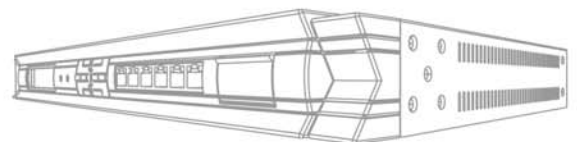


NETDEFEND

WHITEPAPER: 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 environment, businesses 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 rely on a single appliance, which identifies abnormal packets or denies connections which violate certain access rules, all according to the network administrator's pre-defined configurations. However, traditional security devices cannot effectively block massive network connections from the infected victim computers.

This white paper will begin by briefly outlining the functionality of the traditional network security technology. D-Link's 'New Proactive Network Security Architecture', ZoneDefense, 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 ZoneDefense 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 these protection mechanisms, preventing internal users or external visitors from being able to access confidential or private documents, as well as securing the internal network against intruders. These technologies however do not provide pre-emptive measures.

In a traditional network security environment, when businesses suffer from

virus or hacker attacks activated from internal victim computers, network administrators must firstly monitor and analyse traffic between network elements, to identify the source of the threat. They also need to configure 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 on the network, network administrators have to logon to different network security devices and set-up a number of rules to guard their network against the outbreak.

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 hostile attacks, such as Denial of Service. This succinctly pinpoints the inadequacies of traditional network security technologies.

Businesses however, can be furnished with the tools to defend their internal network with D-Link's ZoneDefense, which will be introduced in the next section.

ZoneDefense

ZoneDefense, D-Link's proactive network security, enables D-Link's next generation of firewalls to integrate with D-Link's managed switches, to construct a network security architecture that effectively blocks any malicious host when detected. Therefore, if a host computer displays any abnormal network behaviour, the computer can be timely disconnected from the network without disrupting general network services. 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.

ZoneDefense is triggered when abnormal network traffic conditions meet pre-configured thresholds on the firewall. When this happens, the firewall immediately and automatically contacts the D-Link switches and issues commands to them, that result in blocking any traffic to and from the suspicious

host.

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 behavior 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 on the network. The virus, WORM_SASSER.A, is a good example. When a computer is infected by WORM_SASSER.A at stage 1, it will scan all other hosts on the same subnet via the Address Resolution Protocol (ARP). At stage 2, the infected computer will send out massive amounts of packets within the same network segment, to try and spread its virus through the Windows LSASS vulnerability.

Finally at stage 3, 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: 445) packets, scan all other computers on different subnets and try to infect other hosts with the Windows LSASS vulnerability.

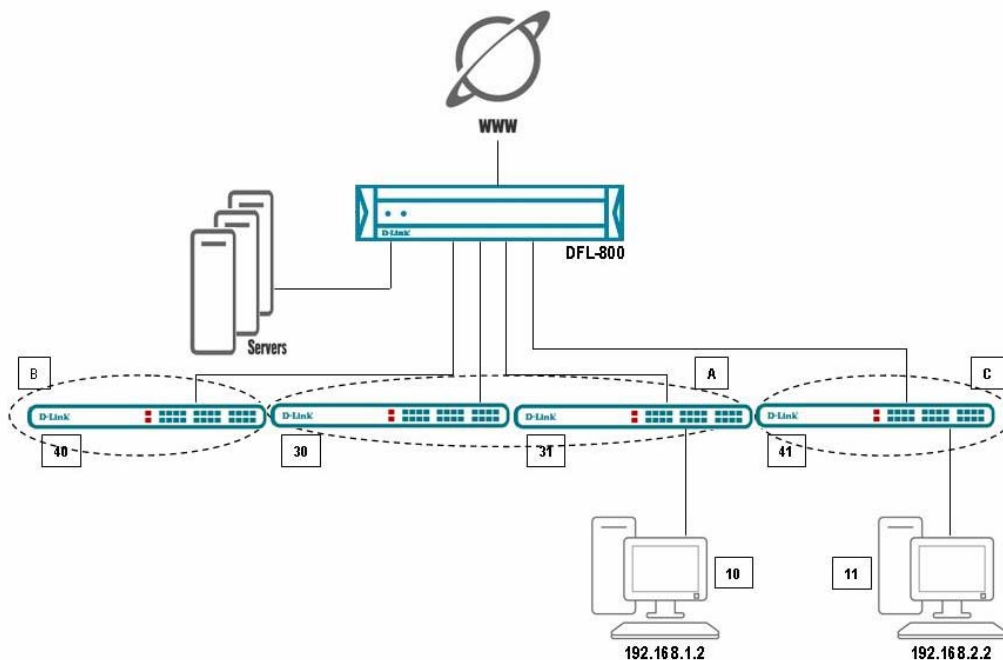
During the first two stages, network administrators can set the Zone Defense threshold to 15 ARP/ sec¹ to trigger ZoneDefense. Once the 3rd and most critical stage has been reached, in which the virus/ worm tries to look for victims on the network, the bulk TCP SYN packets can still overwhelm the L3 network appliances including L3 switches, routers or firewalls; thus network administrators can set the ZoneDefense threshold to 15 TCP (port 445) SYN /sec to trigger ZoneDefense.

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

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 DFL-800 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.

Figure 1: Network Topology in the Test Scenario



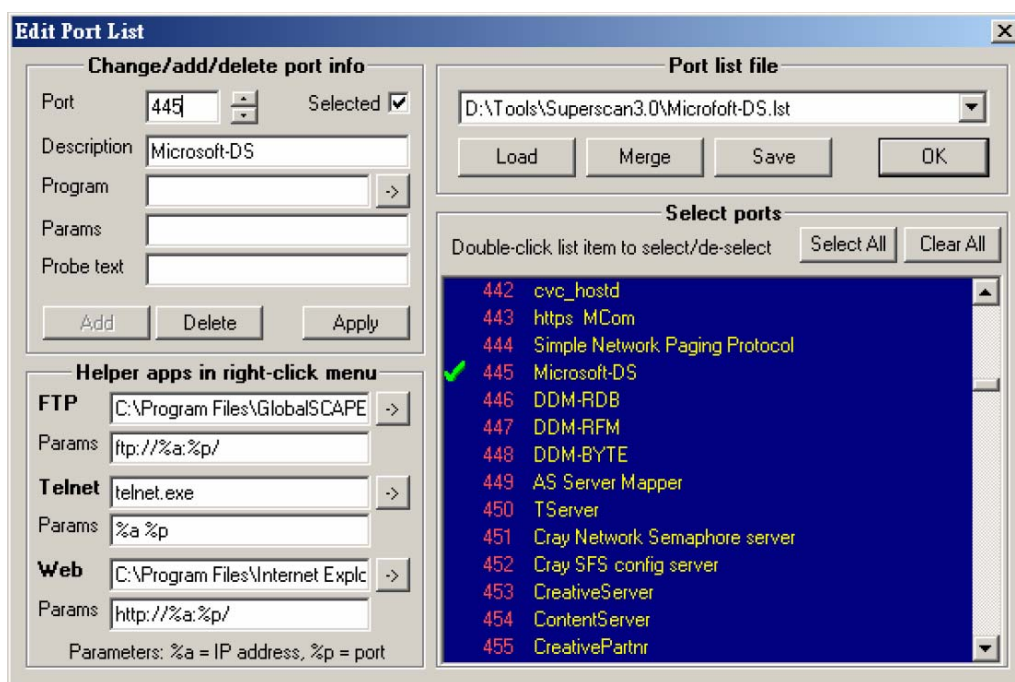
1. User computer 10 (IP: 192.168.1.2) is infected by the virus, WORM_SASSER.A, and starts sending out a large quantity of TCP SYN (DST port: 445) packets to scan all computers on the same and different

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

subnets, spreading the virus in the network through the Windows LSASS vulnerability. Windows LSASS vulnerability is a buffer overrun that 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 on user computer 10 and configured to scan port 445 (See Fig. 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 ZoneDefense on network security appliances, configure as the trigger a condition against Microsoft SMB service (Port 445, please refer to Fig.3) In this test, the trigger threshold is configured as 9 connections/sec (See Fig. 4), as an example.

Note: the value of 9 connections/sec refers to the working behaviour of the port scan tool, as the tool utilized here can only send a maximum of 10 TCP SYN.

Figure 3: Configure the trigger condition towards Microsoft SMB Service (Port 445).

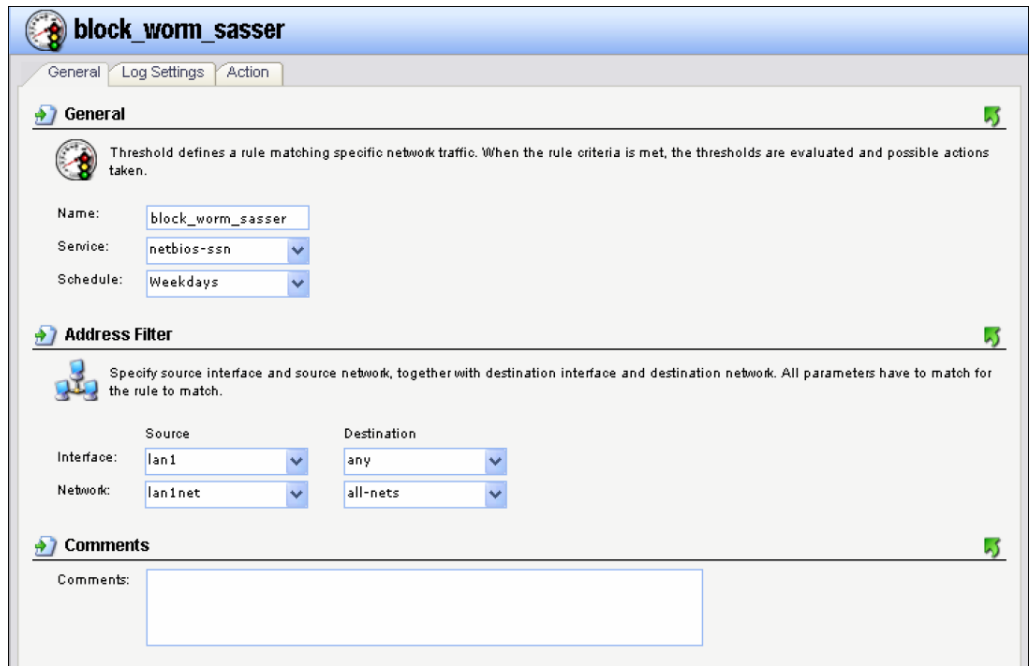
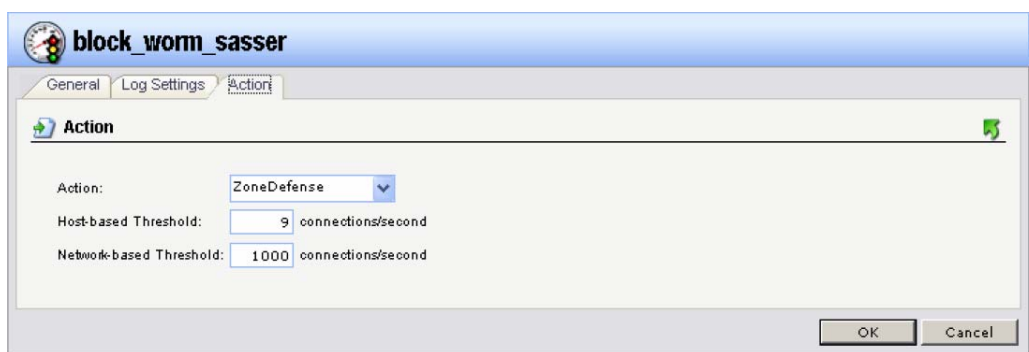


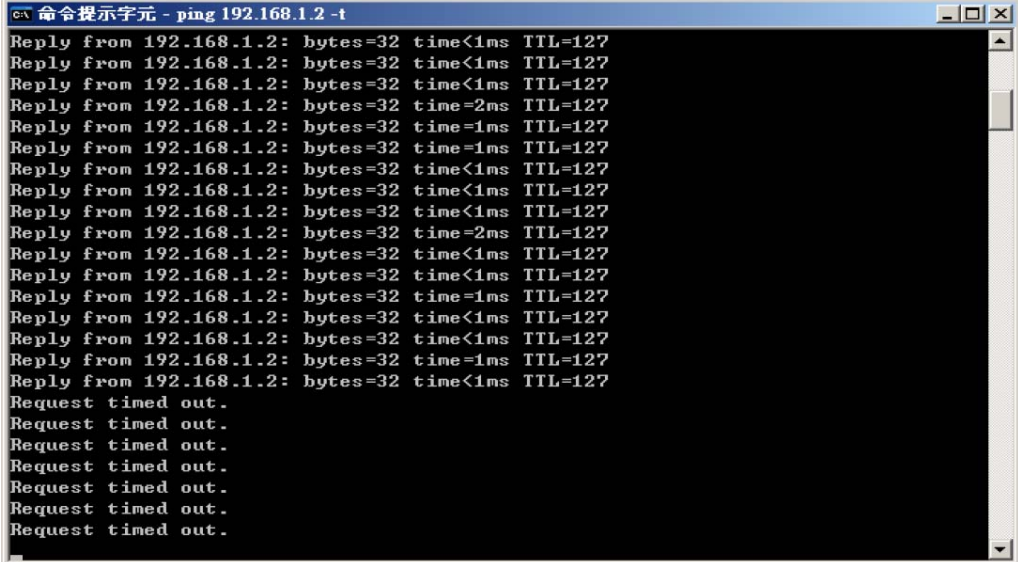
Figure 4: Configure the trigger threshold towards Microsoft SMB Service



- 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 command line for determining the activation of ZoneDefense. If ZoneDefense 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: ZoneDefense is activated and the attack host is blocked.



```
命令提示符 - 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<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
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 ZoneDefense status. This screen confirms that the infected host has been blocked and so in turn demonstrates that ZoneDefense successfully provides the proactive mechanism to enable businesses to guard their critical internal network.

Figure 6: ZoneDefense status for blocking the infected host



Conclusion

ZoneDefense provides businesses with “Proactive Network Security”, integrating network security appliances to automatically detect suspect network traffic. If the packet flow of a host computer triggers the conditions for ZoneDefense, a ZoneDefense command will immediately and automatically be sent to the specified network switch to efficiently block the network connection of the host computer. Thus, for businesses, ZoneDefense greatly reduces the damage and loss caused by viruses and hackers, as well as effectively enhances 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 ZoneDefense effectively guards businesses against internal network risks.

Appendix

D-Link Managed Switches Supported by ZoneDefense

DFL-800/1600/2500 firmware v2.11.02 currently supports the following switches:

- D-Link DES-3226S (firmware: R4.02-B26 or later)
- D-Link DES-3250TG (firmware: R3.00-B09 or later)
- D-Link DES-3326S (firmware: R4.01-B39 or later)
- D-Link DES-3350SR (firmware: R3.02-B12 or later)
- D-Link DES-3526 Rev 3.x (firmware: R3.06-B20 only)
- D-Link DES-3526 Rev 4.x (firmware: R4.01-B19 or later)
- D-Link DES-3550 Rev 3.x (firmware: R3.05-B38 only)
- D-Link DES-3550 Rev 4.x (firmware: R4.01-B19 or later)
- D-Link DES-3800 series (firmware: R2.00-B13 or later)
- D-Link DGS-3324SR/SRi (firmware: R4.30-B11 or later)
- D-Link DXS-3326GSR/3350SR (firmware: R4.30-B11 or later)
- D-Link DGS-3400 series (firmware: R1.00-B35 or later)