Zadanie 6

Ważne przed rozpoczęciem pracy należy wyłączyć regułę domyślną (ze względu na interfejsy wirtual wire)

- 1. Skonfiguruj przełącznik zgodnie z rysunkiem, ustaw adres zarządzalny 192.168.20.254/24 na vlan 20, skonfiguruj port mirroring tak aby komp2 (szpieg) podsłuchiwał ruch na intefejsie 1 i 3
- 2. Skonfiguruj przełącznik zgodnie z opisem
- 3. Zaloguj się na firewall przez przeglądarkę
- 4. Ustaw datę i czas.
- 5. Zmień nazwę urządzenia na nazwisko
- 6. Do interfejsu 4 przypisz adres ip z podsieci 11.11.11.0/30 (utwórz zonę router2)
- 7. Na interfejsie 3 przypisz adres z podsieci 10.10.10.0/30 (utwórz zonę router1)
- 8. Zezwól z komp2 na pingowanie i logowanie się do firewalla (zarządzanie) tylko ten komp
- 9. Skonfiguruj rutery
- 10. Skonfiguruj na R1 serwer DHCP Vlanów
- 11. Sprawdź czy komp1 otrzymał adres ip z serwera DHCP
- 12. Utwórz regułę która pozwoli tylko "pingować" z komputera komp1 i komp2 do rutera R2 i pozwoli na otworzenie strony na ruterze
- 13. Utwórz regułę która pozwoli tylko z komp2 do rutera R2 pozwoli na połączenie za pomocą protokołu FTP
- 14. Pingując komp1 do rutera lub odwrotnie przechwyć pakiety w programie wireshark (zrzut!!!), Na ruterze R1 sprawdź w narzędziu torch interfejsie wejściowym adres ip źródłowy
- 15. Skonfiguruj NAT tak aby adres rutera był ukryty jako adres firewall'a (od komp1)
- 16. Powtórz punkt 12 a następnie zaobserwuj różnicę

17. Skonfiguruj VPN między dwoma firewallmi

vpn

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns/site-to-site-vpn-quick-configs/site-to-site-vpn-with-static-routing#id12184b17-432a-41cf-b10c-67eca32b4bb6

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns



Na zakończenie pracy zrestartuj firewall

https://192.168.1.1/ login:admin, haslo:admin – nie zmieniamy

Aby dodać adres należy wybrać interfejs Zakładka: IPv4 dodajemy adres Zakładka: config – wybrać Virtual Router i utworzyć nową Zonę Zakładka Advanced -> Management Profile I utworzyć nowy profil zezwalający na ping i protokół http i https

Reguły tworzymy w zakładce "Policies" ->Security

| paloalto | | Dashboard | ACC | Monitor | Pol | icies Ot | jects | Network | Device | | | | | | 🏯 Commit 🏼 🖓 🕻 | ionfig • 9. | Search |
|---|---|-----------|------|-----------|----------|----------|-------|-------------|-------------|---------|------------|---------------------|---------------------|-------------|-----------------------|-------------|---------------|
| | | | | | | | | | | | | | | | | 5 | Help |
| Security | • | | | | | | | | | | | | | | | 8 iten | |
| DOS | | | | | Source | | | | Destination | | Rule Usage | | | | | | |
| Policy Based Forwarding Cocyption Tunnel Inspection Tunnel Inspection Covernide Authentication Dos Protection | | Name | Tags | Type | Zone | Address | User | HIP Profile | Zone | Address | Hit Count | Last Hit | First Hit | Application | Service | Action | Profile |
| | 1 | PC1_PC2 | none | interzone | PR PCI | any | any | any | FOR PC2 | any | 343 | 1999-11-29 19:18:06 | 1999-11-29 17:14:58 | any | 🗶 application-default | C Allow | none |
| | 2 | MGMT_STOP | none | universal | PR PCI | any | any | any | PR PC1 | any | 308 | 1999-11-29 19:34:16 | 1999-11-29 17:56:14 | any | 🗶 service-https | O Allow | none |
| | 3 | PC2_PC1 | none | interzone | PR PC2 | any | any | any | PR PCL | any | 967 | 1999-11-29 19:18:27 | 1999-11-29 17:36:22 | апу | 🗶 application-default | O Allon | none |
| | 4 | MGMT | none | universal | (74) PC1 | any | any | any | (70) PC1 | any | 1256 | 1999-11-29 20:04:37 | 1999-11-29 17:33:25 | any | × application-default | O Allow | none |

Rys.1 przykładowe reguły

Przykład podinterfejsu wirtualnego

| nterface | 1 | interface Type | Management Profile | Link State | IP Address | Virtual Route | | |
|------------------------|------------|----------------|-----------------------|---------------|---------------|---------------|--|--|
| 🖬 ethernet1/1 | l | .ayer3 | | 1 | none | none | | |
| a ethernet1/1.10 | l | ayer3 | MGMT | | 10.110.0.1/24 | default | | |
| ethernet1/1.20 | L | ayer3 | MGMT | | 10.120.0.1/24 | default | | |
| a ethernet 1/2 | l | .ayer3 | DMZ | | 10.99.0.1/24 | default | | |
| a ethernet 1/3 | l | .ayer3 | MGMT | 100 | 10.10.0.1/24 | default | | |
| 🖬 ethernet1/4 | l | .ayer3 | MGMT | 10.20.0.1/2 | | default | | |
| Tag Netflow Profile | 10 None | | | | | | | |
| Config IPv4 | IPv6 | Advanced | | | | | | |
| Assign Interface | e To | | | | | | | |
| Virtual Router default | | | | | | | | |
| Security Zo | ne PC1 | | | | | * | | |
| 2 | | | | | | | | |
| | | | | | ОК | Cancel | | |
| | | | | | | | | |

Przykład DHCP

| HETWORKS! | Dashboard ACC | C Monitor Policies | Objects Network | k Device | | |
|------------------------------|-------------------------|-----------------------------------|---------------------------------|---|--------------|----------------------|
| 22 Zones | DHCP Server DHCP Hela | зу | | | | |
| VLANS | 0 | | | | | |
| € Virtual Wires | | | | | | |
| Virtual Routers | Interface * | Mode | Probe IP | Optic | ons | IP Pools |
| PSec Tunnels | ethernet1/2 | enabled | | Leas | e: Unlimited | View Allocation |
| DHCP | 01100 0 | | | | .0.1 | 10.99.0.3-10.99.0.13 |
| T DNS Proxy | DHUP Server | | | | | |
| Portals | Interface ethern | et1/1.10 | | | * | |
| Gateways | Mode auto | | | | - | |
| MDM | | | | | | |
| Bovice Block List | Lease Options | | | | | |
| Clientless Apps | | ing ID when allocating new ID | | | | |
| Clientless App Groups | | ing if which allocating new if | | | | |
| a QoS | Lease 💿 U | | | | | |
| With LLDP | IP Pools | | Reserved Address | MAC Address | | |
| A GlobalProtect IPSec Crypto | | | The second second second second | Provide and a second | _ | |
| IKE Gateways | 192.168.1.20, 192.168.1 | 0/24 or 192.168.1.10-192.168.1.20 | 192.168.1.20 xxxxxxxxxxxxxxxx | cox (Optional MAC Address) | | |
| a IPSec Crypto | | | | | | |
| IKE Crypto | | | | | | |
| 🚵 Monitor | | | | | | |
| Noterface Mgmt | | | | | | |
| Zone Protection | | | | | | |
| QOS Profile | | | | | | |
| CLDP PIONE | 🕂 Add 🔳 Delete | | 🕂 Add 🛛 🚍 Delete | | | |
| | | | | | _ | |
| | | | | ОК Сап | cel | |
| | | | | | | |
| | 🕂 Add 🚍 Delete 🎠 PDF/CS | SV | | | | |

Aby przetestować czy nasza konfiguracja jest poprawna należy w prawym górnym rogu GUI znaleźć przycisk i zapisać naszą konfiguracje oraz przesłać ją do firewalla. Zajmie to moment i możliwe, że wystąpi błąd związany z opcją Virtual Wire (jest to jedna z funkcji urządzenia, która pozwala na przesyłanie informacji z jednego portu urządzenia na drugi port urządzenia bez wewnętrznego przetwarzania tych informacji). Można się go pozbyć usuwając z zakładki Network > Virtual Wires wpis o nazwie default.

W przypadku urządzenia Palo Alto P200 przywrócenie ustawień fabrycznych jest możliwe w trybie CLI (przy połączeniu za pomocą kabla konsolowego do urządzenia). Po podłączeniu się i zalogowaniu należy wydać odpowiednie polecenie :

debug system maintenance-mode co pozwoli nam na zrebootowanie urządzenia i przejście do tego trybu.



Z tego poziomu jesteśmy w stanie przywrócić ustawienia fabryczne urządzenia. Pierwsze co nam się wyświetli to :



Po wybraniu opcji Continue należy przejść do Factory Reset i wybrać za pomocą przycisku Enter.



- ----

| COM1 - PuTTY | - | × |
|----------------------|---|---|
| Factory Reset Status | | ^ |
| Percent Complete | | |
| 0 % | | |
| Working | | |