Network Instruments

—— white paper ——

USING A NETWORK ANALYZER AS A SECURITY TOOL

Network Analyzers are designed to watch the network, identify issues and alert administrators of problem scenarios. These features make the analyzer an excellent tool to locate network security breaches, and to help identify and isolate virus-infected systems. This white paper shows how using a network analyzer can enhance network security, which analyzer features are essential for this task and how an analyzer should be a part of any IT professional's security incident response plan.

NETWORK®
INSTRUMENTS

JDSU Performance Management

SUMMARY

Because firewalls and other defensive security measures are not failsafe, you need additional tools to detect and respond to security breaches as they occur. A network analyzer can detect known (and even some unknown) virus attacks and make the cleanup process much more efficient.

BACKGROUND

A protocol analyzer shows you what is happening on your network by decoding the different protocols that devices on the network use to communicate, and presenting the results in human-readable form. Most mature analyzers also include some statistical reporting functionality. The usefulness of such a tool for day-to-day troubleshooting is obvious; less obvious (and therefore underutilized) is how essential an analyzer becomes when responding to security threats such as hacker intrusions, worms, and viruses.

The purpose of this white paper is to explain how an analyzer can augment firewalls and other perimeter defenses.

EVEN THE BEST DEFENSES FAIL

Every administrator of a corporate LAN of any size these days has already built strong defenses against hackers and virus attacks. But the viruses and hackers continue to get through. Why?

Anti-virus and IDS systems are designed to prevent the incursion of known viruses and attacks. The hackers and "script kiddies" have the same access to all the threat bulletins and Windows patches that you have, and are always looking for the new vulnerabilities. In short, your firewalls and operating systems often won't get a patch until the damage is already done. Imported disks, deliberate actions by employees, and visitors bringing infected laptops are some other weak spots in your security system that perimeter defenses alone cannot address.
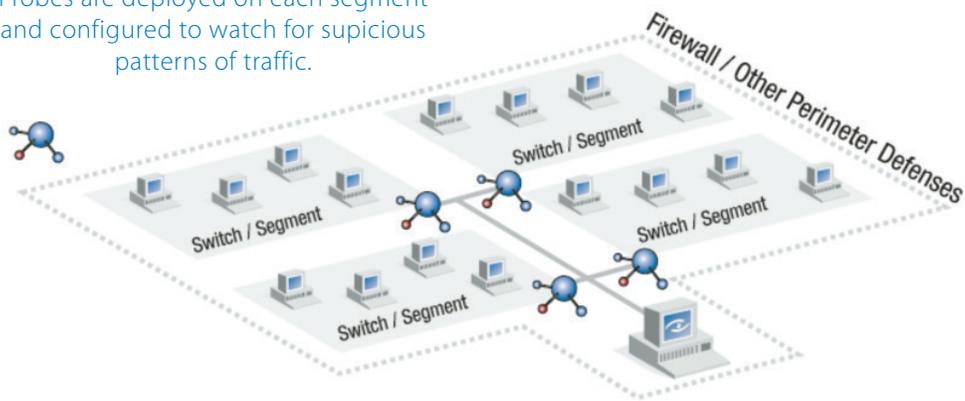
A good network analyzer can both help you detect when breaches have already occurred, and make the cleanup/recovery far less painful once a breach has been identified.

BREACH DETECTION

Viruses and hacker attacks typically generate a recognizable pattern or "signature" of packets. A network analyzer can identify these packets and alert the administrator to their presence on the network via email or page. Most analyzers let you set alarms to be triggered when a particular pattern is seen. Some analyzers can be programmed to send an email or page when these conditions are met. Of course, this assumes that the virus and its signature have been seen before and incorporated the analyzer's list of packet filters. (A filter specifies the set of criteria under which an analyzer will capture packets or trigger an alarm or some other action.)

Security breaches may or may not generate a recognizable pattern.

Firewall / Other Perimeter Defenses

Switch / Segment

Switch / Segment

Switch / Segment

Switch / Segment

The console lets an administrator capture packets and monitor statistics from any segment on the network.

Analyzers can improve the effectiveness of existing security measures by rooting out intrusions that circumvent these defenses.

New viruses and worms have different signatures depending on the vulnerabilities they are trying to exploit, but once systems have been successfully breached, there are a relatively small number of things that hackers actually want to do with your network, the top ones being:

- Use your systems in a Denial of Service (DoS) on a third party. A good network analyzer can easily identify such systems by the traffic they generate.

- Use your system as an FTP server to distribute "warez" and other illegal files. You can configure an analyzer to look for FTP traffic or traffic volume where it is unexpected.

The very nature of viruses and worms is to produce unusual levels of network traffic. High frequency of broadcast packets or specific servers generating an unusual number of packets are logged in the analyzer's record of longer term traffic, allowing the administrator to follow up on suspicious traffic patterns.

The analyzer can also help in identifying inappropriate traffic which may leave your network open to attack, or may signify potential weaknesses. This would vary with the particular network or corporate policy, but could include automatic notification of traffic such as MSN, NNTP or outbound telnet.

The Probe senses a system that is infected or under attack and immediately alerts the console.
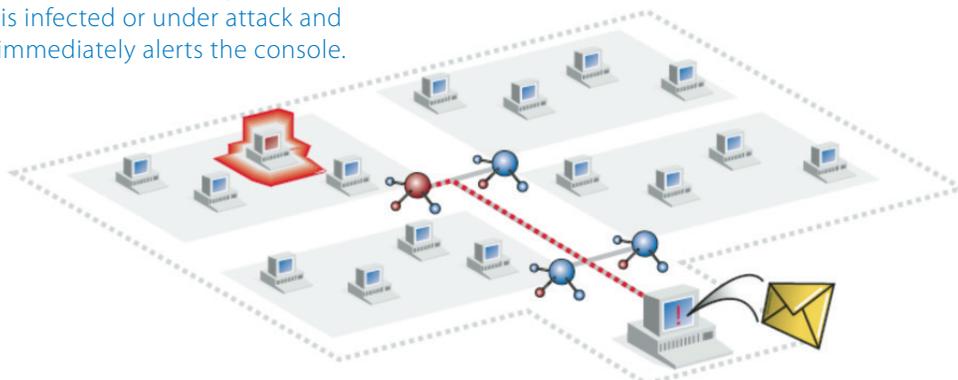
Console notifies administrator via log, email, or page.

CHOOSING AND IMPLEMENTING A NETWORK ANALYZER

To be useful as a corporate security tool, the analyzer must be "distributed" so that it covers all the areas of your network. It must also be able to capture and decode all of the protocols from all of the media (Ethernet, WAN, 802.11, etc.) on which your corporate data flows. The other crucial feature is flexible filtering that allows triggered notification.

A network analyzer can only capture and decode the information that it can "see." In a switched network environment, an analyzer is only able to see traffic local to the switch.

WHAT "DISTRIBUTED" MEANS AND WHY IT IS ESSENTIAL

To overcome this, most modern analyzers are supplied with multiple agents or probes that are installed on each switch in the LAN. An analyzer console can then query the probe for either raw packets or statistical traffic reports.

When an analyzer is used in a general troubleshooting or monitoring mode, it is nice to have as much visibility as possible. When used in a protection mode, the visibility is vital. So – the more distributed the analyzer, the better. The distribution needs to be reviewed in both qualitative as well as quantitative terms. Look for an analyzer that can install probes or agents on the topologies present within both your existing network, and any planned enhancements. Look not only for Ethernet capabilities, but WAN and wireless capabilities if these are either present or possible additions.

Probe functionality is another important factor. They should be able to perform all the functions required by the organization – the capture and decode of packets, analysis of traffic levels both in terms of stations active as well as applications being used. Application analysis is important because a rapid increase in volumes of email is one of the obvious signs of many viruses.

A final consideration would be the method of data transfer between the probe and the analyzer's console or management station. The transfer of data must be minimal (to prevent unnecessary load on the network) and as secure as possible.

Probes need to be placed where they can see the critical points of the network. These would include the network's default gateway (since all broadcast packets and all packets with unknown destination addresses will be sent here), E-Mail server(s) and any other servers deemed as critical or likely to be attacked.

In order for a probe to detect a certain device it will ideally be located on a hub onto which the device is also directly connected. If this is not possible – and the device to be protected is connected directly to a switch port, then the switch should be configured to mirror (or span) all traffic from that switch port onto a separate switch port on which the probe is located.

For continuous monitoring of viruses and attacks, probes must be implemented. More probes may need to be deployed if some are to be used for general monitoring, and some to be used for protection. Alternatively some analyzers are supplied with multi-function probes that can perform both tasks simultaneously.

If you want to analyze WAN, WLAN, or gigabit traffic, you must choose a vendor with solutions for those media as well.

FILTERING POWER AND FLEXIBILITY

Look for a solution that offers the ability to "roll your own" traffic pattern filters as well as offering packaged filters for known viruses and hacker threats. Another thing to look for is the vendor's willingness to offer timely updates as new security threats are discovered.

TRIGGERED NOTIFICATIONS

A quick response to a breach can mean the difference between an inconvenience for a few users and a disaster for your company. Look for an analyzer that can be configured to email or page you when the virus or hacker attack is sensed.

DEPTH ANALYSIS FEATURES

Most analyzers can tell you what machines are generating the most traffic, what protocols are taking up the most bandwidth, and other such useful information allowing you to detect attacks and infected systems. The most powerful analyzers have "expert" functionality available that looks at conversation threads and identifies more subtle problems (missing ACKs, high wireless reassociation counts being two examples) automatically.

CONCLUSION

Network Analyzers will never replace your firewall, anti-virus software or intrusion detection system. However, because it is not possible for these precautions to be completely effective, you cannot maintain the security of your network without a network analyzer. A good analyzer alerts you when the other defenses have failed, and takes much of the pain out of identifying, isolating, and cleaning up compromised machines. Considering the general troubleshooting and monitoring features included "for free" in such tools, the decision to purchase a comprehensive analyzer with network security features is easily justified.

North American Location

10701 Red Circle Drive · Minnetonka, MN 55343 · USA

Toll Free: (800) 526-7919 | Voice: (952) 358-3800

www.networkinstruments.com

NETWORK INSTRUMENTS®

JDSU Performance Management