- Koszalin 2021 -

T: Konfiguracja zapory sieciowej w systemie Windows.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat zapory sieciowej.

Zadania oprogramowania firewall:

- filtrowanie i analiza pakietów jeśli otrzymam taki pakiet, to...,
- blokowanie protokołów lub zawartości,
- autoryzacja użytkowników i szyfrowanie połączeń oraz sesji.

Narzędzie do konfiguracji Zapory systemu Windows odnajdziemy w panelu sterowania lub uruchomimy poleceniem:

control firewall.cpl

Sterowanie stanem usługi Zapora systemu Windows w czasie rzeczywistym:

- konsola Usługi z Narzędzi administracyjnych z Panelu sterowania (services.msc),
- polecenie konsoli tekstowej:

```
tasklist /svc
net stop "Zapora system Windows"
net start mpssvc
netsh firewall set opmode disable (mode offline | enable)
sc config mpssvc start = disable
```

Zadanie2:

Zapoznaj się z dostępnymi opcjami konfiguracyjnymi w narzędziu Zapora systemu Windows. Sporządź na ten temat krótką notatkę w zeszycie.



Konfiguracja zapory systemu Windows również jest możliwa poprzez edytor Zasad grupy (gpedit.msc). Przykładowe wpisy do konfiguracji wyjątku portów:

20:tcp:192.168.11.0/24:disabled:blokada ftp-data 23:tcp:192.168.27.2:enabled:telnet dla s27nau 21:tcp:*:enabled:ftp dla wszystkich

Po dokonaniu konfiguracji zapory sieciowej konieczne jest odświeżenie zasad zabezpieczeń lub ponowne uruchomienie systemu Windows.

gpupdate /force

Zadanie3:

Zapoznaj się z dostępnymi ustawieniami dotyczącymi zapory systemu Windows w edytorze zasad grupy. Sporządź na ten temat krótką notatkę w zeszycie.

Tomasz Greszata

- Koszalin 2021

🚡 Zasady grupy			
Zasady grupy Pik Akcja Widok Pomoc Image: Constraint of the system o	Ustawienie Zapora systemu Windows: chroń wszystkie połączenia sieciowe Zapora systemu Windows: nie zezwalaj na wyjątki Zapora systemu Windows: zdefiniuj wyjątki programów Zapora systemu Windows: zezwalaj na wyjątki programów lokaln Zapora systemu Windows: zezwalaj na wyjątki programów lokaln Zapora systemu Windows: zezwalaj na wyjątki programów lokaln Zapora systemu Windows: zezwalaj na wyjątki protokołu ICMP Zapora systemu Windows: zezwalaj na wyjątki protokołu ICMP Zapora systemu Windows: zezwalaj na wyjątek pulpitu zdalnego Zapora systemu Windows: zezwalaj na wyjątek pulpitu zdalnego Zapora systemu Windows: zezwalaj na wyjątek nchitektury UPnP Zapora systemu Windows: zezwalaj na wyjątek architektury UPnP Zapora systemu Windows: zezwalaj na rejestrowanie Zapora systemu Windows: zezwalaj na wyjątki portów Zapora systemu Windows: zezwalaj na wyjątki pottów	Stan Nie skonfigurowano	
 Harmonogram pakietów QoS Protokół SNMP Usługa inteligentnego transferu w tle Drukarki Konfiguracja użytkownika 	Zapora systemu Windows: zezwalaj na wyjątki portów lokalnych	Nie skonfigurowano	
Kuzszerzony Standardowy /			

Zadanie4:

Utwórz prezentację w programie MS PowerPoint na temat konfiguracji Zapory systemu Windows. Pracę zachowaj w pliku pod nazwą **\$nazwisko_\$klasa_\$gr_firewall.ppt** i prześlij pocztą elektroniczną do nauczyciela w postaci załącznika na adres <u>greszata@zs9elektronik.pl</u>. W prezentacji zachowaj estetykę i jednolite przejścia wszystkich slajdów, bez animacji niestandardowej. Poszczególne slajdy powinny zawierać elementy graficzne. Prezentacja powinna zawierać następujące elementy:

- slajd początkowy (przedstawienie tytułu i autora prezentacji),
- slajd wprowadzający (wyjaśnienie pojęcia firewall),
- metody uruchamiania Zapory systemu Windows,
- wyjaśnienie konfiguracji Ogólnej,
- wyjaśnienie konfiguracji Wyjątków z przykładami,
- wyjaśnienie konfiguracji Zaawansowanej,
- konfigurację zapory sieciowej poprzez edytor Zasad grupy z przykładami,
- przedstawienie przykładowego wpisu w dzienniku zapory,
- podsumowanie, wnioski, wskazania,
- slajd zakończeniowy.

Zapora sieciowa Internet Security and Acceleration Server 2004 dostępna w systemach Windows 2003 Server (SBS) umożliwia profesjonalną kontrolę dostępu użytkowników do sieci. Definiowane reguły pozwalają na wykorzystanie następujących składników danych przesyłanych przez sieć:

- adresy sieciowe źródłowe lub docelowe domenowe lub IP,
- czas działania podawany w godzinach i dniach tygodnia,
- typy plików na podstawie rozszerzenia lub realizowanego zadania,
- nazwy użytkowników lub grup użytkowników,
- protokoły sieciowe oraz numery portów usług sieciowych.

Zdefiniowane reguły można w dowolnym momencie wyłączyć lub włączyć. W przypadku blokowania połączeń możliwe jest przekierowanie sygnału np. do innego komputera.

Okno konfiguracyjne zapory sieciowej ISA Server 2004 oraz konfiguracja rejestrowania zdarzeń zapory:

http://greszata.pl

🖽 Microsoft Internet Secu	rity and Acceleration Server 2004		_ 🗆 ×
<u>Plik Akcja W</u> idok Pomo	5		
← → 🗈 🖬 😫 🖄	i i i i X → C * * Q S		
BSS2005	Microsoft Internet Security & Acceleration Server 2004 Standard Edition		Firewall Policy
Virtual Private Net	Firewall Policy		Toolbox Tasks Help
B.X. conigration	0 Name	Action Protocole	Protocols
	🗉 💽 42 tomek i nauczyciele - przychod 🏪	imek - blokada internetu dla sali 27 Properties Y 🔀	Users 🛞
	🗉 📆 41 🛛 tomek - blokada internetu dla s	General Action Protocols From To	New Edit Delete
	🗉 👔 40 🛛 tomek - blokada internetu dla s	Users Schedule Content Types	nacownia 🔺
	🗑 🕐 39 Pozwalam na użycie komndy PI	This rule applies to requests from the following user sets:	nracownia_localuser
	38 Pozwalam pa powrót komprty P		SBS Internet Users
	27. doctor a lon do chr	Add	System and Network Service
		A 620106	🏝 ti2010a
	36 dostep z sos do lan	A ti2011a Berrove	ti2010b
		2011b	2 ti2011a
	34 SBS Localhost Access Rule		u 🏝 ti2011b
	🚺 33 SBS Localhost Dhcp Access Rul		ti2012a
	💽 32 SBS Smtp Outbound Access Ru		A20120
	1 SBS POP3 Outbound Access Ru		🦰 ti2013b
	30 SBS NNTP Outbound Access Ru	Add,	a tomek.
	29 SRS Smith Server Access Bule	Edit	tor2012
	28 SPS DDTD Outbound Access Du		🐣 uprzywilejowani 🖉
	20 305 PF IF Outbound Access Ru	Remoye	Content Types 🛞
	27 SBS RDP Outbound Access Rul		Schedules
	SRS RDP Server Access Rule		Network Objects 🛞
Sotowe		OK Anuluj Zastosuj	

Okna konfiguracji Zapory systemu Windows:



Wyłączenie systemowej Zapory Windows Defender poprzez edytor rejestru:

regedit => hklm\system\currentcontrolset\services => SecurityHealthService => start = 4/2