Members**: **Finance** and **Sales**
12. Click **OK**.

Apply Antivirus Scanning and SSL Inspection Background
In this exercise, you create an antivirus profile for Sales and Finance to protect network traffic from virus outbreaks. You also apply full SSL inspection to allow FGT-EDGE to inspect encrypted traffic. When you apply full SSL inspection to traffic, network users may receive a security certificate warning in their internet browser. In this exercise, Bob's computer has been pre-configured to prevent any warnings from appearing.

Tasks
1. Return to the **FGT-EDGE** tab.
2. Click **Security Profiles** > **AntiVirus** and click **Create New**.
3. Set the **Name** to Sales and Finance.
4. Under **Inspected Protocols**, turn on all protocol options.
5. Turn on the **AntiVirus scan** and set it to **Block**.
6. Leave the **Feature set** as **Flow-based**. Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content. Proxy-based inspection reconstructs content that passes through the FortiGate and inspects the content for security threats.
7. Under **APT Protection Options**, turn on **Treat Windows Executables in Email Attachments as Viruses** and leave **Include Mobile Malware Protection** turned on.
8. Under **Virus Outbreak Prevention**, turn on **Use FortiGate Outbreak Prevention Database** and set it to **Block**. This allows the FortiGate antivirus database to use third-party malware hash signatures curated by the FortiGuard to block detected viruses before a FortiGuard signature is available.
9. Click **OK**.
10. Click **Policy & Object** > **Firewall Policy**, click **Sales and Finance**, and click **Edit**.
11. Under **Security Profiles**, turn on **AntiVirus**. Use the drop-down menu to select the **Sales and Finance** profile.
12. Use the **SSL Inspection** drop-down menu to select **deep-inspection**. This turns on full SSL inspection so FGT-EDGE can inspect encrypted traffic.
13. Click **OK**.

14. Connect to the **Bob** device.
15. Run Chrome and click the browser bookmark **EICAR**. This website contains a file that you can use to test your antivirus scanning.
16. Under the **Download area, use the secure SSL-enabled protocol https, and** click **eicar.com**.
17. FGT-EDGE blocks the file from downloading.

Add a Default Route Background
In this exercise, you add a default route to the FortiGate that the FortiGate uses to send traffic outside of the internal network.

Tasks
1. Click **Network** > **Static Routes** and click **Create New**.
2. Set **Destination** to **Subnet** and leave the destination IP address set to 0.0.0.0/0.0.0.0.
3. Set **Gateway Address** to 100.65.0.254.
4. Set **Interface** to **ISP1 (port6)**, the internet-facing interface.
5. Click **OK**.
6. To test internet connectivity, click **>_** in the top right-hand corner to connect to the CLI console.
7. Type the command execute ping 8.8.8.8 and press Enter.
8. The FortiGate connects to the internet, producing an output similar to the screenshot below:
9. Close the CLI console by clicking on the **X** in the upper right corner.

Note: Fortinet provided the subset of laboratory examples provided in Appendix B for use by the faculty and students (Fortinet, 2024, August 14).