MODEL LABORATORYJNY DO BADAŃ FEDERACYJNYCH SYSTEMÓW CYBERBEZPIECZEŃSTWA

Adam E. Patkowski

Instytut Teleinformatyki i Automatyki Wydział Cybernetyki WAT
aep@ita.wat.edu.pl

Streszczenie. W opracowaniu naszkicowano możliwości budowy najprostszego systemu obrony federacyjnej przed atakami DDoS. Przedstawiono również wybrane rozwiązania techniczne dla takiego systemu i zaprezentowano tani model laboratoryjny do badań jego właściwości oraz zachowania się. Adekwatność modelu osiągana jest dzięki wykorzystywaniu w badaniach, jako tła, ruchu sieciowego zarejestrowanego w reprezentatywnych lub docelowych sieciach. Wskazano możliwości badań z wykorzystaniem tego modelu i uzyskania odpowiedzi na pytania potencjalnych uczestników federacji.

Słowa kluczowe: bezpieczeństwo, cyberatak, DoS, DDoS, domena, federacja, adaptacja, FoS, IDS, model.

1. Wstęp

W WAT od dawna prowadzone są prace nad sposobami obrony przed cyberatakami wymierzonymi w systemy teleinformatyczne wojskowe[1], pewne systemy przemysłowe[2], czy ogólnie[3] państwowe systemy tzw. infrastruktury krytycznej. Poszukiwano między innymi możliwości odpierania ataków prowadzących do odmowy usługi (*Denial od Service* – DoS lub rozproszonych ataków *Distribted DoS* – DDoS). W polu szczególnej uwagi znalazły się między innymi sposoby tworzenia dużych mechanizmów obronnych powstających z połączenia i współpracy systemów należących do różnych podmiotów. Intencją takiego połączenia – federacji systemów FoS (*Federation of Systems*) było osiągnięcie efektu synergii w cyberobronie.

Istotną cechą łączącą członków FoS jest to, że są oni zwykle na siebie skazani – współpraca wynika z realizowanego zadania (w przypadku woj-

[1] Program Badawczy Zamawiany Nr PBZ–MNiSW–DBO–02/I/2007 Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych.

[2] Projekt Rozwojowy DOBR/0074/R/ID 1/2012/03. System zapewnienia bezpiecznej komunikacji IP w obszarze zarządzania siecią elektroenergetyczną. BIPSE.

[3] Projekt Rozwojowy Nr 0 R00 0125 11. System ochrony sieci teleinformatycznych przed działaniami nieuprawnionymi. SOPAS.

skowych systemów sprzęganych na potrzeby misji) lub po prostu z bezpośredniego sąsiedztwa systemów w topologii sieci. W przypadku systemów zabezpieczeń wejście do federacji wymaga zwykle rezygnacji w pewnym stopniu z własnej suwerenności w dziedzinie bezpieczeństwa na rzecz ogólnego bezpieczeństwa federacji.

Wśród problemów związanych z implementacją obrony federacyjnej w polskiej cyberprzestrzeni, za główne trzeba uznać brak środków na podjęcie centralnie zarządzanego przedsięwzięcia budowania takiego systemu i brak regulacji prawnych, wymuszających włączenie się do niego niezależnych podmiotów gospodarczych. Nie ma zatem warunków, które pozwoliłyby utworzyć dużą federację obronną np. dla infrastruktury krytycznej. Potrzebne były rozwiązania prowadzące do osiągnięcia skutecznej wspólnej obrony, które z jednej strony byłyby tanie, a z drugiej nie wymagałyby znacznych zmian istniejących poszczególnych systemów obrony i zapewniałyby, że ich wprowadzenie nie obniży jakości usług sieciowych świadczonych przez każdy ze sfederowanych systemów. Inaczej mówiąc „przede wszystkim nie szkodzić". Jedno z możliwych rozwiązań, sformułowanych w trakcie prowadzonych prac zdaje się być atrakcyjną pod względem biznesowym ofertą dla partnerów gospodarczych.

O ile idea federacji systemów jest dość prosta, to odpowiedzi na pytania o skuteczność obrony oraz o zagrożenia negatywnym oddziaływaniem na procesy biznesowe właścicieli systemów nie są łatwe. W szczególności nie poddają się metodom analitycznym. Podjęto więc próby znalezienia metody badania skuteczności i wpływu wprowadzenia sfederalizowanej obrony na konkretne systemy.

Główne problemy organizacyjne tworzenia federacji to uzgodnienia między uczestnikami dotyczące wzajemnych zobowiązań i ochrony interesów oraz czas zobowiązań. W [7] wskazano, że możliwe jest zabudowanie federacji do której łatwo przystąpić i ją opuścić, co więcej – możliwy jest stopniowy rozwój takiej organizacji. W niniejszym opracowaniu przedstawiono niektóre rozwiązania prostego systemu obrony federacyjnej pozbawionego centralnego zarządzania. W najprostszym przypadku taka federacja może powstać tylko dzięki dwustronnym umowom pomiędzy jej niektórymi członkami. Istotą jest sprowadzenie wzajemnych świadczeń federacyjnych do obsługi prostych „zleceń blokowania". Taki system może stać się podstawą obrony przed atakami DDoS w skali kraju.

Przedstawiono również możliwości i narzędzie – model laboratoryjny – do badania zachowania się takich systemów ochrony w warunkach zdalnych ataków. Badania za pomocą nagranego ruchu sieciowego w wybranych systemach można prowadzić bez ingerencji w systemy „produkcyjne" z zachowaniem należytej adekwatności.

2. Domeny i odpieranie ataku DDoS

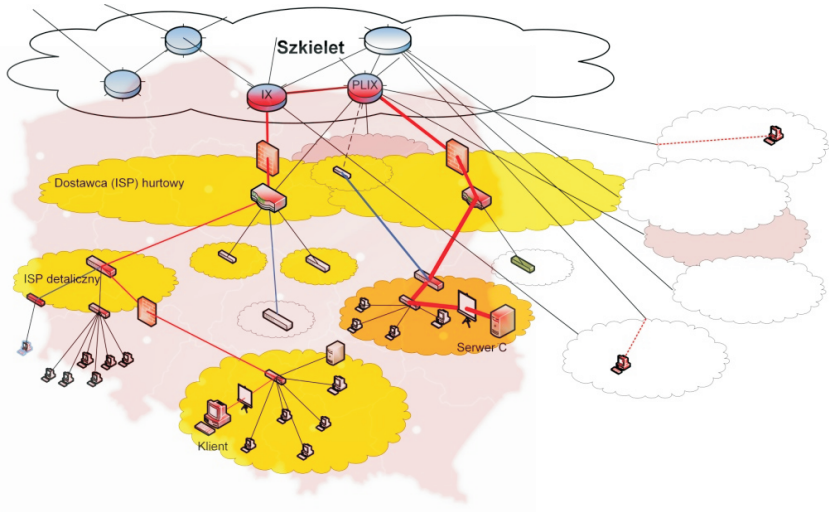
Obecnie sieci telekomunikacyjne stanowiące infrastrukturę Internetu, stanowią połączenie wielu podsieci, których dysponentami (właścicielami i zarządcami) są różne podmioty. Ogólnie za zarządcę podsieci uznaje się podmiot, który legalnie ma prawo podejmować suwerenne decyzje wpływające na ruch sieciowy. Obszary podlegające administracji pojedynczego zarządcy/dysponenta dla których stosuje się wspólną politykę bezpieczeństwa nazwano domenami.

Zarządca domeny zwykle realizuje własną koncepcję utrzymania bezpieczeństwa, dając lub zabraniając dostępu do zasobów informacyjnych oraz zezwalając lub blokując przepływ różnych informacji. Spisany zbiór ogólnych zasad służących z intencji podniesieniu bezpieczeństwa nazywa się polityką bezpieczeństwa. Szczegółowe zbiory zasad sformułowane w sformalizowanej postaci dla poszczególnych urządzeń nazywane są „policy". W przypadku zapór sieciowych mówi się o „konfiguracjach" zawierających „reguły". Zbiory zasad (czy reguł) tworzone są lokalnie w celu zapewnienia bezpieczeństwa interesom podmiotu właścicielskiego. Podmioty administrujące domenami zwykle niechętnie akceptują zasady lub reguły, których celem jest bezpieczeństwo obcych zasobów, obawiając się skutków ubocznych – niekorzystnego wpływu na własne bezpieczeństwo. Wiele podmiotów gospodarczych jest konkurentami na rynku i ma raczej motywację do walki niż współpracy.

Zasoby informacyjne instytucji państwowych oraz ważnych dla życia publicznego organizacji często stają się celem ataków podejmowanych z różnych pobudek: politycznych, terrorystycznych, a także czysto komercyjnych. Szczególnie trudny do ochrony jest atrybut dostępności zasobów informacyjnych. Przyczyną są szerokie możliwości i łatwość wykonywania ataków przeciążeniowych, należących do klasy tak zwanych ataków prowadzących do odmowy usługi (tzw. DoS: *Denial of Service*). Najbardziej rozpowszechnionymi sposobami realizacji ataków DoS są ataki rozproszone *Distributed Denial of Service* (DDoS: [8], [4], [3], [10], liczne opisy można znaleźć w [12]).

Przez atak informatyczny rozumie się celowe oddziaływanie napastnika na zasoby informacyjne ofiary prowadzące do negatywnych skutków dla interesów ofiary. Atakiem zdalnym, albo cyberatakiem nazywa się atak informatyczny, w którym medium takiego oddziaływania jest ruch sieciowy: dane przekazywane między urządzeniami teleinformatycznymi. Na Rys. 1 przedstawiono ilustrację przepływu ruchu sieciowego w trakcie ataków (np. rozproszonych ataków przeciążeniowych DDoS) prowadzonych ze stacji roboczych rozlokowanych w różnych domenach w Internecie (tzw. botnet)

na komputer oznaczony Serwer C. W sieci występują również klienci usług świadczonych przez Serwer C. Można też wskazać domeny o różnych specjalnościach, np. domeny szkieletowe (Tier-1) lub hurtowych/regionalnych i detalicznych/lokalnych dostawców Internetu (Tier-2 i 3).

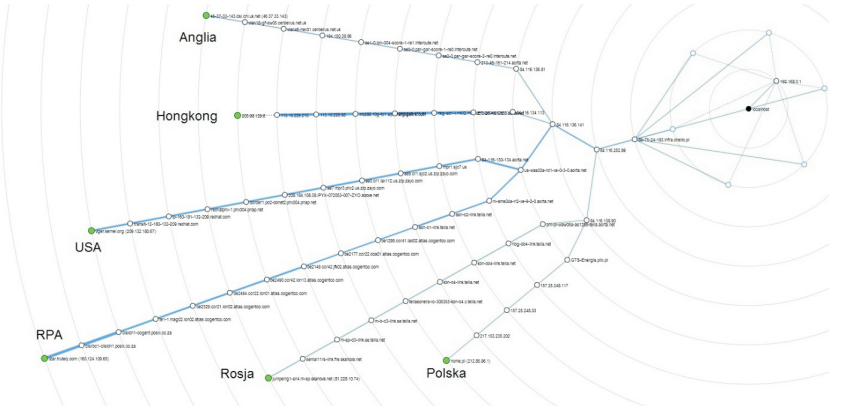


Rysunek 1. Polskie i zagraniczne źródła wrogiego ruchu w ataku DDoS (na Serwer C) w domenach w Internecie

Tradycyjnie te hierarchiczne połączenia wyobrażane są (jak na Rys. 1) jako rodzaj lasu, jednak w rzeczywistości są dużo bardziej skomplikowane, co wynika z tzw. połączeń tranzytowych między operatorami, połączeń peeringowych, oraz grupowania możliwości połączeń peeringowych w tzw. międzyoperatorskich punktach wymiany ruchu (IX). W przypadku ataków zdalnych interesująca jest znajomość tras, którymi wrogi ruch dociera od napastnika do celu ataku. Na szczęście efektywny, aktualny stan połączeń, czyli trasy między poszczególnymi lokalizacjami, można rozpoznać przeprowadzając badanie, np. za pomocą komendy traceroute.

Traceroute odnotowuje jednak tylko urządzenia zmniejszające wartość pola „hops" w pakietach. Spośród przedstawionych na Rys. 2, w Polsce umiejscowione są routery leżące na „polskiej" trasie oraz tylko pierwszych sześć (od źródła „localhost" licząc) routerów na każdej z pozostałych tras. Niestety ten sposób (traceroute) identyfikowania połączeń i tras nie pozwala na rozpoznanie najbardziej interesującej cechy – rozmieszczenia filtrów sieciowych należących do poszczególnych domen. Przez filtry sieciowe

rozumie się wszelkie urządzenia przekazujące ruch sieciowy zdolne do selekcji tego ruchu. Interesujące są urządzenia filtrujące w warstwie trzeciej (L3 modelu ISO/OSI), w tym także listy ACL routerów i routery realizujące tzw. „blackholing".



Rysunek 2. Trasy z localhost" do wybranych lokalizacji wyznaczone za pomocą traceroute: Hongkong, New world telecom (http://www.nwtgigalink.com/lg.html) 203.98.129.6; USA, Level 3 Communications (http://vger.kernel.org/traceroute.html) 209.132.180.67; Anglia, Cerberus Networks Ltd. (http://www.erik.co.uk/lg/) 46.37.33.143; Rosja, TeliaSonera (http://lg.telia.ru/) 81.228.10.74; RPA, TruTeq Wireless (http://services.truteq.com/) 160.124.109.65; Polska, Home.pl (https://home.pl/test) 212.85.96.1

Na Rys. 3 przedstawiono model połączeń międzydomenowych w sieci Internet, zredukowany do elementów interesujących z punktu widzenia obrony federacyjnej pewnego serwera w sieci. Zgodnie z ideą opisaną w [6] wynikającą z założeń obrony przed atakami DDoS, wykrywać ataki trzeba jak najbliżej celu, zaś odpierać je – filtrując ruch – należy jak najdalej od celu. Ten efekt odległego filtrowania, o nazwie „pushback"[4] jest szczególnie ważny w przypadku ataków przeciążeniowych na łącza (nastawionych na tzw. wysycanie pasma). Podkreślić należy, że w dobie powszechnego wykorzystania połączeń SSL (czy TLS) symptomy większości ataków można rozpoznać dopiero w pobliżu celu, gdy pakiety opuszczą już tunel kryptograficzny.

Idea odpierania ataków DDoS dla federacji narodowych zmierza ponadto do tego, by blokowanie ruchu sieciowego adresowanego do atakowanego serwera odbywało się na granicach obszaru wewnątrz którego znaj-

[4] W [10] zaproponowano tę nazwę w 2011 r. prezentując koncepcję podobną do rozwijanej w pracach WAT od 2009 r. ([2], potem [5] itp.).

duje się większość jego klientów. Większość napastników powinna znajdować poza zaporami. Zakłada się wówczas, że federacja jest podobszarem sieci, w którym znajduje się większość klientów chronionych usług. W razie ataku DDoS na cyberprzestrzeń kraju zapewne większość atakujących komputerów będzie poza granicami geograficznymi i poza tą cyberprzestrzenią rozumianą jako domeny zarządzane przez podmioty prowadzące działalność gospodarczą w Polsce.

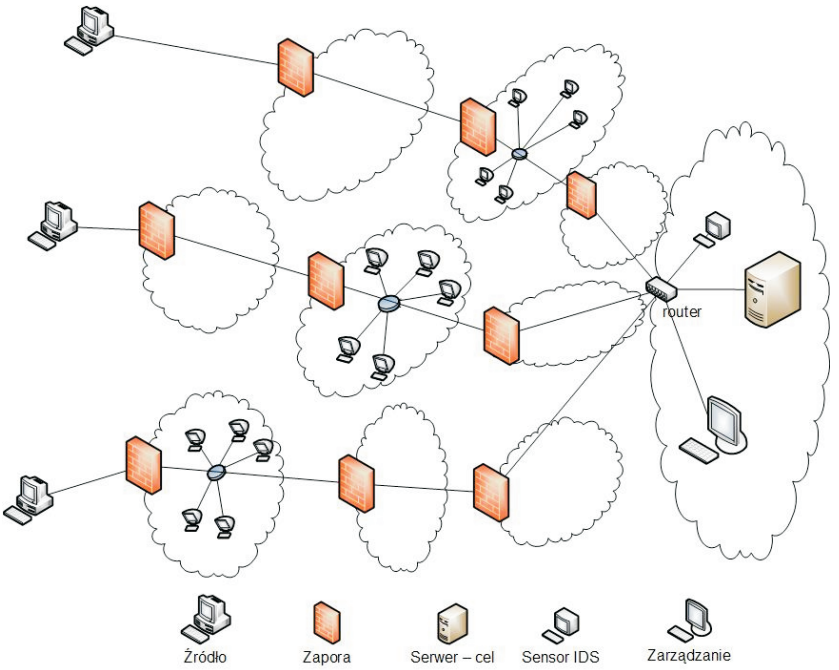
Dla skutecznego odpierania ataku DDoS nie trzeba blokować całego wrogiego ruchu – wystarczy wyciąć go tylko na tyle, aby zniknęło zjawisko przeciążania, tzn. by miara dostępności atakowanych usług osiągnęła minimalną akceptowalną wartość.

W systemie obrony rozpoznawanie ataku odbywa się w pobliżu celu ataku, z wykorzystaniem mechanizmów wykrywania ataków (IDS) pracujących m.in. w warstwie aplikacji serwera. W niniejszym opracowaniu pomija się rozwiązania tych mechanizmów, przyjmując tylko, że na ich wyjściu generowane są reguły dynamiczne z warunkami określanymi dla protokołów w warstwie L3. Te dynamiczne reguły wysyłane są do odległych zapór, na których zachodzić będzie blokowanie ruchu. Np. wykrycie ataku z jakiegoś adresu IP może spowodować wygenerowanie reguły nakazującej blokować pakiety nadchodzące z tego adresu.

Przez regułę rozumie się tu pojedynczą implikację „warunek → reakcja" stanowiącą element tzw. zbioru konfiguracji zapory sieciowej. Konfiguracja jest uporządkowanym zbiorem zadanych reguł. Filtrowanie jednostek ruchu sieciowego (w warstwie L3 – pakietów) polega na sprawdzaniu dla każdej nadchodzącej jednostki kolejnych reguł z konfiguracji. Jeśli któryś z nich jest spełniony, to zostaje zastosowana „reakcja" i sprawdzanie kończy się. Reakcja w dynamicznych regułach generowanych przez IDS to zawsze „drop", czyli zaniechanie przekazania pakietu na interfejs wyjściowy zapory (zablokowanie). Zaznaczyć należy, że to krótkie przypomnienie jest znacznym uproszczeniem i pomija np. oddzielne konfiguracje stosowane dla każdego z interfejsów (zob. [15]).

Pomimo, że środki i sposoby realizacji zaznaczonych na Rys. 3 urządzeń realizujących funkcje generowania reguł nie są tu rozważane, można zasygnalizować, że w ostatecznym przypadku, gdy nie udaje się zidentyfikować ruchu stanowiącego medium ataku a stwierdzono nagłe załamanie się zdolności świadczenia usługi przez serwer można:

— wygenerować reguły blokujące ruch z adresów IP wszystkich nadawców pakietów, które dotarły do serwera w ostatnim czasie przed załamaniem; zabieg ten nie będzie skuteczny w przypadku ataków z fałszowaniem adresu nadawcy (*spoofing*, np. w ataku SYNflood) lub ataków ruchem odbitym (*reflected attacks*);



Rysunek 3. Model poglądowy tras wrogiego ruchu do celu ataku przez zapory poszczególnych domen

— albo wysłać regułę blokującą cały ruch do atakowanej usługi na serwerze niezależnie od adresu nadawcy.

W tym ostatnim przypadku sukces zostanie osiągnięty, jeżeli napastnicy są zlokalizowani głównie poza granicą federacji – blokada nie będzie przeszkadzać klientom wewnątrz FoS. Ceną odparcia ataku będzie odcięcie od usług klientów zlokalizowanych w topologii sieci poza federacją.

Reguły służące do odpierania ataku DDoS przestają być potrzebne po zakończeniu tego ataku. Ogólnie: reguły dynamiczne powinny być szybko aplikowalne i szybko usuwalne. Pewne komplikacje pojawiają się w przypadku ataków o zmiennym natężeniu wrogiego ruchu.

3. Samoadaptująca się konfiguracja zapory

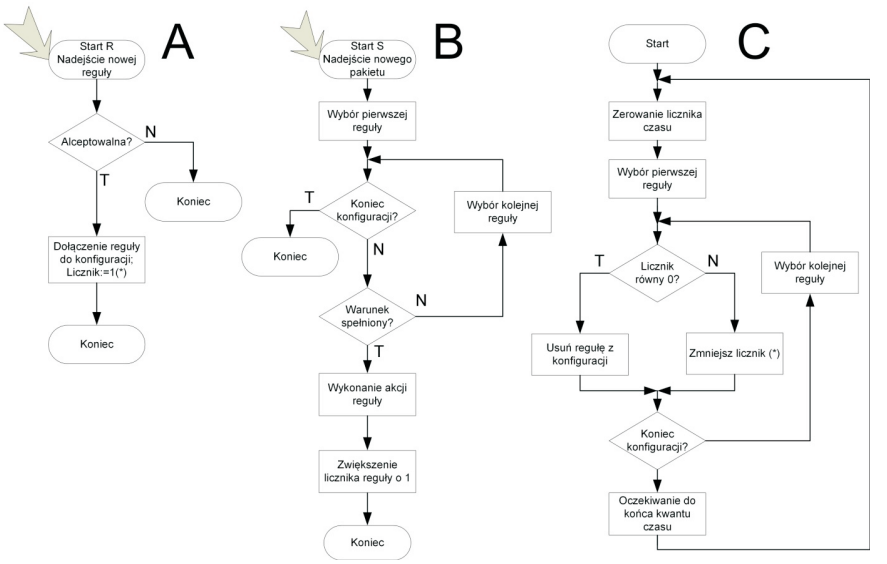
Dla osiągnięcia efektu odsuwania (pushback) filtrowania w domenach skuteczne może okazać się zastosowanie mechanizmu samoadaptującego. Może on polegać na wyłączaniu z konfiguracji zapory tych reguł dynamicz-

nych, których częstość stosowania spadnie poniżej pewnej zadanej wartości progowej. W najprostszej realizacji – gdy w pewnym ustalonym czasie reguła nie zostanie zastosowana ani razu. Przez „zastosowanie reguły" rozumie się wykrycie w ruchu sieciowym informacji spełniającej warunek reguły. To „zastosowanie" każdej reguły może być zliczane a wartość licznika może stanowić podstawę do automatycznego usuwania reguły z zapory. W efekcie reguła znajduje się w konfiguracji zapory tylko tak długo, jak długo na jej podstawie odrzucane są pakiety. Inaczej mówiąc – reguła sama znika z konfiguracji, gdy przestaje być używana. Ten sposób działania ma kilka istotnych zalet:

1. Nie wymaga centralnego sterowania.
2. Zapewnia samoistne zniknięcie reguł, które nie są już potrzebne, bez potrzeby ich odwoływania.
3. Pozwala wykorzystać już istniejące zapory.
4. Pozwala na zachowanie wszystkich dotychczasowych lokalnych reguł (zasad bezpieczeństwa) w tych zaporach i autonomii w decyzjach o zakresie reguł akceptowanych z zewnątrz. Lokalne reguły zapór nie kolidują z regułami dynamicznymi.
5. Daje możliwość stopniowego dołączania (i odłączania) kolejnych podsieci do systemu.
6. Nie wymaga dodatkowych, poza licznikami, mechanizmów oceny efektywności poszczególnych reguł.

Dla sprawdzenia rozwiązania zapory z samoistnym wyłączaniem nieużywanych reguł wybrano system Vyatta ([18]) w wersjach 6.2 i 6.5 (por. [13]). Do tego badania okazał się on całkowicie wystarczający, pomimo zatrzymania jego rozwoju i zamknięciu kodu po przejęciu projektu Vyatta przez firmę Brocade w listopadzie 2012 roku ([20], [11]). W dalszych pracach zapewne bazowym systemem będzie VyOS ([19]) – bezpłatne otwartoźródłowe oprogramowanie z funkcją routera, zbudowane na podstawie Debian Linux. Na Rys. 4 zaprezentowano ogólne algorytmy działań realizowanych przez system zapory po nadejściu nowej reguły (A: zmiana konfiguracji), po nadejściu kolejnego pakietu (B: sprawdzanie reguł) oraz wykonywanego co pewien czas sprawdzania, czy reguły dynamiczne są używane (C: usuwanie nieużywanych reguł).

W przypadku testowanego systemu Vyatta naszkicowany na Rys. 4 algorytm B realizowany jest przez standardowe mechanizmy zliczania spełnień warunku każdej z reguł. Nie wymaga dodatkowego oprogramowania.



Rysunek 4. Przykład związanych z dynamicznymi regułami algorytmów zapory: A – akceptacja nowych reguł; B – sprawdzanie pakietu; C – okresowe badanie aktualności reguł

Wartości takich dopasowań można poznać, wpisując komendę z konsoli Vyatta:

show firewall name FW0 statistics

(gdzie FW0 jest identyfikatorem konfiguracji). Odpowiedź składa się z kolejnych wierszy, każdy dla jednej reguły, gdzie pierwsza liczba w wierszu jest numerem reguły, zaś druga stanowi wartość licznika zastosowań tej reguły. Podobne mechanizmy nie są jakąś szczególną właściwością Vyatta – są udostępniane przez większość urządzeń z listami ACL, ponieważ są wbudowane w iptables. Wywołanie iptables z opcją „-nvL" udostępnia liczniki trafień dla każdej z reguł.

Algorytm A wymaga oprogramowania lokalnego w tych implementacjach, w których wymagane jest badanie akceptowalności, w przeciwnym (także i w testowanym) przypadku za jego realizację wystarczą komendy dopisania nowej reguły wydana w połączeniu SSH. Przez „dołączenie do konfiguracji" należy w takim wypadku rozumieć wprowadzenie reguły do zbioru konfiguracyjnego oraz reorganizację porządku reguł w razie potrzeby. W przypadku Vyatta algorytm A powinien zarządzać również nadawaniem numerów regułom; dla reguł dynamicznych zastosowano numery od

1 do 999, ostatnią regułą jest automatyczna reguła 10000 (z reakcją „drop all); na czas testów wprowadzono regułę o numerze 9999 („accept all").

Algorytm C w testowanych systemach Vyatta wymaga na wstępie włączenia nieskończonej pętli sprawdzania liczników. Ponieważ nie ma specjalnych wymagań czasowych tę operację, nie ma potrzeby budowania specjalnego oprogramowania – wystarczą proste rozwiązania skryptowe. Do testów użyto trzech skryptów:

kwant.sh

```
#!/bin/vbash
#
twhile [ 1 ]; do
cat kwant.cmd | ssh -t -t vyatta@localhost
sleep 15
#sleep 360s
done
```

kwant.cmd

```
show firewall name FW0 statistics | ./sc.sh
clear firewall name FW0 counters
exit
```

sc.sh

```
#!/bin/vbash
#wywolanie: show firewall name FW0 statistics |
            ./ten_skrypt.sh
read x y z
/opt/vyatta/sbin/vyatta-cfg-cmd-wrapper begin
while [ "$x" != "9999" -a "$x" != "10000" ]
do
# echo "regula $x pakietow $y"

  if [ $x -eq $x 2>/dev/null ]  #czy liczba (ign.
                                  komunikat err)
    then
    if [ ! -z $x ]              #czy nie pusty ciag
      then
      if [ $y == "0" ]          #czy zerowy licznik
        then
```

```
          echo "regula $x pakietow $y" #log: usuniecie  \
                                        reguly
          /opt/vyatta/sbin/vyatta-cfg-cmd-wrapper delete  \
          firewall name FW0 rule $x
        fi
      fi
    fi
  read x y z
done
/opt/vyatta/sbin/vyatta-cfg-cmd-wrapper commit
/opt/vyatta/sbin/vyatta-cfg-cmd-wrapper end
```

Należy podkreślić, że przedstawiony sposób realizacji algorytmu C, w postaci skryptów symulujących ręczne wydawanie komend przez połączenie SSH, jest co najmniej mało elegancki, ale za to łatwy w realizacji i dobrze ilustrujący ideę działania. Najmniej rozrzutnym funkcjonalnie rozwiązaniem, nie angażującym warstw pośrednich oprogramowania, wydaje się wykonanie oprogramowania bezpośrednio współpracującego z aplikacją iptables lub wręcz z frameworkiem netfilter ([15]).

W przedstawionym modelu nie uwzględniono środków zapewniających ochronę interesów właściciela zapory przed negatywnymi skutkami przyjęcia „złych" reguł (w algorytmie A). Nie jest to skomplikowany problem – reguły są proste i poddające się sprawdzaniu. Każda nadesłana reguła może być poddana weryfikacji. Zapewne wystarczy sprawdzenie, czy z pewnością oddziaływanie reguły jest ograniczone do wpływania tylko na ruch, którego jedną ze stron (identyfikowaną przez adres źródłowy lub docelowy) jest zleceniodawca reguły. Nie należy oczywiście zapominać o sprawdzeniach syntaktycznych reguł, sprawdzeniach, czy identyczna reguła już nie istnieje lub czy liczba reguł dynamicznych nie osiągnęła dopuszczalnej ze względu na wydajność wartości. Zmiany wartości interwału czasowego (w kwant.sh; w przykładzie ustawiony na 15 sekund) dają możliwość zmian minimalnej częstości zastosowań, przy której reguły są usuwane, a pośrednio ograniczania liczby obecnych w konfiguracji reguł dynamicznych.

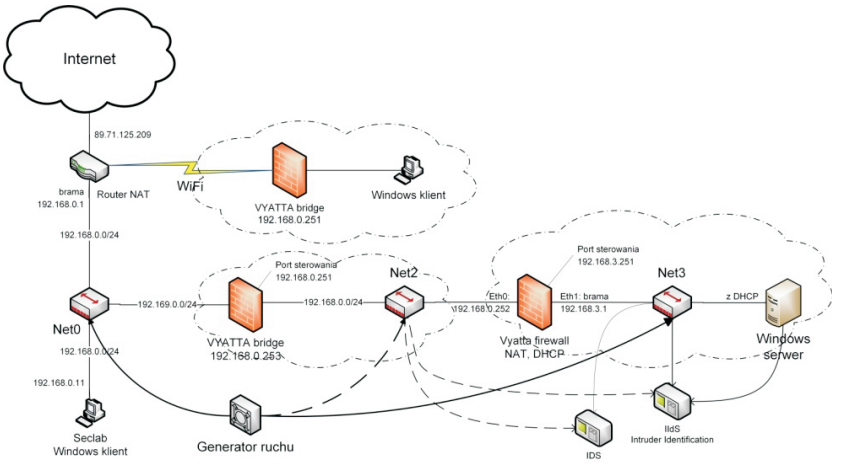
Sprawdzanie funkcjonalne opisanych tu mechanizmów zrealizowano w przygotowanym modelu laboratoryjnym prostych systemów zapór FoS.

4. Model laboratoryjny systemu zapór FoS

Na potrzeby badania rozwiązań rozwojowych systemów FoS dla konkretnych środowisk zbudowano zestaw testowy wykorzystując maszyny wirtualne w systemie VMWare Workstation. Na Rys. 5 przedstawiono model

laboratoryjny systemu FoS, w którym można sprawdzać zachowanie od jednej do trzech zapór takiego systemu, a także budowanych urządzeń IDS i IIdS. Na Rys. 5 badane zapory to systemy Vyatta ([18]) – jeden pracujący w trybie „bridge", drugi w trybie „firewall" z dodatkowymi usługami. Po odłączeniu *Vyatta firewall* i przełącznika Net3 można, wykorzystując połączenia zaznaczone linią przerywaną, badać pojedynczą zaporę (Vyatta bridge). Wszystkie trzy zapory wykorzystano dotąd tylko przy sprawdzaniu, czy zachodzi efekt pushback, przy wprowadzeniu do wszystkich zapór reguł blokowania ruchu wysyłanego z komputerów oznaczonych na Rys. 5 jako „*Windows klient*" do „*Windows serwer*".

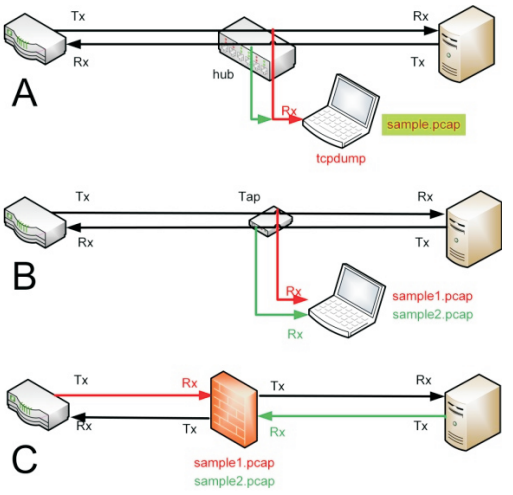
Nie badano jeszcze żadnych rozwiązań IIdS (*Intruder Identification System* – systemu identyfikującego ataki we współpracy z serwerem). Jako IDS (Intrusion Detection System) rozważano zaadaptowany system Snort [16].



Rysunek 5. Schemat modelu laboratoryjnego do testów połączeń szeregowych domen

Bardzo ważną rolę w docelowych badaniach efektywności FoS pełni generator ruchu pokazany na Rys. 5. O ile ruch testowy, symulujący ataki generowany będzie z któregoś z komputerów oznaczonych jako „*Windows klient*" (można na nich w razie potrzeby używać zarówno Windows, jak i Linuxa), o tyle ruch sieciowy stanowiący tło ataku powinien odpowiadać naturalnemu, reprezentatywnemu ruchowi w docelowym środowisku. Ma to szczególne znaczenie dla badań nad mechanizmami wykrywania ataków i generowania reguł (IDS i IIdS na rysunku). Ta możliwość jest również ważna w przypadku zapór działających z analizą stanu (stateful).

Dla zapewnienia adekwatności ruchu generowanego do ruchu oczekiwanego w warunkach rzeczywistych, zaproponowano wykorzystanie zapisu rzeczywistego ruchu zarejestrowanego w odpowiednich punktach obserwacji w docelowym (lub reprezentatywnym wzorcowym) systemie. Sposób pozyskiwania i odtwarzania zapisu ruchu jest technicznie nieskomplikowany i został przedstawiony na Rys. 6 i Rys. 7 odpowiednio.

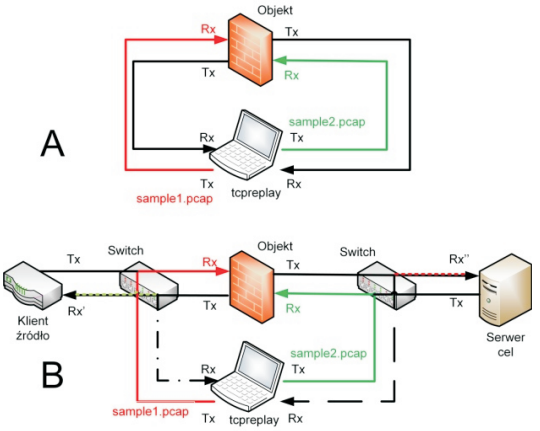


Rysunek 6. Nagrywanie ruchu sieciowego z wykorzystaniem A – huba, B – TAPa, C – routera

Urządzenie rejestrujące powinno być przyłączone do „zewnętrznego", a zatem bardziej odległego od obiektów chronionych, interfejsu zapory sieciowej. Preferowane jest użycie TAPa – neutralnego urządzenia zdejmującego cały ruch sieciowy do rejestracji. Możliwe jest także wykorzystanie właściwości niektórych przełączników (switchów) pozwalających na przekierowanie kopii całego obsługiwanego ruchu sieciowego na tzw. port monitorujący. Na Rys. 6 nie uwzględniono metody zapisu ruchu z portu monitorującego – ten sposób może prowadzić utraty pakietów w momentach szczytowych natężeń ruchu.

Dla ilustracji na Rys. 8 przedstawiono pulpit komputera (z systemem BackTrack[5]) pełniącego rolę generatora ruchu. Jego dwa interfejsy przekazują odtwarzany ruch sieciowy do interfejsów badanego obiektu. Wykorzystano uniwersalne narzędzia uniksowej biblioteki Pcap [17]. Odtwarzany za

[5] Od 2014 r. Kali Linux.



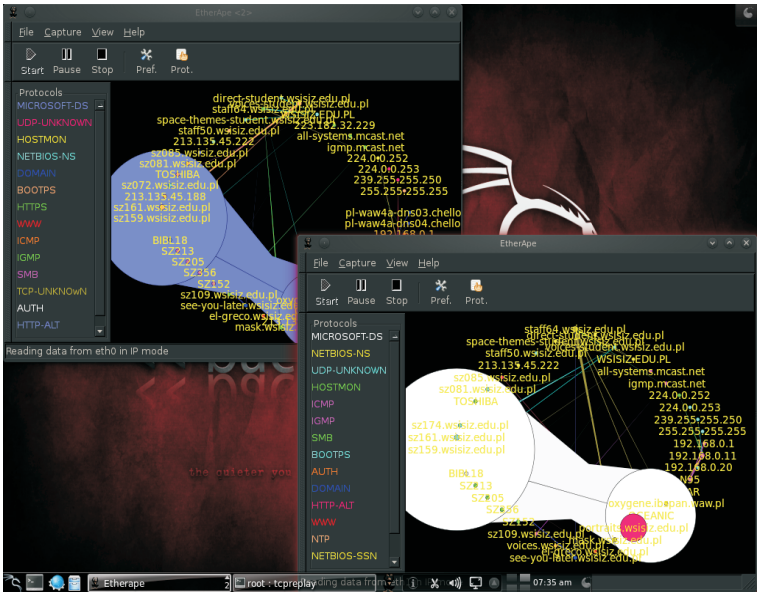
Rysunek 7. Badania z użyciem zapisu ruchu sieciowego: A – jako ruchu testowego; B – jako tła dla ruchu testowego

pomocą programu TCPreplay ruch został wcześniej zapisany za pomocą TCPdump w sieci dydaktycznej jednej z wyższych uczelni warszawskich[6]. Zapis rozdzielono na zapisy poszczególnych interfejsów za pomocą programu TCPprep zapewniając, że pakiety zarejestrowane z linii Tx i Rx zostaną podane na właściwe interfejsy badanego obiektu przybywając doń z odpowiednich kierunków (zob. [17] i [21]).

Na pulpicie pokazanym na Rys. 8 widoczne są dwa okna – dwóch pracujących instancji programu Etherape ([14]). Każda z nich zobrazowuje pakiety widoczne na jednym z interfejsów, zarówno wchodzące, jak i wychodzące. Program Etherape zobrazowuje każdy docierający do interfejsu pakiet w postaci odcinka łączącego dwa punkty na okręgu, przy każdym z punktów zapisywany jest adres (celu albo źródła); barwa odcinka i napisów zależy od protokołu (legenda znajduje się na lewej krawędzi okna) zaś grubość odcinka zależy od objętości przesyłanych danych.

Włączenie rejestracji za pomocą TCPdump w badanym obiekcie (Rys. 7) pozwala na sprawdzenie poprawności odtwarzania – np. za pomocą liczby nadchodzących pakietów. Badanie wykazuje oczywiście zupełną zgodność z liczbą pakietów w odtwarzanym pliku zapisu ruchu.

[6] Wyższa Szkoła Informatyki Stosowanej i Zarządzania.



Rysunek 8. Zobrazowanie odtwarzanego zapisu ruchu sieciowego

5. Użyteczność modelu

Przedstawiony model laboratoryjny pozwolił zweryfikować wnioski o skuteczności uzyskiwania efektu „pushback" i możliwości automatycznego, stopniowego, adaptującego się do siły i przenikalności ataku, odcinania stref sieci.

Model używany w badaniach jest adekwatny do środowisk sieciowych i panujących w nich warunków w miejscu i czasie rejestracji ruchu do badań. Po zebraniu zapisów ruchu sieciowego na „ścieżkach podejścia" od najdalszych osiągalnych w praktyce zapór do chronionego obiektu, można dokonać rzetelnej oceny skutków budowania rozproszonego systemu cyberobrony federacyjnej. Ocena ta pozwoli uzyskać odpowiedzi na pytania interesujące właściciela chronionych obiektów – czy wzięcie udziału w federacji będzie opłacalne i w jakich sytuacjach (głównie dla jakich ataków) obrona FoS może zawieść.

W niniejszym opracowaniu tylko zaznaczono bardzo ważny element zwalczania ataków, jakim jest IDS i/lub IIdS. To te mechanizmy służą do rozpoznawania ataków i generowania niskopoziomowych (w rozumieniu modelu ISO/OSI) dynamicznych reguł dla odległych zapór FoS. W modelu przedstawionym na Rys. 5 można prowadzić badania zachowania się takich

urządzeń. Model pozwala na badania rozpoznawania różnych zdalnych ataków na tle rzeczywistego ruchu zarejestrowanego w różnych środowiskach.

Odpowiedzi na pytania interesujące właściciela ochranianych zasobów mogą być mało użyteczne na potrzeby rozwiania wątpliwości właścicieli domen i zapór pośrednich. Ponieważ będą to zwykle dostawcy Internetu (detaliczni lub hurtowi), dla nich najważniejsze będzie utrzymanie poziomu zapewnianych usług i jak najmniejsze odchylenia od rutyny. Inżynierowie zwykle jak ognia unikają zmiany w działających środowiskach, szczególnie, gdy ich wymagana dostępność musi przekraczać 99,5%. Zasadniczym pytaniem właściciela odległej domeny jest pytanie, czy wprowadzenie „obcych" reguł w jego zaporach lub wręcz cudzych zapór nie spowoduje dostrzegalnych zmian w działaniu okolicznych systemów. W szczególności dysponenta zapory sieciowej interesuje, czy przyjęcie dynamicznych reguł do realizacji nie wpłynie negatywnie na inne rodzaje przekazywanego ruchu. Lub czy taka możliwość w ogóle występuje. W opisywanym modelu badanie neutralności wprowadzanych zmian jest możliwe – wymaga tylko posiadania zapisu reprezentatywnego ruchu w punkcie instalacji zapory. Idea badania jest stosunkowo prosta i polega na rejestrowaniu na wyjściu systemu zapór (np. w komputerze oznaczonym na Rys. 5 jako IDS) charakterystyk ilościowych ruchu: zliczeniu pakietów poszczególnych typów docierających do miejsca pomiaru podczas odtwarzania zapisu. Porównywanie wartości takiego wektora wyznaczonej dla przebiegu bez użycia dynamicznych reguł (wzorcowego) z wartością otrzymaną podczas przebiegu z badanymi regułami pozwala formułować wnioski dotyczące neutralności wprowadzania tych reguł.

Można wyobrazić sobie również badanie neutralności zbliżone do idei „fuzzingu mutacyjnego" znanej z testów bezpieczeństwa oprogramowania czy testów penetracyjnych – polegające na powtarzaniu badania z licznymi, różnymi kombinacjami reguł dynamicznych, nawet pozbawionymi sensownego celu. Jeśli podczas któregoś z takich badań wystąpi nietypowe zachowanie, następuje analiza jego przyczyn.

Z punktu widzenia właściciela zapory groźbę stanowi także zwiększenie liczby reguł, co może prowadzić do przeciążenia zapory i co najmniej zwiększyć opóźnienia w ruchu sieciowym i ich fluktuację (tzw. jitter). Co prawda wykorzystywany w przedstawianym modelu laboratoryjnym program TCPreplay pozwala na odtwarzanie ruchu sieciowego z zachowaniem chronologii pakietów z dużą dokładnością, to jednak nieznany jest wpływ i zakłócenia czasowe wynikające z pracy w środowisku maszyn wirtualnych. Ocena tego wpływu nie została dotąd wykonana.

6. Uwagi końcowe

Zbudowanie modelu zgodnie z Rys. 5 i wykonanie prób z generowaniem ruchu testowego pozwoliło na praktyczne potwierdzenie efektu „pushback" w zaporach sieciowych współpracujących w ramach federacji domen. Potwierdzono również inne przesłanki stanowiące podstawy rozwiązania proponowanego w [6]. Powstały z wykorzystaniem środowiska maszyn wirtualnych model laboratoryjny stanowi tanie i łatwe w obsłudze narzędzie do różnych badań, może zostać wykorzystany do:

— sprawdzenia skutków przyłączenia się do federacji dla kolejnych podmiotów-dysponentów domen;
— badania zdalnych ataków i obrony przed nimi w warunkach rzeczywistego ruchu sieciowego;
— badania skuteczności rozwiązań służących do wykrywania ataków (IDS).

Problemem w prowadzeniu badań jest możliwość pozyskiwania i wykorzystania zapisów ruchu sieciowego. Właściciele sieci komputerowych bardzo niechętnie godzą się na rejestrację ruchu i udostępnianie zapisów obcym podmiotom nawet na potrzeby badań przez nich zleconych. A już w żadnym wypadku nie pozwalają na zachowywanie tych zapisów, ani na użycie ich w innych badaniach. Jest to wynikiem obawy o wrażliwe informacje, które być może znajdują się w zapisach i mogłyby być z nich wydobyte. Formalnie odmowy motywowane są obowiązującą „polityką bezpieczeństwa informacji".

Wnioski z budowy modelu potwierdzają leżące w obszarze rozwiązań technicznych cechy federacji przedstawionej w [6], która:

1. Nie wymaga centralnego sterowania.
2. Pozwala wykorzystać już istniejące urządzenia lub łatwo dodać proste konstrukcje.
3. Zapewnia automatyczne odsuwanie filtrowania tak daleko od celu ataku, jak to możliwe.

Prostota tych rozwiązań pozwala spodziewać się cech tej propozycji istotnych ze względów organizacyjnych:

4. Pozwala zarządcy każdej domeny i zapory na zachowanie lokalnych reguł (zasad bezpieczeństwa) w podsieciach i autonomii w decyzjach o zakresie reguł akceptowanych z zewnątrz.
5. Nie wymaga wielostronnych uzgodnień – między dysponentem domeny zawierającej potencjalny cel ataku, a dysponentem każdej z zapór sieciowych, która ma być używana w FoS powinna zostać nawiązana

umowa dotycząca zlecania reguł. Dysponent zapory udostępnia mechanizm przyjmujący żądania przyjęcia reguł od dysponenta serwera (a właściwie z jego IDS lub IIdS) i wprowadza je do konfiguracji zapory.

6. Daje możliwość stopniowego dołączania (i odłączania) kolejnych domen i podsieci. Dołączenie kolejnej zapory lub jej wycofanie z użytku federacji nie wpływa na innych uczestników federacji poza stronami związanych z tą zaporą umów, nie wprowadza więc dodatkowych biurokratycznych lub prawnych komplikacji.

Podkreślić należy, że zbiór dwustronnych umów już prowadzi do powstania federacji systemów należących do stron tych umów. Nie zamyka to drogi do wprowadzania innych mechanizmów ochronnych, wspólnego sterowania, centralnej dystrybucji najnowszych sygnatur ataków itd.

Minimalnym środkiem do uniknięcia sporów między stronami jest przestrzeganie „zasady własnego ruchu" polegającej na tym, że reguły pochodzące od podmiotu X mogą powodować blokowanie wyłącznie takiego ruchu, który jest generowany z pul adresów należących do X albo jest adresowany do adresów należących do pul adresów, których właścicielem jest X. To, przy odpornym na podszywanie i niezaprzeczalnym protokole przekazywania reguł, wyłącza odpowiedzialność pośrednika - dysponenta zapory, gdyż blokowanie ruchu następuje przez realizację prawa jednej ze stron, której to realizacji pośrednik jest tylko wykonawcą. Możliwe są inne, bardziej rozbudowane modele współpracy federacyjnej, w których dopuszczalne jest generowanie reguł w imieniu i na potrzeby innych podmiotów – bez przestrzegania zasady własnego ruchu. W niniejszym opracowaniu rozważano jednak tylko najprostszy model.

Konkluzją ogólniejszej natury jest spostrzeżenie, że popularne stwierdzenie „W Internecie nie ma granic" jest fałszywe. Po prostu jeszcze nie ma jeszcze wspólnej „CyberStraży" Granicznej.

Literatura

[1] AC/322 – D(2007)0050 – AS1 *Report of the Examination of the lessons learned from the recent Cyber Attacks*, 02 październik 2007.

[2] M. Amanowicz, A.E. Patkowski, *Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w systemach sieciocentrycznych. Metody i techniki ochrony systemu przed działaniami nieuprawnionymi (Cyber Defence)*, Opis zadania badawczego nr 12203. WIŁ 2009.

[3] CISCO, *Defeating DDOS Attacks*, CISCO White Papers, CISCO 2004.
[4] *Four Steps to Defeat a DDoS Attack*, Imperva White Paper, Imperva 2011.
[5] A.E. Patkowski, *Specyfikacja mechanizmów wykrywania działań nieuprawnionych typu DDoS oraz sposobów reagowania na nie w środowisku federacyjnym*, Sprawozdanie z realizacji zadania projektu rozwojowego Nr 0 R00 0125 11: System ochrony sieci teleinformatycznych przed działaniami nieuprawnionymi, WIŁ 2011.
[6] A.E Patkowski, *Cyber Defence – rozproszona obrona przed atakami DDoS*, Biuletyn Instytutu Automatyki i Robotyki nr 31, str. 3–15, Warszawa 2011.
[7] A.E. Patkowski, *Obrona federacyjna cyberprzestrzeni przed atakami terrorystycznymi*, W: "Terroryzm a bezpieczeństwo państwa w erze globalizmu", red.: Jakubczak R., Radziejowski R. WAT, Warszawa 2011.
[8] C. Patrikakis, M. Masikos, O. Zouraraki, *Distributed Denial of Service Attacks*, The Internet Protocol Journal", Vol. 7, No. 4, CISCO, December 2004.
[9] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, *Controlling High Bandwidth Aggregates in the Network*, ACM SIGCOMM Computer Communication Review. Volume 32 Issue 3, July 2002.
[10] T.H. Nguyen, C.T. Doan, V.Q. Nguyen, T.H.T. Nguyen, and M.P. Doan, *Distributed defense of distributed DoS using pushback and communicate mechanism*, In Advanced Technologies for Communications (ATC), 2011 4th International Conference on, pages 178–182, 2011.
[11] *Brocade – Network Provider for Data Centers Everywhere*, http://www.brocade.com/
[12] *Common Attack Pattern Enumeration and Classification*, CAPEC List, http://capec.mitre.org/data/index.html The MITRE Corporation.
[13] *DistroWatch.com: Vyatta*, http://distrowatch.com/table.php?distribution=vyatta
[14] *Etherape. A graphical network monitor*, http://etherape.sourceforge.net/
[15] *netfilter. firewalling, NAT, and packet manglingfor linux*, http://www.netfilter.org/
[16] *SNORT© Users Manual 2.9.7*, The Snort Project, October 13, 2014, http://www.snort.org

[17] *Tcpreplay tcpprep, tcpreplay, tcprewrite, tcpbridge, flowreplay. Pcap editing & replay tools for *NIX*, http://tcpreplay.synfin.net
[18] *VYATTA. The easy tutorial*, WWW.OPENMANIAK.COM, http://openmaniak.com/vyatta.php
[19] *Vyos*, http://vyos.net/wiki/Main_Page
[20] Washi: VyOS – otwartoźródłowy fork Vyatta Core, http://www.virtual-it.pl/5209-vyos-otwartozrodlowy-fork-vyatta-core.html. Virtual-IT.pl. 13.09.2014.
[21] *XModulo. Linux FAQs, tips and tutorials*, http://xmodulo.com/how-to-capture-and-replay-network-traffic-on-linux.html

A LABORATORY MODEL FOR STUDYING FEDERATIONS OF CYBER DEFENSE SYSTEMS

Abstract. The paper outlines the possibility of building the simplest federal defense system against DDoS attacks. It also presents some technical solutions of such a system and presents a not expensive laboratory model for testing its properties and behavior. The adequacy of the model is achieved by using in research a network traffic which has been registered in representative (or target) networks. Some possibilities of tests and to get answers to questions of potential federation participants were indicated.

Keywords: security, cyber attack, DoS, DDoS, domain, federation, adaptation, FoS, IDS, model.