МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Інформаційно-комунікаційна технологія забезпечення безпеки мережі з використанням апаратних міжмережевих екранів Cisco ASA.»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Великодний Д.В.**

Студента групи ІК.м-01 — **Воробйов І.О.**

СУМИ 2021

Сумський державний університет
(назва вузу)

Факультет *ЕлІТ* Кафедра *Комп'ютерних наук*

Спеціальність *«122 - Комп'ютерні науки»*

Затверджую:
зав.кафедрою _____
_____
"_____" _____ 20___р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Воробйов Іван Олександрович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Інформаційно-комунікаційна технологія забезпечення безпеки мережі з використанням апаратних міжмережевих екранів Cisco ASA*

затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проекту (роботи)_____

3. Вхідні данні до проекту (роботи) _____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Огляд технологій, що застосовуються для забезпечення безпеки мережі; 2) Постановка завдання й формування завдань дослідження; 3) Огляд технологій, що використовуються під час розробки WEB-додатків; 4) Моделювання системи побудови мережі; 5) Розробка додатку; 6) Аналіз результатів.*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) *2- Актуальність, 3-Основні завдання, 4-Безпека та атака, 5-Їх види, 6-Cisco ASA, 7-Макет в Cisco, 8-Графічний інтерфейс додатку, 9-Працездатність програми, 10-Отримані дані програми, 11-Висновки*

6. Консультанти до проекта (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
1.	Огляд технологій, що застосовуються для забезпечення безпеки мережі		
2.	Постановка задачі та формування завдань дослідження.		
3.	Опис додатку		
4.	Розробка додатку з використанням Java Script		
5.	Оформлення пояснювальної записки до кваліфікаційної магістерської роботи		

Студент – дипломник _____
(підпис)

Керівник проекту _____
(підпис)

РЕФЕРАТ

Записка: 70 стор., 13 рис., 4 додатока, 16 літературних джерел.

Об’єкт дослідження — Інформаційно-комунікаційна технологія забезпечення безпеки мережі з використанням апаратних міжмережевих екранів Cisco ASA.

Мета роботи — Розробити WEB додаток на HTML, CSS, JavaScript для побудови та налаштування мережі.

Результати — проведений аналіз літератури, методів та інструментів, які дозволяють створити додаток для побудови та налаштування мережі, розглянені механізми захисту. Після ознайомлення з сучасними рішення був розробленний Web-додаток, який є гнучким, тобто дозволяє користуватись на будь-якому гаджеті який спроможний працювати з браузерами. Додаток був реалізований на HTML, CSS, JavaScript.

МЕРЕЖЕВА БЕЗПЕКА, QOS, HTML, CSS, МІЖМЕРЕЖЕВИЙ ЕКРАН, CISCO ASA, WEB-ОРІЄНТОВАНА СИСТЕМА, JAVA SCRIPT.

ЗМІСТ

ВСТУП

На сьогодні ми є глядачами становлення діджиталізації. Технології вже з’явились навіть на кухні, в звичайних побутових пристроях, це не кажучи про промислову галузь та фінансову.

Через таку популярність постає питання створення та організацію мереж таким чином, щоб по-перше, гарантувати безпеку для інформації, яка передається мережею, а подруге, забезпечити пропускну способність для всіх юзерів. Це тільки вершина айсберга, бо завдань куди більше, і вони різняться від сфері, в якій будуть застосовуватись.

Але найбільш гаряче дані завдання ставляться коли будується корпоративна мережа, де з’являється запотрібне з’єднати різні офіси одної компанії. Легко зрозуміти, що в наших умовах будувати власну мережу для цих цілей не є раціональною ідеєю, ні з точки часу на побудову, ні з боку фінансів. Це все легше зробити пустивши корпоративний графік через мережу Інтернет. Але тут постає найважче питання, потрібно захистити трафік від перехвату та від несанкціонованого доступу від неавторизованих користувачів. Та при цьому повинна бути полоса стабільної здатності пропускання для highpriority трафіку, а також полоса телефонування, близько з трафіком, який генерує в корпоративна мережа.

На ринку в даний час широко представлене асорті мережевих пристроїв, які здатні успішно виконувати поставленні вище завдання. Одним із лідерів беспринципно являється компанія Cisco, з її пристроями, зокрема лінійка міжмережевих екранів Cisco ASA. Не схожі пристрої ASA з іншим обладнанням Cisco тим, що має специфічний набір команд для конфігурації, що у свій час, потребує додаткового часу на ознайомлення для мережевих адміністраторів. Але це завдання міг би полегшити орієнтований графічний інтерфейс, розроблений як Web сторінка, який тільки запитував у юзера тільки задати вхідні адреси на інтерфейсах та мріяні сервіси.

1. QOS ТА БЕЗПЕКА КОРПОРАТИВНОГО ТРАФІКУ У МЕРЕЖІ

1.1 Поняття безпеки мережі

Давайте коротко розглянемо концепції, інструменти та завдання, якими користуються щоб запобігти доступу несанкціонованих юзерів або додатків до офісної мережі та вмикнених приладів.

Безпека мережі – це важкий процес з програмним використання та використанням апаратних приладів для забезпечення захисту інфраструктури мережі від несанкціонованого доступу, неправильного використання, несправності, знищення або неналежного розкриття інформації для створення безпечного середовища для користувачів, їх пристроїв та програм. Безпеку мережі доповнює кінцеву безпеку, або іншими словами безпеку для кінцевих приладів. Якщо остання робить увагу на створені захисту інформації на пристроях, то мережева безпека - процесі спілкування користувача на кінцевих пристроях в мережі та засобах забезпечення зв'язку між ними.

Говорячи за мережеву безпеку, має сенс насамперед зосередитися на основних типах атак, які можуть викликати уповільнення роботи мережі, неконтрольований трафік, віруси тощо.

Мережеві атаки можемо ділити на дві групи: пасивні і активні.

Пасивні не впливають безпосередньо на працездатність мережі. Ці атаки не виявляються і призначені для збирання інформації. Ці атаки слідів не роблять і зазвичай являються незапоміченими.

У світі немає суто активних, або тільки пасивних. Як завжди, активному вторгненню в працездатність мережі (активній атаці).

До атак, які активно впливають на мережу відносять:

Modification атака, при якій зловмисний хост змінює маршрут маршрутизації, так що відправник повинен надсилати повідомлення маршрутом, який являється довгим, викликаючи затримку зв'язку через відправник-одержувач.

Wormhole - тип атаки, де злочинець перехоплює в першій точці міжмережеві пакети, tunnel-ює на шкідливий хост в другій точці та повторно відправляє їх.

Denial of services - зловмисний хост відправляє масивні повідомлення атакованого хосту, споживаючи при цьому пропускну спроможність. Основне завдання для атаки – перевантажити вузол мережі, і в цьому випадку реальні юзери мережі не зможуть отримати доступ до ресурсів такого вузла або цей ресурс перевантажено.

Spoofing - заміна змісту пакетів – атака на мережу, при якій зловмисний хост підробляє свою справжню особистість і, таким чином, видає себе за авторизований пристрій або хост із необхідними правами. Захист від атак із підробкою забезпечують міжмережні екрани, які можуть виконувати глибокий аналіз пакетів. У цьому випадку злочиик підмінює значення поля адреси відправниці у пакетах, що ускладнює можливість детекту джерел атак. У той же час, використовуючи інформацію про інші вузли мережі як адресу, зловмисник замінює власників цих комп'ютерів, роблячи їх учасниками атаки.

Sinkhole - це атака, спрямована на запобігання одержанню базовою станцією повної та правильної службової інформації. Коли базова станція запитує службову інформацію, зловмисний вузол спотворює її, змінюючи чи частково видаляючи її.

Sybil – атака виконується шляхом використання декількох шкідливих вузлів. Шкідливий хост розшарює свій секретний ключ іншим шкідливим хостам. Таким чином, кількість шкідливих вузлів у мережі збільшується, а також збільшується ймовірність атаки. Такі атаки можуть здійснюватись через однорангові мережі (наприклад, Tor [4].

Серед пасивних атак:

Traffic analysis - атака, спрямована на захоплення та пакетний аналіз, в якій проходить обмін відправника і одержувача в канальному мережевому рівні OSI. Цей тип атаки дозволяє зрозуміти логіку праці мережі, так як дає змогу отримати таблицю між мережевими подіями і командами, що надсилають мережеві об'єкти один до одного у разі виникнення цих подій.

Sniffing or snooping attack – захоплення незахешованого трафіку. При допомозі спеціального програмного забезпечення - сніфера - зловмисники можуть отримати доступ к вмісту мережних пакетів і перехопити інформацію, що пересилається.

Monitoring - спостерігай за продуктивністю мереж, непомітно збираючи артефакти протоколу, включаючи вміст програми або метадані протоколу, включаючи заголовки [4].

Сетевая безопасность подразумевает организацию защиты как на уровне интерфейса между локальной сетью и транспортной сетью, так и непосредственно внутри самой локальной сети. Каждый уровень сетевой безопасности применяет свою собственную политику и средства управления. В результате авторизованные пользователи всегда имеют доступ к сетевым ресурсам, а злоумышленники - минимизируют возможность вторжения и распространения угроз.

Давайте посмотрим на наиболее распространенные инструменты сетевой безопасности.

1. Контроль доступу - деяким користувачам потрібен доступ до ресурсів мережі. Щоб захистити її від можливих зловмисників, вам потрібен чіткий список авторизованих юзерів мережі та приладів. За допомогою цієї інформації мережевий адмін має змогу налаштовувати політику безпеки так, щоб у разі недотримання дозволеного списку активність приладів в мережі блокувалася, чи доступ до ресурсів мережі обмежувався.

2. Антивірусне програмне забезпечення - шкідливе програмне забезпечення, що містить віруси, черв'яки, трояни і шпигунське програмне забезпечення. Кращі антивірусні програми не тільки сканують пристрій користувача на наявність шкідливих програм, але й постійно контролюють системні файли та процеси, щоб своєчасно виявляти аномалії в їх роботі та, якщо такі є, спроможні видалити злочинне програмне забезпечення.

3. Захист додатків - деякі програми, які використовуються в компанії, повинно бути стійким від загрозних факторів, незалежно від того, створено воно власним IT-відділом або придбано у зовнішніх постачальників

програмного забезпечення. Жодне програмне забезпечення не застраховане помилками розробника і може містити чорні входи і подібні вразливості, які можуть використовувати зловмисники для проникнення в корпоративну мережу.

4. Поведінкова аналітика - при зборі мережевої статистики ви можете використовувати інструменти аналітики, які автоматично порівнюють поточну та еталонну поведінку мережі та розпізнають метрики, що розходяться.

5. Запобігання утрати інформації - компанія повинна гарантувати, що співробітник не надсилає конфіденційну інформацію за межі мережі.

6. Захист електронної пошти - вектор загрози номер 1. Злочинці використовують ідентифікуючу особу і тактику соц-інженіренгу для створення і розсилки складних фішингових кампаній, щоб ввести отримувачів електронної пошти в обман і направити їх в сайти зі шкідливим П. З. Захист пошти дозволяє блокувати вхідну атаку та контролювати вихідне повідомлення, щоб уникнути втрат інформації.

7. Брандмауери - основна функція це бар'єр між внутрішнєю мережею та хрупкими мережами зовні, як Інтернет. Вони користуються набором правил для фільтрування трафіку який входить.

8. Система запобігання втручанню - сканують трафік мережі для блокування атак у режимі реального часу. Це виконується пристроєм IPS наступного покоління (IPS), яке не тільки блокує шкідливу активність, але також відстежує поширення файлів, які можуть бути під підозрою та програм, які шкодять мережі для запобігання спалахам зараженню мережних пристроїв та повторному зараженню.

9. Сегментація мережі - розбиває внутрішній трафік мережі на основі правил, що робить легше використання безпечної політики. Мережевий адміністратор може надати правила доступу залежачи від ролі, місцезнаходження, відділу т. д.

10. VPN - мережа шифрує з'єднання від кінцеві точки до мережі, часто через Internet.

11. Веб-безпека рішення мережевої безпеки забезпечує контроль роботи колег в Internet, блокування загроз та доступ до шкідливих веб-ресурсів [10].

Зазначені інструменти реалізуються комплексом програмно-апаратних засобів як у локальній мережі.

1.2 Управління та користування QOS

Якість обслуговування – це спроможність мережі надавати найкращий сервіс вибраному мережевому трафіку. Основна мета QoS – забезпечити пріоритет, вмикаючи смугу пропускання, контрольоване тремтіння та затримку, а також покращені хар-ки витрат. Важливо, щоб приоритизація деякого або деяких потоків не призводила до краху або втрати деяких потоків.

QoS дає змогу краще використовувати потік. Досягається чи підвищенням пріоритету, або обмеженням пріоритетності іншого. Коли використовується захід контролю навантаження підвищення пріоритету потоку, поставити в чергу та обслужити їх у різний спосіб. Керування чергою використовується для запобігання перевантаженню шляхом переміщення потоків з нижчим пріоритетом на кінець черги перед потоками з більш високим пріоритетом. Полірування та формування забезпечують пріоритет потоку за рахунок обмеження смуги пропускання потоків.

QoS складається з 3 головних компонентів:

- методи ідентифікації та маркування трафіку для наскрізної координації QoS між мережевими пристроями;
- QoS на рівні окремого мережевого пристрою (керування чергами, планування, формування трафіку);
- управління політиками QoS, облік та адміністрування трафіку в окремому сегменті мережі.

Щоб надати пільгову послугу, потрібно спочатку визначити тип трафіку, а потім вибрати його відповідно до певних критеріїв. Ці завдання являють собою класифікацією трафіка.

Ідентифікація трафіку можлива шляхом аналізації пакетів, надісланих мережним вузлом. Знаючи ці дані, мережеві вузли може присвоїти тому чи другому пакету токен.

Поля заголовків деяких протоколів мережі містять спеціальні поля маркування трафіка. Маркування трафіку полегшує його подальшу обробку у чергах.

Сьогодні в IP-мережах існує 2 типи стандартів: старі та нові. У старого було поле ToS (8-бітне), з якого, у свою чергу, було виділено 3 біти, які називають пріоритетом IP. Це поле було скопійоване у полі заголовку Ethernet [15].

Пізніше було визначено новий стандарт. Поле ToS було перейменовано на DiffServ, і додатково 6 біт було виділено для поля точки диференціального коду послуги (DSCP), куди можуть бути надіслані параметри, необхідні цього типу трафіку.

Найкраще позначити свої дані ближче до джерела даних. Тому більшість IP-телефонів самі додають поле DSCP = EF або CS5 в IP-заголовок голосових пакетів. Багато програм також маркують трафік самостійно, сподіваючись, що їхні пакети матимуть пріоритет.

Хоча ми не використовуємо будь-якої технології пріоритезації, це не значить, що черг немає жодних. Черга як і раніше з'являтиметься і буде стандартним механізмом First In First Out. Отака черга, звичайно, дозволяє якийсь час не руйнувати пакети перманентно, зберігаючи їх перед відправкою до буфера, але не надасть жодної переваги, наприклад, голосовому трафіку.

Якщо необхідно надати абсолютний пріоритет певному виділеному класу (тобто пакети цього класу завжди будуть опрацьовуватися першими), ця технологія називається організацією черги з пріоритетом. Всі пакети у фізичному вихідному буфері інтерфейсу будуть розділені на 2 логічні черги, і пакети з привілейованої черги будуть надсилатися доти, доки вона не закінчиться. Тільки тоді почнуть передаватись пакети з другої черги.

Ця технологія проста, досить примітивна та застаріла, оскільки обробка непріоритетного трафіку постійно припинятиметься. На маршрутизаторах Cisco можна створити чотири черги з різними пріоритетами. Слід сувора ієрархія: пакети з менш привілейованих черг не обслуговуватимуться, поки всі черги з вищим пріоритетом не стануть порожніми.

Fair Queuing - технологія, що дає змогу надати рівні права усім класам трафіку. Як правило, використовують його незавжи, тому що він мало що дає для покращення якості обслуговування.

Weighted Fair Queuing - технологія, яка надає різні класи трафіку з різними правами, але одночасно обслуговує всі черги. Це виглядає так: усі пакети поділяються на логічні черги, використовуючи поле IP Precedence як критерій членства у черзі. Це ж поле також визначає пріоритет (що більше, тим краще). Крім того, маршрутизатор обчислює пакет, з якого черга швидше пересилає та пересилає його точно.

Розраховується він за формулою:

$$dT=(t(i)-t(0))/(1+IPP), \quad (1.1)$$

де IPP – значення поля IP Precedence;
t(i) – час, необхідний на реальну передачу пакету інтерфейсом. Розраховується як t(i) = L/S, де L – довжина пакету, а S – швидкість передачі інтерфейсу

Рисунок 1.1 – WFQ Технологія [9]

Основним недоліком WFQ є використання попередньо помічених пакетів, які не дає змогу власноруч визначати класи трафіку та виділяти смугу.

Ще одна розробка WFQ – це виважена справедлива організація черг на основі класів Class-Based Weighted Fair Queuing. В данній черзі адміністратор сам визначає класи трафіку відповідно до різних критеріїв, накштал, використовуючи списки Acess List як default. Крім того, для них визначається вага, і пакети в їхніх чергах обслуговують пропорційно до ваги.

Однак, дана черга необов'язково пересилає найважливіші пакети (зазвичай голосові або пакети з інших інтерактивних програм). В результаті

вийшло поєднання виваженої справедливої організації черг на основі пріоритетів та класів - PQ-CBWFQ, також відомої як організація черг з низькою затримкою (LLQ). За допомогою цієї технології можна вказати до чотирьох черг пріоритету, а інші класи обслуговуються механізмом CBWFQ.

Сьогодні LLQ є найбільш зручним, гнучким і широко використовується механізмом організації черг. Однак для цього потрібно налаштування класів, налаштування політик і застосування політик в інтерфейсі користувача [15].

Існує дві технології надання трафіку QoS: формування та полірування (рис. 1.2). Формування трафіку зберігає додаткові пакети у черзі, а потім міркує дальніш на передачу цих данних через рівні проміжки часу. Результат цього процесу формування трафіку є стабільніша швидкість відправлення пакетів. Для формування трафіку потрібно достатньо черги та пам'яті для буферизації затриманих пакетів, на відміну від полірування трафіка.

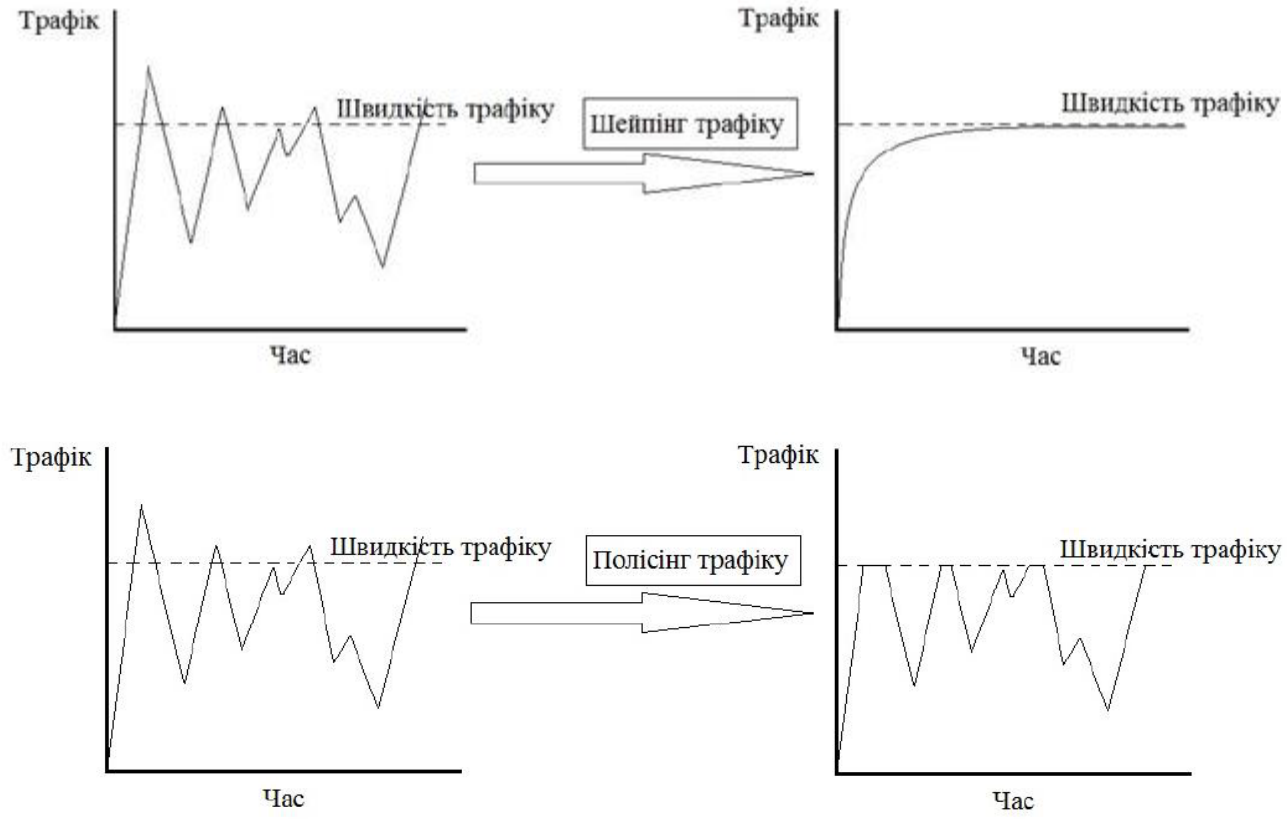

Рисунок 1.2 – шейпінгу і полісінгу, різниця технологій

Де час трафіку досягне вказаного максимума, надлишковий трафік відкидується або позначається знов-таки. Отримуємо швидкість віддачі має пилкоподібний графік з піками та спадами [2].

Черга займається управлінням трафіком, що входить. Вхідні пакети через інтерфейс ставляться у чергу і можуть бути затінені. До вихідного трафіку на інтерфейсі може застосовуватися лише застосування політик.

Існує три основні моделі надання послуг QoS у мережі:

- негарантована доставка, доставка максимальними зусиллями (Best Effort, BE);
- інтегрований сервіс (Integrated Services, IntServ);
- Диференційовані послуги (DiffServ)[1].

Ці три моделі розрізняються механізмами надання дозволів додаткам на відправлення даних та тим, як розподільна мережа обробляє ці дані на заданому рівні обслуговування.

Найкраща модель QoS (BE) - найпростіша із трьох. Це модель QoS, яка використовується за замовчуванням в Інтернеті і взагалі не реалізує будь-якого механізму QoS.

У BE непередбачено резервування ресурсів або будь-який інший механізм, пов'язаний із запитом спеціального доступу до мережі. З цієї логіки модель BE погано працює з програмами, що генерують трафік у реальному часі (RT).

Цю модель годі було використовувати, якщо мережевих ресурсів замало задоволення вимог QoS, що з такими ключовими показниками, як пропускну здатність, затримка, джиттер тощо.

Модель Integrated Services також відома як жорстка QoS-модель. Це модель, заснована на потоках, тобто вихідних і цільових IP-адреси і портах.

При реалізації моделі IntServ програми, очевидно, надсилають запити інформації в мережу, щоб зарезервувати смугу пропускання свого власного потоку. Мережеві пристрої відстежують усі потоки, що проходять через вузли, перевіряючи, чи належать нові пакети існуючому потоку і чи достатньо мережних ресурсів прийому пакета.

Збереження мережних ресурсів для кожного потоку гарантує додаткам ресурси та очікувану мережну поведінку.

Модель IntServ реалізує детермінований доступ контролю (AC) на основі запитів ресурсів та вільно-доступних ресурсів.

Для реалізації цієї моделі потрібні маршрутизатори з підтримкою intServ в мережі та використання RSVP для наскрізного резервування ресурсів:

- перед відправкою даних програми запитують певний рівень обслуговування мережі;
- мережа дозволяє або забороняє резервування (кожного потоку) залежно від доступних ресурсів;
- після очищення мережа очікує, що програма залишиться в профілі трафіку.

Масштабованість цієї моделі обмежена тим фактом, що існує високе споживання ресурсів на мережевих вузлах, викликане обробкою потоків та їх пов'язаних станів: мережні вузли повинні підтримувати надлишковий стан кожного потоку, що проходить через вузол.

Модель диференційованого обслуговування (Diffserv) також відома як м'яка модель QoS. Це модель, що базується на класах сервісів.

У цьому випадку немає потреби у явному запиті резервування ресурсів додатками в мережі. Диференційоване обслуговування базується на статистичних перевагах кожного класу трафіку.

DiffServ дає змогу пристроям на кінцевих точках або хосту зробити класифікацію пакета за різними категоріями обробки чи класами трафіка (TC), з яких кожен отримуватиме різні послуги (Per-Hop-Behavior). Кожен мережний пристрій на своєму шляху обробляє пакети відповідно до локально визначених PHB.

PHB визначає, як вузол повинен працювати із TC. Політики послуг мережі можуть бути специфічними для всього домену QoS, певної частини мережі або навіть одного вузла.

Пріоритети, зазначені у кожному пакеті, обробляються за допомогою DSCP для класифікації трафіку. Це маркування проводиться для кожного пакета, зазвичай, на межі домену QoS.

Переваги DiffServ:

- легко масштабований механізм QoS;
- на кінцевих хостах не потрібно механізм резервування ресурсів;
- простота налаштування, експлуатації та обслуговування;

- підтримка комплексної класифікації трафіку та кондиціювання повітря на краю;
- може об'єднувати кілька потоків додатків обмежену кількість класів трафіку;
- зменшити накладні витрати, пов'язані із підтримкою політики на основі потоків;
- Вузли Diffserv можуть обробляти трафік легше, ніж пристрої Intserv;
- Diffserv – це розподілена модель обслуговування QoS. Розподіл ресурсів розподіляється між усіма маршрутизаторами в домені Diffserv, що забезпечує більшу гнучкість та ефективність у процесі маршрутизації.

Тому модель диверсифікованого обслуговування є найбільш оптимальним рішенням з метою забезпечення необхідних показників якості обслуговування трафіку при найбільш ефективному використанні мережевих ресурсів.

1.3Постановка задачі роботи

В цей час більшість компаній мають розгілля мереж офісів, філіалів, споруд, які повинні мати можливість між собою комунікувати. Найбільш розповсюдженим та стандартним варіантом для виконання завдання з сполучення офісів є використання інтернету.

Але, в наших реаліях інтернет - це вже мультисервісна мережа, та може використовуватись працівниками не тільки для виконання поставлених задач, але і з метою відпочинку, т. д. Важливо запам’ятати, коли проходить обмін інформацією через інтернет, будь-хто має перспективу долучитись до перехоплення, прослуховування, копіювання. Саме через це, стає гостра необхідність захистити конфіденційну інформацію, що проходить через інтернет, від несанкціонованого доступу, а також зробити обмеження для працівників, що користуються службовою мережею не за завданнями.

З поставленими задачами гарно порається міжмережевий фаєрвол, серед яких функціональністю є здатність до шифрування трафіка, розгалуження доступу в інтернет ресурс, які небажані, або просто до роботи окремих

протоколів, покриття пріоритезації трафіку. Зробивши аналіз над літературою, можно зробити висновок, що сьогодні рішення, яке дає Cisco, а саме Cisco ASA - одне з найбільш популярних рішень міжмережевих екранів, що здатне до захисту корпоративної мережі, на кордоні сполучення з глобальною мережею. А широкий набір можливостей дає змогу гнучко налаштувати опції під мережу усіх окремих клієнтів.

Отже, постановка задачі формулюється наступним чином:

1. Створити конфігурацію мережі між головним головним офісом, та його філіалом на базі обладнання Cisco ASA.

2. Створити web-орієнтовану систему, в якій за допомогою графічного інтерфейсу юзер отримує можливість налаштувати параметри безпеки, та автоматично згенерувати конфігурацію пристроїв, з можливістю імпортувати на реальне обладнання. Створене ПЗ повинно дозволяти користувачам далеким від набору команд для налаштування, з легкістю конфігурувати обладнання Cisco. В якості графічного рішення буде web-сторінка, яка має змогу юзеру обирати та вводити необхідні параметри та в результаті отримувати готові конфігурації ASA.

3. Перевірити коректність роботи конфігурацій в симуляторі та на живому обладненні Cisco ASA.

2. ЗАБЕЗПЕЧЕННЯ QOS І БЕЗПЕКИ МЕРЕЖІ ТРАФІКУ ТА ОГЛЯД СУЧАСНИХ РІШЕНЬ

2.1 Рішення Cisco та порівнення їх можливостей QoS та мережевої безпеки

Під час проектування будь-якої комп'ютерної мережі, чи то мережа великої компанії з філіями по всій країні, чи мережа невеликого локального підприємства, виникає питання щодо забезпечення безпеки такої мережі по периметру. Мережевий адміністратор повинен вирішити, який клас обладнання найбільше підходить: міжмережевий екран - Adaptive Security Appliance (малюнок 2.1) або просто обмежити маршрутизатор (малюнок 2.2).

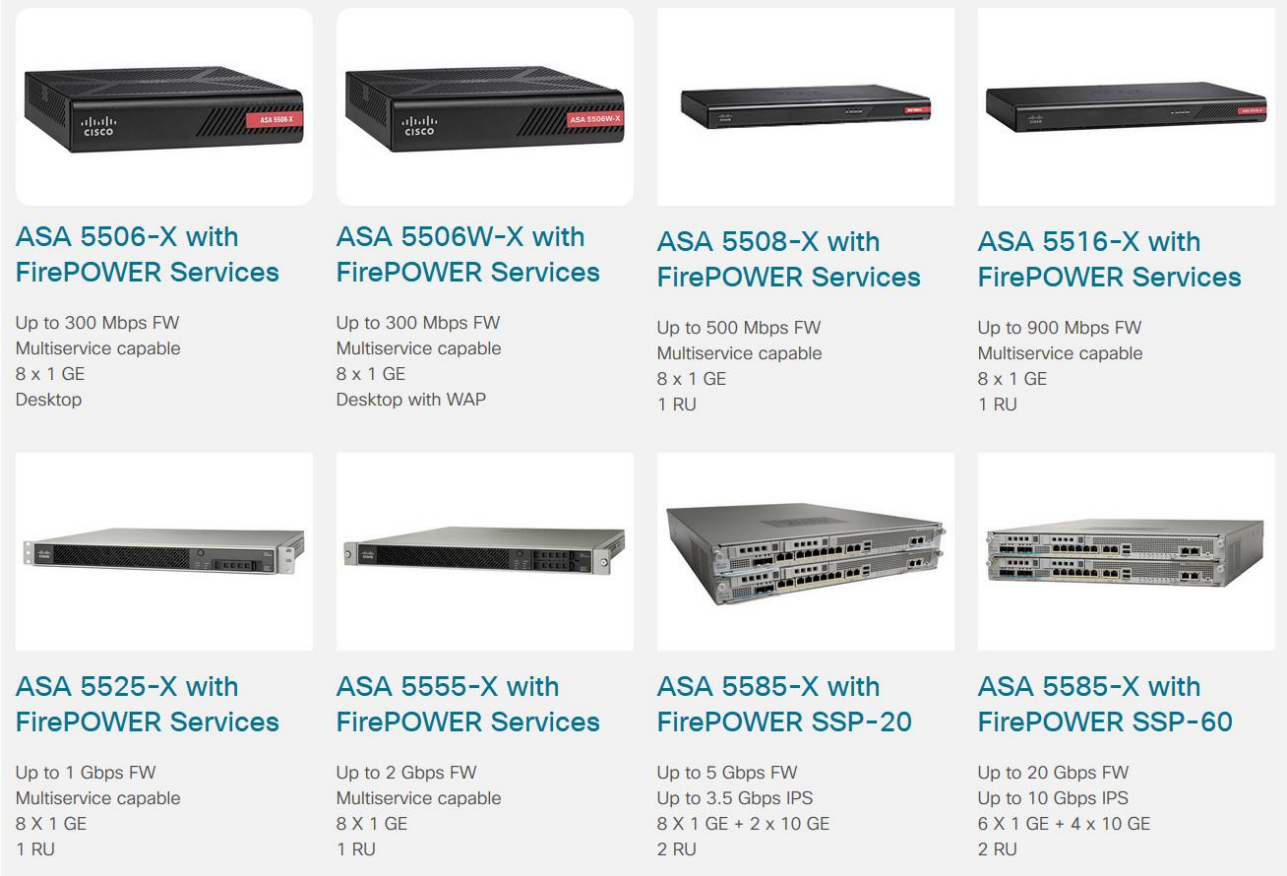

Рисунок 2.1 – Лінійка Cisco ASA 5500

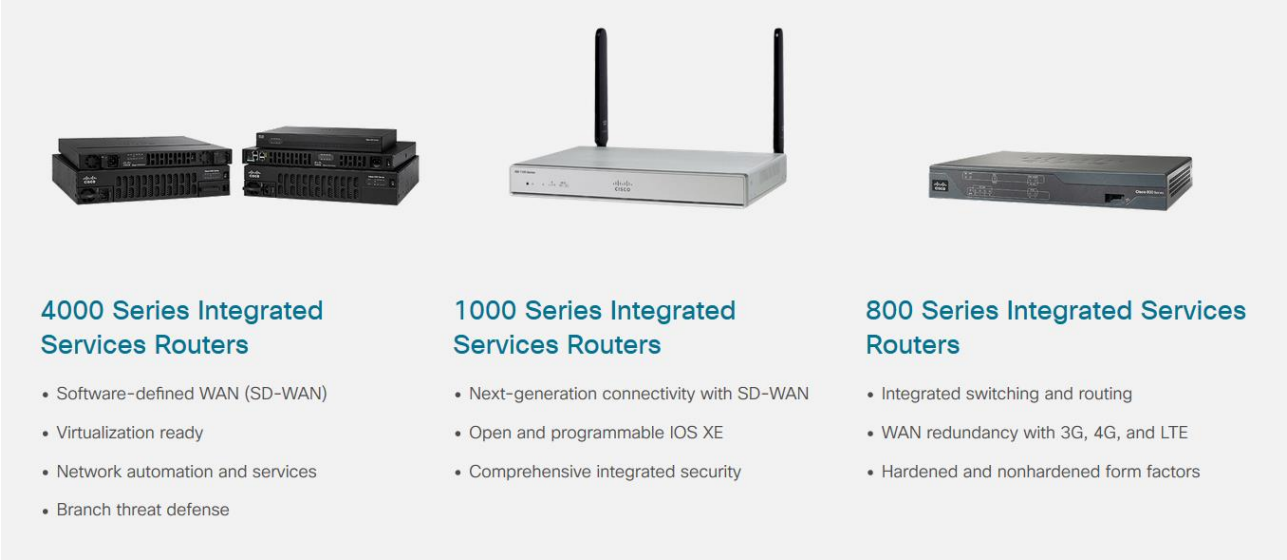

Рисунок 2.2 – Представлений модельний ряд роутерів Cisco ISR

Однозначно відповісти досить важко. Однак спробуємо порівняти ці два класи пристроїв.

Компанія Cisco позиціонує Cisco ASA як обладнання для організації мережевої безпеки і зазвичай, говорячи про Cisco ASA, мають на увазі її міжмережевий екран, а ISR-роутери - обладнання, що здійснює маршрутизацію трафіку. Однак Cisco ASA також вміє маршрутизувати мережевий трафік, навіть підтримує протоколи динамічної маршрутизації, у свою чергу ISR-роутери можуть успішно виконувати функції міжмережевих екранів (на базі технологій ZFW і CBAC).

Виходячи зі свого історичного позиціонування, Cisco ASA сьогодні має переваги перед маршрутизаторами ISR лише у підтримці технологій, що відповідають за організацію мережевої безпеки, зокрема це класичний міжмережевий екран і VPN-хаб для підключення віддалених користувачів. На жаль, друга функція Cisco ASA не так поширена, як у маршрутизаторах ISR, які позиціонуються як армійський службовий ніж, на основі якого можна поліпшити VoIP-телефонію, шифрування та оптимізацію трафіку. Тому вибір оптимального офісного пристрою обмежується лише питанням організації безпеки мережі.

На перший погляд, для такого завдання обидва класи пристроїв мають все необхідне:

підтримка маршрутизації - трансляція статичних та динамічних адрес та NAT;

ви можете підключитись від двох і більше провайдерів одночасно;

Існують функції міжмережевого екрана.

Розберемося з кожним класом пристроїв порізнь.

ASA позиціонує себе як рішення, яке є досить вузькоспеціалізоване, тому більшість функцій по безпеці та її організації вже ідуть із коробки. Просто увімкніть пристрій. Порівнючи з ISR-роутерами, де кожна функція безпеки повинна вмикатися примусово.

Зупинимося на тому, що ASA добре вміє, а яка функціональність суттєво обмежена чи взагалі відсутня.

1. У всіх варіантах, які можливі NAT: статичний, подвійний, динамічний. Ви можете настроїти порядок правил для користування NAT. З погляду гнучкості керування NAT. ASA перевершує маршрутизатори ISR.

2. Міжмережевий екран з глибоким аналізом вмісту протоколу з підтримкою сканування та виявлення DoS-атак. Як брандмауер ASA може працювати у двох режимах: маршрутизації відповідно до налаштованих політик та прозорого (Transparent Firewall). ASA також може працювати в багатоконтекстному режимі (віртуальні міжмережеві екрани, multiple context) або в режимі єдиного контексту. У мульти-контекстному режимі та/або прозорому режимі на доступну функціональність накладаються обмеження залежно від версії операційної системи. Наприклад, VPN з віддаленим доступом не може працювати в мультиконтекстному режимі. Як згадувалося раніше, основна відмінність від маршрутизаторів полягає в тому, що брандмауер включений за замовчуванням, він більш гнучкий і функціональніший, особливо функція брандмауера ідентифікації, яка дозволяє надавати доступ до мережевих ресурсів на основі імен користувачів або налаштованих груп Microsoft Active Directory. Маршрутизатори Cisco поточного покоління також підтримують прозорі та маршрутизовані міжмережові екрани та підтримують аналог контекстів - віртуальну маршрутизацію та пересилання (VRF). Однак налаштування може створити деякі труднощі, пов'язані зі специфікою створення політик для кожної пари інтерфейсів, налаштування класів, списків доступу та групування всього цього конфігурацію.

3. Міжмережевий екран нового покоління Cisco Firepower (NG FW) може надавати функції контролю використання додатків користувачами та групами, веб-фільтр з перевіркою репутації, ретроспективний аналіз файлів тощо. буд. Ці служби раніше не підтримувалися маршрутизаторами ISR. Однак, Cisco пропонує можливість розгортання цих сервісів на універсальних блейд-серверах - мережевих обчислювальних машинах Cisco UCS серії E, які можуть бути встановлені в маршрутизаторі. Щодо ціни, варіант з додатковим блейд-сервером не є економічним рішенням.

4. Система запобігання вторгнень Cisco Firepower наступного покоління (NG IPS) для заміни модуля IPS, що підключається. В даний час можна одночасно запускати служби NG IPS та NG FW на одному пристрої.

5. Підтримка VPN у кількох варіантах:

Безклієнтний SSL VPN – доступ до необхідних програм здійснюється через веб-портал або переадресація портів здійснюється через тонкий клієнт та смарт-тунелі SSL VPN;

Remote Access IPsec VPN та L2TP over IPsec (IKEv1);

Easy VPN – тунелі IPSec IKEv1. Рішення, яке використовується для підключення віддалених користувачів через Cisco VPN Client;

тунелі SSL/IPSec IKEv2 за допомогою AnyConnect Secure Mobility Client. Підтримується більшість сучасних платформ ПК та мобільних пристроїв. Опціонально інтегрується із сервісами та послугами Cisco Secure Desktop, Cisco Cloud Web Security (колишній ScanSafe), 802.1x.

6. Підтримка кластеризації та аварійного перемикання. Аварійне перемикання працює в режимі очікування / активного з одним контекстом і в активному / активному режимі в декількох контекстах. Можлива робота у стані поточних підключень під час перемикання на резервний ASA. Ви також можете налаштувати аварійне перемикання між двома посиланнями на одному пристрої. Для мереж з високими вимогами до продуктивності можна об'єднати до 16 Cisco ASA. Якщо ми подивимося на рішення ISR, вони не підтримують стійкість до відмов та кластеризацію. Для забезпечення стійкості до збоїв вам доведеться налаштовувати кожен протокол або функцію окремо, накшталт налаштовування для шляхів резервного копіювання відрізнятися будуть, а для

VPN - власні. З ASA все в декілька раз легше, достатньо об'єднати пристрій та налаштувати як єдине ціле.

7. Підтримка протоколів маршрутизації. Інженери Cisco зробили великий крок уперед, і поточна модельна лінійка ASA, що широко представлена наринку, може похвалитися підтримкою статичної та динамічної маршрутизації через EIGRP, OSPF, BGP, маршрутизації на основі політик PBR, маршрутизації багатоадресного трафіку (PIM). Проте, є свої нюанси. Зокрема, робота з BGP не підтримує обробку повних таблиць маршрутизації full view, немає підтримки логічних інтерфейсів, а отже, немає можливості реалізувати GRE/VTI тунелі. На відміну від роутерів ISR, у ASA відсутній функціонал Cisco Express Forwarding (CEF). Маршрут визначається для кожної сесії лише один раз під час її встановлення. Якщо на ASA налаштований NAT, це також впливає, куди буде переадресовано пакети для тієї чи іншої сесії. На маршрутизаторах ISR лише таблиця маршрутизації або PBR відповідає за вибір оптимального маршруту. При передачі маршрутизації від одного інтерфейсу до іншого для ASA зовсім не обов'язково перемикати сеанс на цьому інтерфейсі. Для кожного запущеного сеансу ASA запам'ятовує не лише зовнішній інтерфейс – куди відправляти пакети, а й звідки вони приходять – зсередини.

8. Підтримка VPN типу мережа-мережа реалізована з використанням протоколів IPSec та L2TP. Однак через відсутність програмних функцій для роботи з інтерфейсами GRE дає неможливість реалізовувати тунелювання та шифрування трафіка даних через IPSec+GRE. Це означає, що ISR мають повну перевагу в цьому відношенні: IPSec + GRE, VTI, DMVPN, GET VPN, FlexVPN і т.д. Однак тут є суттєве обмеження, оскільки неможливо вказати, який вузол буде витісненим, і тому після відкату головного вузла перемикання на його не відбудеться. Крім того, OSPF + IPSec вимагає лише пристроїв ASA з обох боків, комбінація маршрутизаторів ASA + ISR не працюватиме.

9. Підтримка якості обслуговування. Налаштування ASA досить обмежені, по суті, ви можете настроювати поділ трафіка на кілька черг та розробити кожну з черг пріоритетною, чи призначити обмежувачі - регулятори. Таким планом, пакети з більш пріоритетною чергою завжди

будуть оброблятися пристроями в першій черзі, а спостерігач дає змогу встановити максимальну швидкість для черзі, з якої будуть передаватися пакети в мережу використовуючи інтерфейс зовні. Однак з зору управління QoS найбільш істотним недоліком ASA є його здатність глибоко аналізувати трафік.

10. Особливості команд інтерфейсу CLI. Налаштування деяких ролей на ASA має інший синтаксис, ніж налаштування тих самих ролей на пристроях ISR.

Вибір серед Cisco ISR та Cisco ASA Security Appliance в будь-яких ситуаціях не такий легкий, як може показатись на 1 погляд. Вимоги можна формулювати таким чином: необхідно забезпечити безпечний доступ в Інтернет для користувачів та забезпечити віддалений доступ, щоб колеги могли робити з любого місця, ми можемо порекомендувати Cisco ASA. Якщо цей пристрій має бути встановлений у філії, маршрутизатор може бути більш економічним та гнучким рішенням, оскільки він може підключати більше послуг. Якщо установка планується в штаб-квартирі компанії на межі мережі, то, встановивши два пристрої в одній мережі, ви можете розподілити послуги між ними: міжмережевий екран ASA, для контентної фільтрації, IPS, VPN для виділених юзерів та маршрутизатор серед динамічних протоколів, маршрутизація, міжсайтовий IPSec, DMVPN і т.д.

2.2 Cisco ASA та особливі налаштування приладів

Як зазначалося в попередньому розділі, Cisco ASA – це міжмережевий екран із відстеженням стану. ASA може працювати у двох режимах: маршрутизованому та прозорому. В контексті роботи бажано зупинитись на 1-му режимі роботи.

У режимі маршрутизації кожен інтерфейс ASA налаштовується з IP-адресою, маскою, рівнем безпеки та ім'ям інтерфейса.

Рівень безпеки – це число від 0 до 100, що дозволяє порівняти 2 інтерфейси та визначити, який з них є найбільш безпечним. Параметр використовується якісно, а чи не кількісно, тобто. важливим є лише співвідношення плюс-мінус. За замовчуванням трафік, що йде «зовні», тобто з інтерфейсу з більш високим рівнем безпеки на інтерфейс з нижчим рівнем безпеки, авторизується, сеанс зберігається, і повертаються лише відповіді цих сеансів. За умовчанням рух всередину заборонено.

Зазвичай рівень безпеки інтерфейсів встановлюється так, щоб максимально відповідати логічній топології мережі. Сама топологія є зони безпеки та правила взаємодії між ними.

Проте, як і у разі будь-якого маршрутизатора, мережі, налаштовані на інтерфейсах, автоматично потрапляють у таблицю маршрутизації з позначкою «connected», за умови, що сам інтерфейс перебуває у стані «up». Пакети автоматично маршрутизуються між цими мережами.

Ті мережі, які ASA сама не знає, треба описати. Це можна зробити вручну, використовуючи команду:

route {interface} {network} {mask} {next-hop} [{administrative distance}] [track {#}]

Вказується той інтерфейс, за яким треба шукати next-hop, оскільки ASA сама не здійснює такого пошуку. У таблицю маршрутизації потрапляє тільки один маршрут у мережу призначення.

Маршрут за замовчуванням задається таким же чином:

route {interface} 0.0.0.0 0.0.0.0 {next-hop}

Якщо ASA не знаходить записи в таблиці маршрутизації про мережу призначення пакета, то такий пакет вона відкидає.

Багато функцій ASA реалізовані за рахунок роботи зі списками доступу. Списки керування доступом (ACL, Access Control List) - це правила для керування заголовком IP-пакета рівня 4 моделі OSI. Списки доступу є простими рядковими конструкціями. Кожен рядок містить дозвіл або відмову. Рядки читаються зверху вниз, доки не буде знайдено точний збіг заголовка із зазначеним значенням списку доступу. Список дозволу ASA має змогу грати декілька ролей:

- фільтр вхідного чи вихідного трафіку на інтерфейсі;
- опис правил NAT (NAT Policy);
- опис правил перерозподілу маршрутів (мапа маршрутів);
- критерії попадання до класу трафіку для дальнішої обробки (Modular Policy Framework);
- рух інтересу та опис, який має бути зашифрований. Використовується перелік доступу на криптографічній карті;
- опис привілеїв віддаленого користувача при підключенні через IPSec або SSL VPN.

Списки доступу можуть бути стандартні та розширені. Стандартні списки доступу перевіряють тільки адресу джерела. На ASA такі списки доступу мають досить вузьке застосування (наприклад, для опису трафіку для віддаленого VPN користувача, який необхідно загортати в тунель. Технологія Split Tunneling):

access-list {NAME} [line #] standard {permit | deny | remark} {NETWORK} {MASK}

remark використовується для вставки коментарів у списки доступу;

параметр line # використовується для вставки рядка в певне місце списку доступу.

Мережна маска у списков доступу ASA проста. Для полегшення вказівки адреси існує низка скорочень, які зручно використовувати. Так, якщо вам потрібно описати всі мережі, то замість громіздкого 0.0.0.0 0.0.0.0 можна використовувати ключове слово any.

Порядок чергування каналів у списков доступу є дуже важливим, тому що сканування йде вгору і вниз і зупиняється при першому збігу. Тому найточніші інструкції слід дати вище.

Формат розширених списків доступу трохи складніший, тому що враховує ще й протокол, адреси призначення і може також визначати порти TCP / UDP точки походження і точки призначення:

access-list {NAME} [line #] {permit | deny} {protocol} {source net} {source mask} [{operator} {port #}] {destination net} {destination mask} [{operator} {port # }]

protocol – протокол стеку TCP / IP (ICMP, TCP, UDP, OSPF, IGMP, ESP і т.д.) Якщо треба вказати всі IP пакети, то і писати треба в якості протоколу слово «ip»

operator - літерний запис математичних операторів (eq - дорівнює, gt - більше, lt - менше, range - діапазон)

port - номер або назва TCP або UDP порту.

Якщо мережа містить багато схожих об'єктів (наприклад, мереж користувачів, серверів з однаковим набором сервісів і тощо), то при налаштуванні списків доступу адміністратор обов'язково зіткнетеся з тим, що вони стають занадто важкими для сприйняття та погано розширюваними. Для спрощення написання великих списків доступу на ASA застосовуються так звані об'єктні групи (object group). За допомогою них можна групувати схожі елементи мережі (протоколи, мережі, сервіси, повідомлення icmp).

object-group network {NAME}
network-object host {ip}
network-object {NET} {MASK}
object-group service {NAME} {tcp | udp}
port-object {operator} {port}

object-group protocol {NAME}
protocol-object {PROTOCOL}
object-group icmp {NAME}
icmp-object {icmp type}

Самі об'єктні групи застосовуються замість явного задання однотипного елемента в списку доступу. Наприклад, замість адрес точки походження і точки призначення можна застосувати об'єктну групу мережевого типу (object-group network), а замість явного задання сервісу TCP (ssh, http) можна застосувати групу типу сервісу TCP.

Наприклад:

access-list FROMOUTSIDE permit tcp any object-group SERVERS object-group WEBTCP

Налаштування VPN-з'єднання типу "мережа-мережа" між двома пристроями через незахищене середовище виконується в кілька етапів. Спочатку потрібно активувати IKEv1 на зовнішньому інтерфейсі. Цей протокол відповідає за узгодження роботи учасників у безпечному з'єднанні. Учасники погоджуються, який алгоритм шифрування використовується, який алгоритм використовується для перевірки цілісності та автентифікації іншого.

crypto ikev1 enable outside

Наступним кроком є створення та налаштування тунелю, зокрема, присвоєння йому атрибутів IPsec, встановлення IP-адреси зовнішнього інтерфейсу віддаленого ASA та встановлення визначеного загального ключа:

```
tunnel-group 172.2.0.2 type ipsec-l2l
tunnel-group 172.2.0.2 ipsec-attributes
 ikev1 pre-shared-key cisco
 !Note the IKEv1 keyword at the beginning of the pre-shared-key command
```

2.3 Використані програмні засоби при розробці web-інтерфейсу

Для виконання дипломного завдання з розробки веб-інтерфейсу для конфігурації Cisco ASA використовувалися мови програмування та інструменти, такі як HTML, CSS та JavaScript,

Зробимо короткий огляд. HTML (мова гіпертекстової розмітки) не є мовою програмування, це мова розмітки, яка визначає структуру вмісту сторінки та призначена для написання гіпертекстових документів, опублікованих у всесвітньому павутинні.

Гіпертекстовий документ – це текстовий файл із даними, впорядкованими за допомогою спеціальних міток – тегів, що інтерпретуються браузером з метою виведення на екран монітора структурованого змісту документа. Теги дозволяють розбити дані на логічні блоки, керувати заголовками, кеглем та відображенням тексту, вбудовувати мультимедійні файли, таблиці тощо. Серед іншого гіпертекстовий документ дозволяє розміщувати у своїй структурі посилання, що дозволяють швидко перейти до перегляду іншого документа.

Таким чином, документ HTML з даними та тегами, що фактично відображаються для користувача, - це спеціальні мовні конструкції HTML, які керують поданням документа та його розміткою.

Для того щоб побачити HTML-документи використовують браузери, які можуть інтерпретувати теги розмітки, та на основі отриманої інформації текст та графіка відповідно розміщуються на екрані.

CSS (каскадні таблиці стилів) – це набір параметрів форматування, які використовуються для керування зовнішнім виглядом та станом елементів на веб-сторінці веб-сайту. Однією з основних переваг використання CSS є можливість відокремити вміст сторінки від її зовнішнього вигляду. Опис стилів сторінок веб-сайту перебувають у файлі, а посилання на саме цей файл написані на усіх сторінках. Коли ви змінюєте стиль у загальному файлі, автоматично оновлюється зовнішній вигляд елементів усіх сторінках сайту.

У порівнянні з HTML CSS має набагато більший і більш гнучкий арсенал параметрів для стилізації елементів сторінки сайту. Використовуючи цю мову, можна створювати різні макети сторінок.

Написання та верстка стилю специфічна, дає змогу значно зменшити загальну вагу сторінки веб-сайту, що скорочує час і швидкість завантаження веб-сторінок у браузері.

Для створення структури сторінок сайту використовується метод блокової верстки. Елементи структури веб-сайту згруповані в теги DIV, кожному з яких може бути заданий свій стиль, спрощує для розробника в майбутньому створення та розміщення таких елементів на сторінці в цілому.

JavaScript - це об'єктно-орієнтована мова програмування прототипів, яка переважно використовується у WEB-розробці. Головна ідея JavaScript – це можливість налаштовувати значення атрибутів HTML-контейнера та відображати параметри середовища, коли користувач переглядає HTML-сторінку. Це не перезавантажує сторінку. Програми (скрипти) цією мовою обробляються вбудованим в браузер інтерпретатором.

Сьогодні JavaScript можна назвати безпечною мовою програмування загального призначення. Безпечно, тому що JavaScript не надає розробнику інструментів для роботи з низькорівневою пам'яттю та процесором.

За допомогою JavaScript ви можете реалізувати широкий спектр функцій, які залежатимуть лише від середовища виконання програми. У браузерах JavaScript може реалізовувати сценарії для будь-яких сторінок маніпуляцій та взаємодії з відвідувачами, зокрема:

- працювати з HTML-тегами: створювати нові, видаляти існуючі, змінювати стиль елементів, приховувати чи навпаки, відображати окремі елементи тощо;
- відстежувати дії відвідувачів сторінки: обробка клацань клавіатури, клацань миші, переміщень та положень курсору;

- надсилати запити на сервер та відображати додатковий контент на сторінці без перезавантаження самої сторінки (технологія AJAX);
- отримувати файли cookie, робити запити даних, відображати повідомлення тощо.

З міркувань безпеки більшість JavaScript у браузері обмежена поточним вікном і сторінкою, яку відкрив користувач:

- JavaScript не може читати/записувати довільні файли на жорсткий диск, копіювати їх або викликати програми. JavaScript не має прямого доступу до операційної системи;
- JavaScript, що працює в одній вкладці, не може взаємодіяти з іншими вкладками та вікнами, за винятком випадку, коли він сам відкрив це вікно або кілька вкладок з одного джерела (того ж домену, порту, протоколу);

- JavaScript може надсилати запити на сервер, на який було надіслано сторінку. Запит на інший домен теж можливий, але менш зручний, тому що тут також є обмеження безпеки [13].

Найбільшою перевагою JavaScript є повна інтеграція з HTML/CSS та його підтримка у всіх браузерах, у яких він уже включений за замовчуванням.

У JavaScript він буде використовуватися для читання форм, що налаштовуються, обробки дій користувача на веб-сайті і генерації коду конфігурації Cisco ASA на основі сценаріїв, вибраних юзером на веб-сайті.

3 ПРОГРАМНЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ГРАФІЧНОГО НАЛАШТУВАННЯ ASA

3.1 Графічний інтерфейс та розробка

Графічний інтерфейс конфігурації Cisco ASA - це веб-сайт, структура якого створена в HTML (Додаток А), стиль заснований на CSS (Додаток В), а JavaScript (Додаток С) відповідає за динамічну функціональність.

Функціональні можливості коду JavaScript можна розділити на такі логічні блоки:

- зчитувати значення, введені юзером в текстові поля, та передавати їх в змінні;
- читання логічних значень елемента управління стрілка - увімкнено/вимкнено - та створення на основі значення, отриманого з коду конфігурації, функції Cisco ASA, включеної або вимкненої цим елементом;
- формування готового набору команд налаштування Cisco ASA;
- заповніть форму графічного інтерфейсу значеннями за промовчанням;
- Видалення форми графічного інтерфейсу.

Розглянемо докладніше деякі блоки.

```
var ip_asal_int_gi0_0 = document.getElementById("ip_asal_int_gi0_0").value;
var mask_asal_int_gi0_0 =
document.getElementById("mask_asal_int_gi0_0").value;
var asal_gateway = document.getElementById("asal_gateway").value;
var ip_asal_int_gi0_1 = document.getElementById("ip_asal_int_gi0_1").value;
var mask_asal_int_gi0_1 =
document.getElementById("mask_asal_int_gi0_1").value;

var ip_cmel_int_f0_0 = document.getElementById("ip_cmel_int_f0_0").value;
var mask_cmel_int_f0_0 = document.getElementById("mask_cmel_int_f0_0").value;
var ip_cmel_int_fl_0 = document.getElementById("ip_cmel_int_fl_0").value;
var mask_cmel_int_fl_0 = document.getElementById("mask_cmel_int_fl_0").value;

var site_1 = document.getElementById("site_1").value;
var site_2 = document.getElementById("site_2").value;
```

Приведений код слугує за читання даних, введених у текстові поля форми, а саме:

- IP-адрес на інтерфейсі ASA та CME-Router;
- Маска адреса інтерфейсу ASA та CME-Router;

- IP-адреса шлюзу на зовнішніх інтерфейсах Cisco ASA – адреса інтерфейсу маршрутизатора, через який Cisco ASA виходить із зовнішньої мережі;
- domain - ім'я ресурсу, доступ до якого ви хочете заблокувати в офісній мережі.

Отримані дані зберігаються у відповідних змінних з метою їх подальшого використання для формування готової конфігурації настройок Cisco ASA.

Оскільки для налаштування конфігурації параметрів Cisco ASA необхідно мати інформацію про всі інтерфейси, бажано відразу вбудувати валідацію, яка перевірятиме повноту всіх текстових полів, що відповідають за інтерфейси Cisco ASA та ротори CME.

Оскільки при формуванні конфігурації пристроїв Cisco ASA необхідно мати інформацію про адреси мереж, підключених до інтерфейсів пристроїв, таку інформацію не можна запросити у користувача додатково, але можна отримати, знаючи IP-адресу. та маску такого інтерфейсу безпосередньо. За це відповідає така частина коду:

```
if(mask_cmel_int_fl_0 == "255.0.0.0"){
      var x = ip_cmel_int_fl_0.split('.');
      var net_ip_cmel_int_fl_0 = x[0] + ".0.0.0";


 if(ip_asal_int_gi0_0 == "" ||
       mask_asal_int_gi0_0 == "" ||
       asal_gateway == "" ||
       ip_asal_int_gi0_1 == "" ||
       mask_asal_int_gi0_1 == "" ||
       ip_asa2_int_gi0_0 == "" ||
       mask_asa2_int_gi0_0 == "" ||
       asa2_gateway == "" ||
       ip_asa2_int_gi0_1 == "" ||
       mask_asa2_int_gi0_1 == "" ||
       ip_cmel_int_f0_0 == "" ||
       mask_cmel_int_f0_0 == "" ||
       ip_cmel_int_fl_0 == "" ||
       mask_cmel_int_fl_0 == "" ||
       ip_cme2_int_f0_0 == "" ||
       mask_cme2_int_f0_0 == "" ||
       ip_cme2_int_fl_0 == "" ||
       mask_cme2_int_fl_0 == "" /*||
       site_1 == "" ||
       site_2 == ""*/ ){
 alert("Ви заповнили не всі поля");
 }else{
```

```
}
if(mask_cmel_int_fl_0 == "255.255.0.0"){
      var x = ip_cmel_int_fl_0.split('.');
      var net_ip_cmel_int_fl_0 = x[0] + "." + x[1] + ".0.0";
}
if(mask_cmel_int_fl_0 == "255.255.255.0"){
      var x = ip_cmel_int_fl_0.split('.');
      var net_ip_cmel_int_fl_0 = x[0] + "." + x[1] + "." + x[2] +".0";
}

}
```

Наступний блок – це обробка вибору користувачем елементів «стрілка».

Декларуємо змінні:

```
var qos = 1;

$(".qos").click(function(){
      if(qos == 0){

$(".qos").css("background","url(../application/image/qos_allow.png)");
            qos = 1;

$(".voip").css("background","url(../application/image/voip_allow.png)");
            voip = 1;
      }else{

$(".qos").css("background","url(../application/image/qos_deny.png)");
            qos = 0;
      }

});
```

Як видно з коду, кожна змінна має два значення:

0 – відповідає за відключення функції Cisco ASA;

1 - відповідає увімкненій функції Cisco ASA.

Логіка доступу до веб-ресурсів реалізована у зворотному порядку:

0 – доступ заблокований;

1 - доступ дозволено.

Сфокусуємось на налаштуваннях, які необхідно згенерувати при виборі тієї чи іншої змінної у стрілочних елементах.

Блокування мережі Cisco ASA та керування QoS налаштовуються за допомогою списків доступу, які слід застосовувати до зовнішнього або внутрішнього інтерфейсу.

Відповідний приклад згенерованого кода за вибором певних параметрів у графічному інтерфейсі приведено нижче:

```
//sites blocking for Head Office
if(head_to_site1 ==0){
      var head_to_site1_asa1 = "<br>conf t" +
                                    "<br>object network obj-www." + site_1 +
                                    "<br>fqdn www." + site_1 +
                                    "<br>object network obj-" + site_1 +
                                    "<br>fqdn " + site_1 +
                                    "<br>access-list " + site_1 + "_block
extended deny ip any object obj-www." + site_1 +
                                    "<br>access-list " + site_1 + "_block
extended deny ip any object obj-" + site_1 +
                                    "<br>access-list " + site_1 + "_block
extended permit ip any any" +
                                    "<br>access-group " + site_1 + "_block in
interface inside" +
                                    "<br>end";

}else{
      var head_to_site1_asa1 = "";
}
//VoIP QoS
if(qos ==1){
      var qos_asa1 = "<br>conf t" +
            "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_f1_0
+ " "  + mask_cme2_int_f1_0 + " " + net_ip_cme1_int_f1_0 + " " +
mask_cme1_int_f1_0 + " eq h323" +
            "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_f1_0
+ " "  + mask_cme2_int_f1_0 + " " + net_ip_cme1_int_f1_0 + " " +
mask_cme1_int_f1_0 + " eq sip" +
            "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_f1_0
+ " "  + mask_cme2_int_f1_0 + " " + net_ip_cme1_int_f1_0 + " " +
mask_cme1_int_f1_0 + " eq 2000" +
            "<br>access-list 105 extended permit tcp " + net_ip_cme1_int_f1_0
+ " " + mask_cme1_int_f1_0 + " " +  net_ip_cme2_int_f1_0 + " " +
mask_cme2_int_f1_0 + " eq h323" +
            "<br>access-list 105 extended permit tcp " + net_ip_cme1_int_f1_0
+ " " + mask_cme1_int_f1_0 + " " +  net_ip_cme2_int_f1_0 + " " +
mask_cme2_int_f1_0 + " eq sip" +
            "<br>access-list 105 extended permit tcp " + net_ip_cme1_int_f1_0
+ " " + mask_cme1_int_f1_0 + " " +  net_ip_cme2_int_f1_0 + " " +
mask_cme2_int_f1_0 + " eq 2000" +
            "<br>access-group 100 in interface outside" +
            "<br>class-map Voice-IN" +
            "<br>match access-list 100" +
            "<br>class-map Voice-OUT" +
            "<br>match access-list 105" +
            "<br>policy-map Voicepolicy" +
            "<br>class Voice-IN" +
            "<br>class Voice-OUT" +
            "<br>priority" +
            "<br>end" +
            "<br>conf t" +
            "<br>priority-queue outside" +
            "<br>service-policy Voicepolicy interface outside" +
            "<br>end";
}else{
      var qos_asa1 = "";
}
```

Код, який використовується для шифрування трафіка між декількома офісами, є наступним:

```
//IP Sec VPN
if(ip_sec_vpn ==1){
      var ip_sec_vpn_asa1 = "<br>conf t" +
          "<br>access-list VPN extended permit tcp " + net_ip_cme1_int_f1_0 + "
" + mask_cme1_int_f1_0 + " " +  net_ip_cme2_int_f1_0 + " " +
mask_cme2_int_f1_0 +
          "<br> access-list VPN extended permit icmp " + net_ip_cme1_int_f1_0 +
" "  + mask_cme1_int_f1_0 + " " + net_ip_cme2_int_f1_0 + " " +
mask_cme2_int_f1_0 +
          "<br>access-list ALLOW_VPN extended permit tcp " +
net_ip_cme2_int_f1_0 + " "  + mask_cme2_int_f1_0 + " " + net_ip_cme1_int_f1_0
+ " " + mask_cme1_int_f1_0 +
          "<br> access-list ALLOW_VPN extended permit icmp " +
net_ip_cme2_int_f1_0 + " "  + mask_cme2_int_f1_0 + " " + net_ip_cme1_int_f1_0
+ " " + mask_cme1_int_f1_0 +
          "<br>access-group ALLOW_VPN out interface inside" +
          "<br> crypto ikev1 policy 10" +
          "<br> encr aes" +
          "<br>  authentication pre-share" +
          "<br> group 2" +
          "<br>crypto ikev1 enable outside" +
          "<br>crypto ipsec ikev1 transform-set TRANS_SET esp-aes esp-sha-hmac"
+
          "<br> crypto map CRYP_MAP 10 match address VPN" +
          "<br> crypto map CRYP_MAP 10 set peer " + ip_asa2_int_gi0_0 +
          "<br> crypto map CRYP_MAP 10 set security-association lifetime
seconds 7200" +
          "<br> crypto map CRYP_MAP 10 set ikev1 transform-set TRANS_SET" +
          "<br> crypto map CRYP_MAP interface outside" +
          "<br> tunnel-group " + ip_asa2_int_gi0_0 + " type ipsec-l2l" +
          "<br>tunnel-group " + ip_asa2_int_gi0_0 + " ipsec-attributes" +
          "<br>  ikev1 pre-shared-key cisco123" +
          "<br>end";
```

Наступний блок коду призначений для створення нестандартних конфігурацій та передачі їх у поля виведення графічного інтерфейсу для пристроїв Cisco ASA, вміст залежить від значень змінних, код яких ми розглянули нижче. вище. Наприклад, для головного офісу склад конфігурації виглядає так:

```
var Past_in_asa1 = document.getElementById('result_asa1');
Past_in_asa1.innerHTML = "conf t" +
"<br>int g0/0" +
"<br>ip address " + ip_asa1_int_gi0_0 + " " + mask_asa1_int_gi0_0 +
"<br>nameif outside" +
"<br>security-level 100" +
"<br>no sh" +
"<br>int g0/1" +
"<br>ip address " + ip_asa1_int_gi0_1 + " " + mask_asa1_int_gi0_1 +
"<br>nameif inside" +
"<br>security-level 0" +
"<br>no sh" +
"<br>route outside 0.0.0.0 0.0.0.0 " + asa1_gateway +
"<br>route inside " + net_ip_cme1_int_f1_0 + " " + mask_cme1_int_f1_0 + " " +
ip_cme1_int_f0_0 +
```

```
"<br>class-map inspection_default" +
"<br>match default-inspection-traffic" +
"<br>exit" +
"<br>policy-map global_policy" +
"<br>class inspection_default" +
"<br>inspect icmp" +
"<br>exit" +
"<br>service-policy global_policy global" +
"<br>conf t" +
"<br>access-list ping permit icmp any any" +
"<br>access-group ping in interface outside" +
"<br>end" +
"<br>conf t" +
"<br>dns domain-lookup inside" +
"<br>dns server-group DefaultDNS" +
"<br>name-server " + ip_cme1_int_f0_0 +
"<br>dns expire-entry-timer minutes 1" +
"<br>end" +
"<br>"+
voip_asa1 +
"<br>"+
qos_asa1 +
"<br>"+
ip_sec_vpn_asa1 +
"<br>"+
head_to_site1_asa1 +
"<br>"+
head_to_site2_asa1 +
"<br>wr" +
"<br>";
```

Для філії всі параметри відображено щодо головного офісу. Повний код, включаючи блоки для встановлення значень за дефолтом та відкат, приведено в додатку В.

3.2 Опис взаємодії з інтерфейсом настроювань ASA

Робота із програмою здійснюється через браузер. Графічний інтерфейс доступний користувачеві після запуску title.html.

Сторінка дозволяє користувачеві встановити IP-адреси зовнішнього та внутрішнього інтерфейсів Cisco ASA у головному офісі та його філії, встановити адресу шлюзу (маршрутизатора, з якого Cisco ASA отримує доступ до зовнішньої мережі) та інтерфейси маршрутизаторів. які виконують функцію CME для організації VoIP між офісами, також за допомогою елементів керування Arrow можна увімкнути відключення служб ASA.

На сторінці налаштувань користувачеві доступні три кнопки керування конфігурацією мережі:

- Перша - заповнення полів;

- Друга - конфігурування;
- Третья - скинення налаштуваннь.

Приклад приведено на рис. 3.1.

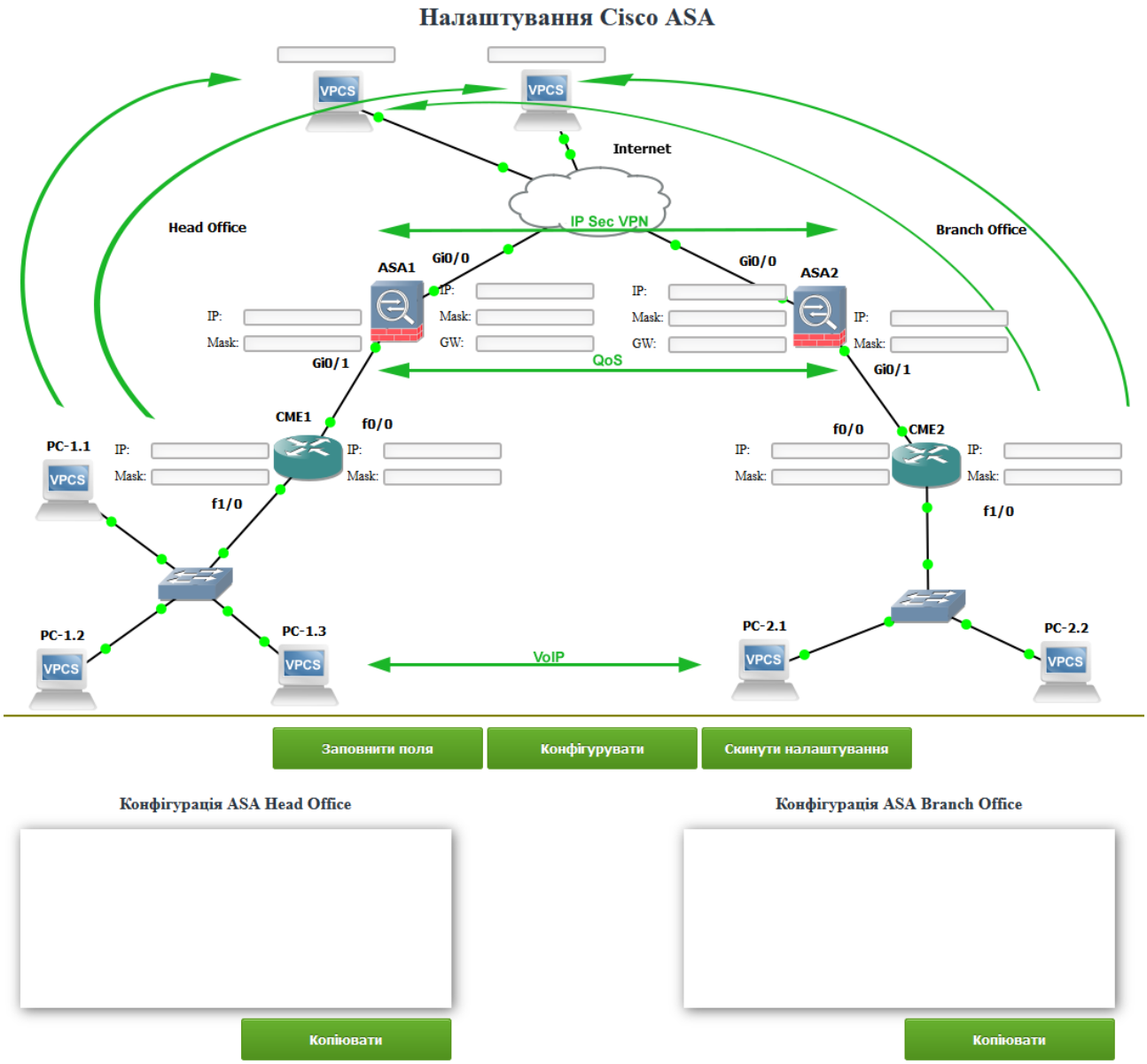

Рисунок 3.1 – Інтерфейс графічний для налаштувань

Заповнити поля - грузить стандартну мережеву конфігурацію в інтерфейс налаштувань (рис. 3.2).

Стандартна мережева конфігурація містить:

- Шифрування трафіку між головним офісом та філією;
- налаштована телефонія з VoIP QoS;
- блокує доступ до ресурсів Facebook та YouTube для користувачів зі штаб-квартири.

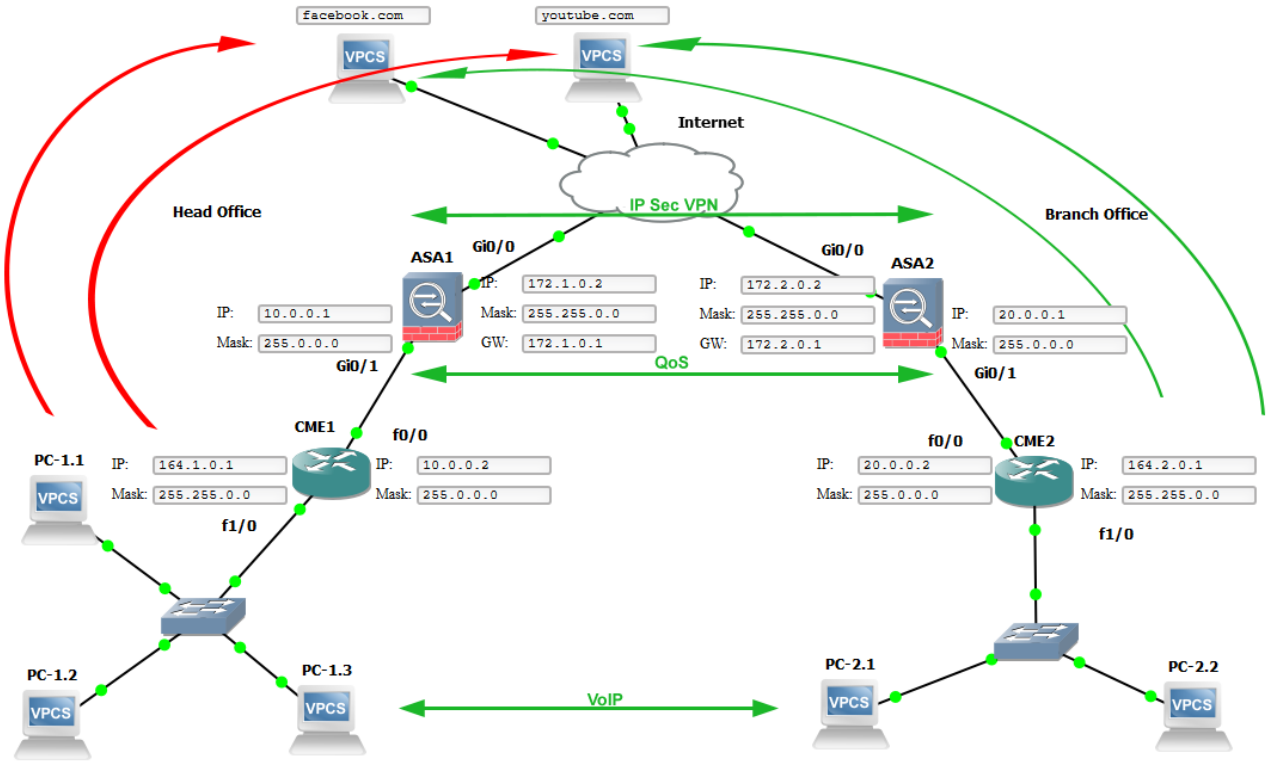

Рисунок 3.2 - Налаштування мережі за замовчуванням.

Скинути налаштування – видаляє введені користувачем значення та вибрані служби Cisco ASA.

Сервіси Cisco ASA включаються/вимикаються стрілками. Зелений колір елемента відповідає за включену послугу, червоний – за відключену (рис. 3.4).

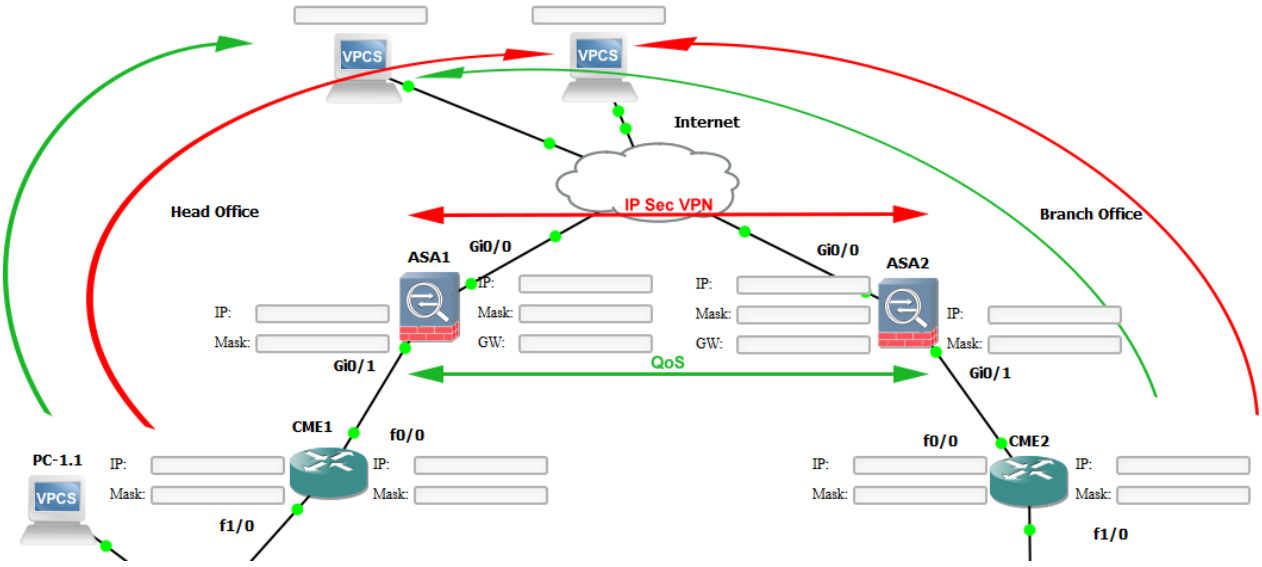

Рисунок 3.4 – Включення/вимкнення сервісів
за допомогою стрілок

Внизу інтерфейсу налаштувань перебувають блоки для виведення готових конфігураційних кодів ASA для кожного робочого столу (рис. 3.5):

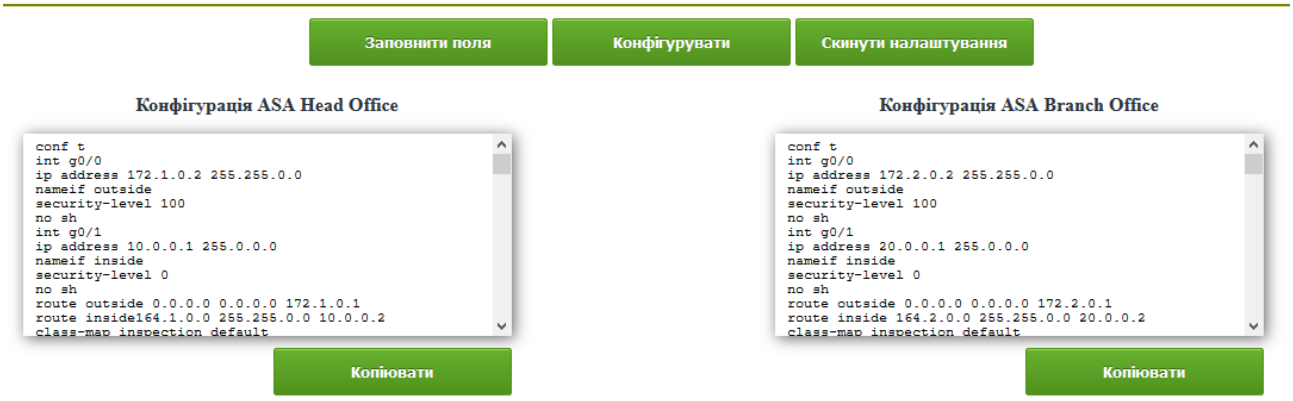

Рисунок 3.5 – Отримана за допомогою конфігурацій налаштування

За допомогою кнопок Копіювати вибрану конфігурацію можна експортувати до буфера обміну ОС і перенести в блокнот, наприклад, для подальшого імпорту на реальний пристрій в мережі або емулювати в CPT, GNS3 і т.д.

3.3 Відладка в GNS3 та на живому обладненні WEB-орієнтованої системи

Тести проводилися в GNS3, яке імітувало безпечну мережу між двома віддаленими офісами з підтримкою QoS VoIP-зв'язку та забороною доступу працівників до соц. мереж.

В середовищі GNS3 мережа будується на:

- Cisco ASA
- Cisco 3640
- Віртуальна машина Windows 7

Схема тестової мережі представлена малюнку 3.6. Дві філії підключені один до одного через Інтернет. По периметру усіх офісів встановлений ASA екран, на нього покладені функції мережевого захисту, забезпечення QoS,

шифрування трафіку даних VoIP. При цьому доступ до сайтів соціальних мереж для співробітників головного офісу заблоковано, а для співробітників філій немає обмежень на доступ до Інтернету. На маршрутизаторах всередині офісних локальних мереж Cisco CallManager Express налаштований для забезпечення IP-телефонії між будівлями.

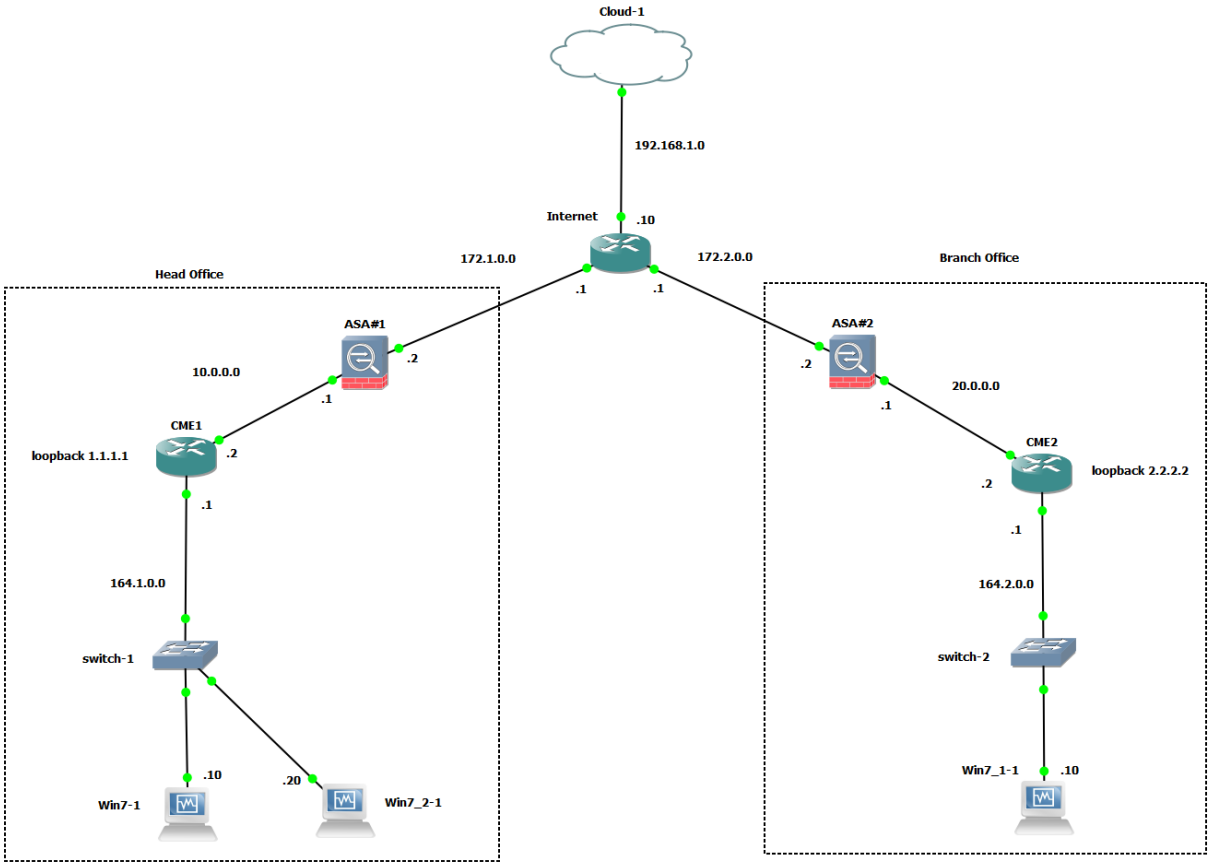

Рисунок 3.6 – Схема тестової мережі

Повну конфігурацію пристроїв у мережі наведено в Додатку G.

В результаті налаштувань комп'ютери, розташовані в локальній мережі штаб-квартири, мають доступ до Інтернету, але не можуть переглядати соціальні мережі. Відсутній доступ до цих ресурсів легко перевірити за допомогою команди ping (рис. 3.7).

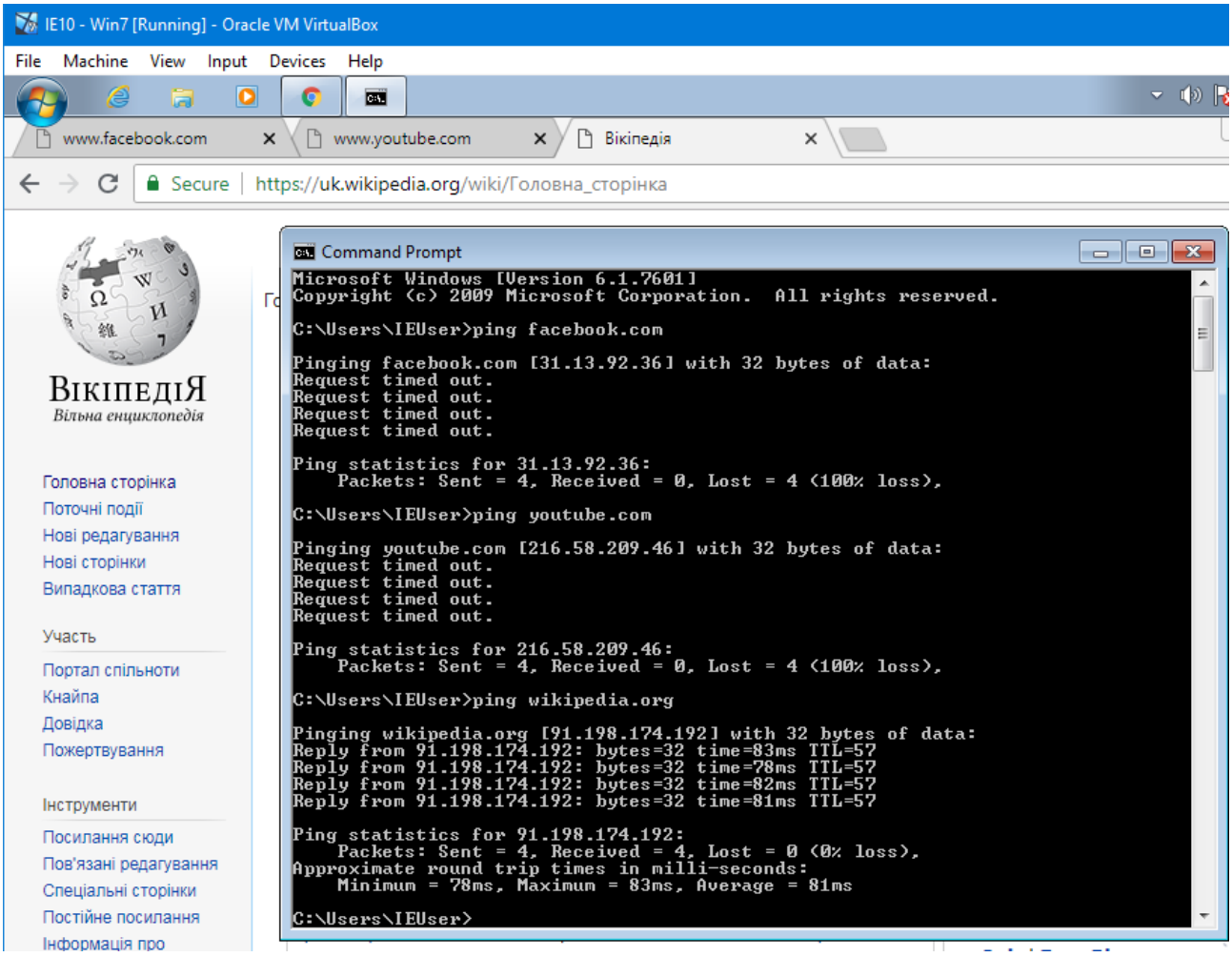

Рисунок 3.7 – ping відсутній з головного офісу до мереж

В мережі філіалу немає блокування приведених ресурсів:

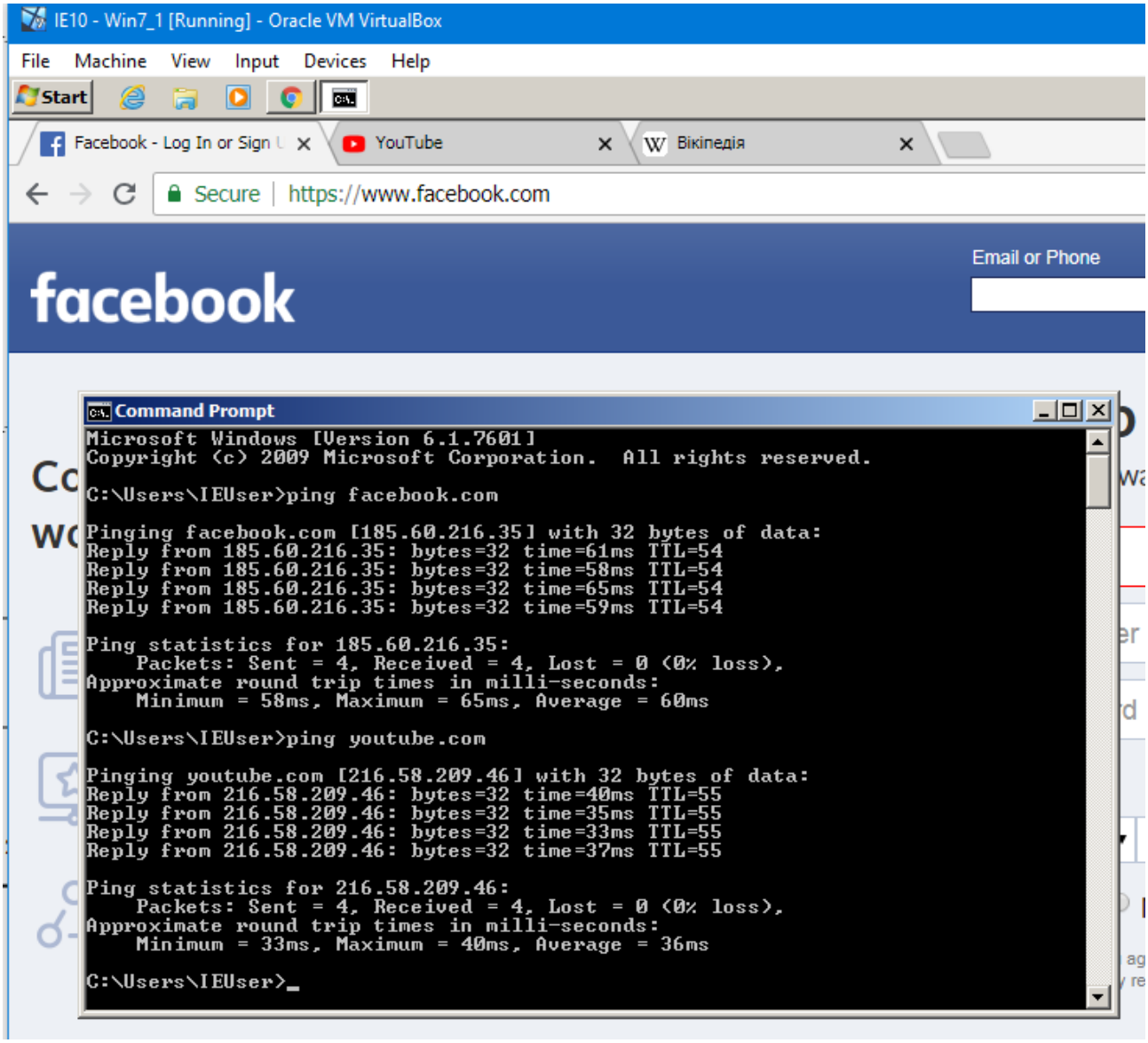

Рисунок 3.8 – Працездатність ping в мережі філії

Кожен офіс може спілкуватися один з одним використовуючи VoIP. Це можна легко перевірити, встановивши Cisco Phone на віртуальних машинах, розміщених у змодельованих мережах головного офісу та філій. Сеанс зв'язку показаний малюнку 3.9.

Рисунок 3.9 – VoIP-зв’язок між
головним офісом і філій

Статистику обслуговування трафіку можна переглянути наступною командою на Cisco ASA:

```
show priority-queue statistics outside
```

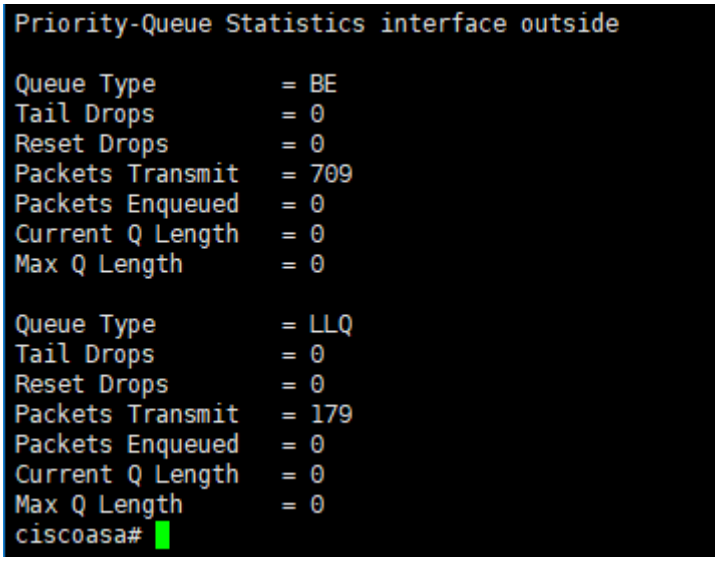

Рисунок 3.10 –Звітність трафіка в головному офісі на outside інтерфейсі

Як можна зрозуміти, згідно з налаштовування політики QOS, Voip пакети, трафік на Cisco ASA обслуговується в пріоритну чергу Low Latency Queuing, увесь залишившийся трафік потрапляє в чергу Best Effort.

ВИСНОВКИ

Під час кваліфікаційної магістерської роботи був проведений аналіз літератури, за результатами якого можна стверджувати, що Cisco ASA є одним із найпопулярніших апаратних міжмережевих екранів. Крім ексклюзивної функціональності забезпечення захисту внутрішньої мережі, він також пропонує основні функції маршрутизатора і тому має здатність успішно використовуватись як прилад два в одному в маленькиз мережах. Побудовано модель корпоративної мережі, що містить в собі 2 локально різні офіси: головний офіс та філію, підключені через Інтернет. Трафік, який йде через глобальну транзитну мережу, зашифровано. Офіси комунікаціюють один з одним за допомогою VoIP, трафік якого надається відповідно до рекомендацій Quality of Service. З цілью підвищити продуктивность мережі та співробітників у головному офісі доступ до соціальних мереж заблоковано.

Після налаштування було виявлено, що Cisco ASA, на відміну класичних рішень Cisco ISR, має ряд відмінностей, саме у командах настройки.

В результаті, щоб полегшити роботу мережевого адміністратора, була розроблена веб-інформаційна система, GUI який дає змогу отримати команди конфігурацій Cisco ASA. Система дозволяє використовувати буфер обміну для підготовки згенерованої конфігурації установок Cisco ASA для імпорту реальних пристроїв. Систему побудована та реалізована у форматі web-додатку з використанням мови програмування JavaScript.

СПИСОК ЛІТЕРАТУРИ

1. Cisco IOS Quality of Service Solutions Configuration Guide [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c.html
2. Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html
3. Mohan V. Network Security and Types of Attacks in Network // International Conference on Intelligent Computing, Communication & Convergence. - Procedia Computer Science 48 (2015) 503 – 506.
4. PIX/ASA 7.x: Enable VoIP (SIP, MGCP, H323, SCCP) Services Configuration Example [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/82446-enable-voip-config.html
5. QoS on the Cisco ASA Configuration Examples [Електронний ресур]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/82310-qos-voip-vpn.html
6. Using hostnames (DNS) in access-lists - configuration steps, caveats and troubleshooting [Електронний ресур]. – Режим доступу: https://community.cisco.com/t5/security-documents/using-hostnames-dns-in-access-lists-configuration-steps-caveats/ta-p/3123480
7. We are protected by a router: QoS [Електронний ресур]. – Режим доступу: http://developers-club.com/posts/62831/
8. Анатомия IPsec. Проверяем на прочность легендарный протокол [Електронний ресурс]. – Режим доступу: https://habr.com/company/xakep/blog/256659/
9. Грайворонський М. В. Безпека інформаційно-комунікаційнихсистем : підручник для ВНЗ / М. В. Грайворонський, О. М. Новіков ;М-вопраці

та соц. політики України. Держнаглядохоронпраці України. - К. : ВНV, 2009. - 607 с.

10. Kantor I. JavaScript language [Електронний ресурс]. – Режим доступу: https://learn.javascript.ru/
11. Комплексна безпека інформаційних мережевих систем : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя , 2016. – 256 с.
12. Olifer V.G. Computer networks. Principles, technologists, protocols: Student for universities / V.G. Olifer, N.A. Olifer. - 5th ed. - SPb .: Peter, 2016. – 992 c.
13. Fundamentals of computer networks: textbook. allowance / Ed. L.G. Gagarina. - M .: Forum ": INFRA-M, 2012. – 272 c.

ДОДАТКИ

Додаток А

```
<html>
<head>
<script src="js/clipboard.js"></script>
<script src="js/jquery.min.js"></script>
<script src="js/conf.js"></script>
<link rel="stylesheet" href="css/style.css">
</head>
<body>
      <div class="title">Налаштування Cisco ASA</div>
      <div class="network_schema">
            <div class="voip"></div>
            <div class="qos"></div>
            <div class="ip_sec_vpn"></div>
            <div class="head_to_site1"></div>
            <div class="head_to_site2"></div>
            <div class="branch_to_site1"></div>
            <div class="branch_to_site2"></div>
            <div class="blacklist">
                  <div class="site1">
                        <div class="parameter"></div><input id="site_1"
type="text" name="" > <br>
                  </div>
                  <div class="site2">
                        <div class="parameter"></div><input id="site_2"
type="text" name="" > <br>
                  </div>
            </div>
            <div class="asa1">
                  <div class="int_gi0_1">
                        <div class="parameter">IP: </div><input
id="ip_asa1_int_gi0_1" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_asa1_int_gi0_1" type="text" name="" >
                  </div>
                  <div class="int_gi0_0">
                        <div class="parameter">IP: </div><input
id="ip_asa1_int_gi0_0" type="text" name="" required
pattern="((^|\.)((25[0-5])|(2[0-4]\d)|(1\d\d)|([1-9]?\d))){4}$" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_asa1_int_gi0_0" type="text" name="" > <br>
                        <div class="parameter">GW: </div><input
id="asa1_gateway" type="text" name="" >    <br>
                  </div>
            </div>
            <div class="asa2">
                  <div class="int_gi0_0">
                        <div class="parameter">IP: </div><input
id="ip_asa2_int_gi0_0" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_asa2_int_gi0_0" type="text" name="" > <br>
                        <div class="parameter">GW: </div><input
id="asa2_gateway" type="text" name="" >         <br>
                  </div>
```

```
                  <div class="int_gi0_1">
                        <div class="parameter">IP: </div><input
id="ip_asa2_int_gi0_1" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_asa2_int_gi0_1" type="text" name="" >
                  </div>
            </div>
            <div class="cme1">
                  <div class="int_f1_0">
                        <div class="parameter">IP: </div><input
id="ip cme1 int f1 0" type="text" name="" > <br>

                              <div class="parameter">IP: </div><input
      id="ip cme1 int f1 0" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_cme1_int_f1_0" type="text" name="" > <br>
                  </div>
                  <div class="int_f0_0">
                        <div class="parameter">IP: </div><input
id="ip_cme1_int_f0_0" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_cme1_int_f0_0" type="text" name="" >
                  </div>
            </div>
            <div class="cme2">
                  <div class="int_f0_0">
                        <div class="parameter">IP: </div><input
id="ip_cme2_int_f0_0" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_cme2_int_f0_0" type="text" name="" >
                  </div>
                  <div class="int_f1_0">
                        <div class="parameter">IP: </div><input
id="ip_cme2_int_f1_0" type="text" name="" > <br>
                        <div class="parameter">Mask: </div><input
id="mask_cme2_int_f1_0" type="text" name="" >
                  </div>
            </div>
      </div>
      <div class="network_config">
            <div class="block_kontr">
                  <div class="block_button_ger">
                        <div class="block_button_conf"><input
class="button_default" type="button" value="Заповнити поля" ></div>
                        <div class="block_button_conf"><input
class="button_generate" type="button" value="Конфігурувати" ></div>
                        <div class="block_button_conf"><input
class="button_clear" type="button" value="Скинути налаштування" ></div>
                  </div>
                  <div class="conf_asa1">
                        <div class="title_conf_asa1">Конфігурація ASA Head
Office</div>
                        <div class="result_asa1" id="result_asa1" ></div>
                        <input class="button_copy_asa1"
id="button_copy_asa1"  data-clipboard-target="#result_asa1" type="button"
value="Копіювати" >
                  </div>
```

```
                    <div class="conf_asa2">
                          <div class="title_conf_asa2">Конфігурація ASA Branch
    Office</div>
                          <div class="result_asa2" id="result_asa2" ></div>
                          <input class="button_copy_asa2"
    id="button_copy_asa2"  data-clipboard-target="#result_asa2" type="button"
    value="Копіювати" >
                    </div>
               </div>
         </div>

</body>
</html>
```

Додаток Б

```
.title {
    text-align: center;
    font-size: 24px;
      font-weight: bold;
    color: #2A3541;
}

.network_schema{
    background: url(../image/network_map2.png) no-repeat center;
      width: 1100px;
      height: 650px;
      position: relative;
      margin: 0 auto;
}

.parameter{
      width: 34px;
      margin: 5px 0;
      display: inline-block;
    font-size: 12px;
}

.cme1 input,
.cme2 input,
.asa1 input,
.asa2 input,
.blacklist input{
      width: 113px;
    padding: 0 3px;
    background-color: #fcfcfc;
    border: 2px solid #b3b2b2;
    color: #000;
    font-size: 12px;
    border-radius: 3px;
    box-shadow: inset 1px 3px 10px 0 #eeeeef;
      font-family: "Courier New";
      font-size: 11;
}

.asa1 input:focus,
.asa2 input:focus,
.cme1 input:focus,
.cme2 input:focus,
.blacklist input:focus {
    border-color: #74d36b;
}

.asa1 input{
      margin: 3px 0;
}

.asa1 {
    position: absolute;
    top: 233px;
    left: 205px;
      z-index: 10;
}

.asa2 {
    position: absolute;
    top: 214px;
    right: 130px;
      z-index: 10;
}

.asa1 .int_gi0_0 {
    display: inline-block;

}
```

```
.asal .int_gi0_1 {
    display: inline-block;
    margin: 20px 70px 0 3px;
}

.asa2 .int_gi0_0 {
    display: inline-block;
    margin: 20px 60px 0 5px;
}

.asa2 .int_gi0_1 {
    display: inline-block;
}

.cmel {
    position: absolute;
    top: 365px;
    left: 110px;
      z-index: 10;
}

.cme2 {
    position: absolute;
    top: 365px;
    right: 22px;
      z-index: 10;
}

.cmel .int_fl_0 {
    display: inline-block;
    margin: 20px 70px 0 10px;
}

.cmel .int_f0_0 {
    display: inline-block;

}

.cme2 .int_f0_0 {
    display: inline-block;
    margin: 20px 70px 0 10px;
}

.cme2 .int_fl_0 {
    display: inline-block;
}

.sitel {
    position: absolute;
    top: 14px;
    left: 240px;
      z-index: 10;
}

.site2 {
    position: absolute;
    top: 14px;
    left: 440px;
      z-index: 10;
}

   .network_config {
       border-top: 2px solid #808000;
       padding: 0 0 0px 0;
   }

   .block_kontr {
       width: 1121px;
       margin: 0 auto;
   }

   .conf_asal {
       display: inline-block;
```

```
margin: 0px 0 0 40px;

}

.conf_asa2 {
    display: inline-block;
    float: right;
    margin: 0px 40px 0 0 ;
}

.title_conf_asa1,
.title_conf_asa2 {
    text-align: center;
    font-size: 16px;
      font-weight: bold;
    margin: 20px 0 15px 0;
    color: #2A3541;
}

.result_asa1,
.result_asa2 {
    width: 400px;
    height: 160px;
    overflow: auto;
    padding: 5px 0 5px 10px;
    box-shadow: 2px 2px 12px 0px rgba(50, 50, 50, 0.75);
      font-family: "Courier New";
      font-size: 11;
}

.block_button_conf{
      margin: 0 auto;
      left: 25%;
      position: relative;
      display: inline-block;
}

input.button_copy_asa1 {
    margin: 10px 0 0 0;
}

input.button_copy_asa2 {
    margin: 10px 0 0 0;
}

input#button_copy_asa1,
input#button_copy_asa2,
input.button_generate,
input.button_default,
input.button_clear {
 display:inline-block;
 margin-top: 10px;
 height:40px;
 width:200px;
 float:right;
 background-color: #68b12f;
 background: -webkit-gradient(linear, left top, left bottom, from(#68b12f),
to(#5091le));
 background: -webkit-linear-gradient(top, #68b12f, #5091le);
 background: -moz-linear-gradient(top, #68b12f, #5091le);
 background: -ms-linear-gradient(top, #68b12f, #5091le);
 background: -o-linear-gradient(top, #68b12f, #5091le);
background: linear-gradient(top, #68b12f, #5091le);
 border: 1px solid #509111;
 border-bottom: 1px solid #5b992b;
 border-radius: 3px;
 -webkit-border-radius: 3px;
 -moz-border-radius: 3px;
 -ms-border-radius: 3px;
 -o-border-radius: 3px;
 box-shadow: inset 0 1px 0 0 #9fd574;
 -webkit-box-shadow: 0 1px 0 0 #9fd574 inset ;
 -moz-box-shadow: 0 1px 0 0 #9fd574 inset;
```

```
        -ms-box-shadow: 0 1px 0 0 #9fd574 inset;
         -o-box-shadow: 0 1px 0 0 #9fd574 inset;
         color: white;
         font-weight: bold;
         padding: 6px 20px;
         text-align: center;
         text-shadow: 0 -1px 0 #396715;
        }

        input#button_copy_asa1:hover,
        input#button_copy_asa2:hover,
        input.button_generate:hover,
        input.button_default:hover,
        input.button_clear:hover {
         opacity:.85;
         cursor: pointer;
        }

        input#button_copy_asa1:active,
        input#button_copy_asa2:active,
        input.button_generate:active,
        input.button_default:active,
        input.button_clear:active {
         border: 1px solid #2091le;
         box-shadow: 0 0 10px 5px #356b0b inset;
         -webkit-box-shadow:0 0 10px 5px #356b0b inset ;
         -moz-box-shadow: 0 0 10px 5px #356b0b inset;
         -ms-box-shadow: 0 0 10px 5px #356b0b inset;
         -o-box-shadow: 0 0 10px 5px #356b0b inset;
        }

        .ip_sec_vpn {
            width: 438px;
            height: 22px;
            position: absolute;
            top: 175px;
              left: 370px;
            background: url(../image/ip_sec_vpn_allow.png) no-repeat;
            cursor: pointer;
              z-index: 3;
        }

        .voip {
            width: 318px;
              height: 20px;
              position: absolute;
              bottom: 40px;
              left: 360px;
            background: url(../image/voip_allow.png) no-repeat;
            cursor: pointer;
              z-index: 3;
        }

        .qos {
            width: 438px;
              height: 23px;
              position: absolute;
              bottom: 320px;
              left: 370px;
            background: url(../image/qos_allow.png) no-repeat;
            cursor: pointer;
              z-index: 3;
}

       .head_to_site1 {
           width: 211px;
           height: 319px;
           position: absolute;
           top: 39px;
           left: 30px;
           background: url(../image/head_to_site1_allow.png) no-repeat;
           cursor: pointer;
             z-index: 2;
}
```

```
.head_to_site2 {
    width: 394px;
    height: 319px;
    position: absolute;
    top: 50px;
    left: 100px;
    background: url(../image/head_to_site2_allow.png) no-repeat;
    cursor: pointer;
      z-index: 1;
}

.branch_to_site1 {
    width: 625px;
    height: 277px;
    position: absolute;
    top: 65px;
    right: 100px;
    background: url(../image/branch_to_site1_allow.png) no-repeat;
    cursor: pointer;
      z-index: 2;
}

.branch_to_site2 {
    width: 526px;
    height: 317px;
    position: absolute;
    top: 40px;
    right: 15px;
    background: url(../image/branch_to_site2_allow.png) no-repeat;
    cursor: pointer;
      z-index: 1;
}
```

Додаток В

```
$(dOcument).ready(function(){
new Clipboard('.button_copy_asa1');
new Clipboard('.button_copy_asa2');

//declare test fields voriables
$(".button_generate").click(function(){
vor ip_asa1_int_gi0_0 = dOcument.getElementByld("ip_asa1_int_gi0_0").value;
vor mask_asa1_int_gi0_0 = dOcument.getElementByld("mask_asa1_int_gi0_0").value;
vor asa1_gateway = dOcument.getElementByld("asa1_gateway").value;
vor ip_asa1_int_gi0_1 = dOcument.getElementByld("ip_asa1_int_gi0_1").value;
vor mask_asa1_int_gi0_1 = dOcument.getElementByld("mask_asa1_int_gi0_1").value;

vor ip_asa2_int_gi0_0 = dOcument.getElementByld("ip_asa2_int_gi0_0").value;
vor mask_asa2_int_gi0_0 = dOcument.getElementByld("mask_asa2_int_gi0_0").value;
vor asa2_gateway = dOcument.getElementByld("asa2_gateway").value;
vor ip_asa2_int_gi0_1 = dOcument.getElementByld("ip_asa2_int_gi0_1").value;
vor mask_asa2_int_gi0_1 = dOcument.getElementByld("mask_asa2_int_gi0_1").value;

vor ip_cme1_int_f0_0 = dOcument.getElementByld("ip_cme1_int_f0_0").value;
vor mask_cme1_int_f0_0 = dOcument.getElementByld("mask_cme1_int_f0_0").value;
vor ip_cme1_int_f1_0 = dOcument.getElementByld("ip_cme1_int_f1_0").value;
vor mask_cme1_int_f1_0 = dOcument.getElementByld("mask_cme1_int_f1_0").value;

vor ip_cme2_int_f0_0 = dOcument.getElementByld("ip_cme2_int_f0_0").value;
vor mask_cme2_int_f0_0 = dOcument.getElementByld("mask_cme2_int_f0_0").value;
vor ip_cme2_int_f1_0 = dOcument.getElementByld("ip_cme2_int_f1_0").value;
vor mask_cme2_int_f1_0 = dOcument.getElementByld("mask_cme2_int_f1_0").value;

vor site_1 = dOcument.getElementByld("site_1").value;
vor site_2 = dOcument.getElementByld("site_2").value;

//valldation of text fields population
if(ip_asa1_int_gi0_0 == "" ||
        mask_asa1_int_gi0_0 == "" ||
        asa1_gateway == "" ||
        ip_asa1_int_gi0_1 == "" ||
        mask_asa1_int_gi0_1 == "" ||
        ip_asa2_int_gi0_0 == "" ||
        mask_asa2_int_gi0_0 == "" ||
        asa2_gateway == "" ||
        ip_asa2_int_gi0_1 == "" ||
        mask_asa2_int_gi0_1 == "" ||
        ip_cme1_int_f0_0 == "" ||
        mask_cme1_int_f0_0 == "" ||
        ip_cme1_int_f1_0 == "" ||
        mask_cme1_int_f1_0 == "" ||
        ip_cme2_int_f0_0 == "" ||
        mask_cme2_int_f0_0 == "" ||
        ip_cme2_int_f1_0 == "" ||
        mask_cme2_int_f1_0 == "" /*||
        site_1 == "" ||
        site_2 == ""*/ ){
alert("Ви заповнили не всі поля");
}else{
 //network address recognizing according to interfaces mask: 164.1.0.1 255.255.0.0 =>
 164.1.0.0
 if(mask_cme1_int_f1_0 == "255.0.0.0"){
         vor x = ip_cme1_int_f1_0.split('.');
         vor net_ip_cme1_int_f1_0 = x[0] + ".0.0.0";
 }
 if(mask_cme1_int_f1_0 == "255.255.0.0"){
         vor x = ip_cme1_int_f1_0.split('.');
         vor net_ip_cme1_int_f1_0 = x[0] + "." + x[1] + ".0.0";
 }
 if(mask_cme1_int_f1_0 == "255.255.255.0"){
         vor x = ip_cme1_int_f1_0.split('.');
         vor net_ip_cme1_int_f1_0 = x[0] + "." + x[1] + "." + x[2] +".0";
 }


 if(mask_cme2_int_f1_0 == "255.0.0.0"){
         vor x = ip_cme2_int_f1_0.split('.');
         vor net_ip_cme2_int_f1_0 = x[0] + ".0.0.0";
```

```
}
if(mask_cme2_int_fl_0 == "255.255.0.0"){
        vor x = ip_cme2_int_fl_0.split('.');
        vor net_ip_cme2_int_fl_0 = x[0] + "." + x[1] + ".0.0";
}
if(mask_cme2_int_fl_0 == "255.255.255.0"){
        vor x = ip_cme2_int_fl_0.split('.');
        vor net_ip_cme2_int_fl_0 = x[0] + "." + x[1] + "." + x[2] +".0";
}


//prepearing the configuration of ASA1, ASA2

//VoIP
if(voip == 1){
        vor voip_asa1 = "<br>conf t" +
                                        "<br>access-list gre extended permit gre
host " + ip_cme2_int_f0_0 + " host " + ip_cme1_int_f0_0 +
                                        "<br>access-group gre in interface outslde"
+
                                        "<br>end";

        vor voip_asa2 = "<br>conf t" +
                                        "<br>access-list gre extended permit gre
host " + ip_cme1_int_f0_0 + " host " + ip_cme2_int_f0_0 +
                                        "<br>access-group gre in interface outslde"
+
                                        "<br>end";

}else{
        vor voip_asa1 = "";
        vor voip_asa2 = "";
}


//sites blocking for Head Office
if(head_to_site1 ==0){
        vor head_to_site1_asa1 = "<br>conf t" +
                                                "<br>object network obj-www." +
site_1 +
                                                "<br>fqdn www." + site_1 +
                                                "<br>object network obj-" + site_1
+
                                                "<br>fqdn " + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended deny ip any object obj-www." + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended deny ip any object obj-" + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended permit ip any any" +
                                                "<br>access-group " + site_1 +
"_block in interface inslde" +
                                                "<br>end";

}else{
        vor head_to_site1_asa1 = "";
}
 if(head_to_site2 ==0){
         vor head_to_site2_asa1 = "<br>conf t" +
                                                 "<br>object network obj-www." +
 site_2 +
                                                 "<br>fqdn www." + site_2 +
                                                 "<br>object network obj-" + site_2
 +
                                                 "<br>fqdn " + site_2 +
                                                 "<br>access-list " + site_2 +
 "_block extended deny ip any object obj-www." + site_2 +
                                                 "<br>access-list " + site_2 +
 "_block extended deny ip any object obj-" + site_2 +
                                                 "<br>access-list " + site_2 +
 "_block extended permit ip any any" +
                                                 "<br>access-group " + site_2 +
 "_block in interface inslde" +
                                                 "<br>end";

 }else{
         vor head_to_site2_asa1 = "";
}
```

```
//sites blocking for Branch Office
if(branch_to_site1 ==0){
        vor branch_to_site1_asa2 = "<br>conf t" +
                                                "<br>object network obj-www." +
site_1 +
                                                "<br>fqdn www." + site_1 +
                                                "<br>object network obj-" + site_1
+
                                                "<br>fqdn " + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended deny ip any object obj-www." + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended deny ip any object obj-" + site_1 +
                                                "<br>access-list " + site_1 +
"_block extended permit ip any any" +
                                                "<br>access-group " + site_1 +
"_block in interface inslde" +
                                                "<br>end";

}else{
        vor branch_to_site1_asa2 = "";
}

if(branch_to_site2 ==0){
        vor branch_to_site2_asa2 = "<br>conf t" +
                                                "<br>object network obj-www." +
site_2 +
                                                "<br>fqdn www." + site_2 +
                                                "<br>object network obj-" + site_2
+
                                                "<br>fqdn " + site_2 +
                                                "<br>access-list " + site_2 +
"_block extended deny ip any object obj-www." + site_2 +
                                                "<br>access-list " + site_2 +
"_block extended deny ip any object obj-" + site_2 +
                                                "<br>access-list " + site_2 +
"_block extended permit ip any any" +
                                                "<br>access-group " + site_2 +
"_block in interface inslde" +
                                                "<br>end";

}else{
        vor branch_to_site2_asa2 = "";
}
//IP Sec VPN
if(ip_sec_vpn ==1){
        vor ip_sec_vpn_asa1 = "<br>conf t" +
           "<br>access-list VPN extended permit tcp " + net_ip_cme1_int_fl_0 + " " +
mask_cme1_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 +
           "<br> access-list VPN extended permit icmp " + net_ip_cme1_int_fl_0 + " "
+ mask_cme1_int_fl_0 + " " + net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 +
           "<br>access-list ALLOW_VPN extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cme1_int_fl_0 + " " + mask_cme1_int_fl_0 +
           "<br> access-list ALLOW_VPN extended permit icmp " + net_ip_cme2_int_fl_0 +
" "  + mask_cme2_int_fl_0 + " " + net_ip_cme1_int_fl_0 + " " + mask_cme1_int_fl_0 +
           "<br>access-group ALLOW_VPN out interface inslde" +
           "<br> crypto ikev1 policy 10" +
           "<br> encr aes" +
           "<br>  authentication pre-share" +
           "<br> group 2" +
           "<br>crypto ikev1 enable outslde" +
           "<br>crypto ipsec ikev1 transform-set TRANS_SET esp-aes esp-sha-hmac" +
           "<br> crypto map CRYP_MAP 10 match address VPN" +
           "<br> crypto map CRYP_MAP 10 set peer " + ip_asa2_int_gi0_0 +
           "<br> crypto map CRYP_MAP 10 set security-association lifetime seconds
7200" +
           "<br> crypto map CRYP_MAP 10 set ikev1 transform-set TRANS_SET" +
           "<br> crypto map CRYP_MAP interface outslde" +
           "<br> tunnel-group " + ip_asa2_int_gi0_0 + " type ipsec-l2l" +
           "<br>tunnel-group " + ip_asa2_int_gi0_0 + " ipsec-attributes" +
           "<br>  ikev1 pre-shared-key cisco123" +
           "<br>end";
```

```
vor ip_sec_vpn_asa2 = "<br>conf t" +
          "<br>access-list VPN extended permit tcp " + net_ip_cme2_int_fl_0 + " "  +
mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 +
          "<br> access-list VPN extended permit icmp " + net_ip_cme2_int_fl_0 + " "
+ mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 +
          "<br>access-list ALLOW_VPN extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 +
          "<br> access-list  ALLOW_VPN extended permit icmp " + net_ip_cmel_int_fl_0
+ " "  + mask_cmel_int_fl_0 + " " + net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 +
          "<br>access-group ALLOW_VPN out interface inslde" +
          "<br> crypto ikevl policy 10" +
          "<br> encr aes" +
          "<br>  authentication pre-share" +
          "<br> group 2" +
          "<br>crypto ikevl enable outslde" +
          "<br>crypto ipsec ikevl transform-set TRANS_SET esp-aes esp-sha-hmac" +
          "<br> crypto map CRYP_MAP 10 match address VPN" +
          "<br> crypto map CRYP_MAP 10 set peer " + ip_asal_int_gi0_0 +
          "<br> crypto map CRYP_MAP 10 set security-association lifetime seconds
7200" +
          "<br> crypto map CRYP_MAP 10 set ikevl transform-set TRANS_SET" +
          "<br> crypto map CRYP_MAP interface outslde" +
          "<br> tunnel-group " + ip_asal_int_gi0_0 + " type ipsec-l2l" +
          "<br>tunnel-group " + ip_asal_int_gi0_0 + " ipsec-attributes" +
          "<br>  ikevl pre-shared-key cisco123" +
          "<br>end";
}else{
        vor ip_sec_vpn_asal = "";
        vor ip_sec_vpn_asa2 = "";
}


//VoIP QoS
if(qos ==1){
        vor qos_asal = "<br>conf t" +
                "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
h323" +
                "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
sip" +
                "<br>access-list 100 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
2000" +
                "<br>access-list 105 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
h323" +
                "<br>access-list 105 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
sip" +
                "<br>access-list 105 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
2000" +


                "<br>access-group 100 in interface outslde" +
                "<br>class-map Voice-IN" +
                "<br>match access-list 100" +
                "<br>class-map Voice-OUT" +
                "<br>match access-list 105" +
                "<br>policy-map Voicepolicy" +
                "<br>class Voice-IN" +
                "<br>class Voice-OUT" +
                "<br>priority" +
                "<br>end" +
                "<br>conf t" +
                "<br>priority-queue outslde" +
                "<br>service-policy Voicepolicy interface outslde" +
                "<br>end";

       vor qos_asa2 = "<br>conf t" +
                "<br>access-list 100 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
h323" +
                "<br>access-list 100 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
sip" +
```

```
                "<br>access-list 100 extended permit tcp " + net_ip_cmel_int_fl_0 + "
" + mask_cmel_int_fl_0 + " " +  net_ip_cme2_int_fl_0 + " " + mask_cme2_int_fl_0 + " eq
2000" +
                "<br>access-list 105 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
h323" +
                "<br>access-list 105 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
sip" +
                "<br>access-list 105 extended permit tcp " + net_ip_cme2_int_fl_0 + "
"  + mask_cme2_int_fl_0 + " " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " eq
2000" +
                "<br>access-group 100 in interface outside" +
                "<br>class-map Voice-IN" +
                "<br>match access-list 100" +
                "<br>class-map Voice-OUT" +
                "<br>match access-list 105" +
                "<br>policy-map Voicepolicy" +
                "<br>class Voice-IN" +
                "<br>class Voice-OUT" +
                "<br>priority" +
                "<br>end" +
                "<br>conf t" +
                "<br>priority-queue outside" +
                "<br>service-policy Voicepolicy interface outside" +
                "<br>end";

}else{
        vor qos_asal = "";
        vor qos_asa2 = "";
}



//filling the block with ASA configuration
vor Past_in_asal = d0cument.getElementByld('result_asal');
Past_in_asal.innerHTML = "conf t" +
"<br>int g0/0" +
"<br>ip address " + ip_asal_int_gi0_0 + " " + mask_asal_int_gi0_0 +
"<br>nameif outside" +
"<br>security-level 100" +
"<br>no sh" +
"<br>int g0/1" +
"<br>ip address " + ip_asal_int_gi0_1 + " " + mask_asal_int_gi0_1 +
"<br>nameif inside" +
"<br>security-level 0" +
"<br>no sh" +
"<br>route outside 0.0.0.0 0.0.0.0 " + asal_gateway +
"<br>route inside " + net_ip_cmel_int_fl_0 + " " + mask_cmel_int_fl_0 + " " +
ip_cmel_int_f0_0 +
"<br>class-map inspection_default" +
"<br>match default-inspection-traffic" +
"<br>exit" +
"<br>policy-map global_policy" +
"<br>class inspection_default" +
"<br>inspect icmp" +
"<br>exit" +
"<br>service-policy global_policy global" +
"<br>conf t" +
"<br>access-list ping permit icmp any any" +
"<br>access-group ping in interface outside" +
"<br>end" +
"<br>conf t" +
"<br>dns domain-lookup inside" +
"<br>dns server-group DefaultDNS" +
"<br>name-server " + ip_cmel_int_f0_0 +
"<br>dns expire-entry-timer minutes 1" +
"<br>end" +
"<br>"+
voip_asal +
"<br>"+
qos_asal +
"<br>"+
ip_sec_vpn_asal +
"<br>"+
head_to_site1_asal +
"<br>"+
```

```
head_to_site2_asal +
"<br>wr" +
"<br>";


vor Past_in_asa2 = d0cument.getElementByld('result_asa2');
Past_in_asa2.innerHTML = "conf t" +
"<br>int g0/0" +
"<br>ip address " + ip_asa2_int_gi0_0 + " " + mask_asa2_int_gi0_0 +
"<br>nameif outslde" +
"<br>security-level 100" +
"<br>no sh" +
"<br>int g0/1" +
"<br>ip address " + ip_asa2_int_gi0_1 + " " + mask_asa2_int_gi0_1 +
"<br>nameif inslde" +
"<br>security-level 0" +
"<br>no sh" +
"<br>route outslde 0.0.0.0 0.0.0.0 " + asa2_gateway +
"<br>route inslde " + net_ip_cme2_int_fl_0 + " " + mask_cmel_int_fl_0 + " " +
ip_cme2_int_f0_0 +
"<br>class-map inspection_default" +
"<br>match default-inspection-traffic" +
"<br>exit" +
"<br>policy-map global_policy" +
"<br>class inspection_default" +
"<br>inspect icmp" +
"<br>exit" +
"<br>service-policy global_policy global" +
"<br>conf t" +
"<br>access-list ping permit icmp any any" +
"<br>access-group ping in interface outslde" +
"<br>end" +
"<br>conf t" +
"<br>dns domain-lookup inslde" +
"<br>dns server-group DefaultDNS" +
"<br>name-server " + ip_cme2_int_f0_0 +
"<br>dns expire-entry-timer minutes 1" +
"<br>end" +
"<br>"+
voip_asa2 +
"<br>"+
qos_asa2 +
"<br>"+
ip_sec_vpn_asa2 +
"<br>"+
branch_to_sitel_asa2 +
"<br>"+
branch_to_site2_asa2 +
"<br>wr" +
"<br>";
}
});

//declare services arrows voriables
vor voip = 1;
vor qos = 1;
vor ip_sec_vpn = 1;
vor head_to_sitel = 1;
vor head_to_site2 = 1;
vor branch_to_sitel = 1;
vor branch_to_site2 = 1;


$(".voip").click(function(){
        if(voip == 0){

        $(".voip").css("background","url(../application/image/voip_allow.png)");
                voip = 1;
        }else{

        $(".voip").css("background","url(../application/image/voip_deny.png)");
                voip = 0;
                $(".qos").css("background","url(../application/image/qos_deny.png)");
                qos = 0;
        }

});
```

```
$(".qos").click(function(){
        if(qos == 0){

        $(".qos").css("background","url(../application/image/qos_allow.png)");
                qos = 1;

        $(".voip").css("background","url(../application/image/voip_allow.png)");
                voip = 1;
        }else{
                $(".qos").css("background","url(../application/image/qos_deny.png)");
                qos = 0;
        }

});
$(".ip_sec_vpn").click(function(){
        if(ip_sec_vpn == 0){

        $(".ip_sec_vpn").css("background","url(../application/image/ip_sec_vpn_allow.p
ng)");
                ip_sec_vpn = 1;
        }else{

        $(".ip_sec_vpn").css("background","url(../application/image/ip_sec_vpn_deny.pn
g)");
                ip_sec_vpn = 0;
        }

});
$(".head_to_sitel").click(function(){
        if(head_to_sitel == 0){

        $(".head_to_sitel").css("background","url(../application/image/head_to_sitel_a
llow.png)");
                head_to_sitel = 1;
        }else{

        $(".head_to_sitel").css("background","url(../application/image/head_to_sitel_d
eny.png)");
                head_to_sitel = 0;
        }

});
$(".head_to_site2").click(function(){
        if(head_to_site2 == 0){

        $(".head_to_site2").css("background","url(../application/image/head_to_site2_a
llow.png)");
                head_to_site2 = 1;
        }else{

        $(".head_to_site2").css("background","url(../application/image/head_to_site2_d
eny.png)");
                head_to_site2 = 0;
        }

});

$(".branch_to_sitel").click(function(){
        if(branch_to_sitel == 0){

        $(".branch_to_sitel").css("background","url(../application/image/branch_to_sit
el_allow.png)");
                branch_to_sitel = 1;
        }else{

        $(".branch_to_sitel").css("background","url(../application/image/branch_to_sit
el_deny.png)");
                branch_to_sitel = 0;
        }

});
$(".branch_to_site2").click(function(){
        if(branch_to_site2 == 0){

        $(".branch_to_site2").css("background","url(../application/image/branch_to_sit
e2_allow.png)");
                branch_to_site2 = 1;
```

```
}else{

        $(".branch_to_site2").css("background","url(../application/image/branch_to_sit
e2_deny.png)");
                branch_to_site2 = 0;
        }

});


//set the defolt network configuration
$(".button_default").click(function(){

        $(".voip").css("background","url(../application/image/voip_allow.png)");
        voip = 1;
        $(".qos").css("background","url(../application/image/qos_allow.png)");
        qos = 1;
        $(".ip_sec_vpn").css("background","url(../application/image/ip_sec_vpn_allow.p
ng)");
        ip_sec_vpn = 1;
        $(".head_to_site1").css("background","url(../application/image/head_to_site1_d
eny.png)");
        head_to_site1 = 0;
        $(".head_to_site2").css("background","url(../application/image/head_to_site2_d
eny.png)");
        head_to_site2 = 0;

        $(".branch_to_site1").css("background","url(../application/image/branch_to_sit
e1_allow.png)");
        branch_to_site1 = 1;
        $(".branch_to_site2").css("background","url(../application/image/branch_to_sit
e2_allow.png)");
        branch_to_site2 = 1;


        d0cument.getElementByld("ip_asa1_int_gi0_0").value = "172.1.0.2";
        d0cument.getElementByld("mask_asa1_int_gi0_0").value = "255.255.0.0";
        d0cument.getElementByld("asa1_gateway").value = "172.1.0.1";
        d0cument.getElementByld("ip_asa1_int_gi0_1").value = "10.0.0.1";
        d0cument.getElementByld("mask_asa1_int_gi0_1").value = "255.0.0.0";

        d0cument.getElementByld("ip_asa2_int_gi0_0").value = "172.2.0.2";
        d0cument.getElementByld("mask_asa2_int_gi0_0").value = "255.255.0.0";
        d0cument.getElementByld("asa2_gateway").value = "172.2.0.1";
        d0cument.getElementByld("ip_asa2_int_gi0_1").value = "20.0.0.1";
        d0cument.getElementByld("mask_asa2_int_gi0_1").value = "255.0.0.0";

        d0cument.getElementByld("ip_cme1_int_f0_0").value = "10.0.0.2";
        d0cument.getElementByld("mask_cme1_int_f0_0").value = "255.0.0.0";
        d0cument.getElementByld("ip_cme1_int_f1_0").value = "164.1.0.1";
        d0cument.getElementByld("mask_cme1_int_f1_0").value = "255.255.0.0";

        d0cument.getElementByld("ip_cme2_int_f0_0").value = "20.0.0.2";
        d0cument.getElementByld("mask_cme2_int_f0_0").value = "255.0.0.0";
        d0cument.getElementByld("ip_cme2_int_f1_0").value = "164.2.0.1";
        d0cument.getElementByld("mask_cme2_int_f1_0").value = "255.255.0.0";

        d0cument.getElementByld("site_1").value = "facebook.com";
        d0cument.getElementByld("site_2").value = "youtube.com";

});

//reset all configurations
$(".button_clear").click(function(){
        $(".voip").css("background","url(../application/image/voip_allow.png)");
        voip = 1;
        $(".qos").css("background","url(../application/image/qos_allow.png)");
        qos = 1;
        $(".ip_sec_vpn").css("background","url(../application/image/ip_sec_vpn_allow.p
ng)");
        ip_sec_vpn = 1;
        $(".head_to_site1").css("background","url(../application/image/head_to_site1_a
llow.png)");
        head_to_site1 = 1;
        $(".head_to_site2").css("background","url(../application/image/head_to_site2_a
llow.png)");
        head_to_site2 = 1;
```

```
$(".branch_to_sitel").css("background","url(../application/image/branch_to_sitel_allow
.png)");
        branch_to_sitel = 1;
        $(".branch_to_site2").css("background","url(../application/image/branch_to_sit
e2_allow.png)");
        branch_to_site2 = 1;

        dOcument.getElementByld("ip_asal_int_gi0_0").value = "";
        dOcument.getElementByld("mask_asal_int_gi0_0").value = "";
        dOcument.getElementByld("asal_gateway").value = "";
        dOcument.getElementByld("ip_asal_int_gi0_1").value = "";
        dOcument.getElementByld("mask_asal_int_gi0_1").value = "";

        dOcument.getElementByld("ip_asa2_int_gi0_0").value = "";
        dOcument.getElementByld("mask_asa2_int_gi0_0").value = "";
        dOcument.getElementByld("asa2_gateway").value = "";
        dOcument.getElementByld("ip_asa2_int_gi0_1").value = "";
        dOcument.getElementByld("mask_asa2_int_gi0_1").value = "";

        dOcument.getElementByld("ip_cmel_int_f0_0").value = "";
        dOcument.getElementByld("mask_cmel_int_f0_0").value = "";
        dOcument.getElementByld("ip_cmel_int_fl_0").value = "";
        dOcument.getElementByld("mask_cmel_int_fl_0").value = "";

        dOcument.getElementByld("ip_cme2_int_f0_0").value = "";
        dOcument.getElementByld("mask_cme2_int_f0_0").value = "";
        dOcument.getElementByld("ip_cme2_int_fl_0").value = "";
        dOcument.getElementByld("mask_cme2_int_fl_0").value = "";

        dOcument.getElementByld("site_1").value = "";
        dOcument.getElementByld("site_2").value = "";

        vor Past_in_asal = dOcument.getElementByld('result_asal');
        Past_in_asal.innerHTML = "";
        vor Past_in_asa2 = dOcument.getElementByld('result_asa2');
        Past_in_asa2.innerHTML = "";
});

});
```

Додаток Г

```
!--- PHASE 1

!---Internet router
en
conf t
int fa 0/0
ip address 192.168.1.10 255.255.255.0
no sh
end

conf t
int fa 1/0
ip address 172.1.0.1 255.255.0.0
no sh
end

conf t
int fa 2/0
ip address 172.2.0.1 255.255.0.0
no sh
end

conf t
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 10.0.0.0 255.0.0.0 172.1.0.2
ip route 164.1.0.0 255.255.0.0 172.1.0.2
ip route 20.0.0.0 255.0.0.0 172.2.0.2
ip route 164.2.0.0 255.255.0.0 172.2.0.2
end



!---Office #1
!---ASA#1
en
conf t
int g0/0
ip address 172.1.0.2 255.255.0.0
nameif outside
security-level 100
no shutdown

int g0/1
ip address 10.0.0.1 255.0.0.0
nameif inside
security-level 0
no shutdown

route outside 0.0.0.0 0.0.0.0 172.1.0.1
route inside 164.1.0.0 255.255.0.0 10.0.0.2



class-map inspection_default
match default-inspection-traffic
exit
policy-map global_policy
class inspection_default
inspect icmp
exit
service-policy global_policy global

conf t
access-list ping permit icmp any any
access-group ping in interface outside

!---CME1
en

conf t
int fa 0/0
ip address 10.0.0.2 255.0.0.0
no sh
end
```

```
conf t
int fa 1/0
ip address 164.1.0.1 255.255.0.0
no sh
end

conf t
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 172.1.0.0 255.255.0.0 10.0.0.1
ip route 192.168.1.0 255.255.255.0 10.0.0.1
ip route 172.2.0.0 255.255.0.0 10.0.0.1
ip route 20.0.0.0 255.0.0.0 10.0.0.1
ip route 164.2.0.0 255.255.0.0 10.0.0.1
end

!---Office #2
!---ASA#2
en
conf t
int g0/0
ip address 172.2.0.2 255.255.0.0
nameif outside
no shutdown

int g0/1
ip address 20.0.0.1 255.0.0.0
nameif inside
no shutdown

route outside 0.0.0.0 0.0.0.0 172.2.0.1
route inside 164.2.0.0 255.255.0.0 20.0.0.2


class-map inspection_default
match default-inspection-traffic
exit
policy-map global_policy
class inspection_default
inspect icmp
exit
service-policy global_policy global

conf t
access-list ping permit icmp any any
access-group ping in interface outside

!---CME2
en

conf t
int fa 0/0
ip address 20.0.0.2 255.0.0.0
no sh
end

conf t
int fa 1/0
ip address 164.2.0.1 255.255.0.0
no sh
end
```

```
conf t
ip route 0.0.0.0 0.0.0.0 20.0.0.1
ip route 172.2.0.0 255.255.0.0 20.0.0.1
ip route 192.168.1.0 255.255.255.0 20.0.0.1
ip route 172.1.0.0 255.255.0.0 20.0.0.1
ip route 10.0.0.0 255.0.0.0 20.0.0.1
ip route 164.1.0.0 255.255.0.0 20.0.0.1
end



!---PHASE2: VOIP

!---CME1
conf t
  int loopback 0
  ip address 1.1.1.1 255.255.255.255
  end

  conf t
  telephony-service
  max-ephones 10
  max-dn 10
  keepalive 15
  system message VoIP from Cisco
  ip source-address 1.1.1.1 port 2000
  auto assign 1 to 10
  create cnf-files
  ex

  voice service voip
  allow-connections h323 to h323
  allow-connections h323 to sip
  allow-connections sip to sip
  allow-connections sip to h323
  sip
  registrar server expires max 600 min 60
  ex

  voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g711alaw
  codec preference 3 g729r8
  ex

  ephone-dn 1
  number 1001
  name Host_A
  ex

  ephone-dn 2
  number 2001
  name Host_B
  ex

  ephone 1
  mac-address 0800.2799.B15F
  type cipc
  ex

  dial-peer voice 1 voip
  destination-pattern 30..
  session target ipv4:2.2.2.2
  voice-class codec 1
  end

  conf t
  int tunnel 0
  ip address 172.10.1.1 255.255.255.0
  tunnel source fa 0/0
  tunnel destination 20.0.0.2
  end

  conf t
```

```
!---CME2
conf t
int loopback 0
ip address 2.2.2.2 255.255.255.255
end

conf t
telephony-service
max-ephones 10
max-dn 10
keepalive 15
system message VoIP from Cisco
ip source-address 2.2.2.2 port 2000
auto assign 1 to 10
create cnf-files
exit
voice service voip
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to sip
allow-connections sip to h323
sip
registrar server expires max 600 min 60
exit
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g711alaw
codec preference 3 g729r8
exit
ephone-dn 1 dual-line
number 3001
name Host_C
exit
ephone 1
mac-address 0800.278F.6CE1
type cipc
exit
dial-peer voice 1 voip
destination-pattern ....
session target ipv4:1.1.1.1
voice-class codec 1
end

conf t
int tunnel 0
ip address 172.10.1.2 255.255.255.0
tunnel source fa 0/0
tunnel destination 10.0.0.2
end

conf t
ip route 1.1.1.1 255.255.255.255 tunnel 0
end


!---ASA1
conf t
access-list gre extended permit gre host 20.0.0.2 host 10.0.0.2
access-group gre in interface outside

!---ASA2
conf t
access-list gre extended permit gre host 10.0.0.2 host 20.0.0.2
access-group gre in interface outside



!---PHASE3: HTTPS blocking via DNS

!---CME1

!---config DNS server
conf t
ip dns server
ip domain-lookup
ip name-server 8.8.8.8
```

```
!---CME2

!---config DNS server
conf t
ip dns server
ip domain-lookup
ip name-server 8.8.8.8


!---ASA1

dns domain-lookup inside
dns server-group DefaultDNS
name-server 10.0.0.2
dns expire-entry-timer minutes 1

object network obj-www.facebook.com
fqdn www.facebook.com
object network obj-facebook.com
fqdn facebook.com
object network obj-www.youtube.com
fqdn www.youtube.com
object network obj-youtube.com
fqdn youtube.com
access-list blacklist extended deny ip any object obj-www.facebook.com
access-list blacklist extended deny ip any object obj-facebook.com
access-list blacklist extended deny ip any object obj-www.youtube.com
access-list blacklist extended deny ip any object obj-youtube.com
access-list blacklist extended permit ip any any

access-group blacklist in interface inside


show running-config access-list
sh access-list | inc blacklist line 1



!---PHASE4: VPN

!---IP SEC
--ASA1


   access-list VPN extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0
    access-list VPN extended permit icmp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0

    access-list ALLOW_VPN extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0
255.255.0.0
    access-list ALLOW_VPN extended permit icmp 164.2.0.0 255.255.0.0 164.1.0.0
255.255.0.0

    access-group ALLOW_VPN out interface inside

    crypto ikev1 policy 10
     encr aes
     authentication pre-share
     group 2

    crypto ikev1 enable outside
   crypto ipsec ikev1 transform-set TRANS_SET esp-aes esp-sha-hmac

   crypto map CRYP_MAP 10 match address VPN
   crypto map CRYP_MAP 10 set peer 172.2.0.2
   crypto map CRYP_MAP 10 set security-association lifetime seconds 7200
   crypto map CRYP_MAP 10 set ikev1 transform-set TRANS_SET
   crypto map CRYP_MAP interface outside

   tunnel-group 172.2.0.2 type ipsec-l2l
   tunnel-group 172.2.0.2 ipsec-attributes
    ikev1 pre-shared-key cisco123


--ASA2
```

```
        access-list VPN extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0
255.255.0.0
    access-list VPN extended permit icmp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0

    access-list ALLOW_VPN extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0
255.255.0.0
    access-list ALLOW_VPN extended permit icmp 164.1.0.0 255.255.0.0 164.2.0.0
255.255.0.0

    access-group ALLOW_VPN out interface inside

    crypto ikev1 policy 10
     encr aes
     authentication pre-share
     group 2

    crypto ikev1 enable outside

    crypto ipsec ikev1 transform-set TRANS_SET esp-aes esp-sha-hmac

    crypto map CRYP_MAP 10 match address VPN
    crypto map CRYP_MAP 10 set peer 172.1.0.2
    crypto map CRYP_MAP 10 set ikev1 transform-set TRANS_SET
    crypto map CRYP_MAP interface outside

    tunnel-group 172.1.0.2 type ipsec-121
    tunnel-group 172.1.0.2 ipsec-attributes
     ikev1 pre-shared-key cisco123


show crypto ikev1 sa



!---PHASE5: VOIP QoS
!--ASA1

conf t
access-list 100 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
h323
access-list 100 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
sip
access-list 100 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
2000

access-list 105 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
h323
access-list 105 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
sip
access-list 105 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
2000

access-group 100 in interface outside

class-map Voice-IN
match access-list 100

class-map Voice-OUT
match access-list 105

policy-map Voicepolicy
class Voice-IN
class Voice-OUT

priority
end
configure terminal
priority-queue outside

service-policy Voicepolicy interface outside
end

!---ASA#2
conf t

access-list 100 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
h323
```

```
access-list 100 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
sip
access-list 100 extended permit tcp 164.1.0.0 255.255.0.0 164.2.0.0 255.255.0.0 eq
2000

access-list 105 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
h323
access-list 105 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
sip
access-list 105 extended permit tcp 164.2.0.0 255.255.0.0 164.1.0.0 255.255.0.0 eq
2000

access-group 100 in interface outside

class-map Voice-IN
match access-list 100

class-map Voice-OUT
match access-list 105

policy-map Voicepolicy
class Voice-IN
class Voice-OUT

priority
end
configure terminal
priority-queue outside

service-policy Voicepolicy interface outside
end
```