cit470

Task: Above-and-Beyond 1: Local GNS3

Complete an optional project that creatively goes “above and beyond” the tasks you and your partner(s) are working on in your team projects.

Students that achieve a passing grade with each of their team tasks and peer evaluations will pass the course with a C grade. Above-and-beyond tasks are projects that students may accomplish individually. There are eight Above-and-beyond opportunities in this course.

After completing this task, your own computer will have a functional working mock-up of your team’s infrastructure. Your mock-up will mimic many aspects of the network that you and your partner(s) build in the Firewalls team task.

Tools

- Sign up for a free gns3.com account: https://www.gns3.com/account/login
- A desktop or laptop computer with at least 16GB RAM
- A Type-II Hypervisor, suitable to run the KVM (kernel-virtual-machine) features of the GNS3 VM that accompanies the GNS3 application:
  - Oracle VirtualBox
  - VMware Workstation Player (Windows) or VMware Fusion Player (macOS)
  - Microsoft Hyper-V Manager
- GNS3 software components:
  - The GNS3 VM: https://www.gns3.com/software/download-vm
  - The GNS3 application: https://www.gns3.com/software/download
    - *(If you are using an Intel-based Apple computer running macOS, you will also need to download and install Royal TSX, then launch Royal TSX and install its VNC plugin component.)*

If your computer isn’t capable of satisfying all of these requirements, you should defer this project and choose to work on different above-and-beyond opportunities. There are still enough opportunities to earn the grade you desire, so don’t fret if you are unable to complete this GNS3 project.

Requirements

- Install the GNS3 VM, and verify that it has KVM support available.
- Install the GNS3 application, and configure it to use the GNS3 VM for appliance images.
- Create a working mock-up of your network diagram, including the following nodes:
    - Deploy a “NAT” cloud endpoint device as your **outside** security zone.
    - Deploy four “Ethernet Switch” devices, with one of each as the central node of your **interconnect**, **dmz**, **inside**, and **secure** zones.
    - Deploy an “Internet-facing” firewall node with four connections: one to your **outside** NAT node, another to your **dmz** switch node, a third to your **inside* switch node, and finally a connection to your **interconnect** switch node.
        - configure this firewall to automatically get a DHCP address from the **outside** “NAT” cloud, but configure your selected static gateway IP addresses on its **dmz**, **inside**, and **interconnect** interfaces.
    - Deploy a “Secure-facing” firewall node with two connections, to your **secure**, and **interconnect** switches.
        - configure your selected static gateway IP addresses on its **secure**, and **interconnect** interfaces.
    - Deploy two “VPCS” (virtual PC stub) endpoints, one each connected to the switches in your **dmz** and **secure** zones.
        - configure and save appropriate static IP addresses and default gateway routes on each VPCS.
    - Download and deploy a “webterm” endpoint device, and connect it to your **inside** switch.
        - configure an appropriate static IP address on the webterm, with its default route through the Internet-facing firewall.
    - configure appropriate policy rules on each firewall, such that:
        - the endpoint devices in the **dmz**, **inside**, and **secure** zones can ping each other (via the usual ICMP Ping protocol)
        - the endpoint devices in the **dmz** and **inside** zones can successfully ping Google’s public DNS server 8.8.8.8, and the (**inside** zone) webterm’s browser can access web sites (such as Google, or Amazon, or Instagram, etc.)
        - the endpoint device in the secure zone *cannot* ping or otherwise connect to any Internet host in the **outside** zone.

Deliverable

Upload an illustrated tutorial, in which you explain what you did and how you accomplished it.

- Your document should be clear enough that one of your peers would be able to follow your instructions and accomplish the same tasks.

- Identify any difficult or challenging parts of the project, and clearly explain how you diagnosed and overcame your obstacles.
- Include a few cropped screen captures where appropriate.
- There are a lot of requirements to satisfy, so your document will be many pages long.

Scoring Rubric

- If your tutorial satisfies every requirement outlined above, you will earn a passing score (one point).
- If your tutorial does not satisfy any one of the above requirements, you will earn no points. Your must then address any deficiencies and re-upload corrected documents until you earn the passing score.

Hints

- A fresh install of GNS3 includes several switch and endpoint device node templates.
  - Ethernet Switch, NAT (cloud), and VPCS are already available.
- Other GNS3 device note templates must be downloaded separately.
  - The “webterm” endpoint is not available by default. To download the webterm template, select “New template” from the file menu, and choose to install from the GNS3 server. You’ll find it in the list of guest appliances.
  - No routing or security devices are pre-installed with GHS3 by default. To download a firewall device, select “New template” from the file menu, and choose to install from the GNS3 server.
    - Recommend free firewall template: pfSense.
    - Other free router or firewall device templates that might be suitable include: ClearOS CE, OpenWrt, OPNsense, Smoothwall Express, or VyOS.
  - Virtual appliances image files for these device templates must be downloaded and imported separately. (Note: most of the other available firewall and router templates are for commercial VMs that require purchased licenses.)