

**White Paper:**

**Combining Network Intrusion Detection with  
Firewalls for Maximum Perimeter Protection**

---

April 2001

**NOKIA**  
CONNECTING PEOPLE

<b>Abstract</b>	<b>2</b>
<b>What is a network intrusion detection system?</b>	<b>2</b>
<b>Electronic security mimics physical security</b>	<b>3</b>
<b>Combining a firewall with the network intrusion detection system</b>	<b>3</b>
<b>Setting intrusion detection policies</b>	<b>4</b>
<b>Other network intrusion detection deployments</b>	<b>5</b>
<b>Summary</b>	<b>6</b>
<b>About RealSecure for Nokia</b>	<b>6</b>

## Abstract

Intrusion detection is a critical element in the overall electronic security infrastructure. When installed in conjunction with a firewall, an intrusion detection system (IDS) provides an additional layer of security that significantly decreases the risk of an attack going undetected.

Firewalls have emerged as the primary tool to prevent unauthorized intrusion into systems. Firewalls should always be viewed as the first line of defense on any system connected to the Internet. However, firewalls are limited in their ability to detect many types of unauthorized behavior. Network IDSs provide an additional layer of security that significantly strengthens an organization's perimeter defense.

Network IDSs are usually installed to identify weaknesses in a company's security policy, alerting the security administrator to enhance or revise the network's security defenses. The primary objective is to assure the firewall's policy is correctly configured, so that unauthorized or suspicious connections are identified and wherever possible prevented.

Perhaps the greatest threat is from Trojan horse programs. Remote control and distributed denial of service Trojans such as Back Orifice, SubSeven, trin00 and over 1,100 others are very dangerous to the integrity of a network. If a user has managed to allow a Trojan to infect their system—this is especially true of telecommuters on VPNs—the firewall dutifully forwards traffic on TCP ports 21, 25 and 80, forwarding Trojan activity while assuming it is servicing FTP, SMTP and HTTP connections. Only by analyzing the content of these packets can one be assured of a Trojan-free network.

## What is a network intrusion detection system?

Network intrusion detection systems stealthily listen on a network segment, evaluating every packet and connection. There are two components to a system, the network sensor and the console.

The network sensor is used to monitor the network. The sensor's network interface card is placed into promiscuous mode so that the intrusion detection software receives all packets on the segment. As an additional security measure, the monitoring interface is not assigned an IP address—it doesn't need one to listen—which prevents it from being addressed and attacked, since the users don't know it is there.

The sensor's intrusion detection software is an expert system designed to detect byte patterns that represent some form of attack or misuse. Some network IDSs merely detect signatures, while the most sophisticated systems actually build state for each connection and detect complex series of events. Since over 99 percent of all packets are normal and can be ignored, the network sensor filters through millions of packets per hour looking for attack and misuse patterns—a task that is impossible for a human to accomplish.

The network intrusion detection console serves two functions. It is usually placed on a side-band channel that has a different data path than the segment(s) being monitored. The console provides a configuration interface to enable remote management and configuration of the network sensors. The best systems have implemented a high quality user interface that allows a relative novice to configure the security policy and responses without extensive training on "C-like languages" or other specialized programming languages. The ability to include custom signatures is critical as well, since a network IDS can be used to detect leaks of confidential information such as business secrets. Once the security policy has been developed, it is "pushed" to each of the sensors.

The console is also used to display, analyze and report on the data collected by the network sensor. The level of analysis is the critical element. If the network sensor detects something, a detailed analysis of the event is sometimes required. Analytical tools such as session replay, detailed event analysis and statistical tools separate the best systems from the weaker offerings. Reporting is another feature often overlooked. Quality management reports that can be understood and evaluated by non-technical business managers often separate the weaker offerings from the leaders.

## **Electronic security mimics physical security**

Interestingly, electronic security mimics time-proven physical security practices. Physical security assigns varying access rights to employees, contractors, partners and the general public. The physical security policy drives the level of access to each of these categories of individuals.

The firewall is similar to a door, and like most doors has a lock on it. Only those with the proper credentials or profiles are allowed to enter. For example, you may be able to enter a bank lobby, but it's unlikely that you will be given access to the vault. Likewise, a firewall will let outsiders into specific system areas, but not to the internal network.

IDSs mimic another physical security practice. A casual glance around most buildings will reveal closed circuit television cameras (CCTVs). The cameras are used to detect an intruder attempting to pick a lock or rob a bank. If a video recorder is connected to the camera it is possible to replay the events and potentially identify the suspects. IDSs are like the CCTV cameras; they detect unusual and unwanted activity at the perimeter and "public" areas of systems and through logs and event trails can identify or help trace an intruder. In the bank example, attempted unauthorized entry or unusual behavior in the lobby will likely tip off a security guard that a problem exists.

IDSs also have the ability to alarm and apply countermeasures if they detect unusual activity. As with physical security, alarm systems significantly enhance the perimeter security of a building. As with alarm systems, IDSs can act as a deterrent by providing countermeasures such as session kill, automated firewall reconfiguration and real-time warnings.

The security administrator uses firewalls and IDSs in much the same way that a security guard uses locked doors and CCTV cameras. As with physical security, the level of electronic security is layered. Each layer provides an enhancement to the overall security level. A locked door is one level, but the addition of cameras and alarm systems greatly enhances the security of a building.

Insurance companies routinely require the installation of alarm systems in buildings to reduce the risk of break-ins. In the same way, electronic insurance programs such as ICISA's® TruSecure™ require IDSs on insured websites and Internet connections.

## **Combining a firewall with the network intrusion detection system**

Effective use of a network IDS requires two things. Proper placement of the IDS and the policy associated with the type of traffic on the Internet connection.

Placement of the network IDS to support a firewall is dependant on the intended objectives for intrusion detection. Ideally, two sensors should be used and placed on both the outside and inside of the firewall (see figure 1).

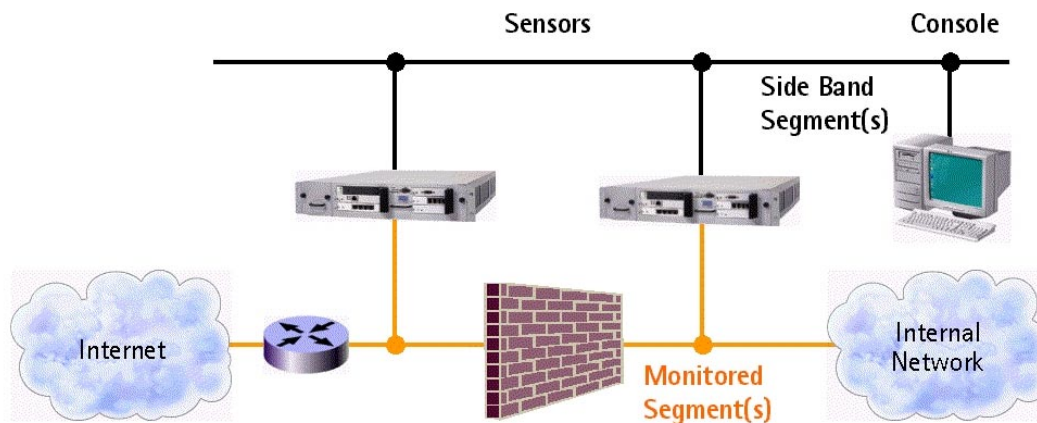


Figure 1. Placement of the network IDS to support a firewall.

One sensor monitors the segment between the router and firewall. The second sensor monitors the segment between the firewall and internal network. Deployed in this configuration, the two sensors perform complimentary functions acting as a "firewall leak detector."

The policy configuration of each sensor is a bit different. The outside sensor is used to monitor for attack attempts and network probes of an organization's Internet connection, while the inside sensor is used to detect certain types of events that have made it through the firewall or are coming from the internal network. The security administrator should make sure the implementation doesn't just focus on external activity. Insiders can have distributed denial of service, Trojan horse programs, worms and attack programs installed on internal computers. There is potential for litigation if an organization is the source of the attack. If the budget is limited, the inside sensor should be deployed in a single sensor implementation.

## Setting intrusion detection policies

Optimally, network IDS policies should be tuned to the environment. Setting policy is not as complicated as it has been portrayed, but efficient policy selection does require knowledge of internal network and systems. There are specific goals and objectives for each sensor. This is where a console's configuration user interface can be a help or hindrance.

It is important to tune the sensor's policies for the type of systems inside the firewall. For example, if the devices such as user workstations and servers are based on Microsoft Windows, there is little need to test for Unix exploits. In addition, if there are no externally available web or FTP servers on the inside of the firewall, there is no requirement to check for those categories of exploits.

The outside network sensor should be configured to detect a variety of probing activities, firewall exploits, suspicious activity and protection of external or DMZ devices at the Internet connection. Since there are large amounts of exploit activity on the Internet, care must be taken in tuning this network sensor to protecting the specific environment. Implementing all of a vendor's signatures can cause all IDSs to get bogged down detecting signatures that have no impact on internal systems.

- Activate detection of port probes such as NMAP and others. The objective is to understand when probing activity increases significantly, maybe a precursor to an attack. Activating probe-oriented

signatures can generate heavy event traffic. Advanced network IDSs offer threshold settings that will reduce the level of "nuisance" alerts and false positives while alerting the security administrator of significant events.

- Implement custom signatures to monitor external connection rules. Nearly all firewalls have some rules that allow for external access to services on the internal network. Normally, these are narrowly defined to include specific addresses and ports. Custom-developed IDS policies should be developed to monitor and log all activity on those external access rules.
- Activation of "suspicious behavior" signatures. These should be tuned to protect the firewall, routers and externally connected devices such as web, mail, DNS and FTP servers that are often attached to specialized or "DMZ" segments.
- Distributed denial of service activity. Ingress and egress DDoS zombie detection is a key element here. Detection of an in-bound DDoS attack gains precious seconds in mitigating the effects of the denial of service attack. It is also important to detect out-bound DDoS activity, unless IP spoof limiting egress filters have been implemented at the external router.

Inside the firewall, the objective is to detect suspicious activity. Detection of Trojans, backdoors, unauthorized access exploits and externally bound attacks signatures are important. Properly configured firewalls will filter many exploits, but are typically weak against Trojan and backdoor activity.

- Activate Trojan and backdoor detection signatures. A good network IDS will be able to detect hundreds of Trojans and their variants by analyzing packet contents and not just their default TCP ports. Note also, many infected computers belong to users attached to DSL and cable modems. A VPN connection does not protect against a Trojaned system outside the perimeter.
- Unauthorized access attempts—mainly buffer overflows—exploit bugs in operating systems and applications. While usually filtered out at the firewall, there are session hijacking techniques that can fool a firewall into allowing traffic to pass.
- Detection of outbound attacks is a very important aspect as well. While not common, insiders attacking external systems from the internal network exposes and organization to potential litigation for being the source of an attack.

## Other network intrusion detection deployments

Currently, the primary use of a network IDS is for perimeter monitoring and protection. There are a number of other uses for the technology. The objective varies in terms of systems being monitored and exploits, but the technology can significantly enhance enterprise security. Below are some examples to consider:

- WAN and Frame Relay connections. Ordinarily, these are considered "private" connections, but they often connect to smaller branch offices that are sometimes lax in physical security and adherence to policy. A malicious hacker may exploit these aspects of branch offices to gain access to the organization's systems and data stores. Configure the sensor for Trojans and unauthorized access attempts.
- VPN and extranet connections. These connections are often on a different Internet connection than the firewall and allow insiders and trusted (or partially trusted) organizations such as partners and

suppliers access to internal systems. Configure policy in the same way as WAN or Frame Relay connections.

- Critical servers and data stores that could be the target of criminal activity. Financial, manufacturing and development servers are an ideal application of intrusion detection technology. Network sensors should be tuned to the specific environment they are protecting to achieve maximum throughput. For example, if there are only Solaris devices running Oracle, only define those signatures specific to that environment.

## Summary

Organizations should view their electronic security in a similar way as their physical security. Network intrusion detection is an excellent technology to augment an organization's security strategy. Like any technology, implementing intrusion detection requires a bit of homework and a careful deployment, but is not a particularly difficult or complex solution. The overall benefit to the enterprise can be significant in terms of risk avoidance and peace of mind.

## About RealSecure for Nokia

RealSecure™ for Nokia combines the award-winning IDS with the market leading security appliance. RealSecure for Nokia sensors detect over 450 specific exploits and hundreds of variants, with alarms and countermeasures. Deploying Nokia-based network sensors requires only a few minutes of installation and configuration versus hours on other platforms.

The RealSecure for Nokia Workgroup Manager console combines a powerful and easy to use policy definition GUI with advanced display and event analysis tools.

## **About Nokia**

Nokia is the world leader in mobile communications. Backed by its experience, innovation, user-friendliness and secure solutions, the company has become the leading supplier of mobile phones and a leading supplier of mobile, fixed and IP networks. By adding mobility to the Internet Nokia creates new opportunities for companies and further enriches the daily lives of people. Nokia is one of the most broadly held companies in the world with listings on six major exchanges.

## **About Nokia Internet Communications**

Nokia Internet Communications, headquartered in Mountain View, California, provides world-class Network Security, Virtual Private Network, SSL Acceleration and Wireless Software solutions that ensure the security and reliability of corporate enterprise and managed service provider networks. Nokia is committed to enhancing the end user experience by bringing a new level of security and reliability to the network, enabling an Internet transaction that is personal and trusted—each and every time.

### **Nokia Internet Communications**

#### **Americas**

313 Fairchild Drive  
Mountain View, CA 94043  
Tel: 1 877 997-9199  
E-mail: [internet.na@nokia.com](mailto:internet.na@nokia.com)

#### **Europe, Middle East and Africa**

1st Floor, Building 3, Southwood  
Farnborough, Hampshire, GU14 0NZ UK  
Tel: +44 (0) 8700 555 777  
European Customer Inquiry Number (toll-free): 00800 5543 1816  
Outside toll-free area: +49 231 754 6011  
E-mail: [internet.emea@nokia.com](mailto:internet.emea@nokia.com)

#### **Asia Pacific**

438B Alexandra Road  
#07-00 Alexandra Technopark, Singapore 119968  
Tel: +65 588 3364  
E-mail: [internet.apac@nokia.com](mailto:internet.apac@nokia.com)

[www.nokia.com](http://www.nokia.com)

