Informatyka techniczna i sztuczna inteligencja
Technical informatics and Artificial Intelligence
Engineer of XXI Century'2024

Practical Methods of Protection Against DDOS Attacks

Bartosz Owczarz [1], Ruslana Ziubina [2]

[1] *University of Bielsko-Biala, 2 Willowa st., Bielsko-Biala, 43-309, Poland*
[2] *University of Bielsko-Biala, 2 Willowa st., Bielsko-Biala, 43-309, Poland, rziubina@ubb.edu.pl*

Abstract: DDoS attacks are one of the most serious threats to modern companies using online services. This article presents an analysis of server security in the Microsoft Azure cloud environment against DDoS attacks. Tests were conducted to evaluate the effectiveness of protection using Network Security Groups (NSG) and additional defensive measures, such as a firewall on a Linux server. The experiment included attack simulations aimed at depleting server resources. Methods of counteraction, including port blocking and identifying attackers' IP addresses, are discussed. The tests confirmed that proper NSG configuration can effectively protect resources, but the introduction of additional tools, such as LoadBalancer, can further enhance defense efficiency in dynamic cloud environments.

Keywords: DDoS, NSG, Server, Microsoft Azure, HTTP;

Praktyczne metody ochrony przed atakami DDOS

Bartosz Owczarz [1], Ruslana Ziubina [2]

[1] *Uniwersytet Bielsko-Bialski, ul. Willowa 2, Bielsko-Biała, 43-309, Polska*
[2] *Uniwersytet Bielsko-Bialski, ul. Willowa 2, Bielsko-Biała, 43-309, Polska, rziubina@ubb.edu.pl*

Streszczenie: Ataki DDoS stanowią jedno z najpoważniejszych zagrożeń dla współczesnych firm korzystających z usług internetowych. Niniejszy artykuł przedstawia analizę zabezpieczeń serwerów w środowisku chmurowym Microsoft Azure przed atakami DDoS. Przeprowadzono testy skuteczności ochrony z wykorzystaniem sieciowych grup zabezpieczeń (NSG) oraz dodatkowych środków obronnych, takich jak zapora sieciowa na serwerze Linux. W ramach eksperymentu wykonano symulacje ataków, które miały na celu wyczerpanie zasobów serwera. Omówiono metody przeciwdziałania, m.in. blokadę portów oraz identyfikację adresów IP napastników. Testy potwierdziły, że odpowiednia konfiguracja NSG może skutecznie chronić zasoby, jednak wprowadzenie dodatkowych narzędzi, takich jak LoadBalancer, może jeszcze bardziej zwiększyć skuteczność obrony w dynamicznych środowiskach chmurowych.

Słowa kluczowe: DDoS, NSG, Server, Microsoft Azure, HTTP;

1. Wprowadzenie

DDoS to jedno z najpowszechniejszych cyberzagrożeń, które mając szeroki zasięg może być wymierzone w różne branże wszelkich rozmiarów na całym świecie. Konkretne firmy, takie jak producenci gier, handel elektroniczny, telekomunikacja są bardziej narażone niż inne, ze względu na swoje zapotrzebowanie na dostęp do sieci publicznej [1].

Ataki DDoS są ukierunkowane na witryny sieciowe i serwery poprzez naruszanie usług internetowych w dążeniu do wyczerpania zasobów aplikacji. Podczas tego typu ataku hakerzy wykorzystują farmę botów lub botnetów, wysyłając do danej witryny internetowej lub usługi, ruch sieciowy i żądania bazujące na najbardziej popularnych protokołach, na przykład typu HTTP. Ogromna ilość zapytań generowana przez boty powoduje zablokowanie dostępu dla zwykłych użytkowników, chcących skorzystać z aplikacji. W rezultacie aktywności działanie serwera może być opóźnione lub

DOI: https://doi.org/10.53052/9788367652292.01

całkowicie zakłócone przez pewien czas ze względu, na zbyt wolne przetwarzanie informacji przez serwer. Ataki DDoS mogą wykorzystywać luki w zabezpieczeniach i być kierowane na dowolny punkt końcowy, który jest dostępny publicznie przez internet. Są na nie podatne zarówno urządzenia osobiste, jak i służbowe [2].

Celem tego badania jest analiza podatności lokalnego serwera na ataki typu DDoS. W artykule przedstawiono pełną konfigurację oraz środki ochrony przykładowej sieci i serwera, a także opisano skutki wywołane takimi atakami. Eksperymenty zostały przeprowadzone w wirtualnym środowisku chmury Microsoft Azure, co pozwoliło zminimalizować ingerencję w działanie fizycznego sprzętu. Wszystkie testy zostały wykonane w kontrolowanych warunkach [3].

2. Przygotowanie środowiska

Aby sprawdzić odporność na ataki DDoS w sieci Microsoft Azure, należy skonfigurować dwa kluczowe elementy, które są podstawą naszych badań. Po pierwsze, trzeba utworzyć sieciową grupę zabezpieczeń (ang. Network Security Group, NSG), która pełni rolę zapory sieciowej w przypadku komunikacji między siecią wirtualną Azure a siecią publiczną. Konfiguracja NSG polega na dodaniu reguł zabezpieczeń , które pozwalają lub blokują ruch sieciowy, zarówno przychodzący (Rys. 1), jak i wychodzący (Rys. 2), dla zasobów platformy Azure oraz sieci publicznej. Każda reguła umożliwia określenie źródła, celu, portu oraz protokołu [4].

Priority	Name	Port	Protocol	Source	Destination	Action
920	NSG-Deny-Inbound-Ko...	Any	Any	192.168.20.0/24	rg-asg	Deny
930	NSG-Deny-Inbound-Oc...	Any	Any	192.168.40.0/24	rg-asg	Deny
940	NSG-Deny-Inbound-O...	Any	Any	192.168.50.0/24	rg-asg	Deny
950	NSG-Deny-Inbound-Pr...	Any	Any	192.168.60.0/24	rg-asg	Deny
960	NSG-Deny-Inbound-inf...	Any	Any	192.168.10.5	rg-asg	Deny
1000	NSG-Allow-Inbound-POP3	110	TCP	Internet	VirtualNetwork	Allow
1020	NSG-Allow-insecure-IMAP	143	TCP	Internet	VirtualNetwork	Allow
1030	NSG-Allow-Inbound-IMAP	993	TCP	Internet	VirtualNetwork	Allow
1040	NSG-Allow-Inbound-SSH	22	TCP	VirtualNetwork	VirtualNetwork	Allow
1050	NSG-Allow-Inbound-UDP-I...	993	UDP	Internet	VirtualNetwork	Allow
1060	NSG-Allow-Inbound-HTTP-I...	80	TCP	Any	VirtualNetwork	Allow
1120	NSG-Allow-Inbound-insecu...	143	UDP	Internet	VirtualNetwork	Allow
1130	NSG-Allow-Inbound-HTTPS	443	TCP	Any	VirtualNetwork	Allow
2000	NSG-Deny-Inbound-FTP	21	TCP	Internet	VirtualNetwork	Deny
2010	NSG-Deny-Inbound-Telnet	23	TCP	Internet	VirtualNetwork	Deny
2020	AllowTagRDPInbound	3389	TCP	VirtualNetwork	192.168.20.4	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Rysunek 1. Reguły przychodzące NSG.

Priority	Name	Port	Protocol	Source	Destination	Action
930	AllowAnyCustomAnyOutbo...	Any	Any	VirtualNetwork	VirtualNetwork	Allow
1000	NSG-Allow-Outbound-DNS	53	UDP	VirtualNetwork	Internet	Allow
1010	NSG-Allow-Outbound-HTTP	80	TCP	VirtualNetwork	Internet	Allow
1020	NSG-Allow-Outbound-HTT...	443	TCP	VirtualNetwork	Internet	Allow
1030	NSG-Allow-Outbound-ICMP	Any	ICMP	VirtualNetwork	VirtualNetwork	Allow
1040	NSG-Allow-Outbound-IMAP	993	TCP	VirtualNetwork	Internet	Allow
1050	NSG-Allow-Outbound-inse...	143	TCP	VirtualNetwork	Internet	Allow
1060	NSG-Allow-Outbound-FTP	21	TCP	VirtualNetwork	VirtualNetwork	Allow
1070	NSG-Allow-Outbound-SMTP	465	TCP	VirtualNetwork	Internet	Allow
1080	NSG-Allow-Outbound-inse...	25	TCP	VirtualNetwork	Internet	Allow
1090	NSG-Allow-Outbound-SSH	22	TCP	VirtualNetwork	VirtualNetwork	Allow
1100	NSG-Allow-Outbound-UDP...	993	UDP	VirtualNetwork	Internet	Allow
1110	NSG-Allow-Outbound-inse...	143	UDP	VirtualNetwork	Internet	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Rysunek 2. Reguły wychodzące NSG.

DOI: https://doi.org/10.53052/9788367652292.01

Po zakończeniu implementacji NSG, kolejnym krokiem jest utworzenie serwera, który będzie celem symulowanych ataków DDoS. W platformie Microsoft Azure konfiguracja maszyny wirtualnej wymaga szczegółowego określenia różnych parametrów związanych z danym urządzeniem. Proces ten obejmuje wybór odpowiedniego systemu operacyjnego, ustalenie wielkości zasobów, takich jak ilość procesorów i pamięci RAM, a także określenie rodzaju i pojemności dysków. Dodatkowo należy przypisać serwerowi adres publiczny, aby umożliwić komunikację z siecią zewnętrzną, co jest niezbędne do przeprowadzenia testów ataków. W tym przypadku zaleca się wybór systemu operacyjnego Linux Debian 24.04, ponieważ zapewnia on stabilność i wydajność, które są kluczowe w kontekście badania reakcji na ataki typu DDoS (Rys. 3-5) [5-6].

Basics

Subscription	Azure subscription 1
Resource group	rg-fw
Virtual machine name	vm-serwer-2
Region	North Europe
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Enable Hibernation	No
Authentication type	Password
Username	Serwer2
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Standard HDD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	rg-vn
Subnet	Serwerownia (192.168.10.0/24)
Public IP	rg-fw-pip-internet
NIC network security group	None
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

Management

Microsoft Defender for Cloud	None
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Enable hotpatch	Off
Patch orchestration options	Image Default

Monitoring

Alerts	Off
Boot diagnostics	On
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Rysunek 3. Podsumowanie konfiguracji maszyny 1

Rysunek 4. Podsumowanie konfiguracji maszyny 2

Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

Rysunek 5. Podsumowanie konfiguracji maszyny 3

Następnie na serwerze skonfigurowano zaporę sieciową (Rys.6), zgodnie z przedstawioną na rysunku konfiguracją. Proces ten realizuje się za pomocą komendy „sudo ufw allow from", która pozwala na definiowanie reguł dostępu do serwera na poziomie lokalnym. Ta zapora stanowi dodatkowy poziom ochrony i może działać jako ostatnia linia obrony

w przypadku zawodności lub obejścia reguł NSG. Dzięki temu serwer zyskuje dodatkową warstwę zabezpieczeń przed nieautoryzowanym dostępem lub atakami pochodzącymi z zewnętrznych źródeł.

```
Serwer@vm-serwer:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
110/tcp                    ALLOW       Anywhere
22                         ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443                        ALLOW       Anywhere
110/tcp (v6)               ALLOW       Anywhere (v6)
22 (v6)                    ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
```

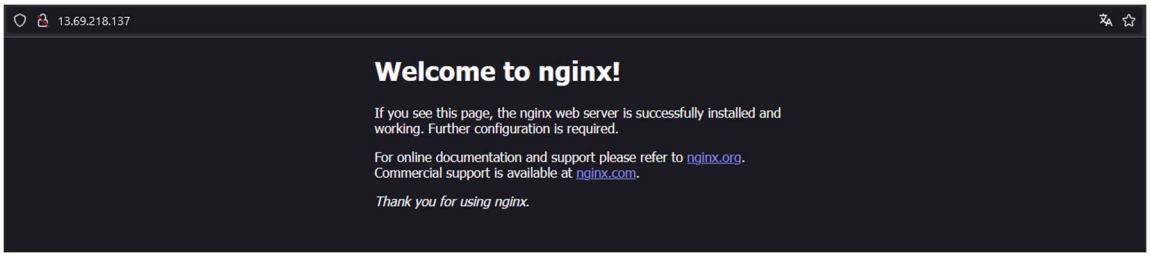
Rysunek 6. Podsumowanie konfiguracji zapory sieciowej serwera Linux Debian 24.04

Po zakończeniu konfiguracji zapory sieciowej, dodano usługę serwera webowego Nginx, co zapewnia istnienie konkretnego zasobu, który może stać się celem ataku. Instalacja i uruchomienie Nginx (Rys. 7-8) pozwala na symulację realnego środowiska, w którym serwer świadczy usługi sieciowe, a tym samym zwiększa realizm przeprowadzanych testów. Dzięki temu możliwe jest obserwowanie, jak ataki typu DDoS wpływają na dostępność usługi oraz jak skutecznie zastosowane zabezpieczenia chronią przed takimi zagrożeniami.

```
Serwer@vm-serwer:~$ sudo service nginx start
Serwer@vm-serwer:~$ service nginx status
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: en>
     Active: active (running) since Sun 2024-10-13 13:08:41 UTC; 6min ago
       Docs: man:nginx(8)
   Main PID: 921 (nginx)
      Tasks: 2 (limit: 4083)
     Memory: 3.2M (peak: 3.7M)
        CPU: 29ms
     CGroup: /system.slice/nginx.service
             ├─921 "nginx: master process /usr/sbin/nginx -g daemon on; master_>
             └─923 "nginx: worker process"

Oct 13 13:08:40 vm-serwer systemd[1]: Starting nginx.service - A high performan>
Oct 13 13:08:41 vm-serwer systemd[1]: Started nginx.service - A high performanc>
lines 1-14/14 (END)
```

Rysunek 7. Podsumowanie instalacji usługi Nginx na serwerze Linux



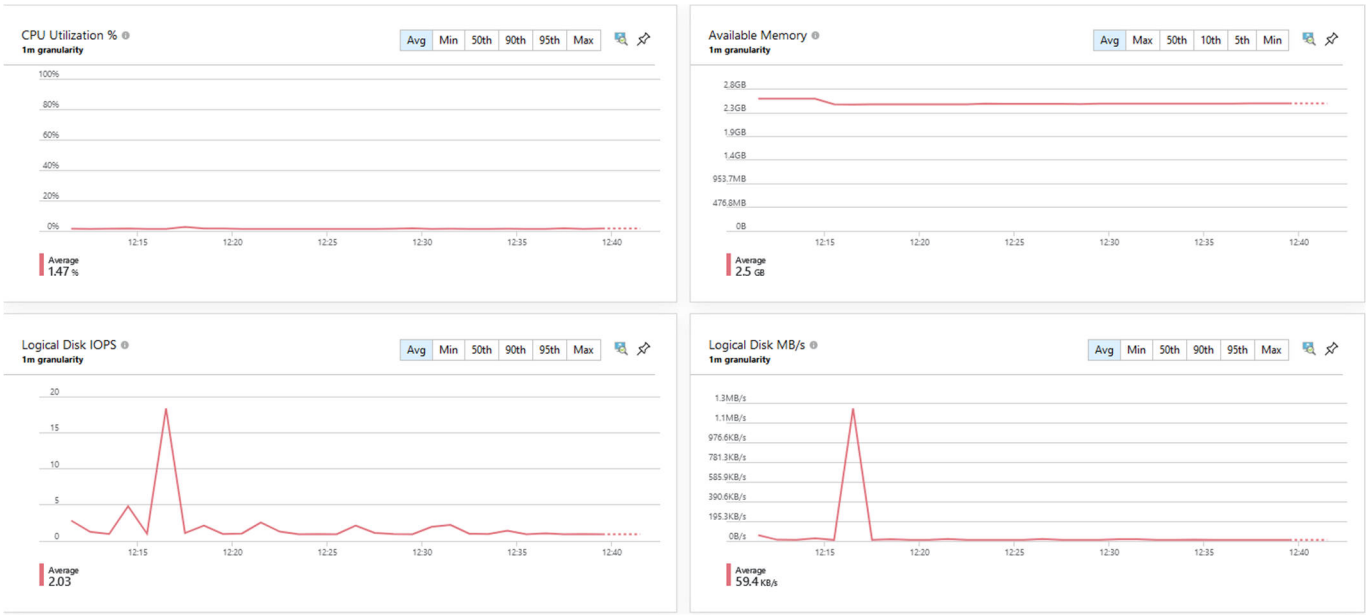
Rysunek 8. Nawiązanie połączenia z serwerem ze strony klienta

3. Testowanie i analiza

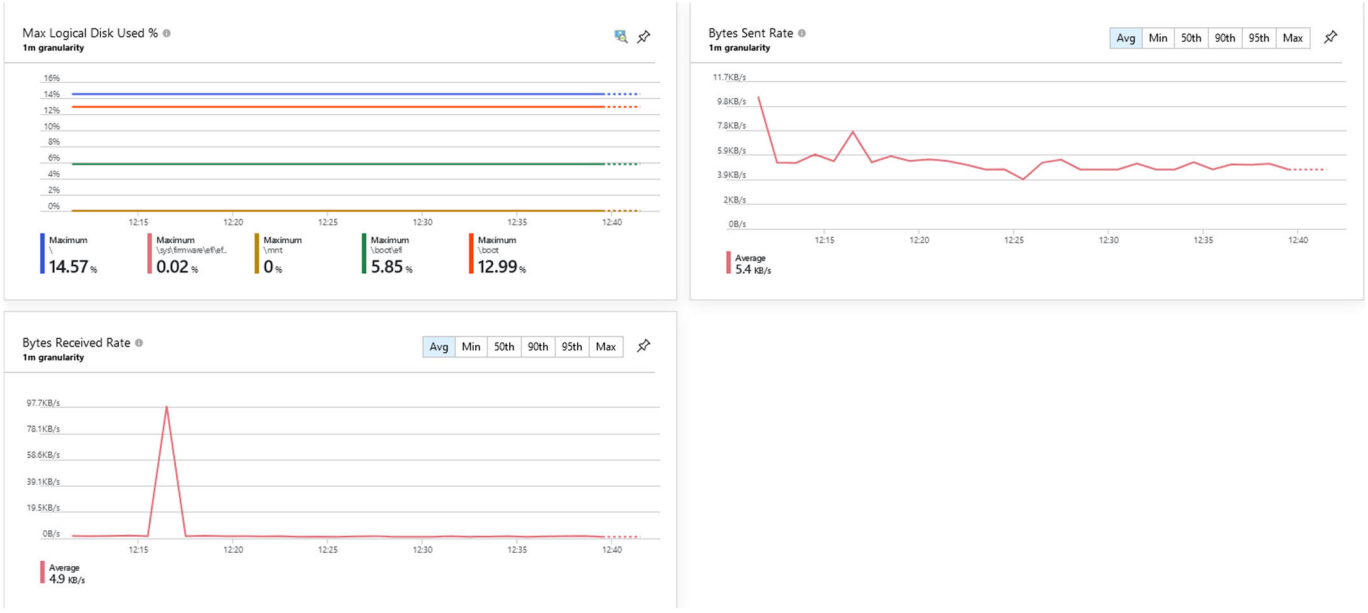
Mając wcześniej utworzone i skonfigurowane zarówno NSG, jak i serwer, przystąpiono do analizy ataków DDoS. W tym celu stworzono program, którego zadaniem było wysyłanie żądań na publiczny adres IP serwera. Ze względu na ograniczenia sprzętowe, użyto jedynie jednego komputera typu PC. Warto jednak zaznaczyć, że dla bardziej precyzyjnych wyników zaleca się wykorzystanie serwera z większą liczbą procesorów lub użycie większej liczby komputerów osobistych, aby symulacja lepiej odzwierciedlała realne warunki ataku DDoS.

Podczas badań zdecydowano podzielić analizę na trzy etapy, aby dokładniej przedstawić różnice w obciążeniu serwera w różnych warunkach pracy.

Pierwszy etap polegał na sprawdzeniu, jak serwer funkcjonuje w normalnych warunkach pracy, bez wpływu ataków (Rys. 9-10). Analizowane były takie parametry jak obciążenie procesora oraz ilość danych przesyłanych do serwera. Celem tego etapu było uzyskanie punktu odniesienia, który pozwoli ocenić skutki przyszłych ataków.



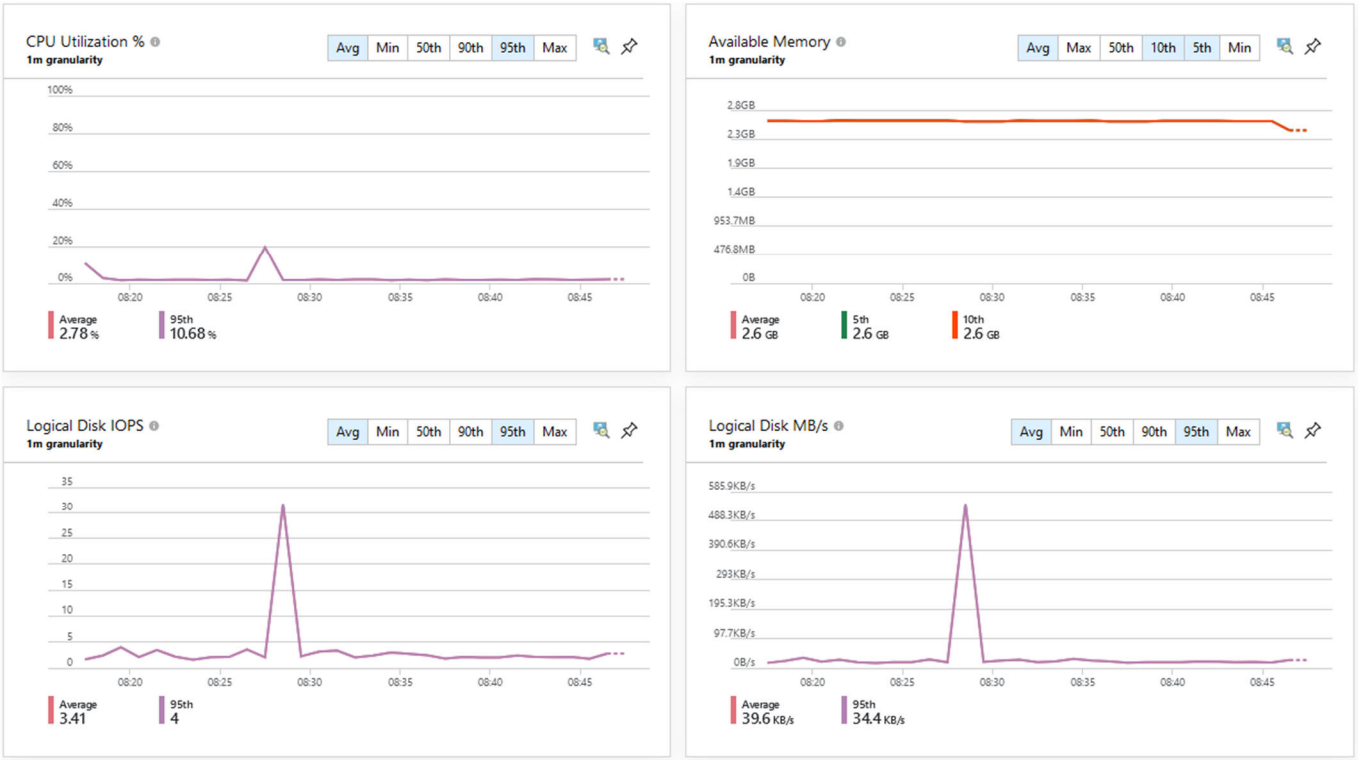
Rysunek 9. Wyniki z metryki serwera podczas normalnej pracy 1



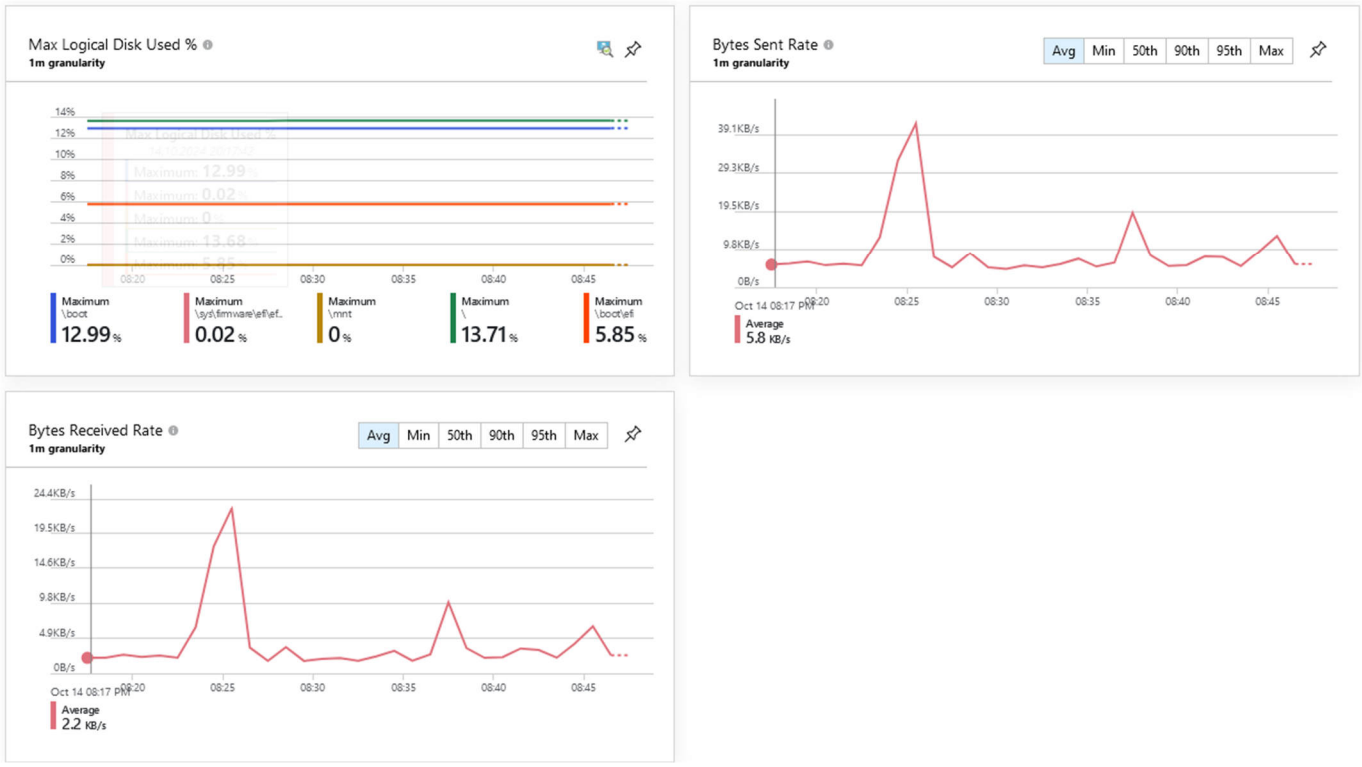
Rysunek 10. Wyniki z metryki serwera podczas normalnej pracy 2

W tym etapie przedstawiono obciążenie serwera podczas jego normalnej pracy, bez żadnych ataków. Analiza wykazała, że jedyne wahania parametrów pojawiają się na samym początku, w trakcie uruchamiania urządzenia. Wówczas zużycie zasobów, takich jak procesor i pamięć, może być chwilowo wyższe. Po zakończeniu procesu rozruchu serwer działa stabilnie, a obciążenie utrzymuje się na stałym, niskim poziomie, co stanowi punkt odniesienia do późniejszych etapów analizy, gdy zostaną symulowane ataki.

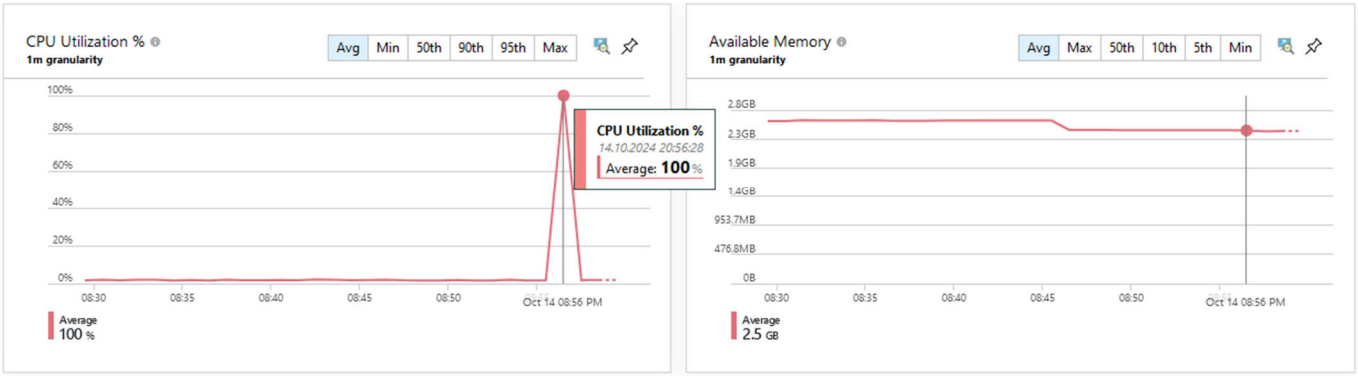
Drugi etap polegał na sprawdzeniu, jak serwer radzi sobie podczas intensywnego ataku DDoS. W tym celu uruchomiono specjalnie zaprogramowany skrypt symulujący atak DDoS, który wysyłał dużą liczbę żądań na publiczny adres IP serwera w krótkich odstępach czasu. Celem tego etapu było zbadanie, w jaki sposób atak wpływa na wydajność serwera oraz jak skutecznie zastosowane środki ochrony, takie jak NSG i zapora sieciowa, radzą sobie z dużym napływem żądań (Rys.11-12).



Rysunek 11. Wyniki z metryki serwera podczas pierwszego DDoSa 1



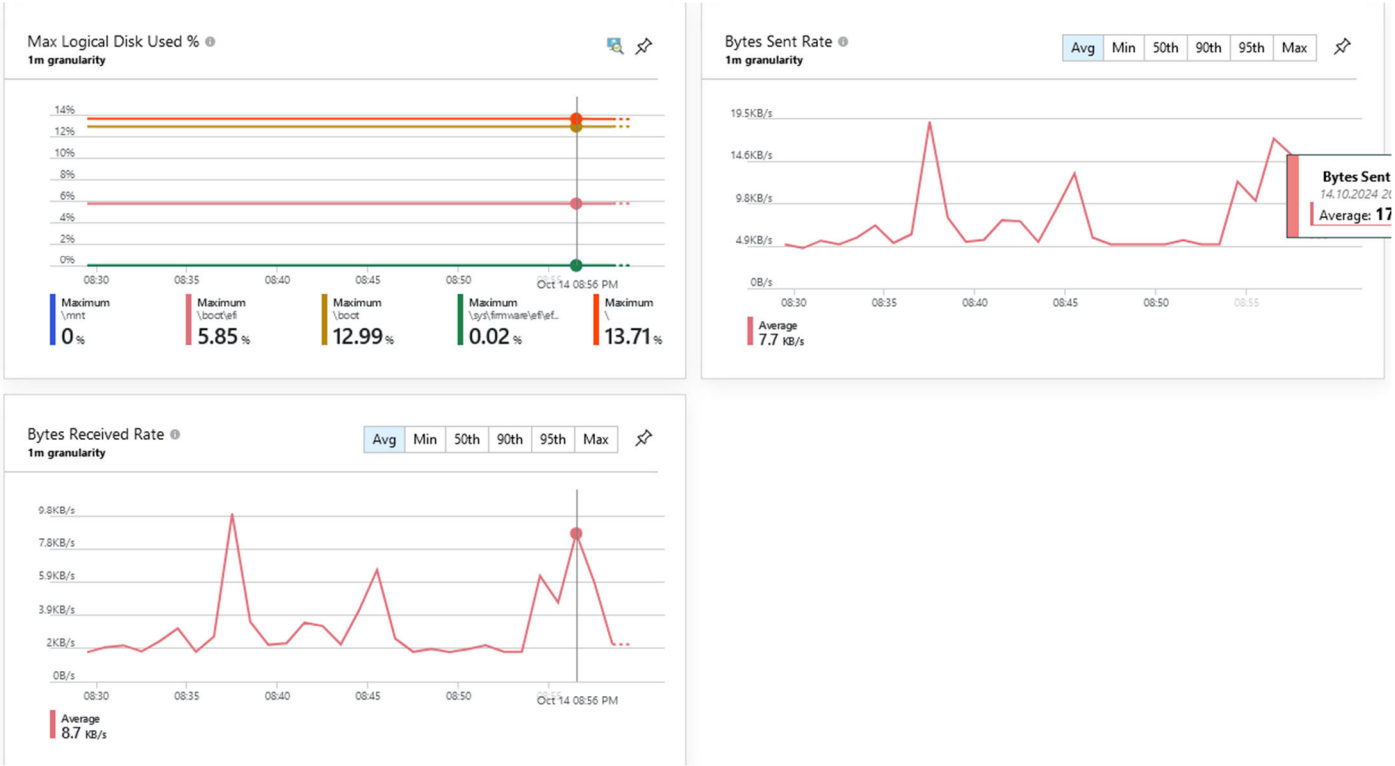
Rysunek 12. Wyniki z metryki serwera podczas pierwszego DDoSa 2



Rysunek 13. Wyniki z metryki serwera podczas drugiego DDoSa 1

W przypadku pierwszego DDoSa nie stwierdzono większych szkód. Zużycie procesora sięgało jedynie 20%, a wielkość otrzymywanych danych była na poziomie 8,7 KB/s. Ten atak może zostać potraktowany przez zabezpieczenia serwera jak i informatyka obsługującego serwer, za standardową pracę tej maszyny. Nie wyróżnia się to niczym od normalnego trybu wykonywania zadań.

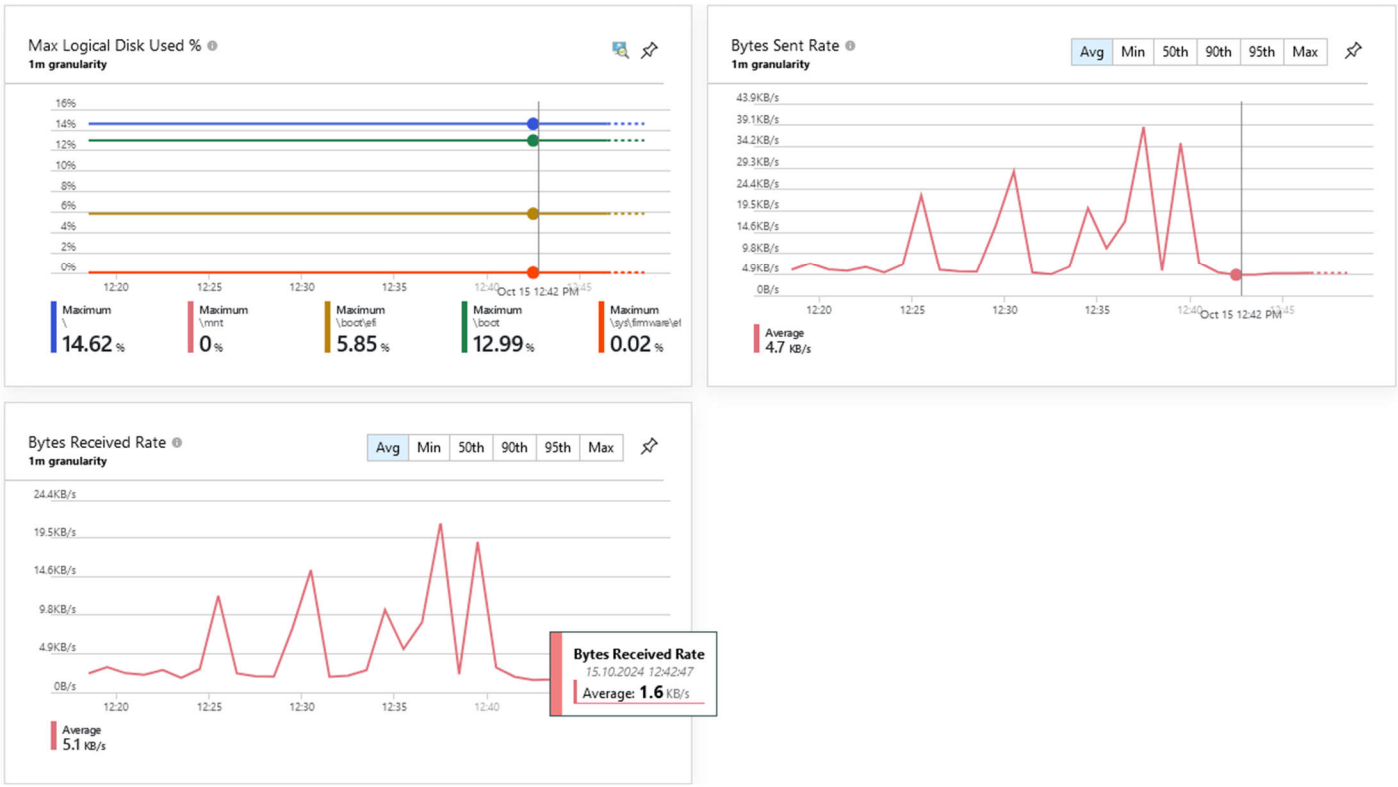
Natomiast drugi atak (Rys. 13-14) przyniósł zdecydowanie bardziej zauważalne rezultaty. Zużycie procesora wzrosło do 100%, a prędkość pobierania danych wyniosła 8,7 KB/s. W rezultacie udało się skutecznie zablokować działanie serwera, co znacząco ograniczyło jego zdolność do przetwarzania żądań i pobierania danych.



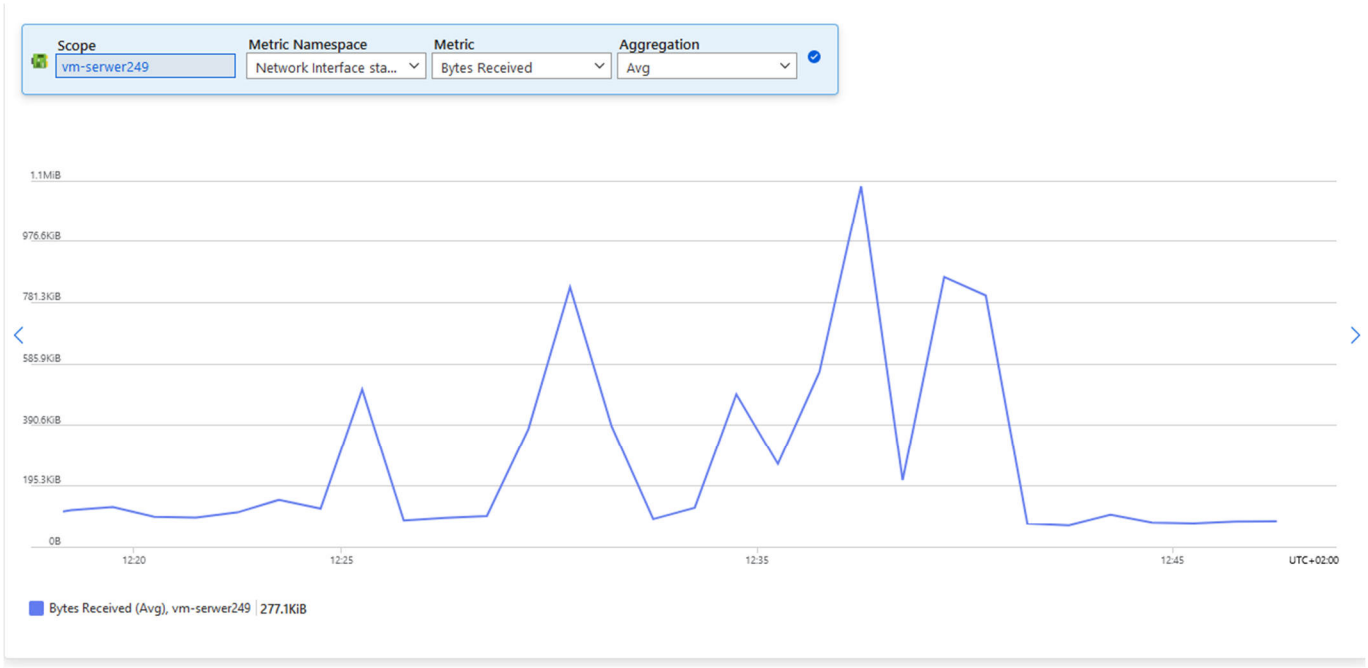
Rysunek 14. Wyniki z metryki serwera podczas drugiego DDoSa 2

Trzeci etap polegał na rozwiązaniu problemu ataków DDoS poprzez zablokowanie portu 80 (HTTP) w NSG. Blokując ruch przychodzący na serwer dla tego protokołu, możliwe było szybkie zatrzymanie niechcianej aktywności związanej z atakiem. NSG oferuje możliwość blokady ruchu zarówno od konkretnego adresu IP, jak i wszystkich przychodzących połączeń do sieci lokalnej. W ramach testów zdecydowano się na blokadę wszystkich adresów IP, co natychmiast

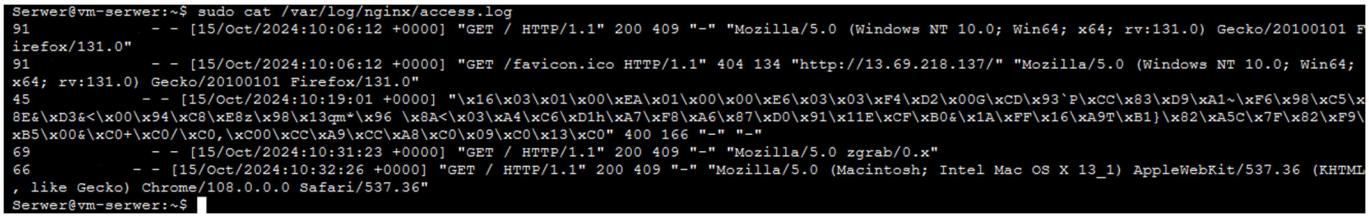
przerwało dostęp do serwera na porcie 80 i skutecznie zatrzymało atak. Tego rodzaju podejście stanowi szybki i efektywny sposób przeciwdziałania atakom DDoS, które wykorzystują otwarty port HTTP.



Rysunek 15. Wyniki z metryki serwera podczas blokady portu 80



Rysunek 16. Wyniki z metryki karty sieciowej serwera podczas blokady portu 80



Rysunek 17. Adresy IP urządzeń nawiązujących połączenie z serwerem

W tym etapie zaprezentowano sposób radzenia sobie z atakiem DDoS poprzez zablokowanie portu 80 dla konkretnego adresu IP lub lub wszystkich przychodzących połączeń. W metrykach (Rys. 15-16) widać natychmiastowe załamanie w pobieraniu danych na serwer, co oznacza szybkie odcięcie ruchu przychodzącego. Jest to szybki sposób, ponieważ wymaga od użytkownika zastosowania tylko jednej blokady w NSG, bez konieczności pisania skomplikowanych komend.

W przypadku znalezienia konkretnego adresu IP atakującego (Rys. 17) zaleca się użycie pliku logowań usługi Nginx, przy pomocy komendy "sudo cat /var/log/apache2/access.log". Zapewnia to użytkownikowi dostęp do wszystkich adresów IP komputerów, mających nawiązane połączenie z atakowanym serwerem.

4. Wnioski

Ataki typu DDoS stanowią istotne wyzwanie w dziedzinie cyberbezpieczeństwa. Duże prosperujące firmy posiadające swoje własne serwery mogą często padać ofiarą tego typu ataków. W związku z tym przedsiębiorstwa wynajdują coraz to nowe sposoby radzenia sobie z tym problemem. W trakcie pracy należy też rozróżniać, czym różni się atak DDoS od zwyczajnego przepływu ruchu sieciowego. Nie można porównywać sytuacji, gdy serwer firmowy odczuwa napływ wielu nowych klientów chcących załatwić swoje sprawy z nagłym i niekontrolowanym zablokowaniem łącza ze stronu kilku komputerów. Trzeba dobierać metody radzenia sobie z tym problemem, proporcjonalnie do rozmiaru szkód wyrządzanych przez atakującego.

Zaprezentowany powyżej sposób obrony przed atakiem DDoS jest autorskim rozwiązaniem, które można zastosować wyłącznie w środowisku chmurowym Microsoft Azure, ponieważ technologia ta oferuje sieciowe grupy zabezpieczeń (NSG), umożliwiające blokowanie przychodzącego i wychodzącego ruchu na podstawie adresów IP i portów. Blokadę portów w NSG cechuje łatwość implementacji z powodu braku zastosowania skomplikowanych komend lub procedur, ponieważ jedyne co należy wiedzieć to adres publiczny atakującego. Dodatkową zaletą jest prędkość przeprowadzanej operacji, bo znając adres IP można szybko utworzyć dodatkową regułę w NSG blokującą ruch na konkretnym porcie.

Jednakże blokowanie portu 80 dla wszystkich połączeń ma swoje wady. Główną z nich jest czasowa niedostępność serwera dla legalnych użytkowników, którzy nie są związani z atakiem DDoS. To może spowodować, że klienci zniechęcą się do korzystania z usług firmy i zdecydują się na ofertę konkurencji. Dlatego warto skonfigurować NSG w taki sposób, aby blokować ruch tylko z konkretnego adresu IP, a nie globalnie na wszystkich połączeniach.

W celu uniknięcia niepożądanych problemów z blokadą portu 80, istnieje możliwość konfiguracji narzędzia LoadBalancer, będącym implementacją protokołu STP dla Microsoft Azure. Jego teoretycznie działanie opierałoby się na równoważeniu przepustowości łącza między serwerem głównym a podrzędnym, dzięki czemu dałoby się zmniejszyć wpływ ataku DDoS na serwer główny.

Bibliografia

1. Microsoft Azure Documentation. Available online: https://learn.microsoft.com/pl-pl/azure/virtual-network/network-security-groups-overview (accessed on 17 October 2024).

2. DigitalOcean Community. How to Set Up a Firewall with UFW on Ubuntu. Available online: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu (accessed on 17 October 2024).
3. Wikipedia. DDoS. Available online: https://pl.wikipedia.org/wiki/DDoS (accessed on 17 October 2024).
4. Microsoft. What is a DDoS Attack? Available online: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-ddos-attack (accessed on 17 October 2024).
5. NGINX Documentation. Available online: https://nginx.org/en/ (accessed on 17 October 2024).
6. DigitalOcean Community. Nginx Access Logs and Error Logs. Available online: https://www.digitalocean.com/community/tutorials/nginx-access-logs-error-logs (accessed on 17 October 2024).