



Dynamic Packet Filtering (DPF)

Introduction to DPF



Copyright © 2002, NetMaster Digital Security, Inc.
All Rights Reserved



Introduction

What is a packet filter?

A packet filter is a mechanism used to provide a level of digital security by controlling the flow of information (data packets) via the examination of key information in packet headers. A packet filter determines if these packets are allowed to go through a given point based on certain access control policies. Typically, this “point” is a firewall, router or gateway into a network or workstation.

An analogy that may put this in perspective is that of a courier sorting service like Federal Express. The sorting system examines packages and ensures that each package is coming from a valid address, and that it is destined for a valid location that FedEx services. The sorter also checks to ensure that this type of package is allowed to be shipped to that location. Restraints in size, weight and content may determine that the package cannot be released and must be returned to sender. This process of sorting and routing packages is the same in how a packet filter functions.

What is a “dynamic” packet filter?

A dynamic packet filter (DPF) builds on the concepts of a normal packet filter but with increased intelligence. Traditional packet filters are often slower and more difficult to manage in larger networks with complex security policies. NetMaster’s DPF implementation minimizes these issues with intelligent firewall “chaining” that makes the system much more optimized and responsive, while simplifying the process of managing firewall rules to enforce complex security policies. In this regard NetMaster’s **Firewall Wizard** works harder so you don’t have to. Combined with **Access Control Groups**, it is further managed intelligently by applying time-based rule sets to security policies in the filter by associated groups of network resources.

What is a “stateful” packet filter?

A stateful packet filter (SPF), quite simply, manages and maintains the connection state of a session through the filter to ensure that only authorized packets of a policy are permitted in sequence. Typically, a stateful packet filter will maintain a table associating active sessions of information to ensure data is not somehow passed through the filter out of sequence. In other words, it makes sure that, before a data packet is allowed through, a connection and establishment sequence has already occurred and has been accepted as part of the policies within the filter. NetMaster uses a level of stateful connection tracking in its DPF while in network address translation (NAT) mode. Since connection tracking is an



integral part of NAT, NetMaster uses this to ensure packets maintain state through the filter. In addition, NetMaster's DPF tracks the connection state in such a way that the filter can use the logging facilities to monitor the headers of connections, data packets and closing packets for later forensic analysis.

What is stateful packet inspection?

Stateful packet inspection (SPI) builds on the process of stateful packet filtering by also analyzing the payload within a packet. In other words, each packet is analyzed to ensure that the content matches the expected service it is communicating with. For example, SPI would check web traffic data to ensure that it was actually HTML type data and not streaming music or other unrelated content. If the data type did not match the acceptable use for the service, SPI would block the packet from passing through. With SPI, it is possible to do anti-virus checks and even quarantine suspicious data if it matched certain criteria.

SPI is a very powerful feature, but it also comes at a cost. The processing overhead incurred in having to analyze every individual packet passing through the filter is extremely resource intensive. Significant processor and memory resources are required in order to provide SPI capability and to minimize network latency. As such, SPI devices are typically quite expensive.

Many security product vendors often obscure the differences between SPF and SPI and how their product(s) actually discern whether a connection is permitted or a data packet is allowed to pass. These two technologies are not the same and special care must be taken when determining your own requirements as to what method best suites your needs.

SPF != SPI

Stateful packet inspection is not the same thing as stateful packet filtering. Not only is SPI more resource intensive, but it can also be quite cumbersome to maintain as common protocols such as HTTP now have more and more services running over it. A common problem with SPI devices is that they can sometimes reject valid data or, worse yet, allow certain data that should not be allowed. A recent example of this are the recent addition of web services using Microsoft's SOAP architecture which runs over HTTP, but can completely bypass the inspection and provide malicious code execution through the filter.

Although SPI is very powerful, the added complexity and significant resource requirements (i.e. expensive hardware) compared to the benefits it provides, often results in it being a less than optimal solution for the small to medium-sized enterprise (SME) customers that NetMaster's products service.



NetMaster's DPF is designed to fit into limited resources, embedded solutions and, therefore, the most efficient filter technology must be utilized. The optimizations and "chaining" functionality that are a part of our DPF often results in our DPF performing much better than other embedded solutions based on SPI.

What about the fact SPI can help prevent attacks?

Well, NetMaster's DPF can do that too. In addition to the dynamic packet filter, NetMaster's DPF uses both ingress and egress filtering to provide a level of anti-spoofing protection. Spoofing is where an attacker will modify the IP packets sent to a remote system to cause that system to think the incoming packets are actually from another, valid host. NetMaster's ingress and egress filters can guard against such attacks.

The DPF also provides mechanisms, both within the kernel and the operating system core it is attached to, to prevent many common Denial-of-Service (DOS) attacks. Examples include:

- **SYN Floods:** If an attacker sends SYN packets with faked source addresses to a vulnerable host, it is possible for the host to allocate a socket for each connection request. This begins to consume resources within the system and eventually can cause the system to become unresponsive. There is no easy way to prevent this. The NetMaster DPF minimizes this by using a special algorithm that utilizes cookies so that only a subset of the memory actually needed for an incoming connection is allocated when a SYN packet is received. After the final and proper packet has arrived with the appropriate cookie, the rest of the memory required for the TCP connection is then allocated. This method also prevents spoofing of particular packets because the host checks the cookie it received in an earlier packet with the one just sent.
- **Ping of Death:** When a huge IP packet (typically larger than 65,535 bytes) is sent from an attacker, network resources may fragment the packet into many smaller pieces so it can be sent over the network to the vulnerable host. When these packets arrive, they may be overlapping and malformed which could cause the host to get confused when trying to put it back together. This then triggers a range of adverse conditions ranging from crashing, freezing and even rebooting. NetMaster's DPF drops such fragmented packets, ensuring vulnerable hosts are not attacked in this way.
- **Land Attack:** If an attacker sends spoofed SYN packets containing the IP address of the vulnerable host as both the source and destination address, the host responds with a SYN-ACK packet to itself, which results in resource utilization in the connection table that can cause the host to freeze, or in some situations, to even reboot. NetMaster's DPF uses a combination of its IP spoofing



protection and its SYN Flood defensive measures to thwart such attacks.

- **Tear Drop Attack:** When the attacker sends two different parts of a fragmented TCP packet that overlap, the host attempting to reassemble the packet can freeze, or even crash. When NetMaster's DPF sees this type of attack, it discards the fragmented packet.
- **IP Source Routing Attack:** If an attacker sends a spoofed packet containing a trusted IP address it could be possible to enter a network with a false IP and then have information sent back to the attacker's real address. This type of information leakage is prevented through NetMaster's DPF by dropping IP traffic that employs the source route option in the packet when trying to pass through the filter.
- **IP Private/Reserved Class Routing Attack:** Particular blocks of IP addresses have been reserved by the Internet Assigned Numbers Authority (IANA) to be used on special or private networks, or for future use. An attacker can fake an IP address within such reserved blocks to hide his true identity during an attack. NetMaster's DPF can be configured to allow or drop such packets from passing through the filter, preventing any such attack attempts.
- **Out Of Band Attack:** Many versions of Windows are susceptible to attacks utilizing Out of Band (OOB) data. When an attacker sends such information to an established connection (typically NetBIOS on port 139) it can have adverse effects ranging from General Protection Faults (GPF/Blue Screen of Death) to loss of network functionality. NetMaster's DPF protects against this by rejecting invalid OOB data to such ports passing through the filter.



Conclusion

Is DPF right for me?

DPF provides the best of both worlds in packet filter architectures. It provides the speed and efficiencies of traditional packet filters, yet also provides the connection state tracking that is essential to mitigating the risk of out of sequence attacks and information leakage. Our products are based on the same technologies used in most networking equipment in use today and, therefore, stability and security is unprecedented. When combined with the intelligence of NetMaster's device management tools, it becomes a simple process to manage complex security policies with a minimum amount of resources. With the functionality we've added to prevent many common hacker attacks, NetMaster's DPF can provide protection levels similar to SPI – at a fraction of the cost.

Give Gateway Guardian a try and see for yourself.

For More Information

For more information about licensing or purchasing a Gateway Guardian solution for your organization, visit NetMaster's web site at <http://www.netmaster.com>

NetMaster Digital Security
Suite 300
1055 West Hastings St.
Vancouver, BC
Canada V6E 2E9
604-609-6184
www.netmaster.com

Updated September 2002

© 2002 NetMaster Digital Security, Inc. All Rights Reserved. NetMaster, the NetMaster logo, Gateway Guardian, GGOS, CSM are trademarks of NetMaster Digital Security, Inc. Other product and company names mentioned herein may be trademarks of their respective companies.