UWAGA!

Do wykonania ćwiczenia wykorzystaj maszynę wirtualną Windows Server 2019 z zainstalowanym kontrolerem domeny.

1. W Serwerze: Pierwsza karta sieciowa sieć wewnętrzna (adresacja IP: 192.167.0.1/24, DNS 192.167.0.1), druga karta sieciowa NAT (adres i DNS otrzymywany z DHCP).
2. W stacji roboczej Windows 10: jedna karta sieciowa sieć wewnętrzna (adresacja IP: 192.167.0.21/24, Brama i DNS: 192.167.0.1). Klient nie podłączony do domeny.
3. Przejrzyj na serwerze ustawienia zapory systemu Windows, w tym reguły przychodzące.
4. Dodaj nową regułę przychodzącą niestandardową dla wszystkich programów (protokół TCP, port lokalny 9000, port zdalny „wszystkie porty"). Reguła ma dotyczyć adresu IP 192.167.0.0/24. Ustaw Akcję „Zezwalaj na połączenie". Pozostaw zastosowanie domyślne (domena, prywatny i publiczny). Nazwij regułę Reguła_XXX (gdzie XXX to Twoje imię bez polskich znaków). Wyświetl listę reguł przychodzących.
5. Dodaj nową regułę wychodzącą. W celu przetestowania reguły zacznij od ustawienia w bezpieczeństwie przeglądarki Internet Explorer – „nie używaj zalecanych ustawień" oraz „wyślij żądania nie śledź informujące witryny, że mają Cię nie śledzić". Otwórz stronę msn.com w przeglądarce. Wybierz „zapora systemu Windows z zabezpieczeniami zaawansowanymi", PPM właściwości. We właściwościach, na karcie „profil domeny", „profil prywatny" i „profil publiczny" ustaw „zablokuj" dla połączeń wychodzących. W przeglądarce spróbuj ponownie wejść na stronę msn.com. Dodaj regułę wychodzącą (tam gdzie przychodzącą) – typ reguły „Program", ścieżka: %ProgramFiles%(x86)\Internet Explorer\iexplore.exe (upewnij się, czy w Twoim serwerze internet explorer ma taką ścieżką, musi być ścieżka z Twojego serwera). Akcja – „zezwalaj na połączenie", profile jak w regule przychodzącej, nazwa „Zezwolenie na wyjście IE". Sprawdź w przeglądarce stronę msn.com.
6. Wyłącz filtrowanie wyjściowe, w profilu domeny, profilu prywatnym i profilu publicznym zmień „zablokuj" na „zezwalaj (domyślne)".