УДК 004

Волошко С.В., доцент,
Фролов А.Ю., студент
Полтавський національний технічний університет
імені Юрія Кондратюка

АНАЛІЗ МЕРЕЖЕВОГО ОБЛАДНАННЯ ДЛЯ ПОБУДОВИ МЕРЕЖІ ІНТЕРНЕТ-ПРОВАЙДЕРА

У статті здійснена порівняльна характеристика пристроїв безпеки, маршрутизаторів і комутаторів від виробників Cisco, Huawei, Juniper, HP, D-Link для прийняття рішення про доцільність вибору того чи іншого для побудови мережі інтернет-провайдера.

Ключові слова: *провайдер, маршрутизатор, коммутатор, Cisco*.

Інтернет-провайдери – компанії, що надають послуги доступу до всесвітньої мережі Інтернет – займають в останні роки одне з провідних положень на ринку послуг. Мережа провайдера з'єднується з іншими мережами по всій планеті, що дозволяє мати зв'язок з будь-якою точкою планети.

З діаграми (рис. 1.1) бачимо що лідером серед виробників найбільш популярного обладнання комутації й маршрутизації для середніх і великих підприємств є Cisco Systems (близько 64% світового ринку). На другому місці HP Networking (приблизно 9%). Далі йдуть Alcatel-Lucent (3%), Juniper Networks і Brocade (по 2,3%), Huawei (1,8%) та інші виробники, які менш помітні на фоні гігантів, але спільно займають близько 17,6% ринку.

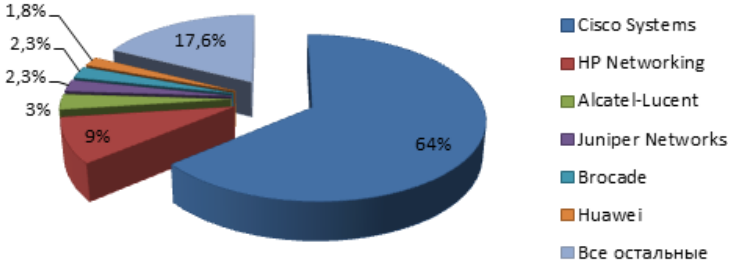

Рис. 1. Структура ринку L-2, L-3, L-4 обладнання

Досить поширені комутатори Nortel і Allied Telesis. Часто зустрічаються пристрої виробників D-Link і Netgear, що пропонують обладнання для малих і середніх підприємств.

Найчастіше в серверних стійках і комутаційних шафах компаній зустрічається обладнання наступних виробників: Cisco, HP (включаючи 3Com), Juniper, Avaya (включаючи Nortel), Alcatel-Lucent, Huawei, Allied Telesis, D-Link, Netgear.

Статистика, наведена на рис. 1.2, говорить про те, що в Cisco і HP Networking найбезпечніше у світі обладнання, або ці дві компанії уважніше інших підходять до пошуку, обробки і виправлення вразливостей у своїх продуктах.

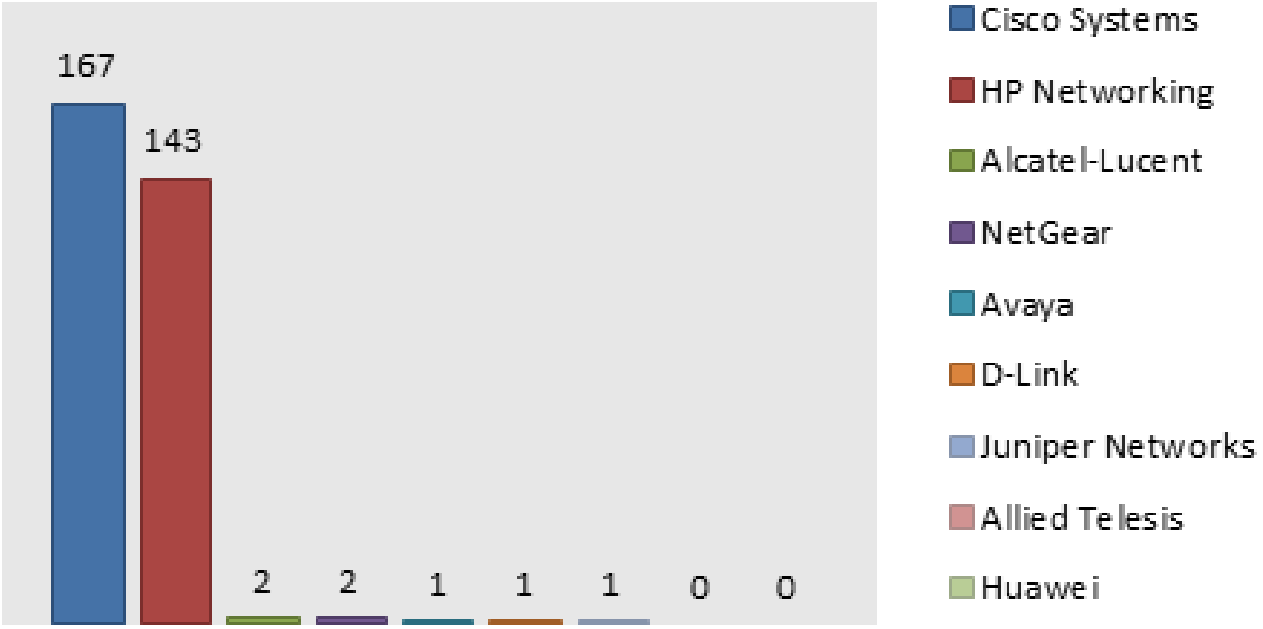

Рис. 2. Кількість вразливостей за рік

Якщо виробник усе робить правильно, то події природно розвиваються в такий спосіб:

Вразливість знайдена. У виробника є якийсь час, щоб підготувати пакет виправлень. Як тільки виправлення (або інший розв'язок) готові – публікується інформація про уразливість і варіантах її усунення.

Так відбувається не завжди. Публікація інформації про вразливість – це визнання власної помилки, але не кожна компанія готова піти на це. Часто виробник випускає пакет виправлень, не згадуючи при цьому, що він тим самим закриває критичну вразливість.

Приміром, фахівці Positive Research вивчали якийсь продукт у лінійці безпеки одного з гігантів індустрії. Практично все настроювання цього продукту проводиться через веб-інтерфейс, у якому були виявлені множинні вразливості, причому одна з них була досить серйозною – 7.0 за шкалою CVSS v.2. Було повідомлено про неї виробнику, і через деякий час було випущене виправлення, однак привселюдно виробник вразливість не визнав і, відповідно, записи про неї на cve.mitre.org ви не знайдете.

З гістограми бачимо (рис.1.2), що розрив в кількості вразливостей між Cisco з HP Networking і всіма іншими гігантський. Однак той факт, наприклад, що на гістограмі всього одна вразливість для обладнання Juniper, – не говорить про те, що їх не було більше. Справа лише в тому, що відомостей про них немає на cve.mitre.org, найбільш доступному і повному ресурсі. Зареєстровані користувачі juniper.net можуть одержати вичерпну інформацію про вразливості, але виявити ті ж відомості у вільному доступі буде набагато складніше.

З обладнанням Avaya, Alcatel-Lucent, Huawei, Allied Telesis, D-Link і Netgear ситуація та ж: вразливості в ПЗ є, але відкритої інформації про них мало. Нижче наведена узагальнена статистика за типами вразливостей для всіх згаданих виробників.

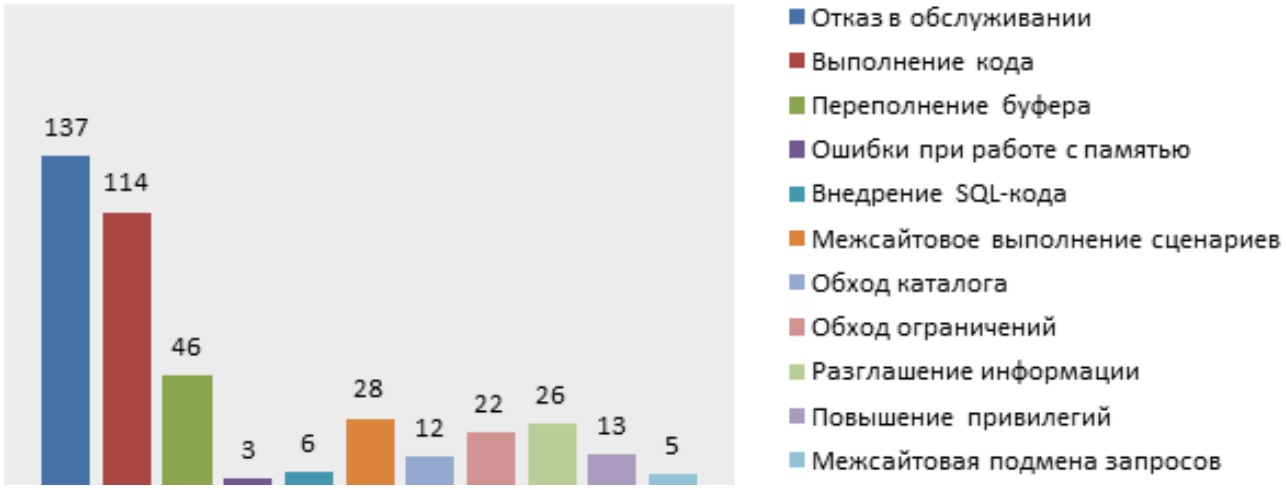

Рис. 3. Вразливості за типом

Відмова в обслуговуванні, як завжди, – найпоширеніша погроза для мережевого обладнання, але виникають і ті вразливості, які призводять до можливості виконання в системі довільного коду.

Cisco послідовно впроваджує інновації, які дають переваги вашому бізнесу. Багато постачальників намагаються запропонувати «досить гарні» мережні рішення, пропонуючи тільки основний функціонал, але для одержання більшого числа функцій ціна зростає. Juniper був постачальником, який послідовно намагався позиціонувати себе як колега Cisco в області інновацій.

У рішень Cisco немає конкурентів за цим параметром. У них найбільш широка лінійка за всіма мережними рішеннями: від ринку SOHO до провайдерських рішень, від невеликих, але функціональних маршрутизаторів, до систем керування мережами великих підприємств.

Головне: Cisco не зупиняється на досягнутому і вкладає гроші в перспективні напрямки й придумує нові. Купуючи перспективні розробки, Cisco вбудовує їх у свої рішення.

Надійність. Виходить з ладу все, питання тільки: коли. В Cisco бували невдалі серії, невдалі релізи операційних систем, однак у цілому відмовостійкість сумнівів не викликає.

Гнучкість. Те саме обладнання, залежно від операційної системи й комплектації модулями, може виконувати зовсім різні функції: захисні, шлюзу уніфікованих комунікацій, сервісні і т.д.

Взаємозалежність. Різне обладнання, що виконує різні функції, може залежати одне від одного і управляти один одним. Це дозволяє зробити мережу живим організмом, а не набором розрізненого обладнання.

Налагодження. Важливі для настроювання найширші можливості з пошуку несправностей, вбудовані практично в усі пристрої Cisco.

Інтелектуальність. Cisco продає не тільки якісне обладнання, а так само ідею й можливості. Все обладнання Cisco містить широкий спектр технологій, протоколів, ідеологій, як стандартних, так і своїх власних, що дозволяють розширити можливості мережі.

Продуктивність. Компанія Cisco є лідером у багатьох сегментах ринку й повинна відповідати цьому високому званню. Тому з'являються унікальні рішення, типу CRS (одного такого пристрою досить, щоб забезпечити зв'язком, скажемо, усю Великобританію). Зараз топові рішення з 10 гігабітними інтерфейсами є і в сегменті міжмережевих екранів, і в сегменті маршрутизаторів, і в сегменті систем запобігання вторгнень.

Централізація. Обладнанням Cisco можна керувати не окремо один від одного, а застосовувати потужні комплекси, наприклад, cisco security manager. Також централізовано можна збирати статистику й аналізувати її – MARS.

Cisco виробляє комутатори, маршрутизатори, сервери доступу й інше обладнання, що різняться за місцем розташування в мережі і її типом. Тобто, у прайс-листі може існувати кілька різних моделей з однаковими зовнішніми параметрами – кількістю й швидкістю портів. Відрізняються вони функціями ПЗ, продуктивністю, можливостями резервування й взаємодією з «сусідами» по мережі.

Маршрутизатор (англ. router) – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних

правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Часто маршрутизатор не обмежується простим пересиланням даних між інтерфейсами, але й виконує інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів інтернету, роздає IP-адреси, шифрує трафік і багато іншого.

Маршрутизатори працюють на мережному рівні моделі OSI: можуть пересилати пакети з однієї мережі до іншої. Для того, щоб надіслати пакети в потрібному напрямку, маршрутизатор використовує таблицю маршрутизації, що зберігається у пам’яті. Таблиця маршрутизації може складатися засобами статичної або динамічної маршрутизації.

Також маршрутизатори можуть здійснювати трансляцію адреси відправника й одержувача (англ. NAT, Network Address Translation), фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/дешифрування передаваних даних тощо.

Крім фільтрації, маршрутизатор може забезпечувати пріоритетний порядок обслуговування буферизованих пакетів, коли на підставі деяких ознак пакетам надаються переваги при виборі із черги.

Маршрутизатори не можуть здійснювати передачу широкомовних повідомлень, таких як ARP-запит.

Маршрутизатори допомагають зменшити завантаження мережі. В основному їх застосовують для об’єднання мереж різних типів, у тому числі несумісних за архітектурою і протоколам, наприклад для об’єднання різних локальних мереж, а так само для забезпечення доступу з локальної мережі в глобальну мережу Інтернет.

У якості маршрутизатора може виступати як спеціалізоване (апаратне) обладнання, так і звичайний комп’ютер, що виконує функції маршрутизатора. Існує кілька пакетів програмного забезпечення (в основному на основі ядра Linux), за допомогою якого можна перетворити персональний комп’ютер у високопродуктивний і багатофункціональний маршрутизатор. Також у ролі

маршрутизатора може виступати робоча станція або сервер, що мають кілька мережних інтерфейсів і оснащені спеціальним програмним забезпеченням.

Маршрутизатори ділять на пристрої верхнього, середнього й нижнього класів.

Маршрутизатори верхнього класу – магістральні маршрутизатори (backbone routers) – найвисокопродуктивніші, служать для об'єднання мереж підприємства (побудови центральної мережі). Центральна мережа може складатися з великої кількості локальних мереж. Магістральні маршрутизатори – це найбільш потужні пристрої, здатні обробляти кілька сотень тисяч або навіть кілька мільйонів пакетів за секунду. Вони підтримують безліч протоколів і інтерфейсів, можуть мати до 50 портів локальних або глобальних мереж. Велика увага приділяється в магістральних моделях надійності й відмовостійкості маршрутизатора, яка досягається за рахунок системи терморегуляції, надлишкових джерел живлення, замінних «на ходу» (hot swap) модулів.

Маршрутизатори середнього класу – маршрутизатори регіональних відділень. З'єднують регіональні відділення між собою і з центральною мережею. Мережа регіонального відділення, так само як і центральна мережа, може складатися з декількох локальних мереж. Такі маршрутизатори, як правило, являють собою деяку спрощену версію магістрального маршрутизатора, підтримувані ними інтерфейси локальних і глобальних мереж менш швидкісні. Дані маршрутизатори підтримують найпоширеніші протоколи маршрутизації й транспортні протоколи. Це найбільш великий клас маршрутизаторів, що випускаються, характеристики, яких можуть наближатися до характеристик магістральних маршрутизаторів, а можуть і опускатися до характеристик маршрутизаторів віддалених офісів.

Маршрутизатори нижнього класу – маршрутизатори віддалених офісів. Призначаються для локальних мереж підрозділів; вони зв'язують невеликі офіси з мережею підприємства. Такі маршрутизатори можуть підтримувати один-два інтерфейси локальних мереж, розраховані на низькошвидкісні

виділені лінії або з’єднання, що комутуються. Маршрутизатор віддаленого офісу може підтримувати роботу з телефонної лінії, що комутується, у якості резервного зв’язку для виділеного каналу. Ці маршрутизатори користуються більшим попитом в організаціях, яким необхідно розширити наявне міжмережеве об’єднання. Існує дуже велика кількість типів маршрутизаторів віддалених офісів. Це пояснюється як масовістю потенційних споживачів, так і спеціалізацією такого типу пристроїв, що проявляється в підтримці одного конкретного типу глобальному зв’язку. Існують маршрутизатори, що працюють тільки по мережі ISDN, існують моделі тільки для аналогових виділених ліній і т.п.

Комутатор (жарг. свіч від англ. switch – перемикач) – це мережевий присирій, який з’єднує кілька комп’ютерів в одну єдину локальну мережу. Сучасні комутатори мають дуже великий ряд функцій, які дуже сильно можуть полегшити подальшу роботу адміністратора. Від правильного вибору комутаторів залежить функціонування всієї локальної мережі й робота підприємства в цілому.

Комутатор працює на канальному (другому) рівні моделі OSI. Комутатори були розроблені з використанням мостових технологій і часто розглядаються як багатопортові мости. На відміну від концентратора, який поширює трафік від одного підключеного пристрою до всіх інших, комутатор передає дані тільки безпосередньо одержувачеві (виключення становить широкомовний трафік усім вузлам мережі й трафік для пристроїв, для яких не відомий вихідний порт комутатора). Це підвищує продуктивність і безпека мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначали.

Комутатор зберігає в пам’яті таблицю комутації (зберігається в асоціативній пам’яті), у якій вказується відповідність MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня і він працює в режимі навчання. У цьому режимі дані, які надходять на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує

фрейми (кадри) і, визначивши MAC-адресу хоста-відправника, записує його в таблицю на якийсь час. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого уже є в таблиці, то цей кадр буде переданий тільки через порт, вказаний у таблиці. Якщо MAC-адреса хоста-одержувача не асоційована з яким-небудь портом комутатора, то кадр буде відправлений на всі порти, за винятком того порту, з якого він був отриманий. Потім комутатор будує таблицю для всіх активних MAC-адрес, у результаті трафік локалізується. Варто відзначити малу затримку і високу швидкість пересилання на кожному порту інтерфейсу.

Комутатори можна так само розділити на:

1. Некерований свіч – це прості автономні пристрої, які управляють передачею даних самостійно і не мають інструментів ручного управління. Деякі моделі некерованих комутаторів мають вбудовані інструменти моніторингу.

Мінусами в некерованих комутаторів є відсутність інструментів управління і мала внутрішня продуктивність. Тому у великих мережах підприємств некеровані комутатори використовувати не розумно, тому що адміністрування такої мережі вимагає величезних людських зусиль і накладає ряд істотних обмежень.

2. Керований свіч – це ті пристрої, які також працюють в автоматичному режимі, але крім цього мають ручне керування. Ручне керування дозволяє дуже гнучко настроїти роботу комутатора й полегшити життя системного адміністратора.

Основним мінусом керованих комутаторів є ціна, яка залежить від можливостей самого комутатора і його продуктивності.

Абсолютно всі комутатори можна розділити за рівнями. Чим вищий рівень, тим складніший пристрій, а отже і дорожчий. Рівень комутатора визначається шаром, на якому він працює в мережній моделі OSI.

Для правильного вибору комутатора потрібно визначитися, на якому мережному рівні необхідно адмініструвати ЛОМ.

Поділ комутаторів за рівнями:

Комутатори 1-го рівня (Layer 1). Це всі пристрої, які працюють на 1-му рівні мережної моделі OSI – фізичному рівні. До таких пристроїв належать повторювачі, хаби й інші пристрої, які не працюють із даними взагалі, а працюють із сигналами.

Комутатори 2-го рівня (Layer 2). Це всі пристрої, які працюють на 2-му рівні мережної моделі OSI – канальному рівні. До таких пристроїв можна віднести всі некеровані комутатори й частину керованих.

Комутатори 2-го рівня працюють з даними як з окремими кадрами (*frame* або жарг. *фреймами*). Вміють аналізувати одержувані кадри й працювати з MAC-адресами пристроїв відправників і одержувачів кадра. Такі комутатори «не розуміють» IP-адреси комп'ютерів, для них усі пристрої мають назви у вигляді MAC-адрес.

Комутатори 2-го рівня складають комутаційні таблиці, у яких співвідносять MAC-адреси мережних пристроїв, що зустрічаються, з конкретними портами комутатора.

Комутатори 3-го рівня (Layer 3). До них належать всі пристрої, які працюють на 3-му рівні мережної моделі OSI – мережному рівні. До таких пристроїв відносяться всі маршрутизатори, частина керованих комутаторів, а так само всі пристрої, які вміють працювати з різними мережними протоколами: Ipv4, Ipv6, IPX, Ipsec і т.д. Комутатори 3-го рівня повністю підтримують усі функції й стандарти комутаторів 2-го рівня. З мережними пристроями можуть працювати за IP-адресами. Комутатор 3-го рівня підтримує установлення різних з'єднань: pptp, pppoe, vpn і т.д.

Комутатори 4-го рівня (Layer 4). До них належать всі пристрої, які працюють на 4-му рівні мережної моделі OSI – транспортному рівні. До таких пристроїв належать маршрутизатори, які вміють працювати вже з додатками. Комутатори 4-го рівня використовують інформацію, яка міститься в заголовках пакетів і відноситься до рівня 3-го і 4-го стека протоколів, таку як IP-адреси джерела й приймача, біти SYN/FIN, що відзначають початок і кінець прикладних сеансів, а також номера портів TCP/UDP для ідентифікації

приналежності трафіка до різних додатків. На підставі цієї інформації, комутатори рівня 4 можуть приймати інтелектуальні рішення про перенаправлення трафіка того або іншого сеансу.

Проведений аналіз мережевого обладнання приводить до прийняття рішення, що доцільний вибір обладнання компанії Cisco.

Література

1. *Популярное сетевое оборудование и статистика уязвимостей / 20 апреля 2012 – http://habrahabr.ru/company/pt/blog/142479/*
2. *Почему Cisco?/ 5 мая 2009 – http://habrahabr.ru/post/58843/*
3. *Официальный сайт компании Cisco Systems – http://www.cisco.com/*
4. *Основы организации сетей Cisco, том 1 [Текст].: Пер. с англ. - М.: Издательский дом «Вильямс», 2002. - 512 с.*
5. *Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство, 3-е изд., с испр. [Текст]: Пер. с англ. – М.: ООО «И. Д. Вильямс», 2007. – 994.*