T: Konfiguracja firewall w Windows Server 2019

Cel ogólny lekcji: Uczeń pozna podstawowe zagadnienia związane z konfiguracją firewalla w Windows Server 2019 oraz będzie w stanie skonfigurować zapory dla określonych podsieci, użyć ustawień zasad grupy, włączyć rejestrowanie Windows Firewall oraz identyfikować komunikację używaną przez aplikacje, aby można było tworzyć reguły dla tej aplikacji.

Cele szczegółowe:

1. Uczeń będzie w stanie skonfigurować zakres reguły zapory do ograniczenia komunikacji do określonych podsieci.
2. Uczeń będzie w stanie skonfigurować autoryzacje połączeń dla reguły zapory.
3. Uczeń będzie w stanie użyć ustawień zasad grupy, aby włączyć zaporę na komputerach klienckich w środowisku domeny Active Directory.
4. Uczeń będzie w stanie włączyć rejestrowanie Windows Firewall, aby można było rozwiązywać problemy związane z regułami zapory.
5. Uczeń będzie w stanie identyfikować komunikację używaną przez aplikacje, aby można było tworzyć reguły dla tej aplikacji.

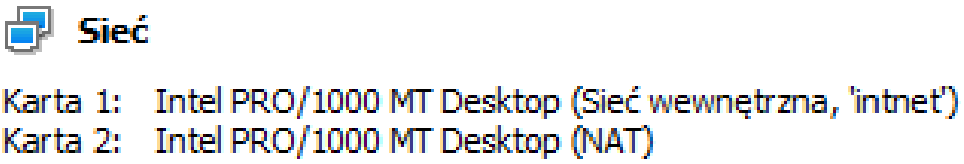
Ćwiczenie 2

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienia

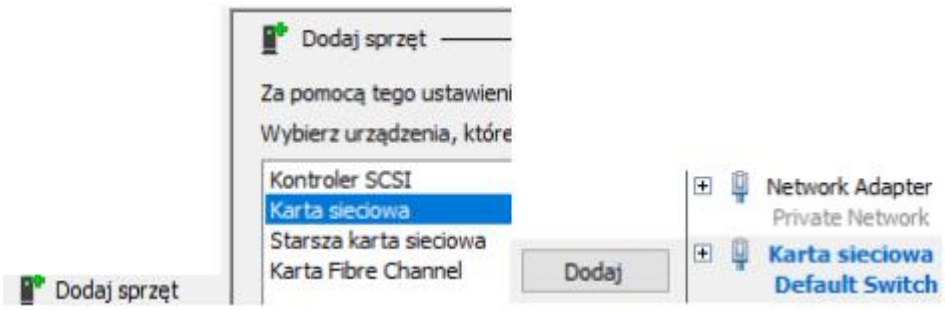
W Menedżer funkcji Hyper-V wybierz nazwa maszynę wirtualna twojej grupy_dc2019

• maszyny wirtualnej z plikiem startowym serwera dc są jak poniżej:

VirtualBox:



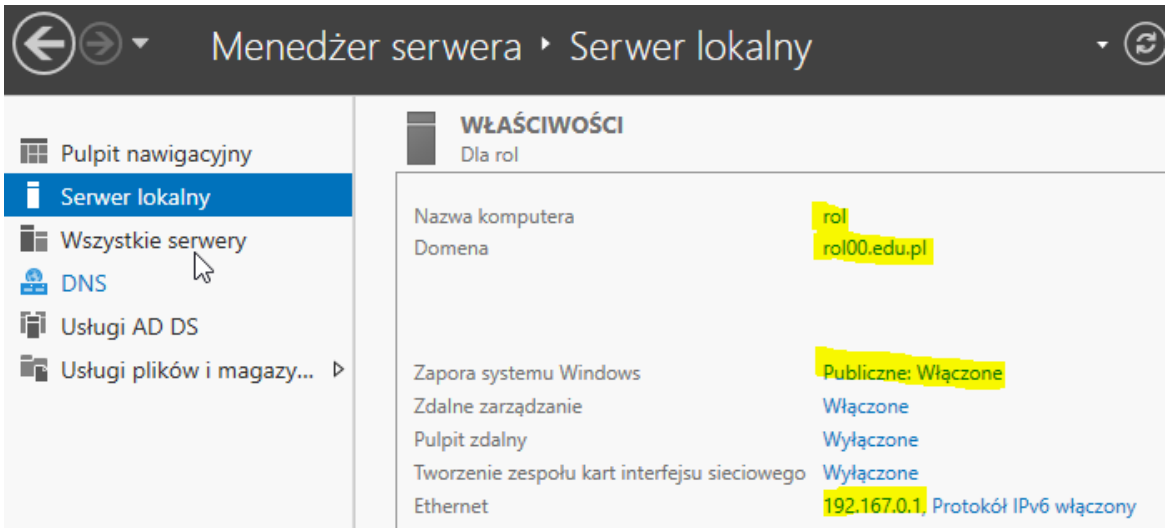
Hyper-V:

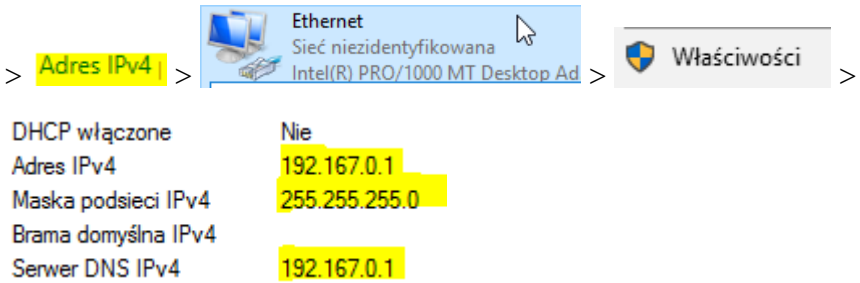


Uruchom maszynę > Ctrl+Delete > Administrator > zaq1@WSX

Upewnij się, że punk kontrolny, zawiera serwer z zainstalowanym kontrolerem domeny.

- system serwera są jak poniżej:





Utwórz kolejną migawkę stanu systemu serwera z informacją o treści przed cw2fw.

- klienta (Windows 10) jak poniżej:

lub

Podaj login: admin > i hasło: zaq1@WSX

Po ukończeniu tej lekcji będziesz umiał:

- Konfigurować zakres reguły zapory do ograniczenia komunikacji do określonych podsieci.
- Skonfigurować autoryzacje połączeń dla reguły zapory.
- Użyć ustawień zasad grupy, aby włączyć zaporę na komputerach klienckich w środowisku domeny Active Directory.
- Włączyć rejestrowanie Windows Firewall, aby można było rozwiązać problemy związane z regułami zapory.
- Identyfikować komunikację używaną przez aplikacje, aby można było tworzyć reguły dla tej aplikacji.

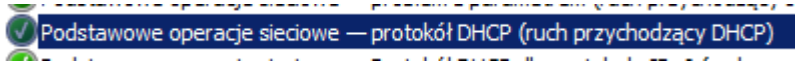
W zeszycie opisz dla każdego zadania procedurę konfiguracji firewall w Windows Server 2019.

Zadanie 1 Konfigurowanie zakresu zapory

Dodaj role srwera dhcp.

Wykonaj następujące kroki, aby skonfigurować zakres reguły:

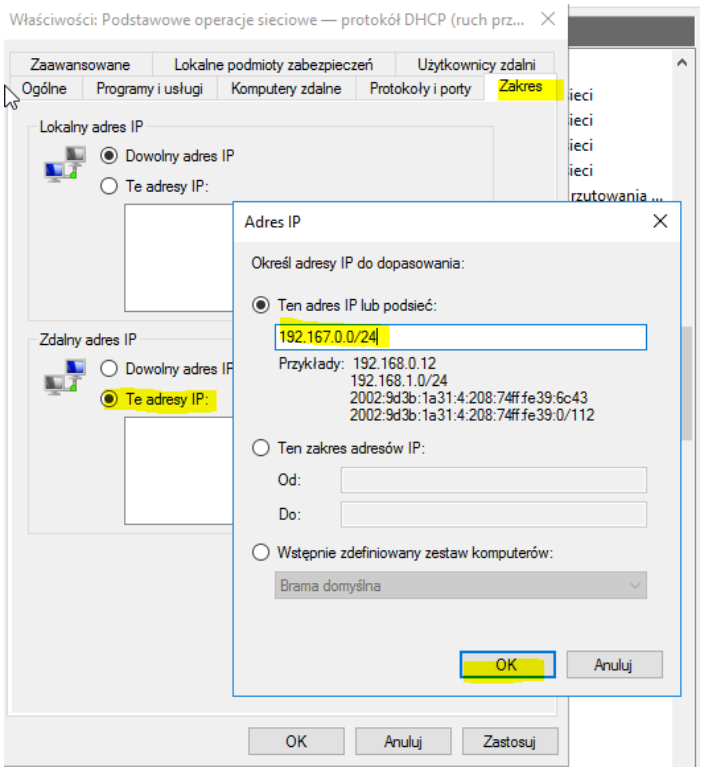
1. W przystawce Zapora systemu Windows z zaawansowanymi zabezpieczeniami wybierz lnbound Rules (Reguły przychodzące).
2. W panelu szczegółów kliknij prawym przyciskiem myszy regułę,



i wybierz Properties (Właściwości).
3. Kliknij kartę Scope (Zakres). W grupie Remote IP Address (Zdalny adres IP) wybierz These IP Addresses (Te adresy IP).
4. Kliknij Add (Dodaj) w grupie Remote IP Address (Zdalny adres IP).

Uwaga Konfigurowanie zakresu dla lokalnych adresów lP
Jedyny przypadek, gdy trzeba konfigurować zakres, używając grupy Local IP Address (Lokalny adres IP) występuje wtedy, gdy komputer ma skonfigurowanych wiele adresów IP, a nie chcemy przyjmować połączeń na wszystkich.

5. W oknie dialogowym IP Address (Adres IP) wybierz jak poniżej i kliknij OK:



Dostępne do wyboru opcje w tym oknie to:

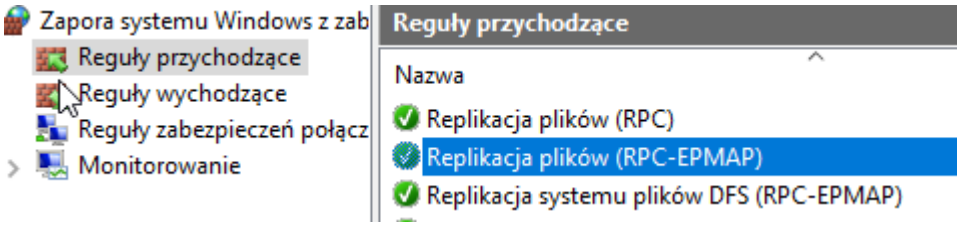
- **This IP Address Or Subnet (Ten adres IP lub podsieć)** gdzie możesz wpisać adres IP (taki jak 192.168.1.22) lub podsieć w notacji CIDR (Classless inter-Domain Routing) (taką jak 192.167.0.0/24), która ma używać tej reguły zapory.
- **This IP Address Range (Ten zakres adresów IP)** gdzie używając pól From (Od) i To (Do), możesz wpisać pierwszy i ostatni adres lP przedziału, który ma używać tej reguły zapory.

Zapisz w zeszycie, kiedy należy stosować powyższe ustawienie.
Poproś o sprawdzenie wykonanych czynności – zgłoszenie 1.

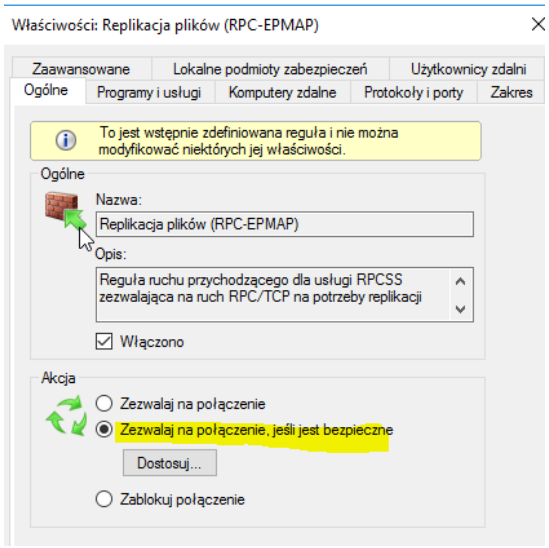
Zadanie 2 Autoryzowanie połączeń

Wykonaj następujące kroki, aby skonfigurować autoryzacje połączeń dla reguły zapory:

1. W Windows Firewall With Advanced Security\Inbound Rules (Zapora systemu Windows z zabezpieczeniami zaawansowanymi\Reguły przychodzące) wybierz Replikacja plików (RPC-EPMAP).



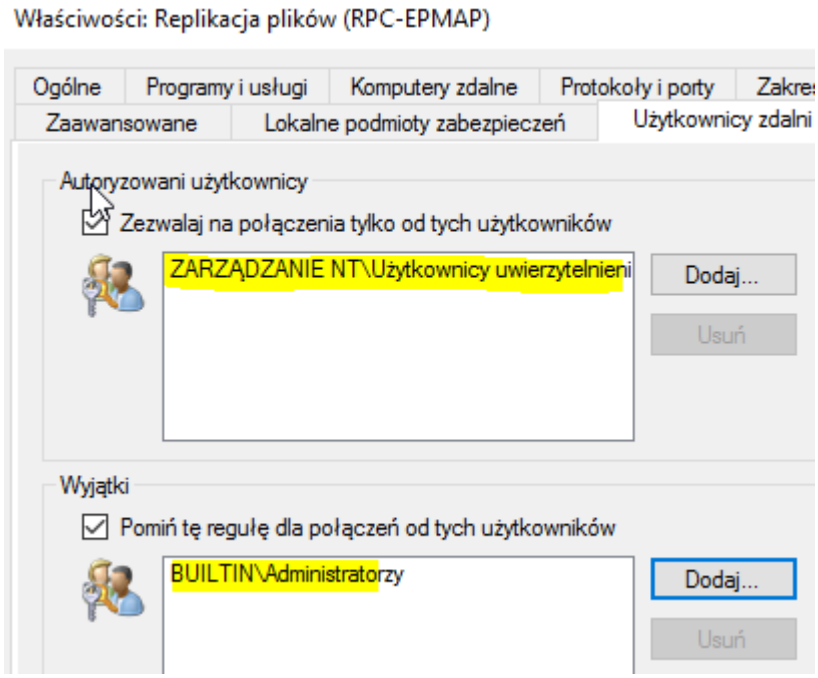
2. W panelu szczegółów kliknij prawym przyciskiem myszy regułę, Replikacja plików (RPC-EPMAP) a następnie wybierz Properties (Właściwości).
3. Kliknij kartę General (Ogólne). Zaznacz Allow Only Secure Connections (Zezwalaj tylko na bezpieczne połączenia). Ponieważ autoryzacja polega na IPsec, można skonfigurować ją tylko na połączeniach bezpiecznych.



4. Kliknij kartę Users (Użytkownicy) dla reguły przychodzącej dla reguły wychodzącej będzie karta Computers (Komputery).

- ***Aby pozwolić na połączenia tylko z pewnymi użytkownikami*** *Jeżeli edytujemy regułę wejściowa, zaznacz pole wyboru Only Allow Connections From These Users (Zezwalaj tylko na połączenia inicjowane przez tych użytkowników). Opcja ta jest dostępna tylko dla reguł połączeń przychodzących.*
- ***Aby pozwolić na połączenia z pewnymi komputerami*** *Zaznacz pole wyboru Only Allow Connections From These Computers (Zezwalaj na połączenia tylko z tych komputerów) dla reguły przychodzącej lub Only Allow Connections To These Computers (Zezwalaj tylko na połączenia z tymi komputerami) dla reguły wychodzącej.*

5. Kliknij Add i wybierz grupy zawierające użytkowników które chcesz autoryzować. Rysunek 2 ukazuje, jak karta Users (Użytkownicy) wygląda po skonfigurowaniu połączeń dla reguły przychodzącej (wejściowej). Kliknij OK.



Rysunek 2 Karta Użytkownicy

6. Kliknij OK.

Zdalne odświeżanie zasad grupy: porty wymagające reguł zapory.

Aby zaplanować zdalne odświeżanie zasad grupy dla komputerów przyłączonych do domeny, musisz mieć reguły zapory, które umożliwiają przyjmowanie przychodzącego ruchu sieciowego na portach wymienionych w poniższej tabeli.

Port serwera	Typ ruchu sieciowego
TCP, dynamiczne porty RPC, harmonogram (usługa Harmonogram zadań)	Zdalne zarządzanie zaplanowanymi zadaniami (RPC)
TCP, port 135, RPCSS (usługa zdalnego wywoływanie procedur)	Zdalne zarządzanie zaplanowanymi zadaniami (RPC-EPMAP)
TCP, wszystkie porty, Winmgmt (usługa Instrumentacja zarządzania Windows)	Instrumentacja zarządzania Windows (usługa WMI — ruch przychodzący)

Od tej pory dowolne połączenia, które odpowiadają regule zapory, będą wymagać lPsec do ustanowienia połączenia. Dodatkowo, jeżeli uwierzytelniony komputer lub użytkownik nie jest na liście uwierzytelnionych komputerów i użytkowników określonych w regule, połączenie będzie natychmiast odrzucane.

Zapisz w zeszycie, kiedy należy stosować powyższe ustawienie.

Poproś o sprawdzenie wykonanych czynności – zgłoszenie 2.

Konfigurowanie ustawień zapory za pomocą zasad grupy

Możemy konfigurować Windows Firewall używając Server Manager lub konsoli WFAS w folderze Administrative Tools (Narzędzia administracyjne) albo używając węzła

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall With Advanced Security (Konfiguracja komputera\Zasady\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi) obiektu GPO (Group Policy Object). Zazwyczaj konfiguruje się zasady, które stosują się do grup komputerów (w tym zasady zabezpieczeń połączeń lPsec), używając obiektów GPO i edytując specyficzne dla serwera zasady (takie jak konfiguracja przedziału adresów IP, od których kwerendy przyjmuje serwer DNS), używając narzędzi lokalnych.

Można użyć zasad grupy do zarządzania ustawieniami Windows Firewall dla komputerów stosujących Windows Server 2019 i Windows 10, używając dwóch węzłów:

- **Computer Configuration\PoIicies\Windows Settings\Security Settings\Windows Firewall With Advanced Security** (Konfiguracja komputera\Zasady\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi) ten węzeł stosuje ustawienia tylko do komputerów z systemami Windows 10 lub Windows Server 2019 i zapewnia dokładnie taki sam interfejs, jak jego odpowiednik w konsoli Sewer Manager. Należy zawsze używać tego węzła podczas konfigurowania komputerów *Windows Server 2019 i Windows 10,* ponieważ zapewnia bardziej szczegółową konfigurację reguł zapory.
- **Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall** (Konfiguracja komputera\Zasady\Szablony administracyjne\Sieć\Połączenia sieciowe\Zapora systemu Windows) ten węzeł wprowadza ustawienia do komputerów z systemem *Windows XP, Windows Server 2003, Windows 10 i Windows Server 2019.* To narzędzie jest mniej elastyczne niż konsola Windows Firewall With Advanced Security, ale ustawienia dotyczą wszystkich wersji Windows wspierających Windows Firewall. Jeżeli nie używamy nowych właściwości lPsec w Windows 10, możemy użyć tego węzła do konfiguracji wszystkich klientów.

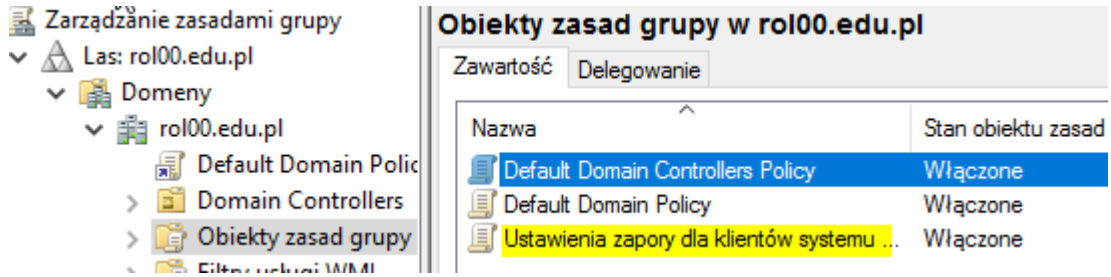
Dla osiągnięcia lepszych wyników można utworzyć oddzielne obiekty GPO dla systemów Windows 10/Windows Server 2019 i Windows XP/Windows Server 2003. Następnie można użyć kwerend WMI do skierowanie tych GPO do komputerów z odpowiednimi wersjami Windows.

Zadanie 3 Dodawanie ustawienia GPO, aby włączyć zaporę na komputerach klienckich.

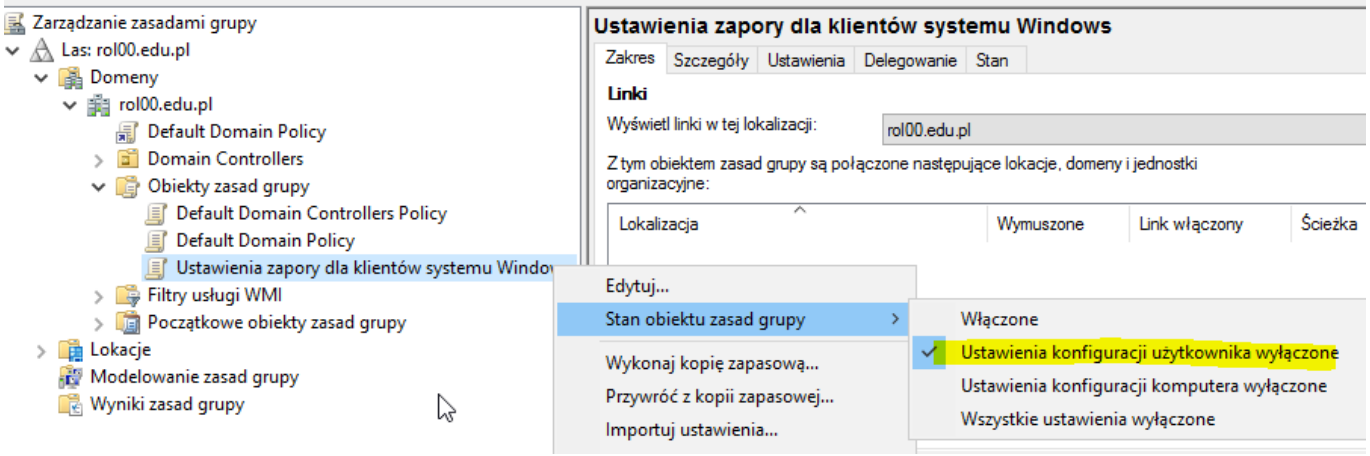
W tym kroku skonfiguruj GPO dla klienta obejmujące ustawienie, które umożliwia Zapora systemu Windows na wszystkich komputerach klienckich z systemem Windows 10 lub Windows Vista, do których ma zastosowanie GPO.

Dodaj ustawienie GPO, aby włączyć zaporę na komputerach klienckich:

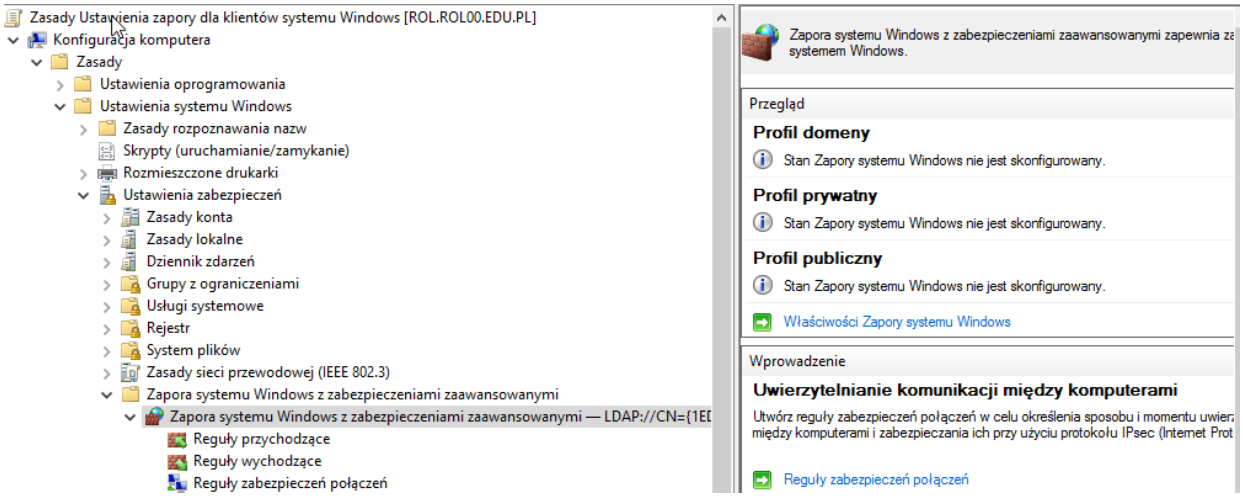
1. Na komputerze IS w Group Policy Management (Zarządzanie zasadami grupy) Group > Policy Objects (Obiekty zasad grupy) utwórz zasadę „Ustawienia zapory dla klientów systemu Windows”, a następnie kliknij przycisk Edytuj



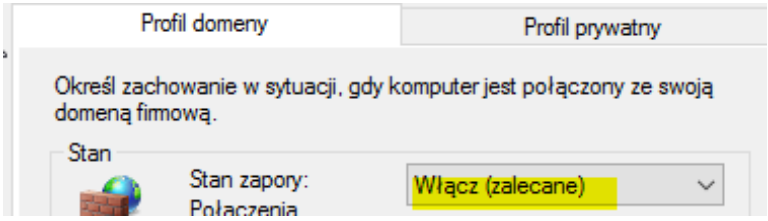
2. W Edytorze zarządzania zasadami grupy, kliknij prawym przyciskiem myszy utworzoną zasadę „Ustawienia zapory dla klientów systemu Windows”, a następnie wybierz Stan obiektu zasad grupy.
3. Zaznacz pole wyboru Ustawienia konfiguracji użytkownika wyłączone.
   Uwaga
   Zaleca się, aby usunąć sekcje użytkownika lub komputera w dowolnym GPO, w którym nie są one wykorzystywane. Poprawia to wydajność na komputerze klienckim, gdy stosuje GPO.



4. Edytuj zasadę „Ustawienia zapory dla klientów systemu Windows”.
5. W obszarze Konfiguracja komputera rozwiń Zasady/Ustawienia systemu Windows/ Ustawienia zabezpieczeń/Zapora systemu Windows z zabezpieczeniami zaawansowanymi.
6. Kliknij węzeł Zapora systemu Windows z zabezpieczeniami zaawansowanymi - LDAP://CN={GUID},CN=POLICIES,CN=SYSTEM,DC=ROL00,DC=EDU,DC=PL, gdzie GUID to unikalny numer przypisany do danej domeny.
7. W okienku wyników w ramach przeglądu należy zauważyć, że w każdym profilu lokalizacji sieciowej stan Zapora systemu Windows nie jest skonfigurowana, a następnie kliknij polecenie Właściwości Zapory systemu Windows.



8. Na karcie Profil domeny, kliknij listę rozwijaną obok stanu zapory, a następnie kliknij opcję Włącz (zalecane).

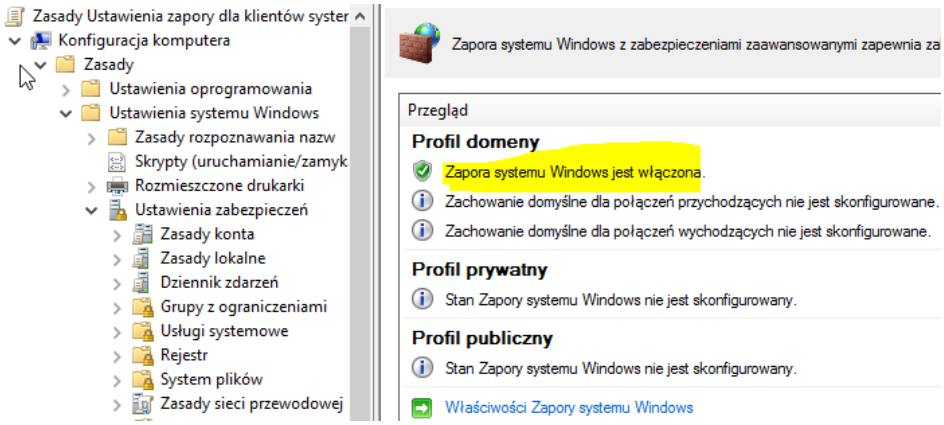


Uwaga

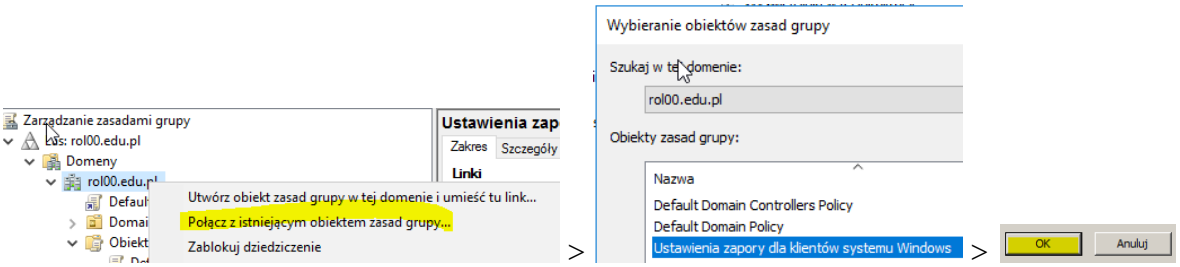
Może to wydawać się niepotrzebnym krokiem, ponieważ zapora jest domyślnie włączona na komputerach klienckich. Jeśli jednak zostawić to ustawienie nie skonfigurowane, lokalny administrator może wyłączyć zaporę. Ustawienie jej w GPO, jak pokazano w tym kroku włącza zaporę i zapobiega wyłączeniu przez lokalnego administratora.

9. Kliknij przycisk OK, aby zapisać zmiany. Uwaga: W panelu wyników, które Profil domeny pokazuje teraz Zapora systemu Windows jest włączona.
10. Zamknij Edytor zarządzania zasady grupy.

Oczekiwany efekt:



11. Połącz domenę z utworzonym obiektem zasad grup „Ustawienia zapory dla klientów systemu Windows”.

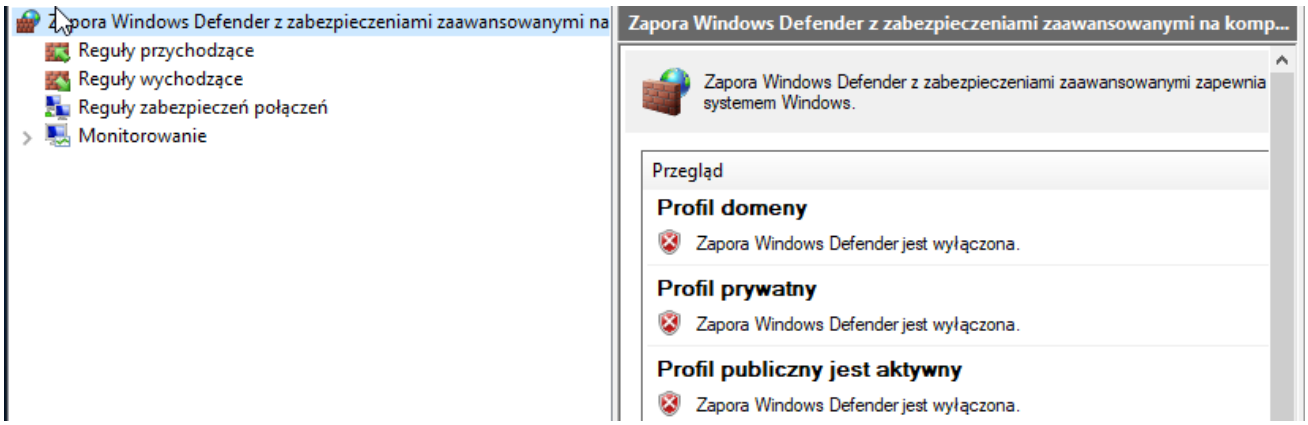


12. Na serwerze wkonaj gpupdate /force w celu odświeżenia zasad

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

13. Na kliencie 10ce zaloguj się do konta lokalnego Admin bez hasła i wyłącz zapory (login: .\Admin hasło: zaq1@WSX) .

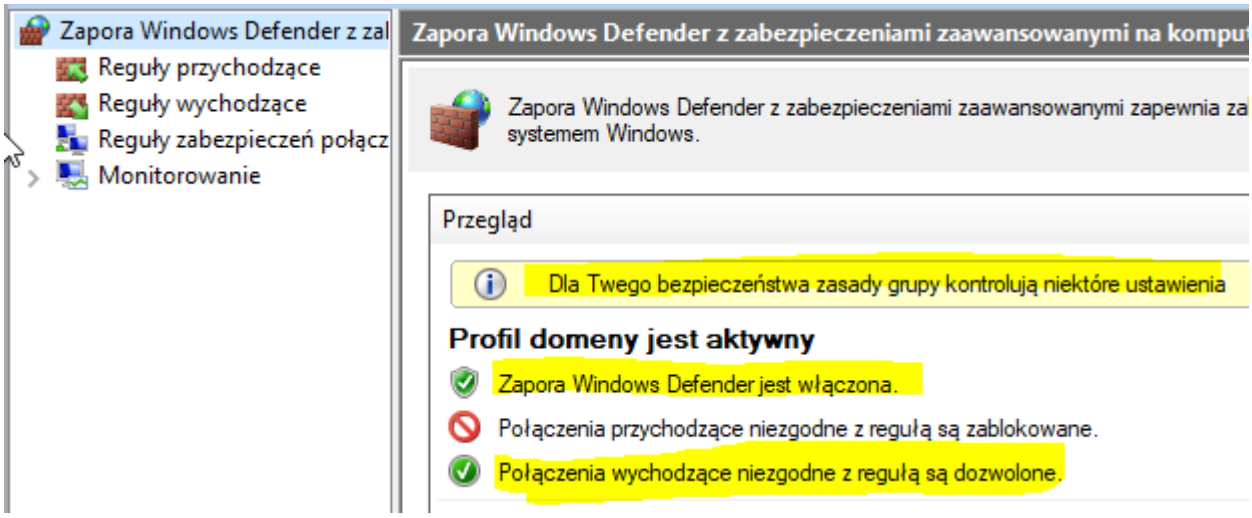


14. Wyloguj się z konta lokalnego Admin i zaloguj do domenowego konta IS\Administrator
15. Na kliencie 10ce wkonaj gpupdate /force w celu odświeżenia zasad

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Oczekiwany efekt:



Zapisz w zeszycie, kiedy należy stosować powyższe ustawienie.

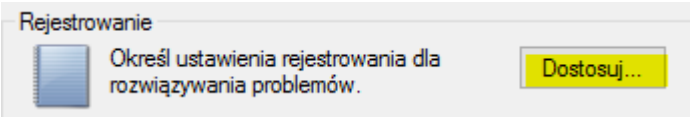
Poproś o sprawdzenie wykonanych czynności – zgłoszenie 3.

Zadanie 4 Włączanie rejestrowania dla Windows Firewall

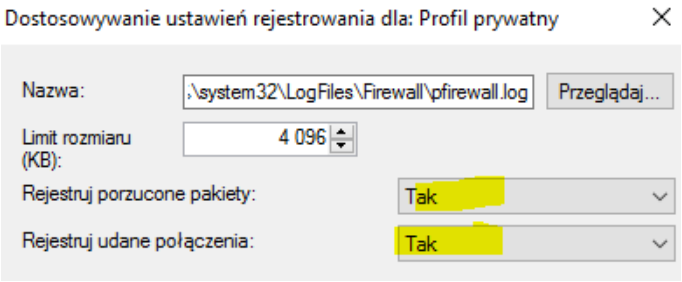
Wykonaj następujące kroki, aby włączyć rejestrowanie:

1. W drzewie konsoli przystawki Windows Firewall With Advanced Security (Zapora systemu Windows z zabezpieczeniami zaawansowanymi) kliknij prawym przyciskiem myszy Windows Firewall With Advanced Security (Zapora systemu Windows z zabezpieczeniami zaawansowanymi), a następnie wywołaj Propcrties (Właściwosci). Pojawi się okno dialogowe Windows Firewall With Advanced Security Properties (Zapora systemu Windows z zaawansowanymi właściwości zabezpieczeń).

2. Wybierz kartę Domain Profile (Profil domeny), Private Profile (Profil prywatny) lub Public Profile (Profil publiczny).
3. Kliknij przycisk Customize (Dostosuj) w grupie Logging (Rejestrowanie).



4. Pojawi się okno dialogowe Customize Logging Settings (Dostosowywanie ustawień rejestrowania).
5. Z listy rozwijanej Log Dropped Packets (Rejestruj porzucone pakiety) wybierz Yes (Tak), aby rejestrować pakiety, które Windows Firewall odrzuca. Z listy rozwijanej Log Successful Connections (Rejestruj udane połączenia) wybierz Yes (Tak), aby rejestrować połączenia, na jakie Windows Firewall pozwala.



6. Kliknij OK.

Domyślnie Windows Firewall zapisuje wpisy dziennika w pliku %SystemRoot%\System32\LogFies\Firewall\Pfirewall.log i przechowuje tylko ostatnie 4 KB danych. W większości środowisk produkcyjnych ten dziennik będzie prawie cały czas zapisywany, co może mieć wpływ na wydajność. Z tego powodu powinno się włączać rejestrowanie tylko wtedy, gdy aktywnie rozwiązujemy problem.
Poproś o obserwację wykonywanych czynności. Pokaż konfiguracje. Po zakończeniu natychmiast należy wyłącz rejestrowanie. (koniec obserwacji)

Zapisz w zeszycie, kiedy należy stosować powyższe ustawienie.

Poproś o sprawdzenie wykonanych czynności – zgłoszenie 4.

Zadanie 5 Identyfikacja komunikacji sieciowej

Po uruchomieniu aplikacji *netstat* należy wykonaj następujące polecenie, aby wyznaczyć porty nasłuchujące aktywnych połączeń:

netstat -a –b | more

Podczas zajęć w zeszycie wyjaśnij dwa wybrane połączenia inne niż w przykładzie poniżej.

Informacja jak czytać wynik powyższego polecenia z przykładem.

Wiersze w danych wyjściowych zawierające w kolumnie State (Stan) wpis LISTENING (NASŁUCHIWANIE) odpowiadają próbie odbioru przychodzącego połączenia w porcie określonym w kolumnie Local Address (Adres lokalny). Nazwa pliku wykonywalnego wymieniona za tym wierszem to program, który nasłuchuje tego połączenia. Na przykład następujące wyjście demonstruje, że RpcSs,

działające pod kontrolą procesu SvcHost.exe (który uruchamia wiele usług), nasłuchuje połączeń na porcie TCP 135:

Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 Dcsrv1:0 LISTENING
RpcSs
[svchost .exel

Podobnie następujące wyjście demonstruje, że usługa DNS (Dns.exe) nasłuchuje połączeń na porcie TCP 531

Active Connectlons
Proto Local Address Foreign Address State
TCP 0.0.6.0:63 Dcsrv1: LISTENING
[dns . exe]

Windows Firewall zawiera już reguły dla tych usług (ponieważ są wbudowane w Windows), ta sama technika pozwala zidentyfikować numery portów używanych przez aplikacje firm trzecich, co można zaobserwować na zajęciach „Metody ataków sieciowych".

Zapisz w zeszycie, kiedy należy wykonać powyższe czynności.

Poproś o sprawdzenie wykonanych czynności – zgłoszenie 5.

Zadanie 6 Podaj i uzasadnij odpowiedz na pytania do lekcji „Konfiguracja firewall w Windows Server 2019" zawarte w pliku „cw Pytania do lekcji".
Poproś o sprawdzenie wykonanych czynności – zgłoszenie 6.

Przywróć pierwszy punkt kontrolny

Podsumowanie:
Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.