Net Integration Technologies, Inc.

http://www.net−itech.com

Net Integrator Firewall

Technical Overview

Version 1.00

TABLE OF CONTENTS

1 INTRODUCTION

At Net Integration Technologies, we take network security very seriously.

A new server joining the Internet today will usually be probed quietly by a potential attacker's scripts within about 24 hours. If the server shows any weaknesses, the attacker will likely be back shortly afterwards to investigate.

When conditions are this harsh, it's simply not reasonable to operate a server or connect an office to the Internet without some kind of firewall protection − that's clear. However, a subtle balance is necessary between security and functionality, and each organization has different security needs. Blocking incoming web requests from visitors will certainly increase security, but if you run an e−commerce web site, that won't be acceptable. Like unlocking the front door to a bank, sometimes security needs to be slightly reduced in order to provide a service. Our customers need a serious firewall that can do what they need it to do and change when their needs change.

Because we take security so seriously, many users of our Net Integrator appliance products are surprised to find that there is no firewall configuration screen: nowhere to add rules and create rulesets, nowhere to make decisions about arcane TCP/IP data structures, and nowhere to select which incoming and outgoing port numbers need to be opened. If security is so serious, then how can we take a firewall seriously when it doesn't have these options?

In fact, we take security *so* seriously that we carefully and deliberately removed each one of these configuration options from the Net Integrator. The rest of this document will explain how and why and describe some of the firewall's more advanced features along the way.

2 FIREWALL ARCHITECTURE

In their most basic form, all routers and firewalls are the same. They always have more than one interface (ethernet, DSL, cable, modem, and so on). They accept an IP (Internet Protocol) packet on one interface, decode it, re−encode it, and forward it along to one of the other interfaces.

Basic firewalls differ from routers mainly because they check each packet's contents and addressing before forwarding it and sometimes drop packets if they aren't following the rules. Modern, advanced firewalls also do other interesting things with the packets, such as encryption, address relabelling, address−to−username correlation, statistical analysis, or caching. In the end, all these operations are expressed as a set of *firewall rules* that define the *security policy*.

Net Integrator's firewall happens to be particularly flexible, but it generally works like all the other ones.

2.1 The Life of a Packet

Net Integrator uses a ruggedized, stripped−down version of the Linux operating system, so it inherits Linux's basic firewall tools. We also added many more advanced features, such as NetGuide, Tunnel Vision VPN (Virtual Private Network), and Internet Failover, which are described later. And of course, Net Integrator configures the Linux firewall tools automatically, creating more than 130 firewall rules to match the current system configuration.

2.2 Stateful Inspection

Net Integrator's firewall uses an advanced technique called *stateful inspection*, which allows it to create temporary firewall rules for new packets depending on past activity. For example, Net Integrator blocks all outside web server responses (called ACK packets) from passing through the firewall unless it has seen a recent request (called a SYN packet) to the same web server from a workstation inside. This sounds like it should be obvious, but it's very difficult to write traditional firewall rules to do this. In many firewall systems, ACK packets are simply passed through the firewall in the hopes that they will be discarded at the destination.

2.3 Permanent NAT

Net Integrator uses a technique called NAT (Network Address Translation) to make it appear as though all outgoing traffic is coming from the Net Integrator. IP addresses used on the protected inside network are never allowed to pass outside the firewall where they could be seen and possibly used in an attack.

Instead, outgoing packets are relabelled with the source address of the Net Integrator. When a response comes back, the destination address of the response is changed back, so neither the originating workstation nor the Internet server can see any difference.

NAT was originally designed to deal with inexpensive Internet accounts that only have one public IP address, so more than one computer could share the same Internet connection. However, Net Integrator makes a few adjustments in order to give another major benefit: since the firewall relabels *all* outgoing traffic, it only needs to accept Internet packets destined for the Net Integrator itself, not for any IP addresses on the inside network. This makes it impossible for an attacker to target any workstation or server inside the firewall directly. Instead, he has to find a security problem with the firewall itself, which is much more difficult.

2.4 Secure By Default

From the first moment it is powered on, the Net Integrator configures itself with an initial set of more than 130 firewall rules to block all incoming connections from the Internet on any port. As time goes on and it analyzes network traffic, Net Integrator adds and removes rules automatically to improve security as part of its Net Intelligence and stateful inspection routines. To allow incoming connections, the user needs to explicitly request that connections to that service be allowed, and it will automatically add firewall rules to match the request.

In contrast, most commercial firewall products and operating systems are *insecure* by default; they require the administrator to block each unwanted service individually, making it very easy to miss one or to make a mistake.

One of the top ten most serious security mistakes listed by SANS (The System Administration, Networking, and Security trade organization) is not *failing to install a firewall* − it's *implementing firewalls with rules that don't stop malicious or dangerous traffic.* In other words, everyone makes mistakes, and making a mistake in firewall

configuration is both common and serious. When it takes several days and more than a hundred cryptic rules just to build an initial security policy, it's easy to see how errors can happen. But every user of Net Integrator automatically gains the benefit of our skilled security analysts, third party review, and years of experience. Net Integrator's firewall is more secure precisely *because* it requires less input from the administrator.

2.5 Multi−tiered Security

To penetrate a Net Integrator firewall and attack a workstation or server on the other side, an attacker would have to defeat several levels of security:

- The firewall rules themselves, including NAT.
- At least one running server process (such as the file server or web server).
- A security gateway process, in order to obtain administrator privileges.

The entire Net Integrator operating system, including the firewall, configuration utilities, and all the server software, fits in less than 10 megabytes on a tiny solid−state memory card. Even if an attacker were to somehow find a leak in the firewall, the software environment is so restrictive that it would be nearly impossible to use this security hole to penetrate further.

By contrast, many commercial firewall products are based on full−sized server operating systems like Windows or Solaris, which are between 100 and 200 times larger than Net Integrator's software. Among the vast amount of code and data in these operating systems are several insecure tools which can help complete an attack once it bypasses the firewall.

3 INTELLIGENT SERVER INTEGRATION

The previous section described the advanced features of Net Integrator's firewall. In this section, we will describe several features that allow a system administrator to use all these features without having to understand them completely.

3.1 Central Configuration Management

The configuration, firewall, and server processes are all tied together very tightly in Net Integrator. Because of this, many internal changes can occur when the administrator changes a single configuration option. For example, creating a new user account automatically creates an e−mail account, a web page, Windows and Macintosh file shares, an addressbook entry, and a VPN account for that user.

In a similar way, changing a single option like "enable web server" or "enable FTP server" not only reconfigures the server in question but also informs the firewall module about exactly what the administrator is trying to accomplish. The firewall module then proceeds to generate a new set of rules automatically to comply with the new security policy.

On systems with a separate firewall configuration screen or on networks where the firewall is a completely separate unit, this process is divided into several steps, increasing the probability of a mistake.

3.2 Trusted and Untrusted Networks

The Net Integrator firewall is always enabled, so there is no "enable/disable firewall" option. Instead, for each network interface there is a "Trusted" setting, and for each service type there are "Enable for trusted hosts only" or "Enable for everyone" settings. Net Integrator automatically configures its firewall based on these settings.

Usually, requests from workstations on trusted networks can pass transparently through the firewall to other trusted or untrusted networks. Most requests from untrusted networks are blocked by default, unless they are explicitly allowed for that type of service.

3.3 Intelligent Rule Generator

The Intelligent Rule Generator module is responsible for converting high−level security policy into a set of specific firewall rules. The generated rules are actually very complicated since they need to consider the interaction between different subsystems (such as the VPN and Internet Failover). However, as a simplified example, it might convert the policy "Enable WWW server: Yes" into a series of rules similar to the ones in Figure 1.

Default behaviour:

- Accept all request (SYN) packets to local port 80 and add them to the Stateful Inspection table.
- Deny all request (SYN) packets from local port 80.
- Deny all response (ACK) packets to local port 80.
- Deny all response (ACK) packets from local port 80.

Stateful Inspection rules:

- Only for connections known to Stateful Inspection, accept ACK packets to and from local port 80.
- Remove connections from the Stateful Inspection table if an error (RST) or transaction complete (FIN) message is received.

Figure 1. *Auto−generated firewall rules for enabling a web server.*

In the example, all six of these rules are created as a result of simply enabling the web server. In reality, the rules are even more complicated since they need to consider whether messages are arriving from a trusted network, whether the response packets should be relabelled using NAT, and so on.

It’s easy to see how a human administrator could forget to add one or more of the above rules after changing a web server setting, thereby introducing security flaws. The Intelligent Rule Generator not only makes the whole firewall system easier to use, it also improves security.

4 Dynamic Address Management

Because Net Integrator's firewall rules are generated automatically from knowledge of the entire system configuration, it can work equally well with dynamic IP addresses and static IP addresses. This also allows the firewall to support more advanced features, like Transparent Multihoming (running more than one firewall−protected web server), Double Vision (multiple dynamic Internet connections) and Internet Failover (automatically switching to a second Internet connection if the first one fails).

4.1 Static versus Dynamic

In a static IP address system, the Internet Service Provider (ISP) provides one or more valid Internet IP addresses to use when making requests. These addresses never change, which means it isn't usually necessary for an administrator to change the firewall rules unless the security policy changes.

On the other hand, dynamic IP addresses change often. Depending on the particular ISP, this can be once per day, whenever the router reboots, or whenever the connection is lost and subsequently restored.

To properly configure a secure firewall, it's necessary to change some of the firewall rules depending on the currently assigned IP addresses, so many firewalls don't work optimally in situations where only dynamic IP addresses are available. However, since Net Integrator rewrites its firewall rules automatically whenever the network configuration changes, it works perfectly with dynamic IP addresses without extra user interaction.

4.2 Transparent Multihoming

Sometimes a single physical server may want to host more than one web site. One way to do this is to request more than one static IP address from the ISP, and then assign all of these addresses to the Net Integrator and configure a different web server on each address.

In this case, the firewall rules will automatically be updated to include each of the assigned static IP addresses, rather than just the primary one.

4.3 Double Vision

Net Integrator uses some advanced features of its firewall system to support load balancing between multiple simultaneous Internet connections. This feature is called "Double Vision."

Usually, this feature is used to improve Internet speed and reliability. When an outgoing connection is created (for example, by a web browser on the local network) Double Vision randomly chooses one of the functioning Internet links and configures its Stateful Inspection rules to relabel addresses for that connection. That way, each connection always uses one particular Internet link, which prevents other firewalls from getting confused and blocking the connection.

4.4 Internet Failover

When using Double Vision to increase reliability, it's important not to use Internet links that are unstable, unreliable, or non−functioning. When the Net Intelligence portion of Net Integrator determines that a link is down, it requests that the firewall block all incoming and outgoing connections on that link. That way, Double Vision will never bind an outgoing connection to that link, and incoming requests will be sent to the functioning link instead.

In a system where firewall rules were written manually by the administrator, a feature such as Internet Failover would normally require either manual intervention or reduced firewall protection.

5 THE VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network creates a secure, trusted, encrypted link between two networks across the Internet. Once the VPN is established, computers on both networks can transparently use any services on either network as if they were directly connected.

In terms of security, VPN allows specific users or computers elsewhere on the Internet to bypass Net Integrator's firewall.

Net Integrator supports two kinds of VPN connection:

- PPTP, Microsoft's Point−to−Point Tunneling Protocol, allows individual Windows workstations (such as laptops or home computers) to connect into the central network. Each user account on the Net Integrator can have PPTP access enabled or disabled.
- Tunnel Vision, a proprietary VPN created by Net Integration Technologies, allows Net Integrators to connect entire networks to each other. This is useful for connecting several branch offices to a central office, for example.

Both PPTP and Tunnel Vision use high−grade 128−bit symmetric encryption to protect data while it traverses the Internet. Tunnel Vision also uses 1024−bit RSA keys to authorize new connections.

6 About Net Integration Technologies

Net Integration Technologies Inc. develops and manufactures affordable, high−performance all−in−one network server appliances designed to fulfill the IT needs of small to medium−sized organizations. The Net Integrator family of products leverages Net Integration's unique technologies to deliver an easy−to−use, reliable, powerful and cost−effective IT solution.

The Net Integration product family includes Net Integrator Lite, Net Integrator Mark I, Net Integrator Mark II, Net Integrator Mark I−idb and Net Integrator Mark II−idb. This family of products is flexible, scalable and does not require specialized IT skills to set up, maintain or manage. By eliminating the need for expensive hardware, software and highly skilled IT professionals, Net Integrator gives small to medium−sized businesses access to the IT services needed to succeed in today's business environment.

Net Integrator products are delivered through a global network of value−added resellers (VARs) and directly from Net Integration Technologies, Inc. Net Integration Technologies is a privately owned, venture−backed company headquartered in Toronto, Canada.

For more information, please visit the Net Integration web site at **www.net−itech.com**