Działania zaradcze atakom sieciowym

16.3.1

Podejście dogłębnej obrony

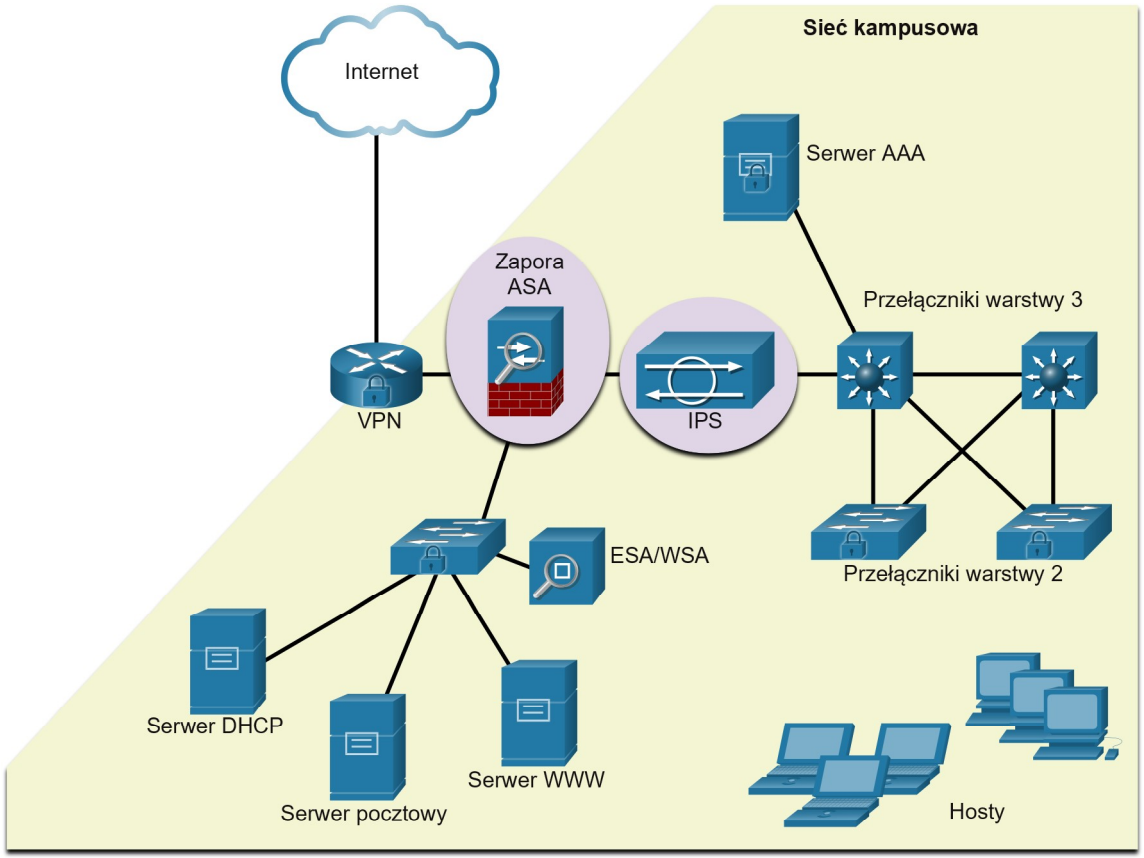
Teraz, gdy wiesz więcej o tym, jak podmioty zagrożenia mogą włamać się do sieci, musisz zrozumieć, co zrobić, aby zapobiec temu nieautoryzowanemu dostępowi. W tym temacie opisano kilka czynności, które można wykonać, aby Twoja sieć była bezpieczniejsza.

Aby ograniczyć ataki sieciowe, należy najpierw zabezpieczyć urządzenia, w tym routery, przełączniki, serwery i hosty. Większość organizacji stosuje podejście dogłębnej obrony (znane również jako podejście warstwowe) do bezpieczeństwa. Wymaga to kombinacji urządzeń sieciowych i usług pracujących w tandemie.

Rozważ sieć na rysunku. Istnieje kilka urządzeń i usług zabezpieczających, które zostały zaimplementowane w celu ochrony użytkowników i zasobów przed zagrożeniami TCP/IP.

Wszystkie urządzenia sieciowe, w tym router i przełączniki, są również zabezpieczone, co wskazują zamki na odpowiednich ikonach. Oznacza to, że zostały one zabezpieczone, aby uniemożliwić podmiotom zagrożenia uzyskanie dostępu do urządzeń i manipulowanie nimi.

Wprowadzenie do sieci



Zaimplementowano kilka urządzeń i usług zabezpieczających w celu ochrony użytkowników i zasobów organizacji przed zagrożeniami TCP/IP.

- **VPN** - Router służy do zapewnienia bezpiecznych usług VPN z witryn korporacyjnych i obsługi dostępu zdalnego dla użytkowników zdalnych za pomocą bezpiecznych szyfrowanych tuneli.
- **ASA Firewall** - To dedykowane urządzenie zapewnia stanowe usługi zapory. Zapewnia to, że ruch wewnętrzny może wyjść i wrócić, ale ruch zewnętrzny nie może inicjować połączeń do wewnątrz hostów.
- **IPS** - System zapobiegania włamaniom (IPS) monitoruje ruch przychodzący i wychodzący w poszukiwaniu złośliwego oprogramowania, sygnatur ataku sieciowego i wielu innych. Jeśli rozpozna zagrożenie, może natychmiast go zatrzymać.
- **ESA/WSA** - Urządzenie zabezpieczające e-mail (ESA) filtruje spam i podejrzane wiadomości e-mail. Web Security Appliance (WSA) filtruje znane i podejrzane strony internetowe złośliwego oprogramowania.
- **Serwer AAA** - Ten serwer zawiera bezpieczną bazę danych i informacjami, kto jest upoważniony do dostępu i zarządzania urządzeniami sieciowymi. Urządzenia sieciowe uwierzytelniają użytkowników administracyjnych przy użyciu tej bazy

danych.

16.3.2

Tworzenie kopii zapasowych

Tworzenie kopii zapasowych konfiguracji urządzeń i danych jest jednym z najbardziej skutecznych sposobów ochrony przed utratą danych. Kopia zapasowa danych przechowuje kopie informacji z komputera na przenośnym nośniku, który może być trzymany w bezpiecznym miejscu. Urządzenia infrastrukturalne powinny mieć kopie zapasowe plików konfiguracyjnych i obrazów IOS na FTP lub podobnym serwerze plików. Jeśli komputer lub router ulegnie awarii, dane lub konfigurację można przywrócić za pomocą kopii zapasowej.

Kopie zapasowe powinny być wykonywane regularnie, jak określono w polityce bezpieczeństwa. Kopie zapasowe danych są zwykle przechowywane poza siedzibą firmy w celu ochrony nośnika kopii zapasowej, jeśli coś stanie się w głównej lokalizacji. Hosty systemu Windows mają narzędzie do tworzenia kopii zapasowych i przywracania. Ważne jest, aby użytkownicy wykonali kopię zapasową danych na innym dysku lub w chmurze.

W tabeli przedstawiono kwestie dotyczące kopii zapasowych i ich opisy.

Kwestia	**Opis**
Częstotliwość	• Wykonuj kopie zapasowe regularnie, jak określono w polityce bezpieczeństwa. • Pełne kopie zapasowe mogą być czasochłonne, dlatego wykonuj co miesiąc lub co tydzień z częstymi częściowymi kopiami zmienionych plików.
Przechowywanie	• Zawsze sprawdzaj poprawność kopii zapasowych, aby zapewnić integralność danych i poprawność procedur przywracania plików.
Bezpieczeństwo	• Kopie zapasowe powinny być transportowane do zatwierdzonego magazynu w zewnętrznej lokalizacji raz na dzień, tydzień lub miesiąc, zgodnie z wymaganiami polityki bezpieczeństwa.

Kwestia	Opis
Walidacja	• Kopie zapasowe powinny być chronione za pomocą silnych haseł. Hasło jest wymagane do przywrócenia danych.

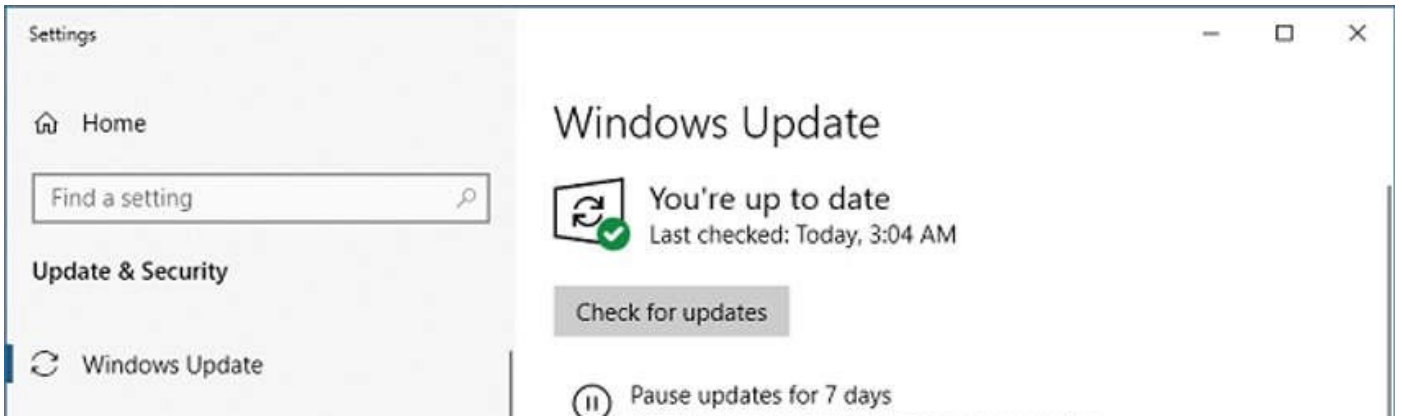
16.3.3

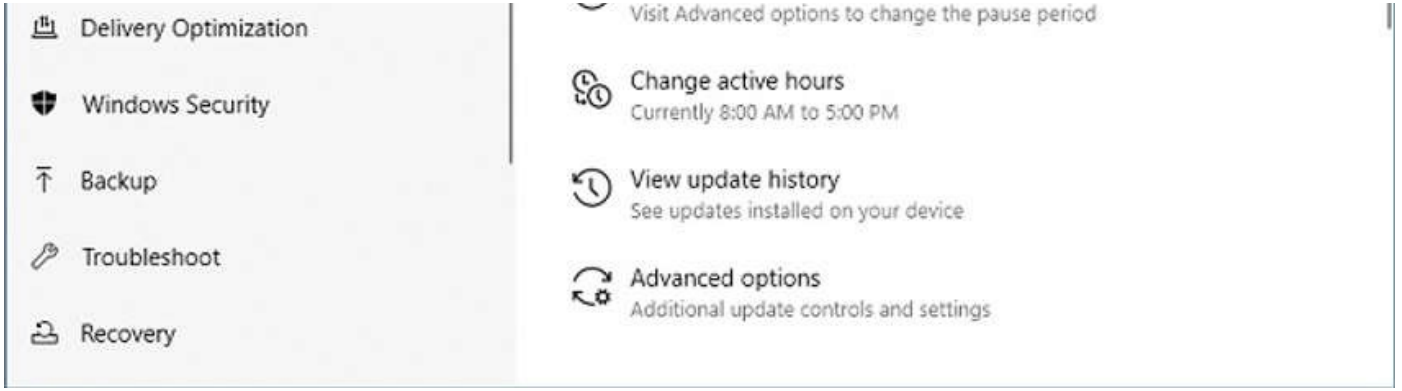
Upgrade, update i poprawki zabezpieczeń

Bycie na bieżąco z najnowszymi wersjami może prowadzić do skuteczniejszej obrony przed atakami sieciowymi. Wraz z wydaniem nowego złośliwego oprogramowania przedsiębiorstwa muszą być na bieżąco z najnowszymi wersjami oprogramowania antywirusowego.

Najbardziej skutecznym sposobem ograniczania ataku robaka jest pobranie aktualizacji zabezpieczeń od dostawcy systemu operacyjnego i zaktualizowanie wszystkich zagrożonych systemów. Zarządzanie wieloma systemami polega na tworzeniu obrazu standardowego oprogramowania (systemu operacyjnego i aplikacji, które są dopuszczone do stosowania w systemach klienckich), który został wdrożony na nowych lub ulepszanych systemach. Jednakże wymogi bezpieczeństwa zmieniają się i już wdrożone systemy mogą potrzebować zainstalowania zaktualizowanych poprawek zabezpieczeń.

Jednym z rozwiązań zarządzania krytycznymi poprawkami zabezpieczeń jest upewnienie się, że wszystkie systemy końcowe automatycznie pobierają aktualizacje, jak pokazano na rysunku dla systemu Windows 10. Pakiety serwisowe zabezpieczeń są automatycznie pobierane i instalowane bez interwencji użytkownika.





16.3.4

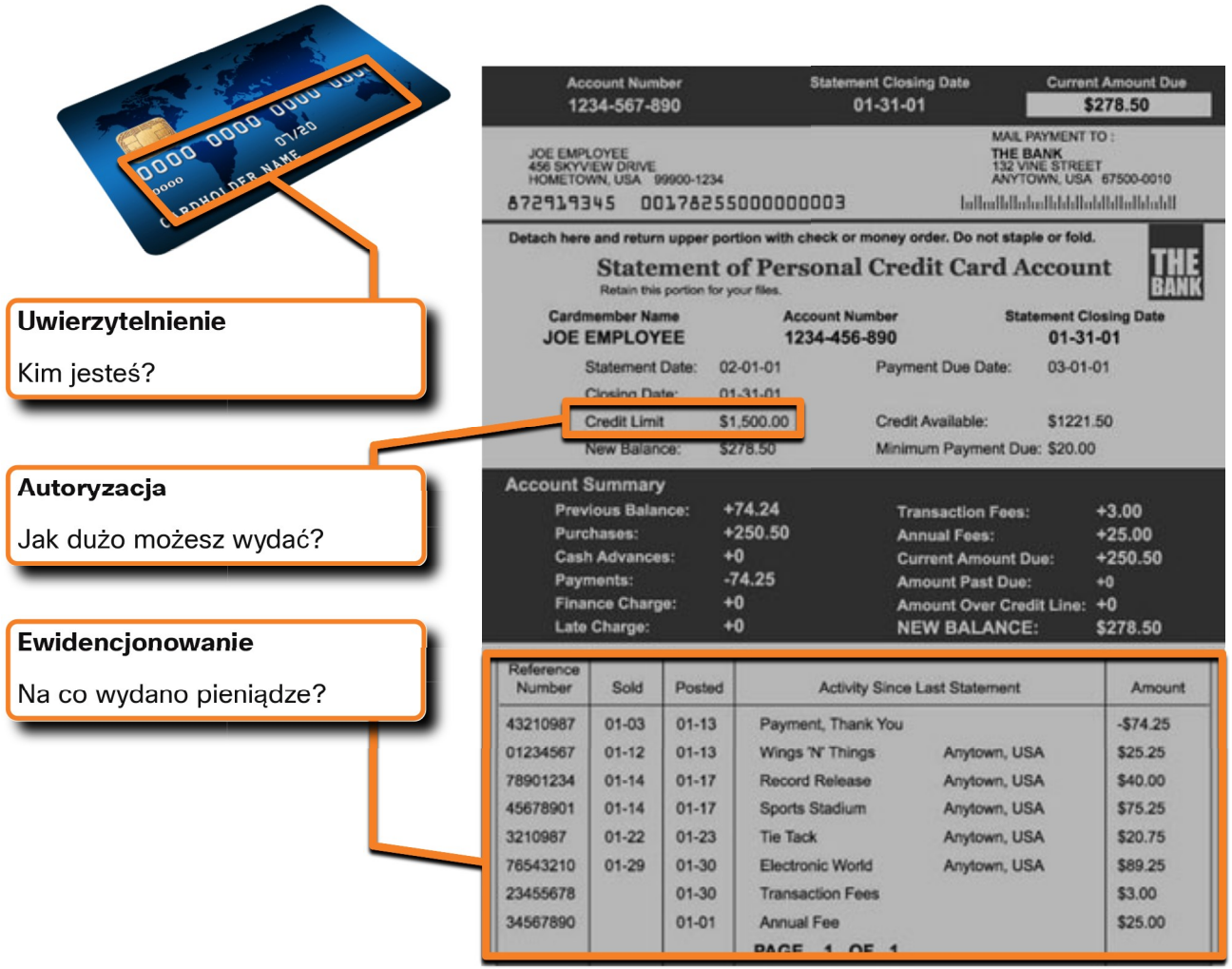
Uwierzytelnienie, autoryzacja i ewidencjonowanie

Wszystkie urządzenia sieciowe powinny być bezpiecznie skonfigurowane tak, aby zapewnić dostęp tylko upoważnionym osobom. Usługi zabezpieczenia sieci uwierzytelnianie, autoryzacja i ewidencjonowanie (authentication, authorization, accounting - AAA) dostarczają struktury pozwalającej skonfigurować kontrolę dostępu do urządzenia sieciowego.

AAA to sposób na kontrolowanie, kto ma dostęp do sieci (uwierzytelnianie), jakie działania wykonują podczas uzyskiwania dostępu do sieci (autoryzacja) i rejestrowanie tego, co zostało zrobione, gdy tam są (ewidencjonowanie).

Pojęcie AAA jest podobne do użycia karty kredytowej. Karta kredytowa określa, kto może jej używać, jak wiele użytkownik może wydać i rozlicza na jakie rzeczy użytkownik wydał pieniądze, tak jak pokazano na rysunku.

Wprowadzenie do sieci



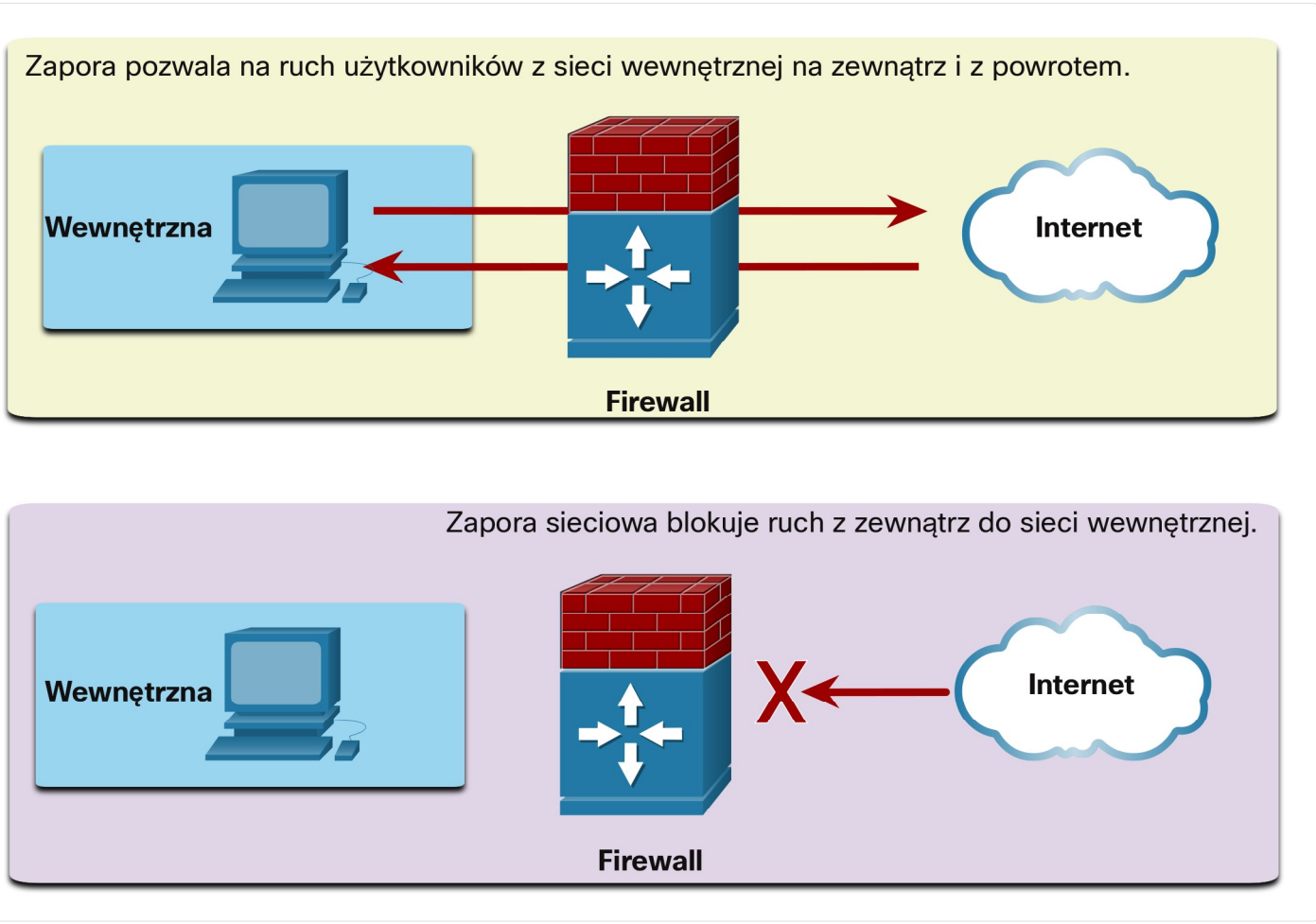
16.3.5

Zapory

Zapora jest jednym z najskuteczniejszych dostępnych narzędzi bezpieczeństwa do ochrony użytkowników przed zagrożeniami zewnętrznymi. Zapora chroni komputery i sieci, zapobiegając przedostawaniu się niepożądanego ruchu do sieci wewnętrznych.

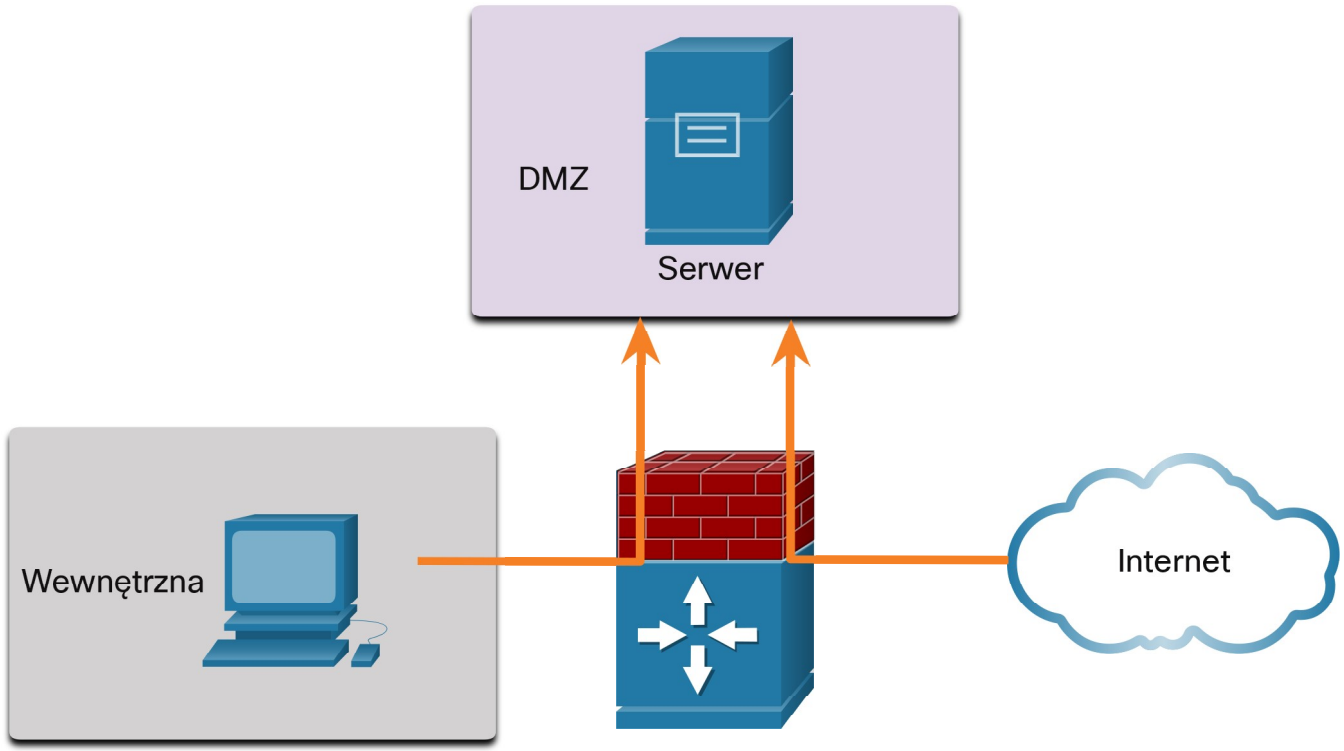
Zapory sieciowe znajdują się między dwiema lub więcej sieciami, kontrolują ruch między nimi i pomagają zapobiegać nieautoryzowanemu dostępowi. Na przykład górna topologia na rysunku pokazuje, w jaki sposób zapora ogniowa umożliwia ruch z wewnętrznego hosta sieciowego w celu wyjścia z sieci i powrotu do sieci wewnętrznej. Dolna topologia ilustruje, w jaki sposób ruch zainicjowany przez sieć zewnętrzną (tj. Internet) nie ma dostępu do sieci wewnętrznej.

Działanie zapory ogniowej



Zapora może umożliwić użytkownikom zewnętrznym kontrolowany dostęp do określonych usług. Na przykład serwery dostępne dla użytkowników zewnętrznych są zwykle zlokalizowane w specjalnej sieci zwanej strefą zdemilitaryzowaną (DMZ), jak pokazano na rysunku. DMZ umożliwia administratorowi sieci stosowanie określonych zasad dla hostów podłączonych do tej sieci.

Topologia z zaporą i DMZ



16.3.6

Rodzaje zapór

Zapory są dostarczane w różnych formach. W produktach tych stosuje się różne techniki określania dozwolonego lub blokowanego dostępu do sieci. Obejmują one:

- **Filtrowanie pakietów** - Blokuje lub zezwala na dostęp w zależności od adresu IP lub MAC.
- **Filtrowanie aplikacji** - Blokuje lub umożliwia dostęp do określonych typów aplikacji w oparciu o numer portu.
- **Filtrowanie URL** - Blokuje lub umożliwia dostęp do określonych stron w oparciu o URL lub słowa kluczowe.

- **Stanowa inspekcja pakietów (ang. Stateful Packet Inspection, SPI)** - Przychodzące pakiety muszą być prawidłową odpowiedzią na żądanie wysłane z wewnętrznych hostów. Niechciane pakiety są blokowane, lecz można ustanawiać pewne wyjątki. SPI może również obejmować funkcję rozpoznawania i filtrowania określonych rodzajów ataków, takich jak odmowa usługi (DoS).

16.3.7

Bezpieczeństwo urządzeń końcowych

Urządzenie końcowe lub komputer stanowi indywidualny system komputerowy lub urządzenie, które działa jako klient sieci. Typowym punktem końcowym są laptopy, komputery stacjonarne, serwery, smartfony i tablety. Zabezpieczenie urządzeń końcowych jest jednym z najtrudniejszych zadań administratora sieci, ponieważ dotyczy natury ludzkiej. Przedsiębiorstwo musi mieć dobrze udokumentowaną politykę, a pracownicy muszą być świadomi tych zasad. Pracownicy muszą być przeszkoleni w zakresie właściwego korzystania z sieci. Polityki często obejmują wytyczne stosowania oprogramowania antywirusowego i zapobiegającego włamaniom do komputerów. Bardziej kompleksowe rozwiązanie bezpieczeństwa punktów końcowych polega na kontroli dostępu do sieci.

16.3.8

Sprawdź, czy zrozumiałeś - Działania zaradcze atakom sieciowym

Sprawdź swoją wiedzę na temat działań zaradczych atakom sieciowym, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Które urządzenie kontroluje ruch między dwiema lub więcej sieciami, aby zapobiec nieautoryzowanemu dostępowi?

- Serwer AAA
- zapora
- ESA/WSA
- IPS

2. Które urządzenie jest używane przez inne urządzenia sieciowe do uwierzytelniania i autoryzacji dostępu do zarządzania?

- Serwer AAA
- zapora
- ESA/WSA
- IPS

3. Które zasady tworzenia kopii zapasowych dotyczą używania silnych haseł do ochrony kopii zapasowych i przywracania danych?

- częstotliwość
- przechowywanie
- zabezpieczenia
- walidacja

4. Ta strefa służy do umeszczania serwerów, które powinny być dostępne dla użytkowników zewnętrznych.

- wewnętrzna
- zewnętrzna
- Internet
- DMZ

5. Co jest odpowiednie dla zapewnienia bezpieczeństwa punktów końcowych?

- serwer AAA
- oprogramowanie antywirusowe
- zapora serwerowa
- ESA/WSA

Sprawdź

Rozwiązanie

Resetuj

16.2 Ataki sieciowe

16.4 Bezpieczeństwo urządzeń