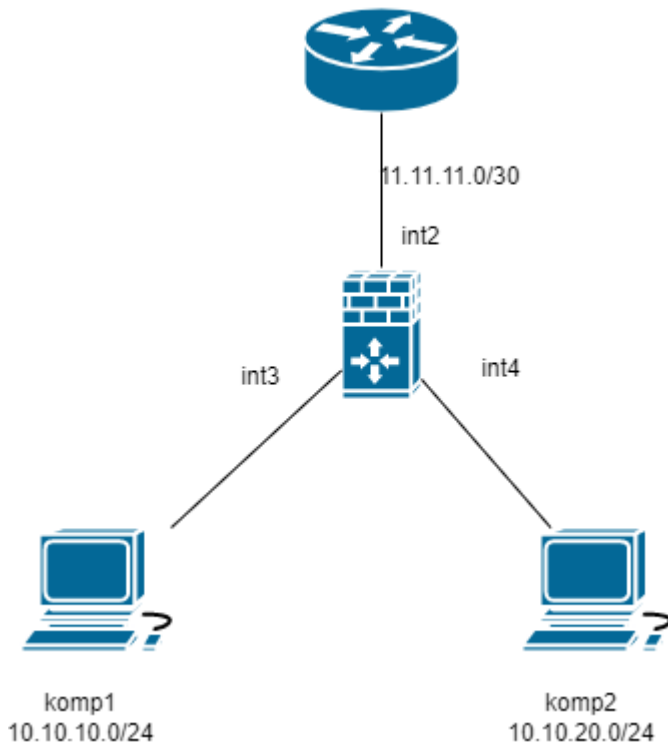


Zadanie 2

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

1. Zaloguj się na firewall przez przeglądarkę
2. Ustaw datę i czas.
3. Zmień nazwę urządzenia na nazwisko
4. Do interfejsu 2 przypisz adres ip z podsieci 11.11.11.0/24 (utwórz zonę router)
5. Do interfejsu 3 przypisz adres ip z podsieci 10.10.10.0/24 (utwórz zonę PC1)
6. Do interfejsu 4 przypisz adres ip z podsieci 10.10.20.0/24 (utwórz zonę PC2)
7. Zezwól z komp1 na pingowanie i logowanie się do firewala
8. Zaadresuj komputery i ruter
9. Utwórz regułę która pozwoli „pingować” z komputera komp1 do komp2 i do rutera
10. Utwórz regułę która pozwoli „pingować” z komputera komp1 i komp2 do rutera, ale nie między nimi

Na zakończenie pracy zrestartuj firewall



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

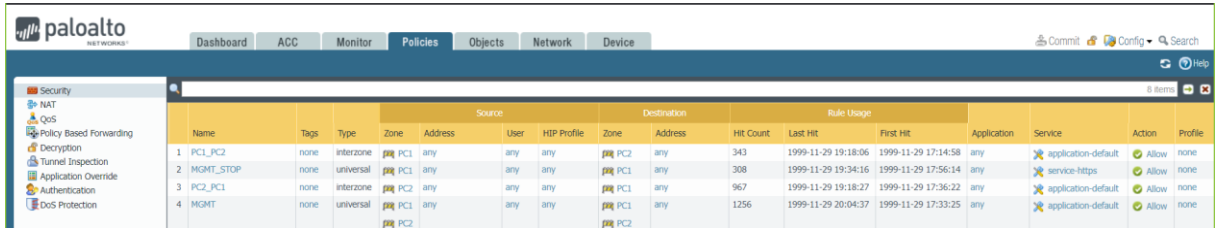
Aby dodać adres należy wybrać interfejs

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

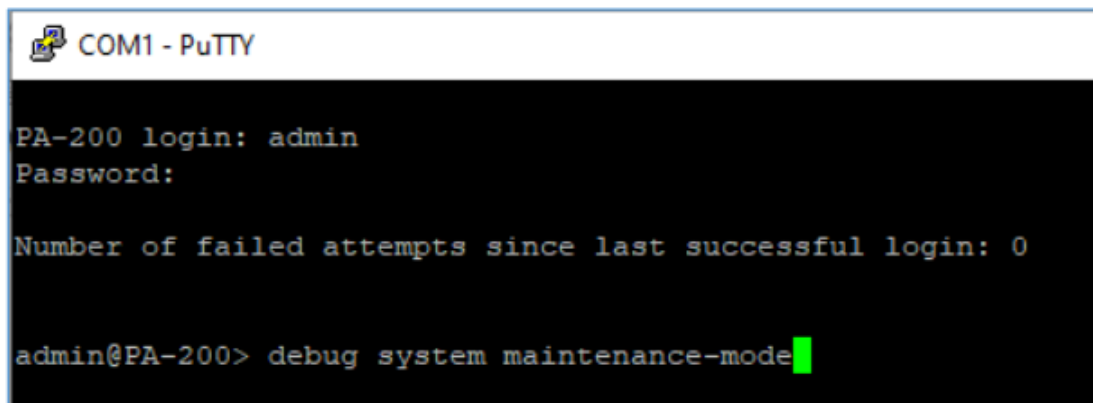


| Name | Tags | Type | Source | | | Destination | | Rule Usage | | | Application | Service | Action | Profile | |
|-------------|------|-----------|--------|---------|------|-------------|------|------------|-----------|---------------------|---------------------|---------|---------------------|---------|-----------|
| | | | Zone | Address | User | HIP Profile | Zone | Address | Hit Count | Last Hit | | | | | First Hit |
| 1 PCI_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

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



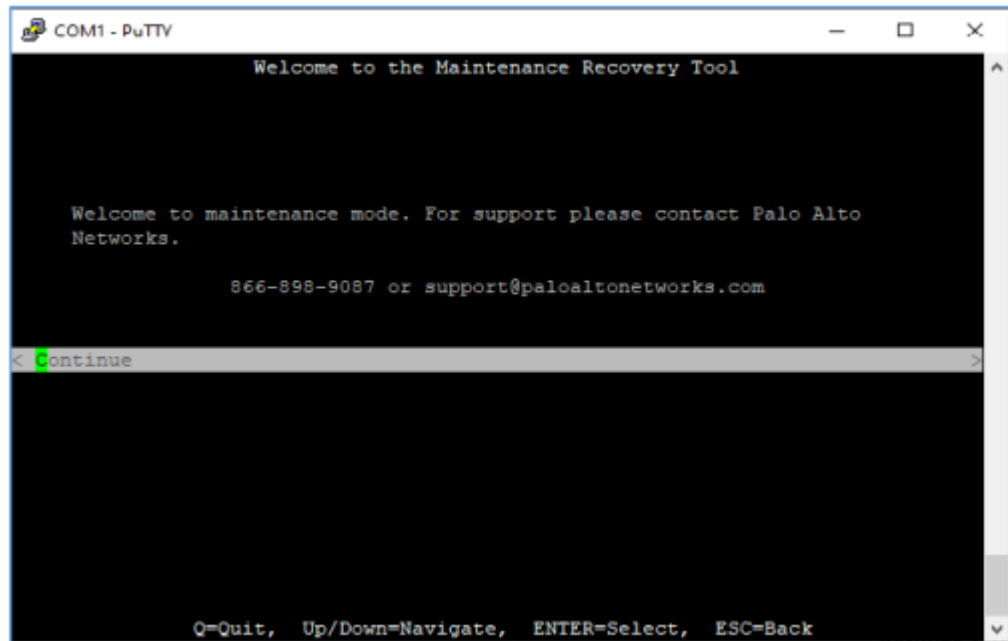
```
COM1 - PuTTY

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 :



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

