

D-Link Zone Defense

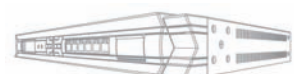
A New Proactive Network Security Architecture

Introduction

With the rapid growth and variety of technology in today's market, most business activities rely heavily on network communication. In this highly competitive business environment, enterprises have to not only weather and withstand business challenges, but also threats to their internal infrastructure from hacker attacks and the spread of viruses.

To respond to the threats from hackers and viruses, traditional network security technologies only check one appliance at a time, searching for abnormal packets passing through or denying connections which violate certain access rules, all according to the network administrators' predefined configurations. However, traditional security devices cannot effectively block massive network connections from the infected victim computers.

This article will begin by briefly outlining the functionality of traditional network security technology. D-Link's 'New Proactive Network Security Architecture', Zone Defense, will be subsequently discussed, to give an insight into how this new network security for enterprises can enhance and improve upon the foundations provided by traditional network security technologies. Finally, a concise test case has been included to illustrate how Zone Defense enables enterprises to pro-actively defend against hackers or virus attacks.



Traditional Network Security Technologies

Traditionally, network security technologies mainly focus on the following control mechanisms: application layer controls, ACLs (Access Control Lists) and packet filters. Nearly all network security appliances, including switches, routers and firewalls, are equipped with the above functionality. Enterprises benefit from using these technologies as they are provided with a level of protection, preventing internal users or external visitors from being able to access confidential or private documents, as well as furnishing them with security for the internal network. These technologies however, in the vast majority, do not provide pre-emptive measures.

In the case of traditional network security technology, enterprises suffer from virus or hacker attacks which are activated from internal victim computers. Network administrators must firstly monitor the traffic status of internal computers or routers, to deal with network paralyzation. Then, network administrators may try to locate the victim computer according to the abnormal traffic information on network devices, before they can resolve the threat of virus or hacker attacks. Meanwhile, network administrators may also set up some ACL rules on network security appliances, such as switches, routers or firewalls, in order to prevent hacker invasions or viruses from spreading. In the event that there are many victim computers in their own network, network administrators have to logon to different network security devices and set-up a number of rules to guard their own network.

There is evidently, as seen above, a lack of interaction between the network security appliances, thus these devices cannot communicate with each other in a timely fashion to effectively prevent network paralyzation. This succinctly pinpoints the inadequacies of traditional network security technologies. Enterprises however, can be furnished with the tools to defend their internal network with D-Link's Zone Defense, which will be introduced in the next section.

Zone Defense

Zone Defense, D-Link's newest proactive network security, enables D-Link's next generation of firewalls to integrate with D-Link switches, to construct a new network security architecture that effectively blocks any malicious host when detected. Therefore, if a user computer performs any abnormal network behaviour, the computer can be timely disconnected from the network and its network service connection interrupted. Consequently, this countermeasure can further avoid the spread of viruses to the same subnet or other subnets, as well as preventing a start of hacker attacks that will paralyze critical servers within enterprises.

By defining the trigger conditions for activating Zone Defense, when abnormal network traffic outbreaks, D-Link firewalls can immediately and automatically connect to D-Link switches and issue commands to them, further constraining the network behaviour of victim computers. This greatly eases the workload of system administrators and thus simplifies the complexity of network management.

A concise test case has been set-out below to demonstrate how Zone Defense prevents a virus-infected computer from paralyzing the internal network of an enterprise.

Test Case

To put the following test into practice, you may need a port scan tool, such as ipscan or superscan, to simulate the virus attack. In this case, superscan will be utilized to simulate the attack behaviour from the virus WORM_SASSER.A.

Before setting out the test scenario, it is necessary to detail how the WORM virus behaves when attempting to infect other computers in the network. The virus, WORM_SASSER.A, is a good example. When a computer is infected by WORM_SASSER.A, first of all, it will scan all other hosts on the same subnet via the Address Resolution Protocol (ARP). The infected computer will subsequently work laboriously to send out massive packets within the same network segment, to try and spread its virus through the Windows LSASS vulnerability.

Finally, all other hosts on different subnets will become targets, that the infected computer attempts to spread its virus to. At this stage, the infected computer starts to send out large amounts of TCP SYN (DST port: G139) packets, scan all other computers on different subnets and try to infect other hosts with the Windows LSASS vulnerability.

During the first two stages, network administrators can set the Zone Defense threshold to 15 ARP/ sec¹ to trigger the Zone Defense.

Once the 3rd and most critical stage has been reached, in which the virus/ worm tries to look for victims in the network, the bulk TCP SYN packets can still always overwhelm the L3 network appliances including L3 switches, routers or firewalls; thus network administrators can set the Zone Defense threshold to 15 TCP (port 139) SYN/ sec to trigger the Zone Defense.

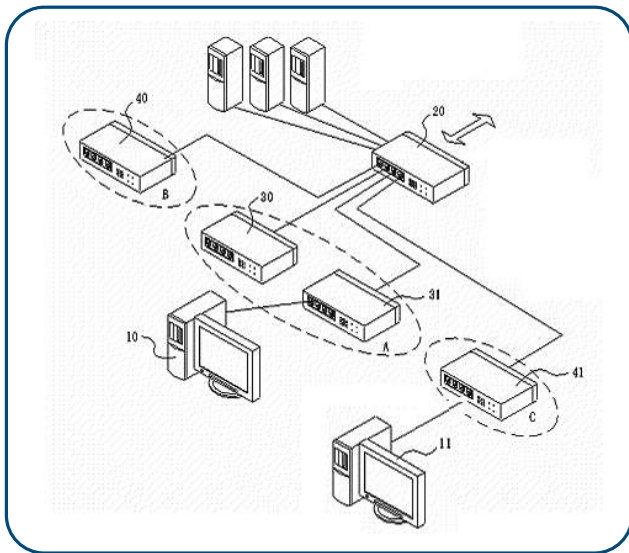
The above explanation on how infected computers might typically spread the virus WORM_SASSER.A, will assist in clarifying the below test scenario.

The test scenario is based on a network topology comprising of a D-Link firewall and D-Link managed switches² 30, 31, 40 and 41 which make up the different network segments A, B, C which in turn are connected to the DFL-800. The two user computers 10 and 11 are then connected to the network switch 31 and 41 respectively.

¹The proactive defense toward ARP layer will be expected soon in the next firmware version.

²For further information about D-Link managed switches, please refer to the appendix.

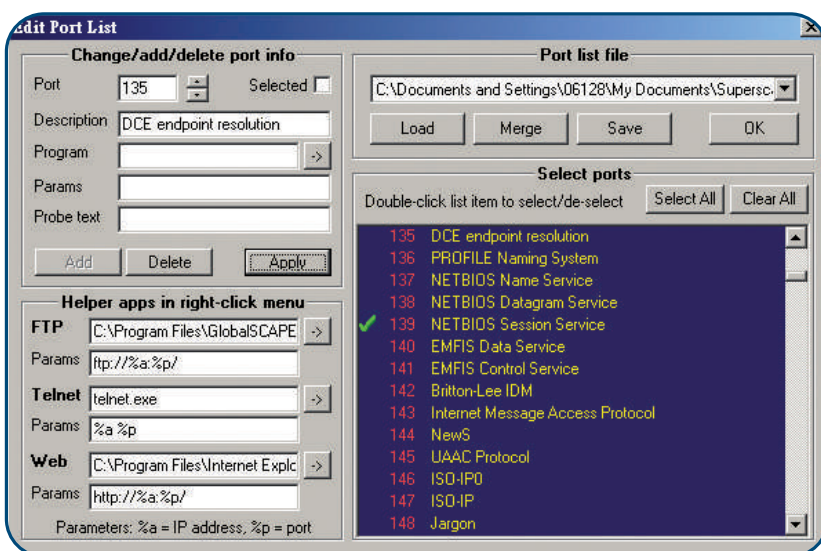
Figure 1: Network Topology in the Test Scenario



1. User computer 10 (IP: 192.168.1.2) is infected by the virus, WORM_SASSER.A, and starts sending out a large quantity of TCP SYN (DST port: G139) packets to scan all computers on the same and different subnets, spreading the virus in the network through the Windows LSASS vulnerability. A buffer overrun allows remote code execution and enables an attacker to gain full control of the affected system. User computer 11 (IP: 192.168.2.2), residing in a different subnet, is the host, that user computer 10 tries to infect.

To simulate the attack behavior of WORM_SASSER.A, port scan tools can be utilized and configured to scan port 139 (See Fig. 2) located in user computer 10 (IP: 192.168.1.2). While configuring the tools, please make sure the scan speed of these tools have been configured to maximum. Also, if possible, please launch any sniffer tools on hand, such as Ethereal or Sniffer Pro, to confirm the port scan tools are working as would be expected.

Figure 2: Configure the port scan tool to simulate the behaviour of the virus WORM_SASSER.A.



2. In order to trigger Zone Defense on network security appliances, configure the trigger condition on the DFL-800 which detects abnormal network traffic toward NetBIOS Session Service (Port 139, please refer to Fig.3) In this test, the trigger threshold is configured as 9 connections/sec (See Fig. 4), as an example. Note: threshold 9 connections/sec here refers to the working behaviour of the port scan tool, as the tool utilized here can only send a maximum of 10 TCP SYN thresholds in this test circumstance.

Figure 3: Configure the trigger condition towards NetBIOS Session Service (Port 139).

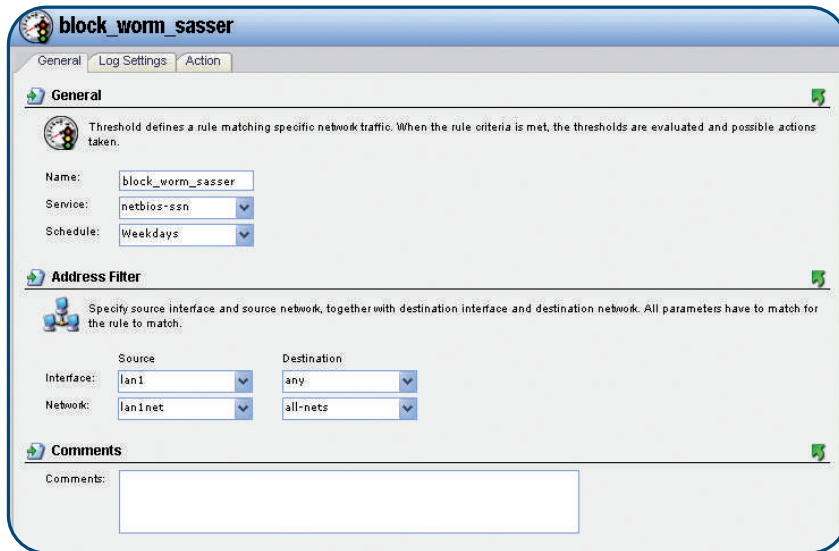
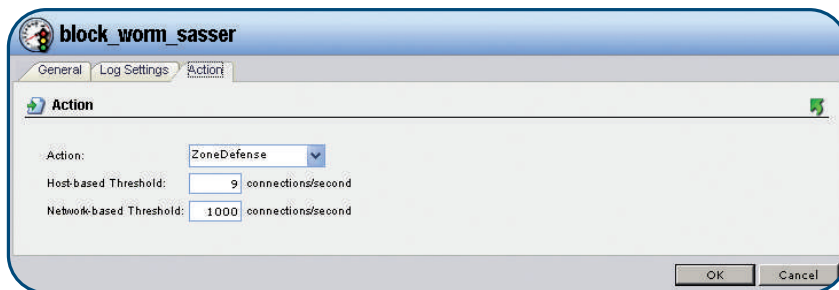


Figure 4: Configure the trigger threshold towards NetBIOS Session Service



3. To implement the simulation of the WORM_SASSER.A attack, launch the sniffer and port scan tools on user computer 10 (IP: 192.168.1.2). On user computer 11 (IP: 192.168.2.2), issue the command 'ping 192.168.1.2 -t' in the command line for determining the activation of Zone Defense. If Zone Defense is activated, the message will turn 'Reply from 192.168.1.2: bytes=32 time=2ms TTL=127' into 'Request time out' (see Fig. 5).

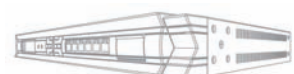
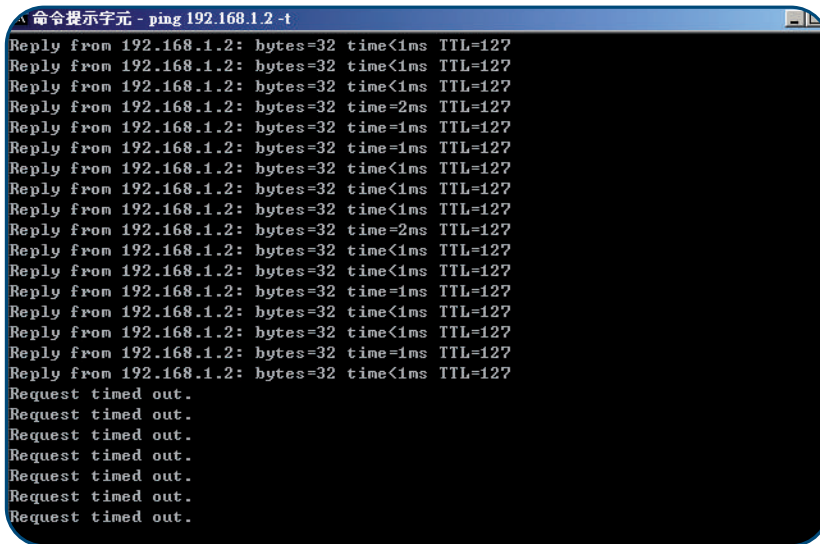


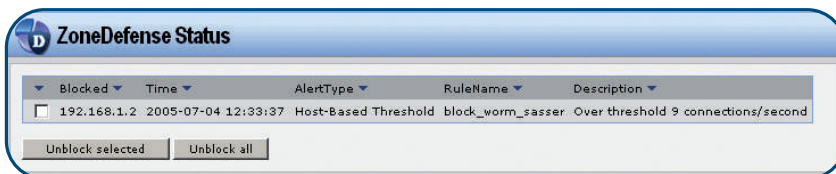
Figure 5: Zone Defense is activated and the attack host is blocked.



```
命令提示字元 - ping 192.168.1.2 -t
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=2ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Figure 6 below displays information regarding the Zone Defense status. This screen gives information that the infected host has been blocked and so in turn demonstrates that Zone Defense successfully provides the proactive mechanism to enable enterprises to guard their critical internal network.

Figure 6: Zone Defense status for blocking the infected host



Conclusion

Zone Defense is the 'New Proactive Network Security' for enterprises, integrating network security appliances to automatically detect network traffic. If the packet flow of a user computer triggers the conditions for Zone Defense, a Zone Defense command will immediately and automatically be sent to the specified network switch to efficiently block the network connection of the user computer. Thus, for enterprises, Zone Defense greatly reduces the damage and loss caused by viruses and hackers, as well as effectively enhancing network performance. Network Administrators benefit as it becomes easier and less timely to locate the infected computers. Once the infected computer has been detected it is no longer necessary to manually issue system commands on network devices. D-Link's Zone Defense effectively enables enterprises to defend their internal networks at the edge of their networks.

Appendix

D-Link Managed Switches Supported by Zone Defense

DFL-800/1600/2500 firmware v2.03.00 (or later versions) currently supports the following switches:

- D-Link DES 3226S (minimum firmware: R4.02-B14)
- D-Link DES 3250TG (minimum firmware: R3.00-B09)
- D-Link DES 3326S (minimum firmware: R4.01-B39)
- D-Link DES 3350SR (minimum firmware: R1.02.035)
- D-Link DES 3526 (minimum firmware: R3.01-B23)
- D-Link DES 3550 (minimum firmware: R3.01-B23)
- D-Link DGS 3324SR (minimum firmware: R4.10-B15)
- D-Link DGS-3427 (minimum firmware R1.00-B35 / firewall firmware 2.05)
- D-Link DGS-3450 (minimum firmware R1.00-B35 / firewall firmware 2.05)