МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Захист інформації в спеціалізованих ІТС

Практичне заняття №7

Практичне використання міжмережевих екранів для завдань сегментації та ізоляції SCADA

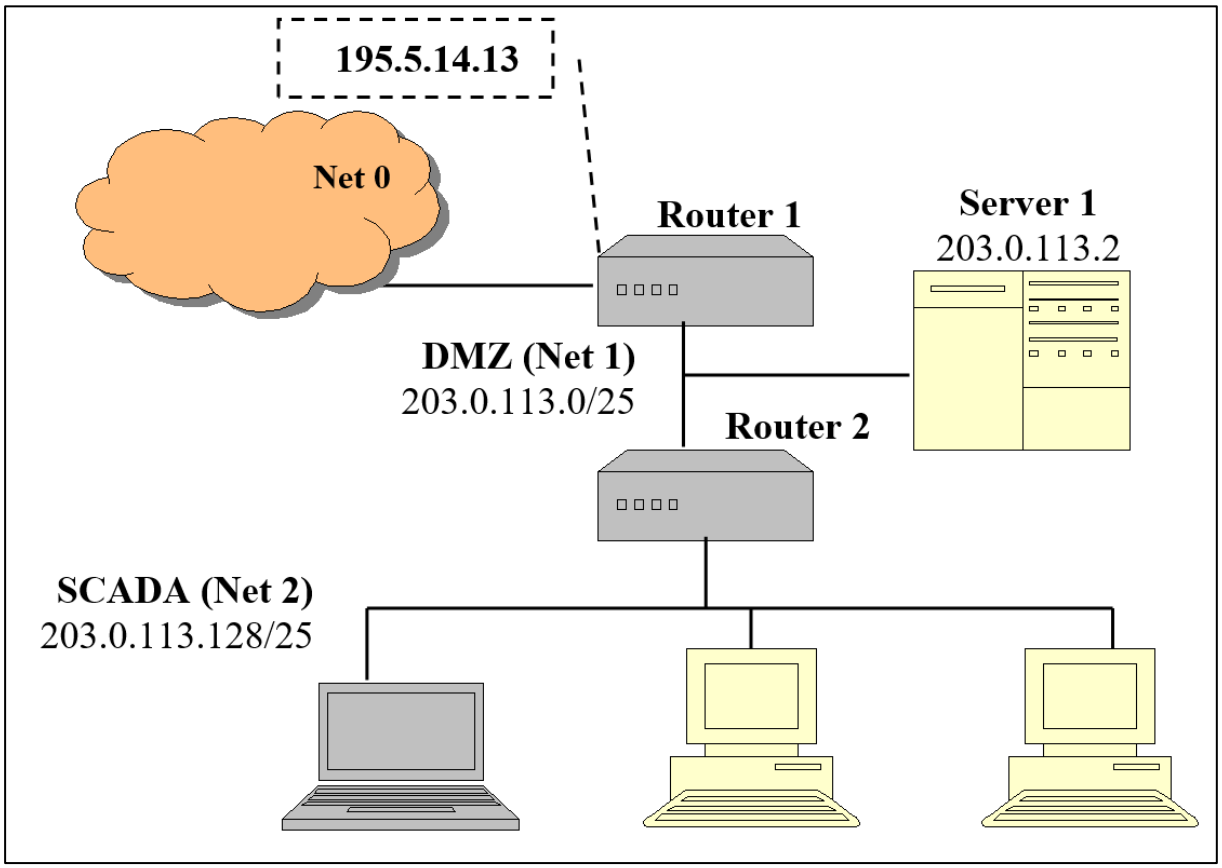
Перевірив:
Зубок В. Ю.

Виконав:
студент І курсу
групи ФБ-41мп
Сахній Н. Р.

Київ 2025

№	Напрямок	Source IP	Порт	Destination IP	Порт	Протокол	Дія
1	вхід	будь-який	>1024	192.168.3.3	25	TCP	pass
2	вихід	192.168.3.3	25	будь-який	>1024	TCP	pass

Завдання (№12): Написати формальною мовою, приклад якої наведений в таблиці вище, правила фільтрації відповідно до варіанту, які мають застосовуватись до сегментованої мережі, зображеної на рисинку нижче:



Задача 12. Пристрої виробничої мережі треба вберегти від атак на службу DNS (DNS spoofing, DNS storm, DNS cache poisonong). Пристрої мають виконувати резолвінг звертаючись виключно до рекурсивного DNS встановлений на Server1. Запишіть правило (правила) для маршрутизатора (вкажіть якого), що убезпечить виробничу мережу від потрапляння DNS-пакетів з зовнішньої мережі. Порт DNS – 53, протоколи UDP та TCP.

№	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action
1	outgress	203.0.113.128/25	>1024	203.0.113.2	53	UDP/TCP	pass
2	ingress	203.0.113.2	53	203.0.113.128/25	>1024	UDP/TCP	pass
3	outgress	203.0.113.128/25	any	0.0.0.0/0	any	any	drop
4	ingress	0.0.0.0/0	any	203.0.113.128/25	any	any	drop

*** Дана політика повинна бути застосована на мережевому обладнанні “Router 2” ↑**

** Вона дозволяє DNS-трафік з виробничої мережі (Net 2) до сервера в DMZ (Net 1), а також забороняє будь-які вхідні/вихідні комунікації виробничих пристроїв зі “світом”.

№	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action
1	ingress	0.0.0.0/0	>1024	203.0.113.2	22	TCP/UDP	pass
2	outgress	203.0.113.2	22	0.0.0.0/0	>1024	TCP/UDP	pass
3	outgress	203.0.113.2	>1024	0.0.0.0/0	any	any	pass
4	ingress	0.0.0.0/0	any	203.0.113.2	>1024	any	pass
5	ingress	0.0.0.0/0	any	0.0.0.0/0	any	any	drop
6	outgress	0.0.0.0/0	any	0.0.0.0/0	any	any	drop

*** Дана політика повинна бути застосована на мережевому обладнанні “Router 1” ↑**

** Вона дозволяє SSH-з’єднання з інтернет-мережі (Net 0) до сервера в DMZ (Net 1), а також дає обмежену можливість серверу здійснювати комунікації зі “світом”. Водночас DNS-трафік із виробничої мережі (Net 2) дозволений, а ззовні буде заборонений.

№	Direction	Source IP	Source Port	Destination IP	Destination Port	Protocol	Action
1	ingress	203.0.113.128/25	>1024	203.0.113.2	53	UDP/TCP	pass
2	outgress	203.0.113.2	53	203.0.113.128/25	>1024	UDP/TCP	pass
3	ingress	0.0.0.0/0	>1024	203.0.113.2	22	TCP/UDP	pass
4	outgress	203.0.113.2	22	0.0.0.0/0	>1024	TCP/UDP	pass
5	outgress	203.0.113.2	>1024	0.0.0.0/0	any	any	pass
6	ingress	0.0.0.0/0	any	203.0.113.2	>1024	any	pass
7	outgress	203.0.113.2	any	0.0.0.0/0	any	any	drop
8	ingress	0.0.0.0/0	any	203.0.113.2	any	any	drop

*** Подібний ACL рекомендовано застосовати на серверному пристрої “Server 1” ↑**

** Він здійснює дублювання правил на сервер, які буде були застосовані на роутерах.