

Laboratorium 7

Temat: DMZ – strefa zdemilitaryzowana

SPIS TREŚCI

1. Streszczenie.....	3
2. Tworzenie nowego projektu.....	4
3. Tworzenie i konfigurowanie sieci.....	6

1. Streszczenie

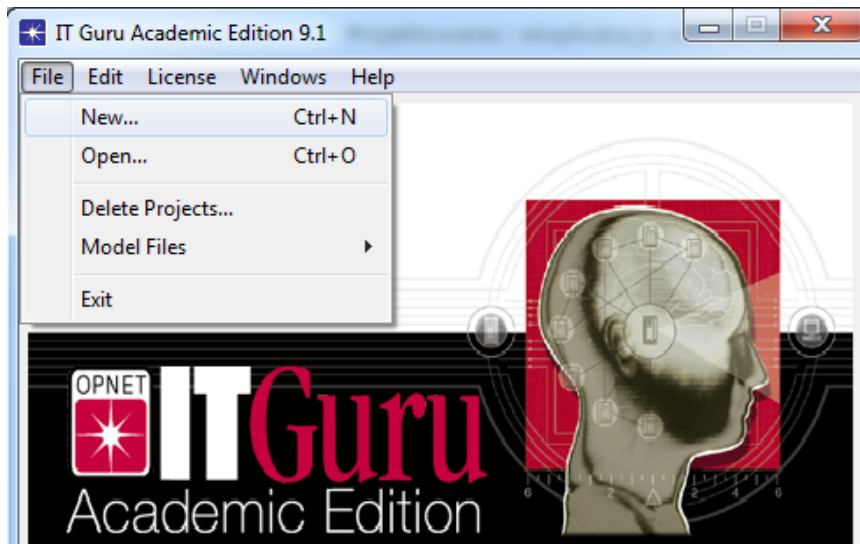
Demilitarized zone (DMZ), strefa zdemilitaryzowana bądź ograniczonego zaufania – jest to wydzielany na zaporze sieciowej – *firewall*, obszar sieci komputerowej nie należący ani do sieci wewnętrznej czyli chronionej przez zaporę, ani do sieci zewnętrznej (tej przed zaporą). W strefie zdemilitaryzowanej umieszczane są serwery "zwiększonego ryzyka włamania", przede wszystkim serwery świadczące usługi użytkownikom sieci zewnętrznej, którym ze względów bezpieczeństwa nie umożliwia się dostępu do sieci wewnętrznej (najczęściej są to serwery WWW i FTP).

W strefie zdemilitaryzowanej umieszczane są także te serwery usług świadczonych użytkownikom sieci wewnętrznej, które muszą kontaktować się z obszarem sieci zewnętrznej (serwery DNS, proxy, poczty i inne), oraz serwery monitorujące i reagujące na próby włamań *IDS- Intrusion Detection System*.

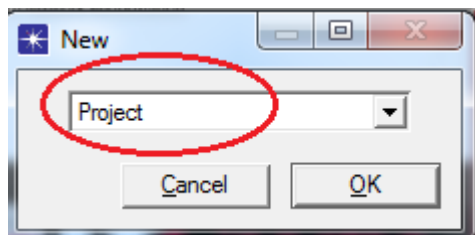
W przypadku włamania na serwer znajdujący się w strefie DMZ intruz nadal nie ma możliwości dostania się do chronionego obszaru sieci wewnętrznej.

2. Tworzenie nowego projektu

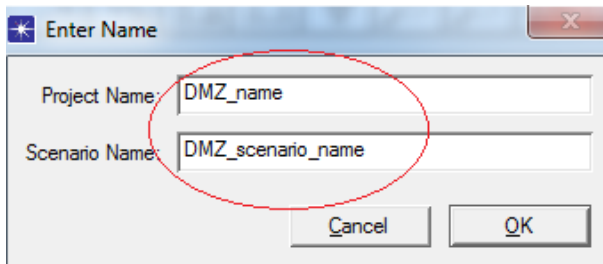
1. Uruchom **OPNET IT Guru Academic Edition**. Z menu **File** wybierz **New**.



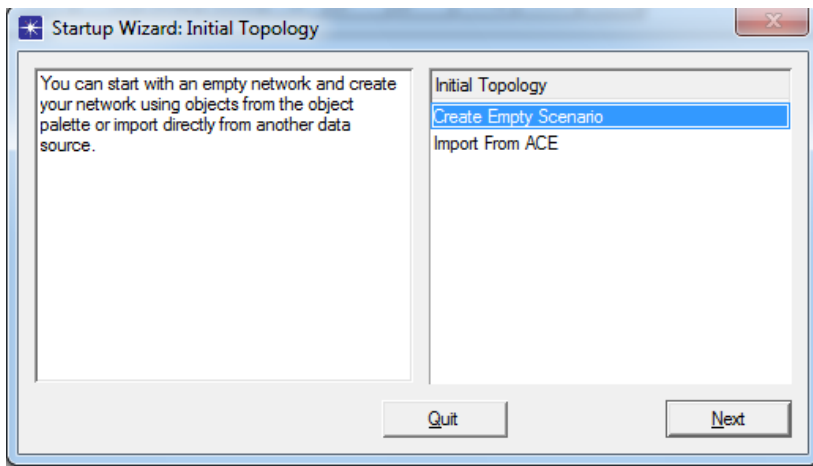
2. Wybierz **projekt** a następnie kliknij **OK**.



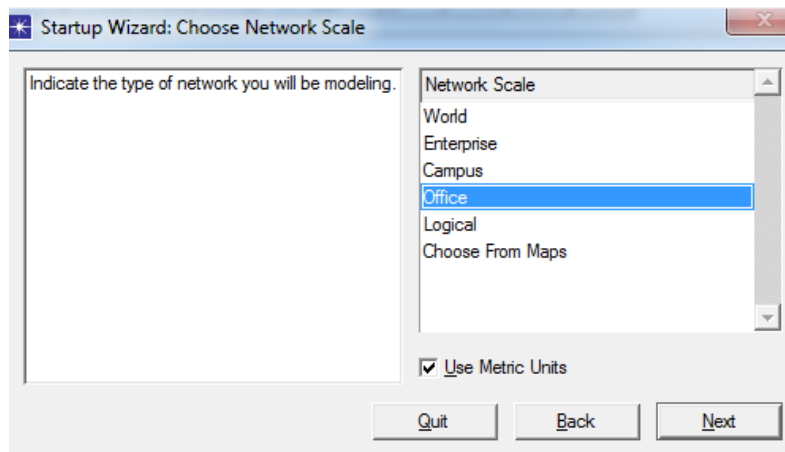
Następnie nazwij: projekt **DMZ_name** a scenariusz **DMZscenario_name**, (gdzie name to twoje imię). Po czym kliknij **OK**.



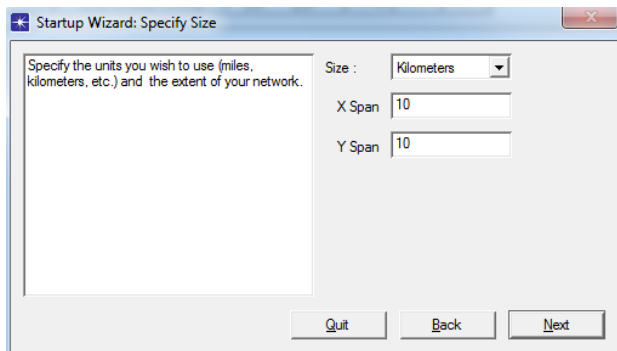
3. Po wyświetleniu okna dialogowego *Startup Wizard: Initial Topology* upewnij się, że jest zaznaczony **Create Empty Scenario**. Kliknij **Next**.



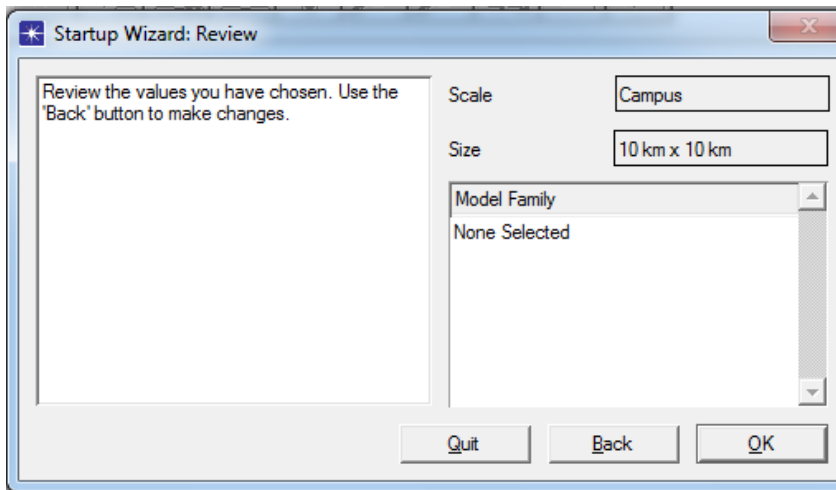
Dobłą mapą do realizacji będzie np. mapa kampusu. Wybierz **Office** z *Map List* po czym kliknij *Next*.



W oknie *X Span* i *Y Span* możesz zmienić rozmiar „office” po czym kliknij dwa razy **NEXT**.



4. W oknie **Startup Wizard: Review** wybierz Model Family po czym kliknij OK.




4. Tworzenie i konfigurowanie sieci.

Czym się będziemy zajmować?.

Stworzymy wewnętrzną sieć z FTP, HTTP i DB serwer. Chcemy chronić wewnętrzny DB i FTP Server przed dwoma rodzajami ataków: zewnętrznym i wewnętrznym. Dodatkowo chcemy zezwolić na ruch do wewnętrznego serwera HTTP.



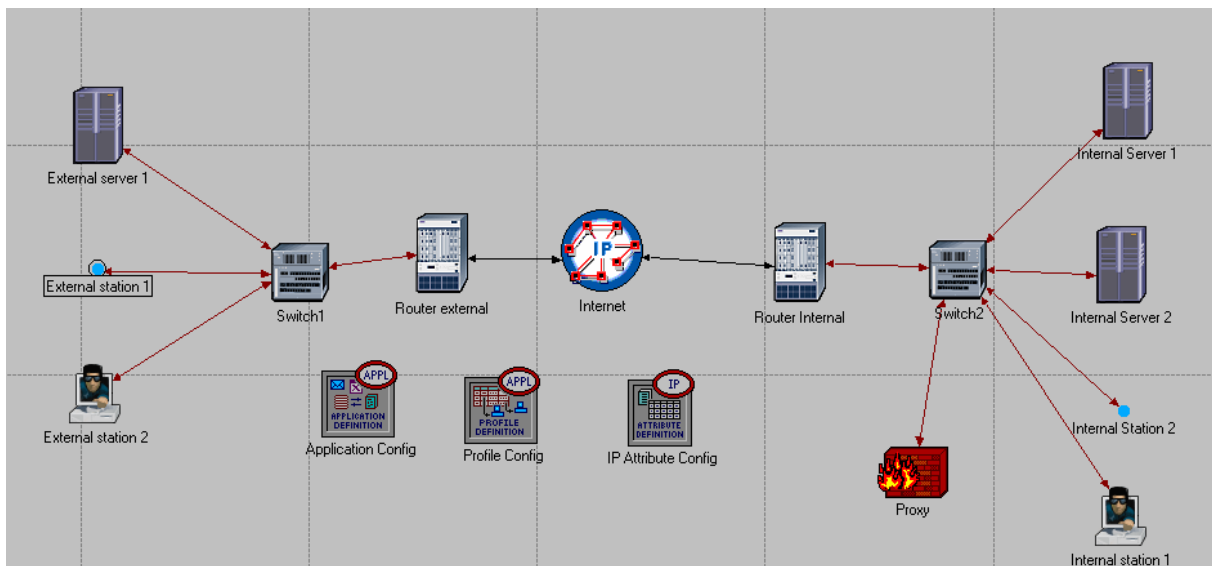
Aby zwiększyć powierzchnie kliknij  , co może być przydatne w późniejszym czasie.

1. Wybierz następujące komponenty.

ilość	Komponent	Paleta	Opis
1	Ip_32_cloud	Internet_toolbox	
1	Application Config	Internet_toolbox	
1	Profile Config	Internet_toolbox	
1	IP Attribute Config	Internet_toolbox	
2	Ethernet4_slip8_gtwy	Internet_toolbox	
1	Ethernet2_slip8_Firewall	Internet_toolbox	
2	Ethernet16_switch	Internet_toolbox	
4	Sm_int_wkstn	Sm_Int_Model_List	
3	Sm_int_Server	Sm_Int_Model_List	
	PPP_DS1	Internet_toolbox	Links to Internet
	100BaseT	Internet_toolbox	Remaining links

Tab.1Komponenty

2. Rozmieść komponenty a następnie zmień ich nazwy jak pokazano poniżej



External Station 2 i Internal Station 1 mogą mieć optymalnie zmienione ikony. Aby zmienić ikony kliknij prawym klawiszem na dany komponent, następnie wybierz **Advanced Edit Attributes** → **icon name** , w dalszej kolejności wybierz ikonę hacker.

icon name hacker

3. Przydziel adresy IP do wszystkich stacji, interfejsów i subinterfejsów.

Edytuj atrybuty wszystkich stacji i Serwerów **IP Host Parameters** → **Interface Information** → **Address** i **Subnet Mask**. Dla routerów **IP Routing Parameters** → **Interface information** → **rozwiń odp. wiersz row** . Do tego celu użyj Tab3.

Stworzymy 5 sieci:

Interface	Address/Subnet Mask
Internal Network	213.180.1.0/24
External Network	194.179.95.0/24
Internet (to External Network)	190.50.50.0/24
Internet (to Internal Network)	190.40.40.0/24
Internal Router – switch2--Proxy	190.30.30.0/24

Tab2. Sieci.

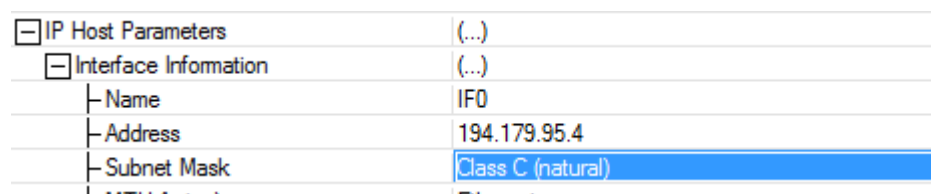
Zawsze będziemy używali maski 255.255.255.0

Interface	Address /Subnet Mask.
External Station 1	194.179.95.4/24
External Station 2	194.179.95.3/24
External Server 1	194.179.95.2/24
External Router –Interface to switch1 (IF0)	194.179.95.1/24
External Router –Interface to Internet (IF10)	190.50.50.1/24

Internet –Interface to External Router (IF0)	190.50.50.2/24
Internet –Interface to Internal Router (IF10)	190.40.40.1/24
Internal Router-Interface to Internet (IF1)	190.40.40.2/24
Internal Router-Interface to switch 2 (IF0)	190.30.30.1/24
Internal Station 1	213.180.1.2/24
Internal Station 2	213.180.1.3/24
Internal Server 1	213.180.1.4/24
Internal Server 2	213.180.1.5/24
Proxy (IF0) –subinterface to Internal Network (IF0.1)	213.180.1.6/24
Proxy (IF0) –subinterface to Internal Router (IF0.2)	190.30.30.2/24

Tab3.Adresacja.

Przykładowa zmiana adresu:



W wierszu gdzie trzeba wprowadzić maskę wybierz : **Class C(natural)**

Nazwy interfejsów zależą od kolejności dodawania więc mogą się różnić.

Proxy posiada dwa subinterfejsy na interfejsie podłączonego do Switch2 (IF0).

Wprowadzić zmiany wykonując kolejno: **Proxy Attributes** → **IP Routing Parameters** → **Interface Information** → rozwiń row:0 → **Subinterface Information** → ustaw wartość row na **2**. Rozwiń obydwie stworzone wiersze i wprowadź w obydwu następujące zmiany.

Row 0:

Name : From/To Gateway, **Address**: 190.30.30.2, **Subnet Mask**: 255.255.255.0, **Layer 2 Mappings** → **VLAN Identifier**: 2 (teraz mamy ten sam interfejs należący do dwóch sieci jednocześnie.)

<input type="checkbox"/>	Subinterface Information	(...)
	rows	2
<input type="checkbox"/>	row 0	
	Name	From/To gateway
	Status	Same as Parent
	Address	190.30.30.2
	Subnet Mask	Class C (natural)
<input type="checkbox"/>	Secondary Address Infor...	Not Used
	MTU (bytes)	Same as Parent
<input type="checkbox"/>	Metric Information	Default
	Routing Protocol(s)	RIP
	Compression Information	None
	Multicast Mode	Disabled
<input type="checkbox"/>	Layer 2 Mappings	(...)
	ATM PVC Name	None
	Frame Relay PVC Na...	None
	VLAN Identifier	2
<input type="checkbox"/>	QoS Information	None
<input type="checkbox"/>	Packet Filter	None
	Policy Routing	None
	VRF Name	None
	Description	N/A

Row 1:

Name: From/To Internal Network, **Address**: 213.180.1.6 , **Subnet Mask**: 255.255.255.0,
Layer 2 Mapping → **VLAN Identifier** : 3.

[-] row 1	
- Name	From/To Internal Network
- Status	Same as Parent
- Address	213.180.1.6
- Subnet Mask	Class C (natural)
[+] Secondary Address Infor...	Not Used
- MTU (bytes)	Same as Parent
[+] Metric Information	Default
- Routing Protocol(s)	RIP
- Compression Information	None
- Multicast Mode	Disabled
[-] Layer 2 Mappings	(...)
- ATM PVC Name	None
- Frame Relay PVC Na...	None
- VLAN Identifier	3
[+] QoS Information	None
[+] Packet Filter	None
- Policy Routing	None
- VRF Name	None
- ...	

Nie ma konieczności przydzielania adresów IP i Maski podsieci. Możemy ustawić **Address: No IP Address** i **Subnet Mask: Auto Assigned**

4. Przydzielenie domyślnej bramy dla stacji i serwerów.

Przydziel domyślną bramę dla stacji i serwerów jako interfejs o adresie **213.180.1.6** i nazwie **From /To Internal Network**.

Aby ustawić domyślną bramę wybieramy **Edit Attributes** → **IP Host Parameters** → **Default route**.

Ustaw domyślną bramę dla: **Internal Station 1, Internal Station 2, Internal Server 1, Internal Server 2**

5. Konfiguracja Application Config:

Edit Attributes → następnie ustaw **Application Definitions: Default**

6. Konfiguracja Profile Config:

Edit Attributes → **Profile Configuration** → ustaw wartość **rows** na 3

Wprowadź następujące profile:

HTTPProfile – zawiera aplikacje WEB Browsing (Heavy HTTP1.1),

FTPProfile – zawiera aplikacje File Transfer (Heavy),

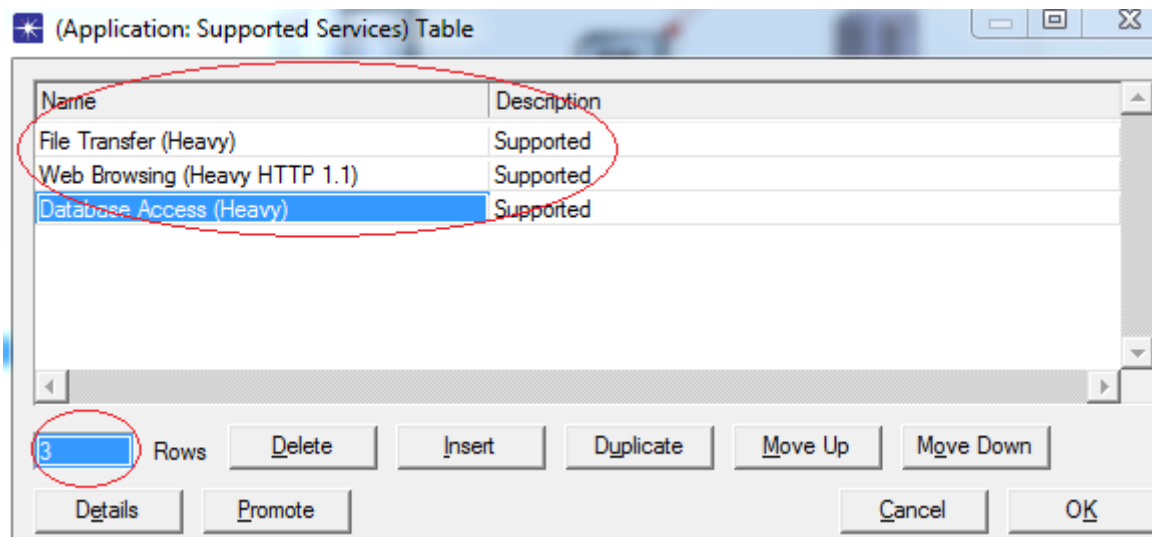
DBProfile – zawiera aplikacje Database Access (Heavy)

USŁUGI WSPIERANE PRZEZ SERWERY:

Server	Services
External Server 1	File Transfer (Heavy), WEB Browsing (Heavy HTTP1.1), Database Access (Heavy)
Internal Server 1	Database Access (Heavy), File Transfer (Heavy),
Internal Server 2	WEB Browsing (Heavy HTTP1.1),

Tab4. Usługi wspierane przez serwery.

7. Kliknij prawym klawiszem na dany Server, następnie wybierz Edit Attributes → Applications: Supported Services.--> kliknij Edit i ustaw wartość rows na 3. Wybierz następujące usługi jak pokazano poniżej.



Postępuj podobnie konfigurując pozostałe serwery.

8. Konfiguracja stacji roboczych.

Kliknij prawym klawiszem na danej stacji. **Wybierz Edit Attributes → Attribute Application: Supported Services → ustaw wartość rows na 1 (w zależności od stacji roboczej) → row0 → Profile Name na HTTPProfile.**

+	Application: Source Preferences	None
-	Application: Supported Profiles	(...)
	└ rows	1
	└ row 0	
	└ Profile Name	HTTPProfile
	└ Application: Supported Services	None
+	Application: Transport Protocol Specifica...	Default

Postępuj analogicznie dla pozostałych stacji roboczych.

Stacja robocza	Profile
External Station 1	HTTPProfile
External Station 2	DBProfile,FTPProfile
Interna Station 1	FTPProfile,DBProfile
Internal Station 2	HTTPProfile,FTPProfile

Tab5.Profile wspierane przez poszczególne stacje robocze.

9. Ustaw adresy serwerów na pokazane w tabeli poniżej:

Server	Server Address
External Server1	SExt1HTTPFTPDB
Internal Server 1	SInt1FTPDB
Internal Server 2	SInt2HTTP

Tab6.Adresy Serverów

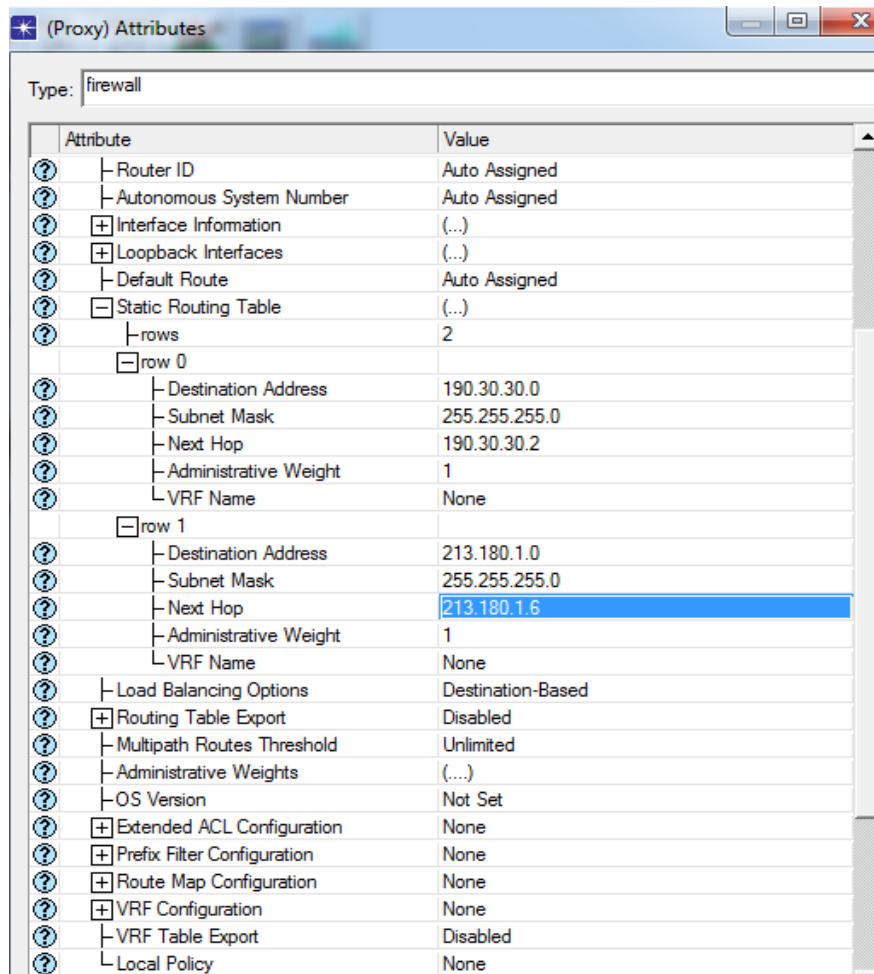
10. w następnej kolejności zmień stacji roboczych.

Attribute → Application:Destination Preferences

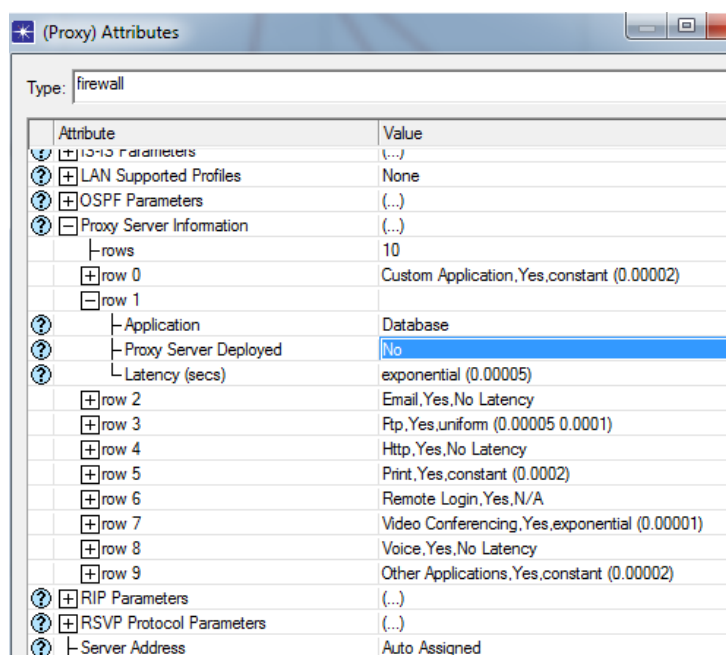
Station	Symbolic Name	Actual Name
External Station 1	HTTP Server	SInt2HTTP
External Station 2	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Interna Station 1	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Interna Station 2	HTTP Server	SExt1HTTPFTPDB
	FTP Server	SExt1HTTPFTPDB

Tab7. Nazwy stacji roboczych

11. Proxy → Edit Attributes → IP Routing Parameters → Static Routing Table → Ustaw wartość **rows** na **2** a następnie skonfiguruj jak pokazano poniżej.



12. Skonfiguruj Proxy tak aby odrzucać ruch FTP i Database z sieci wewnętrznej.



13. Edycja tabeli routingu statycznego dla Internal Router.

Następne czynności wykonamy aby:

- Otrzymywać pakiety od Proxy(przychodzące od sieci wewnętrznej i wysłać je ponownie
- Otrzymywać pakiety z Internetu z przeznaczeniem do wewnętrznej sieci i wysłać je ponownie do Proxy.
- W obu przypadkach wykonywana jest filtracja ruchu na podstawie ACL.
- Odrzucać pakiety otrzymane prosto z sieci wewnętrznej. Zostanie to zrealizowane za pomocą VLAN'ów

Skonfiguruj tabele routingu statycznego jak pokazano poniżej:

└rows	3
└row 0	
└ Destination Address	190.40.40.0
└ Subnet Mask	255.255.255.0
└ Next Hop	190.40.40.2
└ Administrative Weight	1
└ VRF Name	None
└row 1	
└ Destination Address	190.30.30.0
└ Subnet Mask	255.255.255.0
└ Next Hop	190.30.30.1
└ Administrative Weight	1
└ VRF Name	None
└row 2	
└ Destination Address	213.180.1.0
└ Subnet Mask	255.255.255.0
└ Next Hop	190.30.30.2
└ Administrative Weight	1
└ VRF Name	None
└ Load Balancing Options	Destination-Based

14. Konfiguracja ACL.

Najpierw przydziel tabelę ACL do danego interfejsu. Aby to zrobić wykonuj następujące polecenia.

Router→ **Edit Attributes**→**IP Routing Parameters**→**Interface Information**→ **row 1**
 (numer interfejsu który jest podłączony do internetu)→**Packet Filter**→**Send Filter:**
Outgoing Traffic i **Receive Filter: Incoming Traffic**

15. Utwórz VLANy w wewnętrznej sieci.

Musimy najpierw skonfigurować: **VLAN Parameters**→**Scheme: Port Based VLANs**. W dalszej kolejności **Supported VLANs** →Kliknij **Edit** → Ustaw wartość rows na 3 a następnie wprowadź wspierane VLANy: (Name: Default, Gateway, InternalNetwork odpowiednio dla VLANow 1,2,3)

Type	Identifier (VID)	Name	State	MTU (bytes)	SAID
802.1Q	1	Default	Active	1500	100000+VID
802.1Q	2	Gateway	Active	1500	100000+VID
802.1Q	3	InternalNetwork	Active	1500	100000+VID

Aby Proxy mogło pracować w wieloma subinterfejsami na jednym interfejsie, każdy subinterfejs musi należeć do innej sieci. Może to być zrealizowane za pomocą VLAN'ów. Potrzebujemy dwa proste VLAN'y. Pierwszy VLAN o ID=2 dla sieci: 190.30.30.0/24 i drugi VLAN o ID=3 dla sieci 213.180.1.0/24. Przypiszemy identyfikatory VLAN'ów jak pokazano w tabeli poniżej dla interfejsów wewnętrznej sieci,

Dla stacji roboczych:

IP Host Parameters → Interface Information → Layer 2 Mapping → VLAN identifier

Dla routerów:

IP Routing Parameters → Interface Information → row i (gdzie i to numer interfejsu) → layer 2 Mapping → VLAN Identifier

Interface	VLAN Identifier
Internal Router-Interface to Switch 1(IF0)	3
Proxy-subinterface From/to gateway	3
Proxy-subinterface From/ To /Internal Network	2
Internal Station 1	2
Internal Station 2	2
Internal Server 1	2
Internal Server 2	2

Tab8. Ustawienia VLANów.

16. Konfiguracja VLAN dla Switch2.

Port	Port Type	Port VLAN id	Supported VLANs
Interface to Internal Router(P0)	Access	2	2
Interface to Proxy(P13)	Trunk	1	1,2,3
Interface to Internal Station 1(P1)	Access	3	3
Interface to Internal Station 2(P10)	Access	3	3
Interface to Internal Server 1(P11)	Access	3	3
Interface to Internal Server 2(P12)	Access	3	3

Tab9.Konfiguracja VLAN dla switch 2

Aby ustawić wspierane Supported Vlans wykonuj kolejno:

Kliknij prawym klawiszem na Switch→**Edit Attributes**→**Switch Port**

Configuration→wybierz odpowiedni **row**(interfejs)→ **VLAN Parameters**

17. Ustawienia Symulacji.

- Proxy→ Choose Individual Statistics→ IP→ Traffic Dropped(Packets/sec)
- W ten sposób możemy zobaczyć ilość ruchu odrzucanego przez Proxy

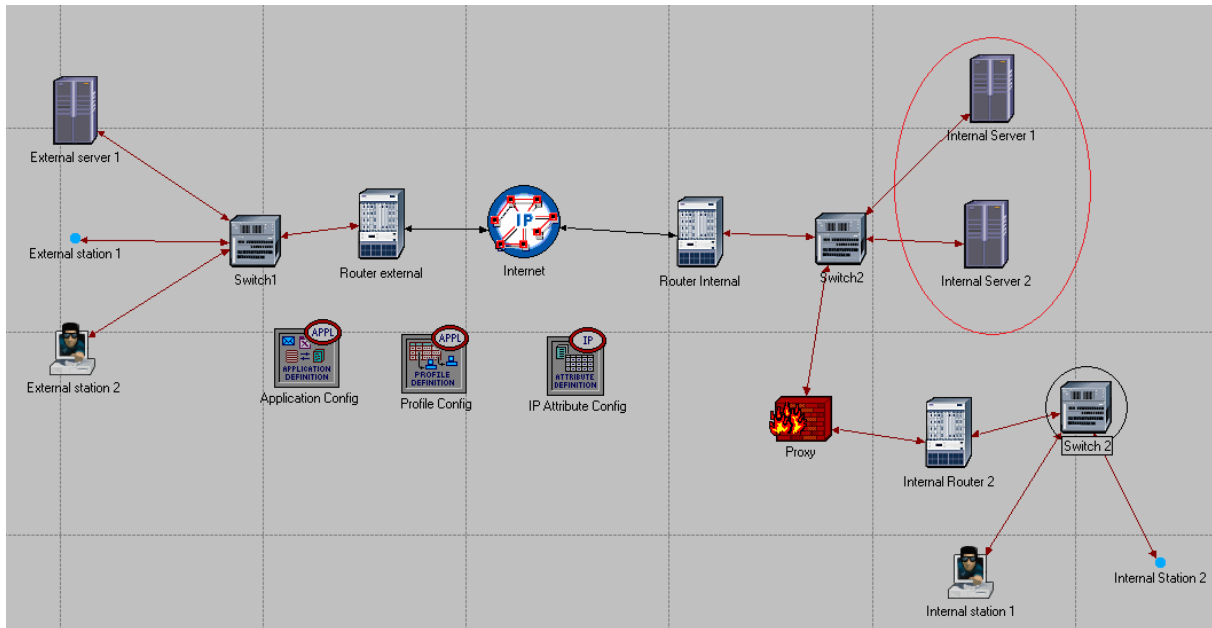
- Kliknij Configure/Run Simulation  , ustaw Duration na 15 minut(s).
Kliknij OK(nie klikaj start)

18. Tworzenie drugiego Scenariusza

Kliknij **Scenarios**→ **Duplicate Scenario**→nazwij drugi scenariusz

ScreenedSubnetWitchDMZ.

Ten scenariusz jest taki sam jak poprzedni lecz tym razem wewnętrzne stacje będą podłączone do Switch 2 przez Ethernet_4_slip8_gtwy router (nazwa w palecie internet_toolbox), który podłączy je do Proxy. Wewnętrzni użytkownicy będą w zmienionej sieci LAN używając ethernet16_switch(w palecie Internet_toolbox). Nowe połączenie będzie używało 100BaseT. Układ serwerów będzie taki sam jak w DMZ.



Utwórz sieć 213.190.1.0/25, oddzieloną od 213.180.1.0 (obecnie będą w niej tylko **servery**). Od teraz sieć ta jest nazywana **Demilitarized Zone (DMZ)**, ponieważ jest oddzielona od wewnętrznych i zewnętrznych ataków. Inna sieć zostanie utworzona pomiędzy Internal Router 2 and Proxy – 190.20.20.0/24

Nowa tabela adresów:

Interface	IP Address
Internal station 1	213.190.1.2
Internal Station 2	213.190.1.3
Internal Router 2-interface to switch 3(IF0)	213.190.1.1
Internal Router 2-Interface to Proxy(IF1)	190.20.20.1
Proxy interface to Internal Router 2(IF1)	190.20.20.2

Tab.10. Nowa adresacja w scenariuszu **ScreenedSubnetWitchDMZ**.

Uwaga.

Nazwy interfejsów mogą się różnić w zależności od kolejności dodawania.

19. Konfiguracja ACL dla Internal Router 2.

Polityka bezpieczeństwa jest w dalszym ciągu taka sama. Naszym celem jest unikanie dostępu do Internal Server 1(FTP and DB server). Skonfigurujemy ACL na Internal Router 1 używając informacji z tabeli poniżej:

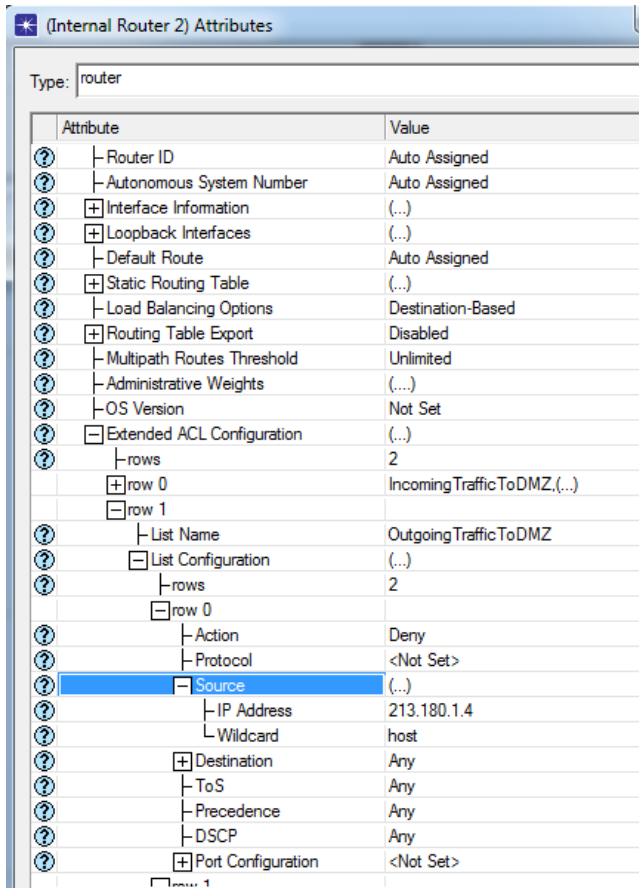
- Lista IncomingTrafficAtDMZ odrzuca cały ruch wysyłany do Internal Server 1 (213.180.1.4) i pozwala na pozostały ruch,
- OutgoingTrafficFromDMZ odrzuca wychodzący ruch z servera Internal Server 1 ale pozwala na pozostały wychodzący ruch.

List Name	Action	Source	Destination
IncomingTrafficToDMZ	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	*
OutgoingTrafficFromDMZ	Deny	213.180.1.4/host	*
	Permit	*	*

Tab11.ACL dla Internal Router 2

Aby utworzyć listę ACL wykonaj kolejno: Kliknij prawym przyciskiem na Routerze → **Edit Attributes** → **IP Routing Parameters** → **Extended ACL Configuration** → zmień wartość **rows** na **2** (row 1 dla IncomingTrafficToDMZ; row 2 dla OutgoingTrafficToDMZ) → następnie utwórz zasady według Tab11.

Przykład podany poniżej.



20. Konfiguracja ACL dla interfejsów Internal Router 2.

Router → Edit Attributes → IP Routing Parameters → Interface Information → row 1
(numer interfejsu który jest podłączony do internetu) → Packet Filter →

- Interface to Proxy (IF1) Send Filter: **IncommingTrafficToDMZ**, Receive Filter: **OutGoingTrafficFromDMZ**
- Interface to Switch 3 (IF0) Send Filter: **OutGoingTrafficFromDMZ**, Receive Filter: **: IncommingTrafficToDMZ**

Tworzenie tabeli routingu dla Internal Router 2 oraz modyfikacja tabeli routingu dla Internal Router 1 i Proxy.

- Dla internal Router 2: **Destination: 190.20.20.0/24, Next Hop : 190.20.20.1;**
- **Destination: 213.190.1.0/24, Next Hop : 213.190.1.1 and Default: 190.20.20.2;**
- Dla proxy dodamy nowe wejście: **Destination: 213.190.1.0 Next Hop 190.20.20.1**

- Dla internal Router 1, dodamy nowe wejście: **Destination: 213.190.1.0/24 Next Hop: 190.30.30.2**
- Ustaw domyślną drogę (Default Route) dla **Internal Station 1** i **Internal Station 2** na 213.190.1.1

Przykładowa zmiana „**Default Route**” dla Internal Station 1 przedstawiona poniżej:

Attribute	Value
Application: Multicasting Specification	None
Application: RSVP Parameters	None
Application: Segment Size	64,000
Application: Source Preferences	None
Application: Supported Profiles	(...)
Application: Supported Services	None
Application: Transport Protocol Specifica...	Default
CPU Background Utilization	None
CPU Resource Parameters	Single Processor
Client Address	Auto Assigned
IGMP Host Parameters	Default
IP Host Parameters	(...)
Interface Information	(...)
Passive RIP Routing	Disabled
Default Route	213.190.1.1
Static Routing Table	(...)
IP Processing Information	Default
RSVP Protocol Parameters	(...)

21. Rekonfiguracja list ACL na Internal Router.

W następnej kolejności musimy wprowadzić małe zmiany dla ruchu przychodzącego i wychodzącego w listach ACL dla Internal Router 1. Umożliwimy ruch dla sieci utworzonych we wcześniejszych krokach, 213.190.1.0/24 (dla nowej wew. Sieci.) i 190.20.20.0 (router pomiędzy Internal Router 2 a Proxy.) W tabeli poniżej znajdują się zasady dla Internal Router 1. Resztę parametrów pozostaw bez zmian.

Aby edytować listę ACL wykonaj kolejno: Kliknij prawym przyciskiem na Routerze→**Edit Attributes**→**IP Routing Parameters**→**Extended ACL Configuration**→ rows 2 (row 1 dla IncomingTrafficToDMZ; row 2 dla OutgoingTrafficToDMZ)

List Name	Action	Source	Destination
IncomingTraffic	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	213.190.1.0/24
	Permit	*	190.20.20.0/24
OutgoingTraffic	Permit	213.190.1.0/24	*
	Permit	190.20.20.0/24	*
	Permit	213.180.1.0/24	*
	Permit	190.30.30.0/24	*

L9.21 Adding up new conditions to the ACL

22. Wykonanie symulacji.

Wybierz kolejno: **Scenarios** → **Manage Scenarios**. Możemy sprawdzić wszystkie scenariusze za pomocą <collected> i **Results** a następnie kliknij **OK**.

Aby przeglądać wyniki wybierz: **Results** → **View Results**.

