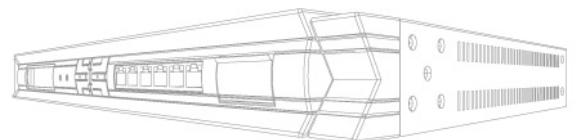


 **NETDEFEND**

WHITEPAPER: D-LINK ZONEDEFENSE

A New Proactive Network Security Architecture



Introduction

Nowadays, with the rapid growth and variation of information technologies, most business activities are heavily relying on network communication. In this highly competitive business environment, enterprises have to face not only harsh business challenges, but also various threats from networks, such as hacker's attacks and viruses spread.

To respond to the threats from hackers and viruses, traditional network security technologies usually use a single appliance to check for abnormal packets passing through the network or deny connections violating access rules according to network administrators' predefined configurations. However, these devices cannot effectively block massive network connections from demented victimized computers, which are usually infected by viruses or manipulated by hackers.

This article provides a brief concept of traditional network security technology and introduces the 'New Proactive Network Security Architecture', ZoneDefense proposed by D-Link, which can enhance network security for enterprises and minimize the inabilities of traditional network security technologies. A concise test case will be used to illustrate how ZoneDefense enables enterprises to defend hackers and virus attacks.

Traditional Network Security Technologies

Traditionally, network security technologies focused mainly on the following control mechanism: application layer controls, Access Control Lists (ACLs), and packet filters. Nearly all network security appliances, including switches, routers and firewalls, have been equipped with such functions. The major benefits of these technologies act as a protection mechanism for enterprises that prevent internal users from having unauthorized access to confidential services or information, as well as increase the security of the internal network from external intruders. These technologies in principle only enable passive measures.

In a traditional network security environment, whenever enterprises encounter virus or hacker attacks activated from internal victimized computers, network administrators will have to monitor the traffic status of internal computers or routers to discover usual traffic information on network devices before the threat can be resolved. Meanwhile, network administrators may also require to configure some ACL rules on the network security appliances, such as switches, routers or firewall to prevent virus spread or hacker invasion. If there are many victimized computers in their network, network administrator will have to logon to different network security devices and setup rules to guard their network against the outbreak.

Based on the above mentioned scenario, it is obvious that there is a lack of an interactive mechanism between the network security appliances, resulting in devices being unable to communicate with each other in a timely manner to effectively prevent network from denial of service. It is this inability in traditional network security technology that approval is sought to introduce the 'New Proactive Network Security Architecture' ZoneDefense solution to enable enterprises' proactive defense of their internal network.

ZoneDefense

ZoneDefense is proposed by D-Link to enable D-Link's next generation of firewalls to integrate with D-Link's switches to construct a new network security architecture that can effectively block any malicious host upon detection. This security feature triggers in the event when a user's computer performs any abnormal network activity, the computer can quickly disconnect from the network without disrupting network service connection. This countermeasure can further prevent virus outbreak to the same subnet or other subnets, at the same time prevent hacker attacks that can paralyze critical servers within enterprises.

By defining the conditions for activating the ZoneDefense feature when there is abnormal network traffic break out, D-Link firewalls can immediately and automatically connect to D-Link switches based on the condition defined and issue commands to restrict the network

behavior of the victimized computers by locking the switch port where the infected host(s) is connected. This will greatly ease the load of system administration and simplify the complexity for network management.

In the next section of this document, a concise test case study will be used to simulate how ZoneDefense prevents a virus-infected computer from paralyzing the internal network of an enterprise.

Test Case

To perform the following test, a port scan tool will be needed, 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 going into the test scenario, it is necessary to first introduce briefly the concept of how the WORM virus behaves in attempting to infect other computers on the network. When a computer is infected by WORM_SASSER.A at Stage 1, the infected computer will scan all other hosts on the same subnet via Address Resolution Protocol (ARP). At Stage 2, the infected computer will next send out massive packets within the same network segment to spread the virus through the vulnerability of Windows LSASS.

Finally, at Stage 3, all other hosts on different subnets will also become targets where the infected computer will spread the virus. At this stage, the infected computer will start to send out large amount of TCP SYN (DST port: 445) packets, scan all other computers on different subnets and attempt to infect other hosts by attacking Windows LSASS vulnerability.

During stages 1 and 2, network administrators can setup a threshold such as 15 ARP/ sec¹ to trigger the ZoneDefense. At Stage 3, which is the stage where virus / worm attempts to look for victims in the network, the bulk TCP SYN packets can overwhelm the L3 network appliances, including L3 switches, routers or firewalls. Network administrators can therefore setup ZoneDefense with threshold such as 15 TCP (port 445) SYN/ sec to trigger the ZoneDefense before it happens.

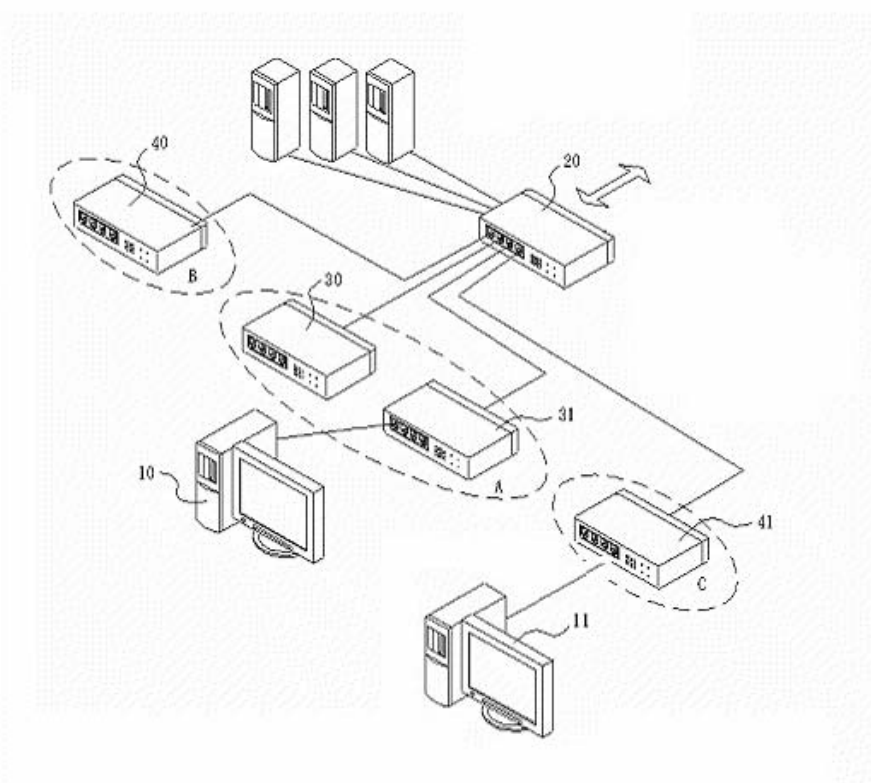
By understanding the stages of how the infected computers are spreading the virus WORM_SASSER.A, the following test scenario described below will be easier to comprehend.

In this test, the network topology comprises of a DFL-800 firewall, and D-Link managed switches² 30, 31, 40, 41 for different network segments A, B, C connected to the DFL-800, with two user

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

computers 10 and 11 connected to the network switch 31 and 41 respectively.

Figure 1: Network Topology in the Test Scenario



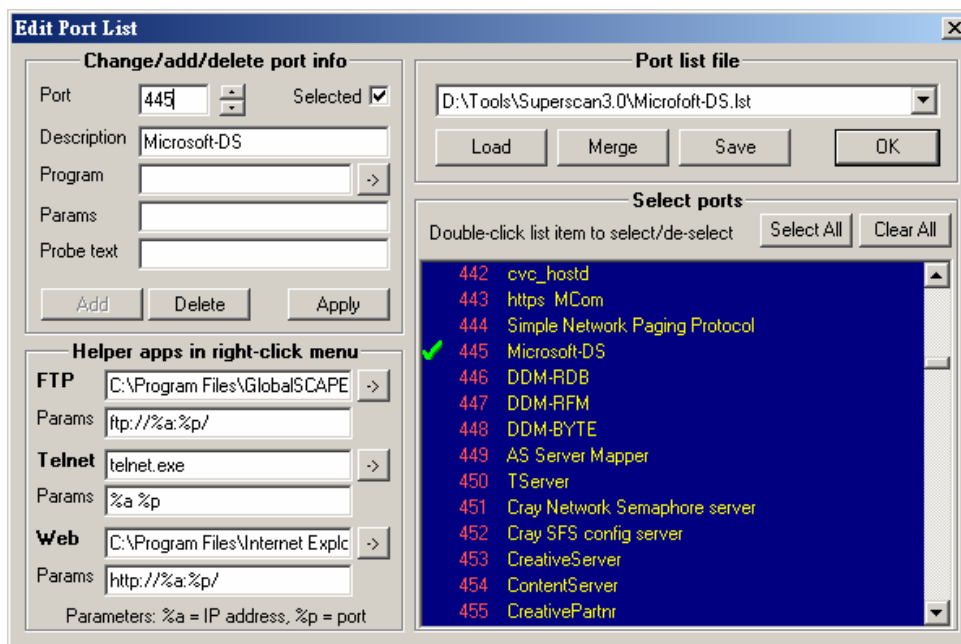
1. User computer 10 (IP: 192.168.1.2) is infected by the virus, WORM_SASSER.A and starts sending out a large quantity of TCP SYN (DST port : 445) packets to scan all computers on the same subnet and different subnets, spreading the virus on the network through Windows LSASS vulnerability. Windows LSASS vulnerability is a buffer overrun that allows remote code execution and enables an attacker to gain full control of the

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

infected system. User computer 11 (IP: 192.168.2.2), residing in 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 the port 445 (See Fig. 2) on User computer 10 (IP: 192.168.1.2). While configuring the tools, set the scan speed to maximum. In addition, if possible, launch the sniffer tools on hand, such as Ethereal or Sniffer Pro, to confirm the port scan tools are working according to expectation.

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



- In order to trigger the ZoneDefense on network security appliances, configure trigger condition of the DFL-800 to detect abnormal network traffic towards Microsoft SMB Service (Port 445). See Fig.3 for details. In this test, the trigger threshold is set to 9 connections/sec (See Fig. 4). The threshold 9 connections/sec here refers to the working behavior of the port scan tool, since the tool utilized here at most can send only 10 TCP SYN, being threshold in this test environment.

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

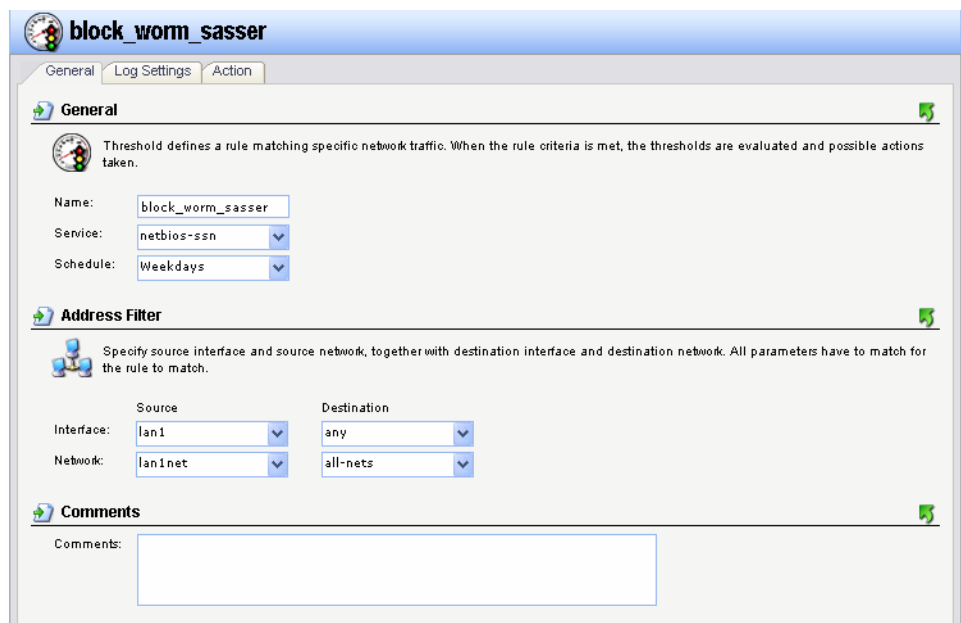
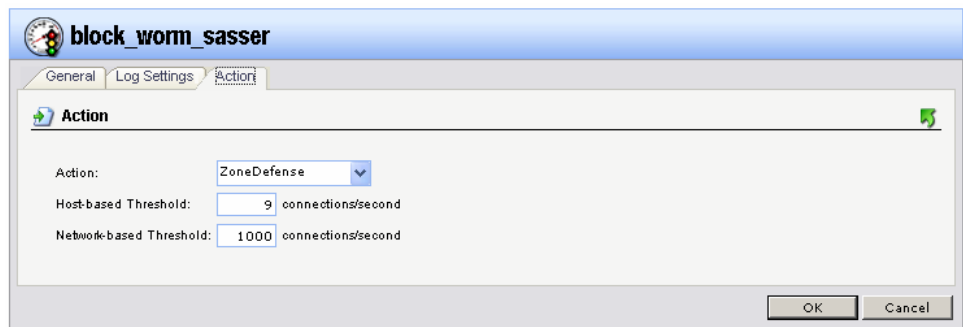
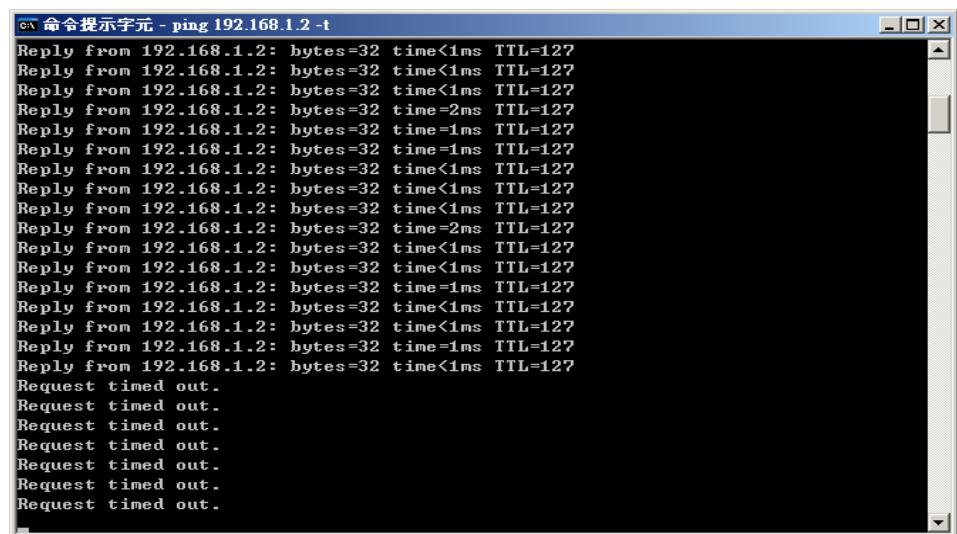


Figure 4: Configure the trigger threshold toward Microsoft SMB Service



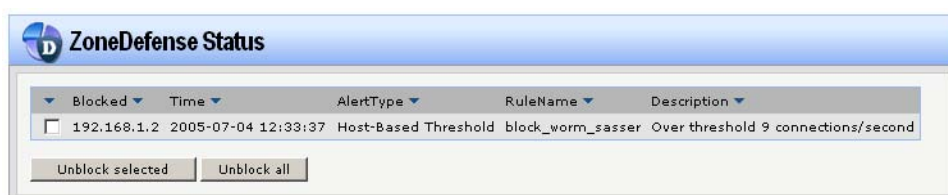
3. To simulate the WORM_SASSER.A attack, launch the sniffer and port scan tools on User computer 10 (IP: 192.168.1.2). On User computer 11 (IP: 192.168.2.2), issue the command 'ping 192.168.1.2 -t' in command line for determining the activation of ZoneDefense. If ZoneDefense is activated, the message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

Figure 5: ZoneDefense is activated, and the attack host is blocked.



In Figure 6, from the information of ZoneDefense status, the infected host has been blocked and ZoneDefense successfully provides the proactive mechanism to enable enterprises in guarding their critical internal network.

Figure 6: ZoneDefense status for blocking the infected host



Conclusion

ZoneDefense provides enterprises with a ***'New Proactive Network Security'*** that integrates network security appliance to automatically detect the network traffic. If the packet flow of a user computer triggers the conditions for ZoneDefense, a ZoneDefense command will immediately and automatically be sent to the specified network switch to block the network connection of the user computer instantaneously. For enterprises, this means ZoneDefense can greatly reduce the damages and losses caused by attacks from viruses and hackers, as well as effectively enhance network performance. For network administrators, this solution provides easy and time-saving approach to locating infected computers. Once the

infected computers are located, there is no need to manually issue system commands on network devices. D-Link's ZoneDefense enables effective enterprises defense of internal network.

Appendix

D-Link Managed Switches Supported by ZoneDefense

DFL-800/1600/2500 firmware v2.04.00 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 R3.x (firmware: R3.06-B20 only)
- D-Link DES-3526 R4.x (firmware: R4.01-B19 or later)
- D-Link DES-3550 R3.x (firmware: R3.05-B38 only)
- D-Link DES-3550 R4.x (firmware: R4.01-B19 or later)
- D-Link DES-3800 series (firmware: R2.00-B13 or later)
- D-Link DGS-3324 SR/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)
- D-Link DHS-3618/3626 (firmware: R1.00-B03 or later)