Добро пожаловать в Gene Office !

Яндекс

Инструменты для раб

Обновлено 07.04.2012 г.

На главную
Домашняя
KERIO
KERIO CONTROL
Kerio CONNECT
ИНСТРУМЕНТЫ
Скрипты KUAS
Скрипты ELUS
Скрипты KEAP
ESOFT WebFilter
SOPHOS
MCAFEE
SNORT
Антивирусы
Прочее
Загрузка
Обновления
Когда все плохо

FAQ Kerio Control - UKAIP от VITJAN:

как применить патч под Windows.

Для исправления большинства ограничений в функциях продуктов Kerio лучшим инструментом является утилита (патч) под названием Universal Kerio And Icewarp Patch FiNAL - UKAIP автор которого - незнакомый мне, но очень мной уважаемый VITJAN, известный по многим сайтам. (Версия 2.64 для Kerio 7.2.x , версия 2.65 для Kerio 7.3.x - суть применения не меняется, главное - правильно выбрать версию Kerio и соответствующую версию патча).

Патч является многофункциональным инструментом для исправления нескольких программных продуктов под разными операционными системами. При всех своих достоинствах у него есть один недостаток вследствие его универсальности - инструкция к нему способна вынести мозг любому.

Попробуем исправить это дело, сделав максимально понятными необходимые действия.

Учтем несколько моментов:

- для исправления разных версий Software Appliance в пакете выложены индивидуальные подробные инструкции, поэтому про эти продукты не будем говорить;

- тот, кто использует продукты IceWarp Corporation, сам способен разобраться в оригинальной инструкции, поэтому об этом тоже упоминать не будем;

- все функции, подлежащие исправлению - проверка лицензии, антивирус McAfee, антивирус Sophos, система IDS\IDL Snort и WebFilter - могут сосуществовать только в одной версии Kerio Control - 7.0.1 build 1098, поэтому будем говорить про нее (в более свежих версиях также все работает, но требуются дополнительные действия в зависимости от номера версии);

- там, где действия будут зависеть от версии Kerio, будем уточнять особенности;

- для исправлений антивирусов и Snort требуется локальное зеркало - веб-сервер. Vitjan использует для целей создания и наполнения контента такого сервера пакет KSUK.v1.02-ViTYAN, в который включены утилиты для обработки исходных файлов Sophos. Мы применим утилиты из этого пакета, но с ограничениями - веб-сервер создадим по-своему, наполнять его также будем по своим правилам, работу с Snort вообще сделаем самостоятельно.

Почему нельзя использовать обновления из триальных версий Kerio?

Начнем.

Мы предполагаем, что создаваемая нами система должна жить долго и счастливо, а потому будем поступать надежно - берем подходящее по производительности железо, берем лучшую на данный момент для этих целей операционную систему Windows

2008 Server R2 SP1, устанавливаем ее и конфигурируем для получения максимальной производительности серверных процессов. Для будущих целей устанавливаем роли Hyper-V, IIS7-сервера, DNS-сервера и можно установить роль WSUS. По горячим следам установки создаем две виртуальные машины с гостевой осью не ниже Windows 7 32- и 64-бит. Выключаем на всех трех машинах ненужные службы, УАК, Дефендер и проч. радости. Если хотим обновлять виртуалки - настраиваем их на обновление с нашего WSUS. Убеждаемся, что сетевые карты установлены, подключены и работоспособны. (я ничего не говорю про настройку виртуальных сетей - полагаю, что этот вопрос затруднений не вызвал). У нас есть доступ к интернету и все необходимые сведения от провайдера.

Все, мы готовы к любым передрягам на долгие годы.

Скачиваем необходимый нам дистрибутив Kerio Control - 7.0.1 build 1098 64-бит

Скачиваем и устанавливаем дополнительные антивирусные программы - McAfee Enterprise 8.8 и Clam Antivirus

Создаем и настраиваем локальный веб-сервер для будущих обновлений. Не задумываемся о том, как бы обойти этот этап - это глупо.

Скачиваем и распаковываем пакет KUAS для управления будущими обновлениями.

Скачиваем и распаковываем пакет Universal Kerio And Icewarp Patch v2.52 FiNAL - UKAIP.

Устанавливаем Kerio Control - 7.0.1 build 1098 64-бит.

А вот тут надо соблюсти несколько несложных условий:

ПЕРВОЕ И ГЛАВНОЕ - ***НА ДАННОМ КОМПЬЮТЕРЕ НЕ ДОЛЖЕН БЫЛ БЫТЬ УСТАНОВЛЕН РАНЕЕ НИКАКОЙ ПРОДУКТ Kerio ! НИКАКОЙ и НИКОГДА*** ! Если ваша установка Kerio пройдет с ошибкой - переустанавливайте систему без сомнений. Именно поэтому мы создали две виртуалки, чтобы можно было легко изобразить новенькую машинку, не отмеченную Kerioтством.

ВТОРОЕ ПРИНЦИПИАЛЬНОЕ - мы будем ставить Kerio Control в директорию

C:\Program Files\Kerio

и ни в какую другую, что бы нам не предлагал инсталлятор. Не пропустите этот момент при установке =- очень пригодится впоследствии, поверьте на слово.

ТРЕТЬЕ ВАЖНОЕ - мы отключили УАК и мы - админы на нашем хосте. Никогда не работайте под встроенной учетной записью Администратор, создайте нового админа с именем латинскими буквами и устанавливайте Kerio под его профилем.

Обычно установка проходит без особых проблем. Повлиять может только глупое вмешательство в настройки системы - изменение настроек NTFS вроде отключения длинных имен и проч. подобные глупости. После установки весьма желательно компьютер перегрузить.

Сразу после установки Kerio Control - 7.0.1 build 1098 64-бит

НИЧЕГО НЕ ПАТЧИМ !!!!!!!

КОНФИГ НЕ МЕНЯЕМ !!!!!!!

В триальной версии настраиваем доступ в интернет БЕЗ КАКИХ-ЛИБО ОГРАНИЧЕНИЙ и ОБЯЗАТЕЛЬНО РЕГИСТРИРУЕМ ТРИАЛЬНУЮ ВЕРСИЮ Kerio - фиксируем полученный номер типа TW029-RT4EW!!!

ОБЯЗАТЕЛЬНО запрашиваем номер лицензии для WEBFILTER !!!!!

После регистрации обязательно обновляем Sophos, Snort и обязательно убеждаемся, что WebFilter активен !!!

ОБЯЗАТЕЛЬНО ПЕРЕГРУЖАЕМСЯ и проверяем еще раз, что все дополнительные модули активны - и Sophos, и Snort, и WEBFilter !!!

Все эти манипуляции придется производить не раз на чистой виртуальной машине, поэтому к отработке навыков по первичным действиям надо отнестись очень серьезно потому, что любая ошибка на виртуалке приведет к бану вашего основного хоста, а это уже серьезно.

Kerio установлен, запускается и останавливается по командам диспетчера служб без ошибок, система не тормозит - значит, пришло время исправлять недостатки.

Применяем Universal Kerio And Icewarp Patch v2.52 FiNAL - UKAIP.

1. Останавливаем службу Kerio Control или через диспетчер задач, или через KerioMonitor.

Физически отключаемся от Интернета.

Не пожалеете об этом - береженого Бог бережет, не береженого конвой стережет.

2. Создадим папку C:\BACKUP и скопируем туда файлы

C:\Program Files\Kerio\WinRoute Firewall\winroute.exe

C:\Program Files\Kerio\WinRoute Firewall\avirplugins\avir_-sophos.dll

мы сохраним на всякий несчастливый случай оригинальные файлы перед исправлением.

3. Из папки .\Windows (X64) пакета UKAIP копируем оба файла ukaip64.exe и ukaip4alt.exe в

C:\Program Files\Kerio\WinRoute Firewall и C:\Program Files\Kerio\WinRoute Firewall \avirplugins

Смысл в двух файлах - на некоторых относительно старых компах и на некоторых типах процессоров файл ukaip64.exe отрабатывает с ошибкой. В таком случае надо использовать файл ukaip4alt.exe, повторно введя такую же команду.

4. На рабочем столе создадим ярлык для **cmd.exe** - командного интерпретатора. Через ПКМ запустим его от имени администратора.

5. В появившемся окне наберем руками или через копи-паст команду для перехода в директорию Kerio:

c:\windiws\system32>cd C:\Program Files\Kerio\WinRoute Firewall

увидим

C:\Program Files\Kerio\WinRoute Firewall>

6. Нам требуется WebFilter, поэтому первым действием будет его исправление (если данный компонент не требуется, то действие можно пропустить - но зачем отказывать себе в лишних возможностях?).

Тут несколько пояснений:

- мы используем созданный нами локальный сервер обновлений, расположенный на этом же хосте, где и Kerio. В принципе, таким сервером может выступать абсолютно любой веб-сервер, в том числе - встроенный сервер Kerio. Совершенно неважно - какой порт слушает этот сервер и где он расположен, он должен быть доступен по имени или адресу и его доступность мы должны проверить через браузер. Главное требование - в корне этого веб-сервера должен находиться файл getkey.php, в котором помещена информация о номере ключа лицензии.

- структура файла getkey.php проста

<?php echo "0:ko:53729:620755653:86400";?>

то, что является номером ключа. представляет собой цифры 53729:620755653. Этот код регулярно меняется и его надо эпизодически вручную перезаписывать в этот самый файл. Мы попозже выясним, что и как надо делать. А пока мы просто его скопируем и все.

Таким образом, при патче мы обязаны указать УРЛ-адрес веб-сервера. Какой? Общее требование - формат http(s)://<имя_или_адрес>:<номер_порта>. Особенность - если указан протокол https, то веб-сервер должен иметь сертификат, выданный одним из мировых поставщиков, а Kerio должен иметь возможность его проверить через Интернет - мы это исключаем полностью ! Поэтому указывать надо только протокол Http - вопреки расхожему мнению для обновлений используются оба протокола - если недоступно шифрование, оно не используется. Т.е. при использовании встроенного веб-сервера Kerio Control можно указать адрес http://localhost:4080/ , при использовании встроенного веб-сервера Kerio коннект - http://localhost:4040/ , для нашего сервера - http://updater/ и т.д.

При создании локального веб-сервера обновлений мы определились с возможными именами (сервер слушает на порту 80):

http://updater/ или http://172.16.101.1/ или http://antivirus-updater.MyLocalDomain.ru/

Выбираем любое - для WebFilter это неважно, например http://updater/ .

Для исправления WebFilter в окне смд набираем одну из команд:

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe -A

или

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe --force-trial-for-plugins-with-license --enable-kerio-to-esoft-redirect --enable-custom-license-server-for-webfilter=http://updater/

ВНИМАНИЕ !!! В версии патча 2.63 не следует использовать

ключ -A - он не работает.

Разница между командами - в подробностях. Со свичом -A патч начнет работать, задавая по ходу дела кучу непонятных вопросов, на которые надо давать ответы. Среди прочего будет запрошен УРЛ-адрес, по которому можно получить скрипт с действующим ключом и сам этот ключ, все остальное - ненужный мусор.

- при патче большинство вопросов относится к генерации файла getkey.php - месте его расположения, содержании и проч. Поскольку у нас есть образец этого файла getkey.php мы просто скопируем его в корень веб-сервера и этим пока ограничимся.

- при вводе ключа по ходу патча надо заменить двоеточие на прямой слэш, т.е. вводить так: 53729/620755653. Можно вводить любые цифры в указанном формате, это ни на что не повлияет.

Таким образом, мы можем на все вопросы патча давать любые ответы, но обязаны указать УРЛ-адрес веб-сервера.

Во втором случае или никаких вопросов не последует, или будет запрошен номер ключа. В любом случае будет установлен указанный адрес для получения файла getkey.php. Свич -A предназначен для любопытных, второй вариант - для опытных.

ВАЖНО: ***этот метод работает и в более ранних версиях Kerio Winroute Firewall, но в версиях Kerio Control 7.1.x есть ноанс - изменен механизм активации лицензии в Kerio, влияющий на активацию Вебфильра при использовании веб-серверов, не поддерживающих PHP, например - на созданном нами локальном зеркале обновлений. Суть изменений состоит в порядке обработки полученного от веб-сервера содержания файла getkey.php,***

Для нормальной работы WebFilter с таким сервером обновлений следует изменить содержание этого файла:

вместо

<?php echo "0:ko:53729:620755653:86400";?>

должно быть

0:ko:53729:620755653:86400

Измененный файл может использоваться на любых серверах, в т.ч. поддерживающих PHP, например - во встроенном веб-сервере Керио.

ВАЖНО: ***мы можем не использовать совсем локальный сервер обновлений и воспользоваться встроенным веб-сервером самого Kerio - никакой разницы для активации веб-фильтра это не имеет и может оказаться более удобным во многих случаях. В этом случае в качестве адреса целесообразно использовать адрес*** http://localhost:4080/ , отключив в консоли Kerio перенаправление на защищенное соединение для веб-интерфейса. Файл getekey.php необходимо расположить по адресу

C:\Program Files\Kerio\WinRoute Firewall\webiface

7. Закончим необходимые действия с файлом winroute.exe. Сгенерируем лицензию для отображения информации в заставке консоли Kerio. В окне интерпретатора наберем команду:

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe -l license.key

Патч попросит указать название организации и имя пользователя - указывайте что угодно. Название организации будет отображаться в консоли Kerio, имя - нигде.

Эта команда сгенерирует файл лицензии license.key (название принципиально), который мы в проводнике перенесем в папку C:\Program Files\Kerio\WinRoute Firewall \license .

ВАЖНО: ***никогда не пытайтесь устанавливать эту лицензию через менеджер лицензий в консоли Kerio ! Суть данного патча - лицензия вообще не нужна, она просто есть картинка и ничего более.***

Ну и, наконец, главное - снимем триальный период (если мы не активировали WebFilter). Это самая простая команда:

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe

ВАЖНО: ***Если проводился патч WebFilter, то данное действие не требуется и скорее всего оно завершится с ошибкой, поскольку указанные свичи уже обеспечивают снятие триального периода. Ничего страшного в таком сообщении нет.***

После этого Kerio работоспособен.

8. Если нам потребуется McAfee - а зачем же отказываться от отличного антивируса - то скачиваем необходимые для этого элементы и размещаем их в соответствии с рекомендациями.

9. Переходим к антивирусам. В окне интерпретатора вводим команды:

C:\Program Files\Kerio\WinRoute Firewall>cd avirplugins

получаем

C:\Program Files\Kerio\WinRoute Firewall\avirplugins>

Нам опять потребуется указать на этот раз имя (или адрес) нашего веб-сервера обновлений, а для McAfee еще и относительный путь. Мы определились, что полный УРЛ для McAfee - http://updater/mcafee/ поэтому, несмотря на то рекомендации Vitjan "UKP вопросит вас ввести DNS имя вашего сервера и относительный путь к папке обновлений" мы укажем именно УРЛ !

C:\Program Files\Kerio\WinRoute Firewall\avirplugins>ukaip64.exe avir_mcafee.dll --enable-custom-update-mirror-for-mcafee

> http://updater/mcafee/

именно так, со слешем !!!

Для версий 7.1.x и новее эта процедура не требуется. В качестве второго антивируса плагин может быть отредактирован прямо из консоли Kerio !

Ну, а теперь Sophos:

C:\Program Files\Kerio\WinRoute Firewall\avirplugins>ukaip64.exe avir_sophos.dll -S

Патч запросит два параметра - имя сервера обновлений и имя файла, описывающего структуру веб-сервера, где размещены обновления для Sophos. Т.е. - не полный путь, как у McAfee, и не УРЛ как у WebFiltera, а IP-адрес или ДНС-имя. Это недоработка автора патча. Ответим:

> updater/ (***antivirus-updater.MyLocalDomain.ru/ - как еще один пример***)

> ukerav.php

Файл ukerav.php свое имя и свое содержание получил от Vitjan , вообще он может называться как угодно - у Keriotов он называется update.php и структура его может быть самой разнообразной. Чтобы не плодить разнообразие, сохраним и имя, и структуру.

ВАЖНО !!! В версии Kerio Control 7.1.x УРЛ сервера обновлений не должен быть корочк 23 знаков, поэтому для этой версии необходимо использовать другой из наших возможных адресов: http://antivirus-updater.MyLocalDomain.ru/ В версиях 7.2.x этого уже не требуется.

10. Остается Snort, но для него патч не требуется - читаем здесь.

С исправлениями все - и ничего сложного, вся сложность в подготовительной работе.

НО ЭТО ЕЩЕ НЕ КОНЕЦ !!!!!!

НИ В КОЕМ СЛУЧАЕ НЕ ПОДКЛЮЧАЕМ Kerio К ИНТЕРНЕТУ !

Сначала осознаем - а что мы сделали? Мы изменили некоторые параметры Kerio и его отдельных модулей, но не все возможные (и недекларированные) параметры. Что-то осталось нетронутым. Мы указали пути к локальному серверу, но в принципе - его еще может и не быть, мы задали условия, но можем их не выполнять. Мы сделали главное - создали возможность для использования Kerio нестандартных параметров.

Если у нас есть файлы конфигурации от предыдущих рабочих инсталляций - копируем их в папку с Kerio. Еще раз проверяем, что Интернет не подключен и стартуем службу Kerio.

Если служба запустилась без ошибок, открываем консоль управления и соединяемся с Kerio. Проверяем заставку - там все без ограничений на имя организации, которую вы указали при патче. Тогда все отлично, и немедленно делаем главное действие - запрещаем доступ к сайтам, которые могут распознать нашу незаконную конфигурацию.

Для этого создаем группу IP-адресов, в которую заносим те адреса и диапазлны, которые указаны вот здесь. В правилах трафика верхними строчками запрещаем любой доступ к \ от этой группе(-ы). Это принципиально важное действие !!!

Если у нас уже создан и актуализирован сервер обновлений Snort, то запускаем скрипт control_snort.bat из пакета KUAS и проверяем лог на наличие ошибок.

Только после этих процедур можно подключить Интернет и начать настройку Kerio согласно вашим потребностям. В консоли управления подключаем внешний антивирусный плагин - McAfee или ClamAV, в настройках Snort отключаем обновленния - они нам больше не нужны, в правилах фильтрации http-трафика настраиваем WebFilter. Все проблемы устраняем правильной настройкой соответствующих модулей по описаниям, изложенным в факе.

РЕЗЮМЕ:

команды для патча Kerio при заданных условиях:

C:\Program Files\Kerio\WinRoute Firewall>**ukaip64.exe winroute.exe --force-trial-for-plugins-with-license --enable-kerio-to-esoft-redirect --enable-custom-license-server-for-webfilter=**http://updater/

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe -l license.key

C:\Program Files\Kerio\WinRoute Firewall>ukaip64.exe winroute.exe

C:\Program Files\Kerio\WinRoute Firewall\avirplugins>ukaip64.exe avir_mcafee.dll --enable-custom-update-mirror-for-mcafee

> http://updater/mcafee/

C:\Program Files\Kerio\WinRoute Firewall\avirplugins>ukaip64.exe avir_sophos.dll -S

> updater/

> ukerav.php

Осталось напомнить о виртуальных машинах. А все просто - вы восстановите любые повреждения, повторив весь этот путь на чистой машине и перекопировав потом папку Kerio на боевой сервер :) при сохраненных конфигах, разумеется. В критических случаях вы обновите все в нужный момент без всяких ухищрений. Да и потренироваться всегда сможете.

Помните:

- применять патч можно только к оригинальным файлам, за исключением пути для WebFiltera;

- отключать группу suki - значит потерять лицензи на WebFilter;

- апгрейд установленной и пропатченной по этой инструкции системы пройдет без проблем - не забывайте отключать Интернет;

- регистрировать повторно Kerio при апгрейде уже не надо;

- примененные для управления обновлениями скрипты - не догма.

На главную | Домашняя | KERIO | KERIO CONTROL | Kerio CONNECT | ИНСТРУМЕНТЫ
Скрипты KUAS | Скрипты ELUS | Скрипты KEAP | ESOFT WebFilter | SOPHOS | MCAFEE
SNORT | Антивирусы | Прочее | Загрузка | Обновления | Когда все плохо

(C) Gene Office 2011

Сайт Контакты