

Securing your network from the inside: adding a portable layer of protection

When it comes to securing your network from internal threats, there are many steps you can take to pre-empt potential risks. First, understand the common causes of security threats; and, second, use the right tool to identify them. This paper will outline some of these causes and will explain why having the right tool can enable network professionals to quickly identify security threats – keeping your network – and users – safe.

Table of contents

Understanding internal security risks . . .	2
How a portable analyzer helps detect security risks.	3
Scenarios:	
Addressing the threat of wireless rogue access points	3
Putting a stop to unauthorized applications	3
Student hacks into university network through default switch setting.	4
Detecting when restricted documents are downloaded.	4
Solution: portable integrated analyzer . .	5

Understanding internal security risks

Security used to be a peripheral issue for network engineers, an outside danger taken care of by other groups in the IT organization. But with the rise of peer-to-peer programs and instant messaging, and the need to comply with regulatory requirements surrounding data security, network engineers now must address security threats generated on the inside. Even the strongest firewall can't keep out a growing problem: employees using unauthorized devices and applications that inadvertently create holes in your network. Whether it's a wireless access point brought in from home or a seemingly innocuous exchange of instant messages, employees are inadvertently compromising security.

The new challenge for network professionals is twofold: scanning the network for unauthorized devices that could cause a breach in security and focusing attention on suspected trouble spots on a case-by-case basis. Security is a never-ending battle. And increasingly, network engineers are being called upon to do more to address security than they have in the past.

One reason for the new, enlarged role network engineers now play is the cost of failure. When internal security issues aren't adequately addressed there can be serious repercussions. A company's confidential documents, private personnel files and other sensitive data can be downloaded and stolen. A weak spot in the company's firewall can increase the threat from hackers.

What's required is another layer of protection that enables network engineers to address threats whenever – and wherever – they emerge. To diagnose security problems, network professionals should use a portable tool they can carry directly to the site in question. Without this equipment, network engineers aren't able to make a diagnosis where it's most beneficial – at the site of a problem. Instead, they must rely on hardware that can't be moved or a laptop running multiple applications that may – or may not – help them to accurately assess the threat.

Using a portable tool, network professionals can investigate a suspected problem where and when it is occurring in real time – immediately taking action and closing gaps in the network when an employee is found using an improper device or application. With routine auditing, vulnerabilities in the network can also be quickly uncovered.

Because ensuring a network runs smoothly is a network engineer's primary duty, security can sometimes be a secondary concern. By using a tool that provides flexibility in addressing both routine maintenance as well as potential security breaches, network engineers can help search out trouble spots, detect and repair them, all while keeping their network functioning at a high level.

“A recent survey released by market research firm NewDiligence and commissioned by security vendor FaceTime Communications, showed applications such as IM, peer-to-peer (P2P), Skype and other consumer VoIP services, and Web conferencing are costing companies up to \$130,000 per year to root out security incidents caused by the unsanctioned applications.”

Devices and applications that put the network at risk:

- Wireless Access Points (WAPs)
- Laptops
- Consumer-grade routers
- Peer-to-peer applications such as Skype, BitTorrent, KaZaA, Freenet, eDonkey and Gnutella
- Instant messaging such as Windows Messenger, AOL Instant Messenger and Yahoo! Messenger

Regarding the increased use of Skype, one senior research analyst at Info-Tech Research Group cites figures showing 30% of the installed base using it for business purposes.

Processor.com <https://www.processor.com/editorial/articl>

How a portable analyzer helps detect security problems

Most companies rely on Internet filtering programs, intrusion detection software and firewalls that run 24x7. These solutions bring good results in preventing outside security threats. But they still leave areas of the network unprotected when an employee sends an instant message outside the network or conducts business using a wireless access point brought from home. These vulnerabilities are often unknown but can be isolated through direct testing.

The best way to address the problem of unintended security breaches is to analyze the network on a routine basis. Plugging in a laptop and running a variety of applications will catch some of the problems. But a significant number will still go unnoticed without going to the source of the problem.

Using diagnostic tools at a problem's source also helps when investigating whether an employee is inadvertently creating a security gap by using unauthorized applications or devices. To trace a problem and get to the root of it in real time requires a portable device that can be moved to any location within the network.

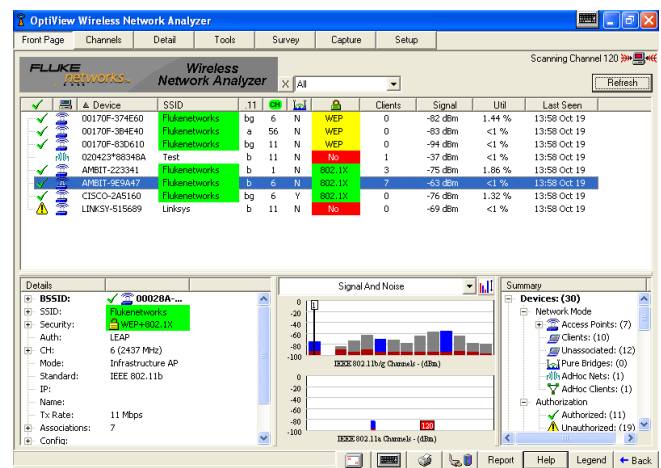
The following scenarios illustrate how a portable network analyzer can help keep confidential information secure, bolster security against potential hackers, and help monitor P2P applications and unauthorized devices brought into the workplace.

Addressing the threat of wireless rogue access points

An outside salesperson visits corporate headquarters once a month and while there connects with the company's network using his laptop. To make the connection, he brings along a wireless access point from home. But while he's busy getting company business done he doesn't realize he has opened a security hole in the network.

A hacker sees an opening and breaks into the company's network, stealing confidential information.

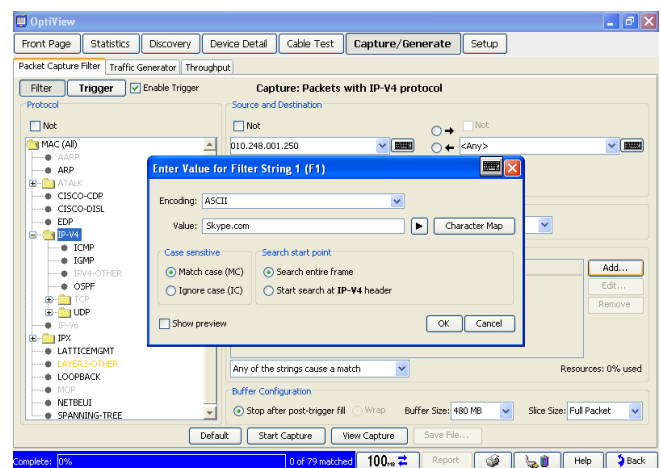
Later, the IT department uses a portable network analyzer to hunt for rogue devices on the wireless network. They're surprised to find not just one but four unauthorized devices. Within a few minutes, the portable analyzer locates the rogue access point and the engineer shuts it down – preventing further theft of information and other malicious mischief. Now the company performs routine monthly audits to make sure all devices on the network are approved. Having a portable analyzer enables the network engineer to discover and manually detect all access points – including finding unauthorized APs from the wired side at remote sites. Once located, the switch port where an unauthorized AP is connected can be shut down directly from a portable analyzer. Or network engineers can physically remove the AP using the portable analyzer to hunt down the exact location using its wireless analyzer and uni-directional antenna.



Putting a stop to unauthorized applications

The marketing and engineering teams of a company with worldwide offices want a better way to talk with one another on a regular basis. A few tech-savvy employees download Skype onto their computers.

But the same technology that allows users to establish direct connections with each other makes the company's network vulnerable to Trojans, worms and viruses. And because it's P2P, it allows private company information to be shared between users, without security precautions. Skype and similar P2P applications such as KaZaA make the host computer and network available to unauthorized users – inviting hackers and corporate spies. Using the free string match filter of a portable analyzer allows the network engineer to look for keywords or phrases to find such use of applications. In this case, the analyzer used the "skype.com" filter via a routine audit. The engineer used the portable integrated analyzer in a temporary monitoring mode from 7 a.m. to 9 a.m., when employees typically logged on. Skype was discovered and the employees informed about the threat to security. Since then, the network engineer regularly uses the portable analyzer to look for any application that compromises company security.



Student hacks into university network through default switch setting

Researchers at a school of medicine are complaining that they are randomly losing network connectivity. Investigation reveals that the affected users are on the fifth floor of a building where a new switch was recently installed. The network engineer uses a portable integrated analyzer to drill into the switch and view the activity on each switch port. Most of the time, the ports appear to be forwarding traffic. But random ports seem to be shutting down intermittently. The network engineer checks the switch configuration using the analyzer and confirms that some ports have been shut down. The engineer also observes a higher than normal amount of SNMP traffic on the network. When the top SNMP conversations are probed, it's clear that traffic is coming from a student who is hacking into the switch and using SNMP to randomly change the status of the switch ports from up to down.

What isn't clear is how the student broke into the SNMP community string. The engineer does some detective work and uses the analyzer to connect to the switch using a web browser. To do so, the engineer has to authenticate, using the correct user name and password. It's revealed that the SNMP community strings haven't been changed from their default values. Once they're changed, the problems stop. Because new switches have also been installed in other places on campus, the network engineer decides to use the discovery feature of the portable analyzer to check for other devices with default community strings and isn't surprised to find others configured in this same unsafe way.

As the above scenarios show, a portable analyzer adds another layer of security that helps keep corporate documents and sensitive personal information safe. And because the analyzer can be applied directly to suspected trouble areas, it can help prevent students and employees from inadvertently opening the network to threats when they use unauthorized devices, instant messaging or any other P2P application.

Detecting when restricted documents are downloaded

Soon after hiring a new receptionist, a company started hearing rumors about inter-office emails with attached documents being forwarded outside the network. Some were benign, while others contained confidential information about company strategy and expansion plans. Network engineers used advanced packet capture and filtered on specific words and text strings to confirm suspicions. The receptionist was confronted and later fired. In this case, the inter-office emails were widely distributed within the company and didn't contain private information protected under federal law.

Due to this incident, new security policies were implemented company-wide including new security requirements for the IT staff. To ensure IT staff complies with HIPAA and Sox, the network manager needed a way to control which IT staff could use the analyzer to capture and read sensitive information transmitted across the network. The network manager was able to solve this by creating individual user accounts in the analyzer used to capture network traffic. He could restrict user access to specific features, preventing unauthorized use of certain analyzer features for easier compliance with regulatory compliance.

Ensuring companies are HIPAA and SOX compliant is important, as there are costly penalties for organizations that fail to do so. Any loss or theft of consumer data – whether related to health, finances or other personal information – poses huge risks for companies. Such a loss of customer information typically requires that companies notify the public of the breach, creating a public relations problem that can tarnish the company's products and services, reputation and customer loyalty.

Solution: Portable, integrated analyzer

With the OptiView Series III Integrated Network Analyzer from Fluke Networks, network professionals are able to address inside security concerns that could seriously impact the business. Using this tool, network professionals can scan the network for unauthorized devices that could cause a breach in security. They're also able to focus attention on suspected trouble spots on a case-by-case basis.

The portability of this tool sets it apart from other devices. In some cases, network professionals use a laptop and run multiple applications in an attempt to diagnose problems, or they rely on hardware that can't be moved. The OptiView Analyzer allows network professionals to make "house calls," whenever and wherever problems arise. Teamed with an existing security system, the OptiView adds another layer of protection that can help root-out existing vulnerabilities.

The OptiView analyzer comes equipped with several key features that allow network professionals to address security problems from the inside:

Free String Match

The OptiView analyzer allows network engineers to use the Free String Match function to match any set of words or phrases – regardless of the position of the packet, payload or header – in real time. An engineer can detect traffic containing certain words or phrases in non-encrypted emails, web pages, file transfers or documents. This allows the engineer to identify improper use of the network as well as detect downloads of restricted documents based on content or file names. The Free String Match feature, and in-depth protocol recognition, also helps engineers identify and track applications that are not allowed on the network, such as streaming media that takes up valuable bandwidth, or P2P traffic that poses a security risk. Up to eight triggers or filters can be defined at any one time, allowing engineers to analyze captures when time allows.

Wireless rogue device identification and location

The OptiView analyzer quickly tracks down rogue and unsecured devices, including ad-hoc networks. Audio and visual indicators lead network engineers to the location of the offending device.

User account restrictions and removable hard drive

The OptiView analyzer's user accounts screen lets engineers add and modify analyzer security information for each individual user. This prevents unauthorized use of certain analyzer features for easier compliance with federal regulations, including HIPAA and SOX. Potentially disabled features include: packet capture and decode, traffic generation, remote user interface and analyzer configuration. Network information discovered by the OptiView Series III Integrated Network Analyzer can be stored on the optional removable hard drive, which ensures any sensitive data stored on a network analyzer's hard drive never leaves that environment. The analyzer can be moved from classified environments of different levels and between classified and unclassified systems or private and public networks by simply replacing the hard drive.

Summary

Inside security threats may be unintentional, but they can no longer be a backburner worry...the risks are simply too great. To address these threats network professionals would benefit from a new tool, one that helps find weak spots in the network and allows them to track down unauthorized devices and applications. The OptiView Series III Integrated Network Analyzer works with existing security programs to add another portable, layer of protection. With this additional protection, network professionals are able to find and address potential problems that could compromise the network – and the business.

The business case for a portable, integrated network analyzer

The OptiView Series III Integrated Network Analyzer helps network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. It gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network. No other portable tool offers this much vision and all-in-one capability to help you:

- Deploy new technologies and applications
- Manage and validate infrastructure changes
- Solve network and application performance issues
- Secure network from internal threats

It shows you where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of OptiView to give you vision and control of your network.

NETWORK SUPERVISION

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.

©2007 Fluke Corporation. All rights reserved.
Printed in U.S.A. 1/2007 2805658 D-ENG-N Rev A