Поддержание безопасности сети с помощью NetTool Series II

Поддержание безопасности сети – это один из важнейших элементов вашей работы. Неавторизованные приложения, такие как шпионские программы и бесплатные программы с рекламными баннерами или объявления внутри, а также вредоносные вирусы, достигли опасного уровня развития и процветания. Эти приложения не только угрожают безопасности данных, но и снижают эффективность работы сети или даже препятствуют подключению пользователя. Поэтому ваша организация планирует использовать, или уже использует, прогрессивные меры безопасности, такие как протокол аутентификации 802.1X.

NetTool Series II с новой функцией **NetSecure** может помочь обнаружить неавторизованные приложения и обеспечить без проблемное внедрение протокола 802.1X. Поскольку в большинстве случаев пользовательские ПК являются либо целью, либо источником угроз безопасности, наилучший способ обнаружить эти угрозы – это тестирование и мониторинг при последовательном подключении между пользовательским ПК и сетью. NetTool Series II обладает уникальными возможностями для проведения таких тестов, благодаря его функциям мониторинга портов при последовательном подключении.

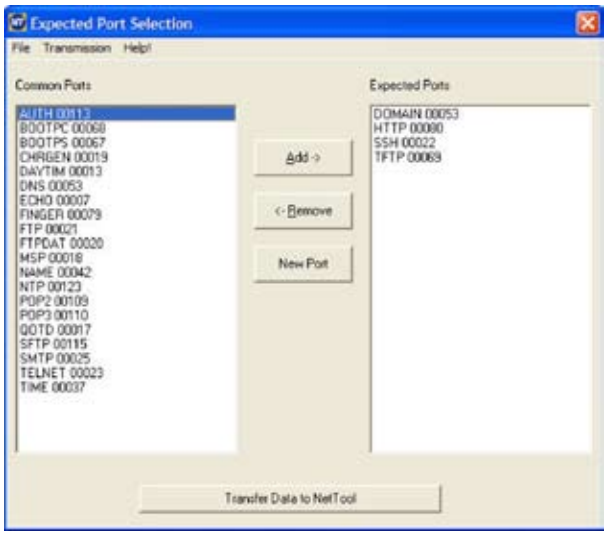
Если вы рассматриваете использование протокола 802.1X, вам также следует подумать об использовании тестера соединения, который может аутентифицироваться в вашей сети. Если тестер не имеет функций 802.1X, вы не сможете получить доступ к сети и провести необходимые тесты. Помимо обеспечения доступа к сетям, защищенным с помощью протокола 802.1X, NetTool Series II может помочь в двух других отношениях. Во-первых, он может эмулировать клиента для проверки правильности настроек 802.1X. Во-вторых, он может отслеживать процесс аутентификации пользователей при последовательном подключении для выявления ошибок.

Отслеживание шпионских и незаконных программ и вирусов

Самой распространенной проблемой безопасности в современных сетях являются скрытые, многократно используемые вредоносные приложения, работающие на пользовательских ПК. Эти приложения, известные как шпионские и незаконные программы и вирусы, обычно устанавливаются без согласия пользователя и могут снижать производительность компьютера, чрезмерно расходовать трафик и даже препятствовать подключению к сети.

Самый лучший способ выявить такие неавторизованные приложения – это тестирование и мониторинг при последовательном подключении между пользовательским ПК и сетью. NetTool Series II обладает уникальной функцией NetSecure для проведения таких тестов путем мониторинга портов при последовательном подключении. При наличии подозрительной активности вы можете подключить прибор между пользовательским ПК и сетью для отслеживания трафика порта. Неожиданный трафик можно отделить от ожидаемого и проанализировать на предмет наличия потенциального злого умысла.

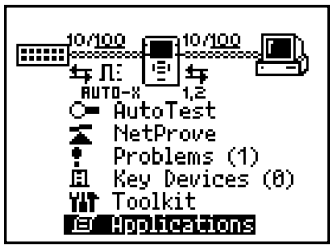
Вот как он работает:
Прежде всего, функцию мониторинга портов NetSecure необходимо настроить на распознавание ожидаемого трафика, входящего на ПК и исходящего с него. Это делается с помощью программного обеспечения NetTool Connect.



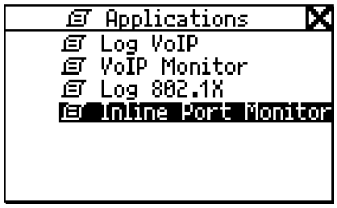
Выберите ожидаемые порты и приложения из списка слева и добавьте их в список справа. Эти приложения – при наблюдении с помощью NetTool Series II – будут указаны как ожидаемые и отфильтрованы из журнала, в котором останется только неожиданный трафик.

Последовательно подключите NetTool Series II к ПК и запустите функцию AutoTest, установив таким образом соединение с обеих сторон – с ПК и с сетью. Выберите «Приложения» в верхнем окне.

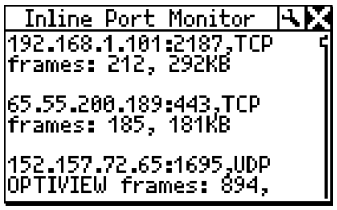
Обезопасьте свою сеть с помощью функции NetSecure прибора NetTool Series II



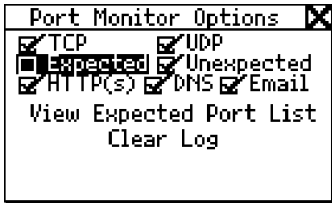
В меню «Приложения» выберите «Последовательный мониторинг портов».



По умолчанию в окне будет отображаться ВЕСЬ трафик, входящий на ПК и исходящий с него, рассортированный по IP-адресу/порту, количеству пакетов и объему данных. При возможности под IP-адресом будет указано DNS-имя.



Список можно фильтровать по ожидаемому и неожиданному трафику. Для выявления в списке неожиданного трафика выберите иконку «Инструменты» и снимите флажок с пункта «Ожидаемый». Затем подождите несколько минут, пока прибор соберет данные из сети, распознает и интерпретирует оставшийся трафик.



Если на ПК работает какое-либо неавторизованное приложение или он заражен вирусом, в списке мониторинга портов могут появиться несколько подозрительных записей для любых IP-адресов и портов. Поскольку таких приложений очень много, значения пар IP-адрес/порт могут быть любыми.

Что искать в списке мониторинга портов:

- Незнакомые адреса за пределами сети
- Несколько записей по одному адресу для нескольких портов
- Адреса в пределах локальной сети, не являющиеся адресами серверов (возможна передача вируса от одного клиента другому)
- Передача данных на другую машину, локальную или удаленную, не инициированная пользователем

При просмотре списка неизвестных IP-адресов для установления владельца адреса можно воспользоваться службой поиска типа «WhoIs», такой как **www.arin.net**. Адреса, принадлежащие компаниям Microsoft, McAfee, Apple или другим известным производителям программного обеспечения, скорее всего не будут связаны с вредоносным трафиком. В большинстве случаев этот трафик состоит из обновлений и законной передачи данных.

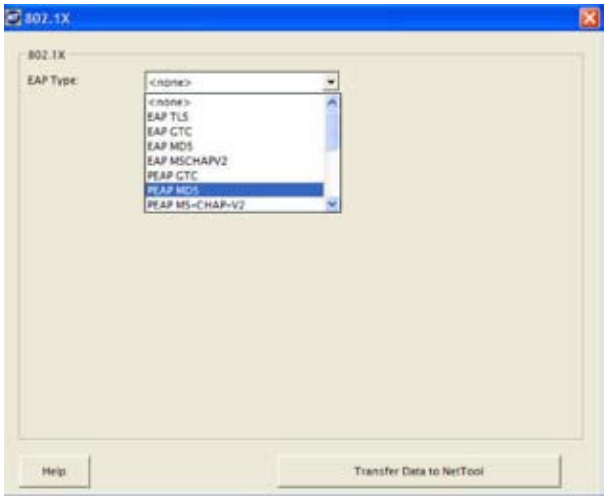
Если трафик признан вредоносным, приложение необходимо удалить. Используйте авторизованный инструмент для удаления шпионских программ или обновите антивирусное приложение и просканируйте ПК на наличие новейших вирусов.

Помощь при внедрении протокола 802.1X

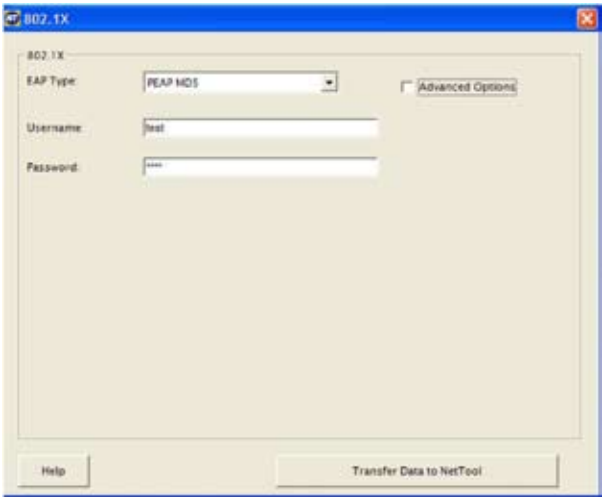
Лучше средства обнаружения вредоносных приложений может быть только система безопасности, которая изначально препятствует их проникновению в сеть. Все более популярным методом становится протокол аутентификации 802.1X, благодаря его надежности и экономичности. Этот IEEE протокол устанавливает стандарты для большинства современных портов Ethernet и позволяет ИТ-администраторам авторизовать доступ к проводным сетям аналогично доступу к беспроводным сетям.

Во время внедрения протокола 802.1X или перемещений, дополнений и изменений в сети на основе протокола 802.1X NetTool Series II может помочь проверить настройки конфигурации, прежде чем подключить нового пользователя, снижая таким образом вероятность последующего устранения неисправностей на этом же компьютере. Прибор может сделать это путем эмуляции клиента с соответствующей конфигурацией, сертификатами и паролем.

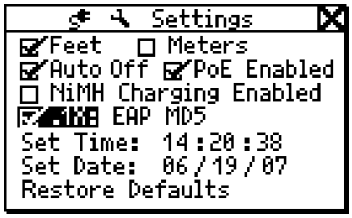
Вот как он работает:
Сконфигурируйте информацию для аутентификации 802.1X, используя входящее в комплект программное обеспечение NetConnect. Запустите программу и нажмите кнопку «802.1X». Это позволит выбрать из раскрывающегося меню нужный тип протокола EAP.



После выбора типа протокола EAP, используемого для аутентификации 802.1X, введите имя пользователя и пароль.



Загрузите настройки конфигурации в прибор NetTool Series II, подключив его к порту USB и выбрав пункт «Передача данных на NetTool». Убедитесь, что в настройках NetTool включена функция аутентификации 802.1X, чтобы при подключении прибор использовал регистрационные данные протокола 802.1X.



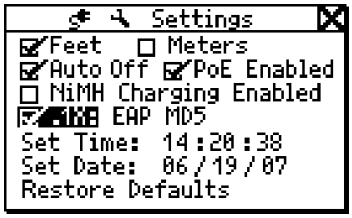
Проведите односторонний тест, подключив NetTool непосредственно к сетевому разъему и включив функцию AutoTest. Если прибор смог установить соединение, используя регистрационные данные протокола 802.1X, на экране появится соответствующее сообщение. Это говорит о том, что в прибор были загружены верные регистрационные данные и что другие устройства с такими же данными также должны работать.

NetTool проследит за ходом аутентификации 802.1X и при наличии проблем обозначит их.

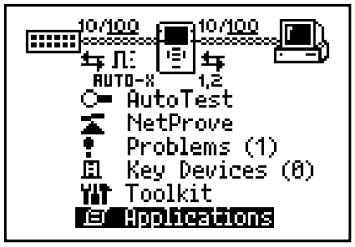
Устранение проблем при аутентификации 802.1X

Если протокол 802.1X уже внедрен в вашу сеть, возможно, вы уже сталкивались с различными проблемами подключения пользователей, причины которых сложно установить. Здесь могут оказать значительную помощь функции последовательного подключения NetTool Series II. При включенной функции NetSecure прибор можно последовательно подключить между ПК и сетью для наблюдения за процессом аутентификации и выявления ошибок.

Прежде всего, последовательно подключите NetTool Series II на участке между ПК и сетью. При этом важно, чтобы был отключен клиент 802.1X в настройках конфигурации NetTool. Таким образом, NetTool не сможет отправить запрос 802.1X вместо ПК, а просто проследит за попыткой подключения ПК.



Включите ПК и запустите AutoTest на приборе NetTool для установки исходной защиты 2-го уровня. Чтобы проследить за ходом подключения, выберите пункт «Приложения» в главном окне прибора NetTool.



Выберите «Журнал 802.1X» для просмотра журнала хода подключения.

При запросе данных начните процедуру авторизации на ПК, используя при тестировании имя пользователя и пароль. Прибор проведет мониторинг запросов и ответов в ходе аутентификации между клиентом и сервером, отображая в журнале всю передачу. Сервер должен запросить у компьютера идентификационные данные и протокол аутентификации. Если аутентификация прошла успешно, NetTool отобразит соответствующую запись в конце журнала. Если в процессе подключения произошли ошибки, NetTool отобразит, где они наблюдались.

Заключение

При регулярном тестировании безопасности сети пользователи будут довольны работой сети, а ИТ-специалисты смогут заранее предупреждать проблемы безопасности или подключения.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks работает более чем в 50 странах мира. Чтобы найти ближайшее к вам представительство, зайдите на веб-сайт **www.flukenetworks.com/contact**.

©2007 Fluke Corporation. Все права защищены.
Напечатано в США. 7/2007 3092020 A-RUS Ред. A