

Endian Firewall 2.2: из Италии с любовью



Валентин Синицын

Организация шлюза в Интернет – типовая задача, которую с разным успехом решает множество специализированных продуктов. Нужен ли нам еще один?

Название этого продукта наводит на мысли о путешествиях Гулливера, остро- и тупоконечниках или, на худой конец, порядке следования байтов. Подозреваю, что на родном языке его разработчиков – итальянском – это слово тоже значит что-нибудь хорошее, хотя документальных подтверждений тому мне обнаружить не удалось. Как бы там ни было, под именем Endian скрывается специализированный дистрибутив Linux, реализующий функции брандмауэра, интернет-шлюз (с поддержкой нескольких подключений), хот-спота (только в коммерческой версии) и контроля за сетевыми угрозами (Unified Threat Management, UTM).

Endian Firewall (EFW) поставляется в двух основных редакциях: свободной (GPLv2) и бесплатной Community и коммерческой Appliance. Последняя, в свою очередь, подразделяется на аппаратные (Mini, Mercury, Macro, Macro X2 – в порядке наращивания возможностей) и программную (Software) разновидности. Endian Firewall Software Appliance можно установить на любой x86-совместимый компьютер подходящей мощности (рекомендуется 1 ГГц и 512 МБ оперативной памяти, а также не менее 4 ГБ на жестком диске, привод CD-ROM, клавиатура и монитор понадобятся только на этапе установки и устранения неполадок). Фирменные аппаратные решения Endian

(за исключением младшей модели – Mini – обладающей пассивным-охлаждением и настольным корпусом) монтируются в стандартной девятнадцатидюймовой стойке и имеют высоту 1U.

Как правило, в продуктах, обладающих открытой и закрытой версиями, первая служит своего рода тестовым полигоном для второй: на ней обкатываются новые идеи и функции, которые (после стабилизации) ложатся в основу бизнес-решения. В случае с Endian, похоже, все происходит наоборот: Community-версия получается путем урезания стандартного Endian Firewall (он же – Software Appliance) и при этом еще проходит свое собственное тестирование! Так,

на момент написания обзора, Endian Firewall Community 2.2 находился в стадии релиз-кандидата, тогда как коммерческая версия готовилась отметить первый месяц продаж.

О «родословной» Endian Firewall ходят противоречивые слухи. Официальный сайт [1] лаконично сообщает, что-де он «includes a Hardened Linux Based Operating System» (именно так, большими буквами, как имя собственное); DistroWatch.com утверждает, что в основе дистрибутива лежит Red Hat Enterprise Linux, а Википедия и вовсе предлагает почти библейскую историю в духе: «IPCor родил Endian, SmoothWall родил IPCor, а SmoothWall родился от LFS и Red Hat». Беглый анализ системы показывает, что каждый из них по-своему прав: скрипты инициализации и схема хранения настроек явно были позаимствованы у SmoothWall/IPCor (сейчас они, по правде сказать, уже достаточно сильно модифицированы), а распространение всего дистрибутива в виде набора RPM-пакетов и выбор языка Python для реализации большей части собственных функций (кроме, пожалуй, веб-интерфейса – он написан на Perl, более традиционном для дистрибутивов такого класса) – это влияние Red Hat. К слову сказать, для EFW выпускается комплект разработчика и исходные тексты (тоже в форме RPM-пакетов), однако на момент написания данной статьи они относились к предыдущей версии – 2.1.

На первый взгляд

Процесс установки Endian Firewall Community (и, надо полагать, не Community) вполне стандартен: система задает минимум вопросов на английском, итальянском или немецком языках – на выбор пользователя – и занимает весь жесткий диск (не забудьте сохранить с него ценные данные). Единственным сюрпризом является последовательная консоль: если на компьютере, отведенном вами для EFW, есть COM-порт и вам посчастливилось найти нуль-модемный кабель, можете начисто избавиться от клавиатуры с монитором и, в случае возникновения неполадок, входить в систему через Minicom или HyperTerminal, как в старые добрые времена. Ну а пока дистрибутив работает, как часы (на-

Основные компоненты Endian Firewall 2.2

- ☑ Ядро Linux 2.6.22.18.
- ☑ Apache 1.3.33 (для веб-интерфейса).
- ☑ Squid 2.6.STABLE-18 и DansGuardian 2.9.9.3.

- ☑ Антивирус: ClamAV 0.93 и Amavisd 2.5.4.
- ☑ Антиспам: SpamAssassin 2.2.7 и Pyzor 0.4.
- ☑ OpenVPN 2.1.
- ☑ Ntop 3.3.
- ☑ OpenSSH 3.9p1.

деюсь, что так и будет), к вашим услугам все блага современной цивилизации: административный веб-интерфейс с элементами AJAX (русский язык здесь присутствует, хотя перевод и не полон) и SSH. Для их использования необходимо только настроить «зеленый» (GREEN) сетевой интерфейс, указав его IP-адрес и маску подсети (по умолчанию это 192.168.0.15/24; если вы намереваетесь включить EFW в существующую локальную сеть, значения, естественно, придется подправить) – что и делает инсталлятор непосредственно перед тем, как начать копирование файлов. Не удивляйтесь, что у вас никто не спросит пароль root – это задача следующего этапа.

Первая загрузка тут же выдает встраиваемую природу EFW с головой: вместо традиционного приглашения ввести имя пользователя и пароль вам сообщают, по какому адресу доступен веб-интерфейс и предложат «сервисное меню» из трех вариантов: вход в систему, сброс настроек и установка заводских параметров и перезагрузка. Вся пост-инсталляционная настройка и сопровождение происходит через веб-интерфейс (см. **рис. 1**), доступный по протоколу HTTPS. SSL-сертификат является самоподписанным, кроме того, он удостоверяет доменное имя (которое автоматически генерируется при установке и может быть изменено впоследствии), а доступ из локальной сети с большой вероятностью будет происходить по IP-адресу – в общем, предупреждения браузера можно спокойно проигнорировать. Когда вы откроете веб-интерфейс в первый раз, вам (совсем как при знакомстве с новой точкой доступа или беспроводным маршрутизатором) предложат выбрать язык и часовой пояс, принять лицензию (GPLv2), восстановить резервную копию настроек (полезно, если вы переустанавливали дистрибутив) и ввести пароль администратора для доступа через Web, а также пароль root. Затем откроется мастер, со-

стоящий из семи шагов. Вас попросят указать, какие зоны будет обслуживать брандмауэр, а также распределить по ним сетевые интерфейсы и настроить стандартные параметры (IP-адреса, маски, имя хоста и т. д.).

Endian Firewall использует стандартную нотацию сетевых зон: зеленая (GREEN) – локальная (доверяемая) сеть, оранжевая (DMZ) – демилитаризованная зона, красная (RED) – Интернет и синяя (BLUE) для беспроводных клиентов. В каждой зоне должен находиться как минимум один сетевой интерфейс, при этом каждый интерфейс может быть ассоциирован лишь с одной зоной. Для красной зоны поддерживаются следующие типы подключений: Ethernet (статический и DHCP), PPPoE, ADSL (PCI и USB), ISDN, аналоговый/UMTS-модем (только в коммерческой версии – и почему бы?), а также специальный вариант Gateway (шлюз), который используется в тех редких случаях, когда машина с EFW не имеет красного интерфейса (то есть не подключена к Интернету напрямую), а для доступа в сеть используется внешний маршрутизатор. Все эти варианты подробно описаны в распространяющемся по лицензии GFDL англоязычном руководстве Endian Firewall [2], которое, на момент написания материала, было помечено как «разрабатываемое» («work in progress»).

На наш взгляд, подсистема настройки сети реализована в EFW не самым лучшим образом. Она, должно быть, прекрасно справлялась со своей задачей в предыдущих версиях продукта, но в 2.2, после реализации поддержки нескольких внешних каналов (uplink), стала несколько путаной. Предположим, у вас есть два Ethernet-интерфейса, подключенных к различным провайдерам, и вы хотите организовать с их помощью отказоустойчивость; красная зона же, по определению, одна. Вы не можете просто расширить ее на обе сетевых кар-

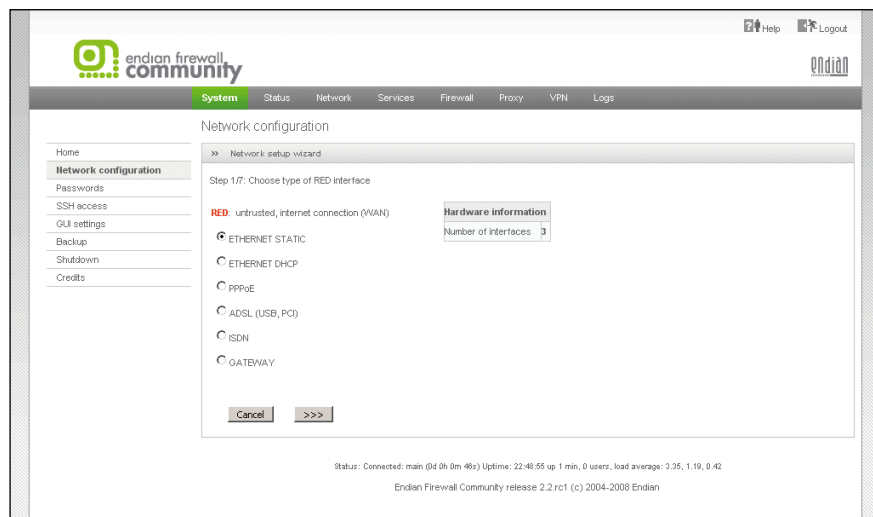


Рисунок 1. Веб-интерфейс Endian Firewall выполнен не слишком просто, но со вкусом

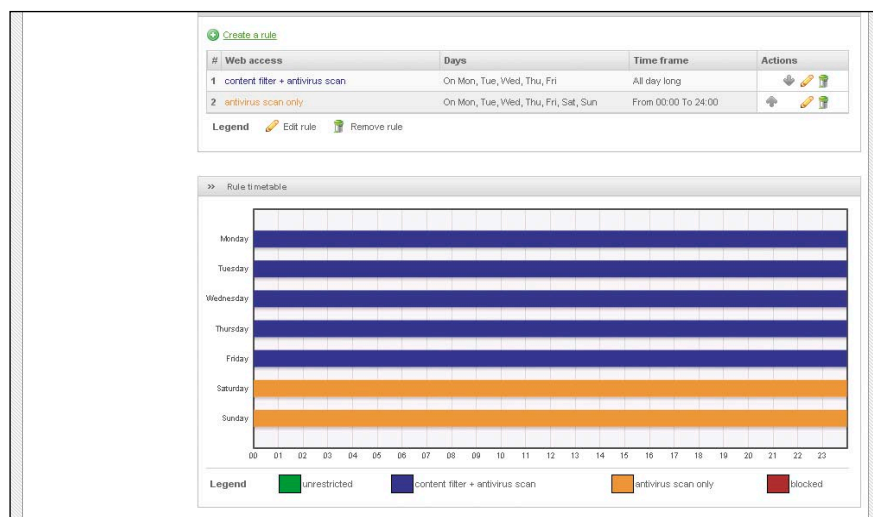


Рисунок 2. «Диаграммы Ганта» для фильтров Squid

ты, поскольку в данном случае они будут включены в мост с одним общим IP-адресом. Для решения данной задачи и были предложены внешние каналы, редактор которых доступен в меню «Networking → Interfaces». Внешний канал обладает таким же набором параметров, что и красная зона (впрочем, здесь есть одно, но важное исключение: uplink может быть PPTP-подключением. Будем считать, что это не архитектурное решение, а просто ошибка) – уже это наталкивает на мысль о «неполной нормализации», хотя сама идея – разделить «локальные» параметры настройки (IP-адрес, маску подсети, имя хоста и т. п.) от глобальных (адрес шлюза в сети провайдера) кажется вполне здравой, особенно если рассмотреть систему, у которой будет более одного канала в Сеть в каждый момент времени. Внешний канал может служить назначением (destination)

правила маршрутизации, задаваемого по соседству («Networking → Routing»). Прискорбно, но маршрутизация на основе политик (policy routing) в Community-версии не поддерживается, так что решать, что и куда посылать, можно лишь на основании сетевых адресов отправителя и получателя.

С маршрутизацией тесно связана другая тема – фильтрация пакетов. В основе ее реализации в EFW лежит, конечно, Netfilter [3], сложность правильной настройки которого (посредством утилиты iptables) уже вошла в хрестоматию стандартных «страшилок» начинающего Linux-администратора. Неудивительно, что Endian Firewall, как и многие другие проекты, стремится скрыть ее за набором человеко-понятных правил. Последние разбиты по группам: Portforwarding/NAT, исходящий трафик (Outgoing traffic), обмен данными между зонами (Inter-

zone traffic), VPN и доступ к системе. Настройки по умолчанию вполне разумны: из любой зоны разрешен исходящий трафик к внешним DNS-серверам и отправка наружу «пингов», беспроводные клиенты (зона BLUE), кроме этого, могут обращаться к веб-серверам по протоколам HTTP/HTTPS, ну а локальным компьютерам (зона GREEN) доступны сверх этого FTP, POP3/IMAP, SMTP и их защищенные разновидности. Все, что не разрешено явно, запрещено, поэтому вам, вероятно, придется добавить, как минимум, правила, открывающие доступ к сетям обмена мгновенными сообщениями (кстати, во встроенном списке сервисов присутствуют ICQ и MSN Messenger, но нет Jabber – для него номера портов придется вводить вручную). Впрочем, фильтрацию исходящего трафика можно и отключить.

Правила взаимодействия между зонами более простые – их суть сводится к тому, чтобы полностью изолировать DMZ (оранжевая зона) и беспроводных клиентов от локальной сети. Опять же, в реальной ситуации может потребоваться оставить некоторые хорошо определенные лазейки – скажем, активировать для зоны BLUE доступ по протоколу SMB. Разрешать все бессмысленно – тогда уж проще не выделять специальную зону. Как и в случае с исходящим трафиком, межзонный брандмауэр можно выключить.

Правила доступа к системе стоят особняком. Во-первых, встроенные записи нельзя редактировать (возможно, разработчики опасаются, что излишне ретивый пользователь отрежет себе доступ к административному интерфейсу), во-вторых, они всегда активны. Доступ к административному веб-интерфейсу разрешается из любой внутренней зоны (т.е. GREEN, BLUE, ORANGE и VPN), а вот SSH-соединение можно установить только из «зеленой» сети. По умолчанию, ICMP-запросы из красной сети не принимаются, и это следует иметь в виду при общении со службами поддержки интернет-провайдеров.

Только через мой... шлюз

Следующая важная вкладка, на которую можно обратить внимание, – это Proxy. Традиционно под данным тер-

мином понимается веб-кэш наподобие Squid [4], но Endian Firewall идет гораздо дальше: здесь собраны прокси-серверы для HTTP, FTP, SMTP/POP3, SIP и даже DNS. Большая часть из них обеспечивает также антивирусный (ClamAV) и антиспам (SpamAssassin/Pyzor) контроль.

Начнем, пожалуй, с World Wide Web. Его проксирование и фильтрация осуществляются традиционной связкой Squid и DansGuardian. Прокси-сервер может быть как прозрачным, так и обычным, причем эта настройка задается в отдельности для каждой зоны (т.е. можно, например, разрешить свободный доступ в Интернет из локальной сети и принудительно «заворачивать» на прокси беспроводных клиентов). Поддерживаются всевозможные механизмы авторизации: локальная (NCSA), LDAP (в том числе, в домене Active Directory), Windows (наверное, было бы уместнее написать NTLM и не вводить людей в заблуждение, тем более что в руководстве раздел по HTTP-прокси еще пока не написан) и Radius, а также политики. С помощью последних можно ограничить порты, доступные для проксирования, веб-клиенты и MIME-типы, а также указать, какие фильтры и когда будут доступны: скажем, активировать фильтрацию содержимого лишь в рабочее время. Конфигурация фильтров отображается в графическом виде внизу страницы (см. **рис. 2**), и можно легко видеть, какой участок недели остался неохваченным.

Вторым по популярности интернет-протоколом является электронная почта. Endian Firewall предоставляет прокси для POP3 и SMTP. Это может показаться странным, но в документации по их поводу не говорится практически ничего, а доступные настройки несколько сбивают с толку. Рискну, однако, упомянуть одну интересную функцию – защиту от спама. На чем можно тренировать спам-фильтр в POP3-прокси, у которого и собственной базы сообщений-то нет? По мнению разработчиков EFW – на любом удаленном сервере с поддержкой IMAP4, достаточно лишь рассортировать хранящиеся на нем сообщения на спамовые и хэмовые (а еще лучше – делать это на регулярной основе, к примеру, попросив пользователей перемещать спам в определенную папку). POP3-прокси позволяет выискивать и помечать спам-сообщения, на какой (внешний) ящик они бы ни приходили – это выглядит интересным, но не снижает нагрузки на интернет-канал организации, так что пользы от такой фильтрации будет едва ли больше, чем от локальной (средствами почтового клиента получателя).


Мы – за безопасные связи

Разумеется, Endian Firewall может быть не только посредником, но и предоставлять сервисы сам по себе. Особого упоминания заслуживает VPN. EFW поддерживает две технологии: IpSec и OpenVPN; мы будем говорить о последней. Доступны два режима работы: OpenVPN-сервер и OpenVPN-клиент (также известный как Gw2Gw – «шлюз/шлюз»; он пригодится, например, при подключении сети филиала к центральному офису). Примечательно, что OpenVPN-сервер запускается в режиме Bridged (а значит, удаленные клиенты смогут работать со всеми протоколами, полагающимися на широкополосную доставку: от Half-Life до SMB Browse) и перевести его в Routing средствами GUI нет никакой возможности. Для VPN-клиентов зарезервированы ад-

реса 192.168.0.129-192.168.0.190 (разумеется, если вы не меняли подсеть, выбранную по умолчанию).

Из других сервисов можно перечислить систему обнаружения вторжений Snort [5] и сетевой монитор Ntop [6]. А вот чего в EFW, по сравнению с его предком – SmoothWall – не достает, так это системы обновлений. Это тем более странно для дистрибутива, обеспечивающего безопасность целой сети, единственная уязвимость в котором может привести к очень серьезным последствиям.

В целом же Endian Firewall можно назвать весьма развитым и законченным решением.

Огорчает только отсутствие в свободной редакции некоторых функций, строго говоря, не являющихся корпоративными (той же маршрутизации по политикам). Схема поддержки нескольких внешних каналов также могла бы быть более удобной, но если перед вами стоит задача обеспечить доступ в Интернет для малой или средней сети и возможностей IPCop/SmoothWall уже не хватает, на данный продукт определенно стоит обратить свое внимание. 

1. Официальный сайт Endian Firewall – <http://www.endian.com>.
2. Endian Firewall Reference Manual r. 2.2.0.2 – <http://docs.endian.com/2.2/en>.
3. Проект Netfilter отвечает за фильтрацию пакетов в ядре Linux – <http://www.netfilter.org>.
4. Прокси-сервер Squid – <http://www.squid-cache.org>.
5. Система обнаружения вторжений Snort – <http://www.snort.org>.
6. Сетевой монитор Ntop – <http://www.ntop.org>.



VPS хостинг

Удобный. Надежный. Мощный.
Для веб-сайтов, баз данных и электронной почты.



➔ PHP5, MySQL5, MS SQL, .NET, FTP,
Mail-сервер, root-доступ.

24 ЧАСА
ТЕХПОДДЕРЖКА

ДОМЕН
ЗА НАШ СЧЕТ!

(495) 799-00-18
<http://www.rusonyx.ru>

Реклама