



---

Two Lincoln Centre  
5420 LBJ Frwy, Suite 280  
Dallas, TX 75240

1.888.ECONET2  
972.991.5005  
FAX 972.991.4242

[www.econet.com](http://www.econet.com)  
[info@econet.com](mailto:info@econet.com)

A discussion on securing open ports on firewalls.

By

David A. Lissberger

EcoNet.com, Inc.

Dallas, TX

This paper is for the purpose of discussing how EcoNet.com Sentinel Service addresses security risks for corporate networks that have been connected to the public internet. Such internet gateways have grown in numbers and bandwidth each year and this represents a trend that is expected to continue. While a corporate network may be subject to a great variety of security risks, it is only those threats that are conducted through the internet gateway that are the subject of this discussion. In addition we will not focus on virus remediation, as there has already been a great amount of information and commercialized software developed in response to that type of threat. The threat we are concerned with is one that the security community has been relatively quiet. That is the vulnerability of an open port.

Total safety is available.

A network administrator can easily “lockdown” a company network by closing all ports on the internet firewall. State-full packet inspection firewalls are well established as providing adequate protection for corporate networks. With such a firewall in place, dropped packets from the device gives the appearance of a dead IP address to a potential offender.

Why this isn't an option.

Significant business leverage is available to corporations that leverage internet technologies. Such web efforts generally take the form as some type of web service, running on machines that are connected to the corporate network. In order for the services to run, portions of the firewall must be disabled. So a port is opened. By definition, an open port on a firewall means there is NO firewall on that port. The architecture of the web requires that ports be open in order to allow data to flow through the firewall.

The current situation.

The following is a hypothetical dialogue that conveys one view of the current state of corporate internet gateway security.

The CEO, "Do we have a firewall?"

IT Director, "Yes boss, we bought a \$10,000 Positively Intrusion-proof X-tragood model.

The CEO, "Are we safe?"

IT Director, "Well it's considered the best. . . . unless we are ready to spend a couple hundred thousand on an IDS and hire two more people."

The CEO, "What are the chances of a problem?"

IT Director, "I keep everything backed up!"

The CEO, "OK, when will Outlook web access be back up?"

IT Director, "End of the day boss."

What does it mean to a company.

Those of us in the business snicker at this hypothetical exchange and admittedly derive some form of prideful pleasure in understanding what the CEO doesn't and what the IT Director won't say. That is, "in most all situations of this type, the organization is quite vulnerable". The shareholders prosecution team will explain it to the CEO's D&O insurance firm in court.

Why are they so vulnerable?

Because they have several open ports on the firewall. It is likely

Port 80        open    (for OWA)

Port 25        open    (for email)

Port 21        open    (for FTP services)

Port 1494     open    (citrix client)

Port 420,421 open    (remote admin by a service company)

Port 500        open    (UDP VPN traffic)

When you take a second look it could be argued that this company has no firewall. A simple port scan would reveal the open ports and finger printing, a common hacker technique, would reveal the hardware and software versions running behind the firewall. Hope all the patches are current or else? It is also likely the firm cannot accurately identify their own network perimeter. The VPN port means there are other remote nodes on the corporate network. When the VPN tunnel stays "nailed up", a new network

perimeter exists at the other end of the secure tunnel and that network perimeter may be unprotected.

Port 25 is one of the most commonly exploited ports because it is normally open. If your company has an email server, this will likely be the case for you. Borderware recently published a list of Port 25 exploits, here are a few;

#	Description	Impact
1	The mail server's underlying operating system is vulnerable to "buffer overflows" and similar types of attacks.	Specially crafted emails exploit this weakness, allowing a hacker to take over the server. (Example: Code Red worm)
2	Incoming mail traffic is passed directly to your internal email servers, providing opportunities to hackers. Firewalls provide only partial protection.	Many SMTP servers have vulnerabilities that can be exploited to take control of the complete system.
3	OWA(Outlook Web Access) requires three components - Windows, IIS and Exchange. Each must be separately installed and secured. Traffic must also be passed through the firewall.	Complex installations present opportunities for error that may be readily exploited. In addition, each component has many vulnerabilities
4	Email clients such as Outlook helpfully "correct" invalidly formatted email messages. Some AV platforms also accept malformed messages.	Hackers construct invalid messages that bypass standard AV scanners and are then accepted, corrected and executed.
5	For convenience, roaming users forward confidential business email to public mail servers like Hotmail or Yahoo.	Unauthorized parties can read the email. Numerous password exploits have been published for Hotmail and other web mail sites.
6	Employees are not restricted in which types of files can be emailed.	Confidential and valuable documents can be revealed, accidentally or deliberately
7	Employees may use an email system to exchange personal files, including jokes, images etc.	Such materials may cause significant offense to other employees, leading to legal liability.
8	Common viruses are propagated as email attachments.	User opens attachment and activates virus. Widespread damage results.
9	Roaming users access email via OWA to internal Exchange server. OWA passwords are passed in the clear on internal networks. OWA sessions are not cleared from public terminals.	Weak passwords can be cracked by "brute force" password cracking programs. Third parties can read confidential mail.
10	Roaming users access email using IPSEC VPN client on laptop.	Seemingly secure, but difficult to use for average employee. Trojans on laptop can penetrate corporate network through VPN. Requires IPSEC deployment and personal firewall on all laptops. Expensive to install and manage.
11	Desktop AV packages out of date or inoperable due to expired subscriptions, technical glitches, disabled by user, etc.	User is wide open to new or existing virus attacks.
12	Newly introduced viruses propagate before pattern files are updated by AV vendors.	Users assume they are secure so open attachments. Widespread damage results.
13	Hackers can send executable Trojans disguised as legitimate email attachments. E.g. "Nimda"	Attachment bypasses AV scanners until signature file is updated. Users open file and massive damages occur.
14	Employees can send unauthorized email to third parties.	Confidential information available to third parties.
15	Harassing email sent to your employees by third parties.	Employees sue company.
16	> Mail server default configuration allows relaying of third party email. Spammers abuse server.	Your server gets placed on "black-hole" list, and you can't send mail to many destinations.
17	Internal email addresses "leak" onto Internet. e.g. fred.smith@secretproject.abc.com.	Competitors or hackers find out about your internal organizational structure.
18	Email traffic between company branches or with business partners travels in the clear.	Email can be "sniffed" in transit and confidential information exposed.
19	Internal email travels in the clear.	Executives email is "sniffed" by any employee using freely available download utilities.
20	Userids and passwords used for POP mail access are not encrypted on internal network.	Can be sniffed by anyone and used to gain access into other servers.
21	Hackers run scanners against mail server to detect operating system and mail server type.	If NT/Exchange detected, a host of attacks are launched automatically.
22	Organization has many mail servers accepting connections from external sources. Security measures are inconsistent, and security responsibility is spread out or unclear.	Hackers or viruses can penetrate at "weakest link" in chain, then disrupt internal network.
23	Mail server not kept up to date with security or other patches. Server becomes vulnerable to new exploits.	Server is compromised and used as launch point into internal network.
24	Network administrator fails to install important NT security patch. This can easily happen due to the large number of patches, and difficulty of installation, especially if multiple servers are involved.	Server is wide open to attacks.
25	NT server running Exchange cannot be updated with new patches because of incompatibilities with other applications running on same system.	Server is wide open to new exploits.
26	Hackers can target your server with SYN floods or other network level attacks.	Denial of service condition. Internal email service stops as well as external email connectivity.
27	Hackers can flood your mail server with huge messages to exhaust resources.	Denial of service condition. Internal email service stops as well as external email connectivity.
28	Overloaded network administrators look after security on a "best efforts" basis.	Hackers take advantage of delays in implementing security fixes to penetrate network.
29	Network administrators are not security experts, and miss the significance of important announcements or developments.	Hackers take advantage of lack of expertise and penetrate your network.
30	Network admin has designed a "home grown" email security system. Admin quits and no-one knows quite how the system works.	System is not maintained and becomes "fragile" and open to compromise.
31	Network admin not able to configure system remotely to deal with new threat. Configuration update has to wait until next day.	Hackers or viruses take advantage of "window of opportunity" to penetrate network.
32	Default installation of Exchange results in an insecure installation	Services - e.g. FTP - are enabled and may be exploited

Who is responsible?

Court cases have held that the officers and directors of a company are responsible for the “safeguarding” of the firm’s assets. This would include digital and information assets just like physical assets. A CEO wouldn’t let a stranger walk into the office and make copies of customer records, so they better not let a stranger into the accounting server and download them. The legal standard to which an officer will likely be held is called, “the prudent man rule”. Interesting that delegation of security decisions does not meet the standard. Directors and officers need to dig a little and make sure they are safe.

What protection is available?

Internet access for employees is a business requirement and ports must be open to run the company efficiently, so what can be done to tighten up security. This area of internet security is one of the last areas to receive attention. One reason is expense. Actively managed firewalls, Intrusion detection, and engineering staff are expensive and may not provide an effective solution. Also companies and their employees are not encouraged to talk about being hacked. Some firms have had to close their doors or suffered financial downturns upon public disclosure of a network security breach. At the end of the day, the answer is quite simple to illuminate, though difficult to accomplish.

“Every packet of data entering a private network from the public internet must be inspected, a determination of safety assessed, and the packet is either dropped or passed.”

Why IDS doesn’t work

Most firms do not use rigorous security procedures around the open ports in their firewalls. For those that do, they have found it difficult, time consuming, and expensive to maintain. The most common open port defense has been to use an IDS to identify potentially threatening IP addresses, then have the engineer write a new rule to the firewall to prevent communication between the offender and their network. The IDS alerts the network administrator but only after the malicious activity has occurred. Proper protection would require extremely rapid response to intrusion alerts and 24x7 engineering support for the firewall. Many IDS systems will provide a high volume of alerts that are false positives, which require a high degree of expertise to identify and diagnose. It is common for an admin to spend many hours reviewing IDS logs on a Monday morning to learn what happened to the network over the weekend. In addition IDS is helpful only to the extent that an attack matched a signature profile in the IDS database. Most of these systems lack the intelligence to use heuristics, anomalous packet identification, or behavior to identify threats, although there are a few exceptions.

The case for immediate remediation.

IDS based systems even if adroitly managed, still have another fatal flaw. They only alert the admin, and then generally, can do little about it. Realize many attacks are propagated in the initial request packet(s). This means that in order to provide real protection the initial request packet from a malicious IP address would need to be dropped prior to entering the network. Waiting for rules to be added to a firewall just won't provide the level of protection that private networks require.

#### EcoNet.com's AP-Core Technology™

AP-Core Technology™ or Active Packet Correlation is a proprietary technology that is both hardware and software based. It allows for simultaneous inspection, correlation, and packet dropping at the internet gateway to a private network. The decision as to whether a packet is to be dropped is based on many factors including construction, behavior, and known threats. AP-Core Technology™ is nearly instantaneous and is compatible with all known firewalls and IDS systems. AP-Core Technology™ is also capable of stopping a DDOS attack if the attack contains malicious code.

#### EcoNet.com's Sentinel Security Product™

EcoNet Sentinel is the first commercially available system to use AP-Core Technology™ and the first system that will protect open ports in a firewall, by dynamically dropping packets from only the malicious IP address. The system operates as an appliance in the bridge mode between the internet router and the existing firewall. The EcoNet Sentinel is both an appliance and a security management service. Standard features include 24/7 monitoring of the device, remote management services, update services, upgrades and enhancements. The EcoNet Sentinel has an easy to use administration tool that is accessible from any web browser. The network Admin can unlock IP addresses, create white lists, set up priority alerts, and review standardized management, log, and alerts reporting.

The next step.

Contact EcoNet.com today for more information on how Sentinel can provide improved security for your network. More information can also be obtained at <http://sentinel.econet.com>