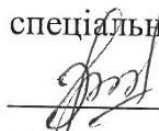


Міністерство освіти і науки України
Державний університет “Житомирська політехніка”
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

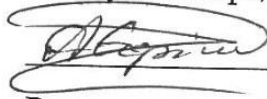
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: “Проект підсистеми захисту мережної інфраструктури
підприємства (на прикладі ТОВ Партнер)”

Виконав студент 4-курсу, групи ЗКБ-17
спеціальності 125 “Кібербезпека”


М.М. Кухарчук
Керівник

завідувач кафедри КІ та КБ, к.т.н.


А.А. Єфіменко
Рецензент

доцент кафедри КІ та КБ, к.т.н., доцент


Ю.М. Россінський

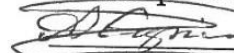
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 А. А. Єфіменко
«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Кухарчука Максима Михайловича

Тема роботи: Проект підсистеми захисту мережної інфраструктури підприємства (на прикладі ТОВ Партнер)

Затверджена Наказом університету від 12 квітня 2021 р. № 134/с

Термін здачі студентом закінченої роботи 16 червня 2021

Вихідні дані роботи (зазначається предмет і об'єкт дослідження) Об'єкт дослідження та модернізації, мережа підприємства ТОВ Партнер.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

Керівник

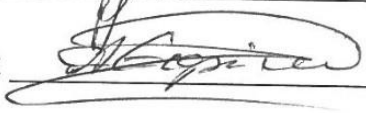


А. А. Єфіменко

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання.	2 березня 2021 – 5 квітня 2021	
2	Розробка та написання розділу 1	6 квітня 2021 – 12 квітня 2021	
3	Розробка та написання розділу 2	13 квітня 2021 – 26 квітня 2021	
4	Розробка та написання розділу 3	27 квітня 2021 – 4 червня 2021	
5	Захист	22 червня 2021	

Студент  М.М. Кухарчук

Керівник  А. А. Єфіменко

РЕФЕРАТ

Випускна кваліфікаційна робота бакалавра складається з аналізу наявної мережі підприємства, побудови схеми, плану модернізації мережі та схеми і налаштування нової удосконаленої мережі підприємства «ТОВ Партнер» Пояснювальна записка містить 59 сторінок та 5 додатків.

Мета мого проекту, показати на реальному прикладі підприємства ТОВ Партнер, того які бувають мережі коли їх будують та обслуговують користувачі без відповідного досвіду і навичок, та того як можна не вкладаючи відносно великих коштів трансформувати таку мережу і її захист до прийняттого рівня, для того, щоб вона відповідала всім сучасним вимогам захищеності та надійності, та могла стабільно функціонувати і виконувати всі поставлені до неї вимоги.

					КІК.КР.Б-125-06-ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту мережної інфраструктури підприємства (на прикладі ТОВ Партнер)	Літ.	Арк.	Аркуші
Розробив		Корсунь М.М.		23.06.21				
Керівник		Богданов А.В.		23.06.21			4	
Рецензент		Росієвський		23.06.21		Житомирська політехніка, група ЗКБ-17		
н. контр.								
Зав. каф.		Богданов А.В.		23.06.21				

ABSTRACT

The final qualifying work of the bachelor consists of the analysis of the existing network of the enterprise, construction of the scheme, the plan of modernization of the network and the scheme and adjustment of the new improved network of the enterprise "LLC Partner". The explanatory note contains 60 pages and 5 appendices.

The pupose of my project, is to show a real example of Partner Ltd., what networks are when they are built and maintained by users without relevant experience and skills, and how it is possible without investing relatively large funds to transform such a network and its protection to an acceptable level, that it meets all modern requirements of security and reliability, and can function stably and fulfill all requirements to it.

					КІК.КР.Б-125-06-ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

Вступ

Розділ 1. Аналіз мережної інфраструктури та стану захищеності мережі підприємства ТОВ Партнер

1.1. Аналіз мережної інфраструктури підприємства

1.2. Аналіз технологій та обладнання мережі підприємства

1.3. Аналіз стану захищеності та засобів захисту мережної інфраструктури підприємства

1.4. Постановка завдання на розробку підсистеми захисту мережної інфраструктури підприємства

Розділ 2. Розробка проєкту підсистеми захисту мережної інфраструктури підприємства ТОВ Партнер

2.1. Розробка проєкту модернізованої інфраструктури мережі підприємства

2.2. Розробка моделі загроз для мережної інфраструктури підприємства

2.3. Розробка проєкту підсистеми захисту мережної інфраструктури підприємства

Розділ 3. Налагодження та тестування підсистеми захисту мережної інфраструктури підприємства ТОВ Партнер

3.1. Налагодження модернізованої мережної інфраструктури підприємства

3.2. Налагодження підсистеми захисту мережної інфраструктури підприємства

3.3. Тестування роботи модернізованої мережної інфраструктури та підсистеми захисту мережі підприємства

Висновки

Список використаних джерел

Додатки

					КІК.КР.Б-125-06-ПЗ	Арк.
						6
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

З кожним роком бізнес все більше стає залежним від сучасних технологій, розвивається інфраструктура та технології, все більше і більше послуг переходять в інтернет простір, а разом з цим зростає і вірогідність потрапити в поле зору зловмисників, які можуть викрасти чи пошкодити конфіденційну інформацію, або вивести з ладу елементи інфраструктури мережі організації і цим самим завдати величезних збитків. Для того щоб захиститися від зовнішніх і внутрішніх загроз, фірми наймають ІТ спеціалістів і витрачають не малі кошти на обладнання і програмне забезпечення для захисту своїх мереж і даних від несанкціонованого втручання, пошкодження та викрадення. На рівні бізнесу дотримання інформаційної і мережевої безпеки є набагато складнішим у порівнянні з фізичними особами, в залежності від сфери діяльності та величини обігу. Щоб надійно захищати свої дані потрібно перш за все визначити, а що ж таке безпека мережі і яким шляхом її досягти.

Безпека мережі (*Network security*) — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека містить у собі дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень. Мережева

					КІК.КР.Б-125-06-ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю. Безпека мережі організації це дуже складний процес і без спеціалістів конкретного профілю з відповідними навичками та досвідом її практично неможливо досягти.

Мета мого проєкту, показати на реальному прикладі фірми ТОВ Партнер, того які бувають мережі коли їх будують та обслуговують звичайні користувачі або люди без відповідного досвіду і навичок, та того як можна не вкладаючи відносно великих коштів трансформувати таку мережу і її захист до прийнятного рівня, щоб вона відповідала всім сучасним вимогам захищеності та надійності, та могла стабільно функціонувати і виконувати всі поставлені до мережі вимоги. В своїй роботі я опишу весь процес від аналізу інфраструктури та захищеності наявної мережі, складання топології, до її модернізації, налагодження і тестування.

Короткі відомості про ТОВ Партнер.

Підприємство засноване в 1992 році, спеціалізується на виготовленні меблевої продукції і всього, що з цим пов'язано. Має свій онлайн магазин. До 2013 року в штаті був відсутній ІТ спеціаліст Після поступового переходу підприємства на роботу в базі 1С на термінальних серверах і розширення мережевої інфраструктури, було прийнято рішення про введення в штат ІТ співробітника.

					КІК.КР.Б-125-06-ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділ 1. Аналіз мережної інфраструктури та стану захищеності мережі підприємства ТОВ Партнер

1.1. Аналіз мережної інфраструктури підприємства

Насамперед хочу зазначити, що інфраструктура підприємства будувалась приблизно 15 років різними людьми які зазвичай не мали достатнього рівня знань і кожен з тих хто щось додавав опирався на свій досвід та рівень знань. Мережа будувалась без чіткого плану по принципу додавання елементів по мірі їх необхідності. Першим етапом аналізу мережі стала побудова схеми наявної інфраструктури мережі, якої до цього не існувало. Схема мережі це важлива складова інфраструктури, яка полегшує роботу ІТ спеціалісту під час виявлення несправностей, або під час розширення чи модернізації. Наявна схема зображена в Додатку А, (Рисунок А.1). Якісний аналіз усієї мережевої інфраструктури в цілому, допомагає виявити точки падіння функціональності, місця, де система неефективна. Крім того, аналіз інфраструктури, дозволяє знайти способи підвищення продуктивності і надійності роботи мережі підприємства. Під час аналізу інфраструктури були перевірені та проаналізовані такі складові:

1. Лінії комутації.
2. Системи безперебійного живлення.
3. Мережеве обладнання (Switch, Комутатор, Firewall)
4. Система відеоспостереження (IP камери, POE Switch, Відеосервер)
5. IP телефони.
6. Персональні комп'ютери користувачів та сервер 1С, а саме:
 - А. Технічні характеристики
 - В. Встановлені операційні системи
 - С. Встановлене програмне забезпечення

					КІК.КР.Б-125-06-ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

- D. Стан носіїв інформації
- E. Наявність резервних копій
- F. Наявність оновлень системи

Під час аналізу системи не використовувалось жодне спеціалізоване ПО, так як вже на першому етапі було зрозуміло, що система потребує серйозних змін і оновлень, і проведення більш складного аналізу не мало ніякого сенсу.

1.2. Аналіз технологій та обладнання побудови мережі підприємства

Після аналізу інфраструктури був складений список встановленого обладнання та технологій, (Додаток D) який включав в себе:

1. Wi-Fi роутери (TP-Link) - 3 шт.
2. Switch (D-Link DES 1024A) - 3 шт.
3. Firewall (ZyXEL USG 100) - 1 шт.
4. 1С сервер (HP proliant на базі Windows 2012R2) - 1 шт.
5. ПК на базі ОС Windows (Win XP та Win7) - 30 шт.
6. IP телефони (Grandstream) - 30 шт.
7. Сервер відеоспостереження (Digistore) - 1 шт.
8. IP камери (HikVision DS-2CD1410F-IW) - 19 шт.
9. POE Switch (TP-Link TL-SG3424P) - 1 шт.
10. Сервер IP телефонії (Asterisk) - 1 шт.
11. Мережевий принтер (HP) - 1 шт.

Доступ до мережі інтернет відбувався через лінії двох провайдерів.

Перший по технології ADSL із заявлено швидкістю з'єднання до 25 Мбіт/сек.

(ADSL — технологія широкосмугового доступу, яка забезпечує передачу швидкісного цифрового сигналу звичайною аналоговою

					КІК.КР.Б-125-06-ПЗ	Арк.
						100
Змн.	Арк.	№ докум.	Підпис	Дата		

телефонною лінією, та дозволяє одночасно користуватися телефоном і Інтернетом. Розроблена Bellcore у 1988 році.)

Другий по оптоволоконній лінії через протокол RPTP із заявленою швидкістю з'єднання до 50 Мбіт/сек.

(RPTP — тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі. RPTP поміщає кадри PPP в IP-пакети для передачі по глобальній IP-мережі, наприклад інтернет.)

Всі внутрішні лінії в мережі прокладені витою парою, персональні комп'ютери користувачів підключені по протоколу Ethernet.

(Вита пара — вид мережевого кабелю, з однією або кількома парами ізольованих провідників, скручених між собою для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Використовується для побудови мереж у багатьох технологіях, наприклад, Ethernet, ARCNet і Token ring.) Також окремий канал зі статичною IP адресою, виділений для віддаленого доступу до сервера IP телефонії Asterisk. В мережі підприємства використовувався віддалений доступ користувачів до термінального серверу 1С та системи відеоспостереження за допомогою стандартних портів, 3389 для доступу до серверу 1С по протоколу RDP та 80 HTTP для доступу до системи відеоспостереження.

1.3. Аналіз стану захищеності та засобів захисту мережі підприємства

Після аналізу інфраструктури, створення схеми мережі, складення списку встановленого обладнання підприємства та аналізу обладнання, був проведений аналіз стану захищеності мережі підприємства на предмет вразливостей для подальшого їх усунення.

					КІК.КР.Б-125-06-ПЗ	Арк.
						111
Змн.	Арк.	№ докум.	Підпис	Дата		

Першим виявленим вразливим місцем в мережі, були роутери (TP-Link) через які здійснювалось підключення до мережі інтернет. Моделі роутерів мали велику кількість вразливостей, по причині того, що були зняті з обслуговування виробником і мали застаріле програмне забезпечення, до того ж, вони мали дуже низьку потужність в результаті чого, відбувалось періодичне зависання пристроїв через перевантаження. Крім того дані пристрої відносяться до категорії звичайних побутових роутерів, які не призначені для роботи з великими обсягами трафіку, що в свою чергу зменшувало продуктивність усієї мережі підприємства. Наступним вкрай вразливим місцем в мережі був Firewall ZyXEL USG 100. Пристрій був встановлений для маршрутизації і захисту мережі від вторгнень, але через застаріле ПО, яке не мало оновлень, мав низку вразливостей. Потенціал Firewall практично не використовувався, чому свідчила відсутність будь-яких правил фільтрації трафіку. Пристрій мав незахищений зовнішній доступ для управління пристроєм, по стандартному 80 порту (HTTP), що призводило до постійних спроб підібрати пароль зі сторони злоумисників. Також при використанні двох провайдерів, було відсутнє автоматичне переключення між каналами в разі збою одного з них, що значно знижувало відмовостійкість доступу до мережі інтернет, та вимагало постійного моніторингу стану каналів і фізичного переключення в разі виникнення проблем з одним з них. Ще однією глобальною проблемою і вразливістю, була повна відсутність оновлень операційних систем, встановлених на ПК користувачів та серверів, а також застарілі операційні системи Windows XP, які зняті з обслуговування розробником та мають безліч вразливостей. Слабким місцем в мережі, також була гостьова Wi-Fi мережа, яка не була ізольована від локальної мережі і таким чином злоумисник міг

					КІК.КР.Б-125-06-ПЗ	Арк.
						122
Змн.	Арк.	№ докум.	Підпис	Дата		

отримати доступ через неї до всієї інфраструктури підприємства. Політики паролів були на вкрай низькому рівні, більшість з них підбирались звичайним методом перебору паролів, та мали стандартні паролі типу Admin/Admin. Одним із вразливих місць було використання Wi-Fi роутерів в якості звичайних Switch, на яких був вимкнений DHCP сервер, що іноді призводить до відмови всієї мережі через конфлікти IP адрес, які роздавали DHCP сервери пристроїв у разі збою. Виявленим слабким місцем яке знаходилося не на останньому місці по критичності, було використання звичайних побутових пристроїв безперебійного живлення, які зазвичай мали несправні або зношені АКБ та не могли ефективно захищати пристрої від перепадів напруги, що в свою чергу призводило до незапланованого відключення пристроїв, та могло призвести до втрати інформації. Важливим елементом, що можна віднести до вразливості, була повна відсутність будь-яких резервних копій бази даних та серверів. І останнім виявленим вразливим місцем було підключення віддалених співробітників до сервера 1С по RDP протоколу без VPN (*RDP — протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на котрому запуснений сервіс термінальних з'єднань. Клієнти існують практично для всіх версій Windows, Linux, FreeBSD, Mac OS X. За умовчанням, використовується порт TCP 3389.*) через стандартний порт 3389, що приводило до постійного перебору паролів зі сторони ботнету. (*Ботнет — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникам виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай*

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		133

використовуються для протиправної діяльності — розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карток та паролів доступу.) і як наслідок могло призвести до злому і втрати інформації. Таким чином підбивши підсумок можна було стверджувати, що захист мережі підприємства був практично відсутній і мав безліч вразливостей, які в будь який момент могли використати зловмисники і паралізувати роботу підприємства або повністю знищити всю інформацію, що призвело до фатальних наслідків для компанії. Використовувати допоміжні інструменти для сканування мережі було не доцільно, так як мережа і без того потребувала серйозної модернізації та оновлення програмного забезпечення.

1.4. Постановка завдання на розробку підсистеми захисту мережі підприємства

В постановку завдання розробки підсистеми захисту мережі підприємства входила модернізація мережі таким чином, щоб при відносно невеликих фінансових затратах, отримати максимально захищену, стабільну та відмовостійку систему, яка б відповідала вимогам сьогодення, та була простою в обслуговуванні. Завдання:

1. Підібрати нове обладнання, яке б відповідало сучасним вимогам та мало відносно невелику ціну (Ціна/якість).
2. Прибрати з інфраструктури застарілі і вразливі пристрої, і замінити їх на нові, або модернізувати інфраструктуру таким чином, щоб виключити застарілі пристрої повністю.
3. Провести повний аудит паролів доступу до серверів, IP телефонів, IP камер та оновити операційні системи всіх наявних ПК та серверів. Також враховуючи, що система тривалий час мала багато

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		144

вразливостей потрібно було провести повне сканування всіх ПК та серверів на наявність в них шкідливого програмного забезпечення.

4. Замінити застарілі операційні системи, на більш нові (Windows 8/8.1/10/Linux).
5. Розробити та ввести в дію протоколи захисту мережі та пристроїв.
6. Провести модернізацію ПК користувачів.
7. Провести навчання персоналу з інформаційної безпеки.
8. Скласти нову схему мережі підприємства.

Увесь цей процес ускладнювався тим, що підприємство було залежним від роботи в мережі інтернет та на сервері 1С. Тож першою і головною вимогою по модернізації мережі підприємства, було не зупиняти роботу підприємства під час виконання всіх робіт, та забезпечити:

- А. Безперебійне функціонування корпоративної пошти.
- В. Безперебійний доступ віддалених співробітників до серверу 1С.
- С. Безперебійний доступ до інтернет магазину підприємства.

Все це значно ускладнювало роботу по модернізації і плануванні роботи з мережею та вимагало чітких узгоджених дій і графіків виконання робіт.

Висновки до розділу 1

В першому розділі я описав покроково, на прикладі мережі ТОВ Партнер весь процес аналізу наявної мережі підприємства, склав схему та список встановленого обладнання існуючої мережі, та визначив вразливі місця. Описав подальші дії для модернізації всієї інфраструктури з урахуванням всіх побажань керівництва та вимог безпеки сьогодення.

					КІК.КР.Б-125-06-ПЗ	Арк.
						155
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділ 2. Розробка проекту підсистеми захисту мережної інфраструктури підприємства ТОВ Партнер

2.1. Розробка проекту модернізованої інфраструктури мережі
Розробка проекту модернізацій інфраструктури мережі підприємства «ТОВ Партнер» включає в себе такі пункти:

1. Заміна резервного каналу (провайдера) та збільшення швидкості основного.

Для того щоб прибрати з мережі вразливий і застарілий роутер для підключення інтернету по технології ADSL, прийнято рішення провести заміну резервного каналу (провайдера) який надавав доступ до мережі інтернет по ADSL зі швидкістю до 25 Мбіт/сек. на інший, який надавав доступ до мережі інтернет по оптоволоконній лінії по протоколу PPPOE зі швидкістю інтернет з'єднання до 50 Мбіт/сек. Також у зв'язку зі збільшенням персоналу на підприємстві, прийнято рішення підвищити швидкість основного каналу виходу в мережу інтернет з 50 Мбіт/сек. до 1000 Мбіт/сек.

2. Вибір оптимальної конфігурації робочих станцій (модернізація ПК користувачів)

Провести модернізацію визначених робочих станцій для того, щоб працівники підприємства могли комфортно виконувати свої функціональні обов'язки, та для продовження строку їх експлуатації.

А саме:

- А. Збільшити об'єм оперативної пам'яті (ОЗУ) з 2-4 Гб. до 8-16 Гб.
- В. Замінити зношені HDD диски на нові SSD диски.
- С. Заміна зношеної системи охолодження (кулерів) та заміну термопасти.
- Д. Заміна застарілих операційних систем (Windows XP) на більш нові (Windows 8/8.1/10/Linux) з розрядністю 64 біт.

					КІК.КР.Б-125-06-ПЗ	Арк.
						166
Змн.	Арк.	№ докум.	Підпис	Дата		

Е. Заміна периферійних пристроїв (Клавіатура, маніпулятор “миша”).

3. Підбір та встановлення Файл-сервера

(Файл-сервер це сервери з потужною дисковою підсистемою для централізації зберігання файлів та розмежування доступу до них, а також для забезпечення надійності зберігання. Окремі випадки файл-серверів - ftp-сервери і сервери-вузли розподілених файлових сховищ.)

Для кращого контролю обігу інформації на підприємстві, та для надійного захисту і резервування інформації, прийнято рішення для встановлення файлового серверу, в якості якого був обраний NAS (NAS — мережева система зберігання даних.) QNAP. В якості носіїв обрані HDD диски ємністю по 2 Тб. В якості дискового масиву, обрана технологія віртуалізації даних RAID 1 (RAID — технологія віртуалізації даних, яка об'єднує кілька дисків в логічний елемент для надійності збереження інформації та підвищення продуктивності накопичувачів. Дисковий масив — це набір дискових пристроїв, які працюють разом, щоб підвищити швидкість і/або надійність системи вводу/виводу.) Таке рішення має суттєво підвищити надійність збереження даних підприємства, та забезпечити контроль доступу до них. Також варто зазначити, що присутність файл сервера на підприємстві це швидше необхідність ніж забаганка ІТ спеціаліста.

4. Вибір та розгортання сервера бази даних (1С).

(Сервери баз даних виконують роль апаратної платформи для СУБД, зазвичай вони характеризуються найвищими вимогами надійності та обчислювальним навантаженням. Майже скрізь сервери БД працюють в режимі 24x7 (24 години, 7 днів на тиждень, займають центральне місце в ІТ-інфраструктурі підприємства і є об'єктом підвищеної уваги системних адміністраторів і інженерів. Основне завдання супроводу таких серверів - недопущення простоїв

					КІК.КР.Б-125-06-ПЗ	Арк.
						177
Змн.	Арк.	№ докум.	Підпис	Дата		

або принаймні їх мінімізація.) Виходячи із завдань і вимог підприємства та подальшого розширення штату працівників, прийнято рішення для заміни застарілого сервера 1С на більш потужний в якості якого обраний сервер ARTLINE Business R35 (Додаток D) з операційною системою Windows server 2012 R2. Також передбачалась модернізація і використання в якості резервного застарілого серверу 1С, шляхом заміни зношених HDD дисків на нові SSD та збільшити обсяг оперативної пам'яті (ОЗУ)

Характеристики сервера ARTLINE Business R35:

1. форм-фактор - 2U Rackmount
2. Процесор - Шестиядерний Intel Xeon E-2136 (3.3 - 4.5 ГГц)
3. Материнская плата - P11C-M/4L
4. Чіпсет - Intel C242
5. Об'єм оперативної пам'яті - 32 ГБ (DDR 4)
6. Тип процесора - Intel Xeon
7. Тип оперативной памяти - ECC DDR4-2666 МГц
8. Кількість ядер процесора - 6
9. Контролери SAS/SATA - Intel Rapid Storage Technology Enterprise (RSTe)
10. Рівні RAID - 0/1/5/10
11. Жорсткі диски - HDD: 2 x 2 ТБ, SSD: 2 x 480 ГБ і SSD: 2 x 240

ГБ

5. Вибір та встановлення Firewall (Головного пристрою)

(Комутаційний сервер, або головний пристрій, найчастіше є альтернативою активного мережевого устаткування, виконуючи важливі функції буферизації для користувача запитів (проху-сервери), динамічного розподілу ір-адрес (dhcр-сервери), забезпечуючи захист мережевої інфраструктури від несанкціонованого доступу та різного роду мережевих атак (firewall). Широке поширення отримали

					КІК.КР.Б-125-06-ПЗ	Арк.
						188
Змн.	Арк.	№ докум.	Підпис	Дата		

сервери-маршрутизатори і сервери для створення віртуальних приватних мереж (VPN). Комутаційний сервер, маршрутизатор, Firewall - це один з головних елементів інфраструктури будь якого підприємства, та чи не найголовніший інструмент ІТ спеціаліста. До підбору такого пристрою потрібно підходити вкрай серйозно, і враховувати всі наявні задачі і задачі які в перспективі доведеться вирішувати за допомогою даного приладу. Нехтування цим елементом інфраструктури, може призвести до фатальних наслідків для підприємства. Тож було прийнято рішення замінити застарілий ZyXEL USG 100, на більш новий і сучасний MikroTik RB3011. Пристрій має більш потужний процесор та об'єм оперативної пам'яті, поєднує у собі DHCP сервер, VPN сервер, NAT, Firewall та маршрутизатор, а також безліч допоміжних функцій, які можуть знадобитися в процесі роботи системному адміністратору.

Встановлення пристрою мало на меті зменшити кількість пристроїв (З мережі прибираються два застарілі роутери (TP-Link) через які раніше здійснювався доступ в інтернет), що в свою чергу підвищує надійність та захищеність роботи всієї мережі, а також спрощує топологію.

Також встановлення даного мережевого обладнання, давало змогу автоматизувати переключення інтернет каналів у разі відмови одного з них. Важливим фактором для вибору саме цього пристрою була цінова політика підприємства.

6. Вибір комутаторів (Switch)

(Мережевий комутатор або свіч (від англ. Switch - перемикач) - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.) Заміні підлягають всі роутери, які працюють в якості Switch. В якості Switch були обрані некеровані пристрої від фірми TP-Link на 6-8 портів зі швидкістю передачі даних

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

10/100 Мбіт/сек, що підвищують надійність і стабільність роботи сегментів мережі.

7. Вибір програмного забезпечення (ПЗ)

(Програмне забезпечення - сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм) Багато фірм в Україні використовують піратське програмне забезпечення, що в свою чергу нівелює практично всі заходи безпеки мережі, тому на ТОВ Партнер було прийняте рішення, використовувати тільки відкрите, або ліцензійне програмне забезпечення для уникнення таких проблем. Вибране таке програмне забезпечення:

А. Заміна застарілих операційних систем Windows XP на більш нові Windows 8/10/Linux (Ліцензійне/відкрите ПЗ)

В. Встановлення базових антивірусних програм від фірми Microsoft (Відкрите ПЗ)

С. Встановлення офісного пакету програм OpenOffice (Відкрите ПЗ)

Д. Встановлення поштового клієнта Thunderbird (Відкрите ПЗ)

Всі обрані програми за виключенням Microsoft Windows є програмним забезпеченням з відкритим кодом (Безкоштовне ПЗ), для систем Windows, підприємством раніше були закуплені ліцензії.

8. Складання оновленої топології (схеми) мережі

(Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі один щодо іншого та спосіб їх з'єднання лініями зв'язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити. У глобальних мережах структура зв'язків

					КІК.КР.Б-125-06-ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

звичайно схована від користувачів і не надто важлива, тому що кожний сеанс зв'язку може виконуватися по своєму власному шляху.)

Скласти оновлену схему інфраструктури мережі з урахуванням всіх внесених змін.

9. Налаштування гостьової мережі Free Wi-Fi.

Побудувати та налаштувати гостьову Wi-Fi мережу, використовуючи безпроводний канал. Ізолювати її від локальної мережі та мережі відеоспостереження для підвищення захисту всієї інфраструктури.

10. Налаштувати систему відеоспостереження.

Оновити та налаштувати програмне забезпечення наявних IP камер, відеосервера та POE Switch. Ізолювати їх від локальної та Wi-Fi мережі. Налаштувати віддалений доступ для керівництва підприємства.

2.2. Розробка моделі загроз для мережної інфраструктури підприємства

Перед тим як розробляти і будувати нову інфраструктуру мережі, нам потрібно розробити модель загроз для нашої інфраструктури, тобто передбачити заздалегідь можливі вразливі місця і наслідки для підприємства, в разі атаки на ці елементи. Також нам потрібно розробити протокол дії на випадок використання цих потенційних вразливостей зі сторони злоумисників.

Виходячи з вищесказаного і маючи завдання на модернізацію мережі з чітким списком обладнання і сервісів які будуть використані, можна скласти певний список потенційних загроз і наслідків вдалих, або частково вдалих атаки на них.

Потенційно вразливі місця мережі ТОВ Партнер:

					КІК.КР.Б-125-06-ПЗ	Арк.
						21
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Головний пристрій (Firewall) У разі вдалої атаки на пристрій зловмисник може паралізувати роботу всієї мережі, а також отримати доступ до певних встановлених пристроїв в ній.

2. Термінальні сервери з 1С базами. У разі вдалої атаки, зловмисник може викрасти, знищити або модифікувати інформацію. Такі дії неминуче призведуть до паралізації або повної зупинки роботи підприємства.

3. Файловий сервер підприємства. Аналогічні наслідки що і для термінальних серверів 1С.

4. Персональні ~~комп'ютери~~ комп'ютери співробітників. У разі взламу, або зараженні шкідливим програмним забезпеченням, виникає ризик втрати персональної даних (логіни та паролі до особистих кабінетів, серверів, акаунт пошти то що.)

2.3. Розробка проєкту підсистеми захисту мережі підприємства

Захист мережі підприємства це невід'ємна складова стабільного та успішного функціонування та розвитку всього підприємства в наш час. Розвиток технологій диктує стрімкий перехід бізнесу в інтернет простір який в свою чергу несе за собою безліч загроз, тому до підходу розробки проєкту підсистеми захисту мережі потрібно підходити вкрай відповідально і чітко розуміти, які вимоги висуваються до безпеки мережі в цілому, та до окремих її вузлів зокрема. В конкретно моєму випадку, розробка проєкту захисту мережі підприємства включає в себе такі пункти:

1. Налаштування VPN для підключення віддалених співробітників до серверів 1С (На заміну звичайного підключення по RDP протоколу по стандартному порту 3389 без VPN)

VPN з'єднання значно підвищує захисту мережі від зовнішніх загроз та посилює контроль доступу до інфраструктури та серверів. З поміж інших протоколів (PPTP, L2TP, L2TP+IPsec, OpenVPN) в якості

					КІК.КР.Б-125-06-ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

VPN обраний SSTP протокол. (*Secure Socket Tunneling Protocol* (протокол безпечного тунелювання сокетів), також званий SSTP — протокол прикладного рівня (*application-layer protocol*). Він спроектований для створення синхронного взаємозв'язку при спільному обміні інформацією двох програм. Завдяки йому можливо утворити декілька підключень програми по одному з'єднанню між вузлами, в результаті чого досягається ефективне використання мережевих ресурсів.) Створити профілі користувачів на сервері VPN та згенерувати ключі доступу. (Таке рішення значно підвищить надійність захищеності мережі та приведе її стан до загальноприйнятих міжнародних стандартів. Обраний протокол SSTP, який працює на 443 порту, та має високий рівень шифрування, підтримується Windows, Linux та Mac OS та чудову проходить через Firewall та NAT, що в свою чергу забезпечує надійність роботи VPN, особливо у випадках коли ви знаходитесь за NAT провайдера і маєте “сіру” IP адресу.)

2. Налаштування Firewall MikroTik RB3011:

(Міжмережевий екран, мережевий екран, брандмауер, фаєрвอลล์, файрвอลล์ — узагальнююча назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки)

A. Налаштування захисту пристрою MikroTik RB3011.

B. Налаштування доступу користувачів до інтернет ресурсів та ресурсів в локальній мережі.

C. Сегментування та налаштування безпеки локальної, відео та Wi-Fi мережі.

D. Впровадження та налаштування методу захисту мережі Honeypot використовуючи загально відомі порти 21, 22, 23, 3389.

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

Е. Впровадження та налаштування захисту пристрою та мережі від Brute Force атак.

Ф. Впровадження та налаштування захисту мережі від сканування відкритих портів.

Г. Створення резервної копії конфігурації пристрою після повного налаштування.

Н. Налаштувати адміністративний доступ до пристрою MikroTik RB3011.

3. Налаштувати права доступу для користувачів серверів 1С:

А. Розподілити користувачів на групи Administrator та Users з наданням відповідних прав доступу до програмного забезпечення та ресурсів серверів.

В. Відключити стандартні облікові записи Guest та Administrator.

С. Налаштувати політики безпеки Серверів 1С.

Д. Налаштувати політику поведінки системи при введенні невірних логінів і паролів користувачами.

Е. Налаштувати автоматичне резервування (BACKUP) системи серверів.

Ф. Встановити антивірусне програмне забезпечення та налаштувати його.

4. Налаштувати права доступу до спільних ресурсів на файловому сервері NAS QNAP.

А. Створити спільні ресурси (папки) користувачів для робочої інформації і назначити права доступу до них (Читання/ Читання та Видалення інформації)

В. Забезпечити автоматичне резервування (BACKUP) інформації на окремі носії.

С. Налаштувати адміністративний доступ до сервера.

					КІК.КР.Б-125-06-ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Налаштувати політики безпеки та права доступу до системи відеоспостереження.

А. Створити облікові записи користувачів відео серверу і надати їм відповідні права.

В. Замінити стандартні логіни і паролі на ІР камерах.

С. Налаштувати політику вводу невірних логінів і паролів.

Д. Налаштувати адміністративний доступ.

6. Налаштування політики безпеки WI-FI.

Замінити стандартні логіни і паролі для доступу до WI-FI роутерів, оновити програмне забезпечення та ізолювати мережу від інших.

7. Налаштування політики безпеки ІР телефонії підприємства.

Оновити програмне забезпечення ІР телефонів, замінити стандартні логіни і паролі для доступу до пристроїв.

Висновки до розділу 2

У цьому розділі були прописані чіткі кроки по модернізації та оптимізації наявної інфраструктури мережі підприємства, підібрані комплектуючі та нове обладнання, яке б замінило застаріле і неефективне обладнання, та забезпечило належне та стабільне функціонування підприємства, а також була прописана чітка схема модернізації і розробка нових політик безпеки мережі з урахуванням всіх побажань керівництва підприємства ТОВ Партнер та вимог до інформаційної та кібербезпеки.

					КІК.КР.Б-125-06-ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділ 3. Налагодження та тестування підсистеми захисту мережної інфраструктури підприємства ТОВ Партнер

3.1. Налагодження модернізованої мережної інфраструктури підприємства

1. Налагодження модернізованої мережної інфраструктури підприємства почав з налаштування головного пристрою, який відповідає за функціонування всієї мережі. Першим кроком було назначено статичну ір адресу 192.168.1.1 маршрутизатору MikroTik RB 3011. В конфігурації Firewall налаштовано проходження встановлених (Established) і пов'язаних (Related) з'єднань і скинуті некоректні (Invalid) з'єднання для транзитних (маршрутизованих) пакетів в ланцюжку Forward і призначених маршрутизатору в ланцюжку Input. Таким чином ми знизили навантаження на маршрутизатор обробивши ці дані на самому початку. Таке рішення заощаджує ресурси процесора, тобто ці правила будуть з самого початку нашої таблиці маршрутизації. Налагодження модернізованої мережевої інфраструктури підприємства продовжив з налагодження підключення до мережі інтернет через два провайдери (основний і резервний) Основний канал працює через протокол RPTP, резервний через RRPOE. Щоб підключитися до них на вкладці PPP додав два відповідні клієнти, в налаштування кожного з них, ввів IP адресу сервера підключення та пароль і логін для авторизації. Наявність інтернет з'єднання перевірів за допомогою штатної утиліти MikroTik - PING. Налаштував моніторинг каналів та автоматичне переключення з одного каналу, на інший у разі виникнення проблем. Моніторинг та переключення реалізоване через інструмент netwatch. Ідея в тому, що інструмент (Додаток В, Рисунок В.1, В.2) кожні 60 секунд (в моєму випадку) відправляє ping пакет на IP адресу 8.8.4.4 (google) і повинен отримати відповідь протягом 1000 мс. У разі “втрати” пакета або

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

перевищенні часу відгуку, канал вважається недоступним і виконується скрипт (додаток 4) для переключення на резервний канал виходу в інтернет. Перехід на основний канал відбувається за іншою схемою, все той же інструмент після переходу на резервний канал продовжує відсилати ring пакети до тих пір, поки не отримує відповідь, після чого скрипт перемикає канал з резервного на основний канал. Після цього на пристрої увімкнув та налаштував DHCP сервери для локальної мережі (пул адрес 192.168.1.2-192.168.254, шлюз 192.168.1.1) та мережі гостьового Wi-Fi (пул адрес 192.168.50.2-192.168.50.100, шлюз 192.168.50.1) Налаштував NAT, для того щоб користувачі мали доступ до мережі інтернет.

2. На відміну від старої схеми, в якій всі пристрої знаходились в одній мережі 192.168.1.0/24, в новій всі пристрої в інфраструктурі я розділив на 3 підмережі з окремими DHCP серверами та назначив для кожної окремий пул ір адрес. Такий поділ полегшує управління пристроями, підвищує захист та дає змогу більш тонкого налаштування всієї інфраструктури.

А. Локальна мережа з пулом ір адрес 192.168.1.2-192.168.1.254 маска 255.255.255.0 шлюз 192.168.1.1

В. Мережа для гостьового Wi-Fi з пулом ір адрес 192.168.50.2-192.168.50.100 маска 255.255.255.0 шлюз 192.168.50.1

С. Мережа для системи відеоспостереження з пулом ір адрес 192.168.10.5-192.168.10.50 маска 255.255.255.0 шлюз 192.168.10.1

3. Налагодження VPN серверу. Для підключення віддалених користувачів. На пристрої MikroTik RB3011 увімкнув та налаштував VPN сервер з окремим пулом IP адрес (10.1.1.1-10.1.1.30). Для користувачів згенерував сертифікати доступу. Увімкнув SSTP протокол з обов'язковою перевіркою сертифіката. Шифрування

					КІК.КР.Б-125-06-ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

трафіку відбувається ключем AES 256 біт, цього на мою думку більш ніж достатньо для захисту інформації всередині тунелю. Для стабільної роботи VPN, обраний спосіб підключення віддалених користувачів через DDNS (*Динамічний DNS - це метод автоматичного оновлення сервера імен в системі доменних імен, часто в режимі реального часу, з активною конфігурацією DDNS його налаштованих імен хостів, адрес або іншої інформації. Термін використовується для опису двох різних понять.*)

(Додаток В, Рисунок В.3) що дає змогу автоматичного переключення тунелю у разі переходу з одного каналу виходу в інтернет на інший. SSTP протокол працює через 443 порт і тим самим забезпечує чудову “прохідність” трафіку між пристроями. Оновлення актуальної IP адреси для DDNS налаштував кожні 60 секунд. Увімкнув режим авторизації “ONLY ONE”, один користувач на один логін і пароль. За допомогою маршрутизації, налаштував проходження трафіку між віддаленими користувачами і серверами 1С.

4. Для вхідного (input) трафіку відкрив порт 443 (VPN) та порт XXXX для віддаленого управління пристроєм за допомогою програмного забезпечення Winbox, а також протокол ICMP (*ICMP — мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних.*) для можливості надсилати ping пакети на пристрій і отримувати відповідь про його доступність. Перевів Firewall в “нормально закритий” стан для підвищення захисту пристрою. Будь який Firewall повинен обов'язково володіти таким правилом, вище ми обробляємо з'єднання і дозволяємо тільки те, що нам необхідно, все інше блокуємо, на мою думку це набагато правильніше, ніж дозволити все і блокувати тільки потрібне вам.

					КІК.КР.Б-125-06-ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

5. На основному сервері 1С встановив систему Windows server 2012R2. (Була в наявності) Всі жорсткі диски попарно сформував в Raid 1 масиви. Перший Raid масив з SSD дисків Samsung EVO на 480GB виділив під систему, другий Raid масив з SSD дисків Kingston HyperX Fury 3D 240GB виділив під базу 1С, третій Raid масив з HDD дисків Toshiba на 2TB виділив під робочу інформацію. Для користувачів створив облікові записи Users з відповідними правами. Налаштував оновлення системи по запиту адміністратора. Налаштував автоматичне резервне копіювання системи на два різні носії з авторизацією за паролем. Назначив статичну IP адресу 192.168.1.4/24. На резервному сервері замінив HDD диски на SSD від фірми Kingston модель DC500M 480GB і об'єднав їх попарно в Raid 1 масиви. Один масив під систему, другий під базу 1С. Встановив систему Windows server 2012R2 яка була в наявності. Назначив статичну адресу 192.168.1.8/24 створив облікові записи для користувачів ідентичні обліковим записам основного серверу.

6. Встановив та налаштував файловий сервер фірми QNAP. На нього встановив два HDD диски Toshiba по 2 Тб, які об'єднав в Raid 1 масив. Налаштував доступ за логіном та паролем для адміністратора. Для робочої інформації персоналу, створив спільні папки з відповідними правами. Налаштував автоматичне резервне копіювання інформації кожного дня. Для сервера назначив статичну IP адресу 192.168.1.48/24.

7. Для покриття всього офісу підприємства Wi-Fi, створив гостьову мережу, яка включає в себе 3 роутера від фірми Asus. Один виступає як точка доступу, під'єднаний до головного пристрою по протоколу Ethernet (*Ethernet — найпопулярніший протокол кабельних комп'ютерних мереж, що працює на фізичному та каналному рівні мережевої моделі OSI.*) два інші під'єднані до нього по WI-Fi і

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

працюють в режимі репітера. (*Wi-Fi репітер* – окремий пристрій, який доповнює роутер. Завдання репітера, збільшити дальність поширення сигналу, який передає роутер, його робота ґрунтується на прийомі сигналу від маршрутизатора та подальшій його передачі для розширення *Wi-Fi мережі*.) Для Wi-Fi мережі виділив окремий DHCP сервера, та пул ір адрес з 192.168.50.5 по 192.168.50.100. з маскою 255.255.255.0

8. Для системи відеоспостереження виділив DHCP сервер та окремий пул ір адрес з 192.168.10.5 по 192.168.10.50 з маскою 255.255.255.0 Всі IP камери підключив через POE до Switch, а його підключив до головного пристрою за допомогою Ethernet в окремий виділений порт. Також до Switch через Ethernet під'єднав відеосервер. Система відеоспостереження обов'язково, за вимогою керівництва повинна була мати віддалений доступ, тому за допомогою VPN, був налаштований доступ за логіном і паролем, для керівництва.

9. Всі робочі станції (ПК) були об'єднані в однорангову локальну мережу і під'єднані в робочу групу (Workgroup) підприємства. (*Робоча група Windows (англійською мовою Workgroup) є функцією операційних систем Microsoft. На практиці це набір комп'ютерів, підключених до мережі, і його функція полягає в тому, щоб закласти основи, необхідні для обміну файлами і принтерами між ПК. Комп'ютер, який є членом робочої групи, може дозволити іншому комп'ютеру, що є членом тієї ж групи, доступ до своїх загальних ресурсів. Комп'ютери, які є членами різних робочих груп, але які належать до однієї локальної мережі, можуть безпосередньо отримувати доступ до загальних ресурсів в групі, до якої вони належать.*) Для локальної мережі виділений окремий DHCP сервер з пулом адрес 192.168.1.2-192.168.1.254 маска 255.255.255.0 На всіх персональний комп'ютерах налаштував автоматичне оновлення

					КІК.КР.Б-125-06-ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

системи. Підключення до серверів 1С організував за допомогою RDP за логіном та паролем.

10. Для кожного робочого місця під'єднав IP телефон.

Налаштував отримання IP адреси для телефонів по DHCP, з пулу адрес локальної мережі 192.168.1.0/24

3.2. Налагодження підсистеми захисту мережі підприємства

1. Налагодження безпеки головного пристрою (маршрутизатора) MikroTik RB3011:

1.1 Захист пристрою від несанкціонованого доступу (взлому) включає в себе відключення служб та протоколів управління пристроєм, які не використовуються (Додаток В, Рисунок В.4) та заміни стандартного порту 8291 на нестандартний з “високого регістру” незайнятих портів віддаленого управління пристроєм, а також створення access list для контрольованого доступу до приладу. Для управління пристроєм виробник передбачив такі варіанти підключення:

- А. Спеціалізоване програмне забезпечення Winbox порт 8291
- В. WWW (Браузер) порт 80 (HTTP) и 443 (HTTPS)
- С. API порт 8728
- Д. FTP порт 21
- Е. Telnet порт 23
- Ф. SSH порт 22

Був обраний єдиний варіант управління за допомогою програмного забезпечення Winbox із заміною стандартного порту 8291 на порт з високого регістру. Всі решта варіантів відключені для захисту маршрутизатора. Пристрій має вбудований DNS сервер який зловмисники часто використовують для “підсилення” DDoS атак.
(DNS Amplification цей вид атак використовує специфіку роботи DNS

					КІК.КР.Б-125-06-ПЗ	Арк.
						331
Змн.	Арк.	№ докум.	Підпис	Дата		

служб в мережі Інтернет. Суть полягає в тому, щоб запросити у публічного DNS-сервера дані про домен і направити його відповідь на сервер що атакується. При реалізації даного типу атаки зловмисник формує запит, у відповідь на який DNS-сервер повертає якомога більше даних. Наприклад, запит списку всіх DNS-записів в певній зоні. Оскільки в протоколі UDP не провадиться перевірка IP-адрес джерела, зловмисник генерує запити від імені сервера-жертви, вказуючи його IP-адресу в поле вихідної адреси. Основною метою зловмисника є заповнення каналу сервера-жертви об'ємними відповідями від публічних DNS-серверів. Так, використовуючи всього кілька ботів для генерації запитів до публічних DNS-серверів, зловмисник може збільшити потік "сміттєвого" трафіку в багато разів. При цьому вичислити зловмисника, або хоча б IP-адреси джерело запитів майже неможливо, тому що реальна вихідна IP-адреса завжди змінюється на іншу.) Для недопущення цієї ситуації правилом Firewall був заборонений вхідний (input) трафік з WAN портів по UDP/TCP на 53 (DNS) порт. Також для захисту маршрутизатора від несанкціонованого доступу було, зміна стандартного логіну та паролю (admin) на більш складний, відповідно до політики безпеки підприємства. Останнім рубежем захисту, були встановлені правила фільтрації трафіку які захищають віддалений доступ на маршрутизатор з WAN портів від Brute Force атак. Принцип роботи цих правил дуже простий, перший фільтр фіксує нове з'єднання через порт управління маршрутизатором і заносить IP адресу з якої надходять пакети в List_1 на 10 хвилин. Якщо протягом 10 хвилин з цієї IP адреси надходять спроби нового з'єднання, то адреса заноситься в наступний фільтр List_2 теж на 10 хвилин. Таких списків я встановив 4. Після попадання IP адреси в List_4, який я назвав Blacklist Winbox, вона залишається там до моменту поки її

					КІК.КР.Б-125-06-ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

звідти не видалить системний адміністратор. І останнім правилом блокується будь який трафік з List_4 (Blacklist Winbox) на маршрутизатор.

1.2 Впровадження та налаштування системи-приманки, для виявлення та блокування вторгнень Honeypot. (*Honeypot («Пастка» (англ. голиця з медом) — ресурс, що є приманкою для зломисників. Мета Honeypot — зазнати атаки або несанкціонованого дослідження, що згодом дозволить вивчити стратегію зломисника та визначити перелік засобів, за допомогою яких можуть бути завдані удари реально наявним об'єктам безпеки. Реалізація Honeypot може бути спеціальним виділенням сервером, або мережевим сервісом, завдання якого — привернути увагу зломисника. Honeypot є ресурсом, що без будь-якого впливу на нього є неактивним. Honeypot збирає невелику кількість інформації, після аналізу якої будується статистика методів, якими користуються зломисники, а також визначається наявність якихось нових рішень, які згодом будуть застосовуватися в боротьбі з ними.*) Для створення пастки були обрані популярні порти, які не використовуються для зовнішнього доступу до мережі підприємства, та які часто сканують зломисники:

- A. 3389 порт (RDP)
- B. 21 порт (FTP)
- C. 23 порт (SSH)
- D. 23 порт (Telnet)
- E. 8291 стандартний порт управління пристроєм за

допомогою програмного забезпечення Winbox.

Ідея полягає в тому, щоб фіксувати будь який трафік на ці порти і додавати всі IP адреси, які їх сканують в окремий blacklist, а потім всі адреси, які входять в цей blacklist блокувати на певний проміжок часу. В моєму випадку такі IP адреси блокуються на 3 доби, для того щоб

					КІК.КР.Б-125-06-ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

не перевантажувати ресурс пристрою. Такий нескладний метод захисту, значно підвищує безпеку мережі підприємства від вторгнень, та дає статистику мережевої активності на зовнішніх інтерфейсах пристрою. До прикладу в середньому за добу фіксується і блокується близько 100-150 ір адрес які потрапляють в пастку.

1.3 Впровадження та налагодження системи запобігання сканування відкритих портів пристрою (PSD – Port Scan Detection). На рахунок даного правила є різні думки, хтось вважає, що воно не потрібно, хтось, що потрібно. Я ж вирішив трохи себе підстрахувати, тим більше, що завдяки цьому правилу blacklist port scanner активно заповнюється зарубіжними ІР адресами. Щоб запобігти скануванню портів пристрою, я налаштував фільтр вхідного (input) трафіку таким чином, щоб він фіксував спроби сканувати “високі” і “низькі” порти. (Додаток В, Рисунок В.5, В.6, В.7). *(Для кожного з протоколів TCP і UDP стандарт визначає можливість одночасного виділення на хості до 65536 унікальних портів, що ідентифікують номерами від 0 до 65535. Перші 1024 порти зарезервовані під різні сервіси та програмне забезпечення і називаються “низькі порти”, всі решта “високі порти” не зайняті і можуть використовуватися будь ким.)* Задум дуже простий, сканер портів генерує пакет SYN, якщо порт на кінцевому хості відкритий, то з нього прийде пакет SYN-ACK. У відповідь сканер відправляє пакет RST, який закриває з'єднання ще до того як завершується встановлення сесії. Саме ці пакети відслідковує фільтр і якщо з однієї ІР адреси приходять запити на різні порти протягом певного відрізка часу, то така адреса заноситься в blacklist port scanner який блокується окремим правилом Firewall. Для низьких портів виставив фільтр спрацювання більше трьох запитів, протягом трьох секунд, на високі два і більше, протягом трьох секунд.

2. Налагодження безпеки гостьової мережі (Free Wi-Fi)

					КІК.КР.Б-125-06-ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

Для безпеки на пристроях замінені стандартні паролі і логіни адміністратора на більш складні, згідно з політикою безпеки. Вся Wi-Fi мережа повністю ізольована від локальної та мережі відеоспостереження підприємства міжмережним екраном, який забороняє будь-який трафік між ними, що в свою чергу включає проникнення з гостьової мережі і нанесення пошкоджень робочим станціям та серверам.

3. Налагодження протоколів безпеки Серверів 1С
Захист серверів 1С включає в себе:

А. Заборона користувачам встановлювати, або змінювати самостійно паролі доступу до облікових записів. Така політика введена для контролю та виключення встановлення слабких та не надійних паролів користувачами.

В. Надання мінімальних прав користувачам, по принципу надання прав по мірі їх потреби, щоб виключити будь-які несанкціоновані дії на сервері з боку користувачів.

С. Блокування облікових записів користувачів у разі невірного вводу паролю, встановлена на рівні 3 спроб протягом 10 хвилин. Встановлюється такий захист від підбору паролів в редакторі локальної групової політики, в політиці блокування облікових записів. (команда gpedit.msc) Якщо користувач ввів за 10 хвилин 3 рази невірно пароль, його обліковий запис блокується на 30 хвилин. Така політика дає змогу мінімізувати можливість підібрати пароль злоумисником.

Д. Автоматичне створення резервної копії системи серверів 1С. Резервне копіювання налаштовано на окремий жорсткий диск з доступом тільки для адміністратора та за паролем. Копіювання налаштоване кожного дня о 12:00 ночі. Такий час вибраний для того, щоб звільнити увесь ресурс серверів для задач резервного копіювання.

					КІК.КР.Б-125-06-ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

Е. Встановлений антивірус і налаштоване автоматичне оновлення та повне сканування системи кожного дня в 2:00 ночі. У разі виявлення шкідливого програмного забезпечення, антивірус по замовчуванню вносить його до карантину і подальші дії щодо таких файлів, вирішуються адміністратором в ручному режимі, щоб виключити випадкового пошкодження або видалення критичних для системи файлів.

Ф. Резервне копіювання бази 1С. Резервування відбувається автоматично за допомогою програмного забезпечення Effector saver з 4:00 до 6:00 ранку. Інформація зберігається за період 10 днів, на двох різних носіях з доступом за паролем.

Г. Заборона використання браузерів для користувачів. Така політика виключає потрапляння на сервери зловмисного програмного забезпечення через браузери, у разів скачування файлів з сумнівних ресурсів, а також підвищує в цілому захист серверів.

Н. За допомогою редактора групових політик (команда gpedit.msc) заборонено користувачам встановлювати та видаляти програмне забезпечення, а також заборонено використання PowerShell та командного рядка.

4. Налагодження безпеки системи відеоспостереження
Зовнішній доступ до системи відеоспостереження налаштований через VPN з'єднання. Логіни і паролі на ір камерах та на сервері відеоспостереження замінені на більш складні та надійні. Мережа ізольована від інших міжмережним екраном, який забороняє проходження трафіку з інших мереж. Доступ в систему чітко контрольований по облікових записах. Також для більшого контролю за системою відеоспостереження, на міжмережному екрані, налаштований фільтр який фіксує всі ір адреси які підключаються, або намагаються підключитися до неї. Таке рішення дає повну

					КІК.КР.Б-125-06-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

інформацію для адміністратора про те, хто коли і з якої ір адреси підключався або намагався підключитися до системи і в свою чергу дає змогу швидко реагувати на інциденти.

5. Налагодження безпеки IP телефонів

На IP телефонах були замінені стандартні логіни і паролі з admin/admin на більш складні і нестандартні, та відключені протоколи Telnet і SSH для доступу до пристроїв. Оновлене програмне забезпечення до останньої доступної версії і налаштовано автоматичне оновлення пристроїв. Додатково на пристроях було обмежено доступ до налаштувань з клавіатури. Для доступу до WEB інтерфейсу залишено стандартний порт 80/433 (HTTP/HTTPS)

3.3. Тестування роботи модернізованої мережної інфраструктури та підсистеми захисту мережі підприємства

Тестування системи почав з перевірки надійності роботи системи безперебійного живлення, було декілька разів відключено живлення, для того щоб переконатися, що система спрацює так як нам потрібно і не виникає ніяких критичних збоїв. Наступним етапом стала перевірка роботи резервування інтернет каналів, по черзі був вимкнений кожний із них, для того щоб перевірити чи спрацьовує автоматичне переключення з одного каналу на інший в разі відключення одно з них. За автоматичне переключення і контроль стану каналів відповідає MikroTik RB3011, а саме інструмент Netwatch.

Суть роботи Netwatch полягає в тому щоб через певний проміжок часу, в нашому випадку кожні 15 секунд, відправляти ping на певну ір адресу і якщо Netwatch не отримує відгук протягом встановленого проміжку часу, то інтернет канал вважається непрацюючим і подається команда на переключення на резервний канал, до моменту поки на основному знов не з'явиться зв'язок. Переключення відбувається за допомогою скриптів.

					КІК.КР.Б-125-06-ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком була проведена перевірка на відкриті порти, для того щоб переконатися в тому, що всі небажані порти закриті і зловмисники не можуть їх використати для проникнення в мережу. Для проведення перевірки були використані онлайн сервіси перевірки відкритих портів.

Як видно з Додатку С, (Рисунок С.1) всі порти закриті, крім 443, який використовується для роботи VPN.

Завершальним етапом тестування стало проведення повного сканування системи на вразливість з середини за допомогою програмного забезпечення netmap. Додаток С, (Рисунок С.2) Сканування з середини проводилось з метою виявити вразливості які були пропущені під час налаштування мережі.

«Network Mapper» — (укр. енмєп) безкоштовне відкрите програмне забезпечення для дослідження та аудиту безпеки мереж та виявлення активних мережевих сервісів.

					КІК.КР.Б-125-06-ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок

В проєкті детально показано увесь процес модернізації мережі підприємства, від дослідження і виявлення вразливих місць, до повної модернізації та тестування.

На першому етапі був проведений аудит всієї мережі підприємства, виявлені вразливі місця, та розроблений план модернізації. На другому етапі був складений детальний план та підібрані комплектуючі для заміни. На третьому було проведено налагодження, тестування модернізованої системи, та складено схему.

В результаті проробленої роботи було значно підвищено відмовостійкість та захищеність мережі, ми отримали надійну та водночас відносно не дорогу інфраструктуру підприємства, яка виконує всі поставлені задачі. Перед нами було поставлено завдання побудувати захищену, надійну і в той же час відносно просту мережу, відповідно до вимог підприємства, та їх фінансових можливостей. В систему були втілені рішення, які підвищували надійність і захищеність системи, після налагодження система пройшла тестування, та до налаштування і на даний час працює на підприємстві ТОВ Партнер.

					КІК.КР.Б-125-06-ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1) Літнарівч Р. М. Сучасні технології інформаційної безпеки – Навчальний посібник – Рівне 2011.
- 2) Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009 (рос.).
- 3) Wikipedia.org/wiki/Інформаційна_безпека.
- 4) Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуци В. Г. — Київ. 2004. — 508 с.
- 5) Степанов И. Шпиономания или обыкновенный промышленный шпионаж – Бизнес и безопасность, 1997, № 5.
- 6) Брягин О. Простая арифметика. – Бизнес и безопасность, 1998, № 1,с.
- 7) Закон України “Про інформацію” // Відом. Верховної Ради УРСР. – 1992. - № 48.
- 8) Низенко Е., Камняк В. Забезпечення інформаційної безпеки підприємництва. – К.: МАУП, 2006.
- 9) Кормич Б. Інформаційна безпека: організаційно-правові основи. – К.: Кондор, 2004.
- 10) Зубок М. Правове регулювання безпеки підприємницької діяльності. – К.: КНТЕУ, 2005.
- 11) Зубок М. Інформаційна безпека. – К.: КНТЕУ, 2005.
- 12) Берлач А. Безпека бізнесу. – К.: Університет «Україна», 2007.
- 13) Електронна комерція: Навч. посібник / А.М. Береза, І.А. Козак, Ф.А. Шевченко та ін. – К.: КНЕУ, 2002. – 326 с.
- 14) Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. №851-IV.
- 15) Вербицкий О.В. Вступление к криптологии. - Львов: Издательство научно-технической литературы, 1998.
- 16) Яскевич В. Секьюрити. Организационные основы безопасности фирмы. – М.: Ось-89, 2005.
- 17) Степанов Е., Корнеев И. Информационная безопасность и защита информации. – М. Инфра – М, 2001.
- 18) Кузнецов И. Бизнес-безопасность. – М.: ИД «Дашков и К», 2006.

ДОДАТКИ

					КІК.КР.Б-125-06-ПЗ	Арк.
						441
Змн.	Арк.	№ докум.	Підпис	Дата		



Схема мережі ТОВ Партнер після модернізації

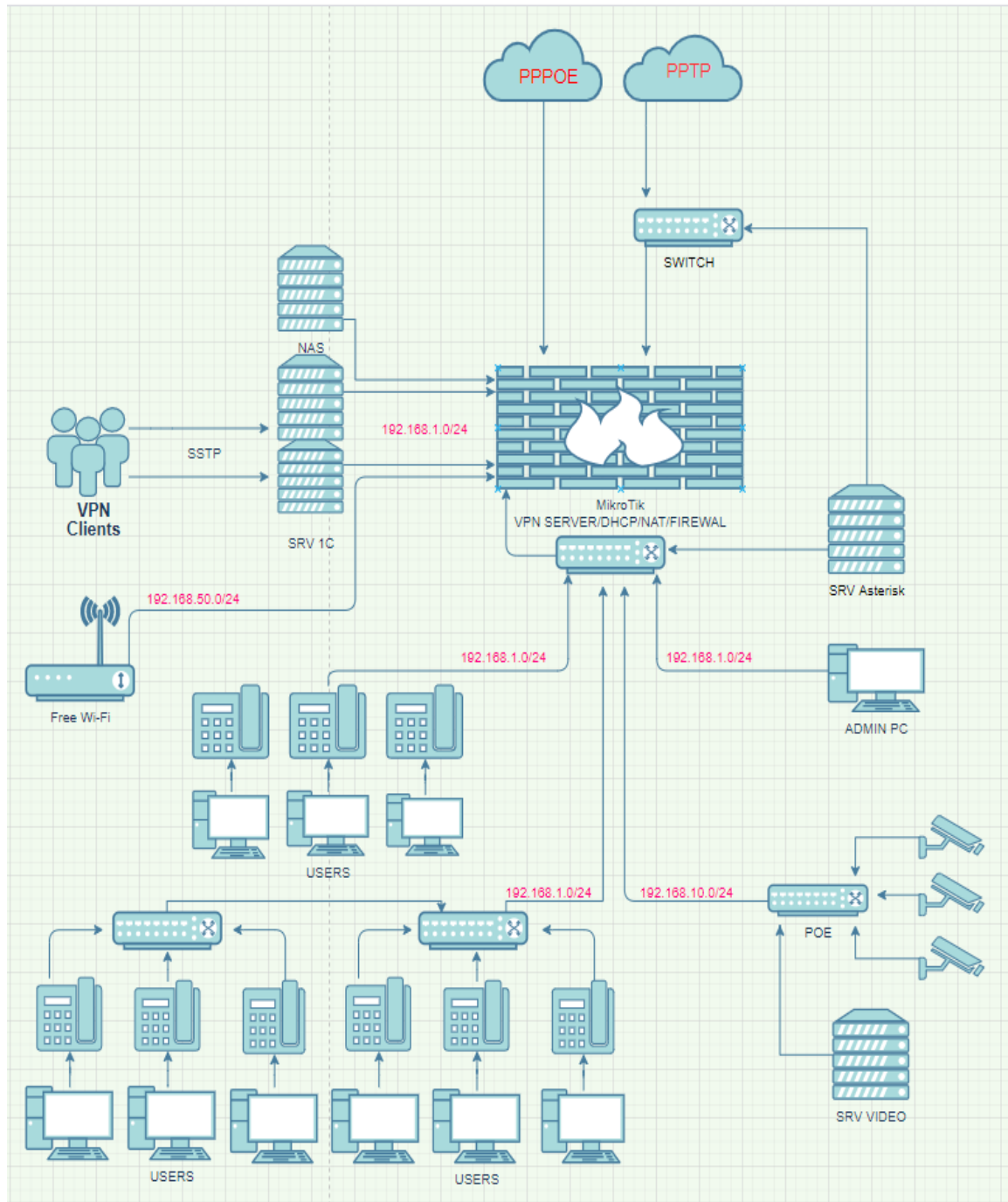


Рисунок А.2

Приклади елементів інтерфейсу налаштування мережних пристроїв

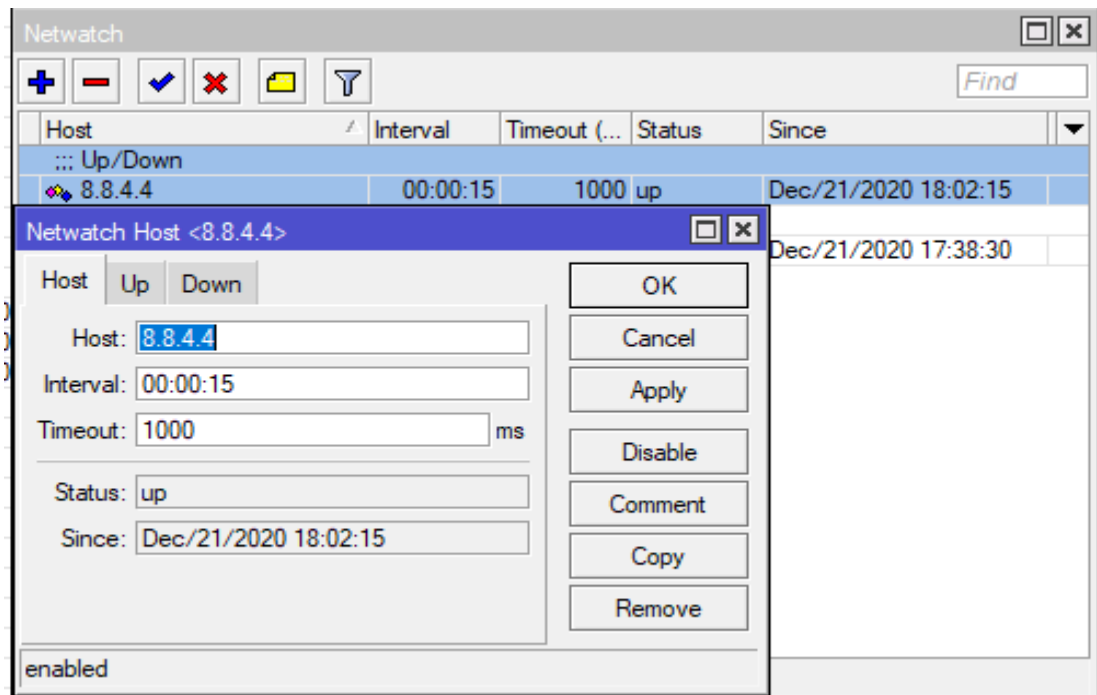


Рисунок В.1

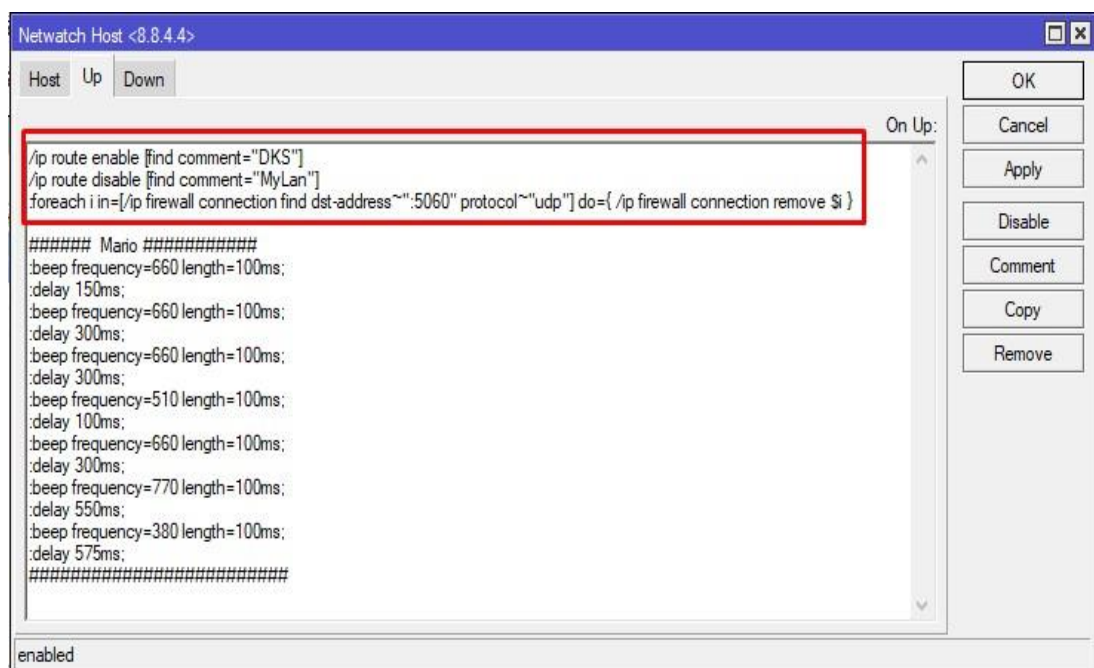


Рисунок В.2

Cloud

☒ DDNS Enabled

DDNS Update Interval: 00:01:00

☒ Update Time

Public Address: 195.244.178.246

DNS Name: 195.244.178.246.mynetname.net

☐ Use Local Address

OK

Cancel

Apply

Force Update

updated Router is behind a NAT. Remote connection might not work.

Рисунок В.3

IP Service List

Find

Name	Port	Available From	Certificate
X api	8728		
X api-ssl	8729		none
X ftp	21		
X ssh	22		
X telnet	23		
winbox	58505	0.0.0.0/0	
X www	80		
X www-ssl	443		none

8 items (1 selected)

Рисунок В.4

Ports scanner

Port	Protocol	Source	Destination	Port Scanners	Size	Count
21	drop	input			360 B	8
22	add src to address list	input	6 (tcp)	WAN	0 B	0
23	add src to address list	input	6 (tcp)	WAN	0 B	0
24	add src to address list	input	6 (tcp)	WAN	0 B	0
25	add src to address list	input	6 (tcp)	WAN	0 B	0
26	add src to address list	input	6 (tcp)	WAN	0 B	0
27	add src to address list	input	6 (tcp)	WAN	0 B	0
28	add src to address list	input	6 (tcp)	WAN	0 B	0
29	add src to address list	input	6 (tcp)	WAN	0 B	0
30	add src to address list	input	6 (tcp)	WAN	0 B	0
31	add src to address list	input	17 (udp)	WAN	0 B	0

Рисунок В.5

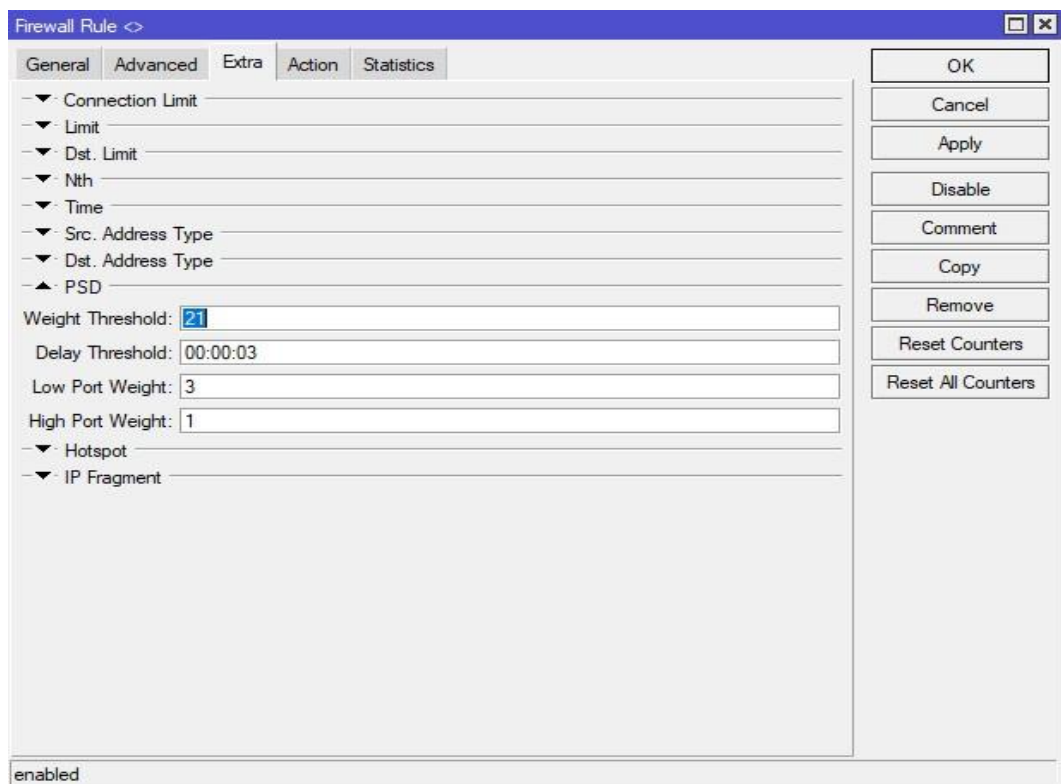


Рисунок В.6

Port Scanners	187.210.226.214	Sep/07/2020 02:56:34
Port Scanners	103.139.212.212	Sep/07/2020 22:23:38
Port Scanners	94.103.87.212	Sep/08/2020 17:34:32
Port Scanners	172.104.242.173	Sep/08/2020 18:49:33
Port Scanners	124.88.55.15	Sep/08/2020 21:11:29
Port Scanners	202.102.67.181	Sep/08/2020 21:30:54
Port Scanners	219.128.254.94	Sep/09/2020 07:46:10
Port Scanners	103.139.212.211	Sep/09/2020 18:45:38
Port Scanners	89.248.168.157	Sep/12/2020 16:38:27
Port Scanners	121.199.53.239	Sep/15/2020 04:55:21
Port Scanners	103.124.107.26	Sep/15/2020 17:45:23
Port Scanners	104.241.228.131	Sep/17/2020 16:16:19
Port Scanners	59.188.7.109	Sep/19/2020 00:16:05
Port Scanners	218.22.223.201	Sep/19/2020 07:28:21
Port Scanners	89.248.172.208	Sep/24/2020 12:46:55
Port Scanners	141.136.37.245	Sep/24/2020 16:13:27
Port Scanners	87.251.70.79	Sep/29/2020 04:34:28
Port Scanners	203.98.96.180	Oct/01/2020 04:17:39
Port Scanners	123.146.23.149	Oct/03/2020 05:02:56
Port Scanners	104.152.52.36	Oct/03/2020 21:25:39
Port Scanners	179.206.208.247	Oct/08/2020 01:20:43
Port Scanners	219.150.189.215	Oct/08/2020 06:41:08
Port Scanners	141.98.10.173	Oct/11/2020 03:26:31
Port Scanners	85.93.20.46	Oct/14/2020 00:15:50
Port Scanners	192.254.75.11	Oct/14/2020 13:30:23
Port Scanners	104.152.52.28	Oct/18/2020 20:07:34
Port Scanners	91.123.157.56	Oct/24/2020 06:49:15

Рисунок В.7

Сканер портів

Він показує, які порти відкриті на вашому комп'ютері або сервері, і за що вони відповідають. Перевірка відбувається через сканер nmap і відображає, наскільки відкритий ваш пристрій для зовнішнього світу.

Введіть IP-адресу або домен

173.216

[Вставити мою IP-адресу](#)

Введіть IP-адресу або домен

Популярні порти

Результати перевірки

Not shown: 999 filtered ports

PORT	STATE	SERVICE
443/tcp	open	https

Nmap done: 1 IP address (1 host up) scanned in 20.36 seconds

Почати сканування

Якщо результат «Host seems down», значить мережевий екран або роутер IP-адреси, що перевіряється, блокує пінг.

Рисунок С.1

					КІК.КР.Б-125-06-ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

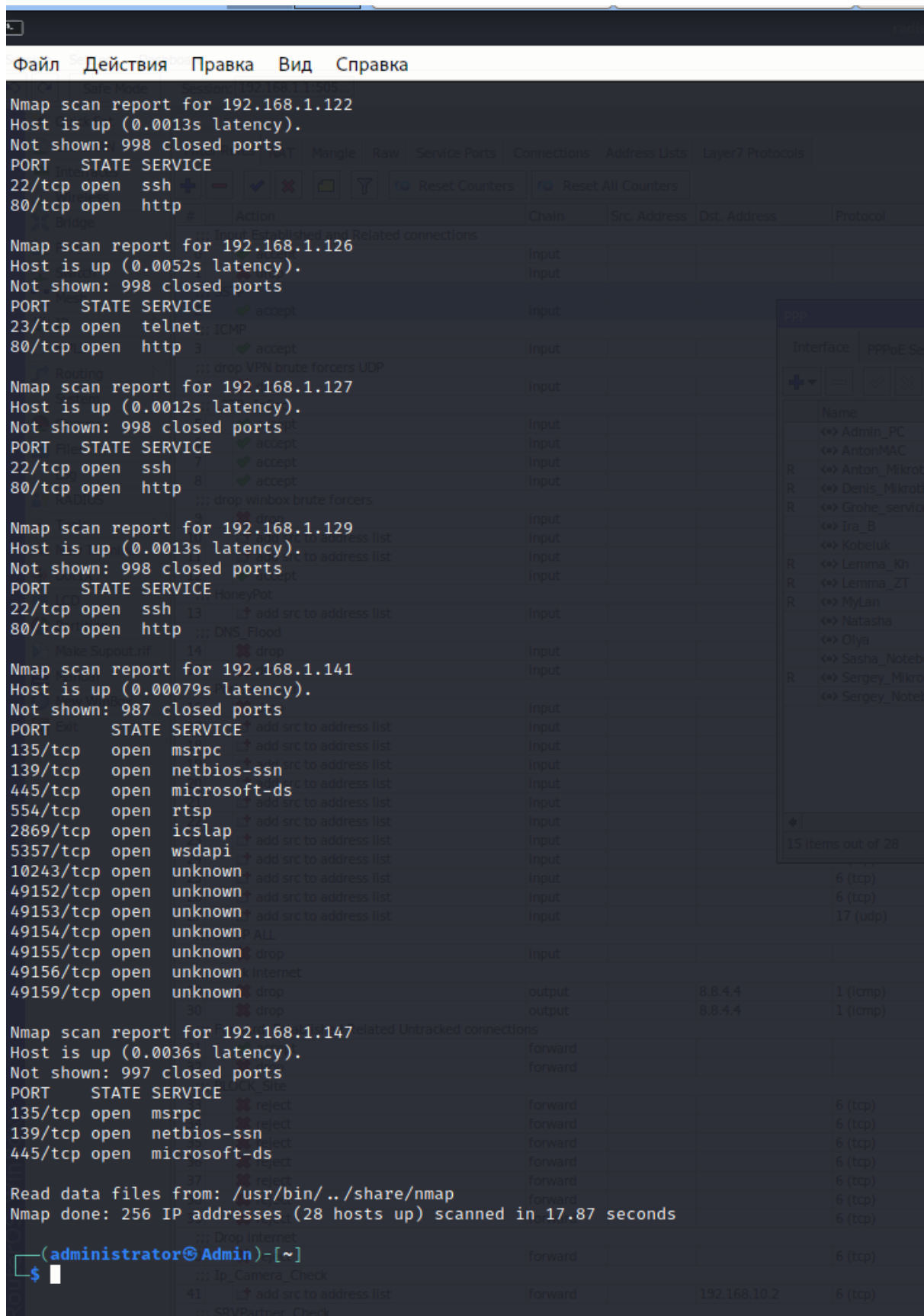


Рисунок С.2

Встановлене обладнання



Конфігурація MikroTil RB3011

MikroTik RouterOS 6.47.10 (c) 1999-2021 <http://www.mikrotik.com/>

[?] Gives the list of available commands

command [?] Gives help on the command and list of arguments

[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level

.. Move up one level

/command Use command at the base level

feb/09/2021 19:41:04 system,info,critical Firmware upgraded successfully, please r
eboot for changes to take effect!mar/17/2021 10:06:08 system,error,critical login failure for user radist from 192.
168.1.8 via winboxmar/17/2021 10:06:21 system,error,critical login failure for user radist from 192.
168.1.8 via winbox

[radist@PARTNER] > export compact

jun/18/2021 11:20:15 by RouterOS 6.47.10

software id = 8UVN-V6A4

#

model = RB3011UiAS

serial number = B8950B03D50A

/interface l2tp-server

add name=Admin_PC user=radist

add name=AntonMAC user=AntonMAC

add name=Ira_B user=Ira_B

add name=Kobeluk user=Kobeluk

add name=Olya user=OlgaN

add name=Sasha_Notebook user=Sasha

add name=Sergey_Notebook user=Uswer_4

/interface bridge

add dhcp-snooping=yes igmp-snooping=yes name=bridge

add igmp-snooping=yes name=bridge_Guest

/interface ethernet

set [find default-name=ether1] name=WAN_1

set [find default-name=ether2] name=WAN_2

set [find default-name=ether3] loop-protect=on rx-flow-control=auto \

					КІК.КР.Б-125-06-ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tx-flow-control=auto
set [ find default-name=ether4 ] loop-protect=on
set [ find default-name=ether5 ] loop-protect=on
set [ find default-name=ether6 ] loop-protect=on
set [ find default-name=ether7 ] loop-protect=on
set [ find default-name=ether8 ] loop-protect=on
set [ find default-name=ether9 ] advertise=\
    100M-half,100M-full,1000M-half,1000M-full loop-protect=on \
    loop-protect-disable-time=1m
set [ find default-name=ether10 ] loop-protect=on loop-protect-disable-time=1m
set [ find default-name=sfp1 ] disabled=yes
/interface pppoe-client
add disabled=no interface=WAN_2 keepalive-timeout=30 name=MyLan password=\
    075389443 user=111317
/interface sstp-server
add name=Anton_Mikrotik user=AntoN
add name=Denis_Mikrotik user="Deni$"
add name=Grohe_service user=Grohe
add name=Lemma_Kh user=Lemma_Hr
add name=Lemma_ZT user=LemmaZT_sstp
add name=Natasha user=N@ta
add name=Sergey_Mikrotik user=Sergey_sstp
/interface list
add name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-128-cbc,3des
/ip pool
add name=dhcp_pool1 ranges=192.168.1.2-192.168.1.250
add name=WIFI ranges=192.168.50.10-192.168.50.50
add name=SSTP_pool ranges=10.1.1.10-10.1.1.20
/ip dhcp-server
add address-pool=dhcp_pool1 disabled=no interface=bridge lease-time=4h name=\
    dhcp1
add address-pool=WIFI disabled=no interface=bridge_Guest lease-time=1h name=\
    Wi-Fi_guest
/ppp profile
add name=VPN only-one=yes use-compression=no use-encryption=no use-mppls=no
add local-address=10.1.1.1 name=SSTP only-one=yes remote-address=SSTP_pool \

```

					KIK.KP.Б-125-06-ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

```

use-compression=no use-encryption=yes use-mpls=no
set *FFFFFFFE change-tcp-mss=default
/queue type
add kind=pcq name="Free Wi-Fi download" pcq-classifier=dst-address pcq-rate=50M
add kind=pcq name="Free wi-fi upload" pcq-burst-time=5s pcq-classifier=\
src-address pcq-rate=50M
/queue simple
add max-limit=100M/100M name="limit Free Wi-Fi" queue=\
"Free wi-fi upload/Free Wi-Fi download" target=bridge_Guest
/system logging action
add email-start-tls=yes email-to=keikokmm@gmail.com name=action1 target=email
/interface bridge port
add bridge=bridge interface=ether3 trusted=yes
add bridge=bridge interface=ether4 trusted=yes
add bridge=bridge interface=ether5 trusted=yes
add bridge=bridge interface=ether6
add bridge=bridge interface=ether7
add bridge=bridge interface=ether8
add bridge=bridge_Guest interface=ether10 trusted=yes
/interface bridge settings
set use-ip-firewall=yes
/ip neighbor discovery-settings
set discover-interface-list=none
/ip settings
set tcp-syncookies=yes
/interface l2tp-server server
set authentication=mschap2 default-profile=VPN enabled=yes ipsec-secret=\
***** use-ipsec=yes
/interface list member
add interface=WAN_1 list=WAN
add interface=MyLan list=WAN
add interface=WAN_2 list=WAN
add interface=bridge list=LAN
add interface=bridge_Guest list=LAN
add interface=Anton_Mikrotik list=LAN
add interface=Denis_Mikrotik list=LAN
add interface=Lemma_ZT list=LAN
add interface=Sergey_Mikrotik list=LAN
/interface pptp-server server
set authentication=mschap2 max-mru=1400 max-mtu=1400
/interface sstp-server server

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		

```

set authentication=mschap2 certificate=SRV_Partner default-profile=SSTP \
    enabled=yes force-aes=yes keepalive-timeout=30

/ip address
add address=192.168.1.1/24 interface=bridge network=192.168.1.0
add address=192.168.10.1/24 interface=ether9 network=192.168.10.0
add address=192.168.50.1/24 interface=bridge_Guest network=192.168.50.0
add address=193.107.73.185/24 interface=WAN_1 network=193.107.73.0

/ip arp
add address=192.168.1.97 interface=bridge mac-address=00:E0:4C:62:D7:2C
add address=192.168.1.4 interface=bridge mac-address=D4:5D:64:3E:A7:09

/ip cloud
set ddns-enabled=yes ddns-update-interval=1m

/ip dhcp-server lease
*****

/ip dhcp-server network
add address=192.168.1.0/24 gateway=192.168.1.1 netmask=24
add address=192.168.10.0/24 gateway=192.168.10.1
add address=192.168.50.0/24 gateway=192.168.50.1

/ip dns
set allow-remote-requests=yes servers=8.8.8.8,1.1.1.1

/ip firewall filter
add action=accept chain=input comment=\
    "Input Established and Related connections" connection-state=\
    established,related
add action=drop chain=input connection-state=invalid in-interface-list=WAN
add action=accept chain=input comment=SSTP dst-port=443 protocol=tcp
add action=accept chain=input comment=ICMP limit=50/5s,2:packet protocol=icmp
add action=drop chain=input comment="drop VPN brute forcers UDP" \
    src-address-list=VPN_blacklist
add action=accept chain=input comment=L2TP+IpSec dst-port=1701,4500 protocol=\
    udp
add action=accept chain=input dst-port=500 protocol=udp
add action=accept chain=input protocol=ipsec-esp
add action=accept chain=input protocol=ipsec-ah
add action=drop chain=input comment="drop winbox brute forcers" \
    src-address-list=winbox_blacklist
add action=add-src-to-address-list address-list=winbox_blacklist \
    address-list-timeout=none-static chain=input dst-port=50505 protocol=tcp \
    src-address-list=winbox_stage1
add action=add-src-to-address-list address-list=winbox_stage1 \
    address-list-timeout=1h chain=input dst-port=50505 protocol=tcp \

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

src-address-list="!Access List"
add action=accept chain=input dst-port=50505 protocol=tcp
add action=add-src-to-address-list address-list=HoneyPot address-list-timeout=\
5d1h chain=input comment=HoneyPot connection-state=new dst-port=\
21,22,23,8291 in-interface-list=WAN protocol=tcp src-address-list=\
"!Access List"
add action=drop chain=input comment=DNS_Flood connection-state=new dst-port=53 \
in-interface-list=WAN protocol=udp
add action=drop chain=input connection-state=new dst-port=53 in-interface-list=\
WAN protocol=tcp
add action=drop chain=input comment="Ports scanner" src-address-list=\
"Port Scanners"
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp psd=21,3s,3,1
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=udp psd=21,5s,3,1
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=!fin,!syn,!rst,!ack
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=fin,rst
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=fin,!ack
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=fin,urg
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input in-interface-list=WAN \
protocol=tcp tcp-flags=rst,urg
add action=add-src-to-address-list address-list="Port Scanners" \
address-list-timeout=none-static chain=input dst-port=0 in-interface-list=\

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

```

WAN protocol=tcp
add action=add-src-to-address-list address-list="Port Scanners" \
    address-list-timeout=none-static chain=input dst-port=0 in-interface-list=\
    WAN protocol=udp
add action=drop chain=input comment="DROP ALL" in-interface-list=WAN
add action=drop chain=output comment="check internet " dst-address=8.8.4.4 \
    out-interface=MyLan protocol=icmp
add action=drop chain=output dst-address=8.8.4.4 out-interface=WAN_2 protocol=\
    icmp
add action=accept chain=forward comment=\
    "Forward Established Related Untracked connections" connection-state=\
    established,related
add action=drop chain=forward connection-state=invalid
add action=reject chain=forward comment=BLOCK_Site dst-address-list=mail.ru \
    log=yes protocol=tcp reject-with=tcp-reset
add action=reject chain=forward dst-address-list=Yandex protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward dst-address-list=zen.yandex.ru protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward dst-address-list=yandex.ua protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward dst-address-list=ya.ru protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward dst-address-list=vk.com protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward dst-address-list=ok.ru protocol=tcp \
    reject-with=tcp-reset
add action=reject chain=forward comment="Drop internet" out-interface-list=WAN \
    protocol=tcp reject-with=tcp-reset src-address-list=\
    "Users without internet"
add action=add-src-to-address-list address-list=IP_Cam_check_list \
    address-list-timeout=1d chain=forward comment=Ip_Camera_Check dst-address=\
    192.168.10.2 dst-port=80 protocol=tcp tcp-flags=syn
add action=add-src-to-address-list address-list=SRVPartner \
    address-list-timeout=1d chain=forward comment=SRVPartner_Check dst-address=\
    192.168.1.8 dst-port=3389 protocol=tcp tcp-flags=syn
add action=add-src-to-address-list address-list=SRVLemma address-list-timeout=\
    1d chain=forward comment=SRVLemma_Check dst-address=192.168.1.4 dst-port=\
    3389 protocol=tcp tcp-flags=syn
/ip firewall mangle
add action=mark-connection chain=prerouting comment=DKS connection-state=new \

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

disabled=yes new-connection-mark=DKS_in nth=2,1 passthrough=yes
add action=mark-connection chain=prerouting comment=MyLan connection-state=new \
disabled=yes new-connection-mark=MyLan_in nth=2,2 passthrough=yes
add action=mark-routing chain=prerouting comment=DKS connection-mark=DKS_in \
disabled=yes new-routing-mark=Out_DKS passthrough=yes
add action=mark-routing chain=prerouting comment=MyLan connection-mark=MyLan_in \
disabled=yes new-routing-mark=Out_MyLan passthrough=yes
/ip firewall nat
add action=masquerade chain=srcnat out-interface-list=WAN
add action=dst-nat chain=dstnat comment=SRVLemma disabled=yes dst-port=55355 \
in-interface=WAN_1 protocol=tcp to-addresses=192.168.1.4 to-ports=3389
add action=dst-nat chain=dstnat disabled=yes dst-port=55355 in-interface=MyLan \
protocol=tcp to-addresses=192.168.1.4 to-ports=3389
add action=dst-nat chain=dstnat comment=SRV1 disabled=yes dst-port=60505 \
in-interface=WAN_1 protocol=tcp to-addresses=192.168.1.19 to-ports=3389
add action=dst-nat chain=dstnat disabled=yes dst-port=60505 in-interface=MyLan \
protocol=tcp to-addresses=192.168.1.8 to-ports=3389
add action=dst-nat chain=dstnat comment="Video SRV" dst-port=53580 \
in-interface=WAN_1 protocol=tcp to-addresses=192.168.10.2 to-ports=80
add action=dst-nat chain=dstnat comment="SSH Asterisk" disabled=yes dst-port=22 \
in-interface=WAN_1 protocol=tcp to-addresses=192.168.1.97 to-ports=22
add action=dst-nat chain=dstnat comment=SRVLemma dst-port=55555 \
in-interface-list=WAN protocol=tcp src-address-list="Access List" \
to-addresses=192.168.1.111 to-ports=80
/ip firewall raw
add action=drop chain=prerouting in-interface-list=WAN src-address-list=\
HoneyPot
add action=drop chain=prerouting in-interface-list=WAN src-address-list=\
BAN_List
/ip firewall service-port
set sip disabled=yes ports=5060,5061,5062 sip-timeout=1m
/ip route
add check-gateway=ping comment=DKS distance=1 gateway=193.107.73.1
add check-gateway=ping comment=MyLan disabled=yes distance=2 gateway=MyLan
add comment="CHECK internet" distance=1 dst-address=8.8.4.4/32 gateway=\
193.107.73.1
add distance=1 dst-address=192.168.0.0/24 gateway=Lemma_ZT pref-src=192.168.1.1
add distance=1 dst-address=192.168.3.0/24 gateway=Sergey_Mikrotik pref-src=\
192.168.1.1
add distance=1 dst-address=192.168.4.0/24 gateway=Anton_Mikrotik pref-src=\
192.168.1.1

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

add distance=1 dst-address=192.168.5.0/24 gateway=Lemma_Kh pref-src=192.168.1.1
add distance=1 dst-address=192.168.6.0/24 gateway=Grohe_service pref-src=\
192.168.1.1
add disabled=yes distance=1 dst-address=192.168.15.0/24 gateway=*32 pref-src=\
192.168.1.1
add distance=1 dst-address=192.168.88.0/24 gateway=Denis_Mikrotik pref-src=\
192.168.1.1
/ip route rule
add action=unreachable comment="Network isolation_1" dst-address=192.168.1.0/24 \
src-address=192.168.50.0/24
add action=unreachable dst-address=192.168.50.0/24 src-address=192.168.1.0/24
add action=unreachable comment="Network isolation_2" dst-address=192.168.1.0/24 \
src-address=192.168.10.0/24
add action=unreachable dst-address=192.168.10.0/24 src-address=192.168.1.0/24
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
set api disabled=yes
set winbox address=0.0.0.0/0 port=50505
set api-ssl disabled=yes
/lcd
set backlight-timeout=2h default-screen=informative-slideshow
/ppp secret
add local-address=10.50.0.10 name=Uswer_4 password=887887kkkKMM_ profile=VPN \
remote-address=10.50.0.14 service=l2tp
add name=Grohe password=*****_ profile=SSTP service=sstp
add local-address=10.50.0.10 name=radist password=*****_ profile=VPN \
remote-address=10.50.0.12 service=l2tp
add local-address=10.50.0.10 name=Kobeluk password=***** profile=VPN \
remote-address=10.50.0.13 service=l2tp
add local-address=10.50.0.10 name=OlgaN password=***** profile=VPN \
remote-address=10.50.0.19 service=l2tp
add local-address=10.50.0.10 name=AntonMAC password=***** profile=VPN \
remote-address=10.50.0.20 service=l2tp
add name=LemmaZT_sstp password=*****_ profile=SSTP service=sstp
add name=Sergey_sstp password=*****_ profile=SSTP service=sstp
add name="Deni$" password=***** profile=SSTP service=sstp
add name=AntoN password=*****_ profile=SSTP service=sstp
add local-address=10.50.0.10 name=Sasha password=*****_ profile=VPN \

```

					KIK.KP.Б-125-06-ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

remote-address=10.50.0.17 service=l2tp
add local-address=10.50.0.10 name=Ira_B password=***** profile=VPN \
remote-address=10.50.0.11 service=l2tp
add name=N@ta password=***** profile=SSTP service=sstp
add name=Lemma_Hr password=***** profile=SSTP service=sstp
/routing ospf interface
add authentication=md5 authentication-key=***** _ disabled=yes \
network-type=broadcast
add authentication=md5 authentication-key=***** disabled=yes interface=\
bridge network-type=broadcast passive=yes
/routing ospf network
add area=backbone disabled=yes network=192.168.1.0/24
add area=backbone disabled=yes network=10.50.0.11/32
add area=backbone disabled=yes network=10.50.0.15/32
add area=backbone disabled=yes network=10.50.0.16/32
/snmp
set enabled=yes
/system clock
set time-zone-name=Europe/Kiev
/system identity
set name=PARTNER
/system logging
add topics=e-mail,!debug
add action=action1 topics=account
/system package update
set channel=long-term
/system routerboard settings
set auto-upgrade=yes
/tool bandwidth-server
set authenticate=no enabled=no
/tool e-mail
set address=smtp.gmail.com from=mikrotik.infopartner@gmail.com password=\
887887kkkKMM_ port=587 start-tls=yes user=mikrotik.infopartner
/tool netwatch
add comment=Up/Down down-script="/ip route disable [find comment=\"DKS\"] \r\
\n/ip route enable [find comment=\"MyLan\"] \r\
\n:foreach i in=[/ip firewall connection find dst-address~\":5060\" protocol\
~\"udp\"] do={ /ip firewall connection remove $i } \r\
\n\r\
\n/tool fetch url=\"https://api.telegram.org/bot1262049343:AAF0zZdXv80RxAG-c\
3R23zZSrFL2vhCUeGE/sendMessage\\?chat_id=923171824&text=Attention! Partner \

```

					KIK.KP.Б-125-06-ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

info! The backup channel is included MyLan! 213.108.41.110\" dst-path=telegr\
am.txt\r\
\n\r\
\n/tool fetch url=\"https://api.telegram.org/bot1383059672:AAHhA2UQCWEa4KoUe\
z1J9kjyn7pm10uTjFM/sendMessage\\?chat_id=608435819&text=Attention! Partner \
info! The backup channel is included MyLan! 213.108.41.110\" dst-path=telegr\
am_1.txt\r\
\n\r\
\n####Marsh#####\r\
\n:beep frequency=500 length=500ms;\r\
\n:delay 500ms;\r\
\n:beep frequency=500 length=500ms;\r\
\n:delay 500ms;\r\
\n:beep frequency=500 length=500ms;\r\
\n:delay 500ms;\r\
\n:beep frequency=400 length=500ms;\r\
\n:delay 400ms;\r\
\n:beep frequency=600 length=200ms;\r\
\n:delay 100ms;\r\
\n:beep frequency=500 length=500ms;\r\
\n:delay 500ms;\r\
\n:beep frequency=400 length=500ms;\r\
\n:delay 400ms;\r\
\n:beep frequency=600 length=200ms;\r\
\n:delay 100ms;\r\
\n:beep frequency=500 length=500ms;\r\
\n#####\r\
\n" host=8.8.4.4 interval=3m timeout=3s up-script="/ip route enable [find co\
mment=\"DKS\"] \r\
\n/ip route disable [find comment=\"MyLan\"] \r\
\n:foreach i in=[/ip firewall connection find dst-address~\":5060\" protocol\
~\"udp\"] do={ /ip firewall connection remove $i } \r\
\n/ip firewall connection {remove [find]} \r\
\n\r\
\n/tool fetch url=\"https://api.telegram.org/bot1262049343:AAF0zZdXv80RxAG-c\
3R23zZSrFL2vhCUeGE/sendMessage\\?chat_id=923171824&text=Attention! Partner \
info! The main channel is included Net-City! 193.107.73.185\" dst-path=teleg\
ram.txt\r\
\n\r\
\n/tool fetch url=\"https://api.telegram.org/bot1383059672:AAHhA2UQCWEa4K
z1J9kjyn7pm10uTjFM/sendMessage\\?chat_id=608435819&text=Attention! Partn

```

					KIK.KP.Б-125-06-ПЗ	Арк.
						59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

info! The main channel is included Net-City! 193.107.73.185\" dst-path=te
ram_1.txt\r\
\n\r\
\n\r\
\n##### Mario #####\r\
\n:beep frequency=660 length=100ms;\r\
\n:delay 150ms;\r\
\n:beep frequency=660 length=100ms;\r\
\n:delay 300ms;\r\
\n:beep frequency=660 length=100ms;\r\
\n:delay 300ms;\r\
\n:beep frequency=510 length=100ms;\r\
\n:delay 100ms;\r\
\n:beep frequency=660 length=100ms;\r\
\n:delay 300ms;\r\
\n:beep frequency=770 length=100ms;\r\
\n:delay 550ms;\r\
\n:beep frequency=380 length=100ms;\r\
\n:delay 575ms;\r\
\n#####\r\
\n"
[radist@PARTNER] >

```

					КІК.КР.Б-125-06-ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		