

T: Konfiguracja firewall w Windows Server 2019

Cel ogólny lekcji: Nauczenie się konfigurowania zapory sieciowej w systemie Windows Server 2019 z zaawansowanymi zabezpieczeniami, włączając w to filtrowanie ruchu przychodzącego i wychodzącego oraz tworzenie niestandardowych reguł.

Cele szczegółowe lekcji:

1. Zrozumienie podstawowych ustawień zapory systemu Windows i dostępnych profili.
2. Umożliwienie konfiguracji filtrów wchodzących i wychodzących.
3. Włączenie filtrowania wychodzącego i włączenie filtrowania na wyjściu.
4. Umiejętność tworzenia niestandardowych reguł zapory.
5. Poznanie procedur konfiguracji zapory w systemie Windows Server 2019 za pomocą interfejsu GUI oraz programu PowerShell.

Ćwiczenie 1

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienia

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

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

- maszyny wirtualnej z plikiem startowym serwera **dc** są jak poniżej:

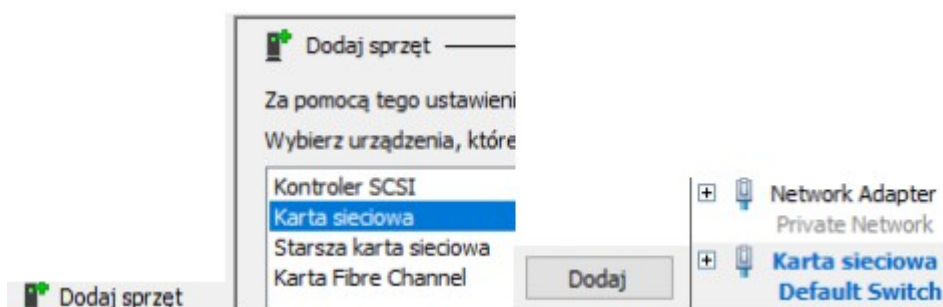


Sieć

Karta 1: Intel PRO/1000 MT Desktop (Sieć wewnętrzna, 'intnet')

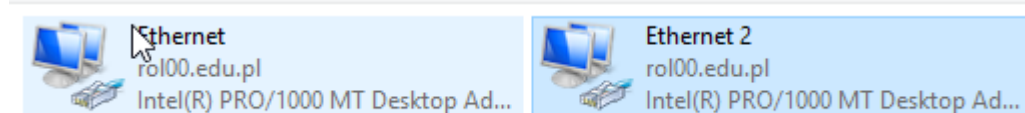
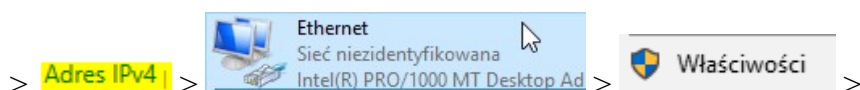
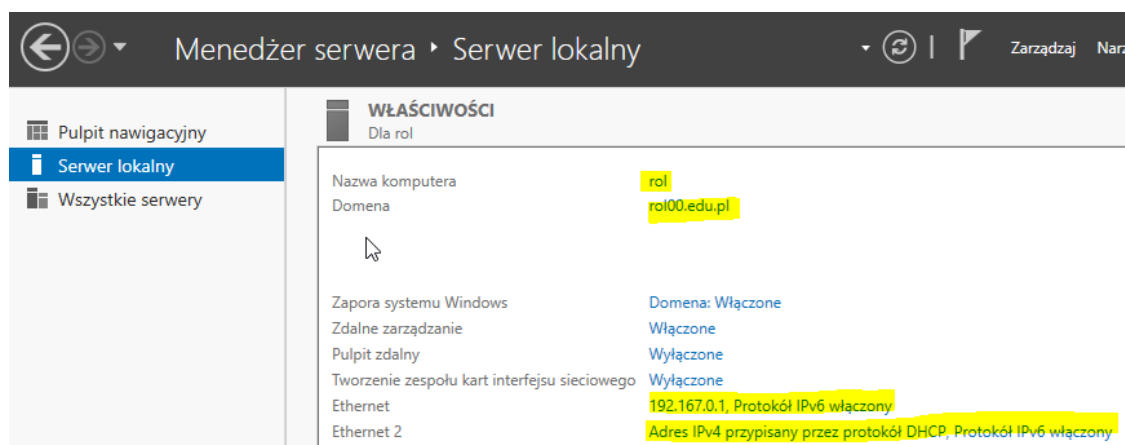
VirtualBox: Karta 2: Intel PRO/1000 MT Desktop (NAT)

Hyper-V:



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

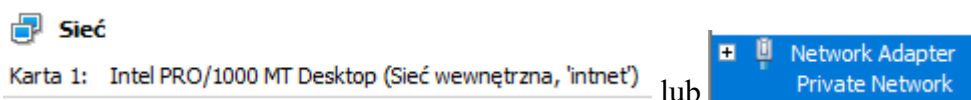
- system serwera są jak poniżej:



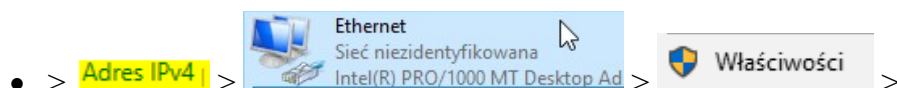
DHCP włączone		Nie	Opis	Microsoft Hyper-V I
Adres IPv4		192.167.0.1	Adres fizyczny	00-15-5D-07-2E-36
Maska podsieci IPv4		255.255.255.0	DHCP włączone	Tak
Brama domyślna IPv4			Adres IPv4	172.27.131.227
Serwer DNS IPv4		192.167.0.1	Maska podsieci IPv4	255.255.240.0
			Dzierżawa uzyskana	wtorek, 3 stycznia 2016
			Dzierżawa wygasa	środa, 4 stycznia 2016
			Brama domyślna IPv4	172.27.128.1
			Serwer DHCP IPv4	172.27.128.1
			Serwer DNS IPv4	172.27.128.1

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

- Klienta (Windows 10) jak poniżej:



Podaj login: admin > i hasło: zaq1@WSX



ip - 192.167.0.21/24; brama - 192.167.0.1; serwer dns - 192.167.0.1;

Klient (Windows 10) nie podłączony do domeny, będzie podłączany w czasie lekcji.

Po ukończeniu tej lekcji będziesz umiał:

- Utworzyć regułę zapory i zezwolić na ruch przychodzący.
- Utworzyć regułę zapory, pozwolić na ruch wychodzący i włączyć filtrowanie na wyjściu.

W tym zadaniu skonfigurujemy filtrowanie wejściowe i wyjściowe. Są to zadania wykonywane podczas instalowania nowych aplikacji w prawie każdym środowisku sieciowym, od małych firm do dużych przedsiębiorstw.

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

W systemie Windows Server 2019 Zapora systemu Windows jest domyślnie włączona. Umożliwia to cały ruch wychodzący do dowolnego miejsca docelowego lub portu, ale ogranicza ruch przychodzący na podstawie określonych reguł. Omówimy, jak skonfigurować Zaporę systemu Windows z Zaawansowanymi zabezpieczeniami, pokazując, jak otworzyć ją za pomocą interfejsu GUI i programu PowerShell, a następnie demonstrację, jak utworzyć niestandardową regułę zapory.

Zadanie 1 Konfiguracja filtrowania ruchu przychodzącego

Podstawowe ustawienia zapory systemu Windows można zmodyfikować, jak pokazano poniżej.

Dostęp do tego interfejsu można również uzyskać za pomocą programu PowerShell lub wiersza polecenia, wpisując „firewall.cpl”.

Stąd możemy graficznie przeglądać status zapory sieciowej dla profili domeny, prywatnego i publicznego. Te różne profile są używane w zależności od bieżącego połączenia sieciowego. Na przykład, jeśli jesteś przyłączony do domeny Active Directory, zostaną zastosowane reguły zastosowane w profilu domeny, a jeśli jesteś podłączony do publicznej sieci bezprzewodowej, zostaną użyte ustawienia w profilu publicznym.

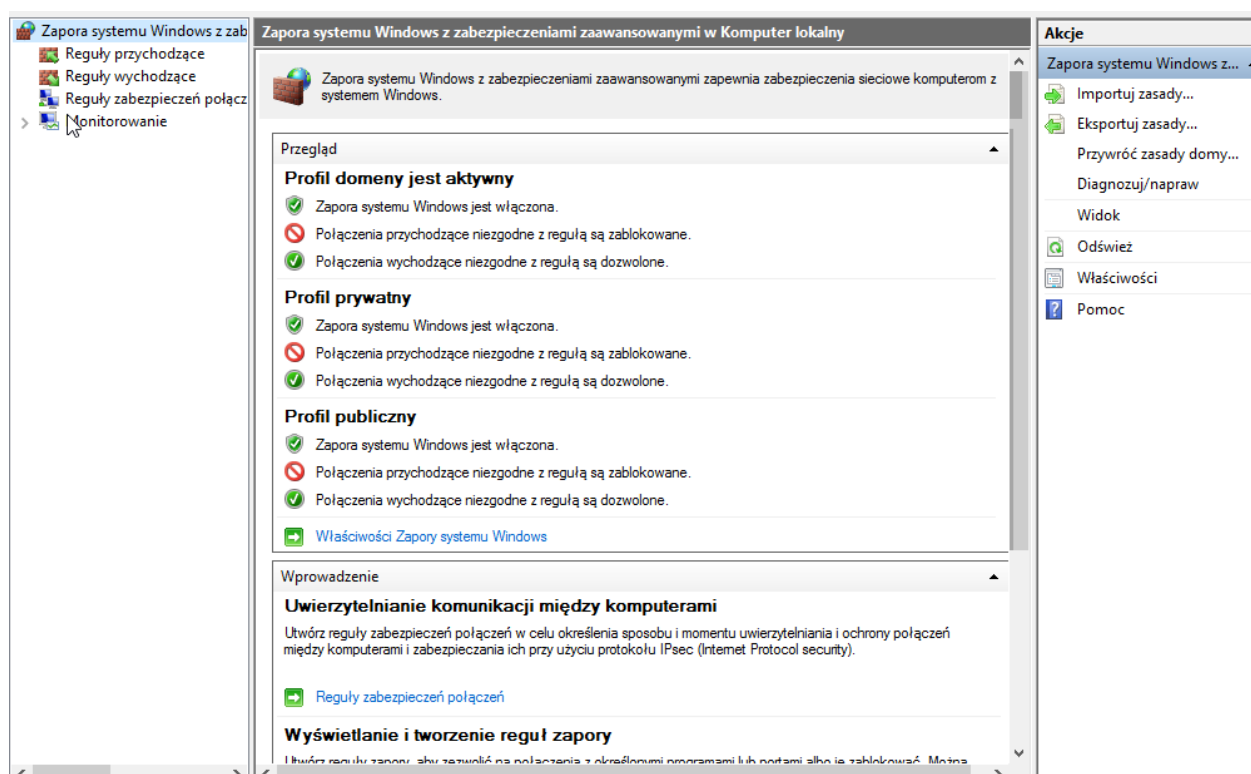
W tym przykładzie widzimy, że profil domeny jest wymieniony jako połączony, ponieważ obecnie jesteśmy połączeni z domeną example.com.

Zadania, które można tutaj wykonać, są pokazane w menu po lewej stronie, nie wchodzimy tutaj w szczegóły, ponieważ zajmiemy się głównie ustawieniami zaawansowanymi. Aby uzyskać dostęp do

ustawień zaawansowanych, możesz wybrać łącznie ustawień zaawansowanych z tego menu po lewej stronie w Zaporze systemu Windows.

Zapora systemu Windows z zaawansowanymi zabezpieczeniami

Jak wspomniano powyżej, możemy otworzyć Zaporę systemu Windows z zabezpieczeniami zaawansowanymi, klikając przycisk ustawień zaawansowanych w Zaporze systemu Windows. Możemy również uruchomić „wf.msc” w PowerShell lub wierszu polecenia, aby bezpośrednio otworzyć zaawansowany interfejs bezpieczeństwa. Poniższy obraz przedstawia zaawansowany interfejs bezpieczeństwa po otwarciu.

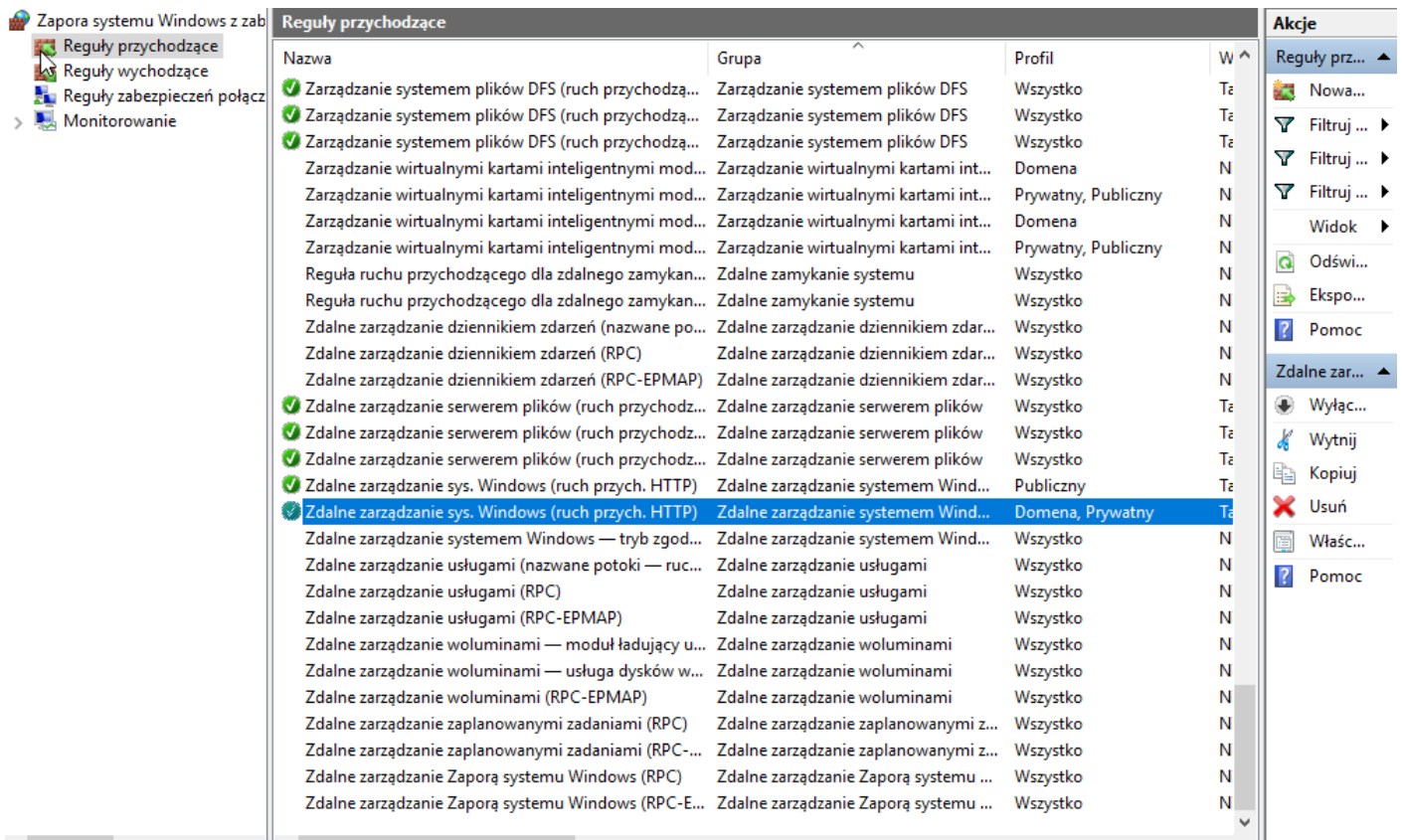


W tym oknie możemy zobaczyć przegląd domen, profili prywatnych i publicznych, które domyślnie powinny być włączone i blokować ruch przychodzący oraz zezwalać na ruch wychodzący.

Z menu po lewej stronie możemy wybrać reguły przychodzące lub wychodzące.

Ponieważ wszystkie wychodzące są domyślnie dozwolone, skupimy się tutaj na regułach przychodzących. Reguły bezpieczeństwa połączeń można również skonfigurować do konfigurowania połączeń IPsec, a monitorowania można używać do rejestrowania różnych zdarzeń zapory.

W ramach reguł ruchu przychodzącego i wychodzącego możemy zobaczyć reguły, które istnieją i które są obecnie włączone. Te reguły są domyślnie dostępne, reguły z zieloną ikoną zaznaczenia po lewej stronie są włączone i zezwalają na ruch, podczas gdy reguły bez ikony są wyłączone.



Wyłączoną regułę można włączyć, klikając ją prawym przyciskiem myszy i wybierając opcję Włącz. Podobnie możemy kliknąć prawym przyciskiem myszy włączoną regułę i zmienić ją na wyłączoną. Możemy wyświetlić właściwości reguły, klikając ją prawym przyciskiem myszy i wybierając właściwości. Pozwoli ci to zobaczyć, co faktycznie robi reguła, w tym porty, które są dozwolone przez zaporę ogniową do określonych programów, zobaczymy to bardziej szczegółowo, kiedy tworzymy własną regułę.

Poproś o sprawdzenie wykonanych czynności - zgłoszenie 1.

Utwórz regułę zapory

Wybierz Reguły ruchu przychodzącego z menu po lewej stronie, a następnie wybierz Nowa reguła z panelu akcji po prawej stronie. Spowoduje to otwarcie nowego kreatora reguł ruchu przychodzącego. Stąd możemy wybrać, czy chcemy utworzyć regułę dla określonego programu, do określonego portu, czy na podstawie istniejącej reguły. W takim przypadku wybierzemy niestandardowy, ponieważ daje nam to największy wybór.

Typ reguły

Wybierz typ reguły zapory do utworzenia.

Kroki:

- Typ reguły
- Program
- Protokół i porty
- Zakres
- Akcja
- Profil
- Nazwa

Regułę jakiego typu chcesz utworzyć?

☐ **Program**
Reguła sterująca połączeniami dla programu.

☐ **Port**
Reguła sterująca połączeniami dla portu TCP lub UDP.

☐ **Upřednio zdefiniowana:**
Administracja zdalna modelu COM+
Reguła sterująca połączeniami na komputerze z systemem Windows.

☒ **Niestandardowa**
Reguła niestandardowa.

< Wstecz **Dalej >** Anuluj

Na następnym ekranie możemy wybrać konkretny program lub usługę, dla których zapora powinna zezwalać na ruch. W takim przypadku wybieramy tylko wszystkie programy, jednak należy pamiętać, że można to wykorzystać do dalszego blokowania reguły, zamiast po prostu zezwalać na podstawie adresu portu / IP, możemy również zezwolić na ruch tylko do określonego programu.

Program

Określ pełną ścieżkę i nazwę pliku wykonywalnego programu, którego dotyczy ta reguła.

Kroki:

- Typ reguły
- Program
- Protokół i porty
- Zakres
- Akcja
- Profil
- Nazwa

Czy ta reguła dotyczy wszystkich programów, czy określonego programu?

☒ **Wszystkie programy**
Reguła dotyczy wszystkich połączeń na komputerze, które pasują do właściwości innych reguł.

☐ **Ta ścieżka programu:**

Przeglądaj...

Przykład: c:\ścieżka\program.exe
%ProgramFiles%\przeglądarka\przeglądarka.exe

Usługi
Określ usługi, których dotyczy ta reguła.
Dostosuj...

Następnie możemy wybrać port i protokół, do których reguła powinna się stosować. Istnieje wiele różnych protokołów do wyboru z listy rozwijanej, w tym przykładzie określamy, że lokalny port TCP 9000 powinien być dopuszczony przez zaporę ogniową. Używamy tutaj portu lokalnego, ponieważ port 9000 jest dostępny lokalnie na tym serwerze i nasłuchuje połączeń.

Protokół i porty

Określ protokoły i porty, których dotyczy ta reguła.

Których protokołów i portów dotyczy ta reguła?

Typ protokołu: TCP

Numer protokołu: 6

Port lokalny: Określone porty

9000

Przykład: 80, 443, 5000-5010

Port zdalny: Wszystkie porty

Przykład: 80, 443, 5000-5010

Ustawienia protokołu komunikacyjnego sterowania Internetem (ICMP):

Dostosuj...

Teraz możemy wybrać adres IP lub zakres adresów, które są dozwolone w naszej regule zapory.

W tym przypadku zezwalam na wprowadzenie zdalnego zakresu adresów 192.168.0.0/24 przez zaporę, więc tylko ten zakres IP będzie mógł łączyć się z serwerem na porcie TCP 9000.

Zakres

Określ lokalne i zdalne adresy IP, których dotyczy ta reguła.

Których lokalnych adresów IP dotyczy ta reguła?

☒ Dowolny adres IP

☐ Te adresy IP:

Dostosuj typy interfejsów, których dotyczy ta reguła:

Których zdalnych adresów IP dotyczy ta reguła?

☐ Dowolny adres IP

☒ Te adresy IP:

192.167.0.0/24

W tym momencie określamy czy chcemy zezwolić, czy odrzucić regułę, którą tworzymy, pozostawimy tę opcję dozwoloną, ponieważ chcemy pozwolić 192.168.0.0/24 na porcie TCP 9000, jednak opcjonalnie możemy to jawnie zablokować zamiast. Opcjonalnie możemy zezwolić na połączenie tylko wtedy, gdy jest bezpieczne, co zależy od konfiguracji IPSec.

Akcja

Określ akcję do wykonania w przypadku, gdy połączenie spełnia warunki określone w regule.

Kroki:

- Typ reguły
- Program
- Protokół i porty
- Zakres
- Akcja**
- Profil
- Nazwa

Jaką akcję należy wykonać, gdy połączenie spełnia określone warunki?

☒ **Zezwalaj na połączenie**
Obejmuje połączenia chronione za pomocą protokołu IPSec, jak i połączenia niechronione.

☐ **Zezwalaj na połączenie, jeśli jest bezpieczne**
Obejmuje tylko połączenia uwierzytelnione przy użyciu protokołu IPSec. Połączenia będą zabezpieczone przy użyciu ustawień określonych we właściwościach protokołu IPSec i reguł zawartych w węźle Reguła zabezpieczeń połączenia.

☐ **Zablokuj połączenie**

Dostosuj...

Możemy wybrać profile zapory, których dotyczy nasza nowa reguła.

Domyślnie wybrane są wszystkie profile, ale można to zmienić zgodnie z własnymi wymaganiami.

Profil

Określ profile, których dotyczy ta reguła.

Kroki:

- Typ reguły
- Program
- Protokół i porty
- Zakres
- Akcja
- Profil**
- Nazwa

Kiedy ma zastosowanie ta reguła?

☒ **Domena**
Ma zastosowanie, gdy komputer jest połączony ze swoją domeną firmową.

☒ **Prywatny**
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci prywatnej, na przykład w domu lub w miejscu pracy.

☒ **Publiczny**
Ma zastosowanie, gdy komputer jest połączony z lokalizacją w sieci publicznej.

Możemy podać nazwę i opcjonalny opis, aby zidentyfikować naszą regułę. Po zakończeniu kliknij przycisk Zakończ, zauważając, że jak tylko to zrobisz, reguła będzie aktywna zgodnie z tym, jak ją skonfigurowałeś.

Nazwa

Określ nazwę i opis tej reguły.

Kroki:

- Typ reguły
- Program
- Protokół i porty
- Zakres
- Akcja
- Profil
- Nazwa**

Nazwa:
nasza zasada

Opis (opcjonalnie):
opisz naszą zasadę

Nasza nowa reguła będzie teraz wyświetlana na górze listy reguł przychodzących ponad wszystkimi regułami domyślnymi. Możemy go zidentyfikować po nazwie i krótko zobaczyć, co robi, pozwala to zakresowi zdalnego adresu 192.168.0.0/24 na komunikację na port lokalny 9000 z protokołem TCP na wszystkich profilach i jest włączony.

Zapora systemu Windows z zaawansowanymi zabezpieczeniami	Reguły przychodzące									Akcje
	Nazwa	Grupa	Profil	Włącz...	Akcja	Zastęp	Progr...	Adres lokalny	Adres zdalny	
Reguły przychodzące	nasza zasada		Wszystko	Tak	Zezwa...	Nie	Dowo...	Dowolne	192.167.0.0/24	Reguły prz...
Reguły wychodzące	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Nowa...
Reguły zabezpieczeń połączeń	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Filtruj ...
Monitorowanie	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Filtruj ...
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Filtruj ...
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Widok
	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Odświ...
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Ekspo...
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Pomoc
	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	nasza zasa...
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Wyłąc...
	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Wytnij
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Kopiu...
	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Usuń
	✓ Odnajdowanie si...	Odnajdowa...	Domena, ...	Nie	Zezwa...	Nie	System	Dowolne	Dowolne	Właśc...
	✓ Odnajdowanie si...	Odnajdowa...	Prywatny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	Pomoc
	✓ Odnajdywanie S...	Funkcjonal...	Publiczny	Tak	Zezwa...	Nie	System	Dowolne	Dowolne	

Tworząc niestandardowe reguły zapory, takie jak ta, możemy pomyślnie skonfigurować zaporę systemu Windows z zaawansowanymi zabezpieczeniami.

Możemy skonfigurować bardzo podstawowe reguły zapory za pomocą Zapory systemu Windows, jednak Zapora systemu Windows z zaawansowanymi zabezpieczeniami służy do tworzenia znacznie więcej niestandardowych i szczegółowych reguł, jak widzieliśmy tutaj.

Jeśli reguła programu zezwala na cały adres IP, ale blokuje określony adres. Czy odmowa blokuje pierwszą zasadę?

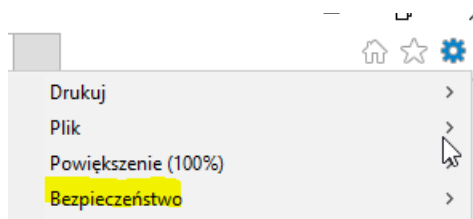
Odmowa powinna być na pierwszym miejscu przed zezwoleniem.

Poproś o sprawdzenie wykonanych czynności - zgłoszenie 2.

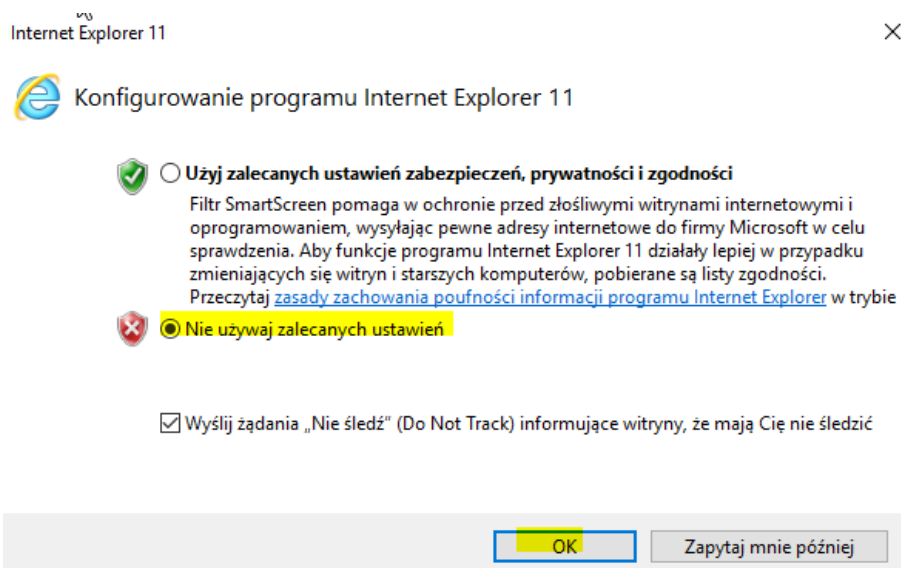
Zadanie 2 Konfigurowanie filtrowania ruchu wychodzącego

W tym ćwiczeniu skonfigurujesz Windows Server 2019, aby domyślnie blokował wychodzące żądania. Następnie przetestujesz to, próbując odwiedzić witrynę WWW przy pomocy Internet Explorer. Później utworzysz wyjściową regułę zezwalającą na żądania od Internet Explorer i zweryfikujesz, że wyjściowa reguła działa poprawnie. W końcu przywrócisz komputer do pierwotnego stanu.

1. Konfiguruj zwiększone zabezpieczenia programu Internet Explorer.



2. Wyłącz:



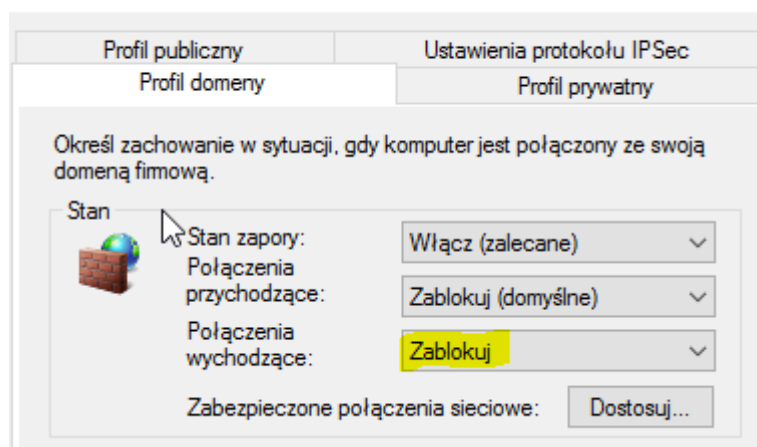
3. Otwórz Internet Explorer i odwiedź <http://www.microsoft.com>. Jeżeli się pojawi okno dialogowe Internet Explorer Enhanced Security Configuration, kliknij Close, aby je odrzucić.

(Nie powinno się pojawić, jeśli wykonałeś/aś pkt2.)

4. Wybierz Configuration\Windows Firewall With Advanced Security (Konfiguracja\Zapora systemu Windows z zabezpieczeniami zaawansowanymi) i kliknij prawym przyciskiem myszy, a następnie wybierz Properties (Właściwości).

5. Kliknij kartę Domain Profile (Profil domeny). Z listy rozwijanej Outbound Connections (Połączenia wychodzące) wybierz Block (Zablokuj).

Właściwości: Zapora systemu Windows z zabezpieczeniami zaawa... >



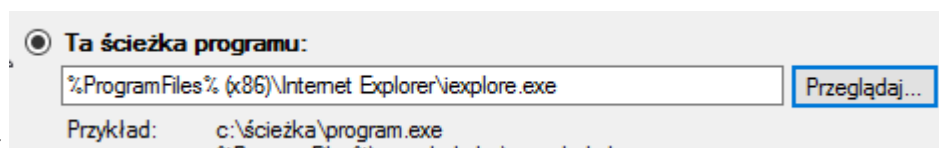
Powtórz ten krok dla kart Private Profile (Profil prywatny) i Public Profile (Profil publiczny).

6. Kliknij OK.
7. Otwórz Internet Explorer i spróbuj odwiedzić <http://support.microsoft.com>.
8. Próba powinna zakończyć się niepowodzeniem, ponieważ wyjściowy filtr blokuje wychodzące żądania HTTP programu Internet Explorer.

Poproś o sprawdzenie wykonanych czynności - zgłoszenie 1.

9. W Windows Firewall With Advanced Security kliknij prawym przyciskiem myszy Outbound Rules (Reguły wychodzące), a następnie wybierz New Rule (Nowa reguła). Pojawi się New Outbound Rule Wizard **Kreator nowej reguły ruchu wychodzącego**.

10. Na stronie Rule Type (Typ Reguły) wybierz Program. Następnie kliknij Dalej.

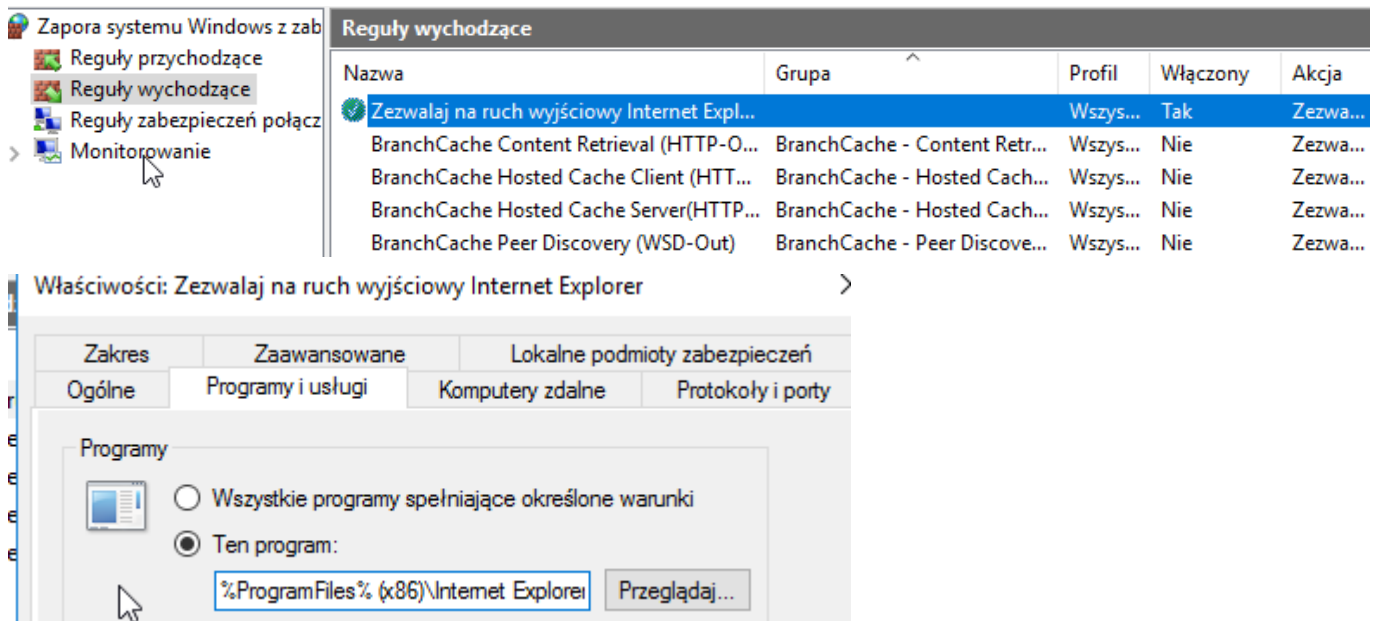


11. Na stronie Program wybierz

W polu wpisz **%ProgramFiles%(x86)\Internet Explorer\iexplore.exe** (ścieżka do pliku wykonalnego Internet Explorer). Kliknij Dalej.

Uwaga: sprawdź ścieżkę do pliku wykonalnego Internet Explorer i podaj aktualną.

12. Na stronie Action (Akcja) wybierz Allow The Connection (Zezwalaj na połączenie). Następnie kliknij Dalej.
13. Na stronie Profile zaakceptuj domyślny wybór zastosowania tej reguły do wszystkich trzech profili. Kliknij Dalej.
14. Na stronie Name (Nazwa) wpisz Zezwalaj na ruch wyjściowy Internet Explorer. Następnie kliknij Zakończ.



15. Teraz w Internet Explorer spróbuj odwiedzić znowu <http://support.microsoft.com>. Tym razem połączenie powinno się udać, ponieważ utworzyliśmy wyjściowy filtr specjalnie dla programu Internet Explorer.

Poproś o sprawdzenie wykonanych czynności - zgłoszenie 2.

16. Wyłącz filtrowanie wyjściowe, klikając prawym przyciskiem myszy Windows Firewall With Advanced Security, a następnie wybierając Properties. Na karcie Domain Profile kliknij listę Outbound Connections (Połączenia wychodzące), a potem Allow (Default) (Zezwalaj (domyślne)). Powtórz ten krok na kartach Private Profile i Public Profile. Kliknij OK.

Poproś o sprawdzenie wykonanych czynności - zgłoszenie 3.

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 wykonanie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.