СЕКЦІЯ: «ЕЛЕКТРОНІКА ФІЗИКО-ТЕХНІЧНИХ СИСТЕМ»

УДК 004.7

Аппаратная реализация средств обеспечения безопасности локальных вычислительных сетей

Каут М.С., доц. к.т.н Терлецкий А.В.

На сегодняшний день безопасность вычислительной сети является одним из самых важных вопросов сетевых технологий, так как у всех пользователей, начиная от одного конкретного пользователя и вплоть до больших корпоративных сетей, локальная сеть может использоваться для передачи конфиденциальной информации (финансовые отчеты, банковские операции и т.д.). Если эта информация попадет не в те руки, это может быть чревато серьезными последствиями, большими финансовыми потерями и даже угрозой развала компании при попадании определенной информации конкурентам. Также внутреннее или внешнее вмешательство может привести к потери информации, ее порче или даже к выходу из строя сетевого оборудования.

Важность системы защиты сети обусловлена следующими факторами:

- Обеспечение сохранности информации.
- Снижение риска остановки критически важных серверов и систем.
- Реализация контроля и ограничения доступа пользователей.
- Возможность отследить внутреннего и внешнего нарушителя.
- Рациональное использование канала доступа в Интернет.
- Основные угрозы безопасности информации локальных вычислительных сетей:
- Ошибки в программном обеспечении.
- Различные DoS- и DDoS-атаки.
- Компьютерные вирусы, черви, троянские кони.
- Анализаторы протоколов и прослушивающие программы.
- Технические средства съема информации [1] .

Обеспечить практически стопроцентную защиту сети позволяет использование

аппаратных межсетевых экранов, так называемых аппаратных фаерволов, и средств для мониторинга сети. Межсетевой экран - это комплекс аппаратных и программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

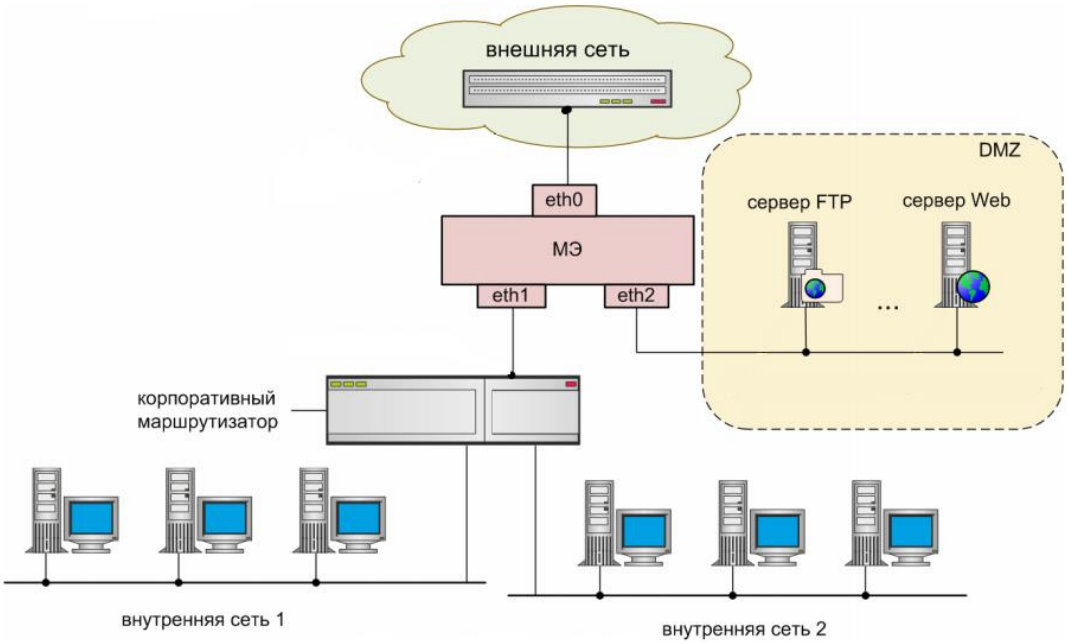

Рис.1 Использование межсетевого экрана в ЛВС

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Преимущества аппаратного обеспечения безопасности и мониторинга сетей:

- Комплексная безопасность: защита от новых угроз при помощи брандмауэра уровня приложений, антивирусной защиты и блокировщика пиринговых сетей;
- Управление пользователями: контроль сетевой активности и повышение производительности труда сотрудников с помощью пользовательских политик, мониторинга интернет-активности и контентной фильтрации;
- Качество обслуживания (QoS): увеличение пропускной способности и доступности интернет-канала с помощью распределения нагрузки на сеть, ограничителя скорости пропускной полосы и

подключения по резервному каналу;

Гибкость развертывания и администрирования: увеличение пропускной способности и доступности интернет-канала с помощью распределения нагрузки на сеть, ограничителя скорости пропускной полосы и подключения по резервному каналу [2] . Для обеспечения безопасности сети необходимо правильно выбрать межсетевой экран. Ниже приведена сравнительная характеристика по основным параметрам некоторых известных марок межсетевых экранов.

Табл.1

Сравнительная характеристика межсетевых экранов

Параметр		NEO	Континент	VIPNet	CiscoASA
Операционная система		Linux	BSD	Linux	Cisco IOS
Интерфейсы	**Количество**	от 4 до 65	от 4 до 34	от 4 до 6	от 4 до 30
Маршрутизация	**Статическая**	+	+	+	+
	Динамическая	+	+	-	+
	DHCP	+	+	+	+
Фильтрация трафика	**Контроль фрагментированных пакетов**	+	+	+	+
	Защита от DoS-атак	+	+	+	+
	Фильтрация одноранговых приложений	+	-	-	+
	Поддержка динамических групп адресов	-	-	-	+
	Фильтрация пакетов на прикладном уровне (L7-filtering)	+	-	-	+
Управление	**Консоль**	+	+	+	+
	Веб-интерфейс	+	+	+	+
Надежность	**Кластер Active/Standby**	+	+	+	+
	Кластер Active/Active	-	-	-	+
	VRRP	+	-	-	+
	Горячая замена блока питания	+	+	+	+
Производительность	**МЭ, Мбит/с**	до 18 000	до 3 000	до 3 500	до 20 000
	VPN, ГОСТ, Мбит/с	до 2 400	до 2 700	до 2 700	до 5 000
	IDPS, Мбит/с	до 3 200	—	—	до 10 000

Из сравнительной характеристики видно, что лучшим вариантом для защиты ЛВС является межсетевой экран Cisco ASA. Помимо высокого быстродействия, большого количества подключаемых устройств, широкого набора функций, его основным преимуществом является то, что в отличие от типичных серверов - "посредников" (proxy), которые выполняют обработку каждого сетевого пакета в отдельности, существенно загружая при этом центральный процессор, ASA использует специальную, не UNIX-подобную, операционную систему реального времени, обеспечивая большую производительность и высокий уровень защиты. Межсетевой экран Cisco ASA привносит новый уровень безопасности корпоративных сетей в сочетании с простотой использования. ASA может полностью скрыть внутреннюю сеть от внешнего мира, обеспечивая полную безопасность.

Рис.2 Структурная схема CiscoASA.

Операционная система

В отличии от многих фаерволов, которые работают под управлением операционных систем общего назначения, Cisco ASA и PIX Firewall имеют защищенную собственную (не-UNIX, не-Windows) интегрированную операционную систему, отвечающую за функционирование устройства, которая похожа на Cisco IOS. Так как эта операционная система изначально разрабатывалась с фокусом на безопасность и необходимую функциональность, она является наиболее защищенной и производительной, чем операционные системы общего назначения. Устройство, например, способно обрабатывать до 500 тысяч одновременных соединений.

Виртуальный фаервол (Security Context)

С седьмой версии операционной системы, Cisco ASA и PIX Firewall поддерживают

технологию виртуальных фаерволов (security contexts). Она позволяет в одном физическом устройстве определить несколько отдельных фаерволов, каждый из которых может работать независимо со своей конфигурацией, логическими интерфейсами, политикой безопасности, таблицей маршрутизации и администрированием. Однако данная функциональность лицензируется и доступна не на всех моделях устройств защиты.

Поддержка отказоустойчивости (Failover)

Любой покупатель или администратор хочет, чтобы сеть функционировала и функционировала очень быстро. Если мы используем один фаервол в нашей сети, он может явиться узким местом в случае отказа. Поэтому Cisco ASA и PIX Firewall поддерживают конфигурацию отказоустойчивости (failover), когда два одинаковых устройства защиты конфигурируются в паре, одно работает активным, а второе резервным. Только активное устройство выполняет свою функциональность, а резервное лишь ведет мониторинг и готово заменить активный фаервол, если он даст сбой. Это конфигурация активный/резервный.

С седьмой версии программного обеспечения поддерживается конфигурация активный/активный, когда оба устройства могут обрабатывать трафик. Данная конфигурация требует поддержки виртуальных фаерволов (security contexts). На каждом устройстве конфигурируется два виртуальных фаервола. При нормальных условиях, в каждом из физических устройств один виртуальный фаервол - активный, а другой - резервный. При выходе одного устройства из строя, второе задействует резервный виртуальный фаервол и обрабатывает весь трафик.

Также в обеих конфигурациях на Cisco ASA и PIX Firewall может быть сконфигурирована динамическая отказоустойчивость (stateful failover). Это значит, что при выходе активного устройства из строя, существующие соединения не теряются.

Управление через Web интерфейс

ASDM (Adaptive Security Device Manager) – это графическая оболочка, разработанная для того, чтобы помочь в настройке и управлении устройством, без знания командной оболочки устройства (CLI) [3] .

ASA

Основой высокой производительности межсетевого экрана ASA является схема защиты, базирующаяся на алгоритме адаптивной безопасности (adaptive security algorithm - ASA), который эффективно скрывает адреса пользователей от хакеров. Устойчивый, ориентированный на соединения алгоритм адаптивной безопасности обеспечивает

безопасность для соединений базируясь на адресах отправителя и получателя, последовательности нумерации пакетов TCP, номерах портов и добавочных флагах TCP. Эта информация сохраняется в таблице, и все входящие пакеты сравниваются с записями в этой таблице. Доступ через ASA разрешен только в том случае, если соответствующее соединение успешно прошло идентификацию. Этот метод обеспечивает прозрачный доступ для внутренних пользователей и авторизованных внешних пользователей, при этом полностью защищая внутреннюю сеть от несанкционированного доступа.

Технология «сквозного посредника»

Cisco ASA также обеспечивает существенное преимущество в производительности по сравнению с межсетевыми экранами-"посредниками" (proxy) на базе ОС UNIX за счет технологии "сквозного посредника" (Cut-Through Proxy). Как и обычные серверы - "посредники" ASA контролирует установление соединения на прикладном уровне. После того, как пользователь был успешно идентифицирован в соответствии с политикой обеспечения безопасности, ASA обеспечивает контроль потока данных между абонентами на уровне сессии. Такая технология позволяет межсетевому экрану ASA работать значительно быстрее, чем обычные межсетевые экраны - "посредники". [4]

Аппаратная часть

Для обеспечения высокой производительности в Cisco ASA используется 24-ядерный процессор Intel с тактовой частотой 2.4 ГГц. Объем оперативной памяти – 24 GB. Также высокое быстродействие достигается путем использования в качестве устройства хранения не обычных HDD дисков, а ATA CompactFlash, который является твердотельным накопителем. Межсетевой экран Cisco ASA поддерживает более 256 тысяч одновременных соединений и, соответственно, обеспечивает поддержку сотен и тысяч пользователей без уменьшения производительности. Полностью загруженный межсетевой экран ASA обеспечивает пропускную способность до 170 Мб/сек. Такая пропускная способность существенно превосходит любой межсетевой экран, базирующийся на ОС UNIX или ОС Microsoft Windows NT.

В заключение следует сказать, что использование межсетевых экранов значительно повышает безопасность ЛВС, при этом не влияя на ее быстродействие за счет своей высокой производительности. Один фаервол может использоваться одновременно для нескольких ЛВС, при этом его можно будет настроить для каждой ЛВС отдельно, путем разделения его на виртуальные фаерволы, что является очень выгодным в экономическом плане.

Литература

1. Алексеева М. С. Угрозы безопасности локальных вычислительных сетей / М. С. Алексеева, Е. В. Иванова // Молодой ученый. — 2014. — №18. — С. 212-213.
2. Аппаратное обеспечение безопасности и мониторинга сетей для малых и средних организаций// www.tensor.ru— 2014. — С. 1-2
3. Функциональность Cisco ASA и PIX Firewall// http://www.ciscolab.ru/
4. Межсетевой экран PIXFirewall// www.cisco.com