

Шлюз в Интернет на ComixWall ISG

Сергей Яремчук

Использование специализированных дистрибутивов для организации доступа в Интернет нельзя назвать чем-то особенным. Выбор только за решением. Сегодня познакомимся с возможностями ComixWall ISG.

Специализированные решения в отличие от применения обычных интересны тем, что позволяют получить нужный результат с минимальными усилиями и за более короткий срок. Большая часть дистрибутивов, построенных на Linux или одной из версий BSD-системы, имеют удобные инструменты для пост-инсталляционной настройки, нетребовательны к ресурсам и распространяются по свободной лицензии. Это делает их востребованными в небольших организациях, не имеющих штатных специалистов.

Дистрибутивов, построенных на Linux, несколько больше, чем на иных платформах. Решения, использующие в качестве основы другие варианты UNIX-систем, можно пересчитать буквально по пальцам. Наверное,

поэтому дистрибутив ComixWall ISG (Internet Security Gateway), появившись в июне 2006 года, сразу привлек к себе внимание. ComixWall [1] построен на OpenBSD, которая считается самой безопасной системой, что и послужило определяющим фактором при ее выборе разработчиками в качестве основы. Номер ComixWall соответствует номеру того релиза OpenBSD, на котором он построен, поэтому начальная версия сразу же получила цифру 3.9. Название Comix произошло из комбинации английских слов COMmunication и unIX. Особо подчеркивается, что ComixWall не является еще одним межсетевым экраном, которых сегодня предостаточно, и удивить ими, наверное, уже никого нельзя. Разработчики позиционируют его как законченное UTM-решение (см. врезку), предназначенное

для создания шлюзов безопасности, защищающих SOHO-сети и способное составить конкуренцию многим коммерческим продуктам.

Интерфейс управления ComixWall распространяется по BSD-лицензии, по этой же лицензии распространяются операционная система и отдельные пакеты. Часть пакетов, входящих в состав дистрибутива, имеет GNU GPL-лицензию.

Возможности ComixWall

Актуальной на момент написания статьи была версия 4.2 от декабря 2007 года, с обновлением в январе 2008 года (ComixWall 4.2_20080109). Следует заметить, что сами разработчики первые релизы пока еще считают пробными (Proof of Concept), больше ориентированными на специалистов, чем

на широкое применение. Хотя учитывая, что работают они стабильно, серьезных недостатков за пару лет обнаружено не было, поэтому ничто не мешало их использовать для защиты сети.

Дистрибутив включает в себя полный спектр самого разнообразного программного обеспечения, обеспечивающего:

- функцию фильтрации пакетов при помощи pf, входящего в состав OpenBSD;
- антивирусную защиту с ClamAV с автоматическим обновлением при помощи freshclam;
- систему обнаружения атак Snort с обновлением правил oinkmaster;
- контентный веб-фильтр DansGuardian с проверкой трафика при помощи ClamAV;
- анти-спам фильтры SpamAssassin и spamd;
- P3scan и smtp-gated антивирусные и анти-спам почтовые прокси;
- прокси Dante (SOCKS), Squid (HTTP), ftp-proxy, IMSPector (IM-прокси с поддержкой Jabber/XMPP, MSN, IRC, Yahoo и других);
- серверы: Apache, DNS, DHCP и OpenSSH.

И некоторые другие приложения, в том числе предназначенные для сбора и вывода разного рода статистики. Все настройки могут быть произведены стандартным способом из командной строки. Начиная с версии 4.0b появился веб-интерфейс, написанный на PHP. Использование gettext позволяет легко перевести его на другие языки. Хотя в настоящее время их немного, доступны только английский, испанский и турецкий варианты. Кроме базовых сетевых установок, с его помощью можно настроить правила пакетного фильтра и сервисов, входящих в комплект, производить мониторинг основных системных параметров и загрузки сети и многое другое. Плюс при помощи веб-интерфейса можно получить доступ к man-страницам и другой документации.

Некоторые возможности (VPN, VLAN, CARP, SNMP) пока настраиваются только из командной строки. Возможность их конфигурирования через веб-интерфейс планируется добавить уже в следующих релизах. Кроме этого, в планах разработчиков добавле-

packages are labelled '[X]'.

```
[X] SpamAssassin SPAM Scanner -> (p5-Mail-SpamAssassin-3.2.2.tgz)
[X] ARJ decompressor -> (unarj-2.43.tgz)
[X] RAR decompressor -> (unrar-3.76.tgz)
[X] ClamAV Virus Scanner -> (clamav-0.92p8.tgz)
[X] P3Scan POP3 Proxy -> (p3scan-2.3.2.tgz)
[X] Smtg-gated SMTP Proxy -> (smtp-gated-1.4.15.1.tgz)
[X] Snort IDS -> (snort-2.8.0.1p1.tgz)
[X] Snort IPS -> (snortips-4.2.tgz)
[X] Oinkmaster snort rule base updater -> (oinkmaster-2.0.tgz)
[X] Squid HTTP Proxy -> (squid-2.6.STABLE13-transparent.tgz)
[X] DansGuardian Web Filter -> (dansguardian-2.9.9.2-clamd.tgz)
[X] IMSPector IM Proxy -> (imspector-0.3.20071130p8.tgz)
[X] Dante SOCKS Proxy -> (dante-1.1.19.tgz)
[X] PHP -> (php5-core-5.2.3.tgz)
[X] Symon system monitoring software -> (symon-2.76.tgz)
[X] Webalizer web server logs analyzer -> (webalizer-2.01.10p3.tgz)
[X] Pmacct network analyzer -> (pmacct-0.11.4.tgz)
[X] ComixWall web interface -> (comixwall42_webif.tar.gz)
[X] ComixWall configuration files -> (comixwall42_config.tar.gz)
[X] ClamAV signature database -> (clamavdb.tar.gz)
[X] Categorized lists for web filter -> (bigblacklist_comixwall.tar.gz)
[X] Snort IDS rules -> (snortrules-snapshot-CURRENT.tar.gz)

Package name? (or 'done') [done] _
```

Рисунок 1. После установки системы последует инсталляция ComixWall

ние будущих версий: антивирусной проверки FTP- и IM-трафика, а также IMAP-прокси с антивирусной и анти-спам защитой.

Эту информацию по дистрибутиву можно получить на сайте проекта [1] и странице на Google Code [2], теперь же познакомимся с ComixWall ближе.

Установка ComixWall

Дистрибутив доступен в двух версиях – для платформ i386 и amd64. Загрузка возможна только через BitTorrent. Размер дистрибутива чуть больше 140 Мб, для установки которого требуется не менее 650 Мб свободного места на диске. Кстати, в первое время версия 4.2 была доступна толь-

ко для amd64, так как разработчики по праву считали, что 64-битные системы имеют ряд преимуществ перед 32-битными и сделали ставку на более высокопроизводительное решение. Затем уже по многочисленным просьбам пользователей появился релиз под i386.

Кроме дистрибутива, советую скачать и документ System Administration Guide (SAG), который поможет быстрее сориентироваться в настройках. К тому же он, как и другие документы, вполне может пригодиться. Как сказано в документации, установка ComixWall это: «is the usual OpenBSD installation», то есть обычная установка OpenBSD. Поэтому опыт в инсталляции этой сис-

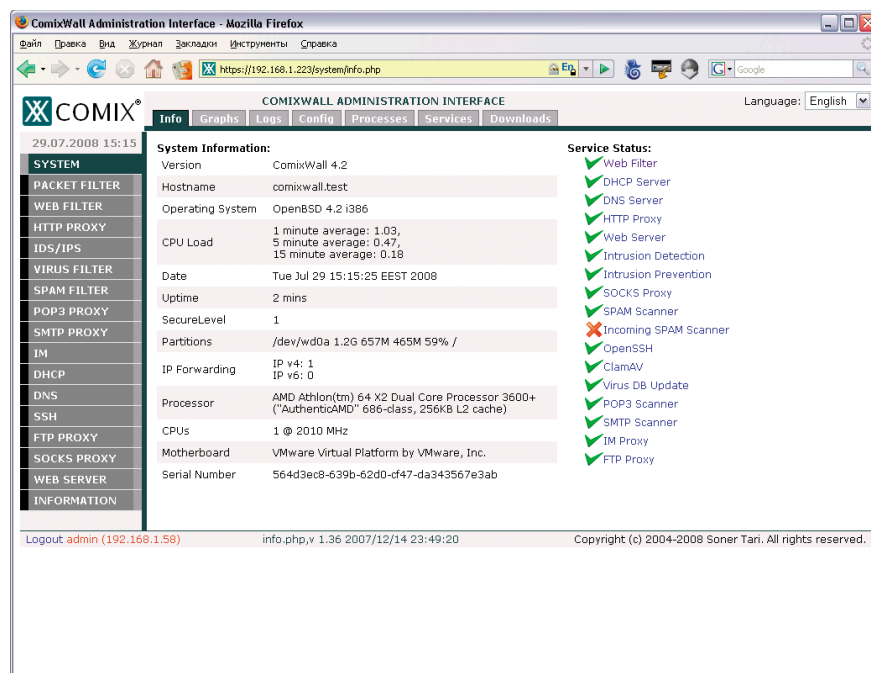


Рисунок 2. Окно ComixWall Administration Interface

Unified Threat Management

Термин Unified Threat Management (UTM, Объединенный контроль угроз) введен Чарльзом Колодги (Charles Kolodgy) из аналитической компании IDC (International Data Corporation) в документе «Worldwide Threat Management Security Appliances 2004-2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance», опубликованном в сентябре 2004 года. В нем предлагалось интегрировать в устройство защиты сети три компо-

нента: межсетевой экран, антивирус и систему обнаружения и предотвращения атак. Сегодня концепция UTM рассматривается несколько шире и предлагает для защиты сети вместо отдельных систем использовать комплексное устройство, которое сочетает в себе функции многих решений. Кроме межсетевого экрана, UTM включает антивирус, систему обнаружения/предотвращения атак, контентный фильтр веб-страниц и антиспам. Все это должно управляться через единый интерфейс.

темы лишним не будет. В крайнем случае следует почитать документы [3, 4], в которых все подробно расписано. Конечно, это несколько портит первое впечатление от ComixWall, ведь не каждый пользователь из SOHO, на которого ориентирован этот дистрибутив, сможет или захочет устанавливать систему таким образом. Например, в том же pfSense [5] весь процесс инсталляции максимально автоматизирован, и справиться с ним может человек без особой подготовки, не боящийся несколько раз нажать Next. Предусмотрено обновление установленной ранее

версии 4.1 до 4.2. В документации рекомендуется создать 5 разделов как минимум таких размеров: / – 181 Мб, /home – 2 Кб, /tmp – 10 Кб, (да, именно Кб) /usr и /var по 230 Мб. Плюс раздел подкачки. Не рекомендуется пропускать сетевые (да и другие) настройки во время установки системы, хотя затем можно к ним вернуться.

По окончании установки системы запустится установочный скрипт ComixWall – install.site или upgrade.site, в зависимости от выбранного режима. Для продолжения установки вводим «y».

```
Welcome to the ComixWall install program.
...
Proceed with install? [no] y
```

Скрипт поначалу запросит синхронизировать время с NTP-сервером:

```
Do you want to sync datetime with
a Time Server? [no]
```

Затем указать расположение пакетов и название привода компакт-дисков:

```
Let's install the packages!
Location of packages?
(cd disk ftp http nfs or 'done') [cd]
Available CD-ROMs are: cd0.
Which one contains the install media?
(or 'done') [cd0]
Pathname to the packages?
(or 'done') [packages]
```

Если диск был нормально обнаружен при установке системы, то во всех случаях достаточно нажимать <Enter>. После чего будет выведен список пакетов. Все пакеты отмечены к установке (см. рис. 1), отказываться от какого-либо обычно смысла нет, поэтому опять нажимаем <Enter>. Повторно подтверждаем свое намерение установить пакеты:

```
Ready to install packages? [yes]
```

После установки пакетов, запустится еще один скрипт, на этот раз пост-инсталляционный. Он повторит некоторые вопросы, задаваемые во время установки системы, предлагая в качестве значения по умолчанию введенное ранее. Последовательно нужно будет подтвердить имя узла, адреса шлюза и настройки сетевых интерфейсов. Далее следует указать, какой интерфейс соответствует LAN и WAN:

```
Which is LAN interface?
Options:
1) pcn0
2) pcn1
Type 'done' to exit
Selection? (#/done) [1]
```

Отмечаем нужный цифрой и аналогично поступаем для WAN. Если все настройки верны, то на запрос:

```
Configuration complete!
You can restart or type 'done' to exit.
Choose configuration method:
Options:
1) Automatic
2) Interactive
Type 'done' to exit
Selection? (#/done) [1] done
```

вводим «done». Если нажать <Enter>, весь процесс пост-инсталляционной

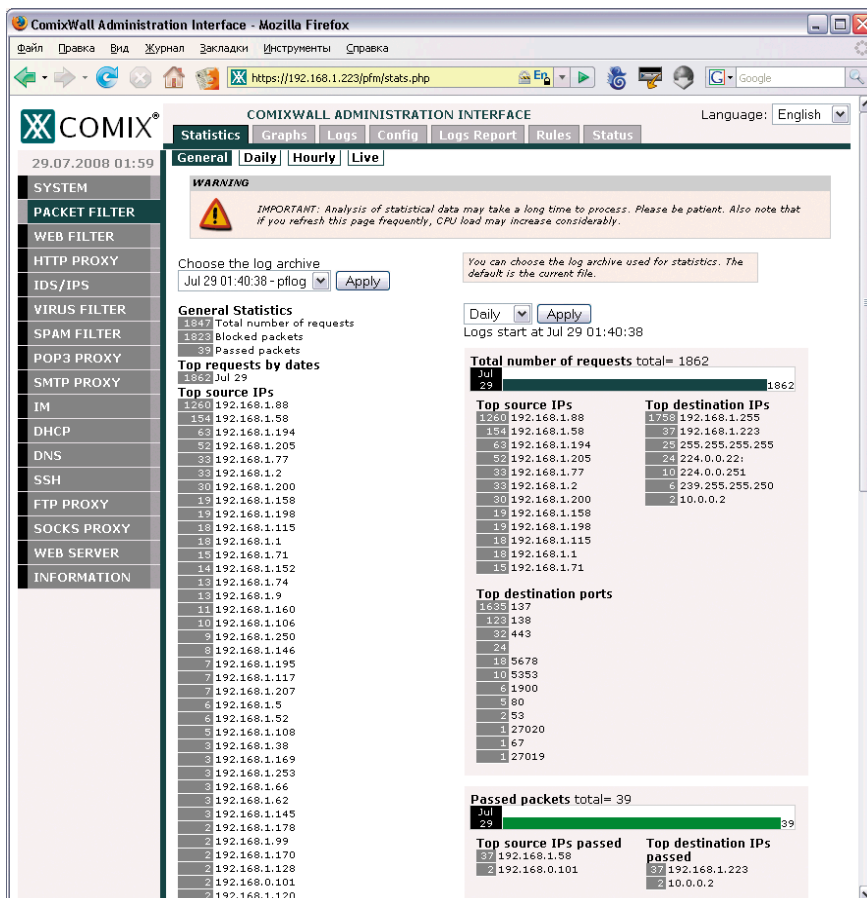


Рисунок 3. Статистика работы pf

настройки повторяется сначала. Прочитав поздравления по окончании установки, перезагружаем систему.

Веб-интерфейс

По умолчанию в системе заведено две учетных записи, имеющих доступ через веб-интерфейс: admin и user. Пароль в обоих случаях одинаков – wwwcomix. Пользователь с учетной записью user получает доступ только к статистике, ее может использовать начальство для контроля. Доступ из WAN блокируется правилом pf, поэтому зайти можно только из LAN. Если набрать адрес локального интерфейса, то в процессе подключения встроенный DNS-сервер выдаст имя узла. Работа осуществляется по протоколу HTTPS. Причем есть одна особенность. Если набрать `http://lan_ip_address`, то клиент будет перенаправлен на `https://hostname`, но вот подключение почему-то блокируется. Хотя в документации сказано, что это должно срабатывать. Поэтому вариант только один – `https://lan_ip_address`. Далее принимаем сертификат и регистрируемся в системе.

Если по удобству установки ComixWall проигрывает тому же pfSense, то по возможностям веб-интерфейса (ComixWall Administration Interface) он выходит далеко вперед. Я считаю, это одна из сильных сторон этого дистрибутива. Еще одна важная особенность веб-интерфейса – отсутствие промежуточных файлов с метаданными, которые часто используются в подобных решениях для генерации окончательных конфигурационных файлов. Поэтому можно без проблем производить параллельную настройку, как в командной строке, так и через веб-интерфейс.

Даже несмотря на наличие большого количества функций, все настройки находятся именно там, где ожидаешь их увидеть. В 96-страничном руководстве установке посвящено всего 10 страниц (плюс ссылка на документацию OpenBSD) все остальное относится к работе с веб-интерфейсом, поэтому рассказать о его возможностях на странице журнала невозможно.

Зрительно интерфейс разбит на три части. Слева находится основное меню настроек, состоящее из 17 пунктов отвечающих за работу с конк-

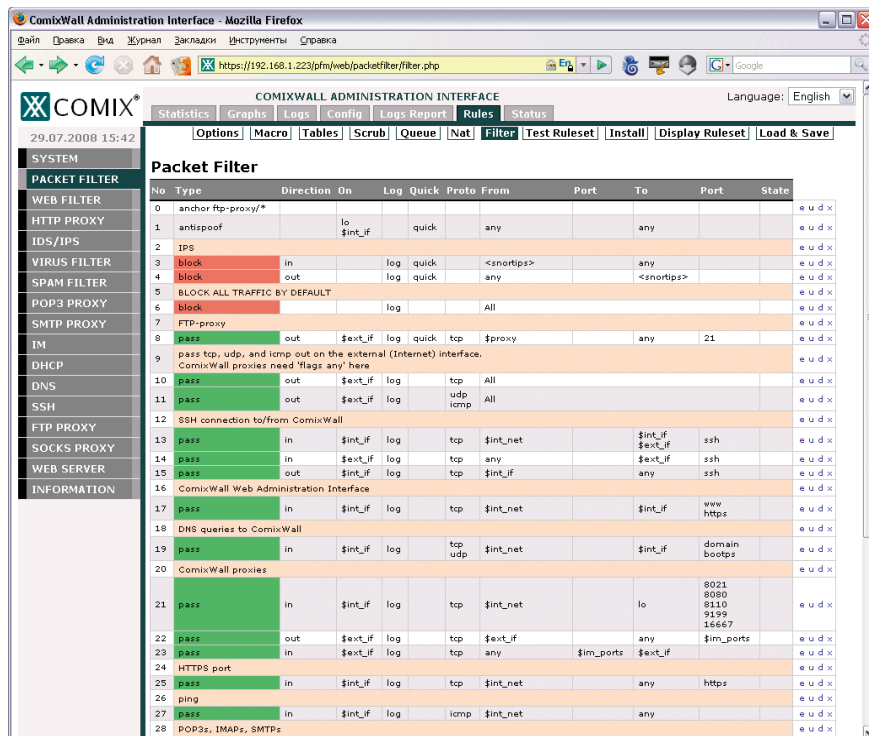


Рисунок 4. Редактирование правил pf

ретным модулем, входящим в состав системы (см. **рис. 2**). Последнее меню Information содержит ссылки на документацию, map-страницы и ссылки на сайты связанных проектов. Под основным меню находится небольшая панель, в которой выводятся показания температурных сенсоров (если они есть). После выбора пункта в основном меню, вверху страницы, будет доступно дополнительное меню, соответствующее выбранному модулю. Для каждого пункта они отличаются, но обычно присутствует пункт Info, в котором можно получить общую информацию, Graphs – графики, Logs – журналы, Configs – настройки. Для PF, например, есть еще пункт Statistic (см. **рис. 3**), в котором наглядно показана статистика работы пакетного фильтра и Rules – настройка правил. Редактирование любого параметра для человека, представляющего конечный результат, не выглядит сложным (см. **рис. 4**). Доступны подсказки, различные меню и списки предлагают предустановленные значения. В анализе журналов поможет система фильтров. Для графиков можно выбрать временной промежуток и вид.

По умолчанию все дополнительные сервисы, кроме антиспам-фильтра для входящих сообщений, включены, о чем будет выведена информация

в первом окне, которое появится после регистрации в системе (см. **рис. 2**). Правила pf по умолчанию разрешают работу по основным протоколам (веб, ftp, почтовый) из внутренней сети, поэтому ComixWall готов к работе сразу после установки.

Заключение

На сегодняшний день ComixWall не выглядит простым в освоении решением и вряд ли подойдет новичкам. Но наличие множества предустановленных сервисов и веб-интерфейса, упрощающего их настройку, будет оценено опытными администраторами, которым требуется удобная, понятная, безопасная, многофункциональная и легко обновляемая система, при помощи которой можно быстро развернуть защитный бастион. ●

1. Сайт проекта ComixWall – <http://comixwall.org>.
2. Страница проекта на Google Code – <http://code.google.com/p/comixwall>.
3. OpenBSD 4.3 Installation Guide – <http://openbsd.org/faq/faq4.html>.
4. Установка OpenBSD 4.2 – <http://www.lissyara.su/?id=1589>.
5. Яремчук С. Дистрибутив для создания межсетевого экрана pfSense. //Системный администратор, № 2, 2008 г. – С. 8-21.