cit470

Task: Perimeter Firewalls

Work with your team to deploy and configure an internet-facing firewall and a secure-facing firewall, with policies that let your server VMs communicate between security zones, and enable Internet access for your DMZ and inside server VMs.

Tools

- A Palo Alto PA-200 firewall to enforce policies regarding Internet-facing network traffic, and a FortiNet FortiGate firewall "VDOM" (virtual domain) to enforce policies regarding secure-facing traffic.

Your instructor will provide credentials for each team to access these firewalls.

- Your team's network diagram, annotated with the following necessary data:
  - Your outside zone's VLAN-id, network address/subnet mask, and your outside router's IPv4 address. **2022/01/11 Update: our entire class section shares the same outside zone.**
    - IPv4 address of your Internet-facing firewall's outside "dynamic-NAT" interface.
    - IPv4 addresses of two publicly available DNS servers. *Examples: Cloudflare DNS (1.1.1.1, 1.0.0.1), Google DNS (8.8.8.8, 8.8.4.4), NeuStar Verisign (64.6.64.6, 64.6.65.6), etc.*
  - Your DMZ VLAN-id and network address/subnet mask.
    - IPv4 address of your Internet-facing firewall's DMZ interface. (This will be your team's DMZ default gateway address.)
    - IPv4 addresses of your DMZ Windows Server and Linux server VMs.
  - Your inside zone's VLAN-id and network address/subnet mask.
    - IPv4 address of your Internet-facing firewall's inside zone interface. (This will be your team's inside zone default gateway address.)
    - IPv4 addresses of your inside zone Windows Server and Linux server VMs.
  - Your secure zone's VLAN-id and network address/subnet mask
    - IPv4 address of your secure-facing firewall's secure zone interface. (This will be your team's secure zone default gateway address.)
    - IPv4 addresses of your secure zone Windows Server and Linux server VMs.
  - Your interconnect zone's VLAN-id and network address/subnet mask

    - IPv4 address of your Internet-facing firewall's "interconnect" interface. (This will be a separate gateway toward your secure-facing firewall.)
    - IPv4 address of your secure-facing firewall's "interconnect" interface. (This will be the corresponding gateway toward your Internet-facing firewall.)

Your team's assigned VLAN IDs and public IPv4 addresses are listed here.

Requirements

Summary: configure admministrator accounts, sub-interfaces, routing, policy rules, and NAT funcitonality on your Internet facing firewall, sufficient for your DMZ and inside servers to access the Internet and receive OS updates. Also, configure appropriate static routes and access policies on both firewalls, so that you can remotely access and administer your servers across zone boundaries.

- Manage your Internet-facing firewall using its OOB (out-of-band) management IP address. Log in with credentials provided by your instructor.
    - Configure a "Device Administrator" account for each team member. Then log out, and log in again with your own credentials.
    - ~~Configure a new "virtual router" named T##-router. (Substitute your team's number for ## in the virtual router's name.)~~ **2022/01/11 Update: our entire class section shares a virtual router named 470-02.**
    - ~~On your team's Internet-facing firewall, configure security zones named T##-outside, T##-dmz, T##-inside, and T##-interconnect. (Substitute your team's number for ## in the zone names.) Select "layer3" for the type of each zone.~~ **2022/01/11 Update: our entire class section shares the same routed zones named outside, dmz, inside, and interconnect.**
    - Configure three sub-interfaces, one for each of your team's DMZ, inside, and interconnect zones. Place each sub-interface in your team's virtual router. Configure each sub-interface with its required 802.1q VLAN tag (layer-2 configuration), and with its required IPv4 IP address and subnet mask (layer-3 configuration). To assist with troubleshooting, configure each sub-interface with a management profile that lets it respond to ICMP "pings" (echo requests).
    - ~~Configure a default route. (The "next hop" should be your outside router's IP address.)~~ **2022/01/11 Update: The default route is already preconfigured for the shared outside zone.**
    - Configure an additional static route to your secure zone. (The "next hop" should be the secure-facing firewall's ~~inside~~ interconnect zone IP address.)
    - Configure a "dynamic NAT" policy that translates outbound connections from your DMZ and inside zones to the address of the outside interface.

    - Configure a “restrict-secure” policy that allows hosts in your secure zone to communicate with DMZ or inside hosts, but disallows them from communicating directly to hosts in the outside zone.
    - Configure an “Internet-egress” policy that allows hosts in your DMZ and inside zones to use any application protocol to communicate with any host in the outside zone.
    - Configure a “DMZ-access” policy that allows hosts in your inside zone to use any application protocol to reach any host in your DMZ.
    - Configure “remote-admin” policies that allow hosts in your DMZ to use SSH or RDP to reach any host in your inside and secure zones.
        - To assist with troubleshooting, configure your firewall policies to log the beginning and end of each network connection.
- Manage your secure-facing firewall “in-band,” using the secure zone IP address already configured for you. Log in with credentials provided by your instructor.
    - Configure an administrator account for each team member. Then log out, and log in again with your own credentials.
    - On your team’s secure-facing firewall, configure another sub-interface for your team’s interconnect zone, configured with its required VLAN tag, IPv4 address/subnet mask, and also configured to respond to ICMP “pings” (echo requests).
    - Configure a default route on the secure-facing firewall. (The “next hop” should be the interconnect zone address of your Internet-facing firewall.)
    - Configure policies that allow hosts in your secure zone to use any application protocol to communicate with hosts in your DMZ and inside zone.
    - Configure policies that allow hosts in your inside zone to use SSH or RDP to communicate with hosts in your secure zone.
- Verify that your DMZ and inside zone hosts can access the Internet and receive OS updates.
- Verify that your VMs can use SSH and RDP to connect across zone boundaries to other VMs.
- Verify that your secure zone hosts cannot directly access the Internet.

Deliverable

Upload an illustrated tutorial, in which you explain what your team 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. Also upload your updated and annotated network diagram.

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 team must then address any deficiencies and re-upload corrected documents until you earn the passing score.

Examples

- Initial PA-200 firewall configuration
- Initial FortiGate firewall configuration