

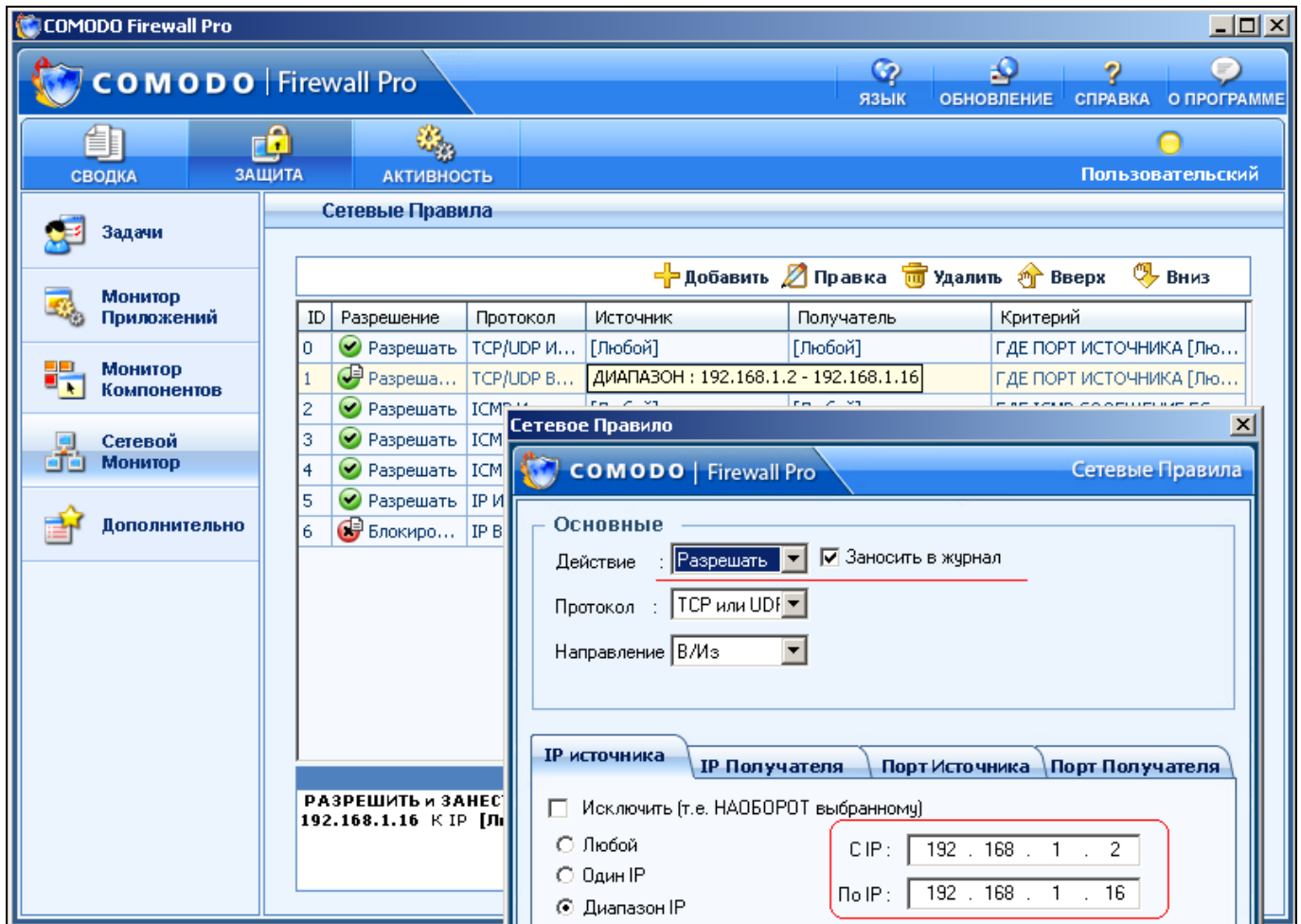
Настройка Comodo Firewall Pro 3 для поддержки FTP-серверов в доверенной сети

Андрей Микитенко

2007.11.25

В новой версии 3.0¹ в отличие от старой версии 2.4, доступные в локальной сети FTP серверы ДОЛЖНЫ быть «расшарены» на машинах, которые желают предоставлять доступ к своим ресурсам. Если ранее этот доступ можно было дать лишь «доверенным», сообщая нужные IP лишь тому, кто включён Администратором в список команды, то теперь² при открытии доступа этот компьютер становится доступным для пингования и FTP-сервер становится «видимым» в сетке...

Настройка изменилась по сравнению с прежней версией. Вот как выглядела страничка «Комодо» 2.4, отвечающая за настройку «прозрачности» для субсети 191.168.1.1 .. 192.168.1.16:



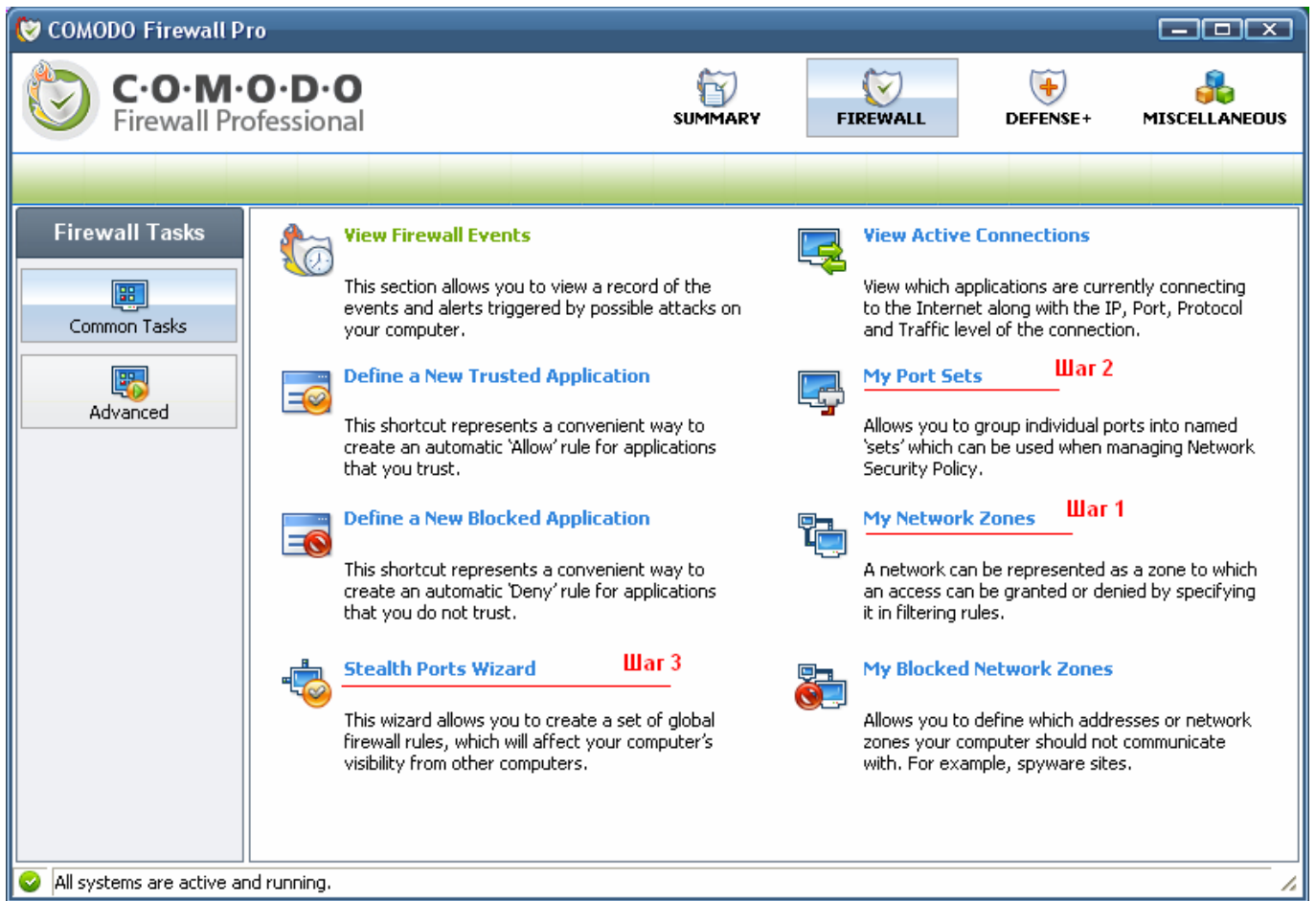
где нами была выставлена ранее в «Сетевом мониторе» эта же субсеть. Но теперь одного правила, увы, недостаточно, и нужно выставлять последовательно аж три правила (настройки).

¹ Это версия 3.0.13.268:

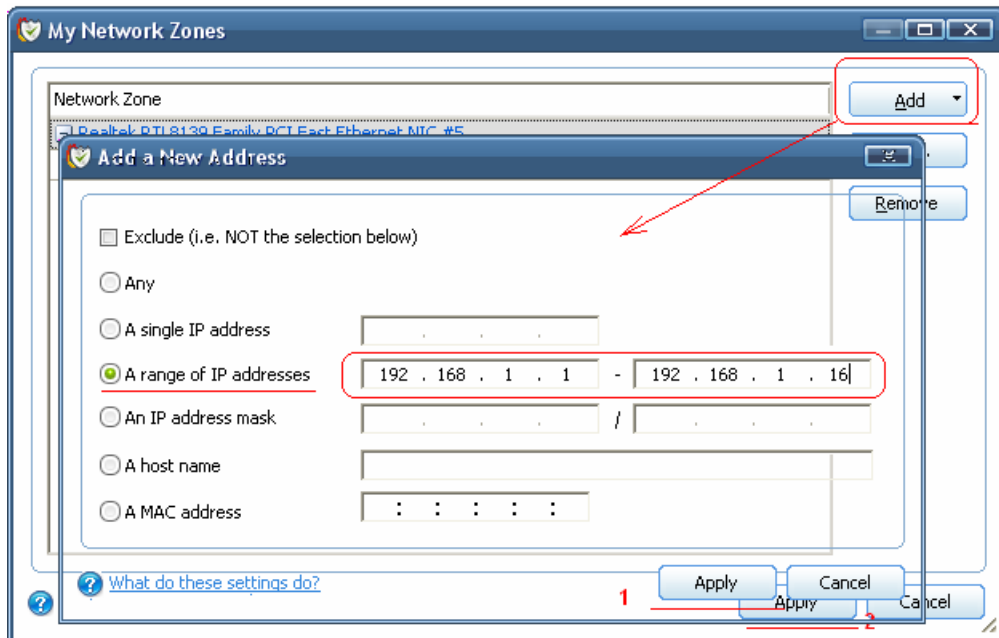


² Считаю, что это обстоятельство есть ослабление безопасности, к тому же неудобно Админу и Юзерам, и должно быть скорректировано в следующей версии Комодо! Нужно сделать так, чтобы была предоставлена возможность ОТДЕЛЬНО разрешить «прозрачный» доступ каким-то сервисам, наподобие FTP, тем самым - их доступность в сети, и ОТДЕЛЬНО разрешать или запрещать «стелле-моду» всего файера!..

Начинаем эти три шага настройки в панели «Комодо»:



Шаг 1. «My New Zones»

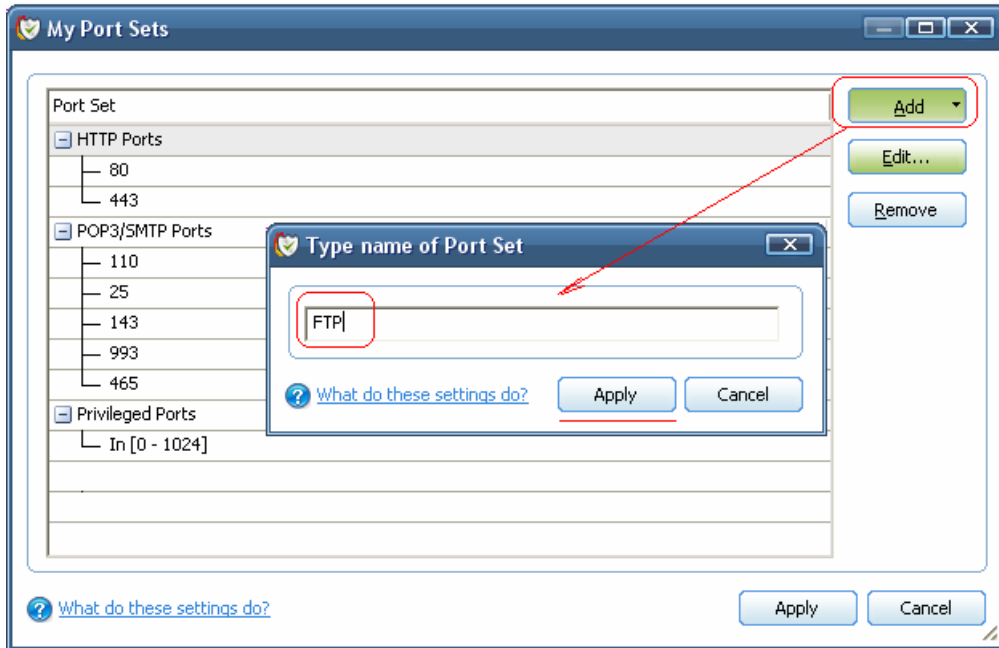


Нажимаем на кнопку «Add» (справа сверху панели) и в ней строку: «A new address...», чтобы вызвать панель «Add New Address». (Здесь для удобства показаны как бы наложенными друг на друга, - как первая панель, так и вызываемая затем по этой кнопке панелька.) На ней выбираем переключатель «A range of IP addresses» и вводим диапазон адресов субсети, в которой должны быть доступны на-

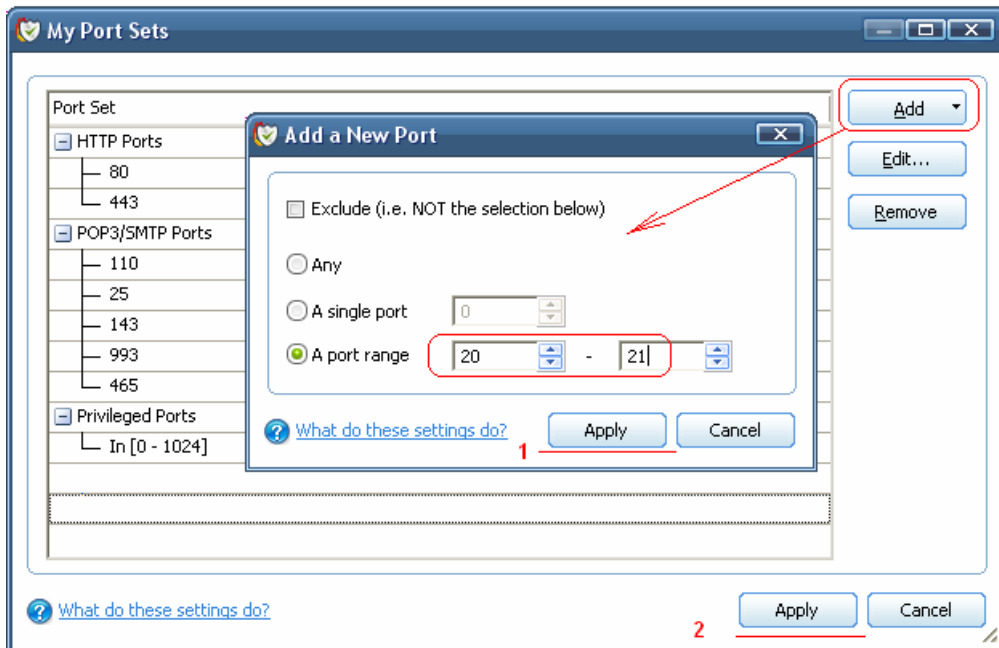
ши FTP-серверы. Нажимаем на ней кнопку «Apply»³ первый раз. Возвращаемся на «большенькую» панель «My New Zones» и там также нажимаем кнопку «Apply»⁴, чтобы зафиксировать всё сделанное.

Шаг 2. «My Port Sets»

Здесь нас ждут три «внутренних шага».



2.1. Нажимаем кнопку «Add» и в ней строку: «A New port set...» и оказываемся в панельке «Add New Port Set». Вводим в окно строчку FTP, нажимаем первую кнопку «Apply», возвращаемся в панель «My Port Sets». Там НЕ нажимаем кнопку «Apply», а просто переходим к следующему пункту.

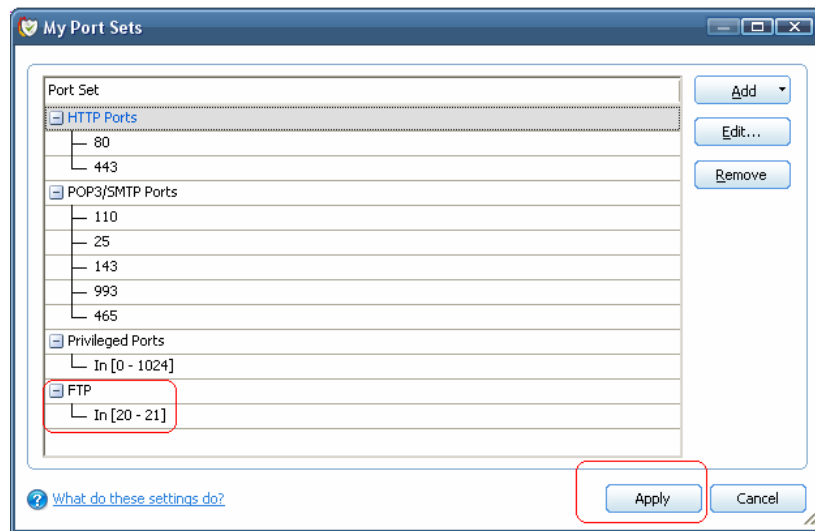


2.2. Опять нажимаем «Add» и в ней строку: «A New port...», чтобы появилась панель «Add New Port». Выбираем переключатель «A port range» и вводим диапазон портов 20 .. 21. Нажимаем первую кнопку «Apply», возвращаемся в панель «My Port Sets».

³ Здесь более уместна была бы традиционная кнопка «ОК»...

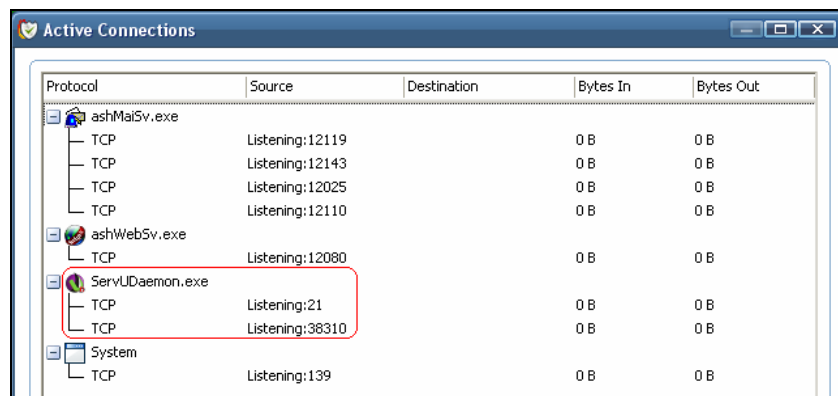
⁴ Межу прочим, создатели пакета явно не в ладу с программистскими стандартами де-факто! Ибо кнопками типа «Применить»/«Apply» испокон веков обозначалось действие, по сути – фиксирования промежуточных результатов *без выхода* из модальной панели! А вот кнопкой «Готово»/«ОК» обозначался как раз выход из панели настройки с фиксированием результата. На подобной панели напрашивается размещение трёх кнопок: «Apply», «ОК» и «Cancel».

Вот что мы увидим в результате:



2.3. Теперь уже нажимаем «Apply», чтобы зафиксировать сделанное. Фактически, создана зона видимости внутри сетки, но по какой-то причине она оказывается недоступной в сети, пока не будет выполнен третий шаг⁵...

Вызывает некоторое удивление не предусмотренные авторами вполне замечательного пакета «Комодо» 3.0 обычные в таких случаях стандартные «пресеты» и для FTP-сервера (для FTP-клиента они есть). А ещё было бы желательно простыми средствами (с помощью предустановленных пресетов) позволять Юзерам настраивать свои FTP-серверы в сетях за файрволом «Комодо» 3.0 для полной возможности раскрытия заложенных свойств, скажем, в такой популярной программе, отличный для Windows как FTP-сервер, каковым является «Serv-U». Имею в виду желательность уже преднастроенной поддержки - не только «пассивного режима», но и обычного...



Наконец, самое главное замечание⁶ по текущей версии:

Образовавшаяся «связка» между опцией снятия «стеллс» режима для доверенной группы адресов сети и возможностью «видеть» в этой группе адресов наши FTP-серверы – это не тот путь, по которому лежит магистральный тракт развития компьютерных технологий!..

Поэтому НУЖНО дать любому юзеру возможность отдельно избирать опцию снятия «стеллс-моды» для избранной субсети, и возможность без этого назначать «прозрачность» передачи для избранной группы адресов, наподобие того, как работал фильтр «Сетевой Монитор» в «Комодо» версии 2.4 - с его гибкими правилами.

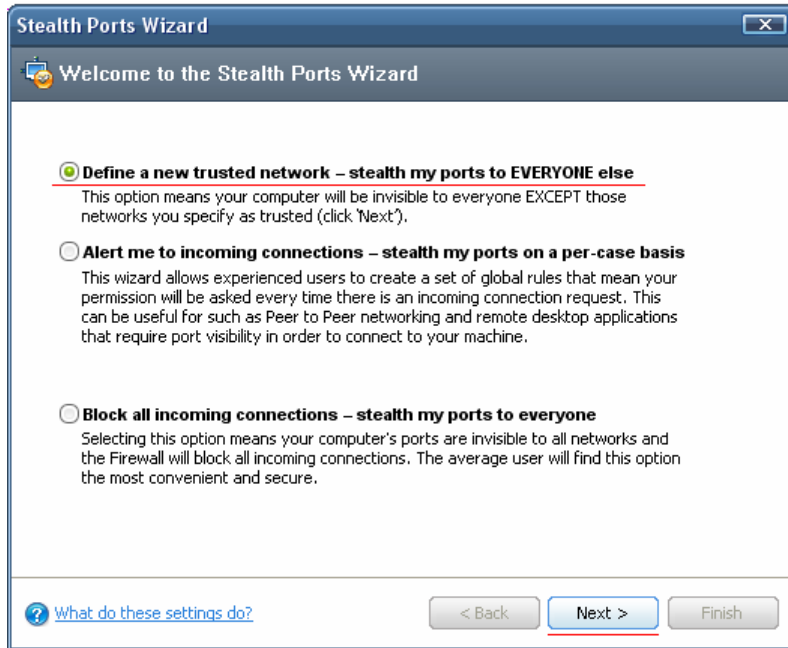
Итак, после небольшого отступления, вызванного недоумением по пути выставления необходимых настроек, возвращаюсь к нашим... баранам.

⁵ Это шаг, между прочим, не вполне-таки «прозрачный» для понимания необходимости его выполнения...

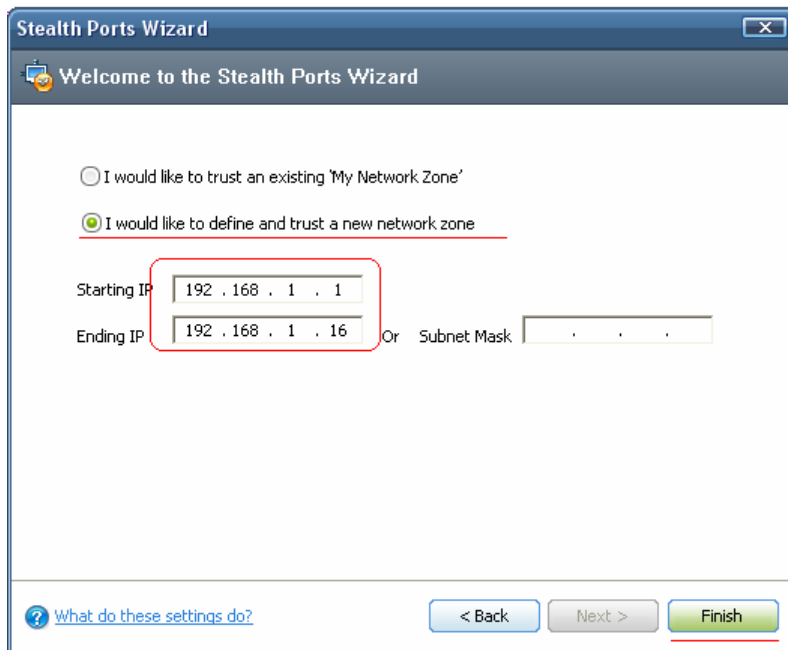
Из-за этого я решил написать эту инструкцию, прежде всего, для своих коллег. Ибо и сам я, несмотря на свой почти 20-летний опыт «юзанья, гм, всего цифрового», далеко не сразу сообразил необходимость настроить третий параметр, многократно пробуя – чего же не хватает файеру, чтобы пропустить FTP-пакеты вовне сервера в доверенную сетку...

⁶ И пусть кто-то скажет: дескать, это «частное мнение» владельца или админа частной сетки!.. ☺

Шаг 3. «Stealth Ports Wizard»



Эта панель имеет 3 варианта настроек, нам нужен первый: «Define a new trusted network – stealth my ports to EVERYONE else». Выбираем этот переключатель и нажимаем кнопку «Next >». Появляется панель:



где нам нужно выбрать переключатель «I would like to define and trust a new network zone» и ввести в поля диапазон адресов (Starting IP – Ending IP) нашей подсети. Затем нажимаем кнопку «Finish» и возвращаемся в предыдущую панель «Stealth Ports Wizard»⁷, где нам нужно нажать кнопку «Apply», чтобы зафиксировать результат настройки.

* * *

В результате этих трёх шагов фаервол окажется настроенным для «прозрачного» перенаправления FTP-пакетов внутри нашей доверенной сетки с диапазоном введённых адресов. Остаётся лишь разрешить доступ к сети (стандартной панелью «Комодо» при первом вызове) всем сервисам и службам, включая «администратора» FTP-сервера, у нас – это приложение (см. ярлык) «Serv-U», чтобы они опознавались фаерволом. Это всё! Успехов!

⁷ Вызывает удивление невозможность увидеть в этой панели уже однажды настроенные предпочтения! Такое ощущение, что программисты поленились дать в панели, вызываемой по кнопке «Next», отображение ранее сделанных установок, подобно тому, как в формах, скажем на форумах, отображены уже ранее сделанные настройки пользователя...