ВСТУП

Інтернет представляє величезні потенційні можливості по розгортанню бізнесу, зниженню витрат на забезпечення обсягу продажів, а також сприяє підвищенню рівня обслуговування клієнтів. Разом з тим, інтернет являє собою підвищену небезпеку для інформації й систем організації. При використанні правильної мережної архітектури інтернет може стати помічником, і при цьому ви зможете контролювати погрози безпеки інформації й систем.

Першим питанням, пов'язаним з архітектурою інтернету, на який необхідно дати відповідь, є, які служби будуть надаватися організації через інтернет. Від складу цих служб і від того, хто буде здійснювати до них доступ, залежить загальна архітектура й навіть місце розміщення служб.

В організації також може діяти комутація публічних повідомлень, наприклад, для реалізації груп обговорення, заснованих на електронній пошті. Такі системи, як правило, називаються серверами списків. Вони дозволяють зовнішнім користувачам відправляти пошту в систему, а система пересилає повідомлення передплатникам списку. Сервери списків можуть розташовуватися на тих же серверах, що й основні поштові системи організації, однак тут необхідно враховувати підвищені вимоги до пропускної здатності каналу в загальній архітектурі з'єднань інтернету.

Якщо в організації здійснюється публікація даних для клієнтів або партнерів через інтернет, необхідно створити ресурс-сервер і розмістити на ньому вміст для публічного перегляду. Цей ресурс-сервер може розташовуватися в іншому місці або перебувати усередині мережі.

Розглянуті в роботі питання побудови та реалізації точок присутності мережі та послуг, дозволяють отримати комплексне рішення щодо запровадження сервісів провайдерами телекомунікацій.

1 АРХІТЕКТУРА ВУЗЛА МЕРЕЖІ ДОСТУПУ

1.1 Вимоги до пропускної здатності та доступності

При розробці архітектури з'єднань із інтернетом, наявних в організації, найважливішими питаннями є вимоги до пропускної здатності й доступності. Пропускна здатність - це властивість, про яке необхідно домовлятися з постачальником послуг інтернету (провайдером). Провайдер повинен порекомендувати використовувати відповідні лінії з'єднань для роботи із пропонованими службами (рисунок 1.1.).

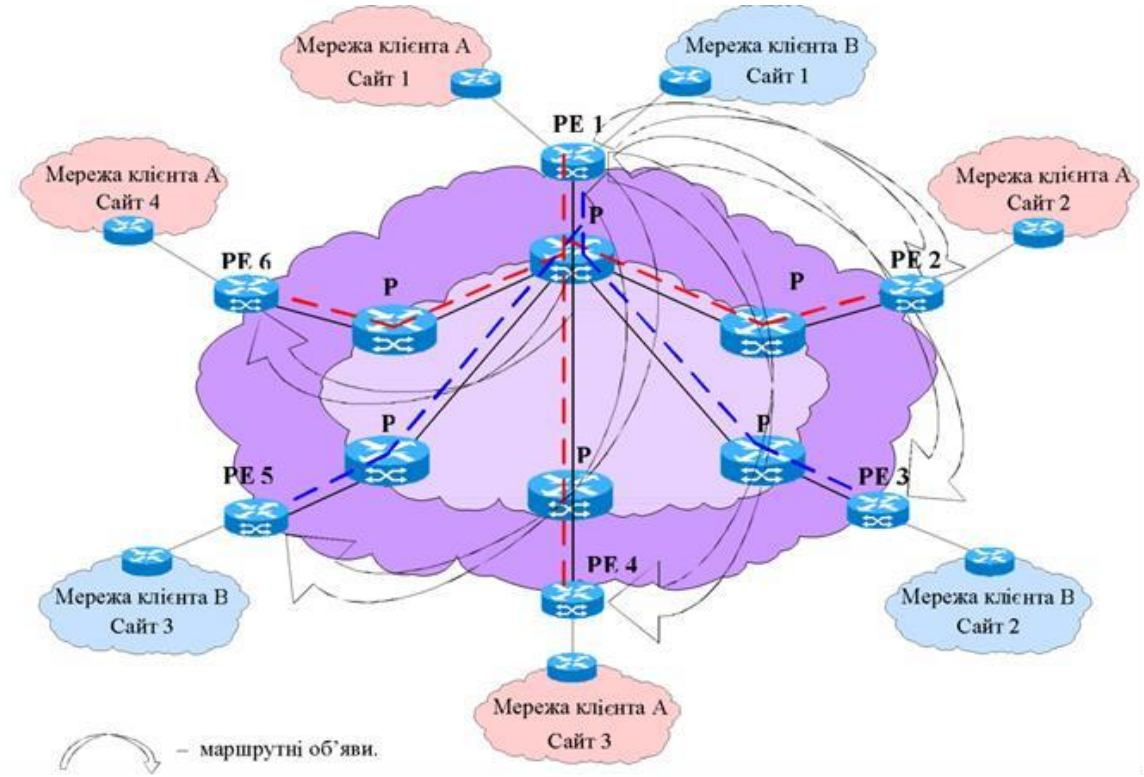


Рисунок 1.1. Архітектура з'єднань мереж провайдерів

Вимоги доступності з'єднання повинні встановлюватися організацією. Наприклад, якщо інтернет-з'єднання буде використовуватися тільки співробітниками для функцій, не критичних для бізнесу, то вимоги доступності будуть невисокими, і збій в електроживленні незначно вплине на справи організації. Якщо в організації планується створити сайт електронної комерції й вести бізнес головним чином через інтернет, то вимога доступності

є ключовою вимогою для успішної діяльності організації. У цьому випадку структура інтернет-з'єднання повинна містити в собі можливості по запобіганню збоїв і відновленню.

1.2 Метод одноканального доступу

Доступ в інтернет через один канал є найбільше широко використовуваною архітектурою інтернету. ISP надає організації один канал зв'язку з відповідною пропускною здатністю.

Як правило, провайдер пропонує підключити маршрутизатор і модуль обслуговування каналу (CSU) безпосередньо для кабелю, що з'єднує обладнання організації із центральним офісом (CO) телефонної компанії. У певному місці неподалік буде перебувати крапка присутності провайдеру (POP). З'єднання із провайдером фактично кінчається на найближчій крапці присутності. Навіть якщо POP розташована не на найближчому CO, локальне циклічне з'єднання зажадає проходження з'єднання через найближчий CO. З POP з'єднання проходить через мережу провайдеру в інтернет.

Якщо проаналізувати з'єднання на рисунку 1.2, стане видно, що існує набір точок, у яких збій обладнання викличе переривання роботи системи. Наприклад:

- може вийти з ладу маршрутизатор;
- може вийти з ладу модуль обслуговування каналу;
- локальне циклічне з'єднання може бути розірвано;
- центральний офіс може піддатися прояву погрози;
- крапка присутності провайдеру може дати збій.

Варто помітити, що не всі ці помилки рівновирогідні. Наприклад, маршрутизатор може вийти з ладу з набагато більшою ймовірністю, ніж імовірність завдання збитків центральному офісу організації. Однак у з'єднаннях збої виникають раптово, і це може викликати значний простій у

роботі. У наведеному списку також не враховані збої, які можуть відбутися усередині самого провайдеру. Такі збої час від часу відбуваються через погодні умови, ушкодження кабелів або впливу атак, спрямованих на відмову в обслуговуванні.

Рисунок 1.2. Стандартна архітектура з доступом через один канал

Беручи до уваги можливість потенційних збоїв, рекомендується використовувати дану архітектуру тільки в тому випадку, якщо інтернет-з'єднання не грають важливої ролі у веденні бізнесу.

1.3 Метод багатоканального доступу

Однієї з альтернатив одноканальному з'єднанню з одною потенційною крапкою збою в архітектурі з'єднання з одним провайдером, є використання декількох каналів з'єднання для зв'язку з одним провайдером. У даному відношенні різні провайдери пропонують різні послуги. Деякі називають цей підхід використанням "тіньових" з'єднань, інші ж використовують термін "надлишковий контур". У кожному разі метою даного підходячи є наявність

другого каналу зв'язку на випадок збою.

Провайдер може надавати доступ, захищений від збоїв, за допомогою настроювання надлишкового контурного з'єднання з тією же крапкою присутності. Надлишковий контур може містити в собі надлишковий маршрутизатор і CSU або може використовуватися один маршрутизатор. Два контури настроюються таким чином, що при виході з ладу головного контуру навантаження прийме на себе друге контурне з'єднання (рисунок 1.3.).

Рисунок 1.3. Доступ з використанням надлишкового контуру

Дана архітектура дозволяє обійти неполадки, що виникають на маршрутизаторі, модулі CSU, контурі з'єднання телефонної компанії із центральним офісом і встаткуванні провайдеру на іншому кінці з'єднання. Ці збої відбуваються найбільше часто. Однак даний підхід не запобігає менш часті, але більше серйозні збої, такі як ушкодження локального контуру, ушкодження самого центрального офісу організації або збій у крапці присутності провайдеру. Аналогічно, якщо на провайдеру відбудеться серйозний збій, то обслуговування також буде неможливо.

Одним з переваг даної архітектури є вартість реалізації надлишкового контуру. Більшість провайдерів надають надлишковий контур, і вартість цієї послуги менше, ніж вартість другого повного циклу.

Щоб забезпечити підвищений ступінь доступності й надійності, можна реалізувати друге з'єднання з іншою крапкою присутності провайдеру. У цьому випадку друге з'єднання може бути надлишковим або перебувати постійно в робочому стані.

Щоб забезпечити правильну роботу даної архітектури, на ISP повинен функціонувати протокол Border Gateway Protocol (BGP). BGP - це протокол маршрутизації, використовуваний для визначення маршрутів між об'єктами при використанні даних типів подвійних з'єднань. Необхідно ретельно підготувати BGP для роботи правильних політик маршрутизації.

Також варто помітити, що в даній архітектурі як і раніше є дві точки збою: локальний контур і центральний офіс організації. Ці точки збою не можна перебороти, якщо тільки в організації не є в наявності два з'єднання локального контуру (рисунок 1.4.).

Даний тип архітектури знижує число точок збою до однієї точки, який є сам провайдер. Якщо на провайдеру відбудеться відчутний збій у роботі, обслуговування організації може надаватися не в повному обсязі, або компанія зовсім може втратитися зв'язку.

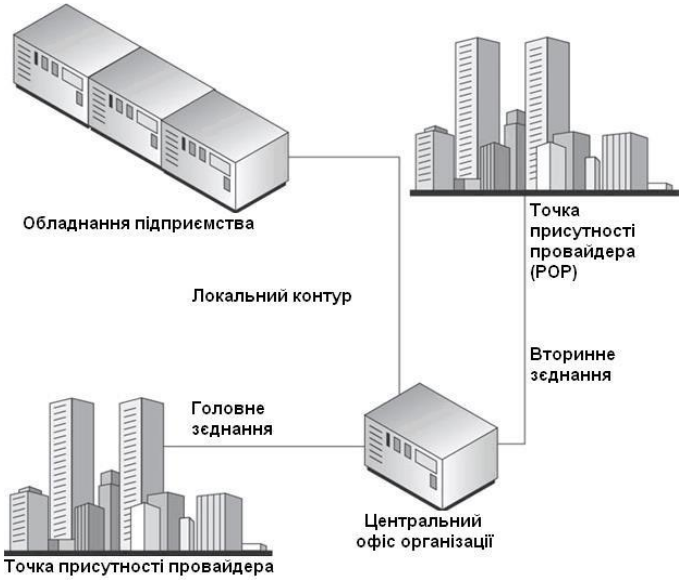


Рисунок 1.4. Кілька з'єднань із декількома крапками присутності провайдеру

1.4 Безперервна доступність з'єднань

При маршрутизації контурів від обладнання вашої організації до точок присутності провайдеру можуть як і раніше використовуватися ті самі фізичні кабелі. У цьому випадку проблема, що виникла з кабелем, приведе до виводу з ладу обох контурів. Щоб запобігти даній ситуації для вашої архітектури, при замовленні контурів з'єднань варто запитувати роздільну маршрутизацію. Після її реалізації необхідно запросити в провайдеру документацію зі схемою поточної фізичної маршрутизації контурів з'єднань між обладнанням вашої організації й двома крапками присутності провайдеру (рисунок 1.5.).

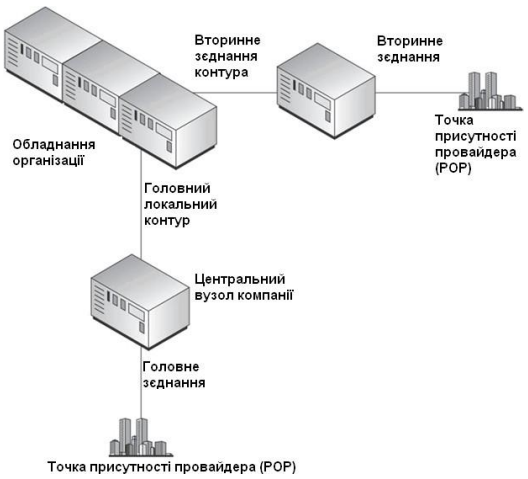


Рисунок 1.5. Кілька з'єднань через кілька локальних контурів

Беручи до уваги потенційні точки збою при використанні одного провайдеру, чому б не розглянути варіант із використанням декількох провайдерів замість одного? На перший погляд здається, що це відмінна ідея (і у випадку з деякими організаціями так і є), однак не варто думати, що даний варіант дозволить уникнути всіх неприємностей і ризиків, пов'язаних з інтернет-архітектурою. Використання декількох провайдерів (рис. 1.6.) при правильній реалізації може знизити ризик тривалого припинення надання послуг. Однак при виборі провайдерів і схеми адресації виникає ряд інших питань.

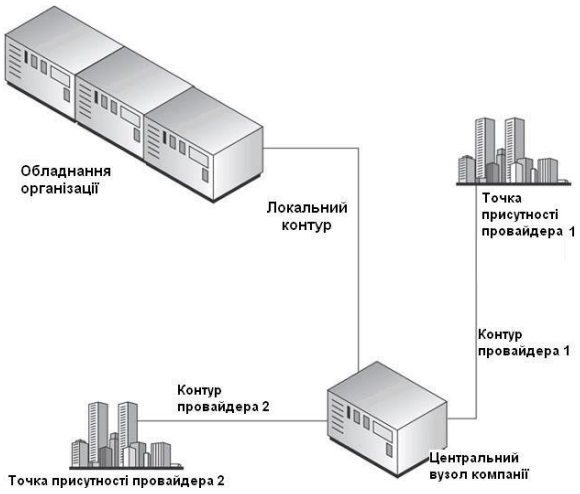


Рисунок 1.6. Архітектура інтернет-мережі з використанням декількох провайдерів

1.5 Фізична маршрутизація з'єднань

Складність реалізації архітектури, що використовує двох різних провайдерів, досить висока й вимагає значних знань і досвіду приваблюваних провайдерів. Однієї з областей, у якій тут повинні розбиратися фахівці, є BGP. BGP буде використовуватися для маршрутизації трафіка й повинен бути правильно настроєний у провайдерів і між ними.

Ще одним питанням, що впливає на вибір провайдеру, є фізична маршрутизація з'єднань. Локальний контур може як і раніше залишатися єдиною крапкою збою, якщо обладнання організації не забезпечує кілька з'єднань локального контуру. Якщо є присутнім тільки один локальний контур, то надмірність може бути реалізована за допомогою вибору провайдеру, що використовує бездротове з'єднання (рисунок 1.7.).

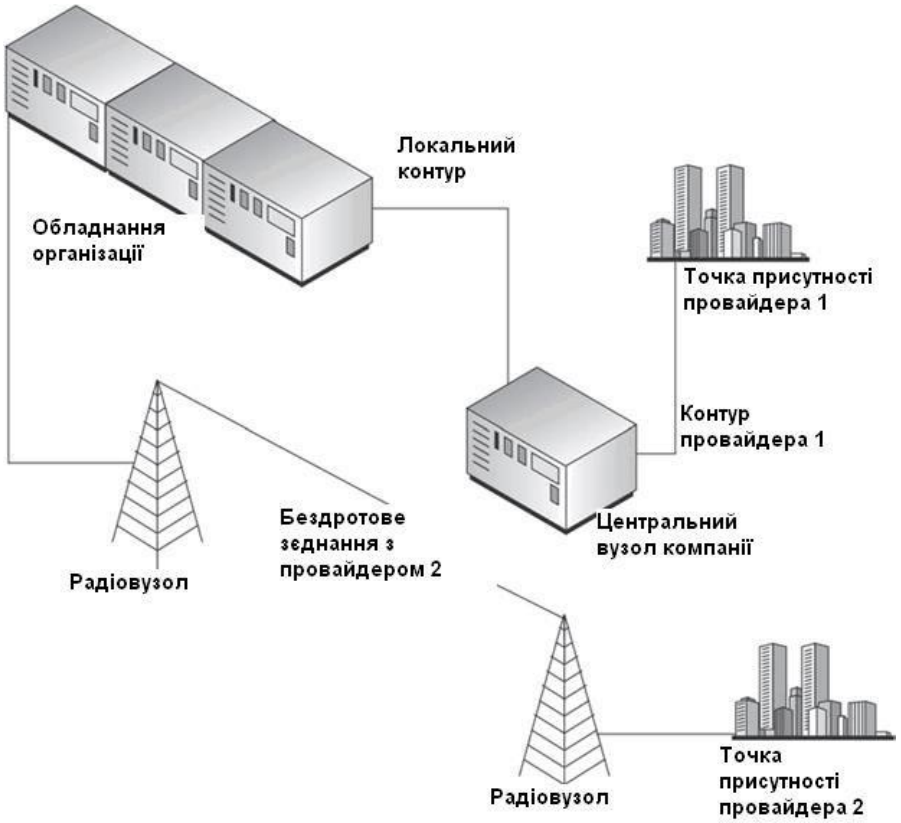


Рисунок 1.7. Використання провайдеру бездротового зв'язку для підвищення ступеня доступності

Використання бездротового каналу зв'язку не запобігає всіх можливих проблем, тому що внаслідок впливу погодних умов, вітри або птахів якість бездротового з'єднання може бути знижено, або з'єднання зовсім може бути перервано. Однак імовірність одноразового виходу з ладу бездротового каналу й звичайного каналу зв'язку із провайдером дуже мала.

При виборі провайдеру послуг бездротового зв'язку варто керуватися тими ж вимогами, що й при виборі звичайного постачальника послуг інтернету. Будь-який ISP повинен надавати угода про рівень надаваних послуг і підкріплювати ця угода усними рекомендаціями.

1.6 Формування адресного простору

Ще одним питанням, якім необхідно розглядати при роботі з декількома провайдерами, є проблема адресації. Як правило, при роботі з одним провайдером ISP привласнює адресний простір організації. ISP набудовує маршрутизацію таким чином, що трафік, спрямований в організацію, досягає її систем. ISP повідомляє маршрут для цих адрес іншим провайдерам, щоб трафік з будь-яких місць інтернету зміг досягти систем організації

Якщо в архітектурі задіяні кілька провайдерів, необхідно визначити, які будуть використовуватися адреси. Адреси можуть надаватися одним із двох провайдерів. У цьому випадку маршрутизація від одного ISP відбувається звичайним образом, а інший провайдер повинен підтвердити свою згоду на передачу маршруту до адресного простору, що належить першому провайдеру. Дана конфігурація вимагає ґрунтовного розуміння роботи протоколу BGP, щоб забезпечити правильну маршрутизацію трафіка.

Ще одним варіантом є придбання набору адрес самою організацією. У той час як цей підхід вирішує деякі проблеми, обидва провайдери повинні бути готові до поширення інформації про маршрути на адреси, які їм не належать. Цей підхід часто використовується в організаціях, де потрібен контроль над своїми власними адресами.

Нарешті, можна використовувати адреси обох провайдерів. При цьому деяким системам можуть бути надані адреси від одного провайдеру, а іншим системам - від іншого. Така архітектура не повністю усуває проблеми доступності, і її не слід використовувати у випадку, якщо можливо інший варіант.

1.7 Системи контролю доступу

У демілітаризованій зоні повинні бути присутнім зовнішні DNS-сервери. Якщо в організації планується містити власну DNS, те сервер DNS повинен бути доступний для запитів із зовнішнього середовища. DNS також є важливою частиною інфраструктури організації. Із цієї причини можна вибрати наявність надлишкових систем DNS або використовувати ISP у якості альтернативної DNS. При виборі останнього варіанта DNS провайдеру повинна буде здійснювати зональні переходи з DNS вашої організації. Жодній системі більше не буде потрібно виконувати ці переходи.

Якщо буде обране використання NTP, то в демілітаризованій зоні необхідна наявність головного локального NTP-Сервера. Внутрішні системи будуть запитувати головний NTP-Сервер для відновлення часу. Як альтернатива функції головного локального NTP-Сервера можуть виконуватися міжмережевим екраном.

Існує безліч архітектур демілітаризованих зон. Як і в більшості питань безпеки, мають місце переваги й недоліки кожної архітектури, і для кожної організації треба в окремому порядку здійснювати вибір конкретної архітектури DMZ. У трьох наступних розділах ми докладно розглянемо три найпоширеніші архітектури.

Демілітаризована зона прирівнюється до зовнішньої мережі, і в ній розташовуються системи, до яких буде здійснюватися доступ з інтернету. Тому що ці системи розміщені в зовнішній мережі, вони повністю відкриті для атак з інтернету. Щоб деяким чином знизити цей ризик, на маршрутизаторі

можна розмістити фільтри (рисунок 1.8.), щоб в DMZ проникав тільки трафік, зв'язаний зі службами, надаваними системами, що перебувають у демілітаризованій зоні.

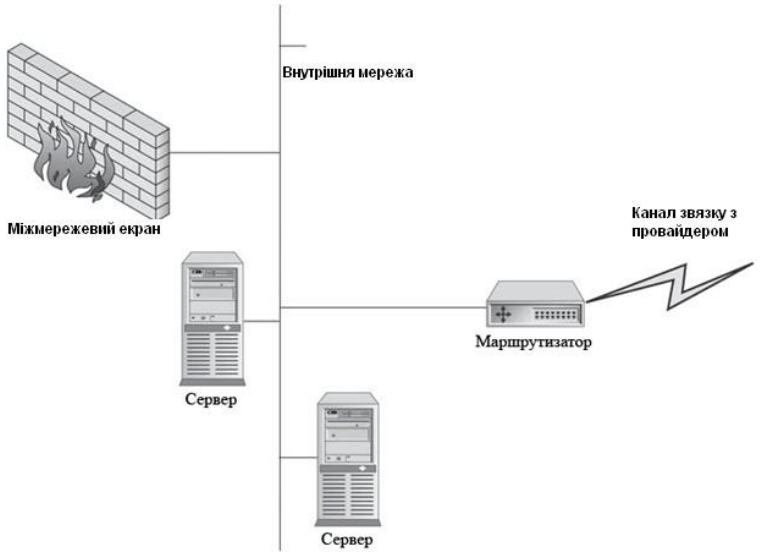


Рисунок 1.8. Архітектура DMZ з маршрутизатором і міжмережевим екраном

Ще одним способом зниження ризику є їхнє блокування таким чином, щоб єдиними службами, що функціонують у кожній системі, були тільки ті, які надаються в демілітаризованій зоні. Це означає, що на веб-сервері повинен працювати тільки веб-сервер. Telnet, FTP, а інші служби повинні бути відключені. У системи варто встановлювати самі останні відновлення й уважно стежити за їхньою роботою.

У багатьох випадках маршрутизатор належить провайдеру й управляється ім. Якщо це так, можуть виникнути труднощі зі зміною фільтрів або їхнім правильним настроюванням. Якщо власником і суб'єктом управління маршрутизатора є організація-клієнт, то ця проблема зводиться до мінімуму. Однак варто мати на увазі, що на маршрутизаторах часто використовуються елементи керування, що працюють із командного рядка, і для правильної роботи фільтрів їх необхідно коректно набудовувати й розташовувати в правильному порядку.

Для створення демілітаризованої зони може використовуватися один міжмережевий екран. При цьому DMZ відділяється від зовнішньої мережі. Зовнішня мережа формується маршрутизатором ISP і маршрутизатором.

DMZ реалізується на третьому інтерфейсі міжмережевого екрана. Міжмережевий екран самостійно контролює доступ до демілітаризованої зони (рисунок 1.9).

Рисунок 1.9. Архітектура демілітаризованої зони з одним міжмережевим екраном

Третя архітектура демілітаризованої зони зображена на рисунку 1.10. Тут використовуються два міжмережевих екрани для відділення DMZ від зовнішньої й внутрішньої мережі. Зовнішня мережа як і раніше перебуває між

маршрутизатором провайдеру й першим міжмережевим екраном. Демілітаризована зона тепер розташовується між міжмережевими екранами 1 і 2. Міжмережевий екран 1 настроєний на дозвіл проходження всього трафіка DMZ, а також усього внутрішнього трафіка. Конфігурація міжмережевого екрана 2 більше обмежувальна й передбачає тільки пропуск вихідного трафіка в інтернет.

Така конфігурація підвищує загальний рівень безпеки, тому що одна єдина атака навряд чи приведе до злочинного впливу на обоє міжмережевих екранів. За аналогією із системами, що мають один міжмережевий екран, системи DMZ захищені від інтернету міжмережевим екраном 1.

Пари міжмережевих екранів підвищує вартість архітектури й вимагає додаткових зусиль по керуванню й настроюванню.

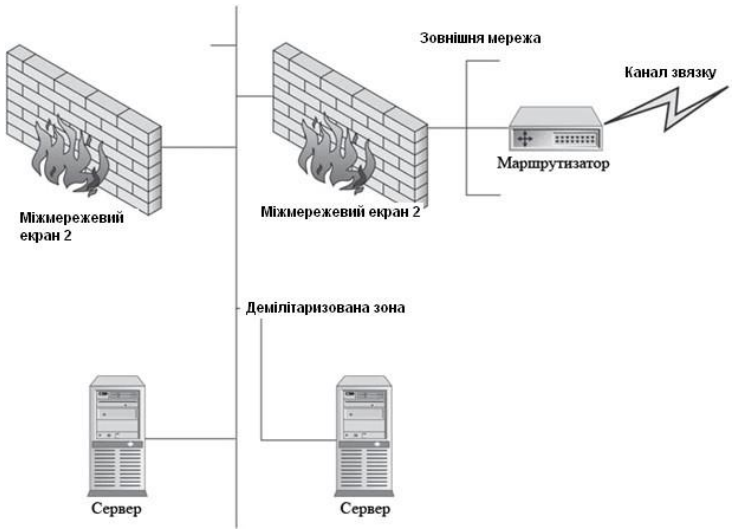


Рисунок 1.10. Архітектура демілітаризованої зони із двома міжмережевими екранами

2 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

2.1 Фактори впливу на безпеку інформації

На безпеку інформації, в основному, впливають людський та технічний фактори. До людського фактору відносять соціальну інженерію. Мається на увазі такі поняття, як фішинг, телефонний фішинг, індивідуальні підходи та ін.

До технічного фактору відноситься рівень захищеності мережі. Саме він впливає найбільше. Розглянемо метод захисту на прикладі встановлення спеціальних серверів.

2.2 Віртуальні з’єднання кешуючих серверів

Proxy-Сервери, що використовуються для з’єднань простіші в конфігурації. Вони функціонують як «передатна ланка» між прикладним і транспортним рівнями, контролюючи обмін підтвердженнями TCP між клієнтами, що заслуговують довіри, або серверами й не заслуговують довірою хостами. Proxy-сервер як і раніше є посередником між двома сторонами, але тепер він установлює між ними віртуальне з’єднання.

При використанні proxy-серверів для з’єднань програмне забезпечення більше не потрібно конфігурувати на кожному клієнті. Наприклад, у випадку Proxy Server від Microsoft після установки програмного забезпечення WinSock Proxy на клієнтський комп’ютер - а це однократна процедура - клієнтське програмне забезпечення, таке, як Windows Media Player, Internet Relay Chat (IRC) або telnet, буде функціонувати так, ніби воно мало пряме з’єднання з Internet. SOCKS була запропонована в 1990 році й тепер досягла п’ятої версії (див. RFC 1928). Вона являє собою не залежний від платформи стандарт для доступу до посередників для з’єднань. Доступ може здійснюватися або через спеціальний «SOCKS» додаток із клієнтського комп’ютера, або з кожного додатка, що виконується на комп’ютері, на якому встановлене передатна ланка SOCKS.

Крім стандартизації SOCKS має й інші переваги. Версія 5 підтримує ідентифікацію як за допомогою імен/паролів (RFC 1929), так і на базі API (RFC 1961). Крім того, вона підтримує шифрування за допомогою відкритих і особистих ключів.

Історично, створення посередників для сервісів на базі UDP являє собою досить важке завдання, тому що даний протокол не припускає встановлення з'єднання: кожний пакет передається як окреме повідомлення. SOCKS 5 здатний вирішити й цю проблему за допомогою встановлення з'єднання TCP з наступною передачею по ньому даних UDP.

Нарешті, функції брандмауерів з фільтрацією пакетів, посередників для додатків і посередників для з'єднань об'єднані в брандмауерах з контекстною перевіркою. Ці пристрої можуть перехоплювати й аналізувати всі минаючі через них пакети з використанням алгоритмів для розпізнавання даних прикладного рівня. На відміну від посередників для додатків, брандмауери з контекстною перевіркою не змінюють клієнт-серверної моделі з метою аналізу даних.

2.3 Ієрархія мережі кешуючих серверів

Кешування теоретично не є обов'язковим для PROXY серверыв, кешування тісно пов'язане з proxy-серверами Web з того моменту, коли вони були вперше описані на Міжнародній конференції по World Wide Web (Женева, квітень1994 р.). Базова функція кешування proxy-сервера працює багато в чому аналогічно убудованій у браузери Web за тим відмінністю, що вміст кешу proxy-сервера доступний для безлічі користувачів. Щораз, коли який-небудь користувач локальної мережі запитує сторінку з Internet, вона зберігається локально, що значно прискорює швидкість доступу (див. рисунок 2.1. [5, с. 243]).

Рисунок 2.1. Функції кешування проксі серверів

Деякі proxy-сервери пропонують кешування що випереджає, тобто вони завантажують у кеш зображення й інші об'єкти на сторінці Web до того, як браузер їх запросить. Кеш може заповнюватися заздалегідь за допомогою механізму, відомого як «множник останніх змін». При цьому proxy-сервер аналізує дати створення часто запитуваних сторінок, прогнозує ймовірний строк зміни й запитує їх по його настанні. І звичайно, proxy-сервери дозволяють адміністраторам проводити планове пакетне копіювання сторінок Web у будь-яку годину дня й ночі, коли обсяг мережного трафіку невеликий (рисунок 2.2. [5, ст.245]).

Рисунок 2.2. Протокол кешування у рівноправних, і вищестоящих кешей

Деякі proxy-сервери мають таку додаткову функцію, як зворотне кешування. При цьому кеш-сервери зберігають не тільки сторінки з Internet

для локальних користувачів, але й локальні сторінки для користувачів в Internet.

2.4 Використання розширень Cache-Control

При розробці веб-сайту частота зміни сторінок сильно коливається. Деякі сторінки будуть змінюватися щодня, деякі не будуть змінюватися із самого моменту свого створення. Для того, щоб дозволити менеджерові веб-сайту регулювати частоту, з якої браузер повинен запитувати HTTP-сервер про зміни в ресурсі, в Internet Explorer 5 представлене 2 розширення HTTP-заголовка Cache-Control: pre-check і post-check. Вводячи ці розширення, Internet Explorer зменшує мережний трафік, тому що відправляє менше запитів до сервера. Додатково Internet Explorer поліпшує користувальницьке сприйняття (*user experience*), коли відображає ресурси з кеша й перевіряє відновлення у фоновому режимі після спеціального інтервалу.

Розширення post-check і pre-check для Cache-control визначені в такий спосіб:

- post-check

Визначає інтервал часу в секундах, після якого ресурс повинен бути перевірений на актуальність. Ця перевірка може бути виконана й після того, як користувач завантажить сторінку з кеша, але при наступному завантаженні він обов’язково повинен одержати оновлену версію.

- pre-check

Визначає інтервал часу в секундах, після якого перевірка актуальності ресурсу повинна бути зроблена перед його відображенням для користувача (рисунок 2.3. [5, ст.93]).

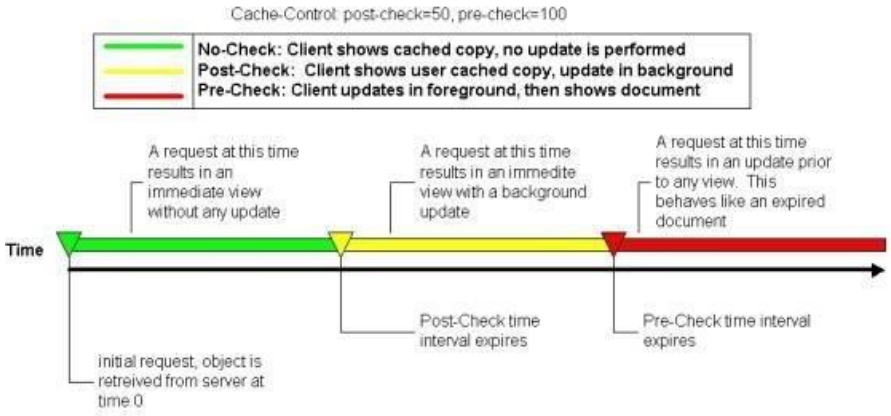


Рисунок 2.3. Послідовність запросу даних з кешу

Коли до браузера надходить запит на відкриття ресурсу, що перебуває в кеші, при цьому кеш містить розширення Cache-Control (відправлені із сервера як частина заголовка HTTP-відповіді), браузер використовує ці розширення й наступну логіку для одержання останньої версії сторінки із сервера.

- Якщо ще не закінчився інтервал часу post-check, то просто відображається сторінка з кеша.
- Якщо з моменту останнього запиту сторінки пройшов час, що лежить між інтервалами post-check і pre-check, то відображається сторінка з кеша. При цьому у фоновому режимі запитується HTTP-сервер, чи змінювалася сторінка з моменту останнього запиту браузером. Якщо сторінка змінилася, то вона запитується й зберігається в кеші
- Якщо вже минув час, відзначений інтервалом pre-check, то при запиті сторінки користувачем спочатку запитаємо в HTTP-Сервера, чи змінилася сторінка із часу її останнього завантаження браузером. Якщо сторінка змінилася, вона завантажується й відображається оновлена версію.

Помітимо, що кнопка «Обновити» (включаючи клавішу F5) не запускає даний механізм, тому що «Обновити» завжди відправляє на сервер запит if-modified-since. Однак, всі посилання будуть відкриватися за допомогою описаної вище логіки.

У наступному прикладі сервер повідомляє Internet Explorer, що зміст не буде змінюватися протягом 1 години (pre-check=3600) і що його можна завантажувати прямо з локального кеша. У тому же випадку, якщо сторінка все- таки зміниться, якщо користувач запросить її по витіканню 15 хвилин, Internet Explorer повинен відобразити локальний кеш, але при цьому у фоновому режимі перевірити, чи є збережена копія сторінки актуальної, і по необхідності завантажити її із сервера.

2.5 Алгоритм взаємодії кешей

В ієрархічній (або багатозв’язній) структурі кожний кеш встановлює стосунки з іншим кешем. Відносини бувають двох типів: підлеглі й рівноправні. При відсутності запитаного об’єкта кеш надсилає запит ICP про наявність необхідного об’єкта в якого-небудь із рівноправних кешей. У випадку його відсутності й у рівноправних кешей запит направляється вищестоящому серверу. Типова ієрархія кешей показана на рисунку 2.2.

Зв’язуючи кеш-сервери між собою, ICP породжує й деякі проблеми. Одна з них полягає в тому, що запити ICP створюють сторонній мережний трафік.

Чим більше кеш-серверів у групі, тим більше трафік. Як наслідок, масштабованість такого рішення обмежена.

Інша проблема з ICP полягає в тому, що згодом такі групи серверів виявляються надлишковими. В остаточному підсумку в кожного із серверів у групі з'являються свої копії часто запитуваних URL. Із цієї причини ICP поступово витісняється протоколом маршрутизації для групи кеш-серверів (Cache Array Routing Protocol, CARP), запропонованим Microsoft.

У випадку CARP кеш-сервери відслідковуються за допомогою «списку членства в групі», автоматично обновлюваного за допомогою функції Time-to- Live (TTL), що регулярно перевіряє дієздатність активних серверів. Потім за допомогою алгоритму хешування визначається, хто зі членів групи повинен обслуговувати запит до конкретного URL.

Кеш-сервери довгий час розглядалися як корисні безкоштовні додатки до proxy-серверів. Тепер, коли навантаження на Internet незмірно зросло, і все більше число клієнтів має високошвидкісні з'єднання, терміни «кеш-сервер» і «proxy-сервер» навряд чи можна як і раніше використовувати взаємозамінно.

Proxy-Сервери будуть продовжувати пропонувати кешування як одну зі своїх функцій. Однак зростаючий попит на спеціалізоване кешування означає, що кеш-сервери всі частіше будуть розглядатися як окремі продукти. Наприклад, CacheQube від Cobalt Networks установлюється між локальною мережею й маршрутизатором для забезпечення прозорого кешування. Streaming Media Cache від Inktomi і MediaMall від InfoLibria призначені спеціально для кешування потокового аудіо й відео.

3 ОБҐРУНТУВАННЯ ВИБОРУ КОМПОНЕНТІВ СИСТЕМИ

3.1 Центральний маршрутизатор

У цей час, у зв’язку з ростом кількості і якості послуг, надаваних інтернет-провайдерами, значно підвищуються вимоги до пристроїв маршрутизації вузла провайдеру Інтернет, причому як з погляду продуктивності пристроїв, так і, у першу чергу, їхньої функціональності.

Підривний ріст числа користувачів і обсягу даних, переданих по мережі Інтернет, привели до того, що недоліку пропозицій пристроїв маршрутизації на телекомунікаційному ринку явно не спостерігається. Тим більшу проблему викликає, найчастіше, для провайдеру вибір оптимального пристрою для здійснення функцій маршрутизації.

До числа вимог, пропонованих до центрального маршрутизатора вузла, можна віднести безумовно необхідні, такі як підтримка протоколів BGP-4 і OSPF, достатній обсяг оперативної пам’яті для розміщення повних таблиць маршрутизації. Однак сьогодні на перший план виходять розширені вимоги до продуктивності, набору додаткових послуг і їхньої реалізації. Тут у першу чергу можна відзначити наступне:

- Сьогодні користувачі Інтернет вимагають не просто доступу до глобальної мережі, а доступу в сполученні з додатковими послугами, такими, як віртуальні частки мережі (VPN), рішення з використанням угод про якість послуги (Service Level Agreement, SLA) із провайдером, причому бажано з використанням єдиної платформи й з мінімальними витратами.
- Реальна продуктивність пристрою, тобто швидкість маршрутизації пакетів у реальних умовах мережного оточення (із включенням

пакетних фільтрів, протоколів підтримки VPN, функцій контролю якості, а, можливо, і апаратної шифрації), а не в режимі "fast switching", повинна бути достатньої для задоволення вимог провайдеру й мати достатній запас із урахуванням перспектив розвитку. Величина реальної продуктивності багатьма виробниками обладнання найчастіше замовчується з маркетингових міркуваннях.

В умовах зрослої конкуренції особливу роль грають економічні питання реалізації послуг, а тут головну роль грають параметри ціна/продуктивність (або ціна/якість) маршрутизатора, а також такі параметри, як компактність і простота в керуванні й конфігурації. Тут варто відзначити, що в цей час існує тенденція до спеціалізації пристроїв, а часи «універсальних маршрутизаторів», «однаково добре» застосовних для використання як магістральний маршрутизатор, крайового маршрутизатора, а також комутатора X.25 і SNA, ідуть у минуле саме через громіздкість, проблем керування й низкою економічної ефективності таких рішень.

3.2 Рішення Lucent Technologies

Виходячи з наведених вище вимог, як центральний маршрутизатор розширеного вузла Інтернет компанії АБВ, пропонується використовувати високопродуктивний мультисервісний маршрутизатор Access Point® 1000.

Access Point® 1000 сполучить у собі високопродуктивний маршрутизатор, передові технології контролю й керування якістю послуг (QoS), повний набір стандартизованих опцій безпеки для створення VPN і унікальну систему фільтрації пакетів. Інтегровані можливості керування трафіком і моніторингу забезпечують повний контроль якості послуг і надання детальної статистики для кожного із клієнтів провайдеру. Будучи системою з можливістю повного керування по SNMP, Access Point® 1000 легко інтегрується, якщо це необхідно, з існуючими системами керування й службами back-office. Access

Point® 1000 включає повну підтримку стандартів RIP, BGP-4, OSPF і статичної маршрутизації.

Access Point® 1000 використовує передову архітектуру, що уможливлює високошвидкісну комутацію пакетів при «включених» додаткових сервісах у дуже твердому режимі. При швидкості комутації пакетів до 450Мбит/с, у тому числі в режимі шифрації 3DES — до 155Мбіт/с, Access Point® 1000 встановлює новий стандарт для мультисервісних IP-маршрутизаторів.

Для організації доступу клієнтів АБВ до глобальних мереж ми пропонуємо використовувати сервера доступу MAX 6000, пристрою із сімейства MAX, що використовують більшість найбільших Інтернет-провайдерів в усьому світі. Поєднуючи функції маршрутизатора, термінального сервера, комутатора ISDN і концентратора Frame Relay, MAX є ідеальним рішенням доступу для глобальних мереж. Кожна з моделей MAX може використовуватися для організації вилученої роботи, передачі файлів і електронної пошти між вилученими офісами, для консолідації трафіку Інтернет. Операційна система TAOS (True Access Operating System), убудована в усі продукти MAX, надає кращий у галузі комплекс функцій доступу ГВС. ОС TAOS також є платформою для створення корпоративних і Інтернет-Додатків наступного покоління, таких як передача голосу в реальному часі по IP. Ця апаратна платформа протестована в умовах найбільших у світі рішень віддаленого доступу.

3.3 Підтримка платформи MAX 6000

Основною платформою для MultiVoice Gateway є MAX 6000. MAX 6000 являє собою нове покоління комутаторів доступу до глобальних мереж фірми Lucent, які забезпечують інтернет-провайдерам, мережним провайдерам і великим корпораціям поліпшену продуктивність і масштабованість, необхідні для існуючих у цей час і майбутні сервіси, включаючи передачу голосу по IP-мережах.

Керуючий DSP взаємодіє з основним процесором шасі MAX на материнській платі для зв'язку з мережею IP і виконання інших керуючих функцій. Після того, як голос оцифрований і стислий, він обробляється основним процесором для передачі по IP-Мережі. Цю архітектуру ілюструє наступний рисунок 3.1:

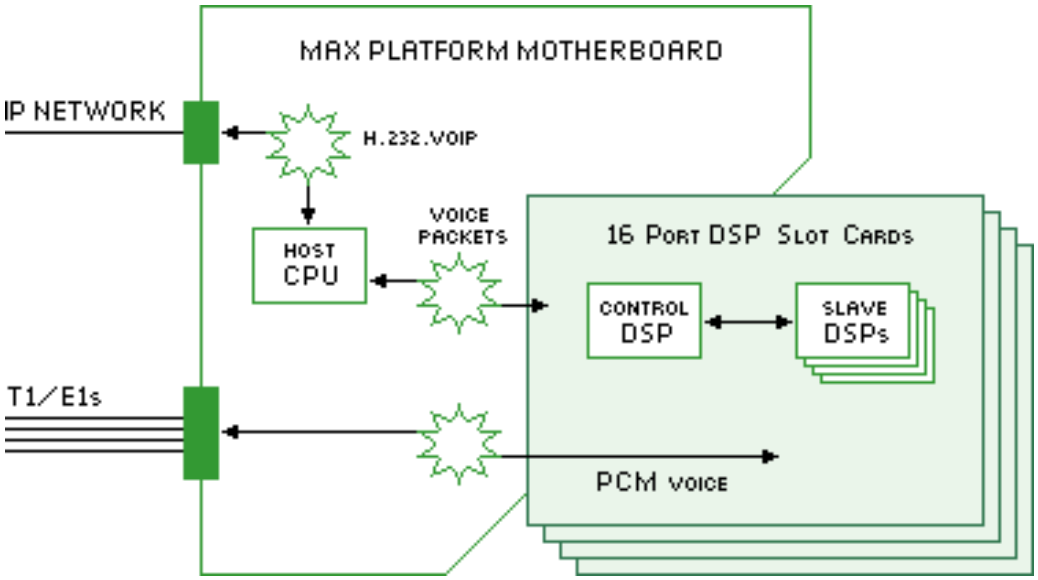


Рисунок 3.1. Платформа MAX 600

Тому що MultiVoice Access Manager являє собою стандартний додаток Windows NT, мережа MultiVoice може використовувати будь-які технології підвищення продуктивності й надійності, реалізовані для цієї операційної системи. Нижче на рисунку 3.2 [7, ст. 432] показана типова схема мережі для надання послуг Інтернет-Телефонії.

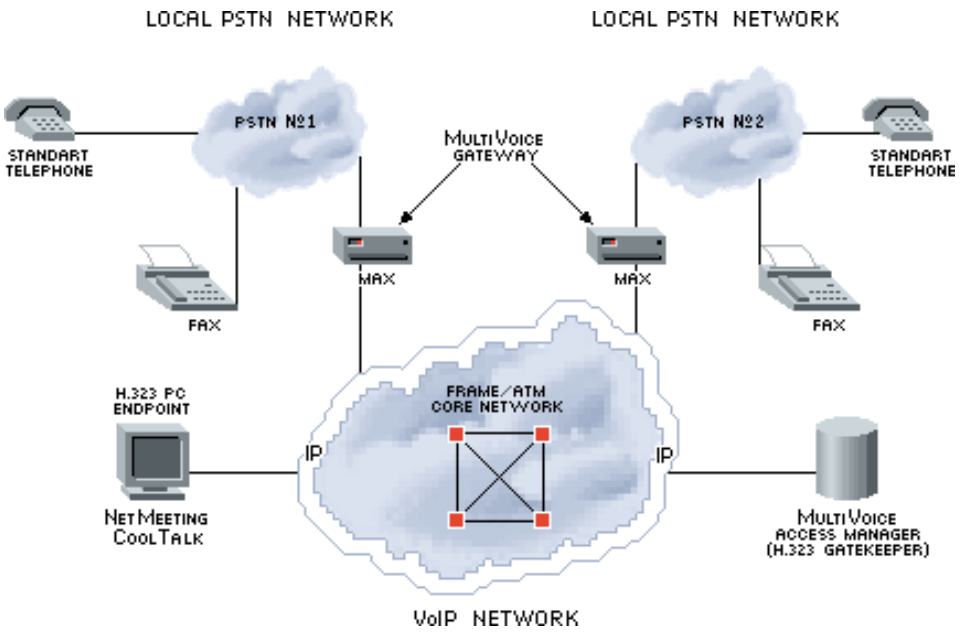


Рисунок 3.2. Типова схема для надання послуг інтернет-телефонії.

Таким чином, надане нами рішення на основі MAX6000 повністю задовольняє вимогам з погляду продуктивності, надійності, масштабованості й керованості вузла. Використання єдиної апаратної платформи MAX6000 для надання послуг доступу, що комутується, і IP телефонії дозволяє безболісно розвивати функціональність мережі, не розширюючи номенклатуру використовуваного встаткування.

3.4 Система керування й моніторингу

Navis® — це комплекс додатків мережного керування й керування послугами, що дозволяє постачальникам послуг пропонувати своїм клієнтам нові, необхідні їм послуги. У числі типових прикладів: віртуальні частки мережі (ВЧМ), оптовий продаж портів і смуги пропущення, гнучке керування смугою пропущення й мережею клієнта, включаючи докладні звіти на базі Web і верифікацію угод про рівень сервісу. Керуючі додатки Navis® максимізують інвестиції в устаткування доступу ГВС за рахунок спрощення

виробничих процесів, що дозволяє знизити витрати, і за рахунок появи можливості швидкого розгортання нових конкурентоспроможних послуг.

Всі продукти лінії Navis® використовують інтуїтивний графічний інтерфейс, доступ на базі Web і інтелектуальну обробку інформації, що дозволяє мережним адміністраторам зосередитися безпосередньо на питаннях керування мережею і її елементами.

NavisAccess - наскрізне рішення керування мережею й послугами різних постачальників, що функціонує на рівні віддаленого доступу й що дозволяє візуалізувати всю мережу як єдине кероване ціле. Велика база даних пристроїв, що входить до складу Navis® Access, дозволяє використовувати його не тільки для керування мережею, що складається з устаткування Lucent, але й включає обладнання інших фірм (наприклад 3COM, Cisco). Є автономна версія, що не вимагає наявності OpenView (рисунок 3.3).

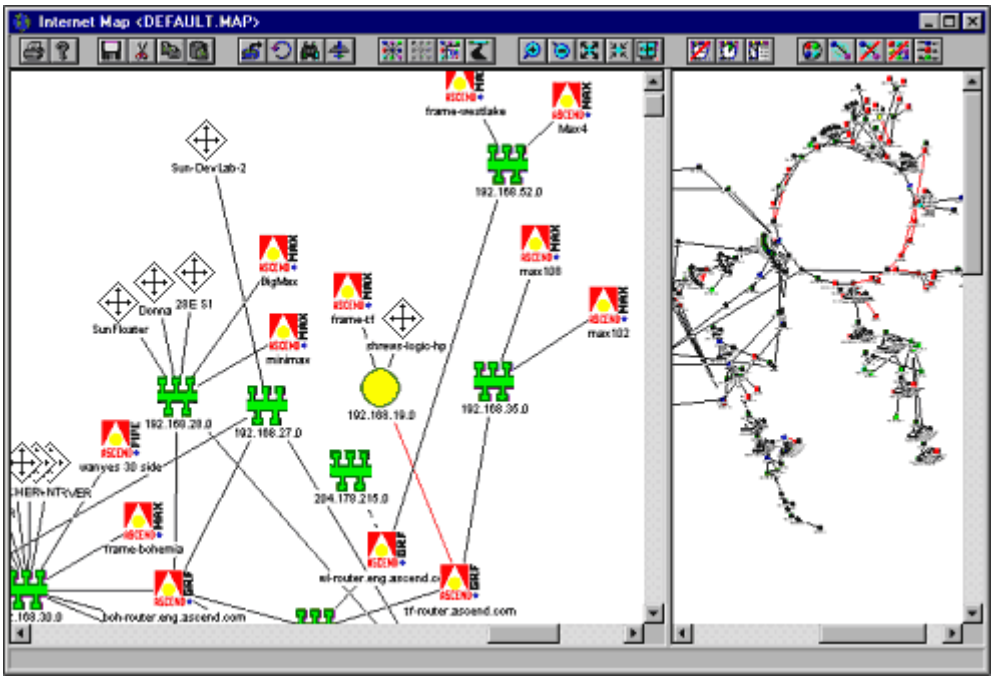


Рисунок 3.3. Графічний інтерфейс NavisConnect.

NavisConnect - графічний конфігураційний інтерфейс для апаратури MAX, MAX TNT і Pipeline 220. Він поставляється безкоштовно із цими й

іншими підтримуваними платформами Lucent TAGS. NavisConnect забезпечує простий і ефективний спосіб конфігурації пристроїв і систем, заміняючи традиційний інтерфейс telnet/консоль комбінацією майстрів, віконних конфігураторів і довідкової системи. Відповідно, він дозволяє адміністраторові зосередитися на розгортанні рішень доступу ГВМ, надаючи найбільш знайомий інтерфейс.

Успіх Інтернет-провайдеру багато в чому залежить від його здатності справлятися із щоденним ростом трафіку, крім того, робити це без зниження продуктивності. Тому, провайдери будь-якого рівня рано або пізно приходять до необхідності використання спеціалізованих серверів, які кешують уміст web-сторінок. Кешування дозволяє провайдеру побудувати надійну інфраструктуру, здатну справлятися з ростом трафіку без необхідності нарощування пропускної здатності зовнішніх каналів (каналів, що з'єднують провайдеру з іншими провайдерами Інтернет або із крапками обміну Інтернет-трафіком).

У результаті установки кешуючого обладнання провайдер очікує одержати наступні переваги:

- Помітне поліпшення продуктивності.
- Динамічна масштабованість.
- Спрощене адміністрування.

3.5 Рішення Lucent Technologies IPWorX

Для того щоб відповідати всім очікуванням провайдеру Інтернет послуг, виробник кешуючих серверів повинен мати великий досвід у мережних технологіях, таких як маршрутизація, комутація, керування мережею й взаємодія комунікаційних систем. Lucent Technologies використовувала всі свої знання в області мережних технологій при створенні комплексу продуктів

IPWorX, службовців збільшенню продуктивності вузлів Інтернет-Провайдерів.

Рішення IPWorX працює за принципом «розділяй і керуй», його функціональність розподілена між трьома різними компонентами, які повністю сумісні з існуючими в провайдеру серверами, комутаторами, маршрутизаторами й міжмережевими екранами. Взаємодія цих трьох компонентів показано на рисунок 3.4:

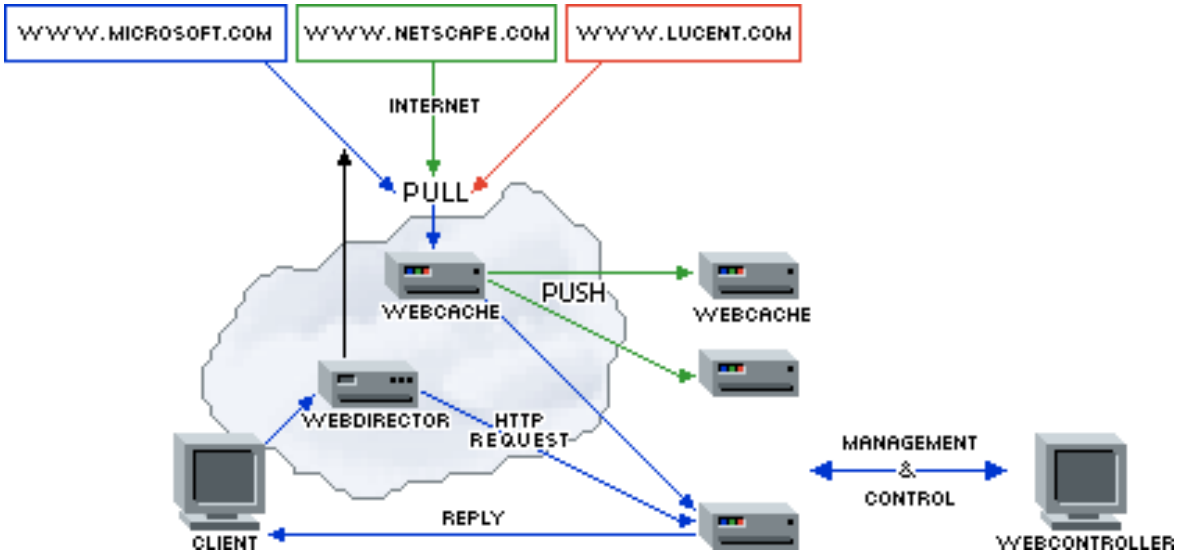


Рисунок 3.4. Система IPWorX

- WebCache - кеш-сервер, завантажує, зберігає (18-36 Гбайт на один кеш- сервер) і обслуговує вміст сховища web-об’єктів. Кеш-сервери можна поєднувати в ієрархію серверів, один їх яким стає «активним» кеш- сервером. Цей сервер здійснює активне керування web-об’єктами, що зберігаються у всій ієрархії.
- WebDirector - це комбінований комутатор, що працює на 4-ом і 7-ом рівнях моделі OSI і трафік-менеджер, що здійснює високошвидкісний розподіл web-трафіку й комутацію з «швидкістю проведення». WebDirector динамічно комутує кешовану

інформацію між кеш- серверами WebCache, для балансування навантаження розподіляє запити від користувачів між кеш-серверами, і перенаправляє некешуємі запити безпосередньо на web-сервери, в обхід кеш-серверів.

- WebController - це станція управління комплексу IPWorX. Вона обчислює параметри необхідні для перерозподілу навантаження, збирає статистику продуктивності, здійснює моніторинг розміщення найбільш запитаних web-об’єктів між кеш-серверами й здійснює оптимізацію зв’язку між всіма компонентами.

Завдяки унікальному сполученню сучасних алгоритмів кешування web-інформації й оптимізації продуктивності роботи серверів, що входять у комплекс, IPWorX є фундаментом інфраструктури для створення нових сервісів у провайдеру.

Забезпечення безпеки комп’ютерної й мережний інфраструктури в будь-якій організації, незалежно від її характеру діяльності, у цей час приділяється велику увагу. Особливо ретельний підхід до створення системи безпеки потрібно в тому випадку, якщо організація є оператором зв’язку або провайдером Інтернет-Послуг, тому що в цьому випадку ймовірність спроб атак на життєво важливі ресурси компанії зростає.

Екран LMF є промисловим продуктом рівня оператора, розробленим для задоволення запитів найбільш вимогливих клієнтів. Він пройшов випробування на сумісність із іншими продуктами Lucent, щоб гарантувати нашим клієнтам таку ж сумісність у їхніх мережах.

Він виконує дві функції:

- Перешкоджає несанкціонованому доступу до мережі.
- Перешкоджає несанкціонованому виходу інформації з мережі.

Безпека повинна підтримуватися на відповідному рівні для того, щоб відбивати атаки досвідчених «зломщиків» ззовні, а також перешкоджати несанкціонованому доступу власного персоналу до інформації й систем, які управляють політикою безпеки компанії.

Вважається, що система виявлення несанкціонованого доступу в мережу є основним компонентом системи захисту мережі будь-якої організації. Вона забезпечує дві важливі функції. По-перше, якщо відбудеться проникнення через міжмережевий екран через помилку у встановленні правил захисту, сканер RealSecure визначає сигнатуру атаки, генеруему зловмисником, що робить спробу завдати шкоди внутрішнім ресурсам. Вона потім записує сеанс зв’язку, від’єднує зловмисника від мережі й посилає сигнал тривоги серверу SMS.

4 СТРАТЕГІЇ КЕШУВАННЯ WEB-СЕРВІСІВ

4.1 Вимоги до продуктивності серверів XML

Незважаючи на зростання швидкостей роботи процесорів і мереж, продуктивність залишається основною турботою розроблювачів додатків. А виходить, незалежно від того, чи розроблюється Web-Сервіс на основі XML (XML Web Service).

Web-Сервіс дозволяє споживачам знаходити якусь статтю, а потім скачувати її. У цьому випадку справедливо припустити, що слідом за успішним пошуком статті піде запит на її скачування. Web-Сервіс може завчасно почати потенційно тривалий процес завантаження статті (з файлу або бази даних), і тоді до моменту надходження запиту на скачування статті інформація буде отримана (рисунок 4.1.).

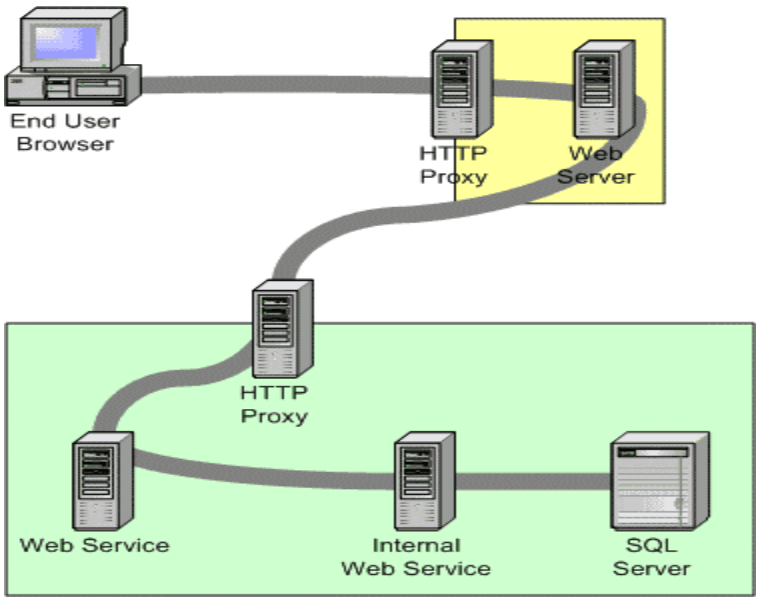


Рисунок 4.1. Можливі варіанти кешування сценаріїв роботи Web-Сервісу XML

Як видно, кінцевий користувач звертається до сайту (він показаний у жовтому прямокутнику), не знаючи, що цей сайт перебуває за HTTP-проксі. Потім Web-Сервер посилає SOAP-запит до Web-Сервісу в іншій організації (у зеленому прямокутнику). SOAP-Запит теж проходить через HTTP-проксі. Після цього перший Web-Сервіс переправляє запит іншому, внутрішньому Web- Сервісу, що запитує необхідні дані в Microsoft® SQL Server і нарешті повертає відповідь. SQL-дані використовуються при підготовці відповіді від внутрішнього Web-Сервісу, а на основі його відповіді створюється відповідь від першого Web-Сервісу. На сайті з відповіді Web-Сервісу формується HTML- сторінка, що і вертається браузеру кінцевого користувача.

Запит і відповідь проходять через безліч проксі-серверів і маршрутизаторів. У цьому сценарії дані керуються - на кожному етапі. SQL-сервер може кешувати результати запиту до сервісу, внутрішній Web-Сервіс - результати SQL-Запиту, перший Web-Сервіс - результати внутрішнього Web-Сервісу (так само як і HTTP-прокси в "зеленій" організації), Web-Сервер - відповідь Web-Сервісу, проксі-сервер в "жовтій" організації - відповідь Web-Сервера, а браузер кінцевого користувача - HTML-сторінку.

4.2 Актуальність збереженої в кеші інформації

При розробці стратегії кешування необхідно відповісти на одне з найважливіших питань: коли видаляти дані з кешу. Іноді це зробити дуже просто, тому що процес, що обновляє дані, запускається через регулярні проміжки часу. Однак в інших ситуаціях дані обновляються через довільні інтервали. Тоді треба з’ясувати оптимальний строк, після закінчення якого варто обновляти кеш, дотримуючи балансу між ризиком повернення з кешу застарілих даних і ростом продуктивності, що досягається за рахунок застосування кешу. Визначивши такий інтервал, потрібно додати цю інформацію в дані, щоб кешуючі системи могли відповідно оновлювати вміст кешей.

Убудовані механізми кешування звичайно містять у собі засоби для завдання строків старіння. У випадку з HTTP-кешуванням ці відомості містяться в HTTP-заголовки, доступні проксі-серверам і клієнтським системам. В ASP.NET є клас кешу, у який можна записувати дані. При цьому у вас їсти можливість указувати, коли дані варто видаляти з кешу.

Отже, "кешування на прикладному рівні" ставиться й до коду Web-сервісу, і до коду клієнта, що теж так чи інакше кешує дані. Кешування в Web-сервісі може полягати в збереженні в пам’яті комп’ютера екземплярів повторно використовуваних класів або не мінливих даних.

На рівні клієнтського додатка кешування - це збереження відповіді Web-сервісу для того, щоб клієнтові не доводилося посилати ще один запит для одержання тих же даних.

Підтримка кешування звичайно пов’язана з наданням відомостей про строк життя даних. Якщо цей строк завжди постійний, його можна документувати й "зашити" у код клієнта. Тоді вказувати його у відповіді Web-Сервісу не буде потрібно. Однак у багатьох випадках строк життя даних мінливий, і відповідні відомості потрібно зберігати разом з кешуємими даними. При кешуванні на прикладному рівні в дані можна включити нове поле, що містить параметр - строк життя. Тому що звичайно строк життя - це фактично метаінформація, що описує дані, що підходять місце для її зберігання цих відомостей - елемент SOAP-Заголовків. Зберігати метаінформацію про SOAP- Повідомлення треба саме там.

HTTP надає ефективні механізми кешування. У його специфікації описується, за якими правилами системні сервіси повинні кешувати дані. В основному HTTP-прокси й клієнтські комп’ютери забезпечують кешування без яких-небудь зусиль із боку розроблювача додатків, що використовують HTTP. Але область застосування HTTP-кешування для Web-сервісів обмежена.

У цей час для звертання до Web-Сервісів використовуються SOAP-повідомлення, що поміщаються в тіло HTTP-Запиту POST. На відміну від HTTP-Запитів GET, тіло POST-Запитів виходить за область дії HTTP. Тому реалізації протоколу HTTP у проксі-серверах і клієнтах не здатні визначати, як кешувати відповіді на HTTP-Запити POST. ASP.NET підтримує виклик Web- Методів через GET-запити, але цей механізм в основному призначений для налагодження й не підтримується більшістю інших інструментальних засобів SOAP.

Одна із приємних особливостей розробки Web-сервісів XML у середовищі ASP.NET - переваги великої функціональності, який уже користуються розроблювачі додатків Web Forms. Вбудована функціональність ASP.NET полегшує кешування Web-Сервісів XML.

Щоб настроїти кешування вихідних даних ASP.NET для Web-Сервісів, потрібно додати параметр CacheDuration до атрибута WebMethod у визначенні Web-Методу. Цей параметр визначає час (у секундах), у плині якого відповідь зберігається в кеше вихідних даних. Наступний фрагмент коду демонструє, як помістити дані в кеш на 60 секунд.

```
<WebMethod(CacheDuration:=60)> _
Public Function HelloWorld() As String
Return "Hello World"
End Function
```

На відміну від кешування вихідних даних ASP.NET кешування HTTP-відповідей - просто спосіб, яким ASP.NET дозволяє настроїти HTTP-заголовки так, щоб клієнт і проксі-сервери знали, як кешувати повертаємі HTTP-відповіді. Для цього застосовується клас HttpCachePolicy. У коді Web-Сервісу він доступний з Context.Response.Cache, але, як уже говорилося,

можливості його застосування до SOAP-Запитів у тілі POST-Запитів обмежені.

Інша форма кешування в ASP.NET реалізована у вигляді досить цікавого класу Cache. Класи HttpCachePolicy і Cache - навіть незважаючи на те, що їхні батьківські класи посилаються на обоє цих властивостей як на "cache". Клас Cache доступний прямо із класу HttpContext Web-Сервісу. Він надає базову підтримку кешування для ASP.NET-Додатка. У кеші можна зберігати будь-які дані з його набору (collection). У багатьох відносинах цей клас схожий на клас HttpApplicationState, що зберігає глобальні дані додатки у своєму наборі.

```
Dim Foo as New MyFooClass()
 Context.Cache.Insert("foo", _
 Foo, _
 Nothing, _
 DateAdd(DateInterval.Minute, 30, Now()), _
 System.Web.Caching.Cache.NoSlidingExpiration)
```

Функція Insert підтримує кілька варіантів додавання даних у кеш. Перший аргумент, "foo", - це ключ для посилання на об’єкт у наборі. Другий параметр представляє сам елемент, що поміщається в кеш. Третій - установлює залежності файлової системи. У нашому випадку ніяких залежностей ні, так що цей параметр дорівнює "Nothing". Наступний параметр явно задає строк старіння елемента в кеші. Викликом функції DateAdd ми вказали, що об’єкт застаріє через 30 хвилин. Нарешті, останній параметр задає "ковзне" (sliding) старіння. Ковзне старіння означає, що кешований елемент віддаляється, якщо до нього не звертаються в плині зазначеного проміжку часу. Тому що ми явно встановили строк життя даних (30 хвилин), цьому параметру привласнюється значення NoSlidingExpiration.

4.3 Кешування каталогу MSDN Pencil Company

Тепер розглянемо конкретний приклад і визначимо стратегію кешування в цьому сценарії. Ціль цього рішення - дозволити "розумним" клієнтським додаткам кешувати весь каталог і забезпечити можливість запитів до даних. Це знизить навантаження на сервіс за рахунок зменшення запитів і, крім того, надасть додаткову інформацію клієнтам, що користується сервісом. В реалізації швидше за все будеме оновлювати дані раз у день, додаючи в каталог нові сторінки або видаляючи ті, котрих більше немає.

З погляду вибору стратегій кешування, рішення цього завдання спрощується завдяки декільком моментам. По-перше, дані загальнодоступні, тобто нам не потрібно турбуватися про те, щоб у різних користувачів були різні подання даних. По-друге, нам відомо точний час, коли дані обновляються, а виходить, можна чітко вказати строк їхнього життя.

Наступний клієнтський код на Microsoft® Visual Basic® .NET ілюструє використання клієнтом властивості ValidUntil для того, щоб визначити, чи треба обновити вміст кешу каталогу до виконання запиту користувача.

```
Dim PencilResults() As org.pencilsellers.Pencil
If PencilCatalog.ValidUntil < Now() Then
Dim Discovery As New org.pencilsellers.DiscoveryBinding()
PencilCatalog = Discovery.GetCatalog()
End If
PencilResults = QueryCachedCatalog(PencilCatalog, QueryCriterion)
```

На серверній стороні потрібно не тільки надати клієнтові відомості про те, коли минає строк зберігання даних (за допомогою елемента ValidUntil), але й подумати про те, як уникнути створення каталогу "із чистого аркуша" при одержанні кожного запиту. Один зі способів домогтися цього - додати параметр CacheDuration до атрибута WebMethodAttribute. У нашім випадку CacheDuration має один недолік: час зберігання даних фіксується на етапі

розробки. Установивши CacheDuration рівним 24 годинникам, ми можемо зштовхнутися з наступною проблемою.

Каталог в 6 ранку 1-го квітня й установлюємо елемент ValidUntil, що відповідає 6 ранку 2-го квітня. Ці дані потраплять у першу ж відповідь, і він виявиться в кеші вихідних даних ASP.NET. Тепер припустимо, що приблизно в 10 вечора 1-го квітня надходить величезну кількість запитів до іншим ASP.NET-сторінкам. Тому що до каталогу запити не надходять, система, імовірно, видалить його з кешу, щоб звільнити ресурси кешу для більше важливих даних. Потім в 10:30 вечори 1-го квітня надходить ще один запит до каталогу олівців. Тому що в кеше вихідних даних відповіді ні, Web-Метод запускається ще раз, при цьому строк життя даних установлюється рівним 10:30 вечора 2-го квітня. Каталог олівців обновиться в 6 ранки 2-го квітня, а з кешу будуть як і раніше надходити дані за вчорашній день. Так що нам потрібна система кешування, що дозволяє явно вказати строк зберігання даних у період виконання.

Помітьте, що я однаково застосовую параметр CacheDuration для додавання відповіді до кешу вихідних даного ASP.NET, але тепер строк життя відносно малий - 10 хвилин. Тим самим я мінімізую час, протягом якого можливе повернення застарілих даних, але однаково збільшується продуктивність за рахунок кешування, що досить корисно, коли до каталогу надходить безліч запитів. Більшість запитів до каталогу надходить у межах 10 хвилин до закінчення строку зберігання даних.

```
<System.Web.Services.WebMethodAttribute( _
CacheDuration:=600), _
System.Web.Services.Protocols.SoapDocumentMethodAttri
bute( _
"http://pencilsellers.org/2002/04/pencil/GetCatalog", _
RequestNamespace:= _
"http://pencilsellers.org/2002/04/pencil/discovery", _
ResponseNamespace:= _
"http://pencilsellers.org/2002/04/pencil/discovery", _
Use:=System.Web.Services.Description.SoapBindingUse.Li
teral, _ ParameterStyle:= _
System.Web.Services.Protocols.SoapParameterStyle.Wrapp
ed, _ Binding:="DiscoveryBinding")> _
Public Overrides Function GetCatalog() As
Catalog Dim PencilCatalog As Catalog
If Context.Cache("PencilCatalog") Is
Nothing Then PencilCatalog =
CreateCatalog()
Context.Cache.Insert("PencilCatalog", _
```

```
PencilCatalog, _
Nothing, _
PencilCatalog.ValidUntil, _
System.Web.Caching.Cache.NoSlidingExpiration)
Else
PencilCatalog = Context.Cache("PencilCatalog")
If PencilCatalog.ValidUntil < Now() Then
Context.Cache.Remove("PencilCatalog")
PencilCatalog = CreateCatalog()
Context.Cache.Insert("PencilCatalog", _
PencilCatalog, _
Nothing, _
PencilCatalog.ValidUntil, _
System.Web.Caching.Cache.NoSlidingExpiration)
End If
End If
Return PencilCatalog
End Function
```

4.4 Ланцюг Web-проксі як форма мережної маршрутизації

Ланцюг web-проксі - це метод переадресації з'єднань web-проксі з одного ISA-Сервера на іншій. Ланцюга web-проксі складаються зі зворотних і прямого ISA-Серверів. Зворотними ISA-Серверами називаються ті, які розташовані ближче всього до з'єднань із Інтернетом, а прямі ISA-Сервери - це ті, які розташовані далі від з'єднання з Інтернетом. Прямі ISA-Сервери переадресують запити web-проксі на зворотні ISA-Сервери. Першим ISA-Сервером у ланцюзі web-проксі є той, котрий ближче всього до Інтрнету, і який відповідає за одержання вмісту Інтернету.

Використання ланцюга web-проксі корисно в наступних випадках:

- ISA-сервери філії можна зв'язати ланцюгом зі зворотними ISA-

серверами головного офісу.

- ISA-сервери окремих відділів, що захищають спеціалізовані мережі відділів усередині організації, можна зв’язати ланцюгом із сегментом мережних служб або зворотними ISA-серверами, прямо з’єднаними з Інтернетом.
- Постачальники послуг Інтернету або великих клієнтів компанії можуть зв’язати ланцюгом масиви ISA-серверів web-кешування зі зворотним ISA-сервером або масивом ISA-сервера web-кешування.

Перевагою використання ланцюга web-проксі в тім, що так ви можете знизити загальне завантаження каналу Інтернету й каналів між прямими й зворотними ISA-Серверами в ланцюзі web-проксі. На рисунку 4.2. показаний приклад ланцюга web-проксі й потік інформації в ланцюзі.

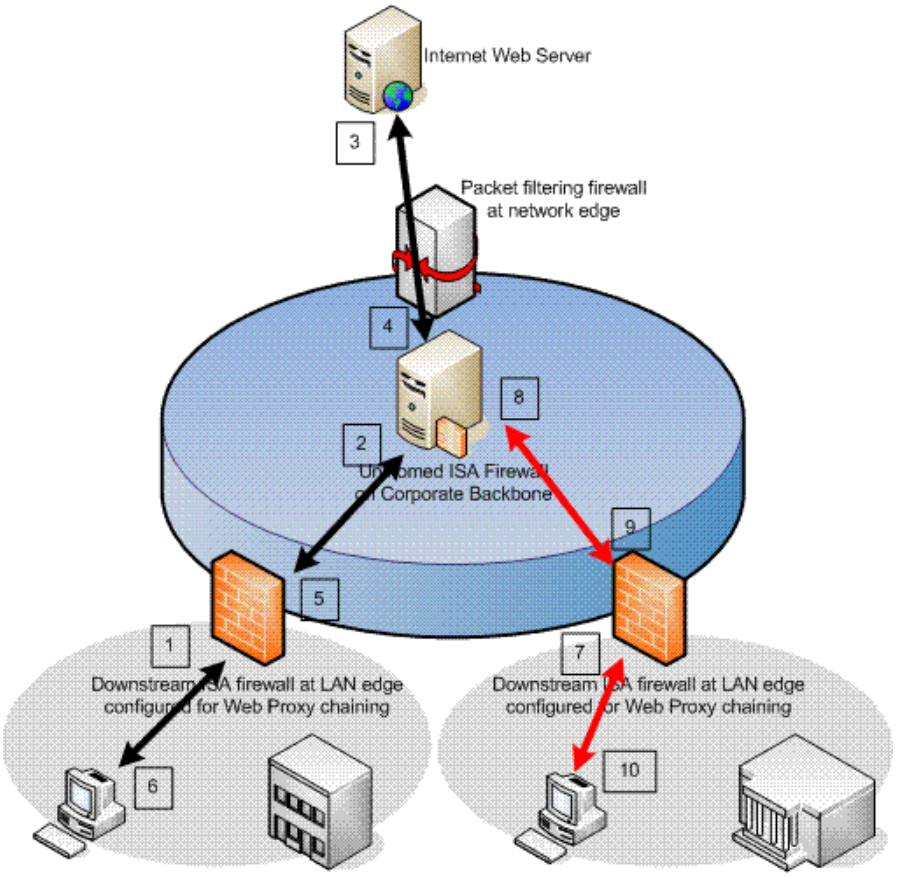


Рисунок 4.2. Структура взаємодії веб-проксі

1. Клієнт, що перебуває в захищеній мережі за ISA-сервером, робить запит до web-сторінки, розташованої на web-сервері в Інтернеті. Запит на з'єднання відсилається через ISA-сервер, що захищає мережу відділу.
2. ISA-сервер переадресує запит на з'єднання до одномережного ISA-серверу, розташованому в основній мережі організації. ISA-сервер відділу настроєний на використання ланцюга web-проксі для зв'язку з одномережним ISA-сервером. Оскільки одномережний ISA-сервер здатний захищати себе від атак, можна майже не обертати уваги на атаки від вузлів основної мережі або від вузлів, розташованих за апаратним брандмауером з функцією фільтрації пакетів перед одномережним ISA- сервером.
3. Одномережний ISA-Сервер, що працює тільки на web-кешування, переадресує запит на з'єднання через апаратний маршрутизатор з функцією фільтрації пакетів.
4. Web-Сервер Інтернету повертає запит одномережному ISA-серверу через апаратного брандмауера з функцією фільтрації пакетів.
5. Одномережний ISA-сервер переадресує відповідь ISA-серверу відділу. Однак, перед тим, як переадресувати відповідь, одномережний ISA- сервер поміщає вміст у свій кеш. Web-вміст у відповіді вертається ISA- серверу відділу з кешу одномережного ISA-сервера.
6. ISA-Сервер відділу повертає відповідь клієнтові, що зробив запит. Але перед цим уміст міститься в кеш. Саме з кешу ISA-Сервера відділу одержує вміст вузол, що зробив запит.
7. Вузол іншої мережі робить запит до цієї ж web-сторінки. Даний вузол також захищений ISA-Сервером. Запит проходить через цей ISA-Сервер.

8. ISA-Сервер перебуває в ланцюзі з одномережним ISA-Сервером основної мережі, на який і переводиться запит. Перед переадресацією запиту на web-сервер Інтернету одномережний ISA-Сервер перевіряє свій кеш на наявність необхідного вмісту.
9. Одномережний ISA-Сервер запитує вміст зі свого кешу й повертає його ISA-Серверу відділу. Одномережний ISA-Сервер не відправляє запит на web-сервер Інтернету, оскільки інформація вже є в його кеше.
10. ISA-Сервер відділу переадресує вміст вузлу, що ініціював запит.

Із цього приклада видно, що заощаджується пропускна здатність не тільки Інтернет-каналу, але й каналу зв’язку з основною мережею. Економія цієї пропускної здатності видна в ситуації, коли інший вузол з кожної з мереж відділів робить запит до того ж. У цьому випадку ISA-серверам відділів, у яких уже є дана інформація в кеші, не потрібно переадресовувати запит на одномережний ISA-сервер основної мережі. У такий спосіб зменшується використання пропускної здатності основної мережі.

Іншим додатком web-ланцюга є настроювання прямого ISA-сервера для зв’язку з масивом web-кешування. Такі масиви створюються в ISA-сервері версії Enterprise Edition. На рисунку 4.3 показаний варіант використання масивів web-кешування в організації.

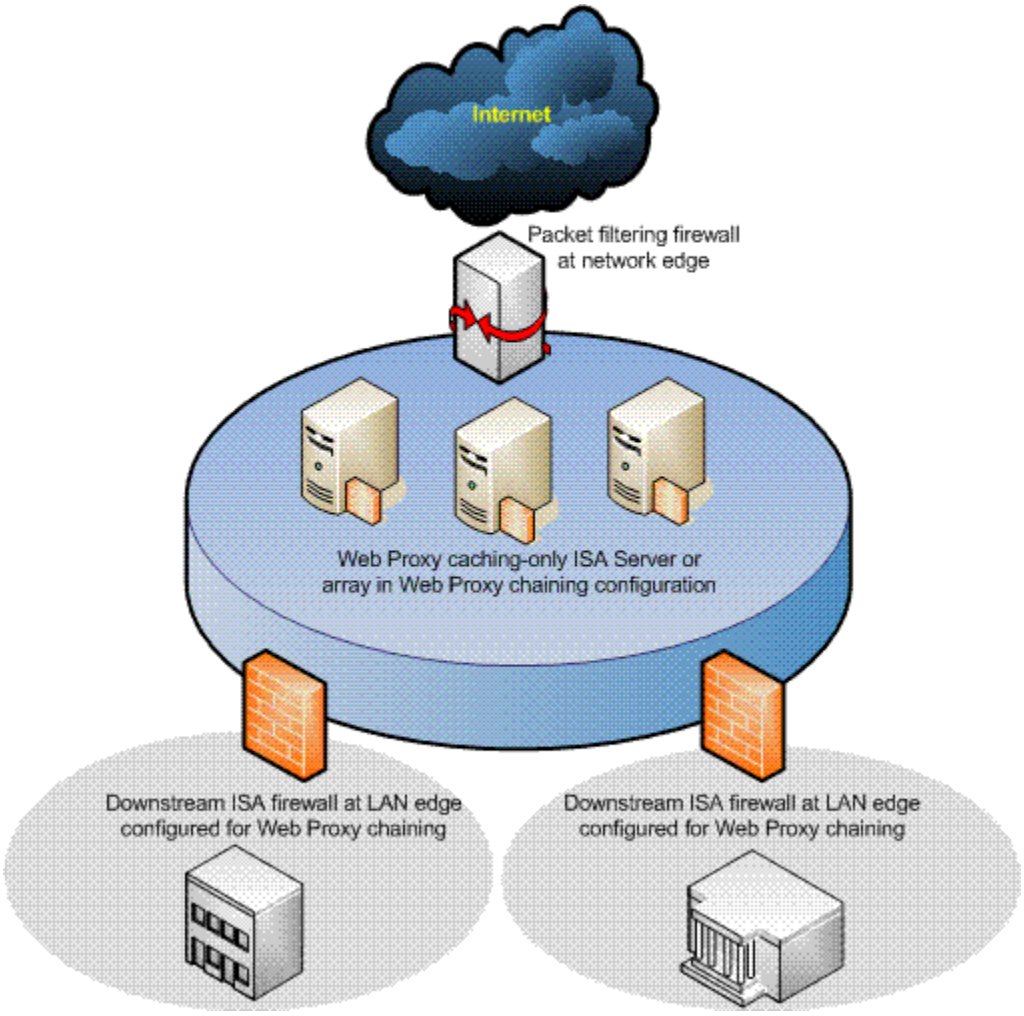


Рисунок 4.3. Створення масивів ISA-серверів

У даному прикладі прямі ISA-Сервери можуть бути настроєні на використання ланцюга з масивом. Масив web-кешування надає інформацію про настроювання прямим ISA-Серверам, включаючи імена комп'ютерів масиву. Якщо один зі членів масиву з якої-небудь причини недоступний, прямі ISA- сервери намагаються з'єднатися з доступними членами масиву.

Крім цього, у випадку неприступності одного зі членів масиву, масив знає, що один з його членів не працює, і видаляє неробочий комп'ютер з масиву. Члени, що залишилися, масиву повідомляють прямі ISA-сервери відділів про те, які члени доступні. Таким чином, прямі ISA-сервери захищені від спроб

зв’язку з непрацюючими членами масиву.

Облікові дані прямого web-проксі ланцюга web-проксі можна настроїти, відзначивши параметр Use this account (використовувати цей обліковий запис). Натисніть Set Account (призначити обліковий запис). У діалоговому вікні Set Account (Настроювання облікового запису), уведіть ім’я користувача в поле User (Користувач) у форматі ІМ’Я_КОМП’ЮТЕРА\Ім’я_користувача. Обліковий запис настроєний у локальній базі даних користувачів зворотного ISA-Сервера. Якщо зворотний ISA-Сервер є членом домена, можна вводити ім’я користувача у форматі ІМ’Я_ДОМЕНА\Ім’я_користувача.

Уведіть пароль і його підтвердження в поля Password (Пароль) і Confirm password (Підтвердити пароль) відповідно. У діалоговому вікні Set Account (Настроювання облікового запису) натисніть ОК. Зі списку, що випадає, Authentication (Аутентифікація) виберіть параметр Integrated Windows (Убудована аутентифікація Windows). Якщо надбудовується використання ланцюга web-прокси з web-проксі сервером, відмінним від ISA-Сервера, доведеться використовувати базову аутентифікацію. Якщо використовується базова аутентифікація, канал ланцюга web-проксі настроєний на використання SSL, оскільки облікові дані базової аутентифікації передаються відкритим текстом. На сторінці Primary Routing (Первинна маршрутизація) натисніть Next (Далі) (рисунок 4.4.).

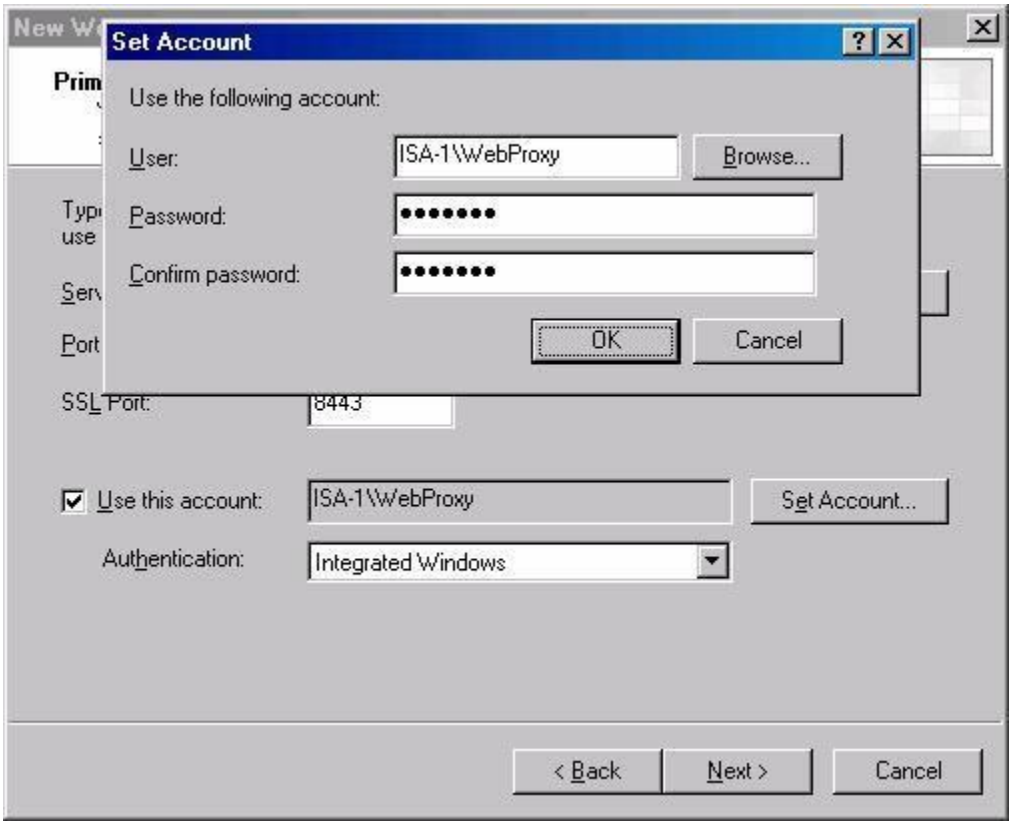


Рисунок 4.4. Налаштування система аутентифікації

На сторінці Backup Action (Резервні дії) є можливість вибору одного з наступних варіантів:

Ignore requests (Ігнорувати запити) Якщо зворотний web-проксі ланцюга web-проксі недоступний, за допомогою даної опції ви обриваєте запити, і клієнт одержить помилку, що повідомляє про неприступність сайту.

Retrieve requests directly from the specified location (Одержувати запити прямо із зазначеного позначка) Цей параметр дозволяє прямому ISA- Серверу в ланцюзі web-проксі використовувати для зв'язку з web-сайтом інший метод, не через ланцюг web-проксі. Дану опцію можна використовувати в тому випадку, якщо зовнішній інтерфейс ISA-Сервера для досягнення запитуваного сайту може використовувати маршрут, відмінний від ланцюга web-проксі.

Route requests to an upstream server (маршрутизувати запити на зворотний сервер) Даний параметр дозволяє прямому ISA-Серверу в ланцюзі

web- проксі використовувати інший ISA-Сервер у другому ланцюзі web-проксі. Ця опція дозволяє встановлювати другий ланцюг web-проксі на прямому ISA-Сервері, що використовується тільки в тому випадку, якщо перший зворотний ISA-Сервер недоступний.

Use automatic dial-up (Використовувати автоматичне комутирувати^ся соединение, щоМ) Дану опцію варто включити при використанні з'єднання, що комутирується, для зв'язку прямого ISA-Сервера з Інтернетом, або ж якщо ви хочете, щоб запити, настроєні за цим правилом, використовували комутируються соединения, щоМ, а не первинне з'єднання ISA-Сервера (звичайно виділений мережний адаптер)

11. На сторінці Backup Action (Резервні дії) виберіть опцію Ignore requests (Ігнорувати запити) і натисніть Next (Далі).
12. На сторінці Completing the New Web Chaining Rule Wizard (Завершення роботи майстри по створенню нового правила web-ланцюга) натисніть Finish (Завершити)
13. Тепер прямій ISA-Сервер настроєний на використання ланцюга у відносинах зі зворотним ISA-Сервером. Не забудьте настроїти правило доступу на зворотному ISA-Сервері для дозволу облікового запису, настроєної в правилі web-ланцюга, доступу до Інтернету по протоколах HTTP, HTTPS і FTP.

Після настроювання ланцюга web-проксі прямій ISA-сервер може бути настроєний на використання клієнтами окремого облікового запису, якщо обліковий запис, використовуваний для аутентифікації на прямому ISA-сервері, не розпізнається зворотним ISA-сервером.

Ім'ям користувача для реєстрації на зворотному ISA-Сервері буде ім'я, використане для аутентифікації в правилі ланцюга web-проксі.

Однак, якщо зворотний ISA-Сервер може аутентифікувати користувача,

що ініціювали споконвічний запит, через те, що зворотний сервер перебуває в тім же самому домені, що й клієнт і прямий сервер, або в локальній базі зворотного сервера є такий користувач, то користувач, що створив з'єднання, з'явиться в журналах і прямого, і зворотного ISA-Сервера.

4.5 Інформаційний захист на рівні додатків

Сервер ISA і пакет доповнень Feature Pack 1 дозволяють створити додатковий зручний у керуванні рівень захисту поштових серверів, веб-серверів і серверів Exchange для OWA (Outlook Web Access), розташованих за брандмауером. Поштові сервери стають більше безпечними, оскільки тепер вони можуть вчасно перехоплювати повідомлення, що містять небажані слова або вкладення. Крім того, сервер ISA і пакет доповнень Feature Pack 1 забезпечують захист користувачів Outlook, віддалено підключаючихся до сервера Exchange за допомогою мереж без довіри, що не використовують VPN. Нові системи перевірки дійсності й безпеки веб-серверів і серверів, що використовують OWA (Outlook Web Access), краще захищають їх від різних типів атак з Інтернету. Ви можете також додати додаткові органи керування й використовувати сервер ISA для захисту серверів BizTalk Server і SQL Server (рисунок 4.5).

Рисунок 4.5. Використовувати серверу ISA для захисту даних

Локальний брандмауер, що використовує сервер ISA для захисту комп'ютерів із серверами IIS, Exchange і BizTalk, об'єднаними в загальній захищеній зоні.

Рисунок 4.6. Сервер ISA для захисту комп'ютерів із серверами IIS

Один із прикладів ретельної перевірки переданих даних (рисунок 4.6.). Сервер ISA Server і пакет доповнень Feature Pack 1 можуть на рівні додатків зупиняти атаки, пов'язані з декодуванням Unicode, проходженням каталогів і неправильним формуванням запитів HTTP, і попереджати проникнення небезпечних запитів у мережу.

Exchange і Outlook Web Access:

- Сервер ISA може виконувати роль ефективного брандмауера для обміну повідомленнями й спільною роботою на базі Exchange і Outlook. Сервер ISA має убудований фільтр RPC, що обмежує трафік, що надходить на Exchange RPC, що робить сервер більше безпечним і зручним у настроюванні.
- Фільтр SMTP, що входить до складу сервера ISA, дозволяє проводити відбір повідомлень по ключових словах, значенням полів і вкладених файлів; Крім того, для забезпечення повної безпеки при

обміні повідомленнями сервер ISA використовує антивірусні програми й засоби масштабування незалежних розробників.

- Сервер ISA і пакет доповнень Feature Pack 1 забезпечують захист користувачів Outlook, віддалено підключених для роботи з повідомленнями до сервера Exchange за допомогою мереж без довіри, що не використовують VPN. Для цього служить динамічний фільтр RPC.

Інформаційні служби інтернету:

- Засіб URLScan для сервера ISA Server і документація, що входять до складу пакета доповнень ISA Server Feature Pack 1, роблять систему безпеки служб IIS ще більш надійної, а роботу з ними — ще простіше.
- Крім звичайних фільтрів HTTP сервер ISA використовує механізм перевірки SSL (Secure Sockets Layer), що здатний захистити навіть безпечні канали. Передача функцій SSL серверу ISA дає й економічну вигоду, оскільки звільняє користувачів від необхідності купувати додаткові сертифікати для веб-серверів.
- Можливості сервера ISA стануть ще ширше, якщо для перевірки законності запитів і даним, одержуваним і відправлятися комп'ютером зі службами IIS, використовувати фільтри ISAPI.

Сервер ISA дозволяє забезпечувати безпека інших продуктів і технологій Майкрософт, у тому числі наступних.

- Сервер BizTalk. Сервер ISA — це брандмауер, що захищає з'єднання між партнерами й забезпечує цілісністю внутрішніх ресурсів.

- Сервер SQL. Сервер ISA може використовуватися як брандмауер для захисту баз даних SQL Server від користувачів і від зайвого мережного трафіку.
- Сервер Microsoft SharePoint™ Portal Server 2001. Сервер ISA із установленим пакетом доповнень Feature Pack 1 має засіб перетворення посилань, що дозволяє швидко й безпечно розміщати портали в інтернеті.

Сервер ISA може підвищити ефективність роботи, збільшивши швидкість доступу в Інтернет. Більше висока швидкість доступу досягається за рахунок зберігання веб-умісту фізично поблизу користувачів. Сервер ISA має легко надбудовану архітектуру, що дозволяє за допомогою протоколу CARP об'єднати кілька комп'ютерів із серверами ISA у кластер і збільшити обсяг кешу. На рисунку 4.7. показаний механізм роботи масивів CARP і ієрархічного кешування. При застосуванні ієрархічного кешування дані автоматично розподіляються між серверами, які можуть бути розташовані по усьому світі. Використання засобів керування доступом забезпечує не тільки високу швидкість доступу в Інтернет, але й контроль над ним.

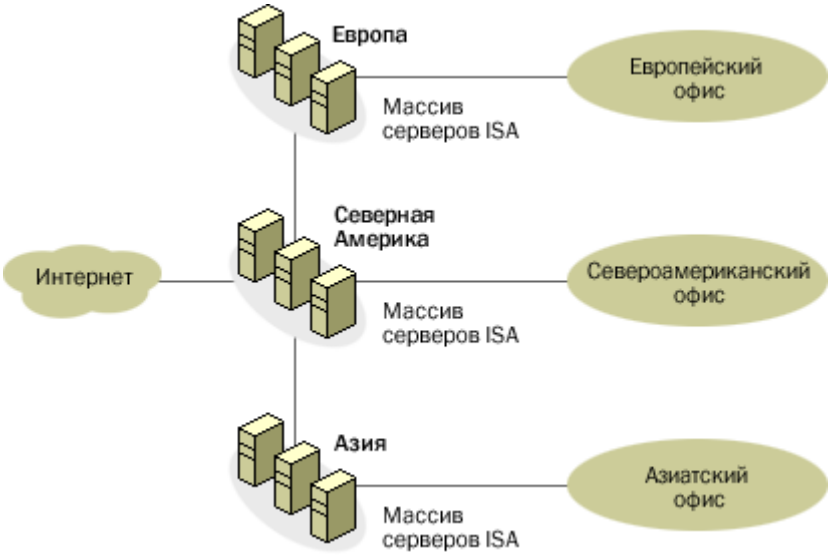


Рисунок 4.7. Масиви CARP і ієрархічна архітектура кешування

Засоби керування доступом, протокол CARP і ієрархічне кешування дають наступні переваги.

- Сервер ISA дозволяє виконувати фільтрацію по адресах URL і типам MIME, а також забезпечувати захист від незаконного використання ресурсів мережі.
- Застосування протоколу CARP дозволяє автоматично масштабувати кеш у масиві серверів, підвищуючи ефективність його використання. При цьому об'єкти автоматично завантажуються, кешируются й передаються клієнтові.
- Ієрархічне кешування дозволяє зберігати дані фізично поблизу користувачів, підвищуючи тим самим продуктивність мережі.

Сервер ISA може вирішити завдання захисту брандмауером, створення віртуальної приватної мережі (VPN), підвищення продуктивності й керування, оскільки він поєднує широкий спектр технологій і продуктів Microsoft. Один сервер ISA може задовольнити всі потреби невеликої компанії або представництва, пов'язані з розгортанням віртуальної приватної мережі, зручністю керування, забезпеченням безпеки, настроюванням проксі й організацією роботи кешу. Сервер ISA дуже простий в установці й адмініструванні, оскільки для керування їм використовується зручна консоль MMC (Microsoft Management Console) (рисунок 4.8). При розгортанні сервера ISA в інтегрованому режимі, ви одержуєте можливість підвищити надійність, безпека й продуктивність своєї мережі за допомогою всього лише одного комп'ютера.

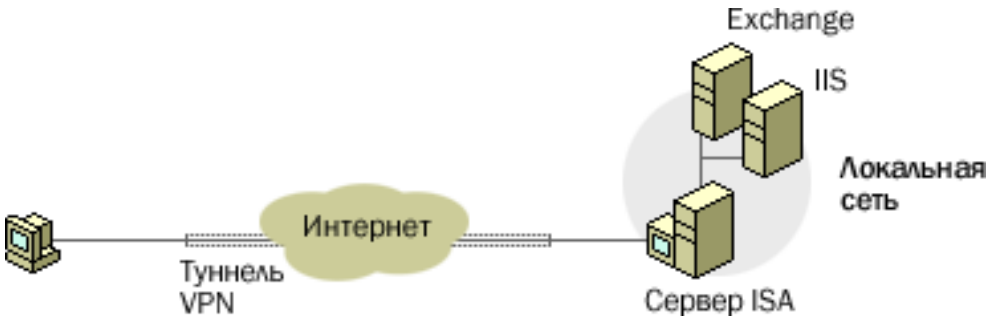


Рисунок 4.8. Підключення сервера ISA

Інтегрований шлюз, що забезпечує кешування, захист брандмауером і роботу служб VPN.

Єдина система кешування, безпеки й служб VPN надає наступні переваги.

- За рахунок зберігання даних фізично поблизу користувачів кешування дозволяє підвищити продуктивність мережі й збільшити максимальне число підтримуваних нею користувачів.
- Сервер ISA підтримує керування доступом як зсередини мережі, так і ззовні, ви можете розміщати в Інтернеті свої служби, будучи впевнені, що ніхто з ваших співробітників не має доступу до незаконних ресурсів Інтернету. Єдина система доступу має на увазі, що підвищення продуктивності мережі за допомогою сервера ISA не створює погроз безпеки.
- Інтеграція з VPN дозволяє вилученим користувачам підключатися до внутрішньої мережі організації й управляти безпекою мережі за допомогою одного перехідного пристрою.

4.6 Брандмауер GEG Express NET

Комп'ютерні віруси, зовнішні мережні атаки, витоки важливих

корпоративних даних - ці й багато інших погроз, так чи інакше, пов’язані з підключенням підприємств до глобальної мережі Інтернет. За даними аналітичних агентств, вони приносять збиток, обчислювальний мільярдами доларів щорічно. Незважаючи на те, що підрахунки не ведуться, неофіційні дані також говорять про багатомільйонні збитки.

Використання існуючих рішень від компаній, що спеціалізуються на захисті інформації, найчастіше має ряд мінусів. Як правило, вони мають "закриту" архітектуру, а отже, відсутня можливість гнучкого настроювання системи, обмежена її масштабованість, висока вартість. Крім того, як показує практика, навіть найвідоміші виробники спеціалізованого встаткування не гарантують 100% безпека, у підсумку підприємство залежить від часу реагування виробника на знову виниклі потенційні погрози й не завжди може самостійно відгородити себе від останніх.

GEG Express NET може використовуватися в організаціях будь-якого розміру для забезпечення безпеки, продуктивності, керованості, а значить і підвищення економічної ефективності роботи корпоративних мереж.

Спрощені можливості настроювання й установки забезпечують єдине керування мережею VPN і міжмережевим екраном, реалізоване за допомогою зручного засобу редагування політик. Передбачені також інтуїтивно зрозумілі мережні шаблони, автоматизовані майстри й удосконалені засоби усунення неполадок, що дозволяє знизити вартість володіння й уникнути помилок у настроюванні параметрів безпеки (рисунок 4.9).

За допомогою брандмауера GEG Express NET реалізуються функціональні можливості, необхідні організаціям для ведення бізнесу в сучасних умовах:

- безпечний і простий метод надання доступу до електронної пошти співробітникам за межами мережі;

- безпечний і простий метод надання інформації з інтрамережі підприємства через Інтернет;
- безпечний метод надання партнерам доступу до даних усередині корпоративної мережі;
- безпечний і гнучкий метод надання віддаленого доступу для співробітників з одночасним захистом корпоративної мережі від можливих атак зловмисників;
- безпечний метод взаємодії філій з основним офісом через Інтернет;
- контроль доступу до Інтернету й захист клієнтів від можливих атак з Інтернету;
- швидкий доступ до часто використовуваному веб-змісту.

Швидка установка захисту сервера Exchange в Інтернеті:

- для швидкого розгортання, а також зниження ризику створення помилкової конфігурації виконання стандартних завдань автоматизує за допомогою майстра web-публікації поштового сервера.

Запобігання можливих атак на поштові сервери:

- команди, які спрямовані на використання можливих атак або розкриття надлишкової інформації, блокуються.

Можливість попередньої перевірки дійсності користувачів:

- блокування потенційно небезпечних анонімних запитів до їхнього влучення на сервер Exchange.

Рисунок 4.9. Метод надання даних корпоративної інтрамережі через Інтернет

Безпечний метод доступу до додатків внутрішньої корпоративної мережі з Інтернету:

- інтегровані майстри web-публікації й публікації сервера автоматизують виконання стандартних завдань, і дозволяють знизити ризик створення помилкової конфігурації.

Засоби перетворення посилань:

- здійснюється інтелектуальне перетворення внутрішніх посилань в адреси зовнішніх веб-вузлів.

Удосконалені захисні функції:

- контроль допустимості змісту потоку даних і примусове підставлення дозволених URL-Адрес.

Рисунок 4.10. Засоби надання доступу до даних усередині мережі

Інтегрований в GEG Express NET компонент VPN:

- можливість підключати партнерів до своєї мережі, одночасно обмежуючи доступ до певних серверів і додатків (рисунок 4.10).

Забезпечення конфіденційності й цілісності даних:

- шифрування всього потоку даних між внутрішніми мережами зовнішніх організацій і корпоративною мережею підприємства.

Захист корпоративної мережі від можливих атак на прикладному рівні:

- можливість призначати строгі правила фільтрації даних додатків.

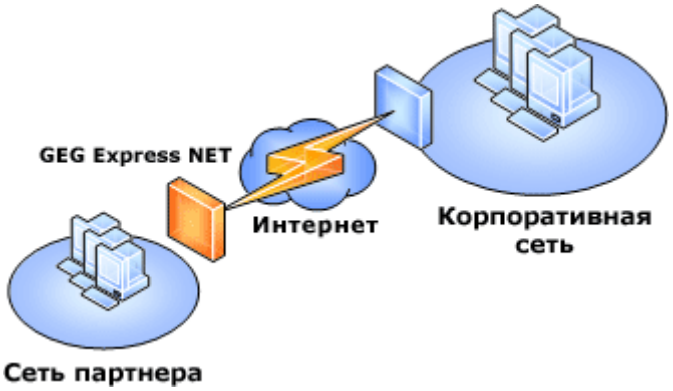


Рисунок 4.11. Метод надання віддаленого доступу

Захист корпоративної мережі від неконтрольованих віддалених комп'ютерів, що встановлюють VPN-Підключення (рисунок 4.11.):

- удосконалена фільтрація на рівні додатків;
- у процесі перевірки й аналізу потоку даних блокуються віруси й "чирви";
- користувачам і групам VPN можуть бути призначені гнучкі мережні політики, що надають доступ тільки до певних серверів і додатків;
- автоматичне блокування доступу до мережі із клієнтських комп'ютерів, що не відповідають прийнятим на підприємстві політикам відносно встановлених пакетів відновлення, засобів антивірусного захисту й інших критеріїв.

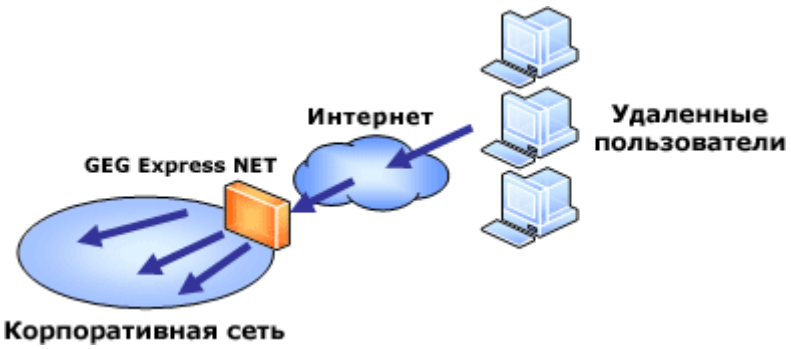


Рисунок 4.12. Метод взаємодії з основним офісом через Інтернет

Об'єднання різних мереж (наприклад, основного офісу й філій) через VPN- Шлюз (рисунок 4.12.):

- можливість VPN-Підключення "вузол у вузол";
- функція маршрутизатора VPN тунельного режиму IPSec використовується для керування доступом користувачів, груп, вузлів, комп'ютерів, протоколів і даних рівня додатків при підключеннях "вузол у вузол";
- користувачі мають доступ тільки до дозволеного змісту вилученої мережі, а користувачі вилученої мережі мають доступ тільки до явно наданих ресурсів локальної мережі.

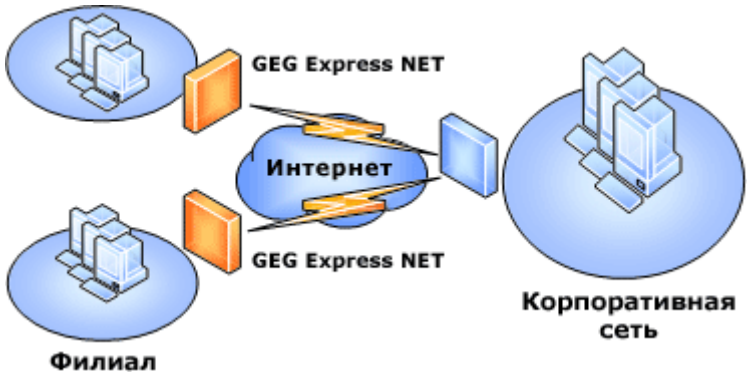


Рисунок 4.13. Керування доступом до Інтернету й захист від атак

Можливість застосування й керування політиками доступу користувачів до Інтернету (рисунок 4.13):

- гнучкі політики міжмережевого екрана служать для блокування web- вузлів, а також проведення фільтрації змісту з метою підвищення продуктивності праці користувачів і відсікання небажаного змісту.
- інтеграція з Active Directory дозволяє створювати елементи керування доступом для різних організаційних ролей і посадових рівнів.

Можливість блокування використання убудованих додатків, наприклад, голосових, відео й інших однорангових служб або засобів обміну миттєвими повідомленнями:

- удосконалена фільтрація даних протоколу HTTP.

Захист робочих комп'ютерів і серверів від можливих атак:

- в GEG Express NET реалізовані засоби фільтрації даних додатків;
- внутрішні клієнти недоступні за межами мережі;
- відповідний вхідний потік даних піддається перевірці;
- допускається підключення надбудов сторонніх виробників, що забезпечують захист від вірусів.

Рисунок 4.14. Доступ до часто використовуваного web-змісту

Попереднє завантаження змісту web-вузлів, до яких користувачі звертаються найбільше часто (рисунки 4.14-4.16):

- засоби попереднього завантаження дозволяють адміністраторові вручну вказувати часто використовувані web-ресурси;
- розпізнавання закономірностей в web-потоці даних за допомогою активного кешування й автоматичне завантаження змісту часто запитуваних web-вузлів;
- відправлення спеціальних запитів зовнішнім серверам кешування при необхідності;
- убудована перевірка вихідних запитів на відповідність заданим умовам.

Рисунок 4.15. Використання кешу при доступі до ресурсів

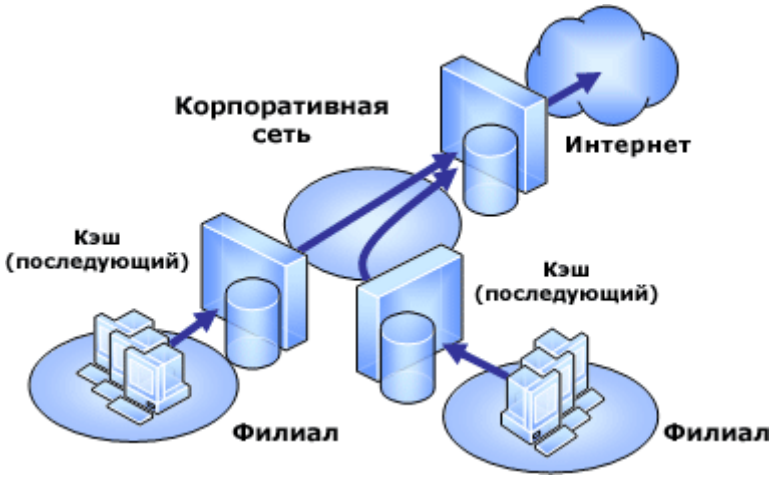


Рисунок 4.16. Переваги використання GEG Express NET

Підвищена безпека віддаленого доступу до сервера Exchange

- поліпшення безпеки Microsoft Office Outlook Web Access за рахунок використання перевірки дійсності на основі форм;
- підтримка привіконних клієнтів Outlook шляхом забезпечення безпечних підключень до сервера Exchange по протоколі RPC;
- поліпшене керування доступом до системи за рахунок застосування

комплексного механізму перевірки дійсності.

Поліпшений захист від атак з Інтернету

- запобігання можливих атак на поштовий SMTP-Сервер шляхом фільтрації трафіку по протоколах SMTP і POP3;
- поліпшений захист електронної пошти у форматі HTML за рахунок удосконаленої фільтрації протоколу HTTP;
- ретельна перевірка вмісту міжмережевого екрану з функціями фільтрації прикладного рівня;
- перевірка минаючі міжмережевий екран зашифрованого трафіку за допомогою моста SSL-SSL.

Підвищення продуктивності й зниження витрат

- новий, зручний у використанні користувальницький інтерфейс і засоби керування;
- раціональне настроювання конфігурації за допомогою майстрів публікації поштового сервера й Outlook Web Access;
- додаткова гнучкість за рахунок застосування конфігурації з підтримкою декількох мереж і унікальної політики для кожної з мереж;
- зменшення кількості небажаних поштових повідомлень за допомогою засобу контролю SMTP-Повідомлень;
- керування GEG Express NET у вилученому режимі дозволяє співробітникам виконувати більший обсяг роботи;
- спрощене адміністрування завдяки впровадженню нових засобів керування;
- більші можливості настроювання за рахунок реалізації розширюваної архітектури фільтрів.

ВИСНОВКИ

Досвід організацій, що займаються захистом інформації показує, що для досягнення вдалих рішень по захисту інформації потрібне поєднання правових, організаційних і технічних заходів. Це поєднання визначається конфіденційністю інформації, що захищається, характером небезпеки і наявністю засобів захисту. У загальному випадку технічні заходи безпеки складають незначну частину від загальних заходів захисту (правових і організаційних). Проте жодну з них упускати не можна. Кожна міра доповнює іншу, і недолік або відсутність будь-якого способу приведе до порушення захищеності.

Викладені етапи можна вважати типовими для процесу розробки систем захисту, оскільки вони значною мірою охоплюють практично увесь об'єм робіт на організаційному рівні.

Зроблено аналіз джерел виникнення інформаційних загроз, наведено методику розрахунку можливих втрат від виникнення інформаційного ризику.

ПЕРЕЛІК ПОСИЛАНЬ

1. С.А.Крашаков, Л.Н.Щур, Кеширование информационных потоков, FREEnet’95 Workshop,
2. S.A.Krashakov, FREEnet Web-caching development, Proc. ICM Workshop on Web Caching "Web Caching on Internet", Warsaw, Poland, September 30 - October 1, 1996
3. S.A.Krashakov, FREEnet Web-caching development, NLANR Web Caching Workshop, Boulder, Colorado, June 9-10, 1997
4. С.А. Крашаков, Высокоскоростные телекоммуникации и кеширование информации в Internet, Proc. BBCC’97: Int. Conf. "Broadband Communications for Research and Education - Collaboration between Russia and the European Union", Moscow, 17-18 June 1997
5. S. Krashakov and L. Shchur. WWW Caching in Russia - Current State and Future Development. Proc. 3d Int. Web caching Workshop, Manchester, June 15-17, 1998.
6. С.А. Крашаков, Л.Н. Щур. Кешування информационных потоков и стратегия оптимизации маршрутов в распределенных системах. Тези докл. Всеріс. конф. "Науковий сервіс у мережі ІНТЕРНЕТ", с. 145-148.
7. С.А. Крашаков. "Кешування информационных потоков и стратегия оптимизации маршрутов в распределенных системах".Современные сетевые технологии, Москва, 20.03.2001
8. С.А. Крашаков, Л.Н. Щур, "Кешування информационных потоков и стратегия оптимизации маршрутов в распределенных системах кеш-серверов".
9. Router Security. Best Common Practices for Hardening the Infrastructure. Juniper Networks, Inc. Application Note, 2002
10. Cisco Router Security Best Practices. CERT - In, Indian Computer

Emergency Response Team, 2004

11. Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC). National Security Agency, 2005
12. Network Security Policy : Best Practices White Paper. Cisco Press
13. Cisco Catalyst Integrated Security - Enabling the Self - Defending Network. White Paper. Cisco Press, 2007
14. RFC 2827 «Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing»
15. RFC 3013 «Recommended Internet Service Provider Security Services and Procedures»
16. RFC 3871 «Operational Security Requirements for Large

Internet» 17.RFC 3631 «Security Mechanisms for the

Internet»

18. М. Мамаев, С.Петренко. Технологии защиты информации в Интернете. - СПб: "Питер", 2002

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Мета та завдання роботи

Мета роботи: визначення оптимального методу забезпечення безпеки інформації.

Завдання:

1. Побудова мережі доступу;
2. Вимоги до безпеки інформації;
3. Обладнання мережі доступу.

Вимоги до безпеки інформації

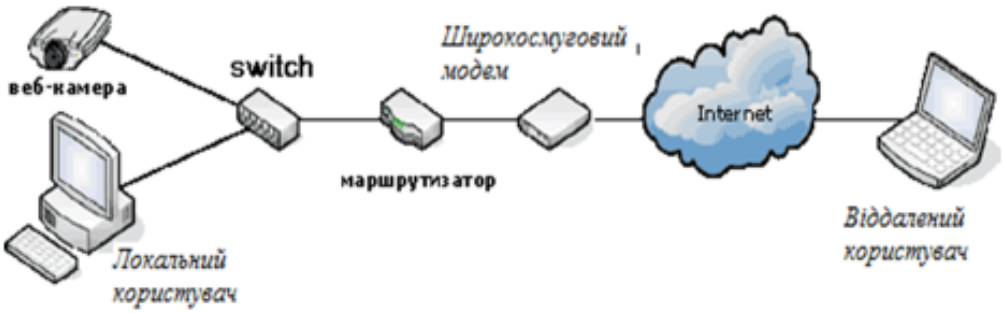
1. Чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
2. Надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
3. Зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;
4. Облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
5. Забезпечення оцінювання ступеня конфіденційної інформації;
6. Забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

Класи безпеки захисту інформації

Клас	Призначення
Перший	означає наявність розвинутої служби безпеки
Другий	включає повний набір механізмів захисту на декількох рівнях
Третій	захист при багатьох суб'єктах і об'єктах, допущених до інформації
Четвертий	захист електронних платежів
П'ятий	захист розподілених інформаційних мереж
Шостий	захист локальних інформаційних мереж
Сьомий	мінімальні вимоги до захищеності

Модель і архітектура мережі доступу

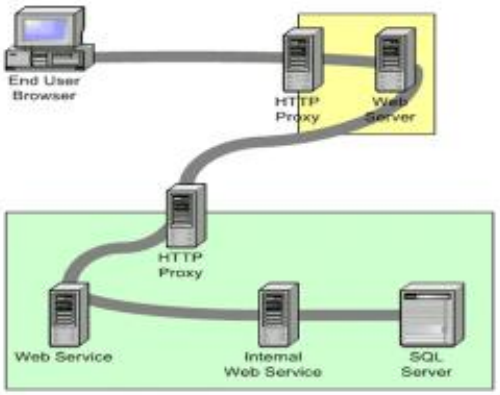
Схема доступу через мережу передачі даних



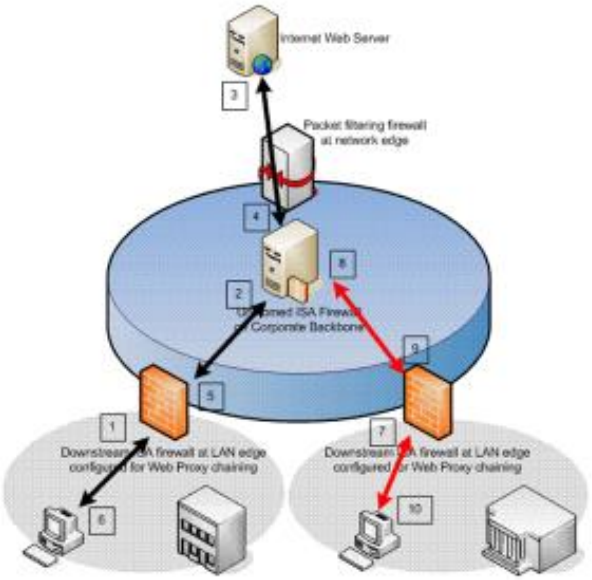
Принципи інформаційної безпеки

Інформаційна безпека		
Доступність	**Конфіденційність**	**Цілісність**
Забезпечення доступу до загальнодоступних даних усім користувачам, захист цих даних від спотворення та блокування зловмисниками.	Забезпечення доступу до даних на основі розподілу прав доступу.	Захист даних від зловмисного або випадкового видалення чи спотворення.

Приклад використання proxy-серверів



Приклад використання firewall



Висновки

- Досвід організацій, що займаються захистом інформації показує, що для досягнення вдалих рішень по захисту інформації потрібне поєднання правових, організаційних і технічних заходів. Це поєднання визначається конфіденційністю інформації, що захищається, характером небезпеки і наявністю засобів захисту. У загальному випадку технічні заходи безпеки складають незначну частину від загальних заходів захисту (правових і організаційних). Проте жодну з них упускати не можна. Кожна міра доповнює іншу, і недолік або відсутність будь-якого способу приведе до порушення захищеності.
- Викладені етапи можна вважати типовими для процесу розробки систем захисту, оскільки вони значною мірою охоплюють практично увесь об'єм робіт на організаційному рівні.
- Зроблено аналіз джерел виникнення інформаційних загроз, наведено методику розрахунку можливих втрат від виникнення інформаційного ризику.