

# Удаленное администрирование активного оборудования узла Интернет-провайдера с помощью средств мобильной связи.

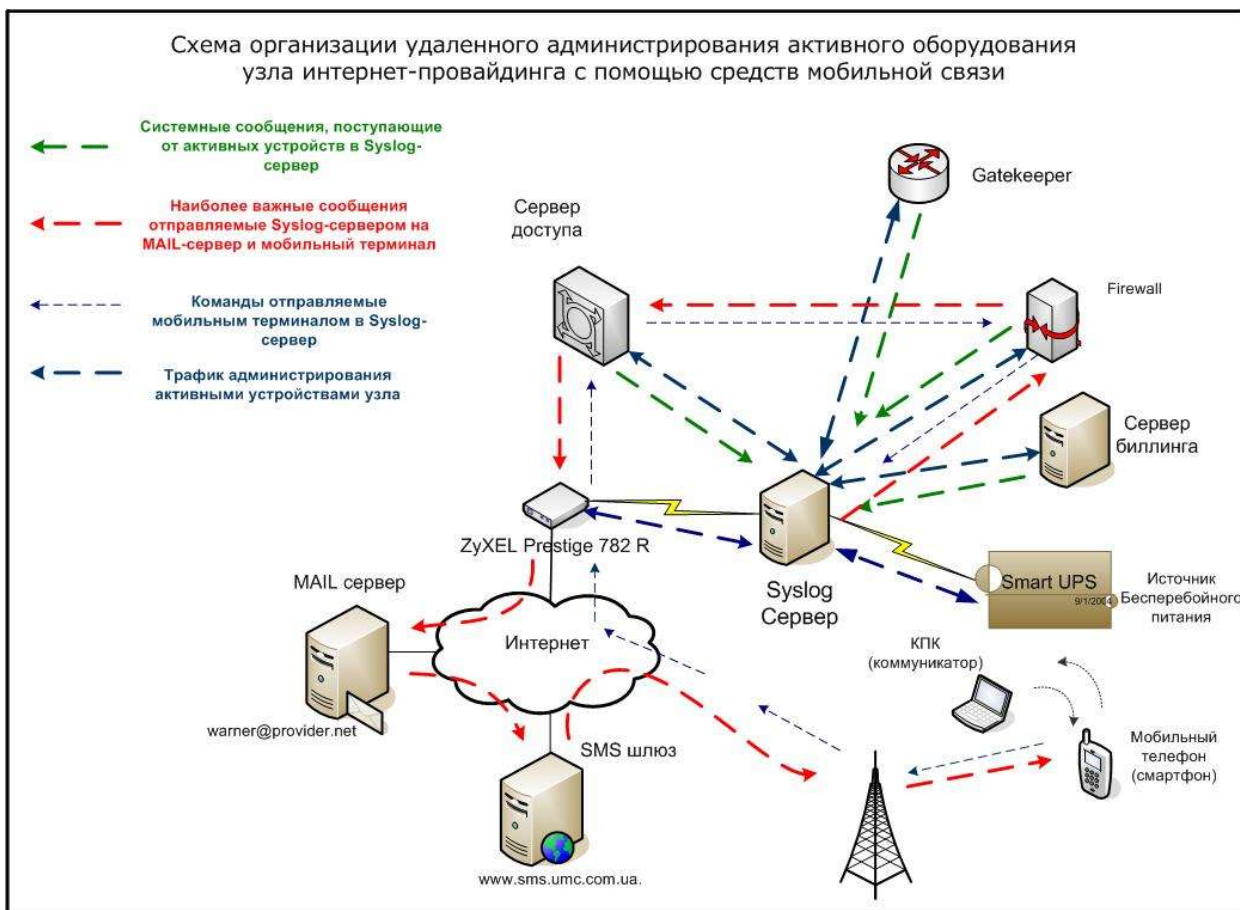
## Введение

Любой администратор знает, что наиболее важными аспектами администрирования узла Интернет-провайдера является мониторинг и систематический аудит активного оборудования – сервера доступа, сервера аутентификации удаленных пользователей, брандмауэра(устройства разделяющего локальные(внутренние) хосты и сети от наружных(Интернет) сетей). Наблюдение за выше упомянутыми устройствами, требуется для своевременного выявления брешей в безопасности, устранения их и совершенствования защиты сети, выявления ошибок в конфигурации и настройках систем и программного обеспечения. Оборудование Cisco также, как и Unix-подобные системы использует для мониторинга и аудита такие средства как отладочный режим для контролируемых служб и приложений операционной системы с выводом результатов отладки на консоль администратора и ведение журнала системных событий. Отладочный режим применяется администратором для устранения каких-либо явных нарушений в работе оборудования. Журнализация системных событий происходит в фоновом режиме в процессе нормального функционирования системы путем отправки сообщений разной важности и приоритетности в специальный файл. Конструктивная особенность Cisco-систем не позволяет размещение такого рода файлов на самих маршрутизаторах, серверах доступа – для этого используется внешний сервер журнализации, который на определенном порту ожидает сообщения от Cisco-устройства. Маршрутизатор (сервер доступа) знает о существовании такого устройства и шлет системные сообщения именно этому серверу журнализации, а не другому, тот в свою очередь, получив сообщения, записывает их в специальный файл. Этот файл системный администратор может прочесть в любое время, и использовать полученную из него информацию по назначению, например, получив сообщения об ошибках провести расследование и разобраться в причинах их появления, а также принять меры по устранению недостатков в работе системы.

В целом мониторинг и аудит обеспечивают постоянный контроль за системами и помогает эффективнее использовать сетевое оборудование.

## Syslog-сервер

Syslog-сервер, в нашем случае, представляет собой приложение «Syslog-ng» от <http://www.balabit.com/> для Unix-подобных систем, и является более гибкой и функциональной альтернативой стандартной службе журнализации Unix и к тому же является полностью бесплатным. "Syslog-ng" может быть установлен на любом i386 железе, работающем под операционной системой Unix, Linux в нашем случае это FreeBSD как зарекомендовавшей себя наиболее устойчивой, безопасной и надежной. Отличительной особенностью этого приложения является более эффективный подход к работе с информацией, подлежащей журнализации – это возможность довольно гибкой фильтрации поступающих сообщений и последующей обработки полученной информации от хостов-клиентов. Например: применение словаря ключевых слов, по которым существует возможность выделить из множества ненужного мусора наиболее важную для администрирования информацию с последующей отправкой этих сообщений на электронную почту или послать в виде sms-сообщения на мобильный телефон системного администратора. Таким образом, рутинная обработка довольно больших по объему файлов журнала, занимающая львиную долю рабочего времени, производится автоматически в реальном времени, благодаря чему администратор гораздо больше имеет времени на устранение тех или иных проблем.



## Удаленное администрирование

Все активные устройства сети узла, зная о существовании в сети сервера журнализации, отправляют ему копии всех системных сообщений. Syslog-сервер записывает эти сообщения в специальные файлы, для каждого устройства свой собственный файл. На схеме этот процесс отражен зелеными линиями. Сроки хранения файлов их размеры и количество определены конфигурацией встроенной службы ротации логов «newsyslog» или же программы «Logrotate».

“Syslog-ng” имеет словарь ключевых слов, если приходит от какой-либо системы сообщение, содержащее хотя бы одно слово, имеющееся в словаре, то копия данной строки целиком отправляется на почтовый адрес [warner@provider.net](mailto:warner@provider.net) (адрес вымышленный) MAIL-сервера.

MAIL-сервер в свою очередь пересылает копию этого сообщения через sms-шлюз мобильного оператора (например: [www.sms.ums.com.ua](http://www.sms.ums.com.ua)) на мобильный телефон в виде sms-сообщения. Довольно малого размера (всего 1 килобайт) сообщения доставляются довольно быстро.

Для чего нам нужен MAIL сервер? Во-первых, допустим часа два мы ничего не получаем – у нас есть возможность с помощью почтового клиента мобильного терминала проверить почту – приходят ли сообщения, и просмотреть их если таковые имеются. Во-вторых, копии всех важных сообщений мы имеем в почтовом ящике как вспомогательный резерв, если злоумышленник удалит файлы журнала с сервера.

Получая в реальном масштабе времени наиболее важные и критичные сообщения о поведении того или иного устройства, независимо от места нахождения системного администратора, предоставляется возможность оперативно реагировать на сложившуюся ситуацию. Например сделать звонок оператору находящемуся вблизи оборудования и дать ему соответствующие рекомендации по устранению проблемы. Либо, если сложилась критическая ситуация, прибыть на место самому.

Рассматривая ситуацию, когда не возможно в срок прибыть на рабочее место ввиду удаленности на больших расстояниях от рабочего места, либо по каким-то другим причинам, появляется потребность в удаленном доступе к системам узла с более

расширенными правами т.е. интерактивной работы с устройством, требующим срочного вмешательства администратора. Это может быть связано с несанкционированным доступом к системам узла, нарушениями и критическими ошибками в работе устройств, атаками на сетевые сервисы, когда оперативность вмешательства может избавить от более тяжелых последствий обслуживающий персонал и клиентов компании.

Организовать полный контроль над системами узла с помощью средств мобильной связи также не проблема. На сегодня определенные модели мобильных компьютеров, смартфонов и коммуникаторов стали довольно развиты в плане программного обеспечения. Для удаленного администрирования Unix-систем через сеть Интернет традиционно используется SSH-клиент, который является довольно надежным средством удаленного доступа к командному интерпритатору Unix-машины. SSH дословно переводится как «защищенная оболочка», поддерживает до десятка различных алгоритмов шифрования. Весь трафик шифруется задолго до аутентификации удаленного пользователя, что исключает не только прослушивание трафика, но и перехват паролей. На сегодня SSH-клиент на мобильном телефоне не новость, такие модели телефонов как NOKIA 6600/9210/9210i/9290/7650/3650, SONYERICSON P800 поддерживают полноценный SSH-клиент PuTTY, который был портирован из Unix-среды.

Доступ к системам с помощью таких устройств осуществляется точно также как если бы с хоста, находящегося в сети Интернет. Мобильное устройство с помощью протокола GPRS подключается к глобальной сети, далее в терминале телефона запускается PuTTY (SSH-клиент) с параметрами для входа на Syslog-сервер узла, проходим аутентификацию и получаем полный доступ к программной оболочке сервера, на схеме это указано тонкими синими линиями. Получив полный доступ к Syslog-серверу мы получаем возможность подключаться ко всем активным устройствам нашего узла (т.к. все они имеют интерфейс командной строки и предварительно для этого сконфигурированы), от имени Syslog-сервера, на схеме это жирные синие линии. Имея такое подключение администратор имеет полный контроль над всеми необходимыми системами узла. Как показано на схеме, если подключить к последовательному порту Syslog-сервера к примеру модем выделенной линии можно управлять этим модемом удаленно, если в COM-порт включить SmartUPS вы сможете удаленно контролировать состояние сети электропитания вашего оборудования, нагрузку на источник бесперебойного питания и реальные значения питающего напряжения, а если к примеру в словарь "Syslog-ng" включить такие слова как UPS или Power, то в случае бросков по питанию или временного отсутствия напряжения в сети вы будете уведомлены sms-сообщением об этом.

Одним словом эффективность использования системы будет ограничиваться только лишь вашей фантазией.

Внимание: при составлении словаря следует ОЧЕНЬ обдуманно подбирать ключевые слова, т.к. к примеру, если включить в словарь что-то вроде "TCP", то "Syslog" вас просто засыплет сообщениями среди которых трудно будет что-то полезное раскопать, так что наберитесь терпения и не пожалейте времени для отладки словаря – оно того стоит!

Ссылки по теме:

<http://www.balabit.com/> - сайт программы Syslog-ng (во FreeBSD присутствует в портах)  
<http://s2putty.sourceforge.net/> - страничка проекта «PuTTY для мобильных телефонов»

1 сентября 2004 г.

Инженер группы информационных технологий Иван Лежнев