T: Konfiguracja firewall w Windows Server 2016.

Sieci z samej natury mogą pozwalać na sytuację, gdy komputery o dobrej kondycji komunikują się z komputerami niewłaściwie skonfigurowanymi a także na atakowanie legalnych aplikacji przez złośliwe narzędzia.

Windows Server 2016 ma zaporę ogniową o nazwie „Zapora systemu Windows z zaawansowanymi zabezpieczeniami".

System Windows Server 2016 jest instalowany z Zaporą systemu Windows, a zaawansowane zabezpieczenia są już zainstalowane i skonfigurowane. Domyślna konfiguracja zezwala na cały ruch i ogranicza ruch przychodzący.

Zapora ogniowa jest jedną z zasad bezpieczeństwa wymaganych do działania serwera lub sieci. Zapora systemu Windows z zaawansowanymi zabezpieczeniami zmniejsza ryzyko zagrożeń bezpieczeństwa i chroni dane. Oprogramowanie zabezpieczające innej firmy może zostać wdrożone na serwerze, a zapora serwera może być wyłączona lub niektóre z jej funkcji wyłączone.

Dostęp do zapory

Dostęp do aplikacji zapory w Server 2016 można uzyskać:

- z wiersza polecenia: wpisz „wf.msc"
- w interfejsie Windows: kliknij Wyszukaj i wpisz „Zapora systemu Windows" i wybierz „Zapora systemu Windows z zaawansowanymi zabezpieczeniami"
- MMC: Dodaj przystawkę do „Zapory systemu Windows z zaawansowanymi zabezpieczeniami" i stamtąd uzyskaj dostęp do zdalnego serwera

Konfigurowanie Windows Firewall

Windows Firewall filtruje ruch przychodzący w celu zablokowania niechcianego ruchu sieciowego. Opcjonalnie Windows Firewall może także filtrować ruch, aby pomóc w ograniczaniu ryzyka związanego ze szkodliwym oprogramowaniem. Domyślne ustawienia Windows Firewall będą działać dobrze z składnikami wbudowanymi w Windows, mogą uniemożliwiać prawidłowe funkcjonowanie innym aplikacjom. Można także znacznie poprawić domyślne ustawienia Windows Firewall, aby zapewnić jeszcze silniejsza ochronę wymagającą autoryzacji lub ograniczając zakres dozwolonych połączeń.

Dlaczego zapory są ważne

Zapory (firewalls) analizują komunikację i odrzucają pakiety, które nie zostały dopuszczone. Łączenie się z Internetem oznacza, że dowolny z milionów innych połączonych z Internetem komputerów może nas zaatakować.
Celem zapory jest odrzucenie niechcianego ruchu, takiego jak ruch od robaków, przy równoczesnym zezwoleniu na legalny ruch, taki jak autoryzowane udostępnianie plików.
Im bardziej precyzyjnie używa się reguł zapory do identyfikacji legalnego ruchu, tym mniejsze będzie ryzyko ekspozycji na ruch niechciany.

Profile zapory

Zapora systemu Windows z zaawansowanymi zabezpieczeniami ma trzy profile dostępne dla użytkownika. Każdy może mieć inne zasady.

- Profil domeny: kontroluje ruch do sieci, która korzysta z tego samego kontrolera domeny, co administrowany serwer.
- Profil prywatny: kontroluje ruch z lokalnym serwerem lub siecią, która zazwyczaj znajduje się za urządzeniem NAT, takim jak sieci domowe lub małe firmy.
- Profil publiczny: kontroluje ruch do i ze wszystkich sieci innych niż sieci domen. W praktyce wpływa to na wszystkie bezpośrednie połączenia z publicznym Internetem.

Zwykle profil domeny ma mniej reguł niż publiczny, ponieważ zakłada się, że wszystkie komputery w sieci są uwierzytelnione.

Większość serwerów zawsze będzie połączonych ze środowiskiem domeny.

Przy konfigurowaniu serwera należy skonfigurować te same reguły zapory dla wszystkich trzech profili, aby zapewnić spójne działanie nawet wtedy, gdy kontroler domeny nie jest dostępny.

Zasady

Istnieją dwa zestawy reguł, które można zastosować: „przychodzące” i „wychodzące”.

Przy pierwszej instalacji będą już obowiązywały pewne zasady.

Reguły mogą być obecne, ale niekoniecznie włączone. Wszystkie aktywne (włączone) reguły mają zielony znaczek obok nich.

Filtrowanie ruchu przychodzącego

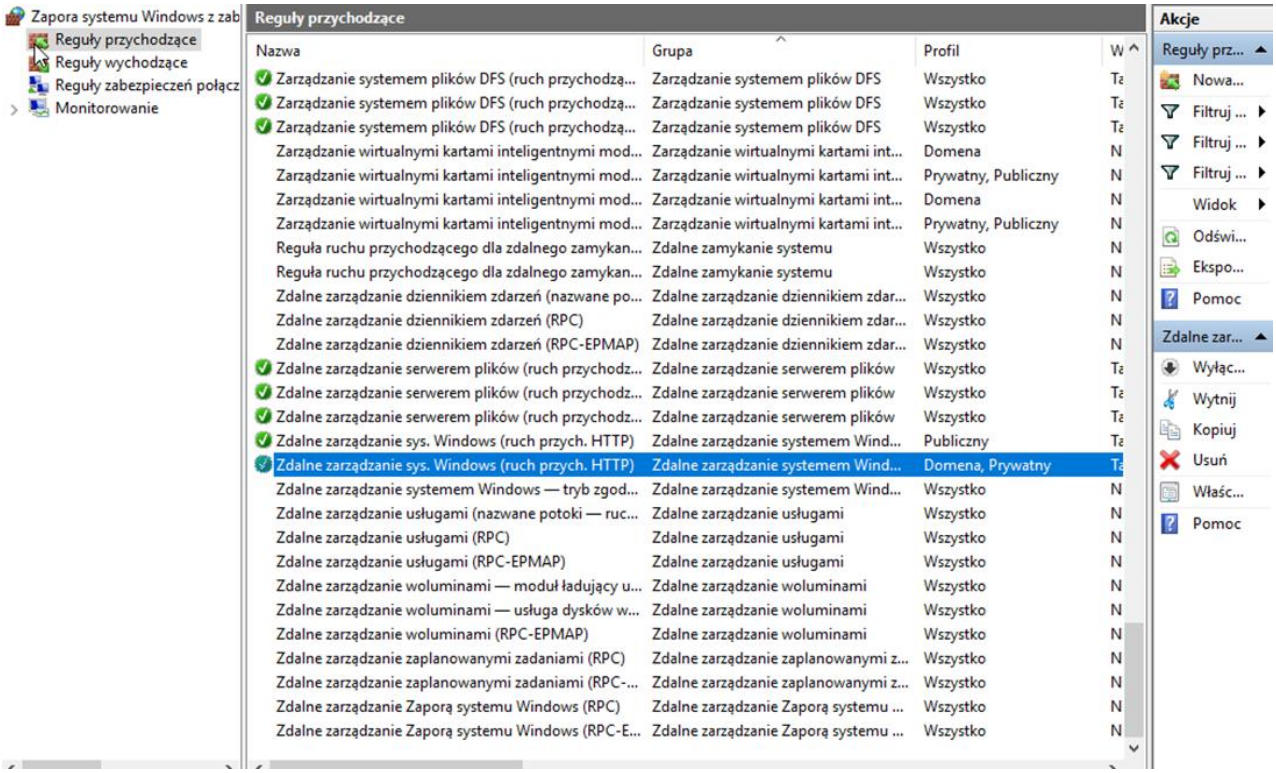
Zapora jest domyślnie skonfigurowana dla wygody, a nie maksymalnej ochrony. Microsoft skonfigurował zaporę, aby blokować wszystkie połączenia przychodzące i zezwalać na wszystkie połączenia wychodzące, z wyjątkiem tych, dla których reguły istnieją domyślnie.

Każdy program, dla którego nie istnieje reguła wychodząca, może wysyłać dane z komputera lokalnego do hostów w Internecie.

Jeżeli instalujemy lub włączamy właściwość Windows, która wymaga przychodzących połączeń, Windows będzie automatycznie włączał reguły zapory. Dlatego nie trzeba ręcznie modyfikować reguł zapory, rysunek 1 ukazuje domyślne reguły przychodzące dla komputera Windows Server 2016 skonfigurowanego jako kontroler domeny. Istnieją reguły zezwalające na każdy z protokołów wymagany przez kontroler domeny.

Jeżeli instalujemy aplikację, która nie włącza automatycznie reguł zapory, będziemy musieli tworzyć tę reguły ręcznie. Możemy utworzyć reguły zapory, używając samodzielnej konsoli Windows Firewall With Advanced Security lub możemy zastosować te reguły za pomocą zasad grupy, używając tego samego interfejsu umieszczonego w węźle Computer Configuration\Policies\Windows Settings\Sectirity Settings\Windows Firewall With

Advanced Security (Konfiguracja komputera\Zasady\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Zapora systemu Windows z zabezpieczeniami zaawansowanymi).



Rysunek 1 Domyślne reguły wejściowe zapory.

Reguły wejściowe przynoszą efekt natychmiast, pozwalając przychodzącym połączeniom na dopasowanie do określonych kryteriów.

Filtrowanie ruchu wychodzącego

Domyślnie Windows Firewall zezwala na dowolny ruch wychodzący. Zezwolenie na ruch wychodzący jest znacznie mniej ryzykowne niż zezwalanie na ruch przychodzący.

Ruch wychodzący nadal niesie pewne ryzyko:

- Jeżeli szkodliwe oprogramowanie zainfekuje komputer, może ono wysyłać ruch wychodzący zawierający poufne dane.
- Robaki i wirusy szukają możliwości replikacji. Jeżeli uda im się zainfekować komputer, będą próbowały wysyłać ruch wyjściowy w celu infekcji innych komputerów.
- Użytkownicy mogą używać niezatwierdzonych aplikacji do wysyłania danych do zasobów internetowych i świadomie lub nieświadomie transmitować poufne dane.

Domyślnie wszystkie wersje Windows (w tym Windows Server 2016) nie filtrują ruchu wychodzącego. Windows Server 2016 zawiera filtry wyjściowe dla głównych usług sieciowych, pozwalając na szybkie włączenie wyjściowego filtrowania przy zachowaniu podstawowej funkcjonalności sieci.

Domyślnie reguły wyjściowe są włączone dla:

- żądań DHCP (Dynamic Host Configuration Protocol),
- żądań DNS (Domain Names System),
- komunikacji Group Policy,
- IGMP (Internet Group Management Protocol,
- IPv6 i związanych z nim protokołów.

Blokowanie wyjściowej komunikacji domyślnie zablokuje możliwość komunikacji przez sieć dla wszystkich wbudowanych funkcji Windows i wszystkich aplikacji firm trzecich, które można zainstalować. Na przykład Windows Update nie będzie mogło już otrzymywać aktualizacji, system nie będzie w stanie aktywować się przez Internet, a komputer nie będzie mógł wysyłać alertów SNMP (Simple Network Management Protocol) – rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami takimi jak routery, przełączniki, komputery czy centrale telefoniczne za pośrednictwem sieci IP.

Jeżeli włączymy filtrowanie wyjściowe, musimy być przygotowani na testowanie każdej aplikacji, aby zweryfikować, że działa prawidłowo. Większość aplikacji nie jest przygotowanych do wspierania wyjściowego filtrowania i będzie wymagać identyfikowania reguł zapory, które muszą być utworzone, a następnie utworzyć te reguły.

Reguły wyjściowe dają efekt natychmiast, pozwalając wyjściowym pakietom na dopasowanie do określonych kryteriów.

Należy przeprowadzić wyczerpujące testy, aby upewnić się, że wymagane aplikacje działają prawidłowo, gdy wychodzące połączenia są blokowane domyślnie. To testowanie powinno objąć także procesy w tle, takie jak Automatic Updates.

Konfigurowanie zakresu zapory

Używając zakresu (scope) zapory, możemy pozwolić na połączenia z sieci wewnętrznej i blokować połączenia z sieci zewnętrznych. Może być to wykorzystane następująco:

- Serwer, który jest połączony z Internetem, może pozwalać komukolwiek z Internetu na łączenie się z publicznymi usługami (takimi jak serwer sieci Web), równocześnie pozwalając tylko użytkownikom w sieci wewnętrznej na dostęp do prywatnych usług (takich jak Remote Desktop).
- Serwery wewnętrzne mogą pozwalać na połączenia tylko ze specyficznych podsieci, które zawierają potencjalnych użytkowników. Planując takie ograniczenia zakresu pamiętajmy o uwzględnieniu podsieci dostępu zdalnego.
- Konfigurując połączenia wychodzące, możemy pozwolić aplikacji na łączenie się z serwerami tyko w specyficznych wewnętrznych podsieciach. Na przykład możemy pozwolić pułapkom SNMP na wysyłanie informacji tylko do naszych serwerów zarządzających. Podobnie można pozwolić aplikacją kopii zapasowej na kontaktowanie się tylko z serwerami kopii zapasowych.
- Komputery mobilne mogą pozwalać na pewną komunikację (taką jak Remote Desktop) tylko z podsieci, której używamy dla zarządzania.

Autoryzowanie połączeń

Jeżeli używamy zabezpieczeń IPsec w środowisku Active Directory, możemy także wymagać, aby zdalny komputer lub użytkownik był autoryzowany przed nawiązaniem połączenia.

Na przykład wyobraźmy sobie, że organizacja ma własną aplikację księgową, która używa portu TCP 1073, ale ta aplikacja nie ma żadnego mechanizmu kontroli dostępu - każdy użytkownik, który połączy się z usługą sieciową, może uzyskać dostęp do poufnych danych księgowych. Używając autoryzacji połączeń Windows Firewall, możemy ograniczyć przychodzące połączenia tylko do użytkowników należących do grupy Accounting - dodając kontrolę dostępu do aplikacji bez pisania żadnego dodatkowego kodu.

Większość aplikacji sieciowych jednak ma wbudowaną kontrolę dostępu. Autoryzacja połączeń za pomocą Windows Firewall może zapewnić dodatkową warstwę zabezpieczeń. Korzystanie z wielu warstw zabezpieczeń, techniki znanej jako defense in depth, redukuje ryzyko, zapewniając ochronę nawet wtedy, gdy jedna warstwa jest osłabiona.

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

Konfigurowanie ustawień zapory za pomocą zasad grupy

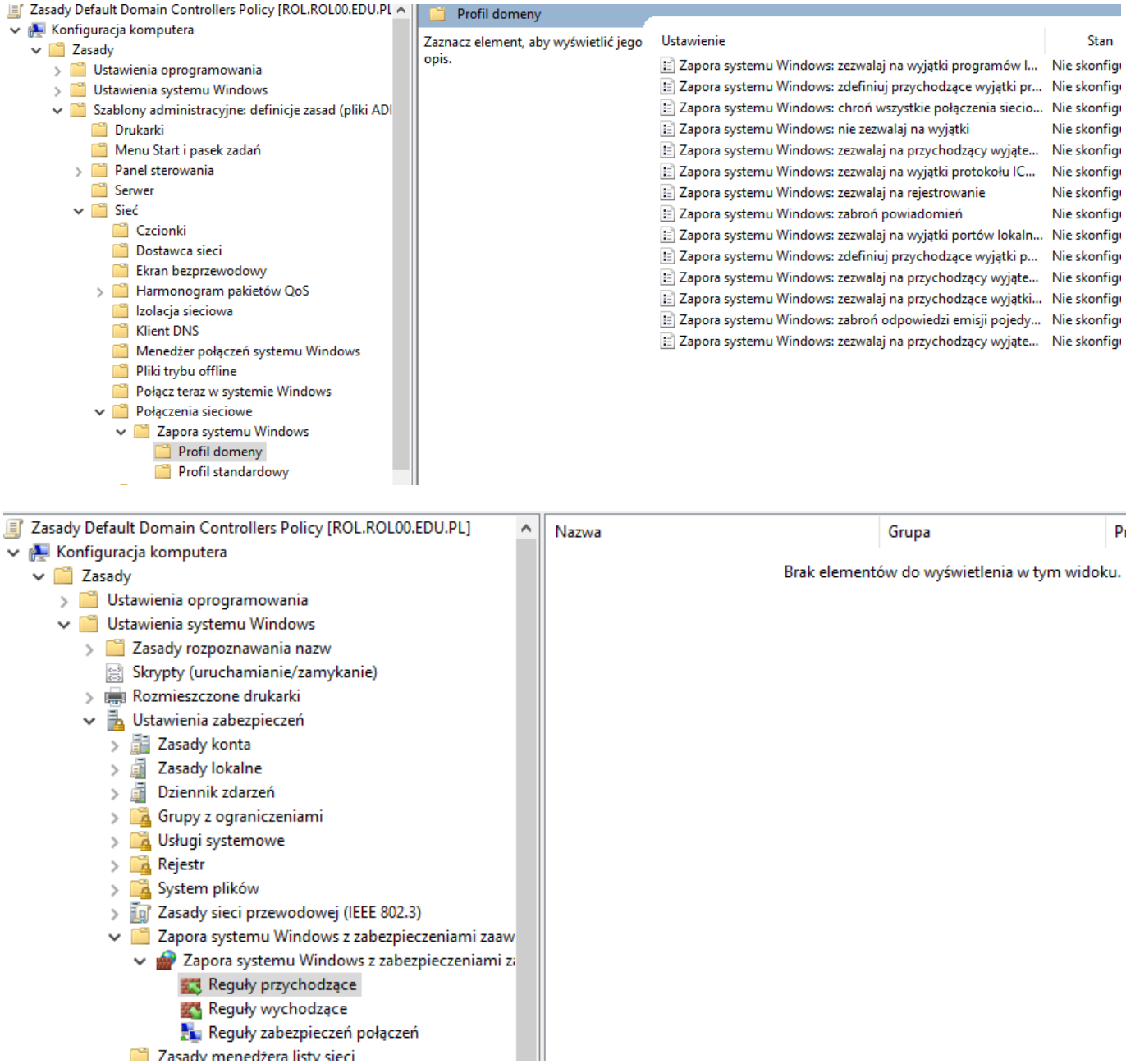
Można użyć zasad grupy do zarządzania ustawieniami Windows Firewall dla komputerów stosujących Windows Server 2016.

Aby otworzyć obiekt GPO w Zaporze systemu Windows Defender:

Otwórz konsolę zarządzania zasadami grupy.

W okienku nawigacji rozwiń Las: Nazwa lasu, rozwiń Domeny, rozwiń Nazwę domeny, rozwiń Obiekty zasad grupy, kliknij prawym przyciskiem myszy obiekt zasad grupy, który chcesz zmodyfikować, a następnie kliknij polecenie Edytuj.

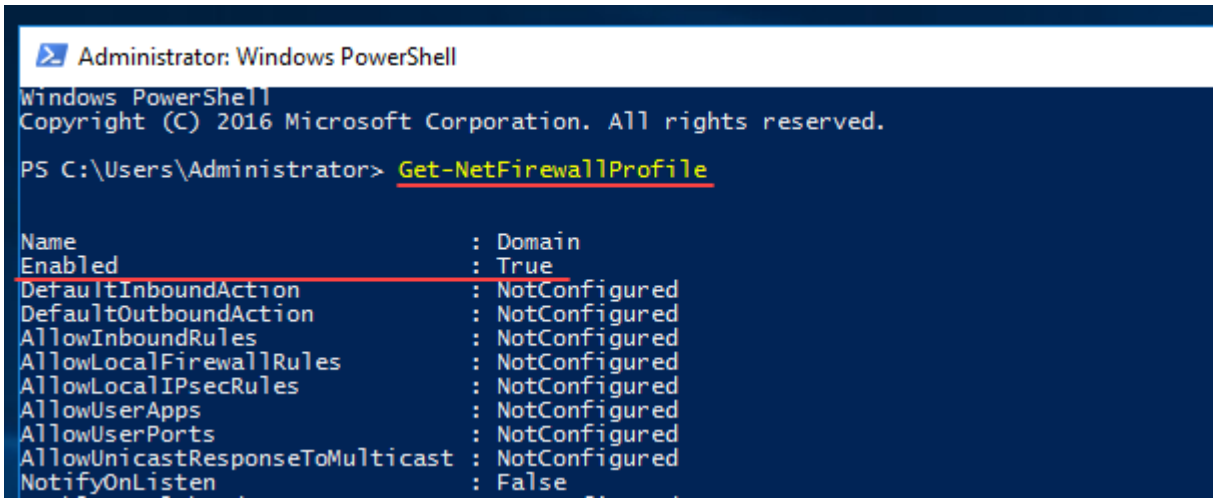
W okienku nawigacji Edytora obiektów zasad grupy przejdź do Konfiguracja komputera>Zasady Szablony administracyjne> Sieć> Połączenia sieciowe> Zapora systemu Windows Defender.



Wyłączanie oraz włączanie Zapory systemu Windows poleceniem PowerShell

Aktualny stan Zapory ogniowej na serwerze, wpisując następujące polecenie.

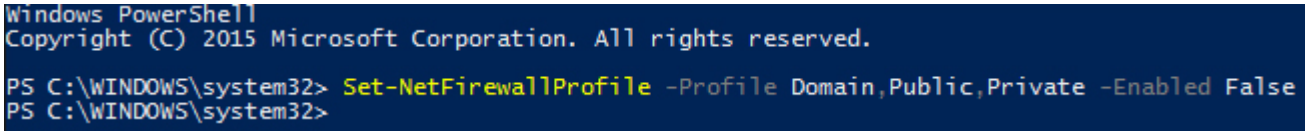
```
Get-NetFirewallProfile
```



Aby wyłączyć zaporę dla wszystkich typów sieci, uruchom następujące polecenie cmdlet.

Następnie wpisujemy (lub kopiujemy z tego miejsca) polecenie:

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False



Wydanie powyższego polecenia automatycznie wyłączy systemowy firewall.

Aby go ponownie aktywować, uruchom następujące polecenie cmdlet.

Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled True

Wyłączanie oraz włączanie Zapory systemu Windows z wiersza polecenia

Aby wyłączyć zaporę dla wszystkich typów sieci, wpisz następujące polecenie.

netsh advfirewall set allprofiles state off

Aby ponownie włączyć zaporę, wpisz następujące polecenie.

netsh advfirewall set allprofiles state on

Włączanie rejestrowania dla Windows Firewall

Jeżeli nie mamy pewności czy Windows Firewall blokuje ruch, który powinien być dopuszczany lub zezwala na niepożądany ruch, powinniśmy włączyć rejestrowanie, ponownie wywołać problem i sprawdzić pliki dziennika.

Domyślnie Windows Firewall zapisuje wpisy dziennika w pliku %SystemRoot%\System32\LogFies\Firewall\firewall.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.
Po zakończeniu natychmiast należy wyłączyć rejestrowanie.

Identyfikacja komunikacji sieciowej

Dokumentacja dołączona do aplikacji sieciowych często nie identyfikuje jasno protokołów komunikacyjnych używanych przez aplikację.

Jeżeli preferujemy reguły zapory Port lub potrzebujemy skonfigurować zaporę sieciową, która może identyfikować komunikację tylko w oparciu o numery portów, a dokumentacja aplikacji nie wymienia wymagań zapory, trzeba zbadać zachowanie aplikacji, aby wyznaczyć, których numerów portów używa.

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

netstat -a –b | *more > a*

notepad a

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]

Wprawdzie 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.

Podsumowanie lekcji

- *Zapory służą do odrzucenia niechcianej komunikacji (takiej jak pakiety generowane przez robaki), równocześnie zezwalając na legalną komunikację (taką jak pakiety generowanie przez narzędzia zarządzania siecią).*

- *Windows 10 i Windows Server 2016 wspierają trzy profile zapory: Domain, Private i Public. Profil Domain stosuje się zawsze, gdy komputer może komunikować się ze swoim kontrolerem domeny. Profil Private musi być ręcznie przypisany do sieci. Profil Public stosowany jest zawsze, gdy kontroler domeny nie jest dostępny, a sieć nie została skonfigurowana jako Private.*
- *Przystawka Windows Firewall With Advanced Security służy do tworzenia wejściowych reguł zapory, która pozwala aplikacji serwera odbierać żądania przychodzące.*
- *Przystawka Windows Firewall With Advanced Security służy również do tworzenia wyjściowej reguły zapory, która pozwala klienckiej aplikacji ustanawiać wyjściowe połączenie. Wyjściowe reguły zapory musimy tworzyć tylko wtedy, gdy skonfigurowaliśmy się domyślne blokowanie wychodzących połączeń.*
- *Możemy edytować właściwości reguły zapory w celu skonfigurowania zakresu, który ogranicza podsieci, z którymi aplikacja może się komunikować. Konfigurowanie zakresu może znacznie zredukować ryzyko ataków z niezaufanych sieci.*
- *Jeżeli używany IPsec w środowisku, możemy konfigurować reguły zapory, aby pozwalać tylko na bezpieczne połączenia pochodzące od autoryzowanych użytkowników i komputerów.*
- *Zasady grupy są najbardziej efektywnym sposobem konfiguracji ustawień zapory dla wszystkich komputerów w domenie. Używając zasad grupy, możemy szybko zwiększyć bezpieczeństwo wielkiej liczby komputerów i kontrolować, które aplikacje mogą komunikować się w sieci.*
- *Rejestrowanie Windows Firewall identyfikuje połączenia, na które Windows Firewall zezwala lub które blokuje. Ta informacja jest bardzo użyteczna, gdy rozwiązuje się problemy łącznością, który może być spowodowany przez Windows Firewall.*
- *Jeżeli aplikacja musi przyjmować przychodzące polaczenia, a deweloperzy nie udokumentowali portów komunikacyjnych, których używa, możemy za pomocą narzędzia Netstat zidentyfikować, na których portach nasłuchuje aplikacja. Dysponując tą informacją, możemy utworzyć reguły* zapory typu Port.

Dla zainteresowanych

Windows Server 2016 - How to open ports and firewall

https://www.youtube.com/watch?v=ZOTDZ2PEB1s

How to allow an inbound port in a Windows 2016 Firewall

https://www.youtube.com/watch?v=MYa0304J_uM

Blokowanie gier i programów w Firewallu

https://www.youtube.com/watch?v=t81oXxless0

Windows 10: Dodanie w Zaporze systemu Windows reguły pozwalającej odpowiadać systemowi na PING.

https://www.youtube.com/watch?v=6ayg9ZnI2EU

Jak skonfigurować zaporę przy użyciu obiektu GPO w systemie Windows Server 2016

https://tiny.pl/7m11w