Zeszyty Naukowe WWSI, No 20, Vol. 13, 2019, s. 7-28
DOI: 10.26348/znwwsi.20.07

Zastosowanie zapór sieciowych we współczesnych sieciach komputerowych

Dariusz Chaładyniak, Paweł Niezgoda[1]

Warszawska Wyższa Szkoła Informatyki

Abstrakt

Artykuł przedstawia podstawowe techniki filtrowania ruchu pakietów IP w sieciach teleinformatycznych realizowane przez zapory sieciowe. W części wstępnej omówiono mechanizmy filtrowania bezstanowego, stanowego i pełnostanowego. W części praktycznej przedstawiono komercyjną zaporę sieciową Cisco ASA oraz darmowe oprogramowanie PfSense, które wykorzystano w przykładowej konfiguracji.

Słowa kluczowe **–** zapora sieciowa, listy kontroli dostępu, filtrowanie ruchu sieciowego, bezpieczeństwo

[1] E-mail: dchalad@wwsi.edu.pl, p_niezgoda@poczta.wwsi.edu.pl

Zgłoszono do druku 5 grudnia 2018 r.

Wprowadzenie

W obecnych czasach standardową czynnością praktykowaną przez prawie wszystkie firmy jest łączenie komputerów w sieć LAN, która następnie poprzez operatorów ISP podłączana jest do sieci WAN. To właśnie styk tych dwóch sieci jest jednym z najbardziej narażonych na zagrożenie miejsc. Każda firma chcąca zapewnić sobie prywatność, integralność i ochronę swoich danych musi regularnie inwestować. Dlatego do zabezpieczenia połączenia z siecią Internet w małych i średnich firmach wykorzystywane są przeważanie sprzętowe zapory sieciowe, których zadanie nie sprowadza się jedynie do filtrowania ruchu. Firewall w dzisiejszych czasach należy bardziej traktować jak platformę (UTM), która dostarcza zróżnicowanych funkcjonalności począwszy od IDS, filtrów anty-spamowych i wirusowych a skończywszy na obsłudze tunelowania i zarządzania ruchem sieciowym. Wraz z liczbą dodatkowych ról, jakie musi pełnić zapora sieciowa ważnym parametrem staje się wydajność, za którą idzie koszt samego urządzenia i licencji. Biorąc to pod uwagę, firmy często poszukują rozwiązań tańszych i równie skutecznych.

Na rynku od dość długiego czasu rozwijane są projekty systemów na bazie darmowego oprogramowania, które są predefiniowane do pełnienia zadań zapory sieciowej. Jednym z takich projektów jest PfSense.

1. Filtrowanie ruchu pakietów IP

1.1. Filtrowanie bezstanowe – listy ACL

W pracy administratorów bardzo ważną rolę odgrywa kontrola tego, co dzieje się aktualnie w sieci. Dlatego, aby ograniczyć ilość ruchu sieciowego i kształtować go według potrzeb, często stosuje się listy ACL (ang. *Access Control List*). To właśnie one odpowiadają za filtrowanie ruchu sieciowego, a zasada ich działania opiera się na przepuszczaniu lub blokowaniu pakietów. Można powiedzieć, że listy ACL są zestawem instrukcji, wykonywanych sekwencyjnie przez urządzenie sieciowe [1].

W urządzeniach firmy Cisco wyróżniamy trzy podstawowe rodzaje list, które przedstawia tabela 1.

Tabela 1. Rodzaje list ACL [1]

Rodzaj	Numer	Opis
Standardowe	1-99 1300-1999	Filtrują ruch jednie na podstawie źródłowego adresu IP.
Rozszerzone	100-199 2000-2699	Umożliwiają bardziej szczegółowe filtrowanie, które może opierać się na: źródłowym i docelowym adresie IP, protokole oraz określonym porcie źródłowym i docelowym.
Established/ Reflective(SPI)		Umożliwi komunikację jedynie w wypadku, kiedy dany host zainicjował transmisję. W przeciwnym wypadku ruch jest odrzucany.

Konfigurację standardowej listy zaczynamy od słowa kluczowego „access-list", po czym wskazujemy numer, który będzie do niej przydzielony. Kolejny etap określa czy ruch ma zostać odrzucany czy przepuszczany. W następnym kroku wymagane jest podanie adresu sieciowego z maską blankietową (odwrotną). Tego rodzaju maska przypomina maskę sieciową, posiada długość 32-bitów oraz jest podzielona na cztery oktety z tą jednak różnicą, iż bit 0 odpowiada za dopasowanie adresu IP, natomiast bit 1 każe zignorować dopasowanie [2].

Maski blankietowe wykorzystuje się wraz z listami kontroli dostępu w celu określenia wydzielonych podsieci oraz części adresów przeznaczonych dla hostów. Dzięki ich zastosowaniu można przypisać jedną listę ACL do pojedynczego adresu sieciowego lub ich grupy, dzięki czemu minimalizujemy liczbę wpisów w listach. Przykłady masek blankietowych zawiera tabela 2.

Tabela 2. Przykłady masek blankietowych

Adres podsieci	Maska podsieci	Maska blankietowa
193.50.20.62	255.255.255.240	0.0.0.15
195.50.20.0	255.255.255.192	0.0.0.63
196.50.20.0	255.255.255.0	0.0.0.255
10.0.0.0	255.0.0.0	0.255.255.255

System IOS stosowany w urządzeniach Cisco umożliwia zastosowanie skróconego zapisu w dwóch przypadkach. Kiedy zachodzi potrzeba zablokowania całego ruchu, można użyć komendy „any", które domyślnie posiada maskę blankietową 255.255.255.255. W przypadku określania ACL tylko dla jednego hosta można użyć komendy „host". Tutaj również stosowana jest niejawna maska blankietowa 0.0.0.0 [1]. Przykłady skonfigurowanych list przedstawia rysunek 1.

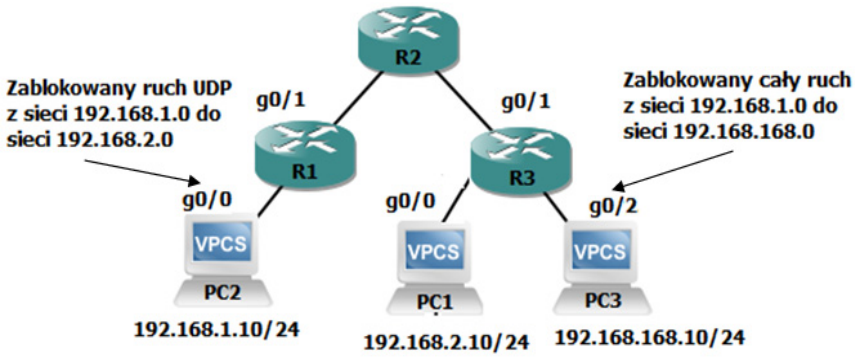
```
1 Router(config)#access-list 1 permit 192.168.1.10
2 Router(config)#access-list 2 deny host 192.168.1.11
3 Router(config)#access-list 3 permit 192.168.2.0 0.0.0.255
```

Rysunek 1. Przykład standardowych list ACL

Po skonfigurowaniu listy trzeba ją przypisać do interfejsu, dlatego też w tym celu w oknie konfiguracji globalnej trzeba wydać polecenie „ip access-group" [numer/nazwa listy], [in/out]. Parametr „in" określa ruch przychodzący natomiast „out" ruch wychodzący.

Poprawne rozmieszczenie list jest istotne, ponieważ często to właśnie od niego uzależnione jest poprawne ich działanie, jak również wydajność przekazywanego ruchu sieciowego. Dobrą praktyką jest stosowanie list standardowych jak najbliżej sieci docelowej. Takie umieszczenie wynika z faktu, iż standardowe listy filtrują ruch na podstawie źródłowych adresów IP. Rozszerzone listy ACL umieszcza się odwrotnie, czyli zazwyczaj jak najbliżej źródła blokowanego ruchu, dzięki czemu ruch sieciowy, który wymaga zablokowania może być odrzucany bez zbędnego przesyłania danych przez sieć [3].

Konfiguracja list rozszerzonych przebiega w analogiczny sposób, jak list standardowych, jednak są one powszechniej używane ze względów na większe możliwości ich dostosowania do specyfiki sieci. Dostosować listy można według protokołu, jakim przesyłane są pakiety np. TCP, UDP, ICMP, OSPF, jak również portów. Przykładowo, jeżeli aplikacje działające na serwerze wykorzystują porty 25 i 110, można przepuszczać ruch sieciowy tylko na nich.



Rysunek 2. Rozmieszczenie list standardowych i rozszerzonych

Kiedy urządzenie sieciowe odbiera pakiet, następuje sprawdzenie, czy dla wewnętrznego interfejsu istnieje lista ACL. Jeżeli lista jest przypisana, urządzenie sieciowe zaczyna ją sprawdzać. W przypadku odnalezienia wpisu z warunkiem zezwalającym, rozpoczyna się przeszukanie tablicy trasowania, aby znaleźć numer interfejsu docelowego, natomiast kiedy urządzenie napotka na warunek blokujący ruch na tym porcie, pakiety zostają automatycznie odrzucane [4].

W następnej kolejności sprawdza się, czy występują listy przypisane do interfejsu zewnętrznego. W przypadku ich wystąpienia sprawdza się je w sposób analogiczny do przedstawionego wyżej, a we wszystkich interfejsach pozbawionych mechanizmu filtracji pakiety są swobodnie przesyłane [4].

W celu weryfikacji, czy dana reguła filtrowania odnosi się do przychodzącego pakietu danych, urządzenie sieciowe sprawdza jego dopasowanie do maski blankietowej. Proces szukania dopasowania przedstawia rysunek 3.

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.1.255
```

Adres IP 1	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 1 1	0 0 0 0 1 0 1 0
Adres IP 2	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0
Maska blankietowa	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	1 1 1 1 1 1 1 1
Dopasowanie	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 X	X X X X X X X X

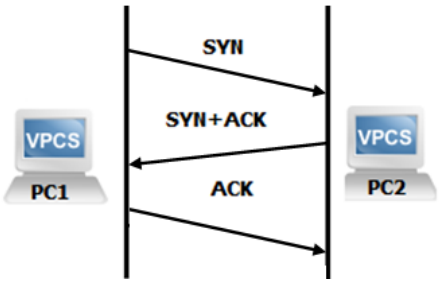
Rysunek 3. Dopasowanie masek blankietowych [3]

W rozpatrywanym przypadku ruch sieciowy „Adres IP 1" zostanie odrzucony, ponieważ nie pasuje do maski blankietowej. „Adres IP 2", czyli 192.168.1.10 z maską blankietową 0.0.1.255 zostanie poprawnie dopasowany, a co za tym idzie, możliwe będzie przesłanie ruchu sieciowego. Na podstawie takiego dopasowywania mechanizm ACL wyznacza przeznaczenie pakietu (przepuszczony lub odrzucony).

1.2. Filtrowanie stanowe – ACL established

Za rozwinięcie rozszerzonych list filtrujących uważa się listy ACL established. Pojawiły się one w odpowiedzi na niedoskonałości wynikające z reguł filtrowania, jakie oferowały dotychczasowe rozwiązania. Przykładowo, jeżeli administrator utworzył regułę na zaporze sieciowej, znajdującej się na styku sieci LAN i Internet, przepuszczającą ruch TCP na porcie 80 (WWW), to możliwe jest zainicjowanie połączenia zarówno w wnętrza sieci LAN (pożądane), jak i z sieci Internet (niepożądane). Rozpatrywany mechanizm jest w stanie zapobiec temu problemowi, ponieważ można wymusić, aby przepuszczany był jedynie taki ruch, który został zainicjowany z wnętrza sieci LAN. Idea mechanizmu bazuje na sposobie działania protokołu TCP (patrz rysunek 4), a co za tym idzie, jest jedynie do niego ograniczona [1]. Podczas nawiązywania połączenia TCP zawsze musi wystąpić trójetapowe uzgadnianie [2]. Wykorzystując ACL established zastrzegamy tym samym, że segment z ustawioną flagą SYN może napłynąć jedynie z wnętrza sieci LAN [1].

Konfiguracja listy ACL wprowadzona na routerze Cisco, zezwalająca na ruch TCP na porcie 80 będzie mieć następujący zapis: „access-list 110 permit tcp any eq 80 any eq 80 established".

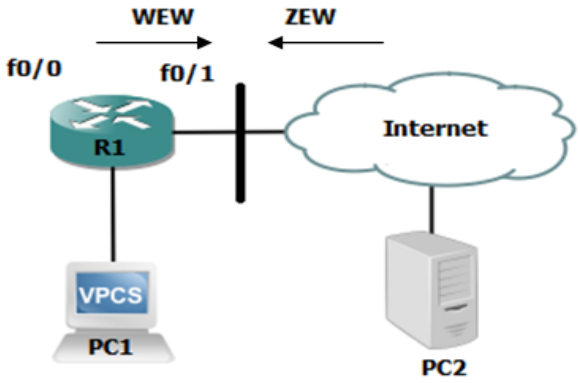


Rysunek 4. Trójetapowe nawiązanie połączenia TCP [2]

1.3. Filtrowanie stanowe – SPI

SPI (*ang. Stateful Packet Inspection*) jest to mechanizm, który umożliwia analizę nagłówków przesyłanych pakietów i ich dalsze przekazywanie bądź blokowanie. Można powiedzieć, że jest to rozwinięcie ACL established, które już nie ogranicza się jedynie do protokołu TCP. Analiza ruchu odbywa się na podstawie źródłowego i docelowego adresu IP oraz źródłowego i docelowego portu. Ruch sieciowy, który wychodzi z sieci wewnętrznej jest zapisywany dynamicznie w tablicy i na jego podstawie tworzona jest reguła do listy kontrolującej ruch przychodzący, która zezwala czasowo na przesłanie informacji zwrotnej. Mechanizm SPI przepuszcza ruch z sieci zewnętrznej tylko w przypadku, kiedy zostanie on zainicjowany przez hosty wewnętrzne [1].

Konfiguracja SPI bardzo przypomina konfigurację listy rozszerzonej.



Rysunek 5. Konfiguracja SPI i wyznaczenie styku sieci

1.4. Pełnostanowe filtrowanie ruchu – CBAC

Filtrowanie CBAC (*ang. Context Based Access Control*) nazywa się również pełnostanową zaporą sieciową, czyli prowadzącą pełną inspekcję stanu połączenia, które odbywa się z sieci wewnętrznej na zewnątrz. Do inspekcji, podobnie jak w przypadku SPI, wykorzystuje się źródłowy i docelowy adres IP, źródłowe oraz docelowe porty, ale także całkowity przebieg uzgadniania sesji. Mechanizm obsługuje

nadzorowanie i monitorowanie protokołów TCP (po numerach sekwencyjnych), UDP oraz ICMP (rozpoznaje typy wiadomości ICMP). Zasada sprawdzania wybranego rodzaju ruchu oparta jest na tworzonych dynamicznie regułach inspekcji (ang. *inspection rules*). Powszechną praktyką jest skonfigurowanie mechanizmu CBAC tak, aby dokonywał inspekcji ruchu z sieci niezaufanej, jednak istnieje możliwość skonfigurowania dwukierunkowej inspekcji. Zaletą dwukierunkowego rozwiązania jest ochrona sieci wewnętrznej (istnieją dziesiątki ataków sieciowych, które infekując hosty w sieci wewnętrznej inicjują z nich ruch do sieci niezaufanej), lecz wadą jest spadek wydajności sieci lub potrzeba instalacji wydajnych urządzeń nadzorujących ruch [1].

1.5. Pełnostanowe filtrowanie ruchu – ZBF

Filtrowanie ZBF (ang. *Zone-Based Firewall*) jest rozwinięciem mechanizmu CBAC, który wprowadza między innymi możliwość tworzenia wirtualnych stref grupujących urządzenia sieciowe o podobnym stopniu zabezpieczenia oraz nowy język C3PL (ang. *Cisco Common Classification Policy Language*), który rozszerza dotąd używane w CBAC listy ACL. Do każdej utworzonej strefy trzeba przypisać interfejsy obsługujące w niej ruch. W domyślnej konfiguracji między wydzielonymi strefami ruch jest zablokowany i dopiero po stworzeniu reguł zezwalających na komunikację może się on odbywać. Odmiennie jest natomiast z ruchem między interfejsami należącymi do tej samej strefy lub ruchem wewnątrz strefy, ponieważ jest on domyślnie przepuszczany. Konfigurując mechanizm ZBF samo urządzenie przydzielane jest do strefy „self", dzięki czemu można wykonać np. połączenia typu „ping" z pozycji firewalla do każdej strefy [1].

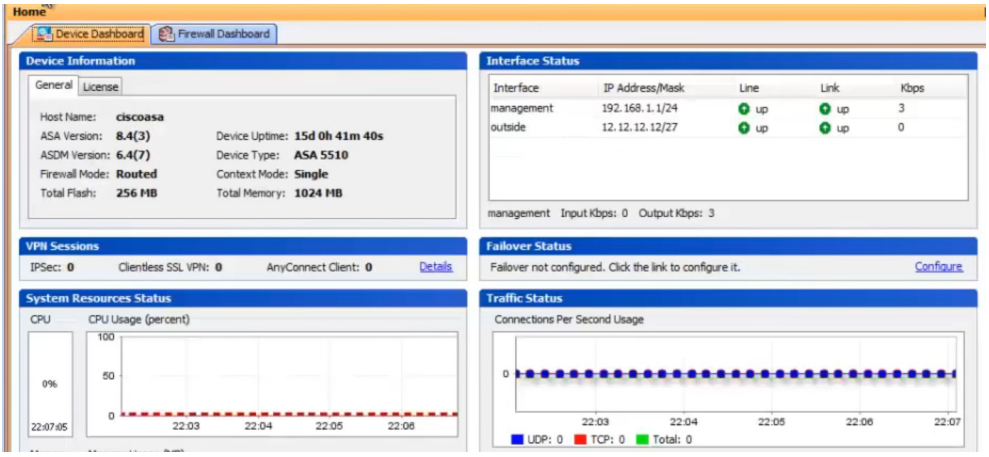
2. Zapora sieciowa Cisco ASA

Cisco ASA (ang. *Adaptive Security Appliance*) jest rodziną urządzeń sieciowych firmy Cisco służących do podniesienia bezpieczeństwa w sieciach komputerowych. Urządzenia te wspierają wymienione w rozdziale pierwszym mechanizmy filtrowania ruchu pakietów IP oraz posiadają liczne funkcje, począwszy od pełnienia roli zapory sieciowej poprzez wykrywanie i informowanie o próbach ataków sieciowych,

a skończywszy na ich blokowaniu (IPS). Ponadto ASA może pełnić funkcję koncentratora VPN pozwalającego na zestawianie zdalnych połączeń, umożliwiając tym samym łączenie się z zewnątrz do lokalnej sieci [4].

Praca tego urządzenia może odbywać się w trybie zwanym „routed mode", w którym to pełni rolę routera przekazującego pakiety do wydzielonych stref. Dostępny jest również tryb transparentny (ang. *transparent mode*), w którym urządzenie jedynie filtruje ruch sieciowy. Zaletą tego trybu pracy jest fakt, iż nie trzeba zmieniać dotychczasowej konfiguracji sieci, a sama zapora jest niewidoczna i nie bierze udziału w trasowaniu [4].

Do konfiguracji i zarządzania wykorzystywany jest znany z urządzeń Cisco widok konsolowy, oferowany przez system IOS oraz aplikacja o nazwie ASDM (ang. *Adaptive Security Device Manager*), która służy do zarządzania zaporą ogniową poprzez przeglądarkę internetową, oferując graficzny interfejs i ułatwiając nadzór nad siecią. Główne okno aplikacji ASDM przedstawia rysunek 6.



Rysunek 6. Główne okno aplikacji ASDM przeznaczonej do konfiguracji zapory sieciowej Cisco ASA

Wyświetlając początkową konfigurację nowego urządzenia ASA 5505 można zaobserwować domyślnie wprowadzony przez producenta podział na dwie strefy, które

mają separować ruch. Analizując rysunek 7 można zauważyć, że interfejs „Ethernet0/0" zarezerwowany jest do przyłączenia sieci zewnętrznej, natomiast reszta portów może być przydzielona na potrzeby hostów wewnętrznych.

Tabela 3. Informacje prezentowane przez ASDM [1]

Nazwa okna	Przedstawiane informacje
Device Information	Informacje o nazwie urządzenia, wersji oprogramowania IOS, wersji aplikacji ASDM, trybie pracy urządzenia, ilości pamięci operacyjnej i pamięci flash oraz kontekście pracy.
Interface Status	Prezentuje nazwy interfejsów urządzenia, ich obecny status (włączony lub wyłączony), przypisane adresy IP oraz ilość przesłanych informacji.
VPN Sessions	Zestawione sesje VPN oraz liczba posiadanych licencji.
Failover Status	Wyświetla szczegóły dotyczące konfiguracji trybu przełączania awaryjnego, które konfiguruje się, aby zapewnić nadmiarowość. W chwili awarii drugie urządzenie ASA przejmuje rolę pierwszego.
System Resources Status	Wykresy przedstawiające wykorzystanie zasobów procesora oraz pamięci RAM urządzenia.
Traffic Status	Wykres ilustrujący ruch sieciowy przepływający przez urządzenie. W tym przypadku podzielony na TCP i UDP.

2.1. Strefy i poziomy bezpieczeństwa oraz inspekcja ruchu

W dalszej części listingu skonfigurowano interfejs VLAN1. Przypisano mu nazwę oraz parametr określający poziom bezpieczeństwa strefy.

Zapora sieciowa Cisco ASA z powodzeniem bazuje na wcześniej omówionym mechanizmie ZBF, jednak go dodatkowo rozszerza o przypisanie do każdej z wydzielonych stref parametru, zwanego poziomem bezpieczeństwa. Parametr ten służy do ograniczania ruchu w sieci i budowania tak zwanego „pierścienia zaufania". Istotą działania tej funkcjonalności jest zapewnienie dostępu strefie o wysokim poziomie zaufania do interfejsów, dla których przydzielony poziom jest niższy. Przykładowo, jeżeli pracownik będący w strefie wewnętrznej (security-level 70) chce nawiązać połączenie z serwerem w wydzielonej strefie DMZ (security-level 50), to taki ruch zostanie przesłany. Nieco inaczej będzie w przypadku, gdy ruch zostanie

zainicjowany ze strefy DMZ do sieci wewnętrznej, ponieważ ze względu na różnicę poziomów bezpieczeństwa komunikacja ta zostanie odrzucona przez zaporę [1].

Może jednak zachodzić potrzeba przepuszczenia takiego ruchu, dlatego aby to umożliwić, stosuje się statyczną translację NAT i listy ACL [4].

W zaporze sieciowej domyślnie włączono także protokół DHCP, którego zadaniem jest pobranie adresu sieciowego z hosta zewnętrznego, którym najczęściej jest urządzenie dostawcy ISP (Vlan2).

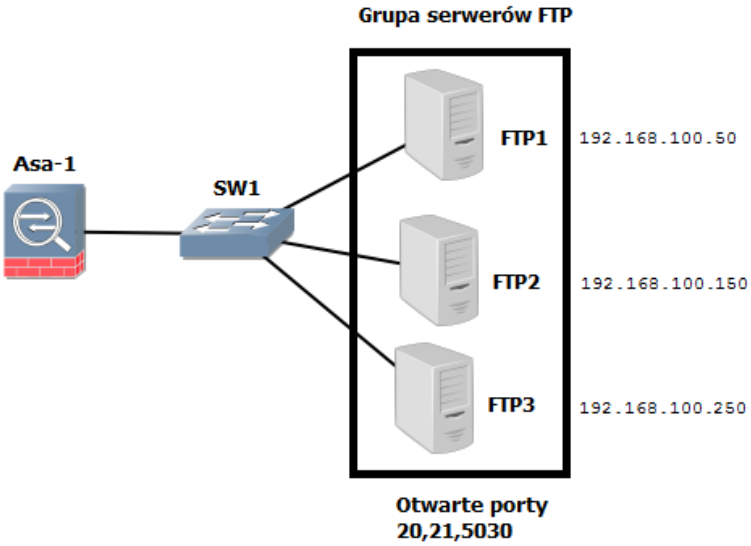
```
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
```

Rysunek 7. Wycinek z konfiguracji domyślnej ASA 5505

Każde urządzenie typu ASA wspiera również inspekcję ruchu sieciowego, która jest domyślnie włączona i obejmuje większość popularnie używanych protokołów.

2.2. Grupowanie obiektów

Kolejną bardzo przydatną funkcją w zaporze jest możliwość grupowania obiektów. Często zdarza się, że konfigurując urządzenia dochodzimy do sytuacji, w której w strefie DMZ występuje kilka hostów udostępniających usługi na zewnątrz. Aby zapewnić kontrolę ruchu dla tych hostów układa się listy dostępowe, które przepuszczają lub blokują określony ruch. Przy niewielkiej liczbie urządzeń ten problem nie występuje, jednak gdy są ich dziesiątki, listy ACL rosną a przez to urządzenie filtrujące może zostać przeciążone, dlatego pomocne w zapobieganiu takiej sytuacji okazuje się wykorzystanie mechanizmu grupowania obiektów. Zasada jego działania polega na stworzeniu wirtualnych obiektów i przyporządkowanie ich do fizycznych urządzeń. Przykład grupowania obiektów przedstawia rysunek 8 [4].




```
ciscoasa(config-if)#object-group service FTP tcp
ciscoasa(config-service)#description Grupa serwerow FTP
ciscoasa(config-service)#port-object eq 20
ciscoasa(config-service)#port-object eq 21
ciscoasa(config-service)#port-object eq 5030
ciscoasa(config-service)#exit
ciscoasa(config-if)#object-group network FTPIP
ciscoasa(config-network)network-objects host 192.168.100.50
ciscoasa(config-network)network-objects host 192.168.100.150
ciscoasa(config-network)network-objects host 192.168.100.250
ciscoasa(config-network)#exit
ciscoasa(config-if)#access-list Wej permit tcp any object-group FTP object-group FTPIP
```

Rysunek 8. Przykład grupowania obiektów – konfiguracja

3. Zapora ogniowa na bazie PFSENSE

Mimo bardzo dobrze prosperującego rynku komercyjnych urządzeń (Cisco, Fortinet, Juniper, Firebox, Zyxel), które mogą pełnić rolę zapory sieciowej, domowi użytkownicy oraz małe firmy często kierowane względami budżetowymi skupiają swoją uwagę na tańszych rozwiązaniach. Takim przykładem może być program PfSense.

O samym oprogramowaniu pfSense można myśleć niejako o platformie UTM, która skupia w obrębie jednego urządzenia wiele funkcjonalności. Nie ze wszystkich użytkownik musi korzystać, a nawet nie jest to zalecane ze względów wydajnościowych. Nie można zapominać, że wszystkie funkcje jakie realizuje platforma z zainstalowanym oprogramowaniem pfSense wymagają zasobów procesora, który z uwagi na

swoją konstrukcję i bogaty zestaw instrukcji nie jest specjalizowany do przetwarzania ruchu sieciowego jak w przypadku układów ASIC.

Niektóre funkcjonalności, jakie oferuje pfSense, przedstawiono w tabeli 4.

Tabela 4. Wybrane funkcjonalności PfSense [5]

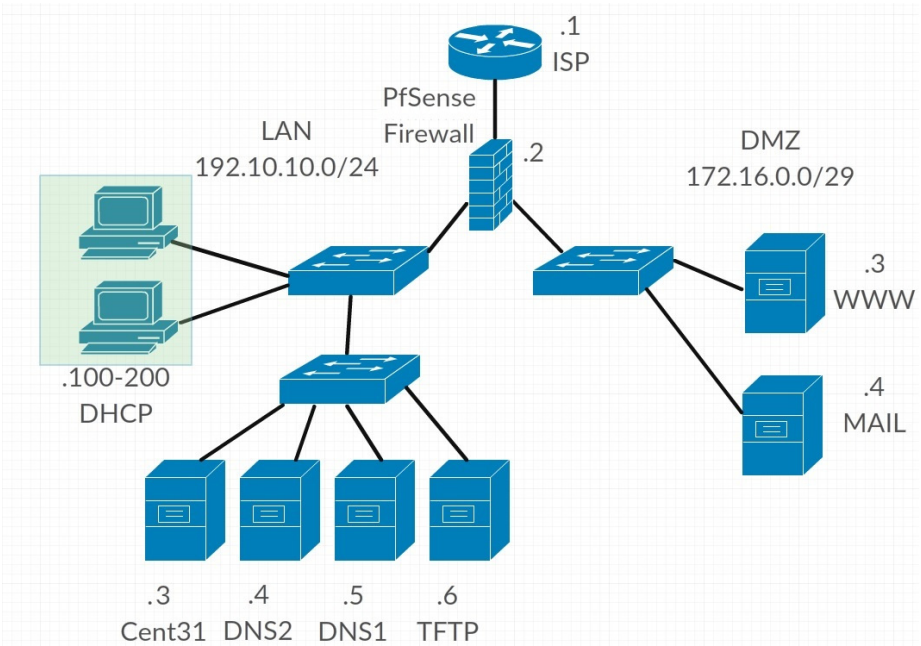
Funkcja	Opis
DHCP	Możliwość uruchomienia serwera DHCP. Domyślnie jest on aktywny dla interfejsu sieci LAN z pulą adresową 192.168.1.100-199, zaś sama platforma z oprogramowaniem ma przydzielony adres 192.168.1.1. Jest on bramą domyślną jak i serwerem DNS.
DNS	Można zastosować jako serwer pośredni. Domyślnie wszystkie zapytania DNS są przekazywane do sieci WAN.
Firewall	Obsługa zarówno bezstanowych jak i stanowych metod filtrowania ruchu sieciowego.
LACP	Grupowanie kilku interfejsów fizycznych w jeden logiczny kanał dzięki obsłudze protokołu LACP.
Load Ballancing	Możliwość rozkładania obciążenia zarówno na połączeniach WAN między kilku IPS jak i LAN np. między dwoma serwerami http.
NAT	Obsługa zarówno translacji statycznych – SNAT, jak i dynamicznych – DNAT.
PPPoE	Umożliwia ustanowienie połączenia użytkowników w oparciu o utworzone wcześniej konta. Pomaga to w zarządzaniu i identyfikacji ruchu pochodzącego od poszczególnych klientów. Popularnie stosowane przez ISP.
Proxy	Umożliwia pośredniczenie i zarządzanie dostępem do treści użytkowników sieci LAN.
RADIUS	Serwer uwierzytelniania, który można skonfigurować do współpracy np. VPN, PPPoE lub Windows Server.
Routing	Obsługuje routing RIP, BGP oraz OSPF.
System Log	Logowanie zdarzeń może odbywać się lokalnie na dysku lub w pamięci RAM. Istnieje także możliwość zapisywania zdarzeń na zdalnych serwerach Syslog.
VLAN	Obsługa sieci logicznych ze znakowaniem według IEEE 802.1Q. Wspierane są również mechanizmy PVLAN oraz podwójne tagowanie QlnQ.
VPN	Umożliwia zestawienie połączeń między lokalizacjami Side-to-Site lub połączeń zdalnych. Powszechnie używany z oprogramowaniem OpenVPN.

Na potrzeby stworzenia testowej platformy został wykorzystany komputer klasy PC, na którym w wirtualnym środowisku zainstalowano oprogramowanie PfSense w wersji 2.4.4. Zasoby przydzielone maszynie wirtualnej zaprezentowane są w tabeli 5.

Tabela 5. Konfiguracja stacji dla oprogramowania PfSense

Podzespół	Dane	Opis
CPU	AMD Ryzen 7 1700X	8 rdzeni po 1 wątku. Wspiera AES-NI CPU Crypto
RAM	2 GB	
HDD	10 GB	SSD Samsung 860 EVO
Karta sieciowa	Marvell i HP	Marvell 1Gb/s – WAN, HP NC365T 4x1Gb/s – LAN

Schemat topologii sieciowej (patrz rysunek 9) dla testowego środowiska został uproszczony, aby pokazać głównie działanie mechanizmów zapory sieciowej.



Rysunek 9. Schemat topologii sieciowej dla testowego środowiska

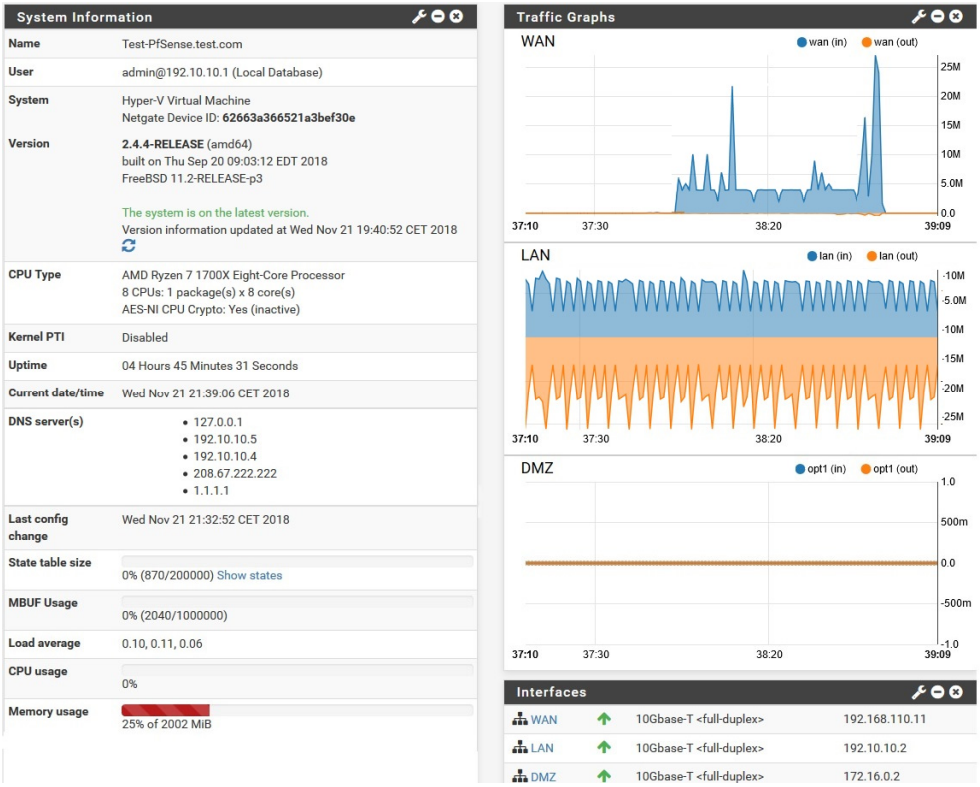
3.1. Podstawowa konfiguracja zapory PfSense

W zainstalowanym systemie dokonano wstępnej konfiguracji:

- nazwa maszyny – „Test-PfSense”;

- nazwa domeny – „test.com”;
- serwery DNS – pierwszy – 1.1.1.1, drugi 208.67.222.222;
- serwer NTP „0.pfsense.pool.ntp.org” ;
- wyłączono konto domyślne i utworzono nowe, które będzie zarezerwowane do zarządzania zaporą sieciową.

Zalecanym sposobem komunikacji z serwisem sieciowym PfSense jest wykorzystanie protokołu HTTPS. Dodatkowo dobrą praktyką jest zmiana domyślnego portu (port 443) [6]. Po zabezpieczeniu komunikacji można przystąpić do konfiguracji puli adresów IP na serwerze DHCP dla komputerów pracowników. Przyjęto przedział adresacji z zakresu od 192.10.10.100 do 192.10.10.200.



Rysunek 10. Schemat topologii sieci dla PfSense

W sieci lokalnej umieszczone są dwa serwery DNS. Z uwagi na to zostały one dodane do konfiguracji. Jeżeli wyszukiwana fraza nie jest dostępna na lokalnym serwerze, to polecenia DNS zostają przekazane do globalnych serwerów OpenDNS (208.67.222.222) lub firmy Cloudflare (1.1.1.1).

W omawianej topologii sieciowej można wyróżnić trzy strefy: LAN, DMZ oraz WAN, w których ruch jest wymieniany za pomocą usługi NAT (patrz rysunek 10). Odpowiedzialna jest ona za translacje adresów między strefami, a dzięki użyciu przekierowania portów umożliwia ona zmapowanie serwera WWW oraz MAIL na udostępniony przez dostawcę ISP adres IP.

3.2. Elementy zapory ogniowej w PfSense

Aby w łatwy sposób zarządzać grupami hostów w sieci, podobnie jak to było opisane w przypadku urządzenia Cisco ASA, wykorzystuje się tzw. aliasy. Dzięki nim w szybszy sposób można tworzyć reguły filtrowania i ograniczyć tym samym liczbę stworzonych reguł.

Typy dostępnych aliasów w PfSense 2.4.4 [5] to:

- alias na adres IP;
- alias na port;
- alias na URL.

Warto zaznaczyć, że jeżeli adres IP, URL lub port ulegną zmianie, to modyfikacja reguł zapory sieciowej ogranicza się jedynie do edycji aliasu. Przypisanie aliasów dla omawianej sieci pokazano na rysunku 11. Widzimy tam między innymi zgrupowane urządzenia sieciowe (ADMIN_LAN) oraz komputery użytkowników (LAN_PC). Dla serwerów DNS, TFTP oraz komputera administratora lokalnego również stworzono aliasy definiujące adresy IP statycznie przypisane do tych hostów.

W omawianym oprogramowaniu reguły filtrowania ruchu sieciowego przypisuje się w zakładce Firewall/Rules. Podczas wstępnej konfiguracji przez stronę internetową tworzone są reguły domyślne, które przypisywane są w zależności od roli, jaką pełni dany interfejs. Domyślnie wszystkie konfigurowane reguły w swoim działaniu wykorzystują zasady podobne do opisanego wcześniej mechanizmu SPI [7].

Firewall Aliases IP

Name	Values	Description
ADMIN_LAN	192.10.10.254	
ADMIN_urzadzenia	192.10.10.1, 192.10.10.2, 192.10.10.3, 192.10.10.4, 192.10.10.5, 192.10.10.6	
DNS_1	192.10.10.5	LAN_DNS_Local_1
DNS_2	192.10.10.4	LAN_DNS_Local_2
LAN_PC	192.10.10.100, 192.10.10.101, 192.10.10.102, 192.10.10.103, 192.10.10.104, 192.10.10.105, 192.10.10.106, 192.10.10.107, 192.10.10.108, 192.10.10.109...	
TFTP	192.10.10.22	TFTP

Rysunek 11. Lista przydzielonych aliasów

W przypadku interfejsu, na który wchodzi ruch z sieci Internet (WAN) zaleca się zaznaczanie opcji filtrowania przedziałów adresowych należących do sieci prywatnych oraz publicznych adresów IP, które nie zostały przydzielone przez organizację IANA (ang. *Internet Assigned Numbers Authority)* [5]. Sieci nieprzydzielone przez IANA określa się mianem „Bogon", a ich lista jest automatycznie aktualizowana. Poza ogólnie widzianymi regułami (patrz rysunek 12) są również niejawne wpisy blokujące cały ruch napływający na poszczególne interfejsy [6].

Prezentowane wybrane reguły zostały skonfigurowane dla interfejsu LAN. Reguły podzielone są na kolumny w celu ich łatwiejszej identyfikacji i tak w kolumnie („States") prezentowane są ogólne informacje na temat ruchu jaki został dopasowany do danej reguły. Jaki widać w pierwszym wpisie („Anti-Lockout Rule") dla automatycznie wygenerowanej reguły zapewniającej dostęp do serwisu web PfSense liczba aktywnych wpisów w tabeli stanów wynosi 3. Druga wartość określa natomiast sumę rozmiaru wszystkich przesłanych pakietów „wyłapanych" przez daną regułę [6].

Kolejna utworzona reguła dotyczy połączenia po protokole TCP na porcie 22 (SSH). Do jej budowy zostały wykorzystane wcześniej utworzone aliasy na komputer administratora oraz grupy urządzeń sieciowych, którymi można zarządzać.

Dzięki temu tylko ze stacji administratora można łączyć się przy pomocy SSH. Dodatkowo cały ruch „wyłapywany" przez tą regułę jest logowany.

Na uwagę zasługuje również pierwszy wpis z sekcji WAN, na który nałożono harmonogram. Dzięki temu reguła ta działa tylko o określonej przez administratora porze.

Jako ostatnie znalazły się reguły z sekcji „Reject", których zadaniem jest odrzucanie w jawny sposób ruchu sieciowego, który zostanie zainicjowany z hostów lokalnych lub stacji administratora. Takie zachowanie pomaga w diagnozowaniu sieci z uwagi na zwracanie komunikatów z informacją, że dany port jest nieosiągalny.

Rules (Drag to Change Order)

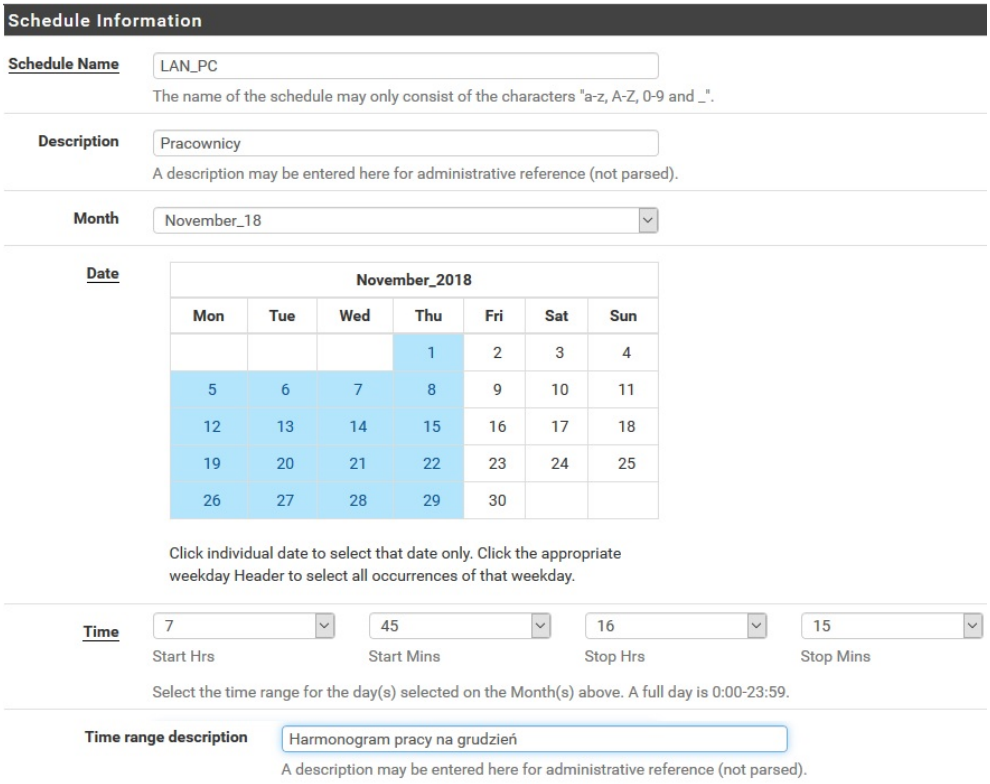
	States	Protocol	Source	Destination	Port	Schedule	Description
✓	3 /8.85 MiB	*	*	LAN Address	12300		Anti-Lockout Rule
LAN							
☐ ✓	0 /0 B	IPv4 TCP	ADMIN_LAN	ADMIN_ urzadzenia	22 (SSH)		Admin_SSH
☐ ✓	0 /0 B	IPv4 UDP	LAN_PC	DNS_1	53 (DNS)		LAN_DNS_Local_1_PC
☐ ✓	0 /0 B	IPv4 TCP	192.10.10.3	93.123.11.23	57383		CENT31_komunikacja
WAN							
☐ ✓	0 /0 B	IPv4 TCP	LAN_PC		80 (HTTP)	LAN_ PC	Z LAN do sieci Internet
☐ ✓	0 /0 B	IPv4 TCP	LAN_PC		443 (HTTPS)	LAN_ PC	Z LAN do sieci Internet
Reject							
☐	0 /10.83 MiB	IPv4+6 *	LAN_PC	*	*		LAN_PC
☐	0 /0 B	IPv4+6 *	ADMIN_LAN	*	*		ADMIN_PC

Rysunek 12. Widok listy przykładowych reguł

Oprogramowanie PfSense, podobnie jak Cisco ASA, oferuje możliwość dodania do reguł filtrowania harmonogramu, według którego dany wpis będzie aktywowany. W testowym środowisku harmonogram został ustawiony dla wszystkich adresów IP przypisanych do komputerów klienckich w sieci (patrz rysunek 13). Zakres dni,

w jakich będzie realizowana konfigurowana reguła, to okres od poniedziałku do czwartku w godzinach od 7:45 do 16:15.

Innym przykładem reguły w jakim można z powodzeniem wykorzystać harmonogram jest wpis, który odblokowuje strony popularnych portali społecznościowych w czasie, kiedy pracownicy mają przerwę śniadaniową lub obiadową. Taki mechanizm pozwala na elastyczne dostosowanie wpisów do rozkładu ruchu, jaki pojawia lub może pojawić się w sieci.



Rysunek 13. Widok okna konfiguracji harmonogramu

Podsumowanie

Porównując funkcjonalności obu opisywanych w artykule zapór sieciowych, czyli Cisco ASA oraz PfSense, można dojść do wniosku, że oba produkty są rozwiązaniami

dopracowanymi, które cały czas są rozwijane, aby sprostać wymaganiom stawianym przez konsumentów. W dziedzinie konfigurowania samych mechanizmów odpowiadających za funkcjonowanie zapory sieciowej oba produkty mają intuicyjne okienkowe menu, które pozwala w prosty sposób zapisywać daną listę ACL lub regułę oraz tworzyć i grupować obiekty.

Śledzenie ruchu, jaki przechodzi przez zaporę, w obu przypadkach da się obserwować na podstawie wykresów pokazujących chwilowy transfer oraz jego przebieg w jednostce czasu, co jest wygodne w przypadku wykrywania anomalii lub problemów związanych z komunikacją.

Porównując bazowe preinstalowane funkcjonalności użytkownik dostaje podobny zestaw funkcji pozwalający na zadowalającą pracę obu platform w charakterze zapór sieciowych. Na tym podobieństwa się kończą. Chcąc rozszerzyć Cisco ASA o moduł IDS/IPS trzeba zakupić odpowiednią licencję, w której skład wchodzi baza sygnatur według, których ruch przechodzący przez zaporę można poddać inspekcji. Z dodatkową opłatą wiążą się również dodatkowe licencje na VPN oraz zaawansowane mechanizmy szyfrowania ruchu (3DES/AES) [8].

W PfSense mimo braku standardowego IDS/IPS użytkownik jest w stanie rozszerzyć jego funkcjonalność. Dlatego oprogramowanie to można porównać do platformy (UTM), która po odpowiednich modyfikacjach i dostosowaniu do własnych potrzeb będzie spełniać żądane zadania, czyli np.:

- IDS/IPS – Snort lub Suricata;
- czarne listy – pfBlockerNG;
- filtry kontekstowe – ntopng lub Squid Guard;
- proxy/ filtr antywirusowy – HAVP jako część pakietu Squid.

W kwestii samego hardware-u wygrywa firma Cisco, dostarczająca predefiniowanych rozwiązań, które w zależności od zapotrzebowania na pasmo oraz inne czynniki można dostosować, wybierając odpowiedni model spośród bogatej oferty producenta. Ponadto firma Cisco oferuje wsparcie techniczne (Technical Assistance Center – TAC) dla swoich urządzeń, jak i samego systemu IOS, które obowiązuje wraz z umową serwisową na dane urządzenie. Poza wsparciem doraźnym, w sieci Internet jest dużo materiałów o samej platformie, a ewentualne pytania można zadawać na wielu licznych forach skupiających specjalistów z branży sieciowej.

Nieco gorzej na tym tle wypada PfSense, z uwagi na brak oficjalnej platformy, na której wydawane jest oprogramowanie. Co prawda firma Netgate oraz kilku innych producentów oferuje predefiniowany sprzęt do obsługi omawianego rozwiązania, lecz z uwagi na „otwarty" charakter platformy istnieje większa szansa na wystąpienie problemów z działaniem.

Obie omawiane zapory sieciowe dobrze pełnią swoje zadania i zasługują na zainteresowanie w przypadku budowy lub rozbudowy środowiska sieciowego. PfSense doskonale nadaje się do zastosowania przez użytkowników indywidualnych lub małych i czasami średnich firm, a w dobie wszechobecnej wirtualizacji z zapewnieniem odpowiednich zasobów sprzętowych nie ma większych problemów. Trzeba jednak pamiętać, że chcąc mieć dodatkowe funkcjonalności użytkownik zdany jest na użycie kodu firm zewnętrznych, który nie zawsze jest w pełni darmowy. W przypadku wykorzystania aplikacji Snort (IDS/IPS) chcąc mieć możliwie najszybszy dostęp do najnowszych sygnatur trzeba wykupić subskrypcję.

Na takie problemy nie napotkają osoby korzystające z produktów firmy Cisco, która zapewnia kompleksową obsługę swoich urządzeń znajdujących powszechne zastosowanie na całym świecie, zarówno w małych sieciach, jak i dużych centrach danych. Trzeba jednak zaznaczyć, że aby uzyskać podobny zakres funkcjonalności trzeba zapłacić więcej, a czasami znacznie więcej.

Ostatecznego wyboru konkretnej zapory sieciowej należy dokonać z uwzględnieniem własnych potrzeb i wymagań konkretnego środowiska sieciowego, zapoznając się również z informacjami oraz funkcjonalnością każdego z rozpatrywanych produktów.

Bibliografia

[1] A. Józefiok, *Security CCNA 210-260. Zostań administratorem sieci komputerowych CISCO*, Wydawnictwo Helion, 2016

[2] A. Józefiok, *CCNA 200-120. Zostań administratorem sieci komputerowych CISCO*, Wydawnictwo Helion, 2015

[3] CISCO, CCNA Routing and Switching: „Podstawy routingu i przełączania" Kurs Cisco NetAcademy

[4] G.A. Donahue, *Wojownik sieci*, Wydawnictwo Helion, 2012
[5] D. Zientara, *Mastering PfSense*, Packt Publishing, 2016
[6] Netgate, *The pfSense Book*, Electric Sheep Feding LLC, Netgate, 2018
[7] M. Williamson, *PfSense 2 cookbook*, Packt Publishing, 2011
[8] Cisco ASA Series General Operations CLI Configuration Guide, CHAPTER 5-1, https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/intro-license.pdf

Application of Firewalls in Contemporary Computer Networks

Abstract

The article presents the basic techniques of filtering the traffic of IP packets in IT networks performed by firewalls. The introductory part discusses the mechanisms of stateless, state and stateful filtering. The practical part shows the commercial firewall of Cisco ASA and the free PfSense software that was used in the example configuration.

Keywords – firewall, access control lists, filtering network traffic, security