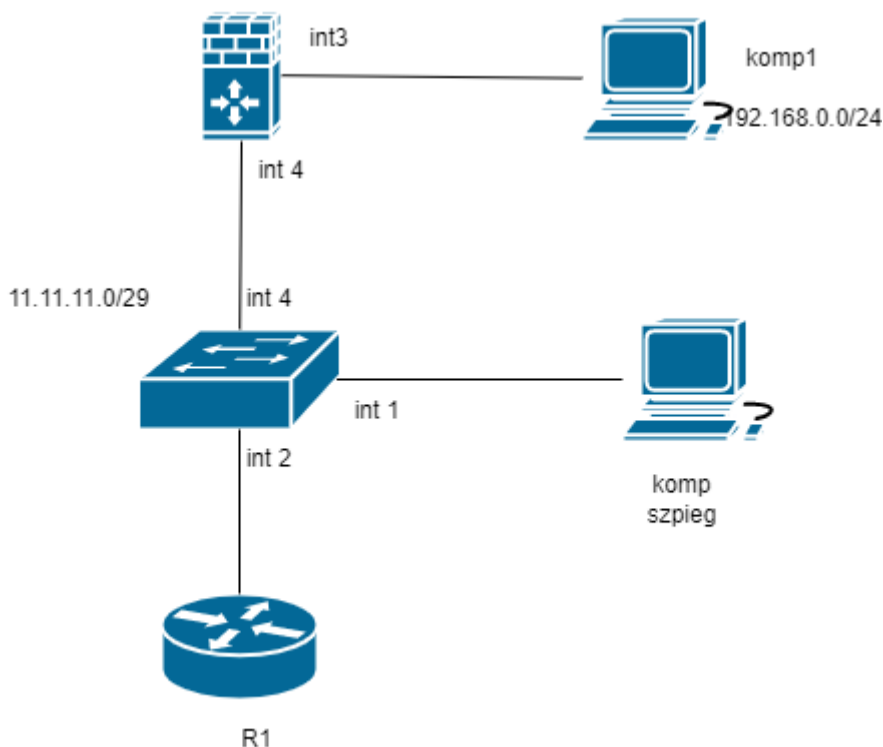


Zadanie 4 NAT

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

Komp szpieg musi mieć wireshark

1. Skonfiguruj przełącznik zgodnie z rysunkiem, ustaw adres zarządzalny 11.11.11.6/29, skonfiguruj port mirroring tak aby komp szpieg podsłuchiwał ruch na interfejsie 4 i 2
2. Zaloguj się na firewall przez przeglądarkę
3. Ustaw datę i czas.
4. Zmień nazwę urządzenia na nazwisko
5. Do interfejsu 4 przypisz adres IP z podsieci 11.11.11.0/29 (utwórz zonę router)
6. Do interfejsu 3 przypisz adres IP z podsieci 192.168.0.0/24 (utwórz zonę PC1)
7. Zezwól z komp1 na pingowanie i logowanie się do firewalla (zarządzanie)
8. Skonfiguruj serwer DHCP dla podsieci 192.168.0.0/24
9. Zaadresuj ruter
10. Sprawdź czy komp1 otrzymał adres IP z serwera DHCP
11. Utwórz regułę która pozwoli „pingować” z komputera komp1 do rutera
12. Pingując komp1 do rutera przechwyć pakiety w programie wireshark (zrzut!!!), Na routerze R1 sprawdź w narzędziu torch interfejsie wejściowym adres IP źródłowy
13. Skonfiguruj NAT tak aby adres komp 1 był ukryty jako adres firewall'a
14. Powtórz punkt 12 a następnie zaobserwuj różnicę
Na zakończenie pracy zrestartuj firewall



<https://192.168.1.1/> login:admin, hasło:admin – nie zmieniamy

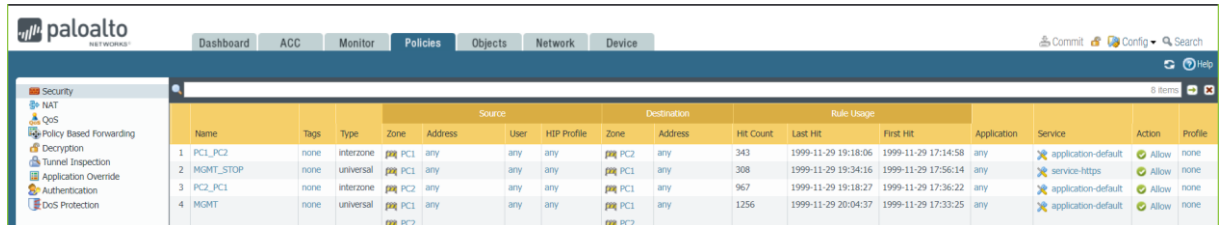
Aby dodać adres należy wybrać interfejs

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

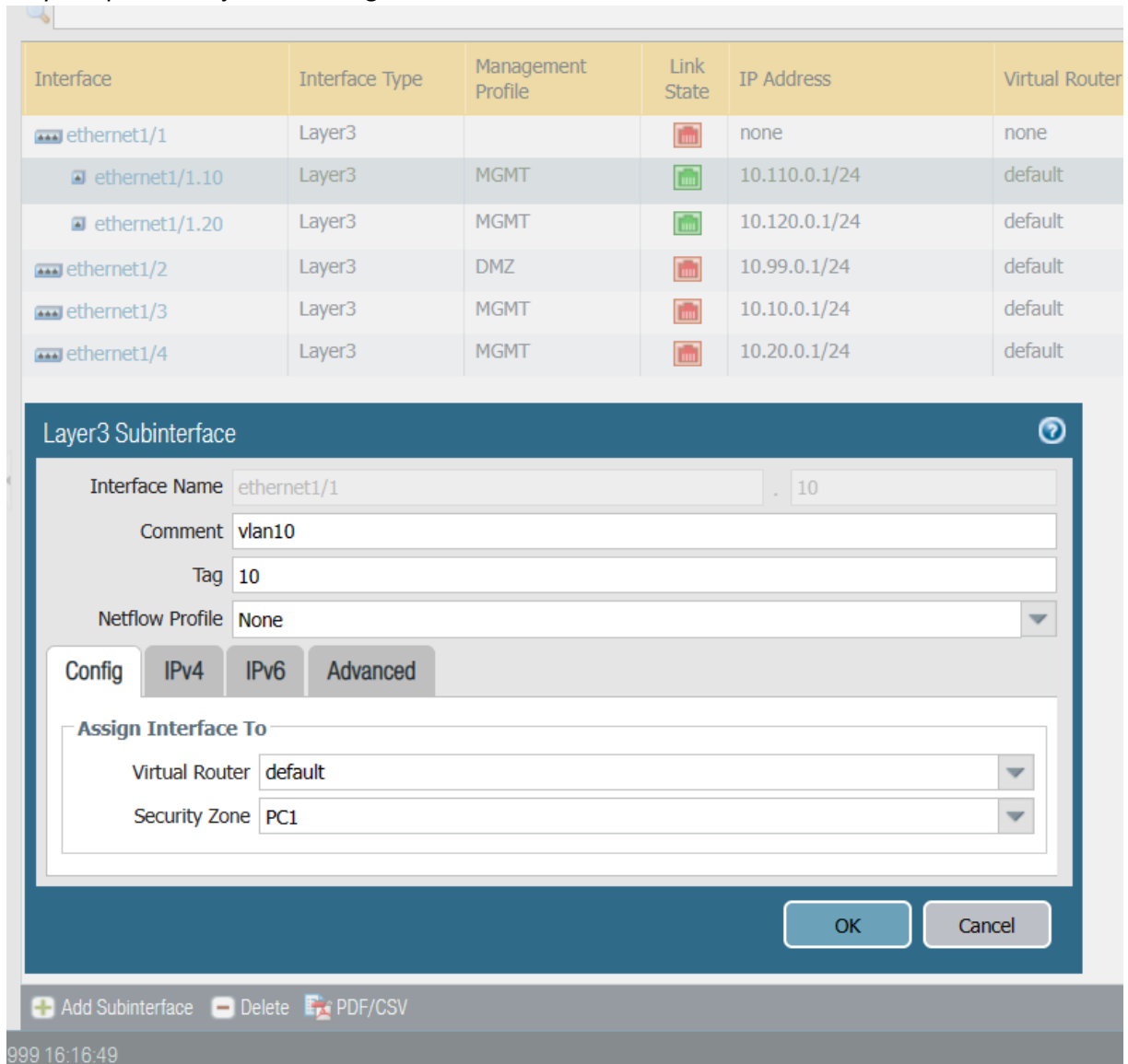
Reguły tworzymy w zakładce „Policies” ->Security



| Name | Tags | Type | Source Zone | Source Address | User | HIP Profile | Destination Zone | Destination Address | Hit Count | Last Hit | First Hit | Application | Service | Action | Profile |
|-------------|------|-----------|-------------|----------------|------|-------------|------------------|---------------------|-----------|---------------------|---------------------|-------------|---------------------|--------|---------|
| 1 PCL_PC2 | none | interzone | PC1 | any | any | any | PC2 | any | 343 | 1999-11-29 19:18:06 | 1999-11-29 17:14:58 | any | application-default | Allow | none |
| 2 MGMT_STOP | none | universal | PC1 | any | any | any | PC1 | any | 308 | 1999-11-29 19:34:16 | 1999-11-29 17:56:14 | any | service-https | Allow | none |
| 3 PC2_PC1 | none | interzone | PC2 | any | any | any | PC1 | any | 967 | 1999-11-29 19:18:27 | 1999-11-29 17:36:22 | any | application-default | Allow | none |
| 4 MGMT | none | universal | PC1 | any | any | any | PC1 | any | 1256 | 1999-11-29 20:04:37 | 1999-11-29 17:33:25 | any | application-default | Allow | none |

Rys.1 przykładowe reguły

Przykład podinterfejsu wirtualnego



| Interface | Interface Type | Management Profile | Link State | IP Address | Virtual Router |
|----------------|----------------|--------------------|------------|---------------|----------------|
| ethernet1/1 | Layer3 | | Red | none | none |
| ethernet1/1.10 | Layer3 | MGMT | Green | 10.110.0.1/24 | default |
| ethernet1/1.20 | Layer3 | MGMT | Green | 10.120.0.1/24 | default |
| ethernet1/2 | Layer3 | DMZ | Red | 10.99.0.1/24 | default |
| ethernet1/3 | Layer3 | MGMT | Red | 10.10.0.1/24 | default |
| ethernet1/4 | Layer3 | MGMT | Red | 10.20.0.1/24 | default |

Layer3 Subinterface

Interface Name: ethernet1/1 . 10

Comment: vlan10

Tag: 10

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: PC1

OK Cancel

999 16:16:49

Przykład DHCP

The screenshot shows the Palo Alto Networks GUI for configuring a DHCP Server. The main configuration window is titled "DHCP Server" and is set for interface "ethernet1/1.10" in "auto" mode. The "Lease" tab is selected, showing "Lease" set to "Unlimited" and "Ping IP when allocating new IP" unchecked. Below this, there is a table for "IP Pools":

| IP Pools | Reserved Address | MAC Address |
|---|------------------|--|
| 192.168.1.20, 192.168.1.0/24 or 192.168.1.10-192.168.1.20 | 192.168.1.20 | xxxx:xxxx:xxxx:xx (Optional MAC Address) |

At the bottom of the window, there are "Add" and "Delete" buttons for both the IP Pools and the DHCP Server configuration. The background shows the "Network" tab with a table of DHCP Servers and Relays.

Konfiguracja Nata

The screenshot shows the Palo Alto Networks GUI for configuring a NAT rule. The "Policies" tab is selected, and the "NAT Rulebase" is visible. A table lists the NAT rules:

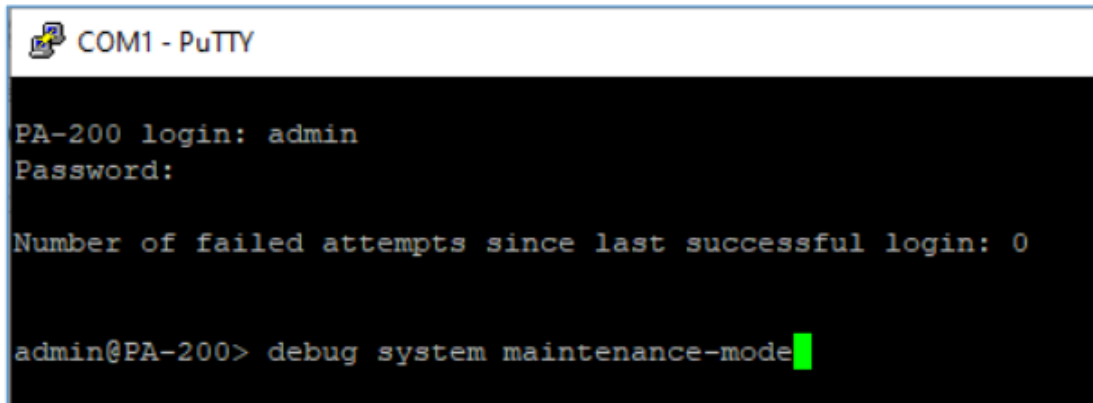
| Name | Tags | Source Zone | Destination Zone | Destination Interface | Source Address | Destination Address | Service | Source Translation | Destination Translation | Hit |
|-------------|------|-------------|------------------|-----------------------|----------------|---------------------|---------|--|-------------------------|-----|
| 1 NAT_P2_P1 | none | PC2 | PC1 | any | any | any | any | dynamic-ip-and-port ethernet1/4 10.20.0.1/24 | none | 676 |

Below the table, there is a "Tag Browser" window showing the rule "NAT_P2_P1" with a "Rule" of "1". The "Filter by first tag in rule" option is checked, and "Rule Order" is selected.

Aby przetestować czy nasza konfiguracja jest poprawna należy w prawym górnym rogu GUI znaleźć przycisk i zapisać naszą konfigurację oraz przesać ją do firewala. 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

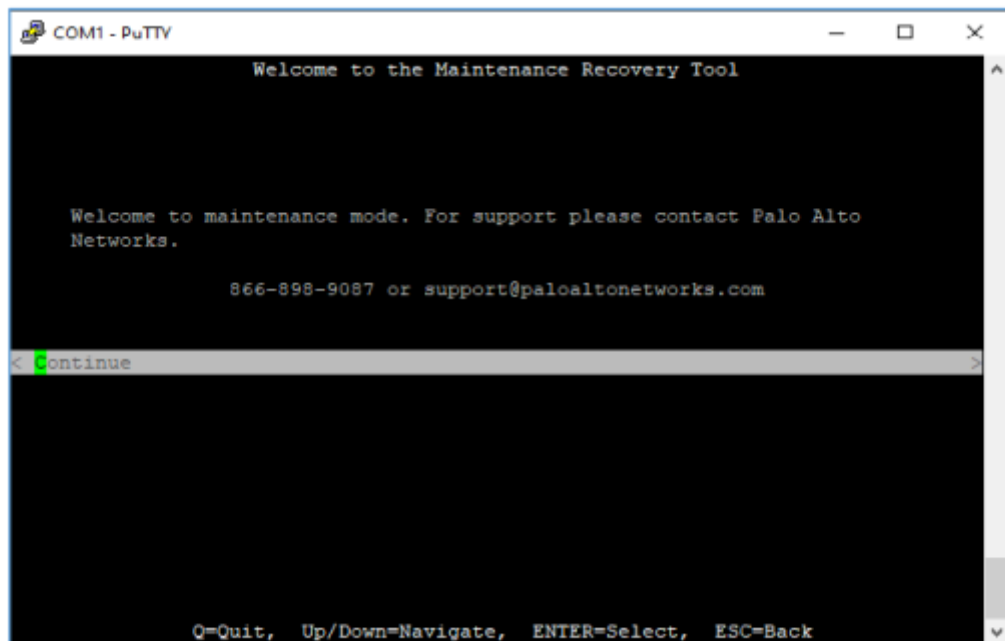
bez wewnętrznego przetwarzania tych informacji). Można się go pozbyć usuwając z zakładki Network > Virtual Wires wpis o nazwie default.

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.



```
COM1 - PuTTY
PA-200 login: admin
Password:
Number of failed attempts since last successful login: 0
admin@PA-200> debug system maintenance-mode
```

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



```
COM1 - PuTTY
Welcome to the Maintenance Recovery Tool

Welcome to maintenance mode. For support please contact Palo Alto
Networks.

866-898-9087 or support@paloaltonetworks.com

< Continue >

Q=Quit, Up/Down=Navigate, ENTER=Select, ESC=Back
```

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

```
COM1 - PuTTY
Welcome to the Maintenance Recovery Tool

< Maintenance Entry Reason
< Get System Info
< Factory Reset
< Set FIPS-CC Mode
< FSCK (Disk Check)
< Log Files
< Bootloader Recovery
< Disk Image
< Select Running Config
< Content Rollback
< Set IP Address
< Diagnostics
< Debug Reboot
< Reboot
```

```
COM1 - PuTTY
Factory Reset Status

Percent Complete

0 %

Working...
```