Maintaining network security with NetTool Series II

Maintaining network security is one of the most important elements of your job. Rogue applications like spyware, adware, and menacing viruses have reached an alarming stage of proliferation and sophistication. These applications not only threaten data security, but can also deteriorate network performance or even prevent user connectivity. As such, your organization is probably considering, if not already using, advanced security measures like the 802.1X authentication protocol.

NetTool Series II, with its new **NetSecure option**, can help both to identify rogue applications and ensure smooth implementation of 802.1X. Because most security threats either target or originate from user PCs, the best way to detect them is by testing and monitoring inline between a user PC and the network. NetTool Series II is uniquely equipped to do this with its inline port monitoring capabilities.

If you are considering 802.1X, you need to consider a connectivity tool that can authenticate on your network. Without 802.1X capabilities in the tool, you will not have access into the network and will not be able to run the tests you need. In addition, to providing access into 802.1X – secured networks NetTool Series II can help in two additional ways. First, it can emulate a client to verify proper 802.1X settings. Second, it can monitor the user authentication process inline to identify any failures.

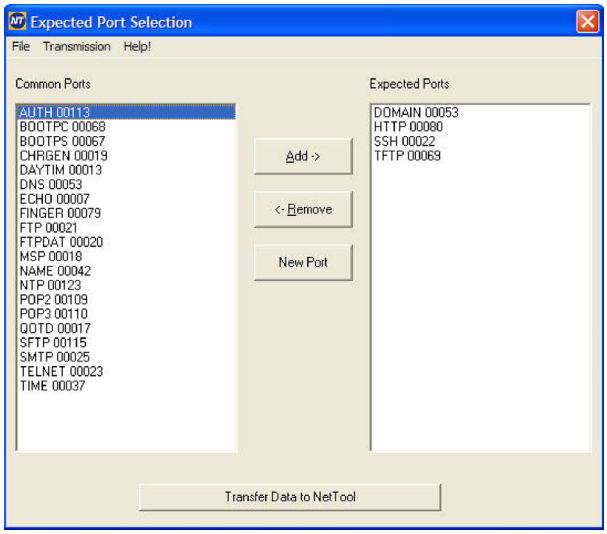
Monitor for spyware, malware and viruses

The most common security problems on today's networks involve hidden and oftentimes malicious applications running on user PCs. Commonly referred to as spyware, malware, or viruses, these applications are usually installed without the user's consent, and can degrade PC performance, introduce excessive traffic and even prevent connectivity.

The best way to detect rogue applications is by testing and monitoring inline between a user PC and the network. NetTool Series II is uniquely equipped to do this with the NetSecure option's inline port monitoring capabilities. When suspicious behavior exists, the tool can be plugged inline between a user PC and the network to monitor port traffic. Unexpected traffic can be separated from expected traffic and analyzed for potential malicious intent.

Here's how it works:

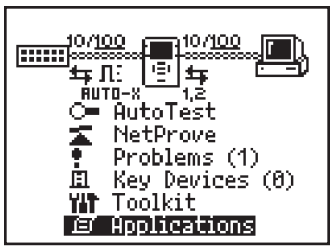
Initially, the NetSecure port monitoring feature must be configured to identify expected traffic to and from the PC. This is done through the NetTool Connect software.



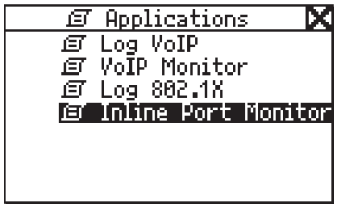
Select expected ports and applications from the list on the left and add them to the list on the right. These applications – when observed by the NetTool Series II – will be listed as expected and can be filtered out of the log, leaving only unexpected traffic.

Connect the NetTool Series II inline with the PC and run "AutoTest" establishing a link on both sides – to the PC as well as the network. Select "Applications" from the top level screen.

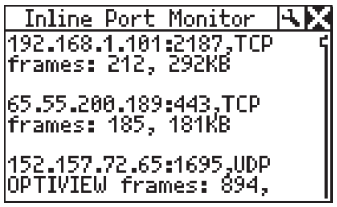
Secure your network at the desktop with the NetSecure option for NetTool Series II



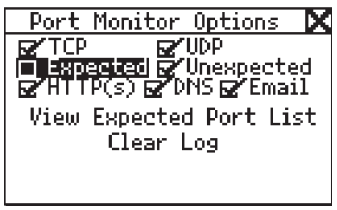
From the Applications menu, select “Inline Port Monitor.”



By default, the screen will display ALL traffic to and from the PC, listed by IP/Port, number of packets, and amount of data. Where possible, a DNS name will be listed under the IP address.



This list can be filtered by expected and unexpected traffic. To isolate unexpected traffic from the list, select the Tool icon and uncheck the “Expected” box. The tool should then be allowed to gather several minutes of data from the network before the remaining traffic is identified and understood.



If a PC is running some type of rogue application or is infected with a virus, there may be several suspicious entries in the Port Monitor list for any number of IP addresses and ports. Since there are so many types of these applications, the IP/Port pairs could be any value.

Things to look for in the Port Monitor list:

- Unfamiliar off-net addresses
- Several entries for a single address on different ports
- Local network addresses that are not servers (a client could be infecting another client on the network with a virus)
- Non-user triggered data transfers to another machine, local or remote

When searching through the list of unidentified IP addresses, it may be helpful to use a “WhoIs” lookup to identify the owner of the address range such as **www.arin.net**. Addresses belonging to Microsoft, McAfee, Apple, or another recognized software vendor is most likely non-malicious traffic. In most cases, these are simply updates and legitimate data transfers.

If the traffic is ultimately deemed to be malicious, you will need to remove the application. Use an authorized spyware removal tool, or update the PCs anti-virus application and scan for recent viruses.

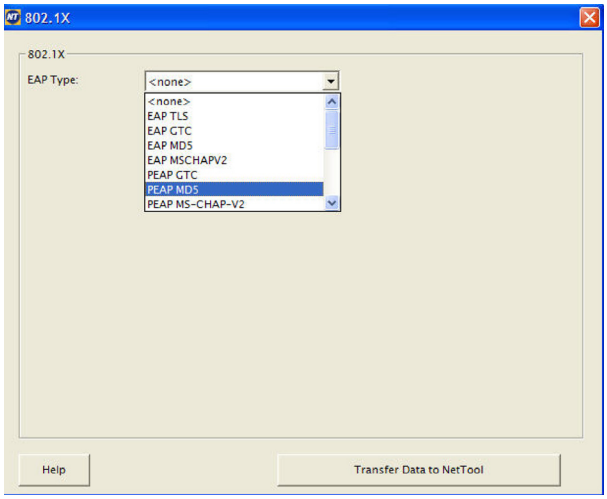
Assist in 802.1X deployment

Even better than having a tool to identify rogue applications is having a security system that prevents them from entering your network in the first place. An increasingly preferred method, because of its robustness and economic feasibility, is the 802.1X authentication protocol. This IEEE protocol ships standard on most of today’s Ethernet ports and allows IT administrators to authorize access to the wired network similar to how they authorize access to the wireless network.

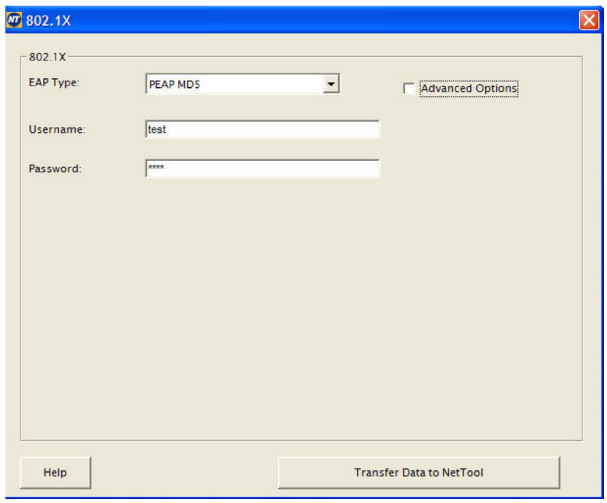
During deployment of 802.1X or moves, adds, changes on an 802.1X network, NetTool Series II can help to verify configuration settings before attempting to connect a new user, thus reducing the likelihood of a return to the user PC for troubleshooting later on. The tool can do this by emulating a client with the proper configuration, certificates and password.

Here's how it works:

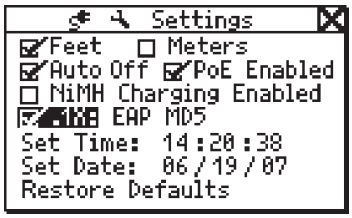
Configure the 802.1X authentication information using the included NetConnect Software. Open the program and click the "802.1X" button. This will allow the appropriate EAP protocol type to be selected from the dropdown menu.



After selecting the EAP type in use for 802.1X authentication, enter the username and password.



Load the configuration settings onto the NetTool Series II by connecting through the USB port and clicking "Transfer Data to NetTool." Make sure that the 802.1X authentication feature is enabled in the NetTool settings so it will use the 802.1X credentials to establish a link.



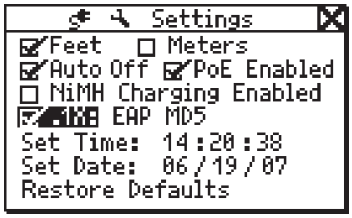
Perform a single-ended test by plugging the NetTool directly into the network jack and executing the AutoTest. If the tool is able to establish a link using the 802.1X credentials, it will be displayed on the screen. This verifies that the proper credentials been loaded into the tool, and other devices with the same credentials should work.

The NetTool will monitor the 802.1X authentication sequence and flag problems should they occur during login.

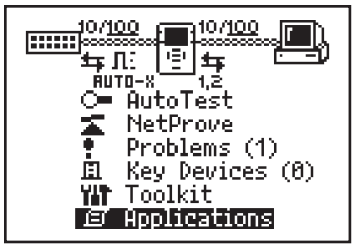
Troubleshoot 802.1X authentication problems

If 802.1X has already been deployed on your network, you have likely experienced various user connection problems that cannot be readily identified. Here is where NetTool Series II's inline capabilities can really help. With the NetSecure option enabled, the tool can be plugged inline between a PC and the network to observe the authentication process and flag failures.

First, connect NetTool Series II inline between the PC and the network. It is important that the 802.1X client be disabled in the NetTool configuration settings. This way, the NetTool will not send an 802.1X supplication on behalf of the PC, it will simply monitor the PC's connection attempt.



Power on the PC and run the AutoTest on the NetTool to establish the initial layer 2 connection. To monitor the connection sequence, select Applications from the main screen on the NetTool.



Select Log 802.1X to bring up the connection sequence log.

On the PC, begin the login sequence when prompted, utilizing the username and password under test. The tool will monitor the authentication requests and responses between client and server, displaying all communications in the log. The server should request an identity and authentication protocol from the PC. If the login is successful, the NetTool will display this at the bottom of the log. If the connection sequence fails at any time, the NetTool will display where it failed.

Conclusion

Taking the steps to ensure your network is secure through testing will keep users happy with network performance, and will keep the IT staff from having to be reactive when there is a problem with either security or a connection.

NETWORKSUPERVISION

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

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 7/2007 3082078 A-EN-N Rev A