CYBERGUARD Corporation

WHITE PAPER

Defense in Depth:

Applying a Fortified Strategy

A CyberGuard Corporation
Case Study
January 2004

What Is Defense in Depth?

Despite the continuous improvement in network security technologies, the bad guys – and the bad code – just keep on coming. It's no longer enough to have a single line of defense, whether that line is virus detection software, a packet filtering firewall, or just an intrusion detection system. Today, you need all three – and more – to keep malicious code and users out.

Defense in depth is the practice of layering defenses to increase data protection. By placing multiple barriers between an attacker and your business-critical information, you simultaneously raise the cost of an attack and give yourself more time to respond when a breach is detected. Defense in depth is augmenting the lock on your front door with a dead bolt, a security system, and a Doberman in the kitchen.

Distributed Firewall Architecture

Most companies of any size today have already installed a firewall to protect their network. However, layering firewalls can provide two to three times the protection *if* the firewalls are implemented in a distributed architecture. This means that the two (or more) firewalls must be physically and logically separate and must have different architectural designs, source code, development environments, and operational procedures. If you now have a packet filtering firewall, you should augment it with another kind of firewall – application-level gateway, stateful inspection, circuit-level gateway, etc. – from a different vendor.

Again, the reasoning is that if a hacker has compromised one firewall, it will take him a lot longer to compromise the other(s). Installing two identical firewalls – two packet filters, for example – is no good. The malicious code that tunnels through one will make quick work of the other. Consider a popular means of inflicting distributed denial of service (DDOS) attacks, through *covert channels*. A covert channels attack maliciously appropriates innocent clients or servers, ordering them to violate the system's security policy. Covert channels easily tunnel through single firewalls but are much more difficult to establish inside distributed firewall architectures.

Requirements for Checking Independence

The Communications-Electronics Security Group (www.cesg.gov.uk) in the United Kingdom and the National Institute of Standards and Technology (www.nist.gov) in the United States have published guidelines for ensuring the independence of firewalls used in a distributed architecture. The guidelines specify that the firewalls used to implement defense in depth must be "independent and distinct" in the following areas:

- Architectural design
- Detailed design
- Source code
- Development environment
- Operational procedures

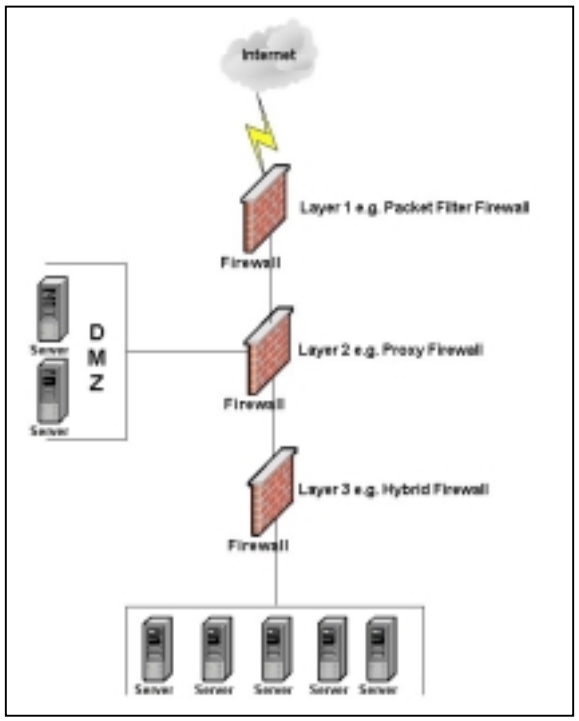
The point is to slow down the time it takes to compromise a system. A recent article on *CNET.com* reported that it took an intruder less than a minute to break into a university computer via the Internet, where he stayed less than 30 minutes. Yet, the process of finding out what he did and restoring the network took 34 hours. The article also points out that the average clean-up cost from an intrusion is $22,000. With a distributed architecture, it's less likely that a hacker can barge into your site in a mere 30 seconds; the harder it is to get it, the greater likelihood that he will give up and try an address that's not so much work.

Designing a Distributed Firewall Architecture

Implementing defense in depth using distributed firewall architecture is not complicated but needs to be customized to each organization and set of data being protected. The point is to secure the most sensitive data at the center of the architecture, with increasingly tighter rings of security at each layer.

For example, most organizations place a packet filtering firewall at the gateway, or outer

perimeter, of the network. This allows for maximum throughput, because only up to layer 3 of the OSI model is checked. Behind this perimeter firewall, you should install an application gateway proxy-based firewall, which verifies the entire contents of each packet all the way through the application layer (layer 7). At this layer, you should also have anti-virus software checking content of each packet for viruses, Trojan horses, and block files.

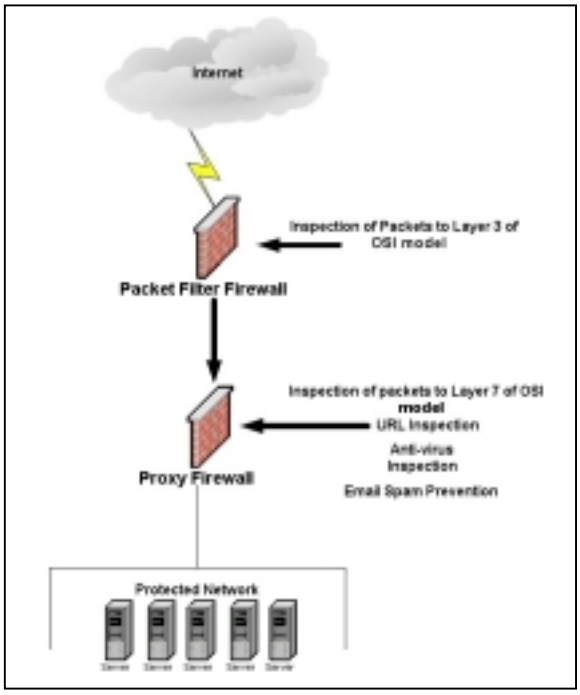


The inner firewall should regularly check the exterior firewall to make sure there have been no breaches. With both firewalls checking on the other (technically easy to do), the firewall administrator will be alerted if one is attacked or disabled, allowing immediate reaction.

Application Gateway Proxies are the Dead-Bolts

Packet filtering is a necessary but incomplete element of any defense-in-depth strategy. Packet filtering operates only on the IP header of a packet, seeing only where the information came from, where it's going, and what kind of connection it wants to make. A packet filter cannot know the difference between a real and a forged address. A hacker can hide malicious commands or data in unexamined headers or within a packet's payload.

An application-level gateway, by contrast, intercepts incoming and outgoing packets from specific applications, runs proxies that copy and forward information across the gateway, and functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. Application-specific proxies examine each packet that passes through the gateway, verifying the entire contents of the packet all the way through the application layer (layer 7) of the OSI model – not just the IP header.



For example, an HTTP application gateway proxy will look at what a user asks for and what is returned to determine if both actions are allowed and safe. A user might make an innocent request for a Web page, but the page returned might contain malevolent code. A packet filter would allow such data to go right through to the end user's computer, but an application proxy will identify the dangerous content and bar it. Application proxies actually participate in the applications they're safeguarding.

Application proxies mirror, or spoof, each end of the connection into thinking it's talking to the ultimate destination. It's an agent application – a

man in the middle. A user thinks he is talking to a Web server, for example, but he's really talking to the firewall in the middle, and vice versa. The firewall is essentially running two pieces of code: one looks like a server to the client and the other looks like a client to the server.

For more information on how application gateway proxies work, specifically CyberGuard's implementations, read "CyberGuard Application Gateway Proxies: Beyond Packet Filtering," a CyberGuard white paper available at http://www.cyberguard.com/SOLUTIONS/whitepapers_intro.cfm.

Why Application Proxies Aren't More Common

Application gateway proxies provide the highest level of firewall security, yet very few firewall companies provide them in their products. Why? Because they are computationally intensive and, if implemented poorly, can negatively impact network performance. Also, application-specific proxies are very difficult to write, since you have to predict all the actions a user might want to perform and write rules to govern those actions.

CyberGuard's strategy for overcoming performance bottlenecks is to doggedly grind away at the computational demands with faster processors and better code optimization. Today's 32-bit programming environment, along with the advent of symmetric multi-processing, makes CyberGuard's application-level gateways as transparent as they are secure. As a result, CyberGuard firewalls offer some of the fastest operations at the proxy level.

Don't Forget a Hardened Operating System

Why should a hacker knock himself out on the steel front door (the firewalls) if the OS back door is wide open? A hardened operating system is a critical layer in any defense-in-depth strategy. A hardened OS is one in which the vendor has modified the kernel source code to provide a secure perimeter between the non-secure application software, the secure application software, and the network stack. This eliminates the risk of exploiting a service running on the hardened OS that could otherwise provide root-level privileges to hackers.

Don't confuse a hardened OS with a "patched" OS. The latter is a commercial OS from which unnecessary services have been removed and on which the latest security patches have been installed. A patched OS has had no modifications made to the kernel source code to enhance security. A patched OS is only secure until the next vulnerability in the underlying OS or allowed services is discovered.

A hardened OS also relieves you of the worry and work of continuously applying OS patches. Be aware that a hardened operating system is no substitute for a firewall. It is just another level of defense in an architecture that should contain multiple, distributed firewalls as well.

Defense in Depth in Demand at Baltimore Technologies

Baltimore Technologies, a leading global IT security company with headquarters in the U.K., counts the British Ministry of Defense and other high-security British government agencies as customers. Simon Godfrey, sales manager for Baltimore Technologies, says that defense in depth is in big demand with customers. "The trend towards defense in depth really took off about two years ago," he says. "Layering firewalls is a very effective way to protect sensitive data. Each time you add a new type of firewall, you dramatically increase security."

Yes, Godfrey admits, adding multiple firewalls increases customer costs, both in terms of hardware and support. But customers with high security needs recognize that the extra protection is well worth the cost. "Repairing a security breach can easily cost five to ten times the cost of implementing defense in depth," Godfrey says. "The costs of a security breach are far-reaching: identifying the problem, stanching it, repairing it, reinstating or recreating lost or damaged data, and don't forget the possibly irreparable cost of bad press and loss of customer confidence. With cyber-terrorism and hacking on the rise, companies protecting sensitive data realize that it's a matter of when, not if, their systems will be attacked."

Summary

Defense in depth is the practice of layering defenses to increase data protection. A distributed firewall architecture is at the heart of an effective defense-in-depth strategy. A packet filtering firewall provides a good perimeter defense, but an application gateway proxy-based firewall is critical to raising the cost of an attack and giving you more time to respond when a breach is detected.

CyberGuard's implementation of application gateway proxies takes advantage of fast processors and optimized code to deliver the highest levels of security with no perceptible latency. Security administrators can leverage CyberGuard's proxies to implement bulletproof security in applications that are most commonly used in the organization and thus offer the greatest vulnerability.

A distributed firewall architecture is more expensive to implement and maintain than a monolithic architecture, to be sure. But the cost of a security breach will almost certainly be far greater.

# # #

References

"CyberGuard Application Gateway Proxies: Beyond Packet Filtering," CyberGuard white paper, http://www.cyberguard.com/SOLUTIONS/whitepapers_intro.cfm

"Secure to the Core – OS Hardening," CyberGuard white paper, http://www.cyberguard.com/SOLUTIONS/whitepapers_intro.cfm

"Defense-in-Depth: An Introduction, Brian Nelson, SANS Institute, June 30, 2001

"Defense in Depth," Brian McKenney, The Edge Newsletter, http://www.mitre.org/pubs/edge/february_01/mckenney.htm

WHITE PAPER

CyberGuard Corporate Headquarters
2000 West Commercial Boulevard Suite 200
Fort Lauderdale, Florida 33309
Phone: 954.958.3878
Fax: 954.958.3901
E-mail: info@cyberguard.com

CyberGuard Europe Limited
Asmec Centre, Eagle House
The Ring, Bracknell
Berkshire, RG12, 1HB
United Kingdom
Phone: +44 (0) 1344 382550
Fax: +44 (0) 1344 382551
E-mail: info@cyberguard.co.uk

www.cyberguard.com

CYBERGUARD WORLDWIDE
DEFEND YOUR DOMAIN