зберігання в ретроспективі й перспективі. - LAN, 2002 – 4 с. ***7.*** *Fujitsy Siemens Computers. Основи зберігання даних – чому важливо забезпечити надійність IT-инфраструктури. – Fujitsu Siemens, 2007 – 84 с.* ***8.*** Steve Guendert. *Buffer-to-Buffer Credits and Their Effect on FICON Performance. - McDATA, 2005 - 5 с.* ***9.*** *Cisco Systems. Storage Extensions over Optical . – Cisco Systems, 2004 – 70 с.*

УДК 681.3

ВАРІАНТИ ЗАХИСТУ ВІД ЗАГРОЗ В КОМУНІКАЦІЯХ РОЗПОДІЛЕНИХ МЕРЕЖ

В'ячеслав Василенко
Національний авіаційний університет

Анотація: **Розглядаються питання захисту інформаційних ресурсів комунікаційної мережі зв'язку розподіленої обчислювальної мережі, наводиться варіант організації багаторівневого захисту ресурсів мережі, розглядаються механізми забезпечення функціональних послуг безпеки.**
Summary: **The questions of defense of informative resources of communication network of the distributed computer network are examined, the variant of organization of multilevel defense of resources of network is pointed, the mechanisms of providing of functional services of safety are examined.**
Ключові слова: **Загроза, порушник, ресурси, модель, комунікаційна мережа**

I Загальний підхід до захисту інформаційних ресурсів розподілених мереж

Для захисту інформаційних ресурсів розподілених обчислювальних мереж (РОМ) пропонується використання корпоративної брандмауер-системи, яка інтегрується в інфраструктуру РОМ і забезпечує виконання встановлених правил доступу до захищеної мережі вузлів РОМ та відслідковування протоколів і послуг із захисту, що використовуються [1].

Така брандмауер-система є єдиною загальною точкою обміну даними кожного вузла РОМ із корпоративною мережею і використовується як бар'єр між захищеною і незахищеною мережами таким чином, що всі дані між мережами проходять безпосередньо через брандмауер-систему. В брандмауер-системі реалізовані механізми безпеки, які роблять цей інтерфейс безпечним і керованим. Механізми безпеки брандмауер-системи дозволяють: аналізувати дані, що проходять через брандмауер-систему; контролювати комунікаційне середовище і партнерів з обміну даними; регламентувати обмін даними відповідно до політики безпеки; реєструвати події, що мають відношення до безпеки.

Використання єдиної загальної точки обміну даними кожного вузла РОМ із корпоративною мережею дає декілька переваг: організація захисту є значно ефективнішою; простіша реалізація корпоративної політики безпеки; використовуються посилені методи автентифікації; забезпечується безпека через розподіл ресурсів; полегшується спостереження за сеансами обміну інформацією.

Основними завданнями брандмауер-системи є: контроль доступу на мережному рівні; контроль доступу на рівні користувачів; контроль доступу на рівні даних; керування правами доступу; контроль доступу на прикладному рівні; ізоляція послуг із захисту; реалізація функцій оповіщення; приховування інфраструктури мережі; конфіденційність комунікацій.

II Варіант організації багаторівневого захисту ресурсів мережі

Для забезпечення захисту інформаційних ресурсів корпоративної мережі РОМ можна реалізувати багаторівневий захист. Необхідність його реалізації обумовлюється, з одного боку, відсутністю універсальних засобів захисту, а з іншого, тим, що жодний окремий компонент не може достатньою мірою захистити мережу. Для ефективного захисту необхідно використовувати множину компонентів, що сумісно працюють таким чином, що здійснення атаки буде неможливим або ускладненим.

Організація багаторівневого захисту пов'язана з визначенням периметра мережі, внутрішньої мережі і політики безпеки системи (фактор персоналу).

Периметр – це посилена границя мережі, яка може включати до свого складу: маршрутизатори (routers); брандмауери (firewalls); систему виявлення вторгнень (СВВ, IDS); пристрої віртуальної приватної мережі (ПВПМ, VPN); програмне забезпечення мережі; демілітаризовану зону (ДМЗ, DMZ) і екрановані підмережі.

Маршрутизатори здійснюють управління вхідним і вихідним трафіком та трафіком в середині мережі. Пограничний маршрутизатор є останнім маршрутизатором перед виходом в незахищену мережу і виконує роль першого і останнього рубежу захисту мережі.

Брандмауер або міжмережний екран аналізує трафік із використанням набору правил, які дозволяють визначити можливість або неможливість передачі трафіка мережею. Область дії брандмауера починається там, де закінчується область дії пограничного маршрутизатора.

Система виявлення вторгнень дозволяє виявити і повідомити про вторгнення в мережу і про потенційно небезпечні події. Система може складатися з множини детекторів різного типу, що розміщені в найважливіших точках мережі. Детектори СВВ шукають задані сигнатури критичних подій або виконують статистичний аналіз функціонування мережі і виявляють аномальні події. У разі виявлення критичних подій детектори СВВ повідомляють адміністратора і/або здійснюють запис у журнал подій.

Віртуальна приватна мережа є захищеним сеансом, для організації якого використовуються незахищені канали зв'язку. Під ПВПМ розуміють технічний комплекс периметра, що забезпечує шифрування сеансів. ПВПМ дозволяє віддаленим партнерам безпечно підключатися до внутрішньої захищеної мережі з незахищеного середовища.

Під *програмним забезпеченням* розуміють додатки, які функціонують в мережі. Архітектура програмного забезпечення має важливе значення, оскільки основним завданням периметра мережі є захист даних, що відносяться до додатків і сервісів.

Демілітаризована зона – це підмережа, що містить ресурси загального користування і підключається до брандмауера або іншого фільтруючого пристрою, який захищає її від зовнішніх вторгнень.

Екранована підмережа є областю, що розміщується поза брандмауером. Екранована підмережа використовується для ізоляції серверів, до яких необхідно забезпечити доступ із незахищеної мережі і які використовуються користувачами внутрішньої захищеної підмережі.

Внутрішня мережа – це мережа, яка захищена периметром. Вона містить всі сервери, робочі станції та інформаційну інфраструктуру. Для забезпечення захисту внутрішньої мережі використовуються наступні пристрої "периметра": маршрутизатори для фільтрування вхідного та вихідного трафіка підмережі; внутрішні брандмауери для розподілу ресурсів; проксі-брандмауери для підвищення безпеки; детектори СВВ для моніторингу трафіка внутрішньої мережі. У внутрішній мережі також використовуються: персональні брандмауери для посилення захисту хостів; антивірусне програмне забезпечення; посилення захисту операційної системи; керування конфігурацією системи; аудит.

Захист хоста – це процес зміни конфігурації операційної системи і додатків хоста з метою перекриття потенційних вразливостей системи. Посилення захисту хоста є останнім рубежем оборони системи.

Управління конфігурацією – процес встановлення і підтримки визначеної конфігурації для систем і пристроїв, що входять до мережі. Управління конфігурацією – це найкращий захід організації захищеної стандартної (базової) конфігурації, який призведе до зниження наслідків інцидентів до мінімуму. Управління конфігурацією дозволяє також контролювати неавторизоване встановлення програмного забезпечення.

Аудит – процес, який дозволяє контролювати стан захищеності мережі і своєчасно вносити зміни в архітектуру системи технічного захисту мережі.

Концепція багаторівневого захисту передбачає створення ефективної інфраструктури безпеки і визначає рівні та можливі механізми захисту інформаційних ресурсів мережі.

III Забезпечення функціональних послуг безпеки механізмами захисту РОМ

Комплекс засобів захисту комунікаційної мережі зв'язку (КМЗ) РОМ має забезпечувати реалізацію основних функціональних властивостей безпеки інформаційних ресурсів РОМ, передбачених вимогами Нормативних документів Системи технічного захисту інформації, таких як: конфіденційність, цілісність, доступність, спостереженість.

Нормативною базою для вибору і реалізації вимог із захисту інформації в РОМ є НД ТЗІ 2.5-005-99 [3]. Профіль може бути або вибраний із профілів, описаних в [3], або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації з обмеженим доступом і призначенням РОМ.

Як уже наголошувалося, забезпечення функціональних властивостей захищеності мережних ресурсів РОМ може досягатися шляхом використання *сукупності засобів та механізмів захисту*: маршрутизаторів, серверів доступу, міжмережних екранів, засобів криптографічного перетворення інформації, що передається відкритими каналами зв'язку, засобів контролю цілісності, засобів антивірусного захисту, систем резервного копіювання та відновлення інформації, програмних засобів централізованого керування системою захисту інформації, аудиту за станом захищеності системи і реагування на критичні події, що пов'язані зі спробами порушення встановленої власником РОМ політики безпеки.

Структура (склад та взаємозв'язки) можливих засобів і механізмів захисту КМЗ РОМ представлена на рис. 1.

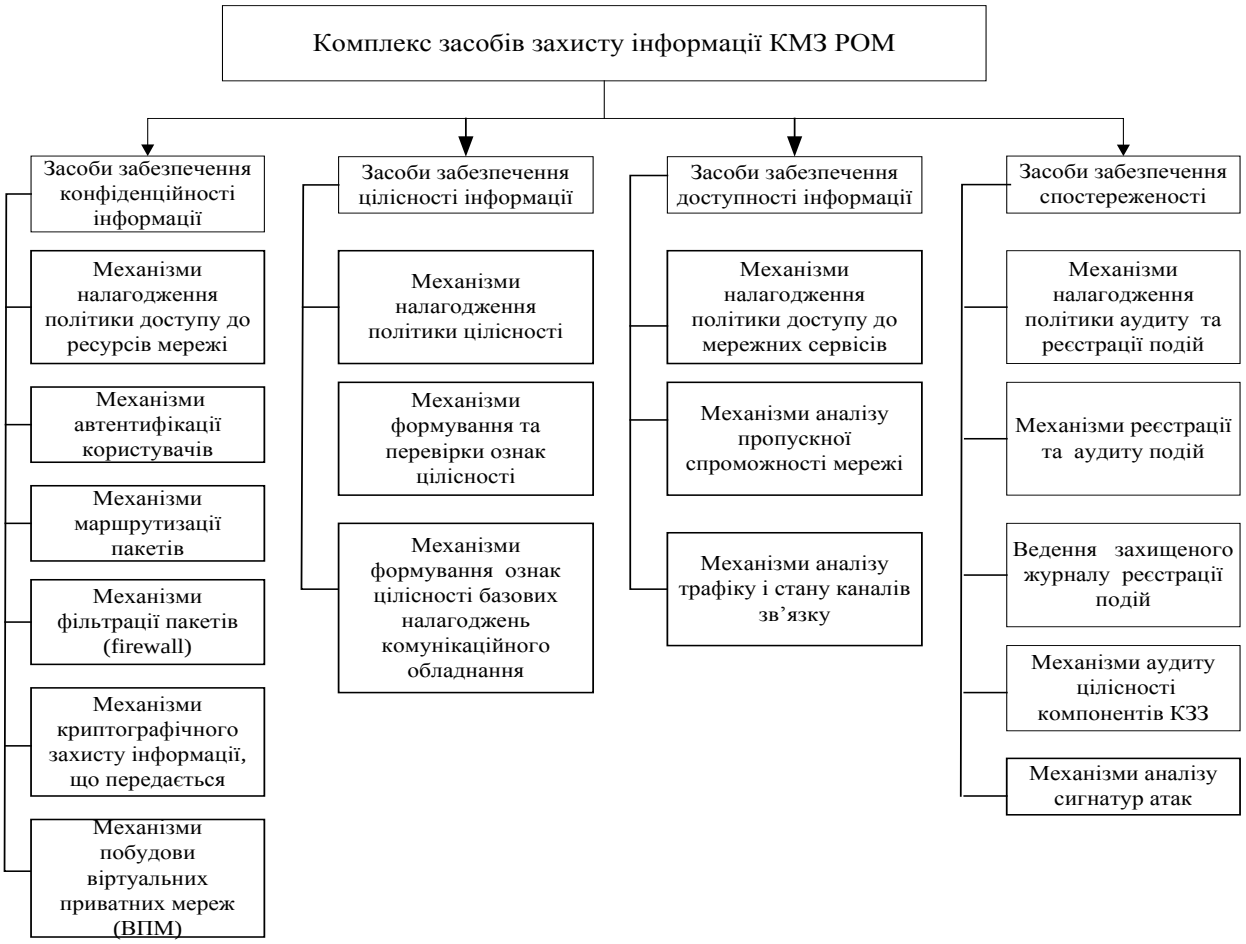

Рисунок 1 – Загальна структура засобів та механізмів захисту інформації КМЗ

Найбільш важливою частиною системи керування безпекою мережі є точна реалізація політики захисту мережі. Використання політики безпеки передбачає вибір, встановлення і налагодження відповідних засобів мережного захисту.

Політика захисту мережі має описувати технологію і процедури, що використовуються для моніторингу стану захисту системи. За допомогою моніторингу виявляються загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи і допомагає виконати аналіз атак. Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки. Він може включати аналіз повідомлень системних журналів маршрутизаторів периметра, брандмауерів і системи керування доступом.

Моніторинг може здійснюватися системою виявлення вторгнень. Сенсори системи виявлення вторгнень аналізують зміст окремих пакетів з метою виявлення наявності в мережному трафіку ознак (сигнатур) загрози або вторгнення. Якщо поведінка потоку даних є підозрілою, сенсори у реальному масштабі часу реєструють порушення політики безпеки і передають сигнал тривоги засобам управління інформаційною безпекою для своєчасного відключення порушника від мережі і недопущення подальшого розвитку атаки.

Політика захисту мережі має визначати процедури, що використовуються для аудиту, тестування і підтримки захисту мережі. Аудит і тестування можуть допомогти при визначенні загального технічного стану та вразливостей мережних компонентів і всієї системи в цілому.

Використання засобів аудита і тестування є найкращим способом перевірки ефективності існуючої інфраструктури системи захисту. В список задач, що виконуються в процесі аудита, мають включатися:

- перевірка кожної нової системи, що встановлюється в мережі;
- перевірка відповідності змін конфігурації мережних засобів діючій політиці безпеки;
- регулярні перевірки системи за допомогою додаткових автоматизованих засобів;

- позапланові перевірки стану системи захисту;
- щоденні перевірки найважливіших системних файлів і файлів системного журналу;
- контроль за активністю користувачів.

На основі результатів регулярних перевірок створюється загальна характеристика стану системи захисту. Такі перевірки можуть моделювати більшість варіантів проникнення порушників в систему. Також може бути виявлена і незаконна активність користувачів.

Позапланові перевірки можуть використовуватися для виявлення дій порушників, а також як тест для виявлення певних проблем захисту. Позапланові перевірки можуть використовуватися для контролю відповідності системи вимогам і стандартам політики безпеки.

Моніторинг і аудит можуть виявити слабкі місця системи захисту. На підставі результатів перевірок необхідно удосконалювати стан системи захисту, використовуючи останні поновлення програмних засобів, технічні рекомендації, нові версії існуючого програмного забезпечення, новітні технології. Безперервний контроль, супроводження і модифікація системи захисту забезпечує безпеку мережі. Основними напрямками вдосконалення системи є:

- регулярне відслідковування інформації про нові типи атак, точки вразливості;
- відслідковування інформації про нові технології захисту мереж і нових методів захисту обладнання і систем;
- своєчасне поновлення програмного забезпечення, "латок", сервісних пакетів;
- поновлення політики безпеки і методів захисту інформаційних активів;
- підготовка персоналу з питань захисту інформації;
- використання нових технологій захисту, що дозволяють забезпечити наскрізний захист потоку даних між кінцевими пунктами;
- забезпечення розслідування, координації дій, документального підтвердження і необхідного оповіщення про інциденти захисту.

Умовно можливо визначити наступні основні групи задач захисту, що реалізовані в КЗЗ КМЗ:

- захист периметра мережі вузлів РОМ;
- захист віддаленого доступу до ресурсів РОМ;
- захист ресурсів МВ РОМ;
- захист інфраструктури мережі;
- засоби антивірусного захисту мережних ресурсів вузлів;
- забезпечення надійного (безперервного) функціонування КЗЗ КМЗ.

IV Варіант захисту периметра мережі вузлів РОМ

Захист периметра мережі є складним комплексом технологічних рішень із захисту кордону мережі від вторгнень. Завданням захисту периметра є забезпечення безпечного зв'язку вузлів корпоративної мережі. Відсутність або слабкість захисту периметра мережі відкриває дірки в захисті, які можуть використовуватися порушниками. Система захисту периметра РОМ може бути побудована на базі архітектури екранованої підмережі, де перша лінія оборони будується за допомогою маршрутизатора периметра (екрануючий маршрутизатор), друга – на базі брандмауера Firewall.

*Маршрутизатори периметра мережі***.** Маршрутизатор повинен мати гнучкі засоби захисту периметра, що дозволить захистити зв'язок з корпоративною мережею і надати наступні можливості:

- створення першої лінії оборони, яка визначає демілітаризовану зону (ДМЗ), забезпечує захист бастіонних вузлів ДМЗ і брандмауера від спрямованих атак і виконує роль системи оповіщення при виявленні спроб зламати маршрутизатор периметра або бастіонний хост;
- гнучкий набір налагоджень, які можливо адаптувати до постійно виникаючих нових загроз захисту і новим сервісам;
- використання вбудованих можливостей захисту периметра.

Для обмеження доступу до сервісів і додатків TCP/IP маршрутизатор периметра має використовувати в основному правила фільтрування пакетів. Реалізацію правил, що обумовлюються вимогами політики мережного захисту, слід здійснювати за допомогою списків доступу. Можливості захисту включають автентифікацію користувачів, авторизацію доступу, обмеження зв'язку з вузлами, що мають невідомі або небажані адреси, маскування внутрішніх IP-адрес для зовнішніх спостерігачів, контроль потоку даних, що проходять через маршрутизатор, а також використання спеціальних засобів адміністрування, що дозволяють реалізувати вимоги політики захисту в системі захисту периметра мережі.

Управління сервісами TCP/IP. Програмне забезпечення маршрутизатора має включати спеціальні

команди управління сервісами TCP/IP, що дає можливість зменшити ризик підслуховування, проведення атак блокування сервісу і атак несанкціонованого доступу. За замовчуванням слід активізувати значний набір сервісів TCP/IP. Тому їх належить вимкнути вручну за допомогою команд управління сервісами.

Захист від несанкціонованих змін маршрутів. Маршрутизатори периметра вразливі відносно перехоплення повідомлень маршрутизації, що розкривають структуру ДМЗ і внутрішньої мережі. Є можливість вказати статичні маршрути, за якими повинні направлятися вхідний та вихідний трафіки маршрутизатора периметра, а також вказати наступний транзитний маршрутизатор в мережі постачальника послуг. Коли для зв'язку з іншими маршрутизаторами периметра необхідно використовувати протокол маршрутизації (для зв'язку з мережею зовнішніх систем або з іншими вузлами корпоративної мережі), можливостями об'яви маршруту можливо керувати за допомогою команд і стандартних списків доступу, а також шляхом автентифікації маршрутизаторів, що встановлюють зв'язок. Це забезпечує захист трафіка маршрутизації і виключає можливість фальсифікування параметрів маршрутизації.

Статичні маршрути. В маршрутизаторі периметра статичні маршрути використовуються для направлення всього трафіка на адресу маршрутизатора постачальника послуг. Відповідальність за подальшу пересилку пакетів відповідним адресатам покладається на маршрутизатор постачальника послуг. В цьому разі у маршрутизатора периметра не виникає необхідності динамічного обміну інформацією про маршрутизацію.

Контроль об'яви маршрутів. Протокол маршрутизації можливо використовувати для зв'язку між маршрутизатором периметра і маршрутизатором постачальника послуг або іншим маршрутизатором периметра корпоративної мережі. Фільтри маршрутів можливо встановити для будь-якого інтерфейсу, щоб не дозволити несанкціоноване розповсюдження інформації про маршрути. Протокол маршрутизації (наприклад, для маршрутизаторів Cisco – Enhanced IGRP) дозволяє використовувати фільтр, що заперечує об'яву певної частки маршрутів мережі. Протоколи маршрутизації дозволяють фільтрувати і вхідні маршрути, щоб маршрутизатор визнавав тільки ті маршрути, які належать надійним мережам.

Автентифікація маршрутів. Якщо для зв'язку між маршрутизаторами периметра використовується протокол маршрутизації, можливо використовувати автентифікацію маршрутів. Механізми автентифікації залежать від протоколу і є досить слабкими. Однак, автентифікація може збільшити надійність мережі через запобігання несанкціонованого втручання інших маршрутизаторів і хостів в процес маршрутизації незалежно від того, випадковим чи навмисним є таке втручання.

Керування доступом. Маршрутизатор є ефективним засобом управління доступом користувачів до мереж і даних при міжмережній взаємодії. Основним засобом управління доступом маршрутизатора є списки управління доступом. Програмне забезпечення маршрутизатора підтримує використання стандартних і поширених списків доступу. Списки доступу підтримують фільтрацію вхідних і вихідних пакетів. Управління доступом означає фільтрацію вхідного і вихідного трафіків, контроль адміністративного доступу до маршрутизатора периметра, використання захисту типу замка, а також опосередковану автентифікацію користувачів (проксі-автентифікацію).

Вхідний пакетний фільтр. Пакетний фільтр із списками доступу використовується для контролю вхідного трафіка маршрутизатора периметра. Типові правила політики контролю вхідного потоку даних, що проходять через периметр мережі, містять наступне:

- фільтрування пакетів, де як джерела вказані внутрішні адреси з метою захисту від атак фальсифікування IP-адрес;
- фільтрування пакетів, де як джерела вказані зареєстровані RFC-адреси з метою захисту від атак фальсифікування IP-адрес;
- дозвіл TCP з'єднань, що встановлюються із внутрішніх мереж з метою захисту від атак фальсифікування IP-адрес;
- заборона прямого сканування інтерфейсу із зовнішнього боку з метою захисту від атак розвідки;
- дозвіл вхідних з'єднань (електронної пошти) тільки із серверами ДМЗ з метою захисту від віддалених атак.

Вихідний пакетний фільтр. Пакетний фільтр із списками доступу використовується для контролю вихідного трафіка маршрутизатора периметра. Маршрутизатори периметра мають пересилати тільки IP-пакети з дозволеними IP-адресами джерел, щоб не дозволяти використання мережних пристроїв в розподілених атаках блокування сервісу, спрямованих проти інших мереж.

Типова політика захисту для вихідного трафіка забезпечує наступне: пропускає тільки пакети, які спрямовані в корпоративну мережу і, як адреси джерела, мають відповідні адреси (або трансльовані адреси) хостів внутрішньої мережі; пропускати тільки пакети (електронної пошти), які спрямовані в корпоративну мережу і, як адреси джерела, мають адресу бастіонного вузла; фільтрувати всі IP-адреси, що

недозволені встановленою політикою безпеки.

Захист від блокування сервісу. Маршрутизатори периметра мережі забезпечують першу лінію захисту від блокування сервісу. За допомогою маршрутизатора можливо звести до мінімуму вірогідність використання мережі в розподілених атаках блокування сервісу інших мереж. Використовуючи засоби TCP-перехоплення можливо обмежити вплив синхронних атак (SYN- атак).

Запобігання розподіленим атакам блокування сервісу. Для запобігання розподіленим атакам блокування сервісу необхідно: прийняти заходи для заборони несанкціонованому доступу до бастіонного хосту, щоб не дозволити розміщення на ньому програмного забезпечення, що використовується для здійснення розподілених атак блокування сервісу; заборонити всі сервіси IP, в яких немає необхідності; виключити можливість використання маршрутизатора в ході розподілених атак; фільтрувати весь вхідний трафік із приватними і зарезервованими адресами; фільтрувати весь вихідний трафік, щоб не дозволити фальсифікування IP-адрес джерела. За межі периметра мають пропускатися тільки пакети з адресами джерела їх ДМЗ і іншими дозволеними адресами; встановити обмеження швидкості для пакетів SYN; активізувати реєстрацію подій в пристроях периметра для своєчасного виявлення ознак проведення розподілених атак.

Засоби TCP-перехоплення. За допомогою засобів TCP-перехоплення програмного забезпечення маршрутизатора захищають TCP-сервери від лавинних (синхронних) атак (ЛА, SYN). Засоби TCP-перехоплення виявляють запити TCP-з'єднань TCP-клієнтів до TCP-серверів і, коли це необхідно, підтверджують або забороняють такі запити. Таким чином, засоби TCP-перехоплення можуть запобігти розвитку лавинної атаки. В режимі перехоплення відповідне програмне забезпечення перехоплює пакети синхронізації від клієнтів до серверів і перевіряє їх згідно з розширенням списком доступу. Засоби TCP-перехоплення забезпечує проксі-сервер, що генерує відповіді клієнту замість сервера і перевіряє право клієнта на встановлення зв'язку із сервером. У разі правомірності запиту клієнта, система TCP-перехоплення встановлює зв'язок із сервером від імені клієнта і забезпечує нормальний потік від джерела до адресата. При цьому засоби перехоплення продовжують перехоплювати і переправляти пакети за весь час існування з'єднання. В режимі моніторингу засоби TCP-перехоплення виконують пасивне спостереження за запитами на встановлення з'єднань. Система TCP-перехоплення переходить в агресивний режим у разі наявності ознак лавинних атак, коли кількість напіввідкритих з'єднань перевищує порогове значення. При цьому напіввідкриті з'єднання, що перевищили порогове значення, припиняються.

Засоби транслювання IP-адрес. Маршрутизатори периметра дозволяють розширити простір IP-адрес, сховати внутрішні IP-адреси і спростити адміністрування. Для цього маршрутизатори периметра використовують засоби трансляції мережних адрес (ТМА, NAT – Network Adress Translation) і трансляції адрес портів (ТАП, PAT – Port Adress Translation).

Засоби ТМА пропонуються маршрутизаторами периметра і брандмауерами з метою трансляції внутрішніх локальних IP-адрес в зовнішні глобальні адреси. Засоби ТМА використовуються для розширення відносно вузького простору IP-адрес, приховування IP-адреси внутрішньої мережі від зовнішніх спостерігачів, забезпечення виходу із внутрішньої мережі без урахування обмеженості глобальних адрес і проблем дублювання адрес.

Засоби ТМА можуть бути налагоджені на статичну або динамічну трансляцію адрес. При статичній трансляції внутрішні локальні адреси статично відображаються на внутрішні глобальні адреси. При динамічній трансляції з інтерфейсом зв'язується група внутрішніх глобальних адрес і маршрутизатор динамічно відображає внутрішні локальні адреси в доступні глобальні з тієї ж групи.

Множину внутрішніх адрес можливо транслювати в одну зовнішню за допомогою засобів ТАП (перевантаження засобів ТМА). Технологія трансляції адрес портів забезпечує можливість розширення IP-адрес: при використанні ТАП одна IP-адреса може представляти до 64000 хостів; засоби ТАП відображають різні номери портів TCP і UDP в одну IP-адресу; технологія ТАП забезпечує частковий захист – адреси клієнтів приховуються за допомогою однієї IP-адреси в маршрутизаторі периметра.

Реєстрація подій маршрутизатора периметра. Всі події маршрутизатора периметра реєструються і відповідні повідомлення направляються серверу syslog.

Демілітаризовані зони. ДМЗ або ізольована локальна мережа є буфером між вузлом і корпоративною мережею. ДМЗ має унікальний мережний адрес, який відрізняється від адрес вузла корпоративної мережі. ДМЗ – це єдина частка мережі вузла, яку можна побачити ззовні. ДМЗ створюється засобами захисту периметра, що формують систему брандмауера, яка складається з маршрутизатора периметра, бастіонного хосту і брандмауера. Маршрутизатор створює "брудну" ДМЗ, яка є частково захищеним середовищем бастіонного хосту, що забезпечує обслуговування зовнішніх і внутрішніх користувачів.

Бастіонний хост. Бастіонний хост є захищеним сервером, який розміщується в ДМЗ. Бастіонний хост має бути надійно захищеним, оскільки він відкритий для інших вузлів корпоративної мережі і є головною

точкою взаємодії вузла з корпоративною мережею. Бастіонний хост є також доступним для користувачів внутрішньої мережі вузла. Бастіонний хост виконує функції посередника і він повинен мати відомості щодо додатків, відносно яких він є посередником. Необхідно здійснювати моніторинг стану бастіонного хосту, щоб спроби його компрометування своєчасно ліквідовувались.

Брандмауери (Firewall). Брандмауер – це мережний пристрій, призначений для захисту внутрішньої мережі від зовнішніх атак. Брандмауер має наступні особливості:

- весь потік даних із внутрішньої мережі в зовнішню і навпаки має пройти через брандмауер;
- пропускається трафік, що пройшов авторизацію відповідно до локальної політики захисту;
- брандмауер налагоджується таким чином, щоб його захист неможливо було подолати;
- приховує внутрішню мережу від зовнішньої.

Одним із типів брандмауерів є PIX Firewall – брандмауер, який забезпечує надійний захист корпоративної мережі шляхом контролю стану з'єднань. Він надає широкі можливості захисту, повністю приховану архітектуру внутрішньої мережі від зовнішнього спостерігача.

Корисними особливостями брандмауера PIX Firewal є те, що він:

- використовує фільтр, враховуючи детальну інформацію про пакети даних. Для дозволу сеансу інформація про з'єднання має відповідати встановленій політиці безпеки;
- ускладнює можливість визначення порядкових номерів IP-пакетів, генерує їх за допомогою спеціального алгоритму рандомізації;
- працює під управлінням вбудованої операційної системи реального часу, яка не залежить від проблем захисту операційних систем серверів і робочих станцій; операційна система PIX Firewal посилена з точки зору захисту від мережних атак;
- адаптивний алгоритм захисту (ААЗ, ASA – Adaptive Security Algorithm) і сервіс наскрізного посередництва (cut-through proxy) надають брандмауеру можливість демонструвати високу продуктивність.

Брандмауер має наступні можливості захисту:

- вхідні з'єднання забороняються, якщо вони не є автентифікованими за допомогою спеціальної процедури або спеціально не дозволені;
- модель захисту є двохярусною; вона використовує маршрутизатор периметра, ДМЗ для загально доступних серверів, брандмауер PIX Firewal і маршрутизатор внутрішньої мережі;
- PIX Firewal використовує захищені канали для вхідних/вихідних статичних транзакцій;
- вихідні з'єднання при наявності списків глобальних адрес дозволяються, якщо вони не заборонені спеціально.

PIX Firewal дозволяє наступні варіанти проходження трафіка через брандмауер.

Адаптивний алгоритм захисту. Алгоритм ААЗ є базовим для функціонування брандмауера PIX Firewal. ААЗ записує характеристики з'єднань, зберігає цю інформацію в таблиці і використовує її для перевірки вихідних і вхідних пакетів з метою контролю за незмінністю "стану сеансу". При виявленні будь-яких змін пересилання даних зупиняється.

Після запиту на з'єднання ААЗ записує IP-адреси джерела і адресату, порти джерела і порядкові номери TCP, що пов'язані з інтерфейсом, по якому приходить запит. На основі цих даних створюється шифрований запис, який використовується брандмауером для того, щоб розпізнати відповідний хост в подальшому. Підпис дійсний тільки в проміжок часу існування даного з'єднання. Після закриття з'єднання підпис стає недійсним. При кожному новому запиті на з'єднання для хоста створюється новий підпис. Порушнику для подолання PIX Firewal і отримання доступу до хоста внутрішньої мережі необхідно імітувати роботу ААЗ і в реальному масштабі часу генерувати повноцінні пакети (з випадковими порядковими номерами TCP, відповідними IP-адресами і номерами портів) згідно з записами бази даних з'єднань ААЗ.

ААЗ має наступні можливості:

- жоден з пакетів, у яких інформація про з'єднання і стан не відповідає даним таблиці ААЗ, не в змозі пройти через брандмауер;
- дозволяються всі вихідні з'єднання і стани сеансів крім тих, що заборонені вихідними списками доступу;
- вхідні з'єднання і стани забороняються, якщо тільки вони спеціально не дозволені каналами;
- всі спроби обійти вказані правила відхиляються і серверу syslog посилається відповідне повідомлення.

Канали і статичні карти для вхідного доступу. Канали і статичні карти використовуються для представлення користувачам зовнішньої мережі (менш захищеної) доступу до ресурсів внутрішньої (більш захищеної) мережі, наприклад, при використанні ПВПМ (тунелів IPSec). Конфігурація брандмауера має спеціально дозволити трафік IPSec від зовнішньої мережі до внутрішньої, оскільки політика захисту брандмауера по замовчуванню забороняє весь вхідний трафік. Для дозволу руху даних IPSec через

брандмауер створюються канали і статичні карти. Статична карта відображає IP-адресу відкритого інтерфейсу сервера ПВПМ в зовнішню глобальну IP-адресу. Канал діє подібно списку доступу в маршрутизаторі, фільтрує трафік, статично дозволений трансляцією. Вибірковий дозвіл руху даних ПВПМ через брандмауер в захищеній частині мережі надає можливість серверу ПВПМ обробляти трафік ПВПМ незалежно від брандмауера. Розміщення сервера ПВПМ в захищеній частині мережі дозволяє захистити його від атак із зовнішньої мережі. При цьому засоби ААЗ брандмауера забезпечують повноцінний захист трафіка ПВПМ, що рухається відповідним каналом.

Наскрізна опосередкована автентифікація користувачів. Система наскрізної опосередкованої автентифікації брандмауера виконує початкову перевірку користувача на рівні застосування. Як тільки користувач ідентифіковано за допомогою сервера бази даних захисту (типу системи управління доступом до контролера термінального доступу (СУДКТД, TACACS+) або послуги ідентифікації віддалених об'єктів RADIUS), брандмауер починає використовувати інший підхід. Після автентифікації користувача і перевірки політики захисту брандмауер повертає з'єднання системі ААЗ на весь час супроводження стану сеансу TCP/IP. Система наскрізної опосередкованої автентифікації користувача дозволяє брандмауеру працювати значно швидше, ніж звичайні proxy-сервери, але не зменшує захист.

Рівні безпеки. Використання рівнів безпеки для інтерфейсів є основою захисту інфраструктури, через яку проходить важлива інформація. Не всі мережі однакові за своєю важливістю, і тому зв'язок між окремими мережами або їх сегментами може бути небажаним. Розподіл мереж на сегменти з різними рівнями безпеки надає можливість адміністраторам мережі визначити, які сегменти мережі мають більш високий ризик порушення захисту.

Для вихідного трафіка з внутрішньої мережі з рівнем безпеки 100 і спрямованого в зовнішню мережу з рівнем безпеки 0 використовується наступне правило: дозволяється весь трафік IP, не обмежений спеціально списками доступу, автентифікацією або авторизацією. Для вхідного трафіка із зовнішньої мережі з рівнем безпеки 0 і спрямованого у внутрішню мережу з рівнем безпеки 100 використовується наступне правило: відхиляються всі пакети, що недозволені спеціально. Додаткові обмеження на трафік можуть накладати процедури автентифікації і авторизації. Між двома мережами з однаковим рівнем безпеки зв'язок забороняється, крім спеціальних випадків.

Налагодження брандмауера. Для підключення до маршрутизатора або брандмауера при виконанні задач супроводження і налагодження найчастіше використовуються засоби віддаленого управління і моніторингу (ЗВУМ), наприклад, типу віддалений доступ (SSH). Брандмауер не дозволяє доступ ЗВУМ із зовнішнього інтерфейсу, тому всі завдання конфігурації мають вирішуватися за допомогою з'єднань із внутрішнього інтерфейсу. Крім того, доступ по ЗВУМ здійснюється з використанням паролю.

Віртуальні приватні мережі на базі протоколу управління безпекою IP мереж (ПУБІМ, – IPSec). Мережа ПВПМ (Virtual Private Network) є мережею, що розгортається в межах загальнодоступної інфраструктури і використовує можливості захисту, управління і політики якості сервісу. Протокол ПУБІМ є стандартом підтримки ПВПМ. ПУБІМ надає механізм захищеної передачі даних в IP-мережах, забезпечує конфіденційність, цілісність і достовірність даних, що передаються через незахищені мережі. ПУБІМ забезпечує наступні можливості ПВПМ:

- конфіденційність даних; відправник даних має можливість шифрувати пакети перед їх відправленням по мережі;
- цілісність даних; одержувач даних має можливість автентифікувати пристрої або програмне забезпечення, в яких починаються і закінчуються тунелі, і пакети, що надсилаються, щоб бути впевненим в тому, що дані не були змінені при передаванні;
- автентифікація джерела даних;
- захист від відтворення; одержувач має можливість виявляти і відхиляти відтворені пакети, не дозволяє фальсифікації і проведення атак посередника.

ПУБІМ діє на мережному рівні, забезпечує захист і автентифікацію IP-пакетів, що пересилаються між пристроями ПУБІМ: маршрутизаторами, брандмауерами, клієнтами і концентраторами ПВПМ. Засоби підтримки ПУБІМ дозволяють гнучке масштабування захищених мереж.

ПУБІМ надає стандартний спосіб автентифікації і шифрування з'єднань між сторонами ПУБІМ. В ПУБІМ використовуються відкриті стандарти узгодження ключів шифрування і управління з'єднаннями. Технологія ПУБІМ надає методи, що дозволяють сторонам ПУБІМ домовитися про узгодження використаних сервісів. Для узгодження параметрів використовуються асоціації захисту.

Асоціація захисту (АЗ, SA – Secutity Association) є узгодженою політикою або способом обробки даних, обмін якими передбачається між двома пристроями ПУБІМ. Діючі параметри АЗ зберігаються в базі даних асоціацій (Security Association Database) захисту сторін. Протокол IKE (Internet Key Exchange - обмін Internet ключами) є гібридним протоколом, який забезпечує спеціальний сервіс для ПУБІМ –

автентифікацію сторін ПУБІМ, узгодження параметрів асоціацій захисту ІКЕ і ПУБІМ, а також вибір ключів для алгоритмів шифрування. Протокол ІКЕ базується на протоколах управління асоціаціями і ключами захисту в мережі Internet, які використовуються для управління процесом створення і обробки ключів шифрування в перетвореннях ПУБІМ.

V Варіант захисту віддаленого доступу до ресурсів РОМ

Несанкціонований доступ, а також можливість фальсифікації і шахрайства в мережному середовищі надають порушнику змогу отримання доступу до мережного обладнання і мережних послуг із захисту. Тому для захисту мережних ресурсів РОМ від несанкціонованого доступу доцільно використовувати сервери доступу, що підтримують архітектуру ААА (автентифікація, авторизація, аудит) і дозволяють обмежити можливості порушників, але залишають право доступу до мережних ресурсів законним користувачам МВ РОМ.

Реалізація захисту також потребує використання *сервера захисту* віддаленої бази даних захисту з технологією автентифікації, авторизації, аудиту (*ААА*), системи управління доступом до контролера термінального доступу (СУДКТД, TACACS+) або послуги ідентифікації віддалених об'єктів (ПІВО, RADIUS). Використання технології ААА, сервера мережного доступу і сервера захисту (послуги ідентифікації віддалених об'єктів) забезпечить захист віддаленого доступу. Для надання сервісу ААА слід застосувати сервер мережного доступу, який використовує протоколи ААА.

Засоби ААА підтримують контроль доступу за допомогою або локальної бази даних на сервері доступу, або віддаленої бази даних захисту, що використовує протокол захисту ААА. Коли необхідно забезпечити доступ до мережі невеликої кількості віддалених користувачів через один-два сервери доступу, є можливість зберігати інформацію про їх імена і паролі на сервері доступу. Такий підхід називають локальною автентифікацією або автентифікацією за допомогою локальної бази даних захисту.

До особливостей використання засобами ААА локальної автентифікації слід віднести:

- застосування до малих мереж із невеликою кількістю віддалених користувачів і серверів мережного доступу;
- збереження імен користувачів і параметрів авторизації в локальній базі даних захисту на сервері мережного доступу;
- автентифікація і авторизація віддалених користувачів проходить за допомогою локальної бази захисту;
- обмежена підтримка авторизації і аудиту при використанні локальної бази даних захисту;
- зменшення витрат на встановлення і підтримку віддаленої бази даних шляхом контролю доступу за допомогою локальної бази даних захисту .

Віддалену базу даних захисту доцільно використовувати при великій чисельності серверів мережного доступу, що контролює доступ до мережі. Така база даних дозволяє централізовано керувати параметрами доступу (файлами профілів) віддалених користувачів, що виключає необхідність зміни файлів профілів кожного віддаленого користувача на всіх серверах мережного доступу. Віддалена база даних захисту допомагає створити та реалізувати узгоджену політику захисту віддаленого доступу для всіх користувачів мережних ресурсів.

До особливостей засобів ААА з віддаленою базою даних захисту слід віднести наступне:

- автентифікація за допомогою віддаленої бази даних захисту оптимальна для середніх і великих мереж із великою чисельністю віддалених користувачів і множиною серверів мережного доступу, коли витрати на утримання сервера захисту можуть бути виправдані;
- імена користувачів, паролі і параметри авторизації централізовано зберігаються в віддаленій базі даних захисту на сервері захисту;
- віддалені користувачі проходять процедури автентифікації і авторизації за допомогою віддаленої бази даних;
- авторизація і аудит підтримуються сервером мережного доступу з використанням віддаленої бази даних захисту;
- віддалена база даних може використовуватися для контролю доступу до сервера мережного доступу або до мережі через сервер мережного доступу; протоколи віддаленої бази даних захисту підтримують контроль доступу до маршрутизаторів, комутаторів і брандмауерів;
- централізований контроль за допомогою віддаленої бази даних захисту дозволяє зменшити витрати, виключає необхідність керувати кожним сервером мережного доступу окремо; для захисту віддаленої бази даних необхідно посилити захист хосту, на якому вона розміщується.

Для використання віддаленої бази даних захисту спочатку потрібно заповнити локальну базу даних захисту кожного сервера мережного доступу. Крім того, потрібно налагодити сервер мережного доступу та

інше мережне обладнання на взаємодію з віддаленою базою даних захисту при виконанні операцій AAA.

Основною перевагою використання віддаленої бази даних захисту є спрощення адміністрування і забезпечення узгодження реалізації політики безпеки відносно віддаленого доступу, доступу телефонними каналами зв'язку і керування маршрутизаторами за рахунок централізованого керування.

Існують декілька стандартів віддаленої бази даних захисту, що забезпечують уніфікований підхід до управління доступом у мережі СУДКТД і послуги ідентифікації віддалених об'єктів. Наприклад, сервери мережного доступу при взаємодії із серверами захисту СУДКТД і ПІВО є клієнтами TACACS+ і RADIUS.

VI Варіанти захисту інфраструктури мережі

Захист інфраструктури мережі передбачає захист адміністративного інтерфейсу мережного обладнання і контроль доступу до мережних пристроїв за допомогою відповідних протоколів (наприклад, Telnet, SNMP), а також захист файлів конфігурації в серверах з протоколами передачі файлів TFTP (Trivial File Transfer Protocol – простий протокол передачі файлів). Такі сервери доцільно використовувати для передачі бездисковим станціям ядра і початкової файлової системи та маршрутизаторам – конфігураційних файлів і спеціалізованих операційних систем. Оскільки всі ядра і файлові системи знаходяться на TFTP сервері (що реалізує протоколи передачі файлів), то зручно такий протокол створювати на DHCP сервері.

В свою чергу, DHCP-протокол (Dynamic Host Configuration Protocol) доцільно застосовувати для конфігурації TCP/IP хостів усередині мережі. При цьому DHCP-сервер вибирає відповідні параметри конфігурації (IP-адреси з відповідною маскою підмережі і іншими допоміжними параметрами, такими, як IP-адреса шлюзу за умовчанням, адреси DNS-серверів, імена доменів і т. д.), призначених для користувача станцій. DHCP-сервер призначає клієнтські IP-адреси всередині заданого діапазону на певний період (lease time).

Тоді конфігурація пристроїв, що забезпечують захист інфраструктури мережі, має забезпечити захист:

- фізичних пристроїв;
- адміністративних інтерфейсів;
- зв'язку між маршрутизаторами.

Захист фізичних пристроїв. Фізичний доступ до мережного обладнання може забезпечити порушнику можливість повного контролю над ним. Фізичний доступ до каналів зв'язку дає можливість перехоплювати повідомлення або відтворювати додаткові дані. Нема підстави встановлювати складні програмні засоби захисту, якщо не контролюється доступ до мережного обладнання або каналів зв'язку. Захист мережного обладнання має бути здійснено за допомогою:

- вибору правильної конфігурації обладнання і політики контролю;
- обмеження доступу до обладнання і забезпечення надійності його електроживлення та охолодження;
- контролю прямого доступу до всього мережного обладнання;
- забезпечення захисту каналів зв'язку;
- розробки плану відновлення системи у разі катастрофи.

Захист адміністративного інтерфейсу. Однією з головних точок атак порушників є адміністративний інтерфейс маршрутизаторів, серверів мережного доступу і брандмауерів. Якщо порушник отримує доступ до адміністративного інтерфейсу, він може визначити конфігурацію пристою, змінити її відповідно до своїх цілей і отримати право керування цим пристроєм або право доступу до інших елементів мережного обладнання, пов'язане з даним пристроєм. Захист адміністративного інтерфейсу включає:

- захист доступу до консолі;
- використання шифрування паролів;
- використання багаторівневої системи привілеїв доступу;
- використання інформаційних банерів пристроїв;
- керування віддаленим доступом (Telnet);
- керування доступом SNMP.

Захист доступу до консолі. Консоллю є термінал, що пов'язаний з мережним пристроєм через консольний порт. Захист консолі передбачає вимоги до ідентифікації користувачів шляхом введення паролю. В конфігурації мережних пристроїв, що встановлюється за замовчуванням, паролі консолі не призначаються. Тому необхідно встановити цей пароль за допомогою команд зміни конфігурації. Паролі можуть призначатися безпосередньо в мережному пристрої і контролюватися віддаленою базою даних захисту. Мережні пристрої можуть працювати в різних режимах: користувацькому або привілейованому. Спочатку користувач отримує доступ до консольного порту в користувацькому режимі. Якщо пароль рівня користувача (пароль початку сеансу) був встановленим, то користувач повинен ввести пароль. Для отримання доступу в привілейованому режимі необхідно ввести відповідний пароль. Привілейований

режим надає права доступу до режиму глобальної конфігурації, що дозволяє змінити конфігурацію мережного пристрою. Для привілейованого режиму можливо встановити різні рівні привілеїв команд і різні рівні адміністрування.

Шифрування паролів. За замовчуванням всі паролі консолі і віддаленого доступу зберігаються у відкритому вигляді і є вразливими. Крім того, їх можливо перехопити під час сеансу віддаленого доступу при введенні пароля привілейованого доступу або перегляду конфігурації за допомогою команд привілейованого режиму. Паролі є вразливими і при зберіганні конфігурації на сервері TFTP. Існує можливість зберігати паролі конфігурації в зашифрованому вигляді. Шифрування стосується всіх паролів: користувачів, ключів автентифікації, привілейованих команд доступу до консолі.

Налагодження параметрів каналу зв'язку. Якщо консоль або сеанс зв'язку віддаленого доступу залишається без контролю в привілейованому режимі, то будь-який користувач може змінити конфігурацію мережного пристрою. Є можливість встановити обмеження на час відкритого стану каналів несупроводжуваних сеансів зв'язку і тим самим забезпечити додатковий ступінь захисту.

Використання багаторівневої системи привілеїв. Командам кожного з режимів роботи мережного пристрою (користувацького і привілейованого) є можливість призначити до 16 ієрархічних рівнів, що дозволяє делегувати адміністративні повноваження. Команди конфігурування пристрою можливо зв'язати з будь-яким рівнем, що дозволяє забезпечити достатньо широкі можливості керування доступом користувачів. За допомогою множини паролів можливо дозволити різним групам користувачів доступ до різних наборів команд. Рівень привілеїв задається за допомогою команд глобальної конфігурації.

Використання інформаційних банерів пристроїв. Є можливість використовувати банерні (рекламні) повідомлення, які інформують користувачів про права доступу (дозволено або недозволено) до мережних пристроїв при спробах реєстрації входу в систему. Банерні повідомлення можуть супроводжувати спроби входу в привілейований режим, активізацію каналу зв'язку, встановлення зв'язку з віртуальним терміналом.

Керування віддаленим доступом (доступ Telnet). Основною можливістю захисту мережного пристрою є керування доступом Telnet. При спробі доступу до пристрою за допомогою віддаленого доступу користувач отримує запрошення на реєстрацію в користувацькому режимі.

Керування доступом з використанням засобів збору і передачі службової інформації (status information) між різними комп'ютерами (SNMP). Ці засоби можуть використовуватися порушником для проникнення в мережу, коли вони не налагоджені. Для захисту інфраструктури мережі важливо контролювати доступ SNMP. Протокол SNMP дозволяє різні рівні доступу: доступ на читання дозволяє читати бази MIB; доступ читання/запису дозволяє як читати, так і записувати дані; доступ запису – тільки записувати дані. SNMP є простим протоколом керування мережею, що являє собою протокол прикладного рівня і забезпечує зв'язок між диспетчерами (NMS) і агентами SNMP.

Захист зв'язку між маршрутизаторами. Зв'язок між маршрутизаторами можливо використовувати для прослуховування, маніпулювання даними, відтворення сеансів зв'язку і зміни параметрів маршрутизації. Захист зв'язку між маршрутизаторами може бути забезпечений шляхом:

- автентифікації протоколу маршрутизації;
- захисту файлів конфігурації маршрутизатора;
- застосування політики захисту, що передбачає контроль потоку даних;
- керування доступом через протоколи обміну гіпертекстовою інформацією (HTTP) до маршрутизатора.

Автентифікація протоколу маршрутизації. Протоколи маршрутизації вразливі щодо прослуховування і фальсифікації поновлень маршрутизації. Існує можливість автентифікації поновлень маршрутизації, щоб виявити несанкціоновані або фальсифіковані повідомлення маршрутизації від незнайомих джерел. Автентифікація протоколу маршрутизації називається також автентифікацією сусіднього вузла. Якщо в маршрутизаторі передбачена автентифікація сусіднього вузла, то він виконує автентифікацію джерела для всіх пакетів поновлень маршрутизації. Для цього використовується процедура обміну ключами автентифікації або підписами, що налагоджуються в маршрутизаторах як в таких, що відправляють, так і у таких, що отримують.

Захист файлів конфігурації маршрутизатора. Коли маршрутизатор використовує файли конфігурації із сервера TFTP (що реалізує протоколи передачі файлів), то будь-хто, хто має доступ до такого сервера, може змінити файли конфігурації маршрутизатора. Обмін файлами TFTP є вразливим відносно їх перехоплення на шляху між клієнтами і сервером TFTP. Необхідно забезпечити надійний захист серверів TFTP, на яких зберігаються файли конфігурації маршрутизаторів, шляхом обмеження доступу до них. Доступ до серверів TFTP, які використовуються для збереження і завантаження файлів конфігурації за протоколом SNMP, можливо обмежити за допомогою списків доступу.

Політика контролю потоку даних. Списки доступу мають бути налагоджені згідно з політикою захисту мережі відносно контролю трафіка:

- дозволяється весь вихідний трафік;
- дозволяти вхідний трафік, який встановлений в середині мережі, щоб заборонити можливість фальсифікування адрес;
- дозволяти вхідні відповіді на встановлений вихідний трафік;
- заборонити будь-який інший вхідний трафік і реєструвати всі спроби несанкціонованого доступу.

Керування доступом HTTP до маршрутизатора. Програмне забезпечення маршрутизатора для спрощення процесу налагодження передбачає використання серверу HTTP. Але це відкриває нові дірки в системі захисту. Тому за замовчуванням сервер HTTP має бути вимкнутим. Для керування доступом до сервера HTTP можливо використовувати список доступу або автентифікацію користувачів сервера (локальну або віддалену базу даних захисту) за допомогою протоколів СУДКТД, або послуги ідентифікації віддалених об'єктів.

VII Варіант антивірусного захисту мережних ресурсів РОМ

Розвиток технологій інформаційного обміну неминуче зіштовхується з проблемою проникнення вірусів у комп'ютерну систему. Усього лише одна шкідлива програма може завдати серйозної шкоди інформаційній безпеці мережі. Установка ефективного і надійного антивірусного комплексу дозволить уникнути втрат інформації.

Для вирішення питань антивірусного захисту мережних ресурсів РОМ, як варіант, може використовуватися Антивірус Касперського Business Optimal, спеціально розроблений для боротьби з вірусами всіх типів у корпоративних мережах середнього і малого масштабу. Антивірус Касперського Business Optimal дозволяє створити систему антивірусної безпеки, що максимально відповідає конфігурації мережі вузлів РОМ, захищає вузли мережі і створює надійний бар'єр проти вірусних атак.

VIII Висновки

Таким чином Забезпечення надійного функціонування пристроїв захисту мережних ресурсів є однією з важливих задач при побудові КЗЗ КМЗ. Одним із основних засобів для захисту КМЗ є міжмережний екран (брандмауер). Відмова брандмауера призведе до розриву з'єднання між внутрішньою та зовнішньою мережами. Це питання має особливе значення для вузла ЦР РОМ тому, що в цьому разі централізована база даних буде ізольована від інших рівнів РОМ і функціонування системи в цілому буде зупинено до відновлення роботоспроможності брандмауера.

Для забезпечення надійності функціонування РОМ в захищеному режимі пропонується використовувати механізм повного відновлення стану брандмауера типу Cisco PIX (режим резервування брандмауера), який є доступним, наприклад, в брандмауерах Cisco PIX 515. Механізм повного відновлення стану (failover) забезпечує безперервну роботу такого брандмауера у разі виникнення збоїв в його роботі. Сутність цього механізму полягає в тому, що при відмові одного брандмауера його функції починає виконувати резервний брандмауер. Таким чином, для реалізації режиму повного відновлення необхідно використовувати два брандмауери: основний (primary) і резервний (secondary). У нормальному режимі основний брандмауер виконує функції активного брандмауера. Резервний брандмауер знаходиться в режимі очікування і є спроможним у будь-який момент взяти на себе функції активного брандмауера у разі виникнення збоїв в роботі основного брандмауера.

*Література: **1**. Буточнов О. М., Гончар Г. В., Деревянко С. М., Короленко М. П. Захист інформації в комунікаційній мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 − 58; **2**. Матов О. Я., Василенко В. С., Будько М. М. Оцінка захищеності в локальних обчислювальних мережах. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 59 − 73; **3.** НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу"*