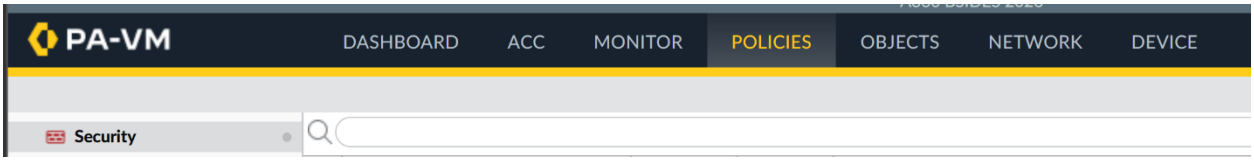
Welcome to the ADVANTUS360 BSides Calgary 2026 Blue Team Walkthrough! This document is meant to serve as an introductory guide to a Palo Alto Networks NGFW. I encourage you to explore the documentation when possible. There are questions at the end of this walkthrough that are on the bingo card, but there are also questions that help you deepen your understanding of the material. I implore you to try your best on all questions!

Walkthrough:

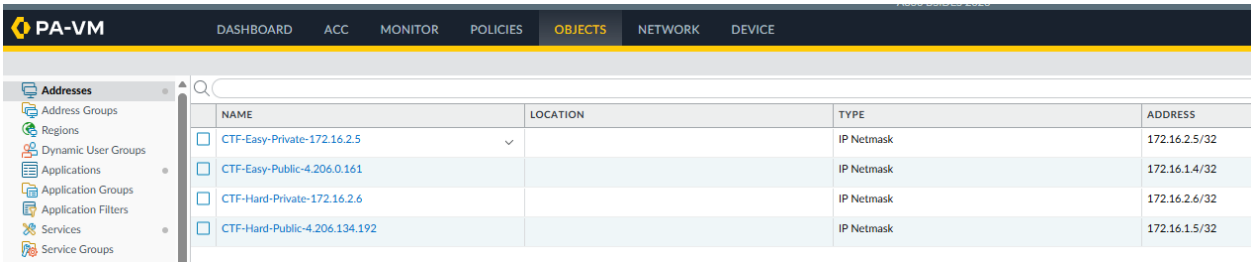
- Here is what you need to access the PA-VM NGFW:
    - Firewall: https://firewall.advantus360.xyz
        - Note that you may need to disable any client VPNs in use on your endpoint. Ironic, isn't it? To access the firewall above you may need to circumnavigate your own firewall!
    - Credentials:
        - Username: bsidesuserRO
        - Password: Bsid3s2026!4ever
- In the first section we discuss Security Policy Rules (SPRs). It is critical to remember that every NGFW has two pieces of functionality:
    - 1. Routing
    - 2. Security
- PAN-OS is the underlying proprietary OS used on a Palo Alto NGFW. It uses the logical concepts of *zones* which are associated with physical and logical interfaces. Interfaces are assigned to zones, and zones are referenced in Security Policy Rules.
- Let us start by examining Security Policy Rules (SPRs)! Navigate to the Policies tab, and select Security on the left-hand side



- Take a moment to review the existing SPRs. SPRs process in a top-down order. Processing stops once a match is found.
    - There are three SPR types:
        - Intrazone --> used to match traffic within the same zone (you cannot specify a destination zone).

        - Interzone --> used to match traffic between different zones (the source and destination zones must be different).
        - Universal --> used to match traffic between different zones and/or within the same zone (combination of both intrazone and interzone).

- Every SPR consists of various categories of matching criteria, and an associated action. Click on any SPR to observe the matching criteria:
    - Source
        - Zone
        - Address
        - Users
        - Device
    - Destination
        - Zone
        - Address
        - Device
    - Application
    - Service/URL Category
    - Actions
- PAN-OS uses the concepts of *objects*. The power behind objects is that you can define an object once in the configuration, and reference it numerous times elsewhere! Let us detour to the Objects tab to see! Navigate to Objects --> Addresses



    - Address objects can be used in various policies. There are four kinds of address objects:
        - IP Netmask
        - FQDN
        - IP Range

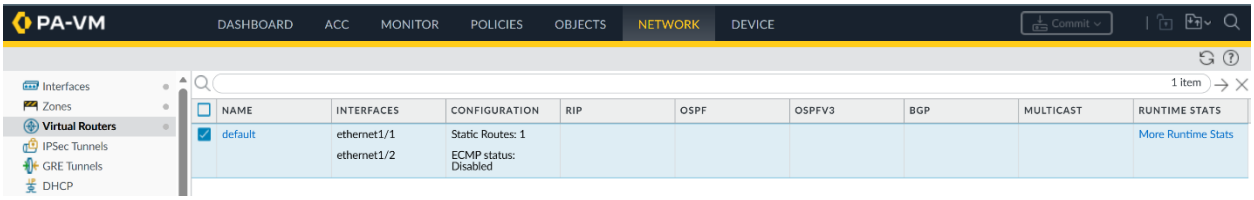
        - IP Wildcard Mask
    - Pivot back to the SPRs and observe how and where different address objects are used.

- It is important to note that the Palo Alto NGFW operates at layers three, four, and seven of the OSI model. Therefore (contingent on the configuration), match criteria of SPRs goes far beyond traditional ACLs. Various mechanisms exist to determine content inside the traffic (for security analysis and filtering), usernames, device information, etc. This information can be used by the firewall to enforce SPRs!
- Let us expand on the mechanisms the Palo Alto NGFW uses to go beyond a traditional firewall. Two pieces of functionality (amongst others) includes App-ID, and User-ID
- App-ID: identification of applications used in traffic flows based on regex and behavior.
    - App-ID is a critical piece of functionality because it allows the firewall administrator to either allow or deny traffic flows *based on the application itself*, rather than just layer three and layer four information.
    - Navigate to Objects --> Applications to see a list of currently available applications that you can reference in various types of policies on the firewall.
    - Ultimately, the list of applications identified, and how the applications are identified are provided by Palo Alto Networks through content updates. This ensures that new applications are added to the list, and App-IDs are updated as modifications to them are made.
    - One item to note is that most web traffic is identified as SSL given the widespread use of TLS. A firewall administrator can be granular in their policy rules using App-ID, but they need to leverage *decryption* for the threat prevention and threat detection mechanisms on the firewall to ensure encrypted threats are not missed. Decryption is a complex topic, and is out of scope for this walkthrough, however, I encourage you to read more about it in the context of a Palo Alto NGFW here: https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview
    - For those app developers out there: yes, you can create custom App-IDs!
- User-ID: association of usernames to IP addresses.
    - User-ID lies at the core of network visibility and segmentation, and answers the question of "how do I restrict network access when my users are not always on the same IP?"
    - One can also see problems with shared workstations, and shared logins. User-ID enhances the level of granularity to which you can restrict flows in your network.
    - User-ID can be thought of as the *mapping of usernames to IP addresses*. This way, we can specify users in policy rules rather than just IP addresses. In this sense, a

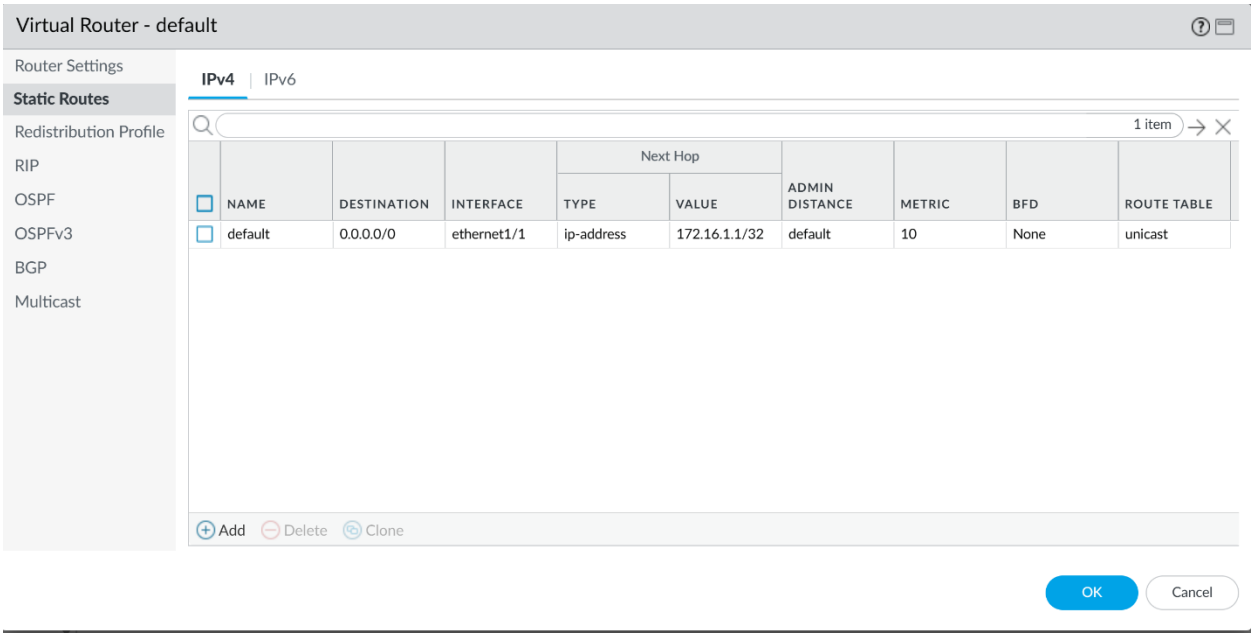
user will be able to access resources on the network only if the security policy rule allows them to do so through specification of their *username*.

- The key question is: how does the firewall *associate* the IP address and username together? There are various User-ID mapping mechanisms that can be leverage in an environment:
  - Server Monitoring
  - Port Mapping
  - Syslog
  - XFF Headers
  - Username Header Insertion
  - Authentication Policy and Authentication Portal
  - GlobalProtect
  - XML API
  - Client Probing
- It should be noted that group mapping also exists in addition to user mapping.
- I encourage you to read more on both topics here:
  - https://docs.paloaltonetworks.com/ngfw/administration/user-id/user-id-overview
  - https://docs.paloaltonetworks.com/ngfw/administration/user-id/user-id-concepts

- As previously mentioned: every NGFW contains both routing and security functionality. Let us revisit routing!
  - In short: without traffic flows there is nothing to enforce from a security standpoint.
  - PAN-OS uses the concept of virtual routers. Every interface and zone defined on the firewall must be associated to a virtual router.
  - Every virtual router is comprised of a Forwarding Information Base (FIB), and Routing Information Base (RIB). Furthermore, PAN-OS participates in static routing, and dynamic routing protocols such as RIP, OSPF, OSPFv3, and BGP.
  - Let us examine the forwarding table, and route table on the firewall. Navigate to Network --> Virtual Routers --> default --> More Runtime Stats (far right-hand side)

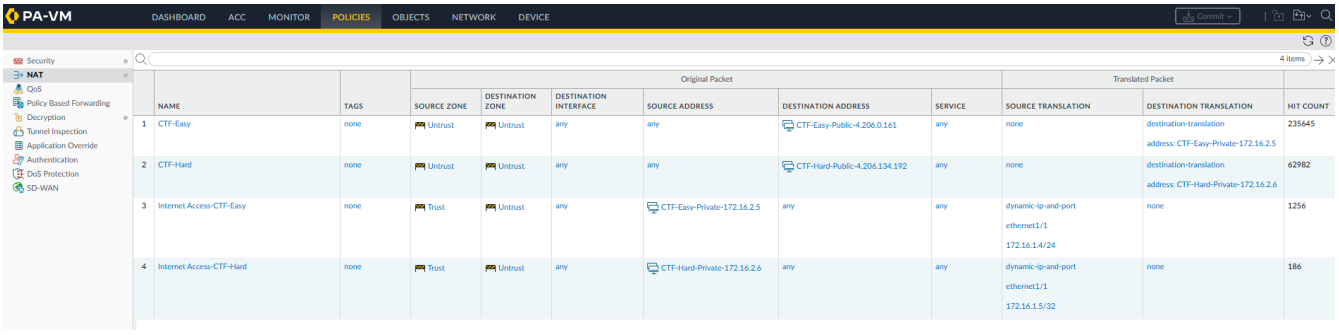


- The Route Table (RT) and Forwarding Table (FT) are vital when troubleshooting traffic flows.
- One of the most important routes in every RT is the default route. The essence of the default route is to provide a next-hop for a packet that does not have a route explicitly defined. The easiest giveaway to spot a default route is the 0.0.0.0/0 address in the destination field.
- We can define routing protocols and static routes by clicking on the default router itself. In our case, there is only the default route assigned:



- We've briefly discussed zones, so let us expand our routing themed conversation with an overview of *interfaces*. Interfaces can be either physical, or logical. The number of physical interfaces is contingent on the model of NGFW, however, subinterfaces can also be configured. Palo Alto produces various sizes of physical firewalls. These scale up drastically and include use cases at branch sites, office buildings, campus environments, data centres, and ISPs. The NGFW you are accessing for this walkthrough is running on a VM in Azure. There are various VM options available (VM Series versus Cloud NGFW) in addition to the CN-Series for containers. There is a type of firewall available for every network setup!
    - Dependent on the type (physical or virtual) and specific model of firewall there are two interface types:

        - Physical
            - Tap
            - High Availability
            - Log Card
            - Decrypt Mirror
            - Virtual Wire
            - Layer 2
            - Layer 3
            - Aggregate Ethernet
        - Logical
            - VLAN
            - Loopback
            - Tunnel
    - Network Address Translation (NAT)
        - NAT is essential for ensuring access to the internet (source NAT), but it can also be used to map traffic to servers that sit behind a router or firewall (destination NAT).
        - In our case there are examples of both configurations. Head to Policies --> NAT to view examples of both configurations. The first two rules are required in order for you to access the easy and hard CTF challenge boxes. The last two rules are how those boxes communicate outbound to the internet.



        - NAT also processes in a top-down order. Processing stops once a match is found.

Thank you for taking the time to go through this walkthrough! I hope you learned something of value, and added to your knowledge of NGFWs. I invite you to visit the ADVANTUS360 booth at BSides Calgary 2026 to discuss all things Palo Alto NGFW, what you learned or found interesting about this walkthrough, and the bingo card! You can find the bingo card, information about the Red Team challenge, and how to enter the prize draw here: https://advantus360.com/misconfig-bingo. As a friendly reminder: you are only entered to win if you submit your answers in-person.

Do not forget to answer the questions below!

Cheers,

Robert

Questions:

- Which of the three security rule types is default?
- Can you remove the default SPRs?
- What are all the possible actions associated with a SPR? When and why would you use them?
- How do you specify a port number as match criteria within a SPR?
- In what case is it more logical to use an address object of type FQDN?
- [BINGO CARD] Which App-IDs are used in the security policy rules on the bsidespaloaltovm firewall?
- [BINGO CARD] What security policy rule exemplifies User-ID functionality?
- [BINGO CARD] Find the hidden flag in the SPRs on the PA-VM NGFW.
- What is the difference between the FIB and RIB?
- What is the next hop of the default route on the default virtual router?
- [BINGO CARD] Find the hidden flag on an interface.
- Bonus: what are the three types of decryption configurations possible on the firewall?