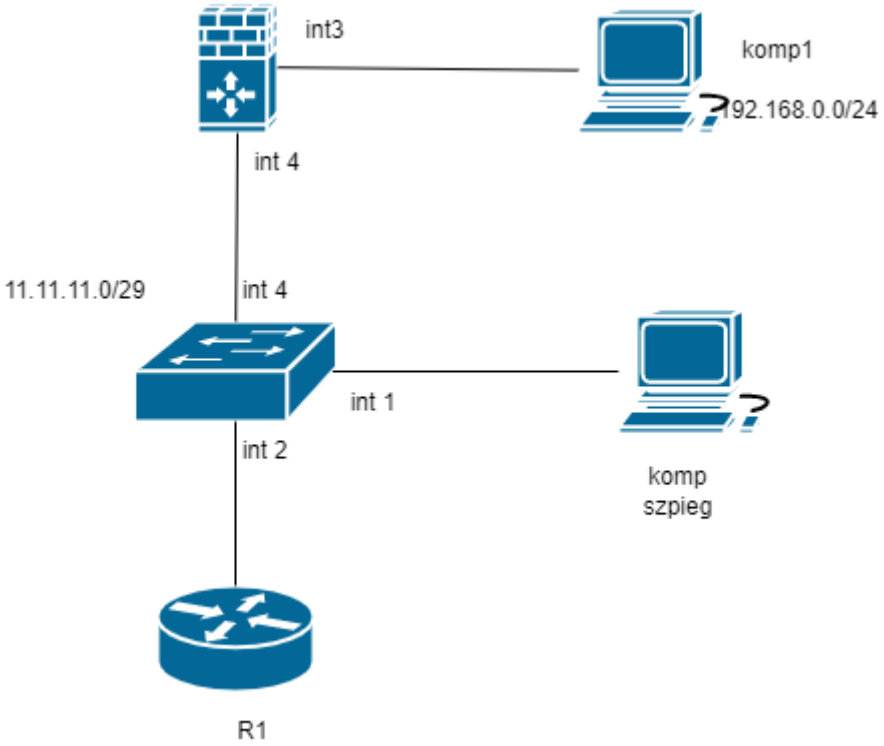
Zadanie 4 NAT

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

Komp szpieg musi mieć wireshark

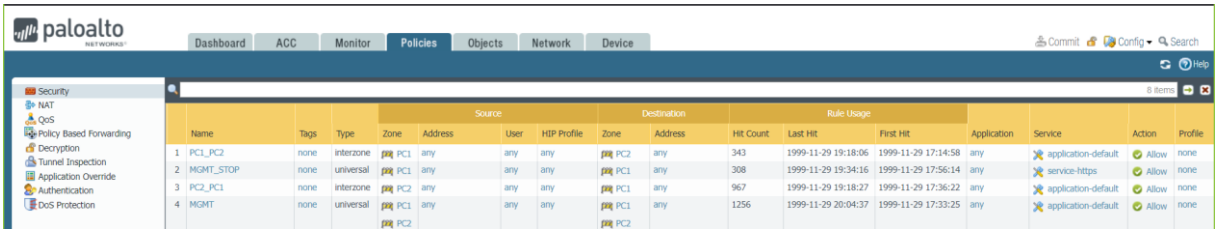
1. Skonfiguruj przełącznik zgodnie z rysunkiem, ustaw adres zarządzalny 11.11.11.6/29, skonfiguruj port mirroring tak aby komp szpieg podsłuchiwał ruch na intefejsie 4 i 2
2. Zaloguj się na firewall przez przeglądarkę
3. Ustaw datę i czas.
4. Zmień nazwę urządzenia na nazwisko
5. Do interfejsu 4 przypisz 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 reguły która pozwoli „pingować" z komputera komp1 do rutera
12. Pingując komp1 do rutera przechwyć pakiety w programie wireshark (zrzut!!!), Na ruterze 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 propracy zrestartuj firewall



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

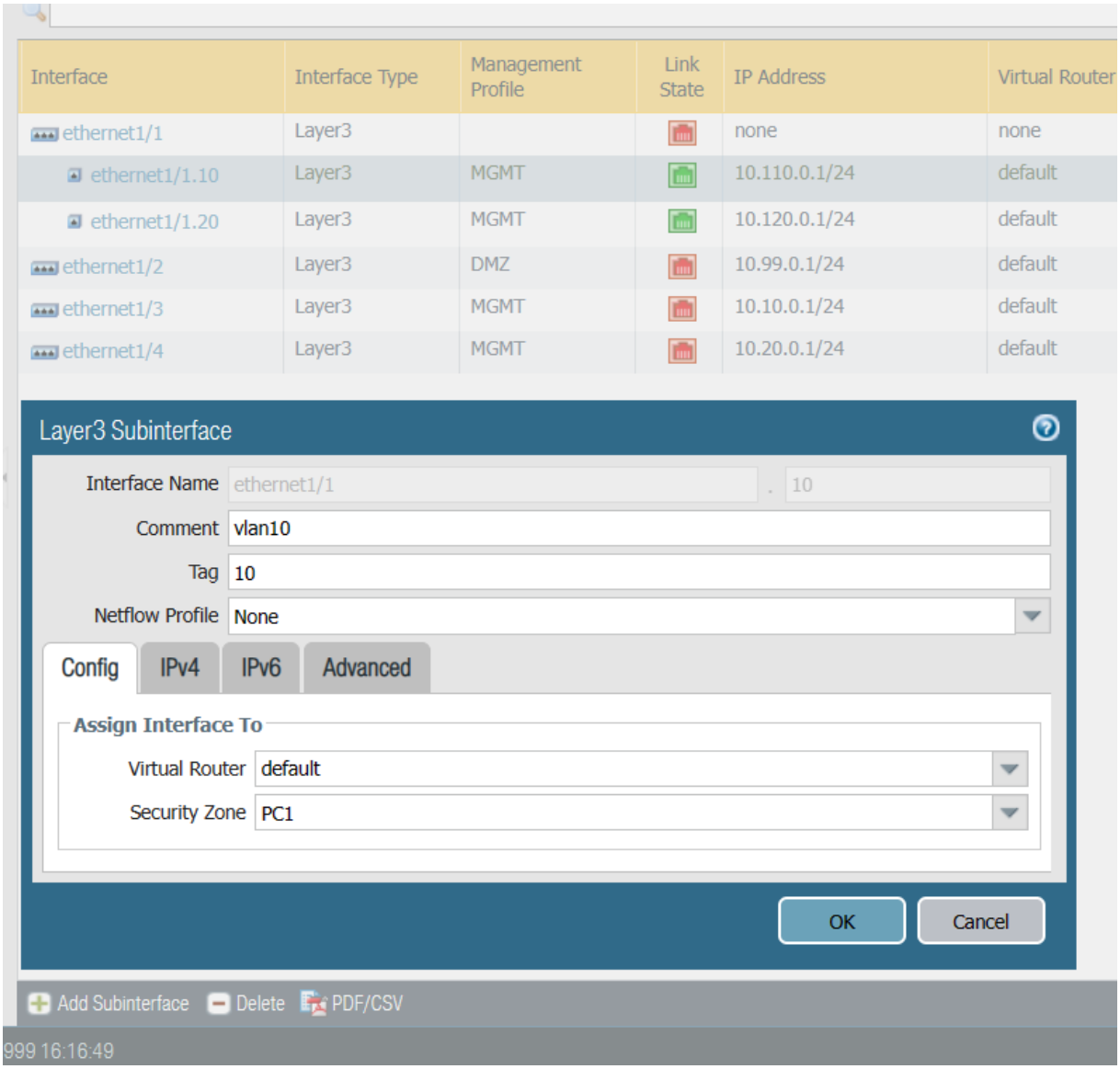
Aby dodać adres należy wybrać interfejs
Zakładka: IPv4 dodajemy adres
Zakładka: config – wybrać Virtual Router i utworzyć nową Zonę
Zakładka Advanced -> Management Profile I utworzyć nowy profil zezwalający na ping i protokół http i https

Reguły tworzymy w zakładce „Policies” ->Security

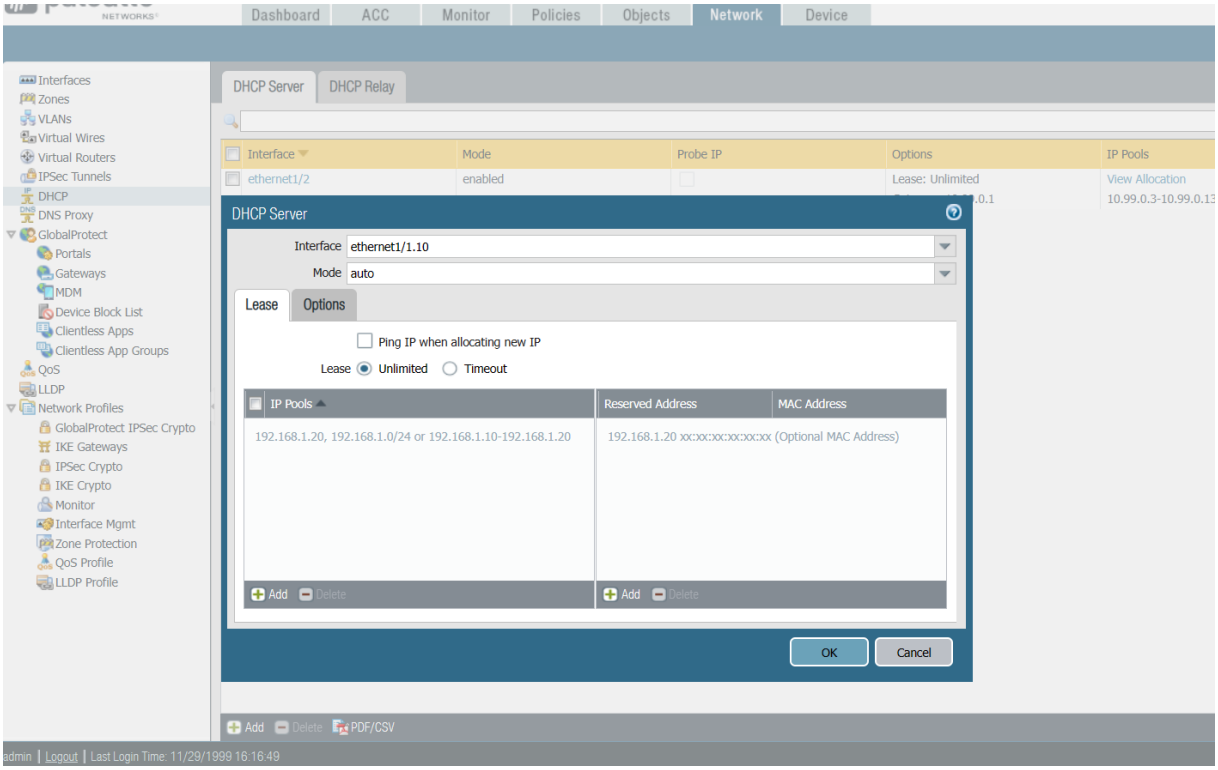


Rys.1 przykładowe reguły

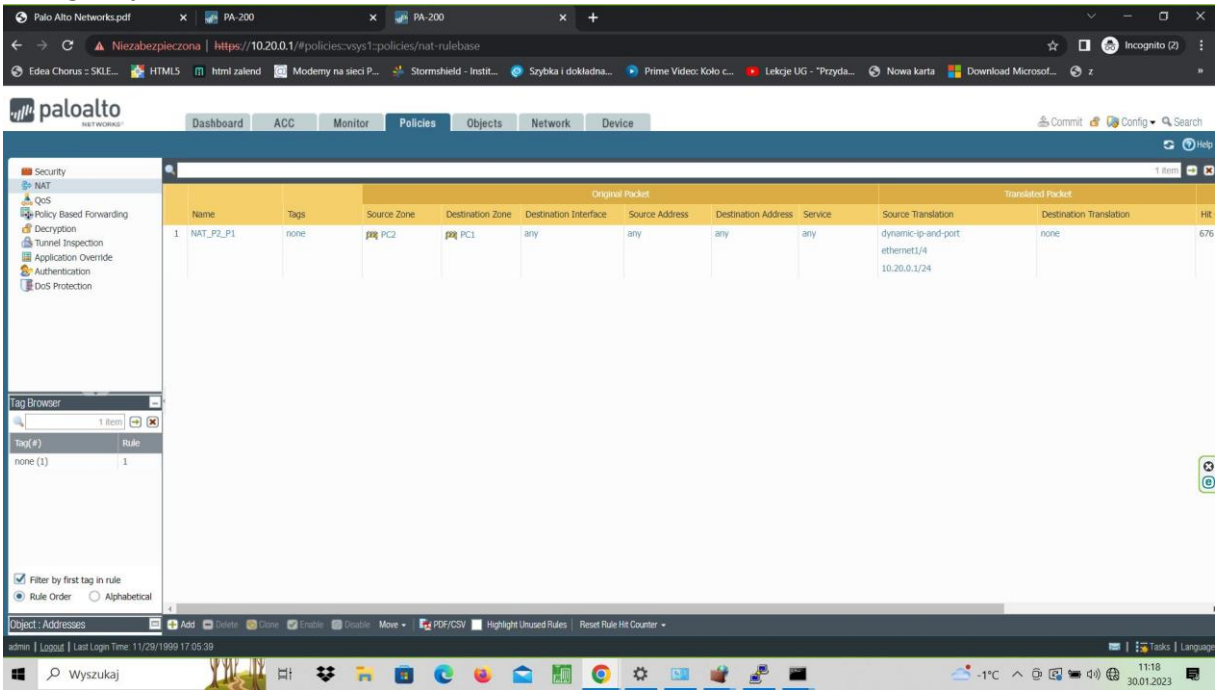
Przykład podinterfejsu wirtualnego



Przykład DHCP



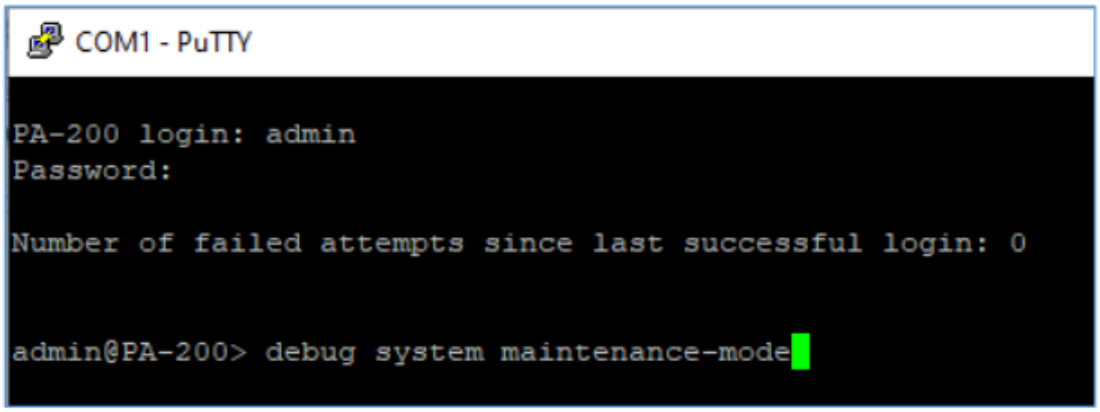
Konfiguracja Nata



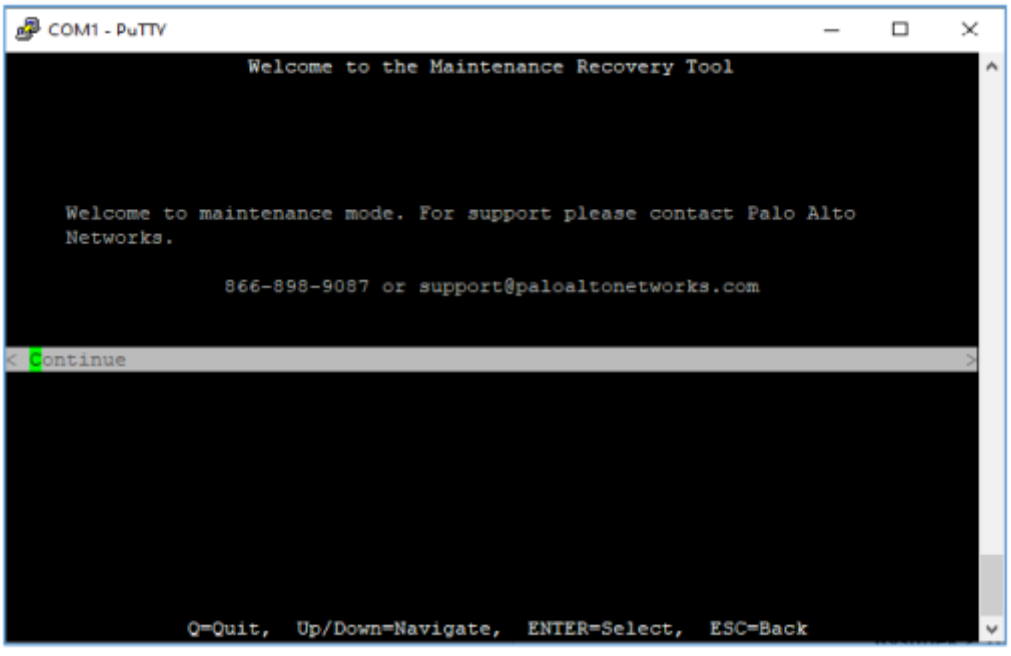
Aby przetestować czy nasza konfiguracja jest poprawna należy w prawym górnym rogu GUI znaleźć przycisk i zapisać naszą konfiguracje oraz przesłać ją do firewalla. Zajmie to moment i możliwe, że wystąpi błąd związany z opcją Virtual Wire (jest to jedna z funkcji urządzenia, która pozwala na przesyłanie 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.

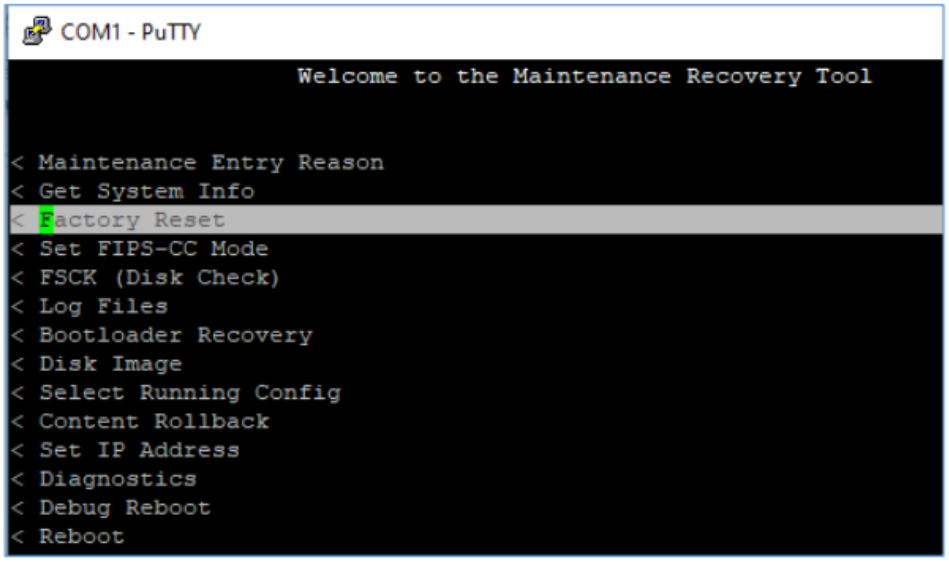
W przypadku urządzenia Palo Alto P200 przywrócenie ustawień fabrycznych jest możliwe w trybie CLI (przy połączeniu za pomocą kabla konsolowego do urządzenia). Po podłączeniu się i zalogowaniu należy wydać odpowiednie polecenie :
debug system maintenance-mode co pozwoli nam na zrebootowanie urządzenia i przejście do tego trybu.

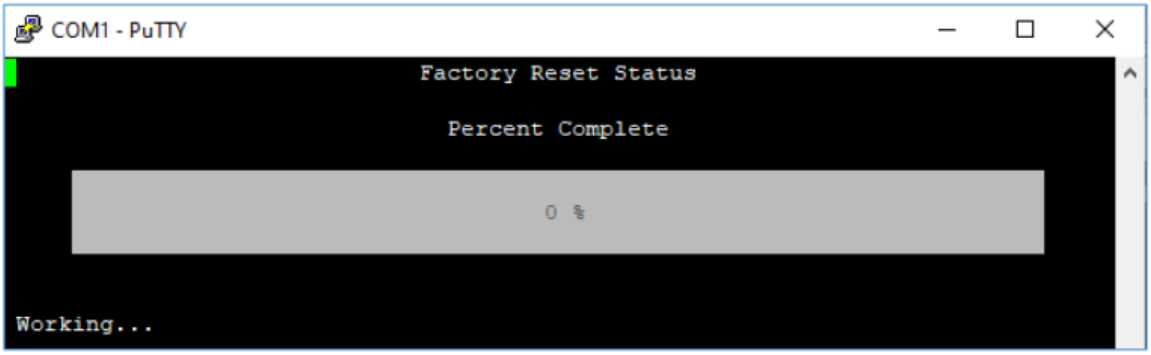


Z tego poziomu jesteśmy w stanie przywrócić ustawienia fabryczne urządzenia. Pierwsze co nam się wyświetli to :



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


COM1 - PuTTY
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...