ЗАХИСТ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Наталенко П. П., доц., к.т.н.; Шолудько В. Г.
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

Найбільш поширеною технологією при побудові корпоративних мереж в нашій державі є технологія *Internet*. Основними факторами визначаючими це є розвинута система сервісних послуг які сприяють підвищеному інтересу системи управління до видимих переваг у використанні цих послуг в процесі управління. Найбільш поширеним мережевим обладнанням для побудови мереж є обладнання компанії *Cisco*. Незважаючи на те, що ОС *Cisco IOS* підтримує аутентифікацію поновлень маршрутизації актуальною є задача побудови захищеної мережі на основі використання технології *VPN*. В доповіді розглянуті конкретні підходи по створенню такої захищеної мережі які підкріплені конкретними програмними рішеннями по її реалізації.

Об'єми створюваної, переданої по каналах зв'язку і збереженої інформації постійно зростають. Ефективність інформаційних систем і мереж забезпечується по двох основних напрямках — стиснення об'ємів і захист інформації.

Сьогодні створюють апаратно-програмні комплекси захисту інформації в *IP*-мережах. Розроблено ряд стандартизованих підходів спрямованих на захист інформації і розмежування доступу до неї. Одним із заходів захисту інформації в таких мережах є фіксація mac-адресів робочих станції користувачів, що підключаються до мережі. Портам комутатора прописують відповідну mac-адресу, і якщо в процесі роботи мережі, до цього порту буде підключено комп'ютер з мережевою картою у якої інша адреса, то він буде блокований даним портом. Іншими словами здійснюється «прив'язка» *mac*-адресів комп'ютерів посадових осіб до портів комутатора на основі технології *VLAN* (*Virtual LAN*). Виробники комутаторів випускають їх уже із фіксованою конфігурацією, коли всі порти прописані до *VLAN*1, тобто обмін між портами не розмежований і можна створювати дзеркальний порт, а також контролювати інформацію, що передається через будь-який із портів.

Технологія *VLAN* дає можливість при конфігуруванні портів комутаторів і визначенні їх режимів роботи, здійснити групування портів по напрямкам діяльності посадових осіб, комп'ютери яких планується підключати. Причому, окремі порти різних комутаторів входять до однієї віртуальної мережі *vlan*10, *vlan*20 і т.д. Пакети, що передаються від абонента не входять за межі конкретної *VLAN*. Така мережа повністю захищена він небажаного втручання. Для виходу із локальної мережі і підключення до ін-

ших мереж потрібний маршрутизатор (*gateway*), який працює на мережевому рівні.

В комунікаційних системах використовують такі засоби мережевого захисту інформації [1]:

1. Міжмережеві екрани (*firewall*) — для блокування атак з зовнішнього середовища (*Cisco PIX Firewall, Symantec Enterprise Firewall* TM та інші). Вони керують проходженням мережевого трафіку відповідно до правил (*policies*) захисту. Як правило, міжмережеві екрани встановлюють на вході мережі (на прикордонних маршрутизаторах) і розділяють її на внутрішні (приватні) і зовнішні (загального доступу) мережі.

2. Системи виявлення втручань (Intrusion Detection System) — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder alert та інші).

3. Засоби створення віртуальних приватних мереж *VPN* (*Virtual Private Network*) — для організації захисних каналів передачі даних через незахищене середовище (*Cisco IOS VPN, Cisco VPN concentrator*) .

4. Технологія *VPN* забезпечує прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.

5. Засоби аналізу захищеності, призначені для аналізу захищеності корпоративних мереж та виявлення можливих каналів реалізації загроз інформації (*Symantec Enterprise Security Manager, Symantec NetRecon*). Їх застосування дозволяє передавати інформацію про можливі атаки на корпоративну мережу, оптимізувати втрати та захист інформації і контролювати поточний стан захищеності мережі.

Для захисту інформації та управління потоками даних між корпоративними мережами використовують[2, 3]:

1. Фільтри , а саме — *ACL*–списки управління доступом.

2. Формування між автономними системами захищених тунелів на основі використання технології *VPN*.

3. Аутентифікацію і криптографічний захист інформації в тунелях в граничних маршрутизаторах.

Література

1. Уэнстром М. Организация защиты сетей Cisco. Anaging Cisco Network Security : пер. с англ. / М. Уэнстром. — М. : СПб., Киев: Вильямс, 2005. — 758 с. : ил. — ISBN 5–8459–0387–4

2. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3–издание, исправленное — Cisco Press; 2008, 1 кв.; Вильямс — 1168 с. — ISBN 978–5–8459–0842–1, 1–58713–150–1

3. Сандул Г. Д. Возможности технологии Cisco IOS IP SLA [Електронний ресурс]: Г. Д. Сандул — Режим доступу до статті: http://www.securitylab.ru/analytics/309557.php. — Назва з екрана.