УДК 004.056.5 (076.5)

Б.Я. Корнієнко, канд. техн. наук

О.К. Юдін, канд. техн. наук
Л.П. Галата

АНАЛІЗ ТЕХНОЛОГІЙ МІЖМЕРЕЖНИХ ЕКРАНІВ

НАУ, кафедра комп'ютеризованих систем захисту інформації
E-mail: kszi@ukr.net

Для дослідження властивостей і забезпечення захисту інформації в телекомунікаційних мережах та інформаційних системах проведено порівняльний аналіз технологій міжмережних екранів. Розглянуто три технології міжмережних екранів: на основі загальнодоступних безкоштовних джерел програмного забезпечення, комерційне програмне вирішення, апаратно-програмне вирішення. Результати досліджень подано в таблицях.

With the purpose of research of properties and maintenance of protection of the information in telecommunication systems and information systems is lead the comparative analysis of technologies of firewalls. Three basictechnologies of firewalls are considered: on the basis of popular free-of-charge sources of program maintenance, commercial program decisions and hardware-software decisions. Results of researches are presented in tables and conclusions.

Постановка проблеми

Високу актуальність у разі підключення будь-якої закритої комп'ютерної мережі до відкритих мереж, наприклад, до мережі Internet набувають загрози несанкціонованого вторгнення в закриту мережу з відкритої, а також загрози несанкціонованого доступу з закритої мережі до ресурсів відкритої. Тому проблема захисту від несанкціонованих дій при взаємодії з зовнішніми мережами успішно може бути вирішена за допомогою спеціалізованих програмно-апаратних комплексів, що забезпечують цілісний захист комп'ютерної мережі від ворожого довкілля. Такі комплекси називають міжмережними екранами.

Мета дослідження – порівняльний аналіз технологій міжмережних екранів для забезпечення захисту інформації в телекомунікаційних мережах та інформаційних системах.

Існує три варіанти створення брандмауерів:
– на основі загальнодоступних ("open source") безкоштовних джерел програмного забезпечення;
– комерційне програмне вирішення;
– апаратно-програмне вирішення.

Загальнодоступне програмне забезпечення для створення брандмауерів

Серед існуючих загальнодоступних брандмауерів завжди можна знайти такі рішення, які задовольняли б вимоги щодо рівня безпеки, були відкриті для постійних доробок і розвитку та мали б надійну підтримку [1].

Серед загальнодоступного програмного забезпечення можна назвати такі продукти:
– пакет TCP Wrappers;
– пакет Trusted Information Systems Internet Firewall Toolkit (FWTK);
– протокол SOCKS;
– сервер SQUID;
– пакет Drawbridge.

Пакет TCP Wrappers застосовується для керування доступом до стандартних служб TCP і UDP, що запускаються на вузлі мережі або міжмережному екрані. Хоча домен пакета TCP Wrappers нездатний цілком задовольнити потреби в захисті мережі, він виявляється корисним, особливо завдяки наданим їм можливостям аудита.

Пакет FWTK – це набір компонентів, що застосовується для створення міжмережного екрана на комп'ютері з укріпленою системою UNIX, який розташований на межі мережі.

Пакет FWTK дозволяє сформувати міжмережний екран, що забезпечує роботу всіх стандартних мережних служб.

Крім того, proxy-сервер plug-gw полегшує взаємодію через міжмережний екран клієнтських і серверних додатків, для яких не існує стандартного proxy-сервера.

Протокол SOCKS призначений для встановлення з'єднань через міжмережний екран.

Протокол SOCKS дозволяє вузлам, розташованим по різні бокі сервера SOCKS, взаємодіяти один з одним, забезпечує аутентифікацію і блокує передачу IP-пакетів між ними.

Сервер SQUID – proxy-сервер, що функціонує на платформі UNIX застосовується або як окремий сервер, або в складі ієрархії інших серверів SQUID.

Пакет Drawbridge – продуктивний пакетний фільтр, спочатку написаний для платформи DOS, а потім працюючий під FreeBSD.

Пакет Drawbridge містить три основні компоненти [2]:
– механізм фільтрації;
– компілятор фільтрів;
– менеджер фільтрів.

У разі програмного вирішення пропонований виробником продукт цілком складається з програмного забезпечення. Щоб проаналізувати ситуацію в сфері програмного забезпечення брандмауерів, наведемо порівняльний огляд деяких продуктів.

McAFEE Desktop Firewall 7.5 + EPO

Компанія Network Associates запропонувала потужне рішення, що складається з персонального брандмауера McAfee Desktop Firewall і єдиного центру керування ePolicy Orchestrator, яке дозволяє адміністраторам безпеки автоматично роз-гортати і централізовано керувати цілими мережами з персональних брандмауерів, установлених на робочих станціях на основі груп політик безпеки. Перший запуск персонального брандмауера відбувається в режимі «навчання», коли будь-який запит на з'єднання з Інтернет будь-якого додатка на робочій станції блокується до моменту дозволу такого з'єднання користувачем. Існує механізм оповіщення про напад (Mcafee's Alert Manager), що дозволяє передавати таку інформацію з використанням широкомовних пакетів, протоколу SNMP, пейджерів або електронних листів. Програмне забезпечення Orchestrator керує всією системою.

Агенти передають на Orchestrator значний обсяг інформації про свою діяльність, що дозволяє одержувати вичерпну інформацію про функціонування всієї системи безпеки цілком або кожного персонального брандмауера окремо.

Zone Labs Integrity 1.5

У системі безпеки Integrity використовується технологія «stateful» інспекції пакетів. Агент Integrity, установлений на кожній робочій станції, одержує політики безпеки від центрального сервера системи. Система Integrity для ідентифікації користувачів використовує ідентифікацію домена Windows і дозволяє імпортувати користувачів і групи користувачів.

Утиліта Policy Studio використовується для того, щоб визначити правила (політики) безпеки та ґрунтується на рівнях і зонах захисту при доступі до різних мереж. Основна особливість системи – безперервність захисту.

Symantec Enterprise Firewall 6.5

Завдяки унікальній гібридній архітектурі міжмережний екран забезпечує високий ступінь захищеності й одночасно відрізняється підвищеною швидкодією.

Symantec Enterprise Firewall (раніше Raptor Firewall) може бути використаний для подовження периметра корпоративної мережі за рахунок економічного й безпечного підключення віддалених філій і дистанційних користувачів, що досягається в результаті повної інтеграції з окремим стандартним продуктом Symantec Enterprise VPN (раніше відомим як POWERVPN) і персональним міжмережним екраном.

Продукт підтримує широкий спектр способів перевірки достовірності (в т.ч. Radius, цифрові сертифікати, LDAP, перевірку достовірності користувачів домена Windows NT). Symantec Enterprise Firewall призначений для платформ Windows NT, Windows 2000 і Solaris.

Адміністратор має можливість із центральної консолі задавати правила безпеки для локальних і віддалених мережних екранів, а також одержувати різні звіти про керування системою і журнали, які реєструють події, пов'язані з її безпекою.

FireWall-1

Комплекс модулів, що складають ядро будь-якої системи безпеки на продуктах CheckPoint, крім функцій міжмережного екрана на основі запатентованої технології Stateful Inspection, підтримує аутентифікацію користувачів, трансляцію адрес, контроль доступу за змістом та аудит, містить систему централізованого керування на основі правил політики, що може керувати роботою модулів FireWall-1 і продуктів VPN-1, FloodGate-1.

VPN-1 – набір продуктів для організації віртуальних приватних мереж як з боку центральної мережі, так і з боку віддалених користувачів.

RealSecure – засоби виявлення вторгнень у реальному часі. Експертна база атак становить більш 160 зразків.

Засоби керування якістю обслуговування FloodGate забезпечують гнучкий розподіл смуги пропущення для різних класів трафіка, а також окремих з'єднань.

Система керування інфраструктурою IP-адреса підприємства MetaIP інтегрує служби DHCP, DNS і аутентифікації, доповнюючи їхнім власним сервісом UAM відображення імен користувачів на IP-адреси.

BorderManager Enterprise Edition

BorderManager створює міжмережний екран (продукт фірми Novell), що захищає важливу інформацію як від атак із середини, так і ззовні мережі організації.

За допомогою BorderManager можна організувати віртуальні приватні мережі та захищений віддалений доступ до мережі.
Важливою перевагою BorderManager є можливість керування більшістю його підсистем через службу каталогів NDS у мережах:
– NetWare;
– Windows NT;
– UNIX.
Міжмережний екран BorderManager підтримує різні режими фільтрації пакетів на мережному рівні.
За допомогою шлюзів сеансового рівня (IPX/IP і IP/IP) контролюється міжмережний доступ на рівні користувачів, груп користувачів, NDS, IP/IPX-адрес комп'ютерів, підтримується широкий спектр посередників додатків, що забезпечують контроль доступу на рівні прикладних сервісів:
– HTTP разом з HTTPS і SSL;
– FTP;
– SMTP/POP3;
– DNS;
– SOCKS 4;
– SOCKS 5.
BorderManager Enterprise Edition складається зі служб:
– брандмауера (BorderManager Firewall Services);
– аутентифікації (BorderManager Authentication Services);
– віртуальних приватних мереж (BorderManager VPN Services).

Black Hole 3.0

Black Hole – повномасштабний шлюз-посередник, що взаємодіє зі всіма популярними додатками Internet, включаючи такі засоби обробки захищених транзакцій, як SNews і HTTPS.
Black Hole здійснює підтримку мереж VPN, посиленого ядра Unix BSD (Berkeley Software Distribution) та екранування адрес URL. Крім того, цей брандмауер підтримує такі потокові мультимедіа-додатки, як RealAudio і VDOLive, містить узагальнені уповноважені посередники TCP і UDP, що дозволяють визначати доступ для нових додатків і он-лайнових служб, а також засоби протоколювання й аудиту.
Black Hole – повністю двонапрямлений брандмауер, який виконує аутентифікацію як вхідного, так і вихідного трафіку.
Для захисту адресації в мережі цей продукт працює з роздільними системами DNS і NAT.
Black Hole використовує для локального адміністрування брандмауера систему X Window.
Продукт Black Hole підтримує VPN, включаючи автоматичне розповсюдження цифрових сертифікатів.

CyberGuard Firewall 3.0

Брандмауер CyberGuard Firewall відрізняється потужним набором засобів і надійним захистом. Цей пакет пропонує розширені можливості настроювання конфігурації і фільтрації додатків і працює в «посиленій» версії SCO UnixWare.
Унікальним засобом цього продукту є MVSE (Multiple Virtual Secure Environment), яке дозволяє реалізувати в одній фізичній мережі декілька захищених каналів.
CyberGuard реалізує комбінацію методів фільтрації. Для моніторингу ви-хідного трафіку CyberGuard застосовують фільтр пакетів, який перевіряє коректність протоколів, фільтри додатків, які містять функції шлюзу каналів, забезпечуючи пропускання через брандмауер тільки потрібних запитів.
Наявність файлів повідомлень і журналів – одна з переваг CyberGuard. CyberGuard підтримує VPN, включаючи автоматичне розповсюдження цифрових сертифікатів.
Захищений канал шифрується за допомогою алгоритму DES з 56-розрядним ключем або патентованого алго-ритму під назвою Atlas.

Tiny Personal Firewall

Програмний продукт Tiny Personal Firewall (TPF), призначений для захисту від атак типу "троян" за допомогою функції аутентифікації додатків відповідно до протоколу MD5, реалізує три рівні безпеки:
– Don't bother me;
– Ask me first;
– Cut me off.
Вікно Advanced Firewall Configuration надає доступ до всіх правил, а також можливість створювати власні.
У Tiny Personal Firewall існують функції фільтрації веб-трафіку та електронної пошти, ведення звітів, а також реалізована підтримка віртуальних приватних мереж VPN.
Вхідний трафік контролює наявність вірусів.

Norton Internet Security

До складу одного з лідерів програмних міжмережних екранів Norton Internet Security (NIS) належать Norton Personal Firewall, Norton AntiVirus, модуль Parental Control для блокування доступу до заборонених веб-вузлів і модуль захисту конфіденційності Privacy Control.
Цей досить «інтелектуальний» брандмауер здатний розпізнати найбільш поширені програми

й автоматично конфігурувати правила доступу до них.

Розвинені функції захисту від шкідливих Java- і ActiveX-додатків NIS дозволяють забезпечити анонімний веб-серфінг шляхом блокування cookies і http-ref. Для кожного модуля (антивіруса, брандмауера, модуля захисту конфіденційності та батьківського контролю) можна вибрати один з чотирьох режимів:
–Automatic;
– Permit all;
– Block all;
– Custom.

Black Ice Defender

Black Ice Defender забезпечує додатковий рівень захисту, надаючи користувачам докладні відомості про спроби несанкціонованого доступу до персонального комп'ютера (ПК) або мережі.
Black Ice Defender виявляє підозрілі дії після того, як дані пройшли через брандмауер. Для цього програма відстежує характер операцій обміну інформацією. Black Ice Defender має в своєму розпорядженні базу даних, що містить сигнатури і шаблони відомих хакерських прийомів. У разі виникнення підозр зв'язок між ПК і небезпечною IP-адресою блокується.
Black Ice Defender дозволяє ідентифікувати користувачів, що намагаються встановити зв'язок із ПК і визначити їх наміри. Якщо хакер спробує «обстежити» ПК, то Black Ice Defender виявить пошукові операції, блокує доступ до ПК з IP-адреси хакера і сповістить користувача.

Agnitum Outpost Firewall Pro

Програмний продукт Agnitum Outpost Firewall Pro_3 призначений для захисту від шкідливих програм та атак з Інтернет, фільтрує увесь вхідний та вихідний трафік, захищає від несанкціонованих дій зловмисників. Переваги Outpost Firewall Pro такі:
– модуль «Anti-Spyware» захищає від програм-шпигунів та крадіжки персональних даних;
– монітор «Мережна активність» забезпечує постійний контроль за активністю системи;
– модуль «Інтерактивні елементи» забезпечує конфіденційність при роботі в мережі;
– контролюється взаємодія додатків;
– аналізуються можливі загрози.
Отже, сучасний програмний міжмережний екран – це складна модульна система, що здебільшого не може бути надійно налаштована тільки за допомогою типових програм – «майстрів». Тому сумарні витрати на її розгортання будуть складатися з вартості комплекту модулів і робіт зі встановлення і настроювання.
Вирішення «під ключ» пропонує брандмауер – систему, що складається з програмного забезпечення та апаратного обладнання.
Апаратні брандмауери мають одну істотну перевагу перед програмними – вони утворюють повний комплекс (програмне забезпечення й апаратну платформу, оптимізовану для вирішення задачі міжмережного екранування), що дозволяє здійснювати захист на високому рівні.

Cisco PIX 520

Перше підключення до спеціалізованого пристрою відбувається за допомогою утиліти – майстра конфігурації, за допомогою якого призначаються IP-адреси інтерфейсів, трансляція мережних адрес (NAT), Web і mail сервера. Від виробника брандмауер у базовій конфігурації поставляється з двома мережними інтерфейсами типу Fast Ethernet, однак ця конфігурація може бути змінена шляхом інсталяції додаткових dual-port NICs або VPN акселератора, які можна придбати окремо.
Адміністратор задає імена двом інтерфейсам. За замовчуванням це «inside» і «outside». Отже, реалізується класична схема міжмережного захисту. Правила фільтрації ґрунтуються на аналізі трафіка між цими двома інтерфейсами. Додатково до функцій міжмережного екрана PIX 520 також може здійснювати URL-фільтрацію і виявлення атак (Intrusion Detection). Висока продуктивність фільтрації дозволяє використовувати брандмауер на рівні підприємства [3].

WatchGuard FireBox 4500

Потужний брандмауер WatchGuard FireBox 4500 компанії WatchGuard на базі комп'ютера AMD працює під керуванням ПЗ WatchGuard. Брандмауер має три мережних інтерфейси Fast Ethernet – внутрішню, зовнішню і демілітаризовану зони.
Перший запуск після інсталяції програмного забезпечення починається з виконання майстра конфігурації брандмауера, що повідомляє міжмережному екранові первинну конфігурацію.
Після виконання майстра конфігурації адміністратор одержує доступ до консолі керування
брандмауером.
Консоль керування має два різні компонента:
– моніторинг стану;
– конфігурацію.
Компонент конфігурації – це програмне забезпечення, на якому безпосередньо здійснюється настроювання правил фільтрації. Ряд сервісів має додаткові критерії фільтрації. Наприклад, сервіс HTTP дозволяє використовувати URL-фільт-

рацію, а також блокувати потенційно небезпечний вміст.

Firebox 4500 забезпечує трансляцію мережних адрес (NAT) для приховання топології внутрішньої мережі.

Додатковий захист забезпечується за рахунок використання VPN, що у цій моделі має апаратний криптоприскорювач. Продуктивність брандмауера значна. Збільшення навантаження ніяк не позначається на швидкості обробки трафіка. Тільки, починаючи з 10 000 сесій за 1 с, завантаження процесора стає помітним. Максимальне завантаження приладу досягається на рівні 65 000 сесій за 1 с.

Symantec VelociRaptor 1100

Після придбання компанії Axent Technologies Symantec змінив зовнішній вигляд брандмауера. Програмне забезпечення брандмауера має дві версії: з алгоритмом DES і 3DES.

Після інсталяції адміністраторові стає доступною досить зручна консоль керування. Майстер первісного настроювання дозволяє призначити правила фільтрації для Web і e-mail, а також всі основні параметри мережі.

Адреси внутрішньої мережі автоматично транслюються на публічну адресу брандмауера.

Кожен мережний інтерфейс має засоби визначення атак типу Syn flooding, IP spoofing і сканування портів.

SonicWall Pro 300

Модель Pro 300 компанії SonicWall – це брандмауер масштабу підприємства. Усі міжмережні екрани SonicWall будуються на базі спеціального процесора CyberSentry Security Processor, що забезпечує апаратне прискорення для віртуальних приватних мереж. Прилад має три порти Fast Ethernet, що «жорстко» вбудовані в конфігурацію Lan, Wan, DMZ. Pro 300 через свою конфігурацію має єдине місце застосування – шлюз на межі локальної і глобальної мереж.

Пакет програм Global Management System (GMS) використовується для дистанційного керування будь-яким брандмауером SonicWall.

Крім функцій брандмауера є додаткові засоби фільтрації, антивірусний сканер. На додаток до stateful-фільтрації брандмауер має сервер аутентифікації користувачів і функцію трансляції мережних адрес (NAT).

Для цієї моделі брандмауера максимально можливо 30720 одночасних сесій.

SonicWall може обробити до 1000 сесій за 1 с, але це викликає уповільнення швидкодії.

Отже, апаратні брандмауери – це готовий апаратно-програмний комплекс, в якому всі компоненти вже встановлені і по можливості налаштовані. Такі брандмауери поставляються з вбудованим програмним забезпеченням і прив'язані до апаратної платформи, що спрощує їхнє встановлення і настроювання порівняно з суто програмними вирішеннями.

Це вирішення найкраще підходить для тих організацій, яким потрібно кілька брандмауерів, керованих з одного центрального пункту.

Для досліджень міжмережні екрани були розділені на дві групи:

– міжмережні екрани для робочих станцій та невеликих локальних мереж;

– міжмережні екрани для корпоративних мереж.

За результатами досліджень була дана інтегральна оцінка за наявності функціональних властивостей кожного міжмережного екрану.

Хоча безпека доступу до Internet вважається однією з головних проблем, через які багато компаній побоюються розширювати свою наявність у мережі, вже доступні досить недорогі та дієві інструменти забезпечення захисту, накопичений великий досвід їхнього ефективного використання. Під час вибору міжмережного екрана для організації важливо пам'ятати, що будь-яка версія такої системи вимагає постійної професійної уваги.

Порівняльні характеристики міжмережних екранів наведено у табл. 1, 2, 3.

Таблиця 1

Інтегральна оцінка функціональних властивостей міжмережних екранів (за п'ятибальною шкалою)

Критерій оцінок	Zone Alarm Pro 4.0	McAfee Desktop Firewall 7.5	Black Ice Defender 3.6	Norton Internet Security 2005	Tiny Personal Firewall 6.5.110	Agnitum Outpost Firewall 2.1
Інсталяція	4	5	5	5	4	4
Простота застосування	3	4	4	4	3	5
Адаптованість	5	4	3	4	4	5

Функції брандмауера	3	5	4	5	3	4
Додаткові функції захисту	0	5	0	4	2	5
Загальна оцінка	4	5	4	5	3	5

Таблиця 2

Характеристика міжмережних екранів для робочих станцій і локальних мереж

Критерій	Zone Alarm Pro 4.0	McAfee Desktop Firewall 7.5	Black Ice Defender 3.6	Norton Internet Security 2005	Tiny Personal Firewall 6.5.110	Agnitum Outpost Firewall Pro 2.1
"Майстер" настройки конфігурації	–	+	–	–	–	+
Вибір рівнів безпеки	+	+	+	+	+	+
Створення правил безпеки	+	+	-	+	+	+
Переустановлені правила: для системного трафіку	+	+	+	+	-	+
для додатків	+	+	–	+	-	+
Інформація про активні порти і прикладні програми	+	+	–	+	+	+
Демілітаризована зона або довірені IP	+	–	+	+	+	+
Журнал реєстрації нападів, що експортується	+	+	+	+	+	+
Вистежування / визначення IP-адрес джерела атаки	+ / +	+ / +	+ / +	+ / +	+ / +	+ / +
Фільтрація вхідних / вихідних даних	+ / +	+ / +	+ / -	+ / +	+ / +	+ / +
Сумісність з TCP / UDP	+ / +	+ / +	+ / +	+ / +	+ / +	+ / +
Сумісність з ICMP / ARP	+ / +	+ / +	+ / +	+ / -	+ / -	+ / +
Блокування: ICMP (PING) за замовчуванням	+	+	–	+	+	+
активних елементів в Web	–	+	–	+	–	+
реклами в Web	–	–	–	+	–	+
активних елементів в email	–	+	–	+	–	+
Виявлення прикладних програм на ходу	+	+	+	+	+	+
Аналіз змісту Web	–	–	–	+	–	+
Кешування DNS	–	–	–	–	–	+
Фільтрація ключових слів / блокування вузлів	– / –	– / –	+ / +	– / +	– / –	+ / +
Список заборонених вузлів, що завантажується з мережі	–	–	–	+	–	–
Секретність конфіденційних даних	–	–	–	+	–	–
Вбудована функція пошуку вірусів	–	+	–	+	–	+
Оновлення файлів сигнатур вірусів через Web	–	+	–	+	–	–
Блокування IP-адреси джерела заражених файлів	–	+	–	+	–	–

Критерій	Zone Alarm Pro 4.0	McAfee Desktop Firewall 7.5	Black Ice Defender 3.6	Norton Internet Security 2005	Tiny Personal Firewall 6.5.110	Agnitum Outpost Firewall Pro 2.1
Автоматична відправка файлів в карантин / видалення заражених файлів	– / –	+ / +	– / –	+ / +	– / –	+ / +
Планувальник операцій пошуку вірусів	–	–	–	+	–	–

Таблиця 3

Характеристика міжмережних екранів для корпоративних мереж

Характеристика	Raptor Firewall 6.5	Firewall-1	Secure PIX Firewall 520	Border Manager EE 3.5	Black Hole 3.0	Cyber Guard Firewall 3.0
Компанія	AXENT Technologies	Check Point	Cisco Systems	Novell, Inc.	Milkyway Networks	CyberGuard Corporation
Підтримувані ОС	Compaq Tru64, HP HP-UX 11.x, Linux, Microsoft Windows 2000, NT 4.x, Sun Solaris 2.6 і 2.7(32-розрядна)	Solaris SPARC), Microsoft Windows NT (X86), HP-UX (HP)	ОС власної розробки	NetWare 5 (X86), IntraNetWare (X86)	BSDI (X86), Solaris (SPARC)	UnixWare (X86), Windows NT (X86)
Рівень фільтрації	Прикладний, мережевий	Прикладний, сеансовий, мережевий	Сеансовий, мережевий	Прикладний, сеансовий, мережевий	Прикладний, мережевий	Сеансовий
Фільтрація URL	+	+	+	–	+	-
Прозорість для додатків	+	+	+	+	–	+
Блокування мобільного коду	+	+	+	+	+	+
Трансляція мережевих адрес	+	+	+	+	+	+
Виявлення сканування портів	+	+	+	+	+	+
Типи фільтрів прикладного рівня	Exec, FTP, login, shell, SMTP, SQL, telnet	FTP, rlogin, SMTP, telnet	DNS, H.323, SMTP, інші	http, ftp, generic TCP/UDP (telnet), smtp, POP3, gopher, https (SSL), nntp, RealAudio, RTSP, SOCKS 4 and 5	http, ftp, telnet, smtp, nntp, gopher, X11	http, smtp, telnet, rlogin, rsh, nntp, X11, gopher, SSL, lp
Аутентифікація користувачів	+	+	+	+	+	+

Характеристика	Raptor Firewall 6.5	Firewall-1	Secure PIX Firewall 520	Border Manager EE 3.5	Black Hole 3.0	Cyber Guard Firewall 3.0
Підтримувані типи аутентифікації	Axent Defender, CryptoCards, Gateway Password, Window NT Domain, RADIUS, SDI, S/Key, TACACS+	Axent Defender, внутрішній пароль FireWall-1, пароль ОС, RADIUS, SECURID, S/Key, TACACS/TACACS+, цифровий сертифікат X.509	CryptoCards, RADIUS, SECUREID, TACACS+	BMAS (RADIUS+ NDS)	S/Key, SECURID, Enigma Logic Safeword	SECURID, SecureNet

Закінчення табл. 3

Характеристика	Raptor Firewall 6.5	Firewall-1	Secure PIX Firewall 520	Border Manager EE 3.5	Black Hole 3.0	Cyber Guard Firewall 3.0
Інтерфейс віддаленого керування	+, з шифруванням	+, без шифрування, з шифруванням або через клієнта VPN	+, без шифрування, з шифруванням або через клієнта VPN	+, з шифруванням	+	+, у додатковому модулі
Підтримувані методи протоколювання	Простій ASCII-файл	Файли реєстраційного журналу	Віддалений, системний журнал	Файли реєстраційного журналу	Файли реєстраційного журналу	Файли повідомлень і журнал подій
Спосіб оповіщення	Звуковий, електронною поштою, через пейджер, пастка SNMP	Звуковий, електронною поштою, через пейджер, пастка SNMP	Електронною поштою, через пейджер	Електронною поштою, через пейджер	Звуковий, електронною поштою, через пейджер	Звуковий, електронною поштою, через пейджер
Підтримувані протоколи захисту	IPsec, SwlPe	IPsec, FWZ, SSL	IKE, IPsec, PPTP, SKIP, фірмові	IPsec	IPsec	IPsec
Підтримка антивірусних продуктів сторонніх фірм	–	Продукт, що реалізує підтримку протоколу CVP	MIME sweeper, Trend	AVP, INOCULAN	–	ViruSafe

Висновки

1. Загроза нападу ззовні на корпоративну та локальну мережі чи на робочу станцію наразі є настільки великою, що компаніям та користувачам необхідно враховувати її і вживати заходи щодо захисту інформації. Користувачам пропонується великий вибір міжмережних екранів.

2. Залежно від масштабів підприємства і особливостей політики безпеки оптимальними для мережі можуть бути різні версії міжмережного екрана.

Під час вибору необхідно враховувати:

– вимоги до функціональності;
– вимоги до масштабованості;
– топологію інформаційної системи;
– доступність кваліфікованих спеціалістів;
– бюджетні обмеження.

3. Після проведення досліджень серед міжмережних екранів для робочих станцій та локальних мереж найвищу оцінку отримали Mcafee Desktop Firewall 7.5, Norton Internet Security 2005 та Agnitum Outpost Firewall 2.1.

4. Серед міжмережних екранів для корпоративних мереж найвищу оцінку отримали Firewall-1 та Secure PIX Firewall 520.

Література

1. *Польман Н., Кразерс Т.* Архитектура брандмауэров для сетей предприятия. – М.: Изд. дом «Вильямс», 2003. – 432 с.

2. *Оглтри Т.* Firewalls. Практическое применение межсетевых экранов. – М.: ДМК Пресс, 2001. – 400 с.

3. *Кейт Е., Страссберг Р., Гондек Г.* Полный справочник по брандмауэрам. – М.: Диалектика, 2004. – 848 с.

Стаття надійшла до редакції 26.05.06.