Автор:
12.01.12 12:48 - Последнее обновление 02.03.12 12:40

Небольшой FAQ для тех кому руководство поставило задачу

мониторить сетевую активность пользователей.

Конкретно руководство хотело знать, на какие сайты ходят пользователи и сколько времени там проводят.
Т.к. пошагового руководства для начинающих, коим являюсь сам я не нашел, решил исправить ситуацию и написать.

Версия на pfSense на которой у меня работают данные настройки 2.0-RC3 built on Tue Jun 21 16:50:25 EDT 201 (i386), 2.0.1-RELEASE (i386) built on Mon Dec 12 17:53:52 EST 2011

1. Устанавливаем Squid + Lightsquid
Идем в System -> Packages -> Available Packages
- Находим squid stable в списке доступных пакетов, жмем + и ждем окончания установки.
- Тем же методом устанавливаем Lightsquid
- Проверяем, переходим в Installed Packages, убеждаемся что устанавливаемые пакеты присутствуют в списке.
Если присутствует идем дальше, если нет пробуем установить еще раз.

2. Настраиваем Squid
Переходим Services -> Proxy Server
- Proxy interface: LAN
- Transparent proxy: ставим галку
- Log store directory: /var/squid/log
- Language: Russian-1251
Остальные поля оставляем как есть
Жмем Save

3. Включаем ssh доступ и подключаемся
- System -> Advanced -> Admin Access
- Ставим галку на "Enable Secure Shell", по желанию меняем порт "SSH Port" (по умолчанию порт 22) Жмем Save.

Скачиваем и устанавливаем Putty и WinSCP.

4. Открываем WinSCP

- Жмем на New
- "Host name" указываем локальный ip адрес pfSense'a
- "Port number" если меняли в 3 пункте, то вводим его же.
- "User name" root
- "Password" можно оставить пустым, придется вводить каждый раз при подключении.
- Жмем Save.
- Указываем имя соединения, например pfSense
- По желанию жмем Language -> Get More... и скачиваем русский язык.
- Жмем "Войти"
- Принимаем открытый ключ, жмем "Да"
- Вводим пароль

Если все сделали правильно, увидим файловую систему.

5. Русифицируем отчеты LightSquid'a

- открываем /usr/local/etc/lightsquid/lightsquid.cfg

Находим WEB VARIABLES (можно воспользоваться поиском, достаточно нажать Ctrl+f)
-Меняем $lang = "eng"; на $lang = "ru";
Отключаем графический отчет, т.к. для него нужен внешний модуль.
-Меняем $graphreport = 1; на $graphreport = 0;
-Сохраняем жмем Ctrl+s
-Вводим пароль

6. Открываем Putty

- "Host name" указываем локальный ip адрес pfSense'a
- "Port number" если меняли в 3 пункте, то вводим его же.
- "Connection type" SSH
- Жмем save и open
- Принимаем открытый ключ, жмем "Yes"
- "Login as" root и ваш пароль
- Enter an option: 8

Если все сделали правильно, увидим консоль.

Проверяем конфиг Lightsquid'a
-Исполняем cd /usr/local/www/lightsquid/ && ./check-setup.pl
Если ошибок нет, увдим "all check passed, now try access to cgi part in browser"

Запускаем парсер squid логов
- Исполняем /usr/local/www/lightsquid/lightparser.pl и ждем завершения
- Открываем браузер и вводим http://ip pfSense/lightsquid/index.cgi

Если все сделали без ошибок, увидим то к чему шли.

7. Присвоим реальные имена пользователей по ip адресу

Обязательное требование, нужно чтобы ip адреса были статичными т.е. не менялись.
- открываем /usr/local/etc/lightsquid/realname.cfg и прописываем

Пример:

10.0.0.10 Admin
10.0.0.11 Офис Худолей
10.0.0.12 Турабелидзе Давид
10.0.0.13 Гурешидзе Мераб
10.0.0.14 Монтьева Наталья
10.0.0.21 Ардашева Ирина
10.0.0.22 Сердюков Игорь
10.0.0.23 Мурашева Елена
10.0.0.24 Шкаликова Дарья
10.0.0.25 Шкаликова Дарья
10.0.0.26 Резерв
10.0.0.27 Бохова Валентина

8. Объединим пользователей в группы, для удобства.
- открываем /usr/local/etc/lightsquid/group.cfg и прописываем
Пример:
10.0.0.10 02 Администрация
10.0.0.43 02 Администрация
10.0.0.11 02 Администрация
10.0.0.12 02 Администрация
10.0.0.13 02 Администрация
10.0.0.14 02 Администрация
10.0.0.21 03 Бухгалтерия
10.0.0.22 03 Бухгалтерия
10.0.0.23 03 Бухгалтерия
10.0.0.24 03 Бухгалтерия
10.0.0.25 03 Бухгалтерия
10.0.0.26 03 Бухгалтерия
10.0.0.27 03 Бухгалтерия

9. Если будем давать ссылку руководству, чтобы не светить свой зад сделаем следующее)
- открываем /usr/local/etc/lightsquid/skipuser.cfg и добавляем ip адреса, по которым статистика не будет учитываться.
Пример:
10.0.0.10

10. Авто обновление отчетов раз в час.
- Открываем /var/cron/tabs/root и после текста, вставляем */60 * * * * /usr/local/www/lightsquid/lightparser.pl
- Сохраняем закрываем.
Теперь каждый час у вас будут свежие отчеты.

{morfeo 19}

Enjoy.

оригинал: http://forum.pfsense.org/index.php/topic,43240.15.html

ссылка на материал: http://thin.kiev.ua/index.php?option=com_content&view=article&id=495:---http--squid--lightsquid--pfsense-20&catid=50:pfsense&Itemid=81

{jcomments on}