Podstawowa konfiguracja firewalla Palo Alto Networks

Damian Strojek 4G

1. Logowanie się do firewalla

a) Za pomocą strony internetowej

Aby dostać się na firewall firmy Palo Alto Networks należy najpierw podłączyć go do napięcia za pomocą specjalnego zasilacza, który znajduje się w pudełku razem z urządzeniem. Następnie należy poczekać od 2 do 5 minut aż dioda Status na przedniej części obudowy urządzenia zacznie świecić się na zielono. Kolejnym krokiem jest podłączenie się za pomocą normalnej skrętki UTP do portu MGT na przednim panelu firewallla.

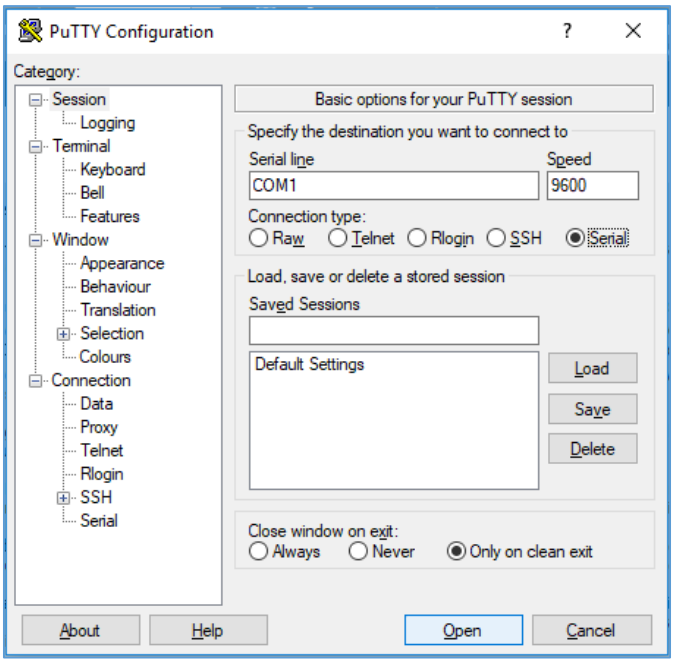
Wchodzimy wtedy za pomocą przeglądarki Google Chrome (inne przeglądarki mają problem z połączeniem) i wpisujemy w pole adresu strony internetowej : ***https://192.168.1.1*** – jest to domyślny adres IP za pomocą którego można się dostać na urządzenie.

Login i hasło domyślnie to **admin** i **admin .**

Rysunek 1.1 Logowanie się za pomocą strony internetowej

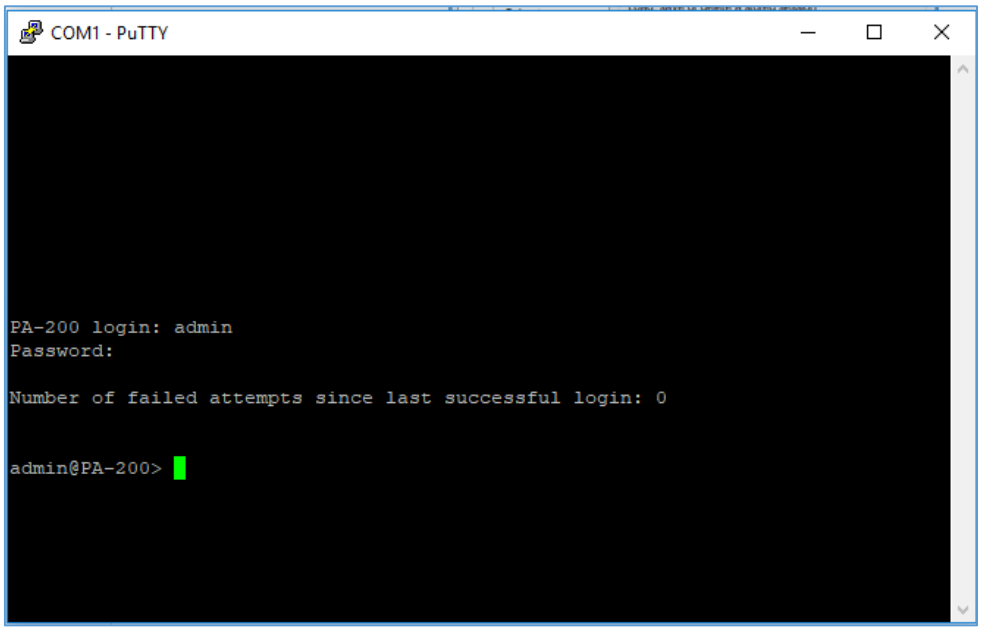
b) Za pomocą CLI

Aby poruszać się po konfiguracji firewalla za pomocą poleceń (CLI) należy pobrać jeden z programów, które emulują linie poleceń np. **PuTTY**. Po zainstalowaniu i włączeniu tego programu należy podłączyć się do urządzenia za pomocą kabla, który z jednej strony posiada zakończenie Ethernet, a z drugiej port VGA. Zakończenie Ethernet idzie do urządzenia Palo Alto Networks do portu *CONSOLE*, a VGA idzie do urządzenia, z którego będzie przeprowadzana konfiguracja. Ostatnim krokiem jest wybranie w programie PuTTY **Connection type : Serial** i otworzenie sesji pomiędzy zaporą ogniową, a np. komputerem.



Rysunek 1.2 Logowanie się za pomocą CLI

Podstawowy login i hasło to również **admin** i **admin**.

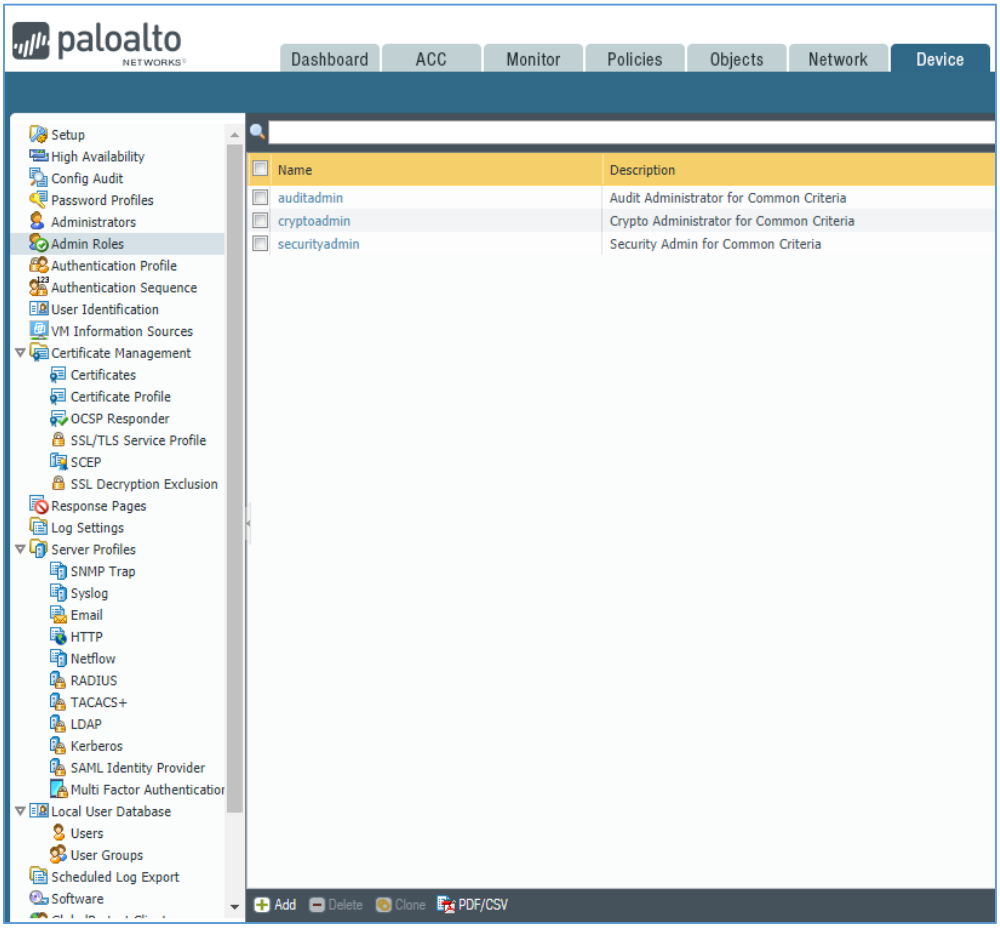


Rysunek 1.3 Wygląd CLI w programie PuTTY

2. Konfiguracja podstawowych opcji w urządzeniu firewall Palo Alto Networks za pomocą strony internetowej (GUI)

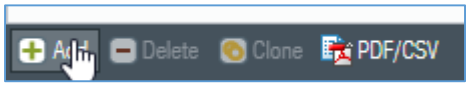
a) Dodawanie użytkowników oraz praw dla tych użytkowników

Zaczniemy od objaśnienia na czym polegają prawa dla użytkowników. Możemy tworzyć różne grupy praw dla użytkowników, a następnie je przypisywać nowo utworzonemu użytkownikowi. Robimy to w zakładce **Device > Admin Roles** tak jak na screenie poniżej.



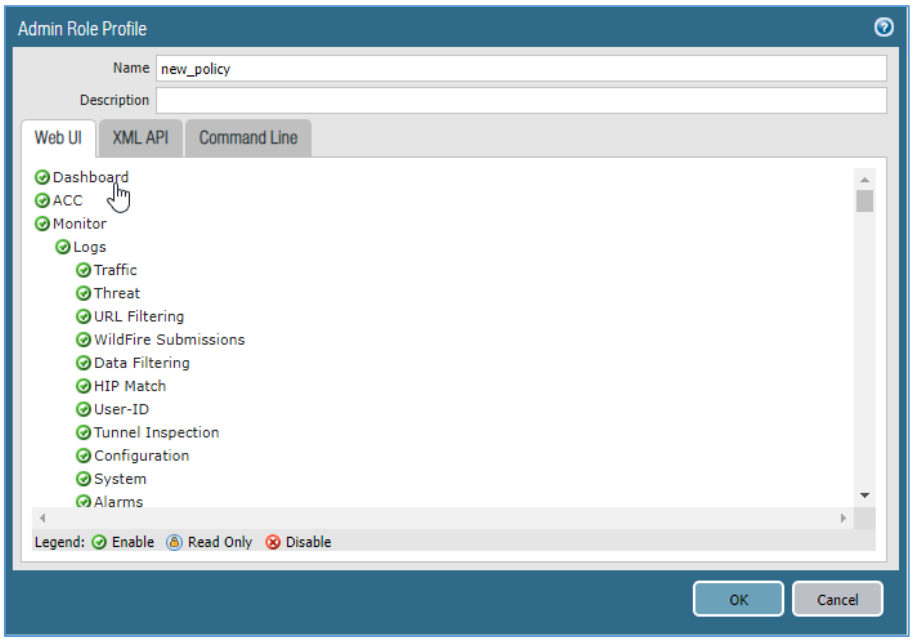
Rysunek 2.1 Zakładka Device > Admin Roles

Następnym krokiem aby dodać własną grupę pozwoleń i zakazów należy znaleźć w lewym dolnym rogu przycisk **Add**.



Rysunek 2.2 Dodanie nowych zasad

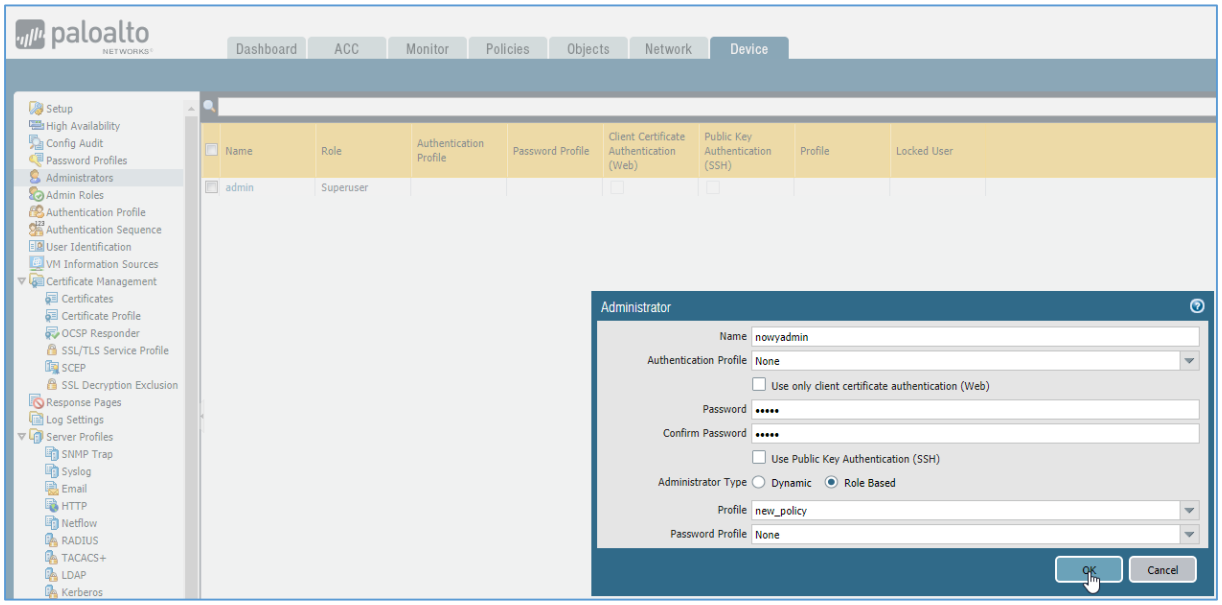
Okno konfiguracyjne wygląda w taki sposób:



Rysunek 2.3 Okno konfiguracyjne nowej grupy zasad

Jak widać można tam nadać nazwę naszemu profilowi zasad, opis oraz powybierać, które opcje chcemy żeby dany profil posiadał. Mamy trzy zakładki, ale nas interesuje tylko Web UI, czyli na co pozwalamy danemu profilowi w przypadku konfiguracji urządzenia za pomocą strony www. Z kolei zakładka Command Line to zakładka zasad, na które ma pozwolenie ten profil przy konfiguracji po CLI. Po zakończeniu konfiguracji klikamy **OK** w prawym dolnym rogu.

Teraz możemy przejść do zakładki **Device > Administrators** gdzie możemy dodać nowych użytkowników. Robimy to znowu za pomocą przycisku **Add** i widzimy nowe okno konfiguracyjne tak jak na rysunku poniżej.



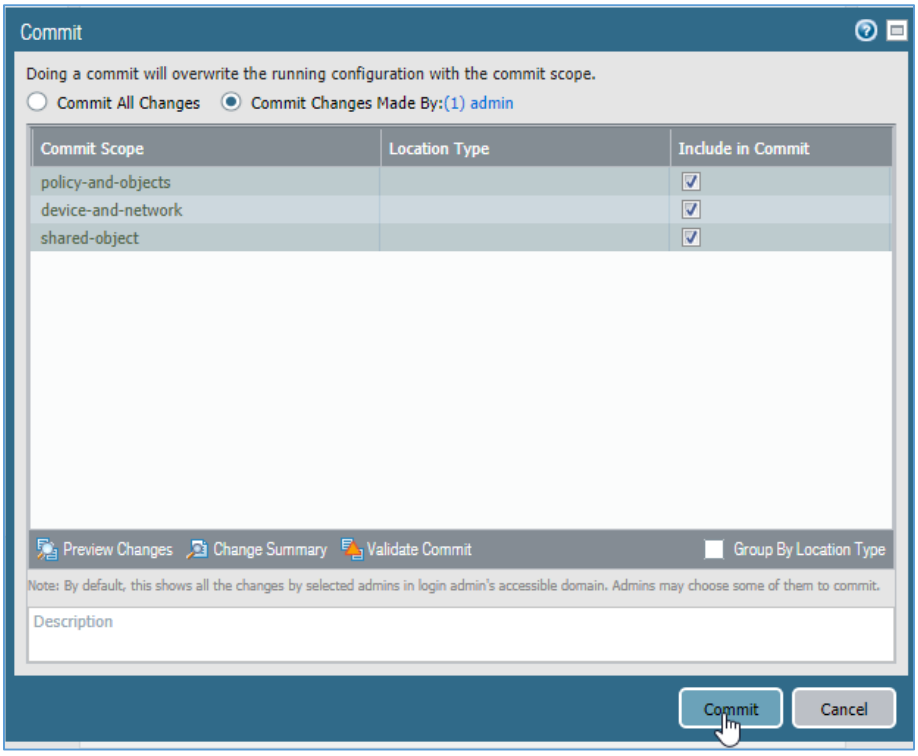
Rysunek 2.4 Dodawanie nowego użytkownika w zakładce Device > Administrators

Możemy nadać nazwę naszemu nowemu użytkownikowi, wybrać profil autoryzacji, nadać hasło oraz wybrać typ użytkownika oraz profil zasad. W naszym przypadku typ użytkownika będzie **Role Based** i wybierzemy nowo zrobioną grupę zasad. Następnie klikamy **OK** i nasz nowy użytkownik został dodany.

b) Zapisywanie konfiguracji

Aby zapisać konfigurację należy znaleźć w prawym górnym rogu przycisk **Commit** tak jak na rysunku poniżej. Po naciśnięciu tego przycisku zobaczymy opis zmian, które zostały wykonane od rozpoczęcia pracy w tej sesji. Jeśli wszystko się zgadza z naszymi założeniami możemy przejść dalej i kliknąć znów **Commit** co spowoduje załadowanie tych zmian do firewalla.

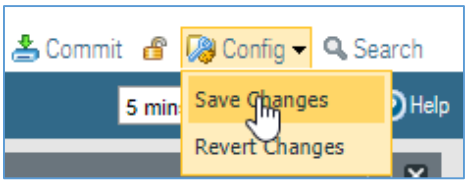
Rysunek 2.5 Przycisk Commit na panelu górnym



Rysunek 2.6 Okno zmian dokonanych w tej sesji

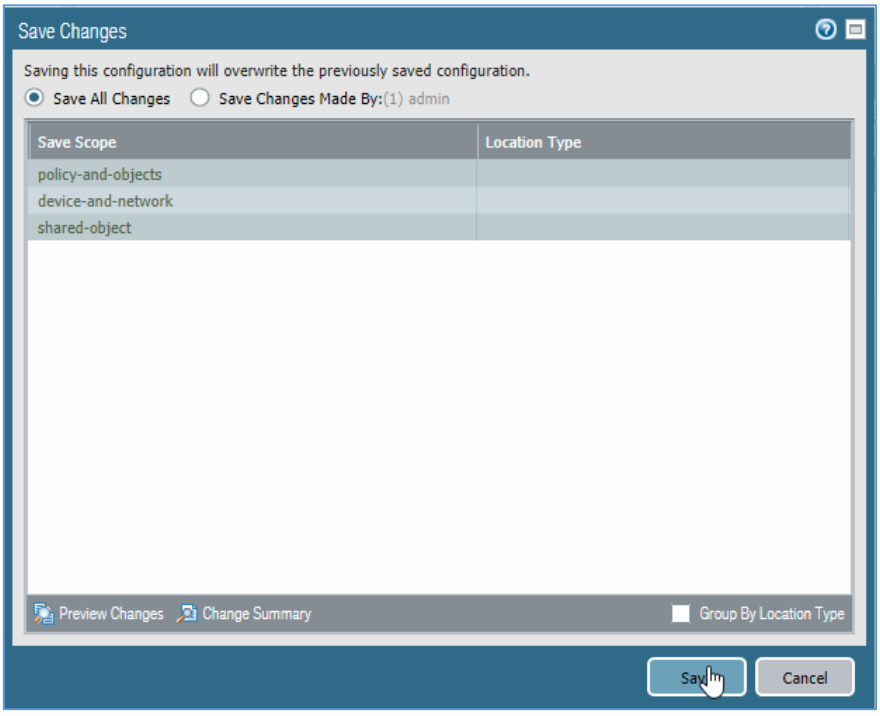
Po naciśnięciu przycisku **Commit** zobaczymy pasek ładowania konfiguracji do firewalla. Potem dostaniemy powiadomienie o tym czy konfiguracja została załadowana (Success) czy nie (Failed).

Kolejnym krokiem przy zapisywaniu konfiguracji jest zapisanie zmian już w urządzeniu co pozwoli na załadowanie tej konfiguracji ponownie przy resecie. Należy znaleźć przycisk **Config > Save Changes** zaraz obok przycisku **Commit**.

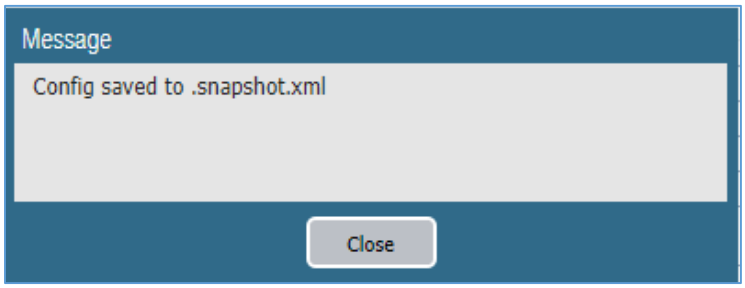


Rysunek 2.7 Przycisk Save Changes

Znów mamy podsumowanie zmian dokonanych i należy je zapisać za pomocą przycisku **Save.**



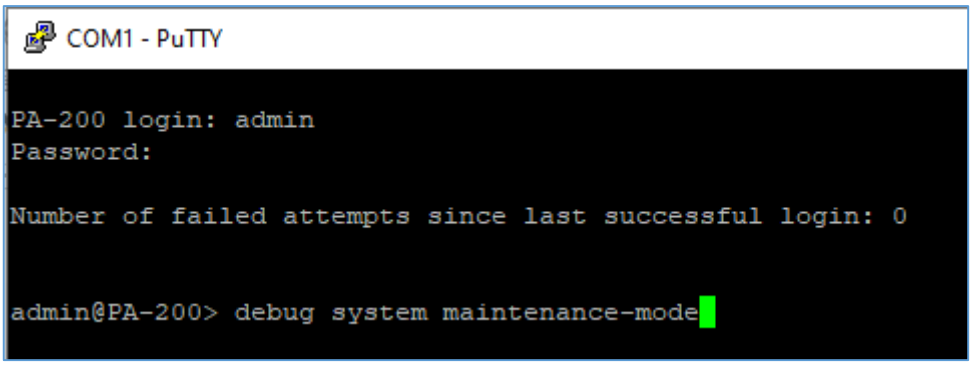
Rysunek 2.8 Zapisanie zmian w konfiguracji



Rysunek 2.9 Potwierdzenie zapisu zmian

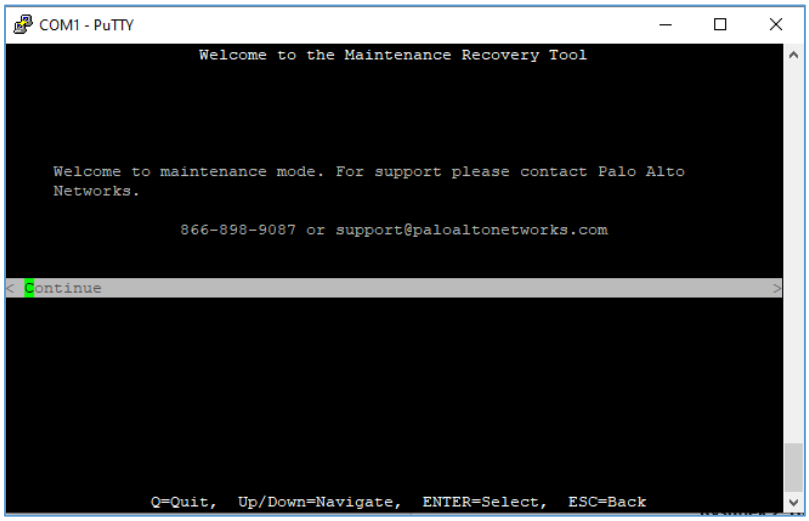
c) Przywracanie ustawień fabrycznych na urządzeniu (cały proces około 5-10 minut)

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.



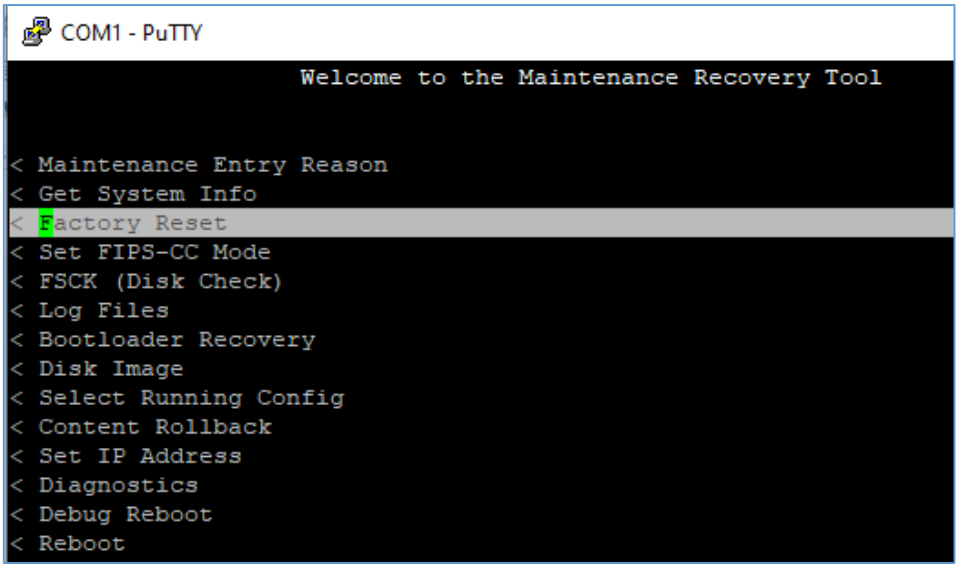
Rysunek 2.10 Przejście do trybu maintenance

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

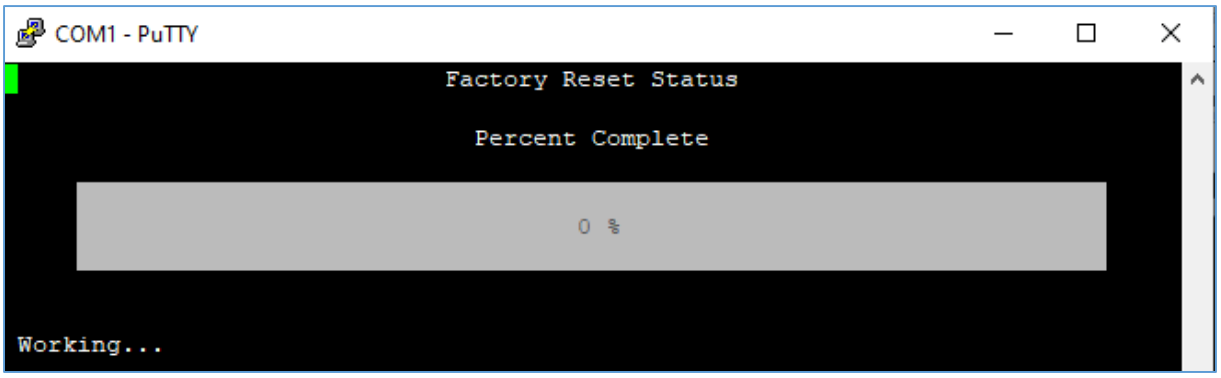


Rysunek 2.11 Tryb maintenance

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



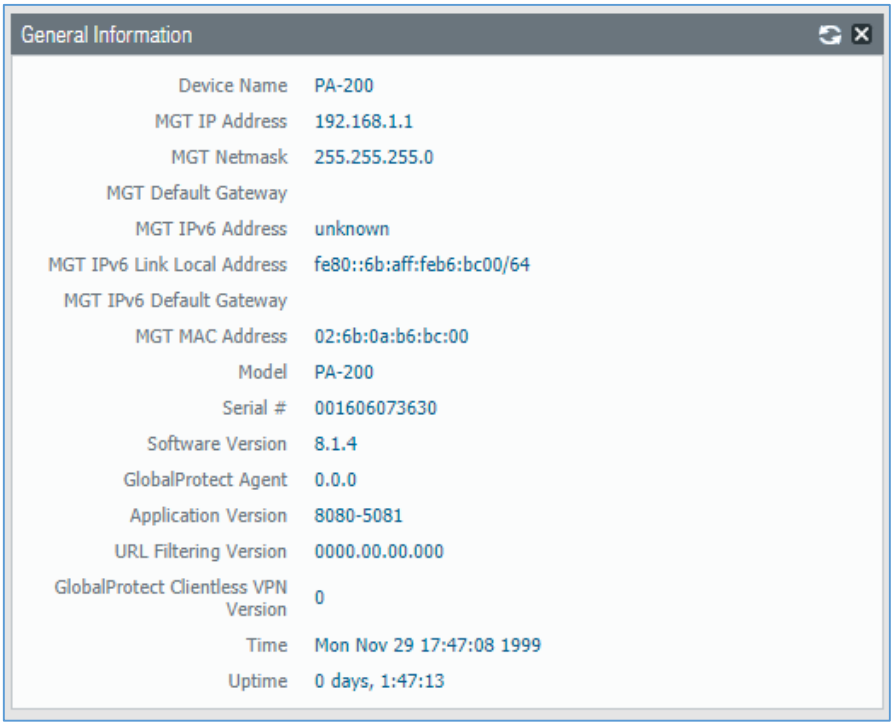
Rysunek 2.12 Wybór opcji Factory Reset



Rysunek 2.13 Progress stanu przywracania ustawień fabrycznych

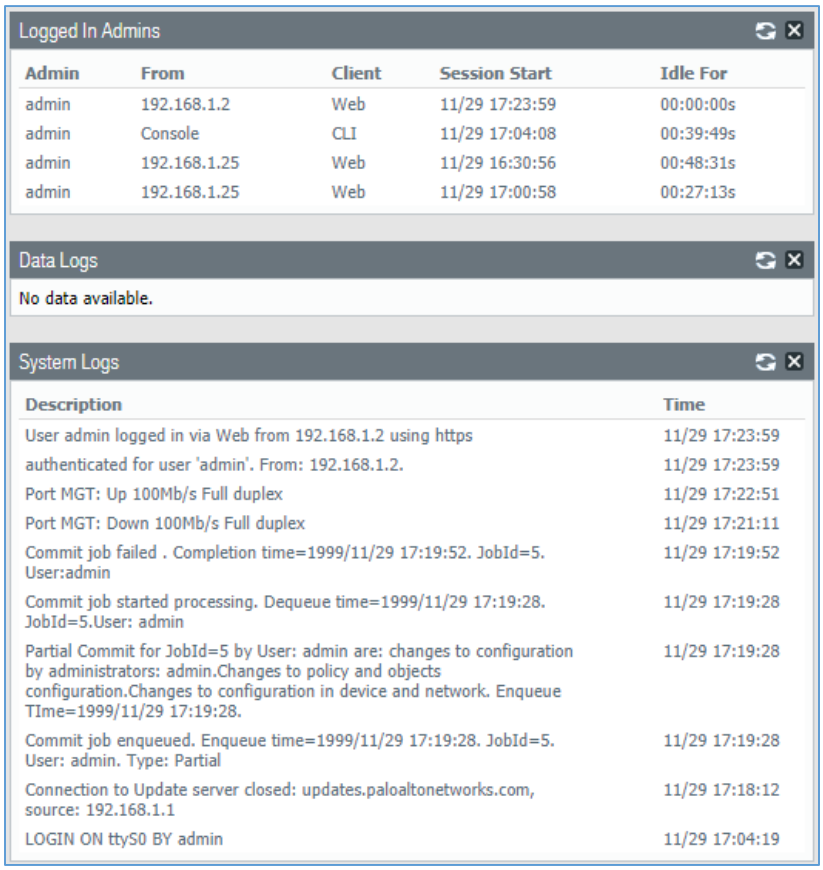
d) Informacje podstawowe na głównym panelu

Wróćmy teraz do głównego panelu tzw. **Dashboard,** który widzimy od razu po zalogowaniu się na firewall. Możemy znaleźć tutaj wiele przydatnych informacji na temat urządzenia. Między innymi widnieje tam okienko **General Information**, które opisuje główne informacje na temat danego urządzenia. Widzimy tam adres IP za pomocą, którego się łączymy z firewallem, wersje programowania, adres MAC etc.



Rysunek 2.14 Okienko Dashboard > General Information

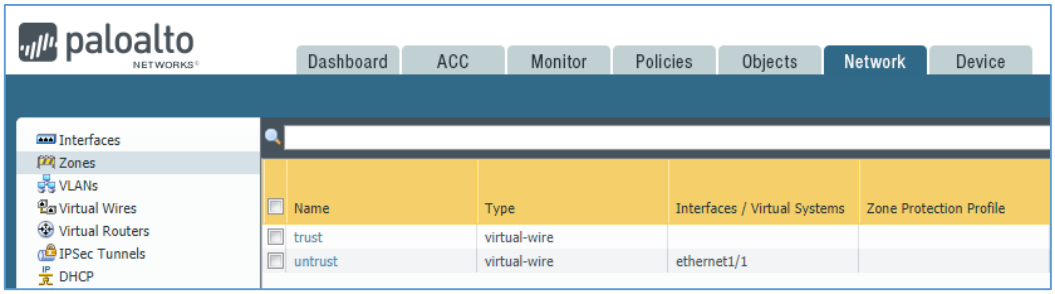
Kolejnymi informacjami, które możemy znaleźć na tym panelu są informacje dotyczące logów systemowych oraz użytkowników, którzy logowali się na to urządzenie.



Rysunek 2.15 Okienka Dashboard > Logged in / Data Logs / System Logs

e) Konfiguracja interfejsów urządzenia

Jako że znajdujemy się na urządzeniu firewall to nie możemy podejść do konfiguracji interfejsów tak jakby to było normalne urządzenie warstwy trzeciej. Najpierw musimy zająć się tzw. Zone'ami dlatego, że każdy interfejs powinien się znajdować w jednym obszarze. Typowo są to obszary **inside, outside** oraz **DMZ**. Możemy je znaleźć w zakładce **Network > Zones** tak jak na rysunku poniżej.



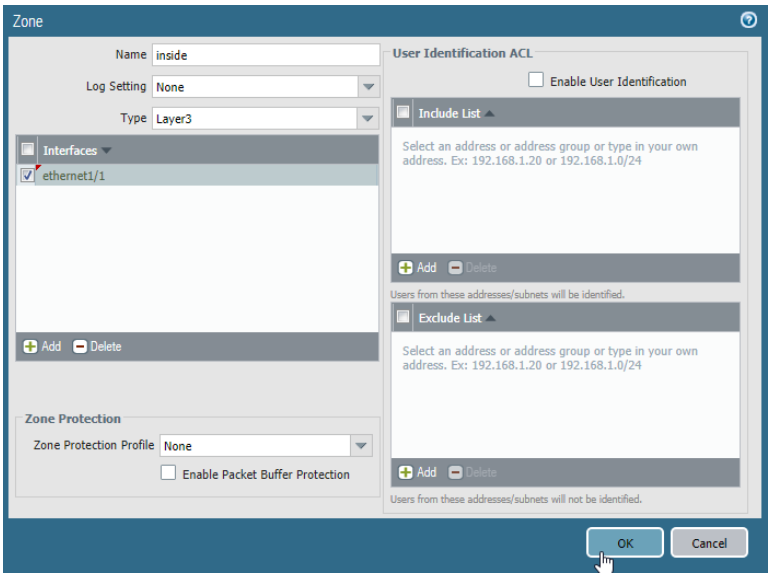
Rysunek 2.16 Zakładka Network > Zones

Jeśli chcemy to możemy edytować już istniejące wpisy, usunąć je lub dodać nowe. Dla przykładu zedytujemy obszary, które już istnieją oraz dodamy nowy – **DMZ.**

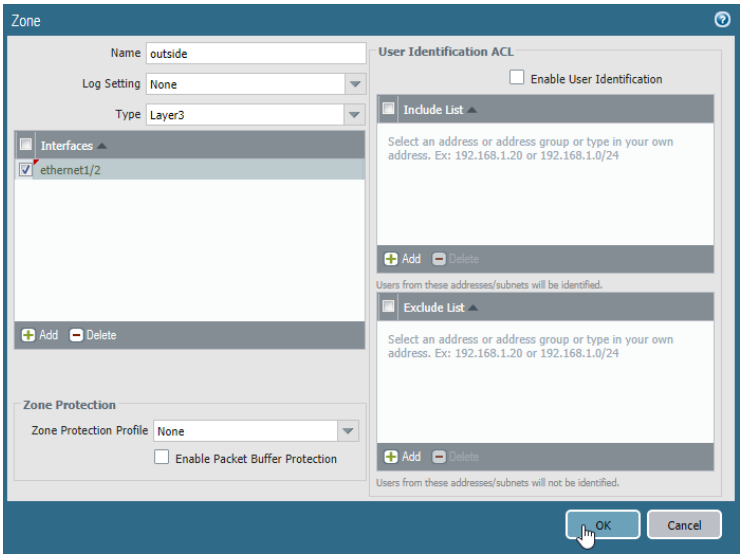
Interfejs **inside** jest to interfejs, który prowadzi do sieci wewnętrznej I jest zaufany w 100%. Żadne zagrożenie z niego nie napływa bo jest to sieć zaufana – ta którą kontrolujesz jako administrator sieci.

Interfejs **DMZ** jest to interfejs, który prowadzi do tzw. “strefy zdemilitaryzowanej”. Jest to część Twojej sieci wydzielona na firewallu, ale poświęcona np. serwerom, lub innym rzeczom do których dostęp mają mieć użytkownicy spoza Twojej sieci. Ten obszar nie należy ani do sieci wewnętrznej, ani do sieci zewnętrznej. W przypadku włamania się na serwer znajdujący się w strefie zdemilitaryzowanej intruz nadal nie ma możliwości dostania się do chronionego obszaru sieci wewnętrznej.

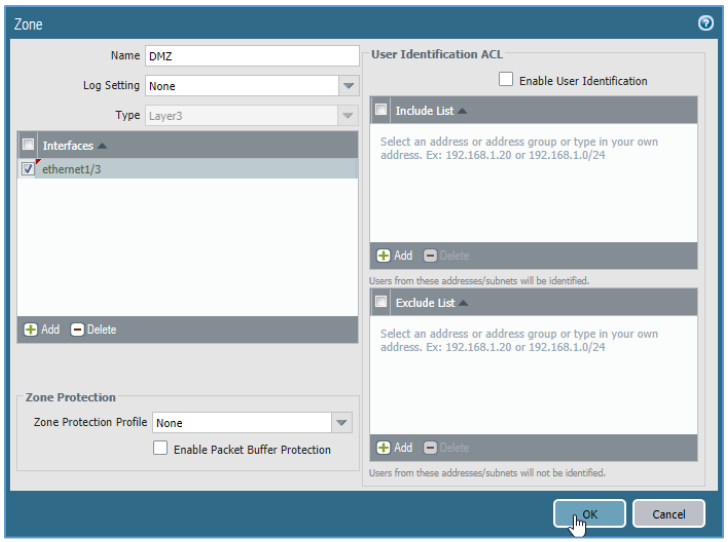
Interfejs **outside** jest to interfejs niezaufany, który prowadzi do sieci zewnętrznej. Jest to najczęściej trasa do Internetu.



Rysunek 2.17 Edytowanie obszaru trust

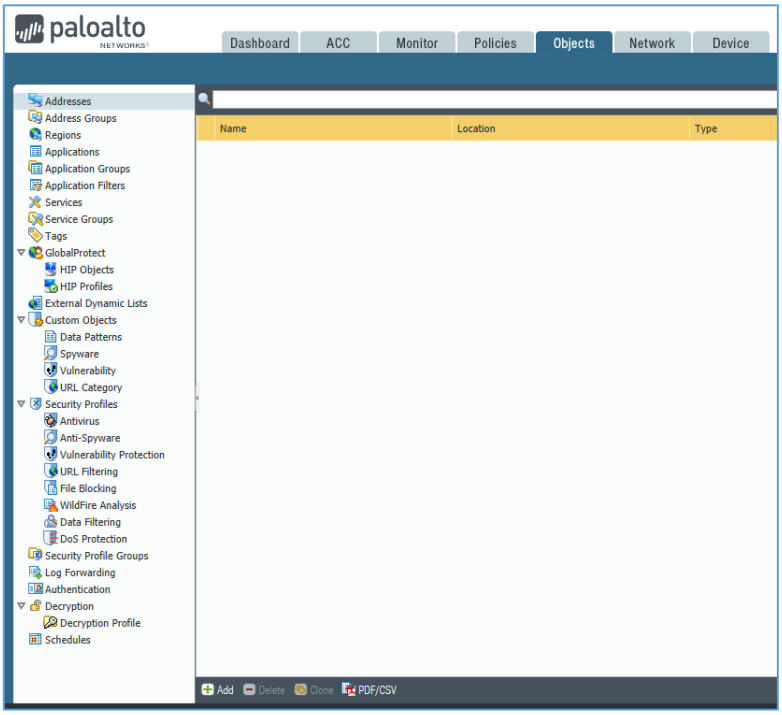


Rysunek 2.18 Edytowanie obszaru untrust



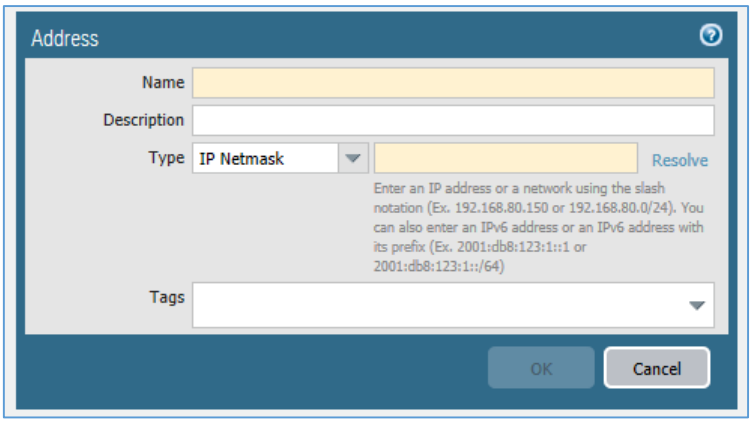
Rysunek 2.19 Dodawanie obszaru DMZ

Kolejnym krokiem, aby skonfigurować interfejsy urządzenia firewall Palo Alto jest zaadresowanie interfejsów Trusted, Untrusted oraz DMZ. Aby dodać interfejsy do bazy danych należy wpierw przejść do zakładki **Objects > Addresses** :



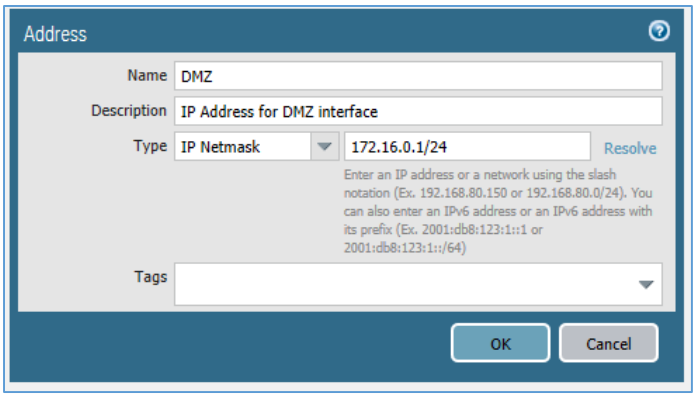
Rysunek 2.20 Zakładka Objects > Addresses

Domyślnie nie znajduje się tutaj żaden wpis. Żeby dodać trzy wpisy (po jednym adresie IP na każdy interfejs) należy w lewym dolnym rogu znaleźć przycisk **Add.**



Rysunek 2.21 Okno Add IP Address

Dla przykładu rozkład sieci do których będą należały nasze interfejsy to : *192.168.0.0/24* dla *Trusted*, 172.16.0.0/24 dla DMZ oraz *215.100.14.0/27* dla interfejsu Untrusted. Warto również w uporządkowany sposób nazywać wszystkie interfejsy, adresy IP etc oraz dodawać opisy. Poniżej widnieje przykładowe skonfigurowanie adresu IP:



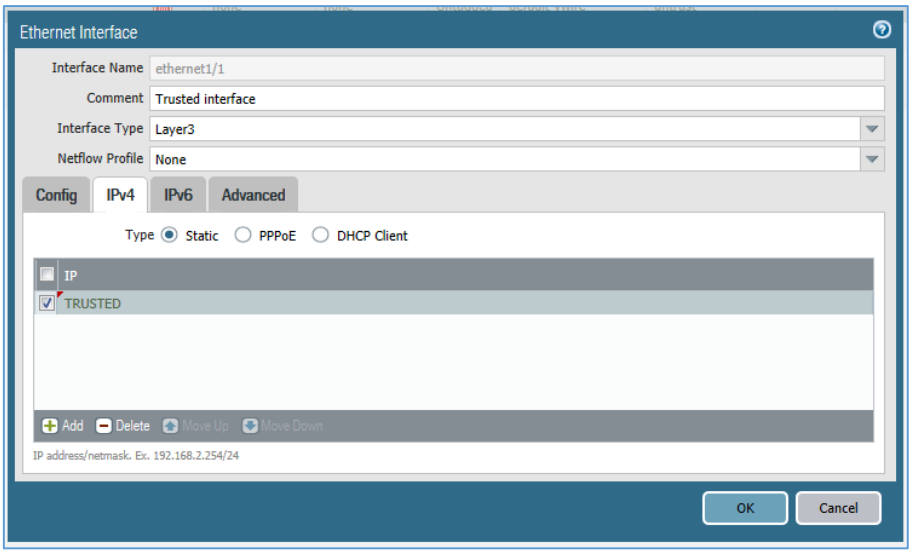
Rysunek 2.22 Przykładowy adres IP

Po skonfigurowaniu trzech adresów IP nasza tabela powinna wyglądać tak:

Name	Location	Type	Address
DMZ		IP Netmask	172.16.0.1/24
TRUSTED		IP Netmask	192.168.0.1/24
UNTRUSTED		IP Netmask	215.100.14.1/27

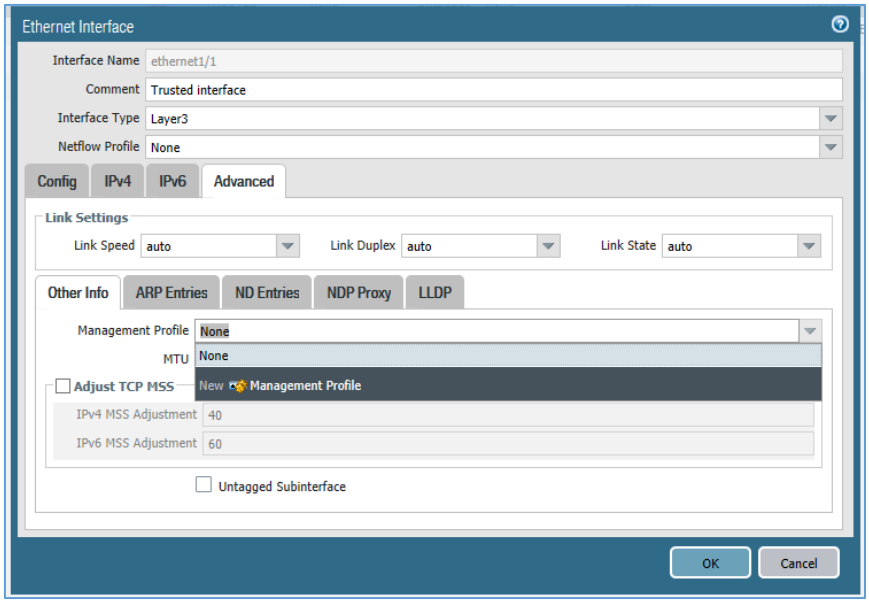
Rysunek 2.23 Tablica adresów IP

Teraz pozostało przypisać te adresy IP do odpowiednich interfejsów w zakładce **Network > Interfaces.** Po naciśnięciu LPM na odpowiedni interfejs powinno wyskoczyć nam takie okno jak poniżej. Należy wybrać opcje aby interfejs ten był interfejsem warstwy trzeciej oraz przypisać mu odpowiedni adres IP za pomocą przycisku **Add.**



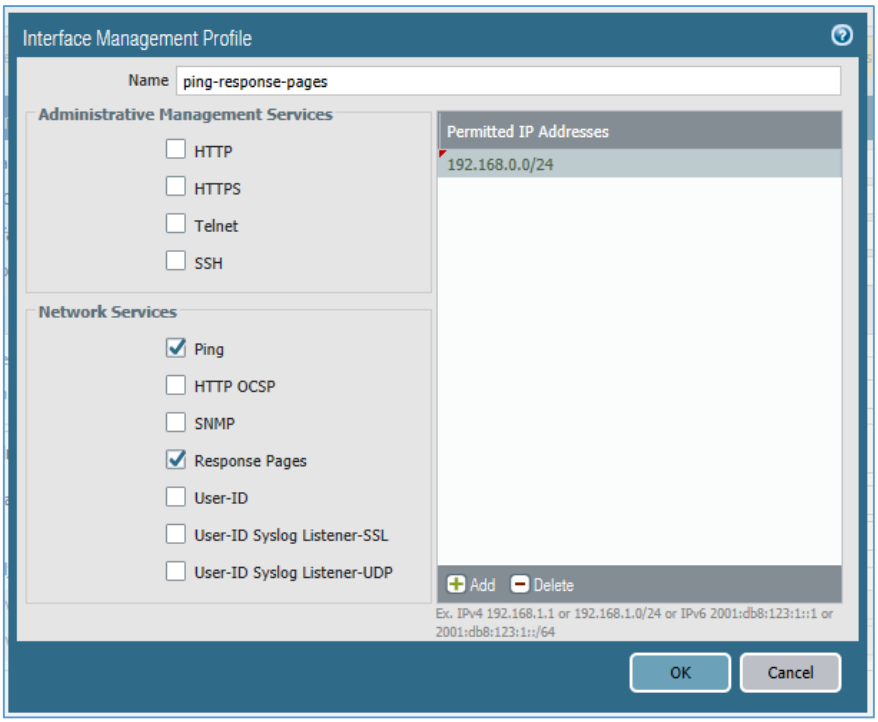
Rysunek 2.24 Przypisanie adresu IP do interfejsu

Po skonfigurowaniu trzech interfejsów w ten sposób oraz upewnieniu się, że każdy należy do odpowiedniego **Security Zone'a** należy przejść w przypadku interfejsu **Trusted** do zakładki **Advanced > Management Profile** aby stworzyć zasadę, która będzie pozwalała na ping tego interfejsu.



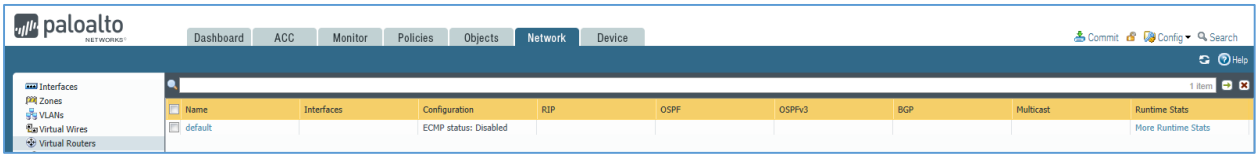
Rysunek 2.25 Zaawansowane opcje konfiguracji interfejsu

Tak jak poniżej widać należy wybrać opcje : **ping** oraz **response pages** i dodać adresy IP danej sieci.



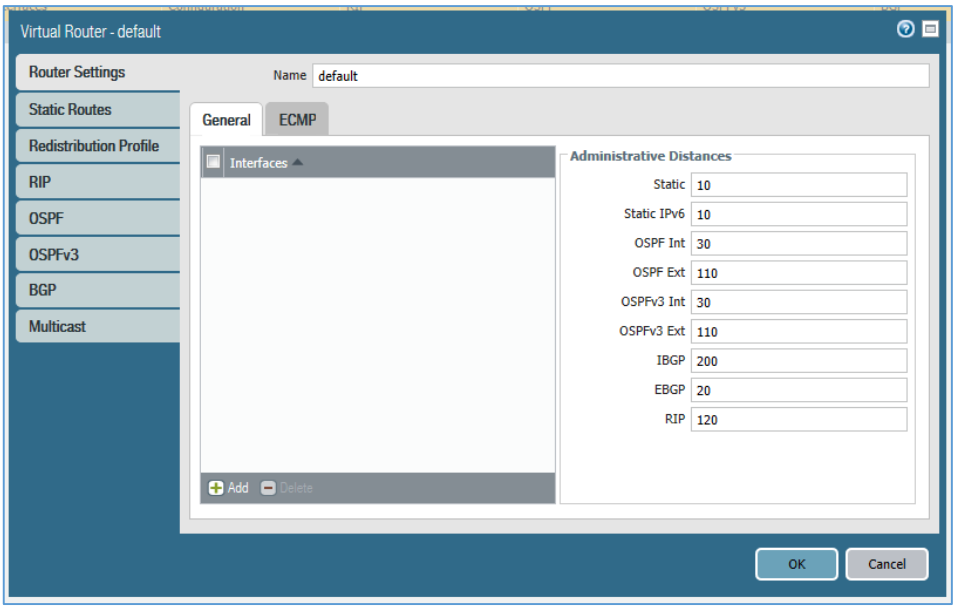
Rysunek 2.26 Konfiguracja Interface Management Profile

Kolejnym i ostatnim krokiem do skonfigurowania interfejsów warstwy trzeciej jest skonfigurowanie Routerów wirtualnych. Wynika to z tego, że firewall potrzebuje tych routerów, aby otrzymywać trasy do innych podsieci (dynamicznie lub konfiguracja statyczna). Jest t o możliwe w zakładce **Network > Virtual Routers.**



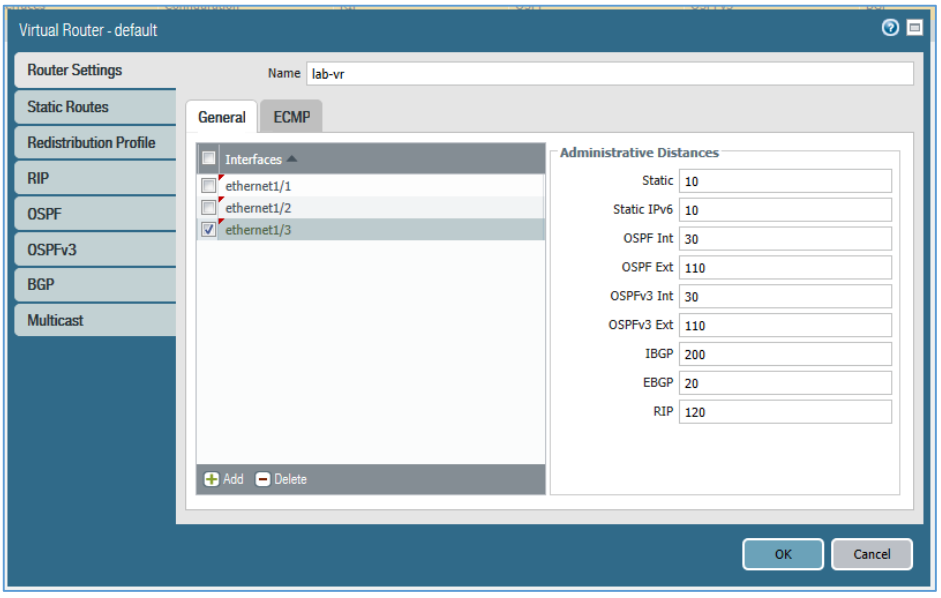
Rysunek 2.27 Zakładka Network > Virtual Routers

Nie będziemy dodawać kolejnego wirtualnego routera tylko zajmiemy się konfiguracją **default.**



Rysunek 2.28 Podstawowy router wirtualny „default”

Zmienimy jego nazwę na „lab-vr” i będzie on wirtualnym routerem dla interfejsów Trusted, Untrusted oraz DMZ.

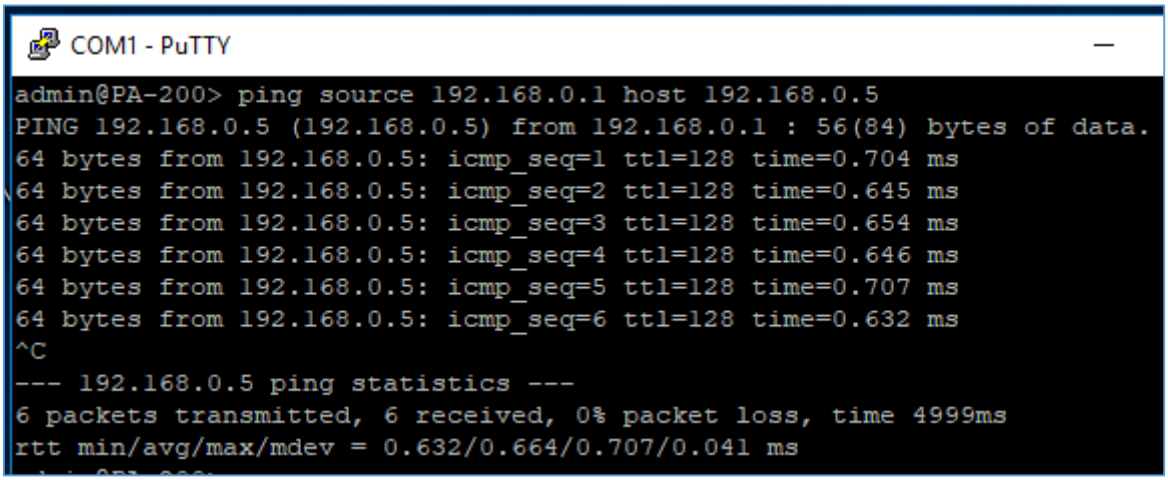


Rysunek 2.29 Skonfigurowany router wirtualny „lab-vr”

Aby przetestować czy nasza konfiguracja jest poprawna należy w prawym górnym rogu GUI znaleźć przycisk Commit 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.**

Gdy uda nam się zapisać konfigurację bez żadnych błędów i w zakładce **Dashboard** zobaczymy, że każdy z naszych interfejsów jest **up and running,** możemy przejść do testów za pomocą polecenia PING. Wychodzimy z GUI i podłączamy się za pomocą jakiegoś programu do symulacji CLI (np. PuTTY), a nasz komputer stacjonarny podłączamy za pomocą kabla Ethernet do portu ethernet1/1 **Trusted** i nadajemy mu np. adres IP *192.168.0.5/24.*

Przez CLI logujemy się do urządzenia oraz pingujemy stacje roboczą z firewalla.

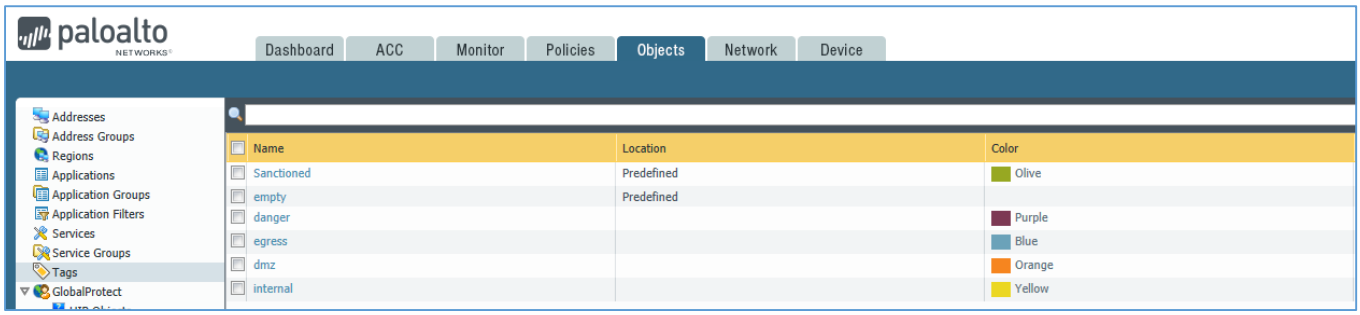


Rysunek 2.30 PING w stronę stacji roboczej

f) Tworzenie podstawowych reguł i zasad NAT

Porządek przy konfiguracji oraz zarządzaniu urządzeniami sieciowymi to pierwszy krok do sukcesu. Aby utrzymać porządek na urządzeniu Firewall Palo Alto używa się m.in. „**Tags**” . Służą one do grupowania, sortowania i filtrowania obiektów używając słów-kluczy lub fraz. Mogą być one zastosowane do grupowania adresów, usług, polityk etc. Dodatkowo można każdemu **Tagowi** nadać kolor, aby poruszanie się po środowisku GUI było jeszcze łatwiejsze.

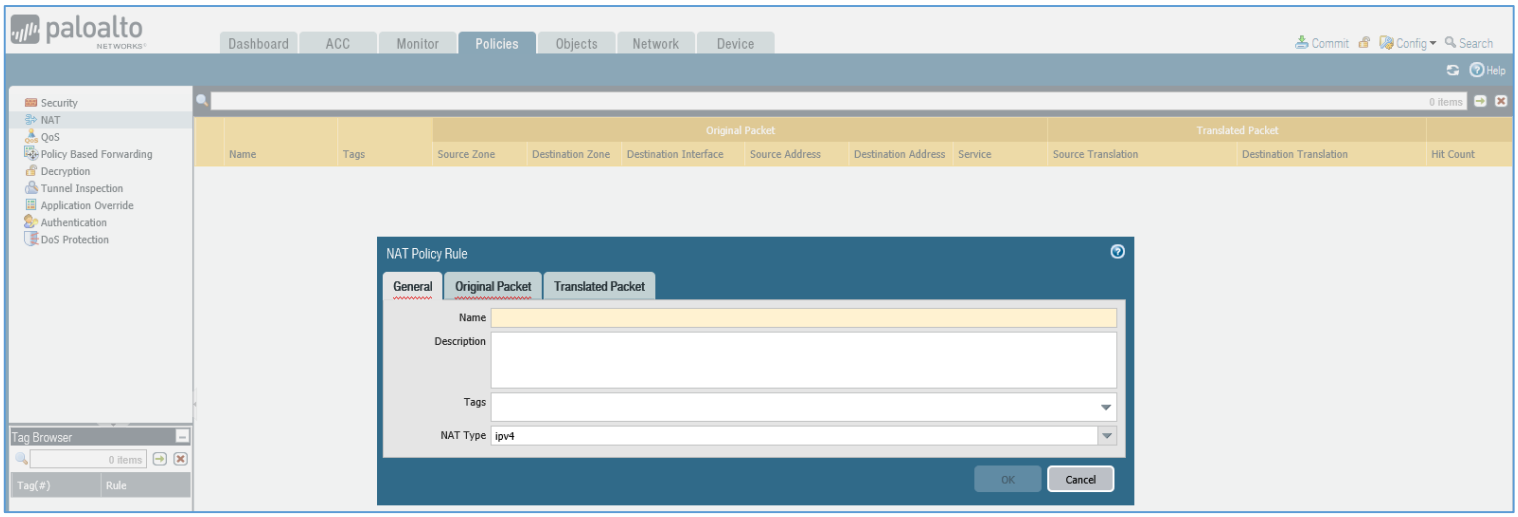
Tworzenie nowych **Tagów** znajduje się w zakładce **Objects > Tags** gdzie wybieramy opcje **ADD** aby zdefiniować nowy **Tag.** W naszym przypadku będą to tagi : „danger” o kolorze fioletowym, „egress” o kolorze niebieskim, „dmz” o kolorze pomarańczowym i „internal” o kolorze żółtym.



Rysunek 2.31 Zakładka Objects > Tags

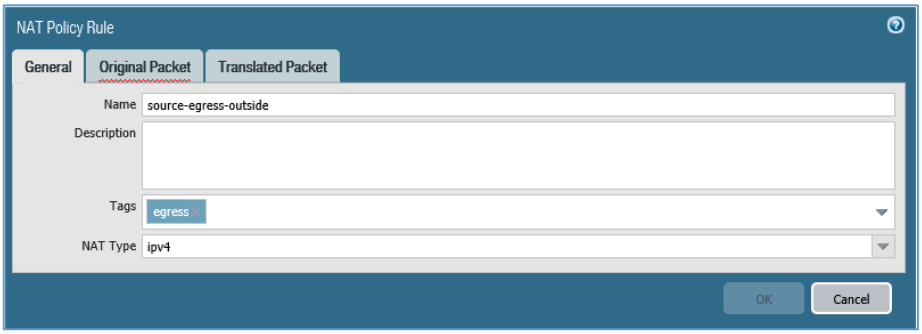
Dwa pierwsze wpisy to wpisy podstawowe, których nie można usunąć.

Następnie przechodzimy do konfiguracji źródłowej polityki NAT. Opcja ta znajduje się w zakładce **Policies > NAT** . Po wciśnięciu przycisku **ADD** mamy okno definiowana nowej polityki źródłowej NAT:



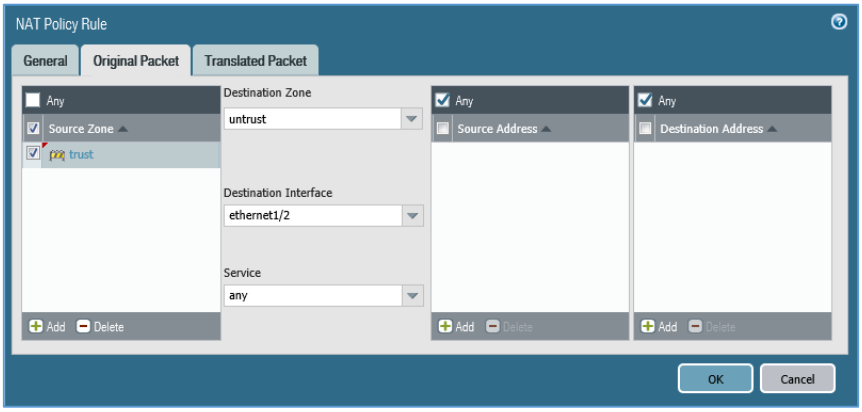
Rysunek 2.32 Okno Policies > NAT > Add

Musimy tutaj skonfigurować w odpowiedni sposób każdą zakładkę jaką mamy. Najpierw nadajemy nazwę *source-egress-outside* naszej polityce NAT oraz przypisujemy do niej tag **egress**.



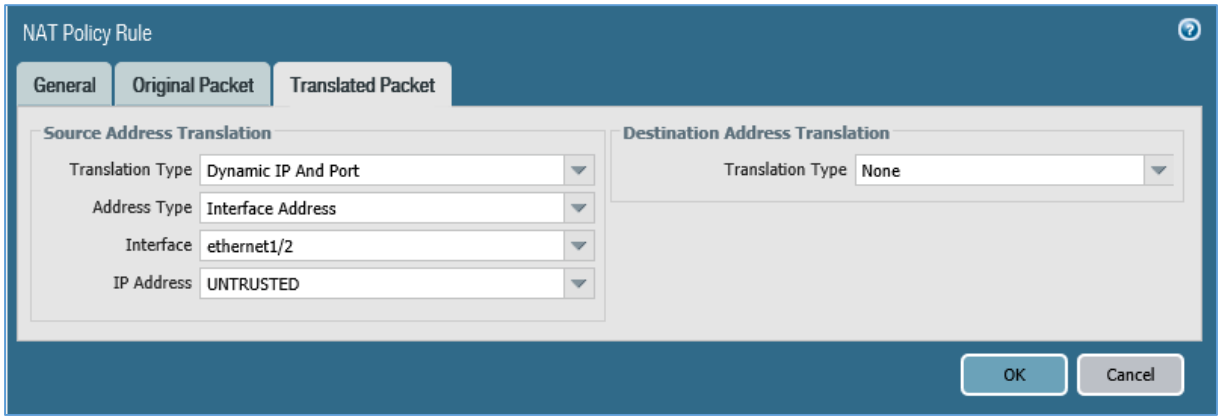
Rysunek 2.33 Zakładka General w NAT Policy Rule

W kolejnej zakładce należy wybrać source i destination zone oraz destination interface. Dla nas source zone to **trusted,** a destination zone i destination interface to **untrusted**.



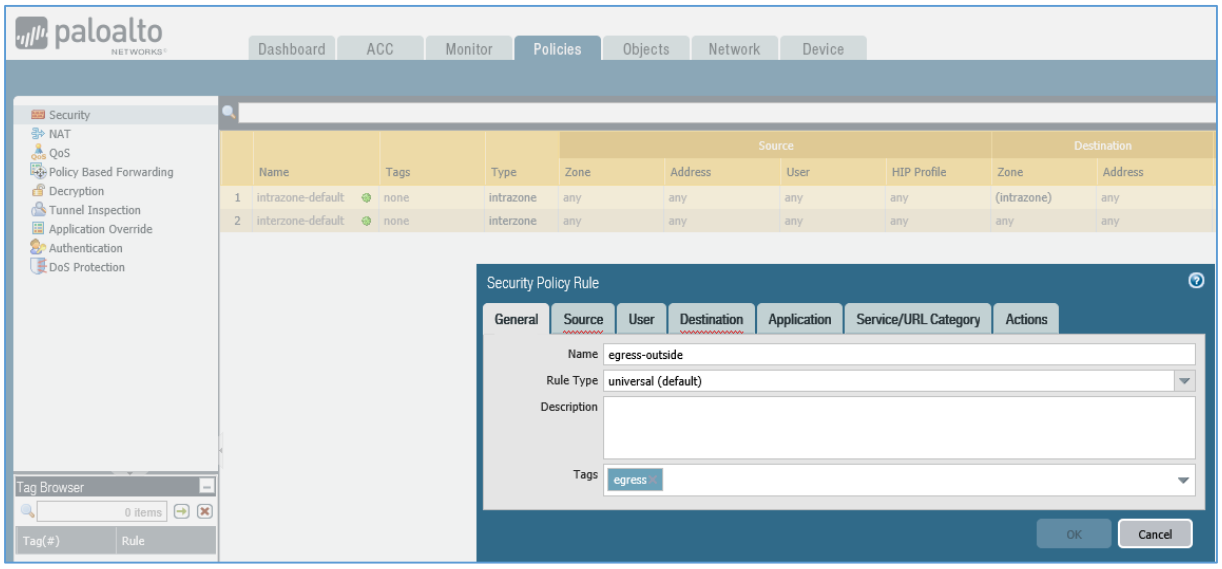
Rysunek 2.34 Zakładka Original Packet w NAT Policy Rule

Tematyka ostatniej zakładki skupia się wokół translacji adresów IP oraz numerów portów. My wybieramy rodzaj translacji : **Dynamic IP and Port**, rodzaj adresu : **interface address**, interfejs : **ethernet1/2 (untrusted)** oraz IP Address wybieramy **adres IP tego interfejsu lub nazwę interfejsu.**



Rysunek 2.35 Zakładka Translated Packet w NAT Policy Rule

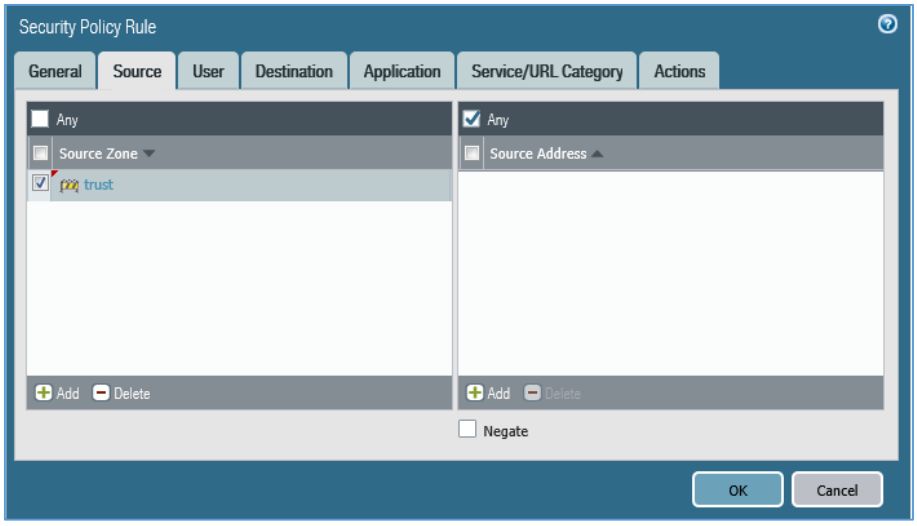
Jesteśmy już blisko uzyskania dostępu do Internetu na tym interfejsie (przykładowo), ale pozostało nam skonfigurować Security Policy Rules. Przechodzimy do nich za pomocą **Policies > Security.** Po wciśnięciu przycisku **ADD** możemy dodać nowy wpis. Nasz nowy wpis będzie wpisem uniwersalnym o nazwie *egress-outside* .



Rysunek 2.36 Okno „ADD" w Policies > Security

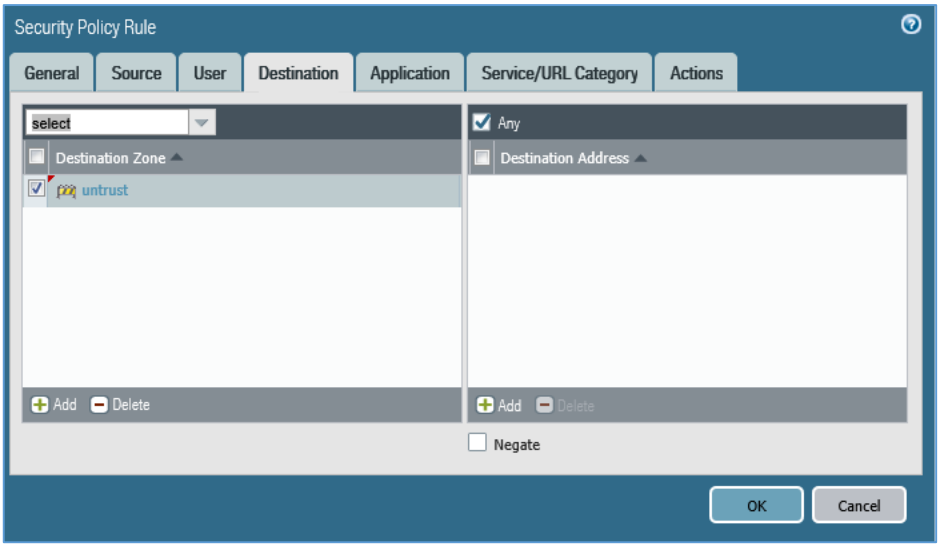
Kolejnymi zakładkami tego okna, na których się skupimy są : **Source i Destination**. W reszcie okien należy się upewnić czy : w oknie **Application** jest zaznaczone *Any* , w oknie **Service/URL Category** jest zaznaczone *application-default* oraz czy w zakładce **Actions** mamy wybrane *Action setting – Allow oraz Log Setting – Log at Session End.*

W oknie **Source** należy wybrać source zone **trust** oraz source address **any.**



Rysunek 2.37 Zakładka Source w Security Policy Rule

Natomiast w oknie **Destination** destination zone **untrust** i destination address **any.**



Rysunek 2.38 Zakładka Destination w Security Policy Rule

Ostatnim krokiem jest wysłanie konfiguracji do urządzenia sieciowego za pomocą funkcji **Commit.** Był to przykład typowej konfiguracji NAT z dynamiczną translacją adresów i portów.