[Background]

Anti-Virus triggered ZoneDefense is a feature for isolating virus infected hosts and servers on a local network. While the virus scanning firewall takes care of blocking inbound infected files from reaching the local network, ZoneDefense can be used for stopping viruses to spread from an already infected local host to other local hosts. When the virus scanning engine in the gateway has detected a virus, the gateway will upload blocking instructions to the local switches and instruct them to block all traffic from the infected host or server.

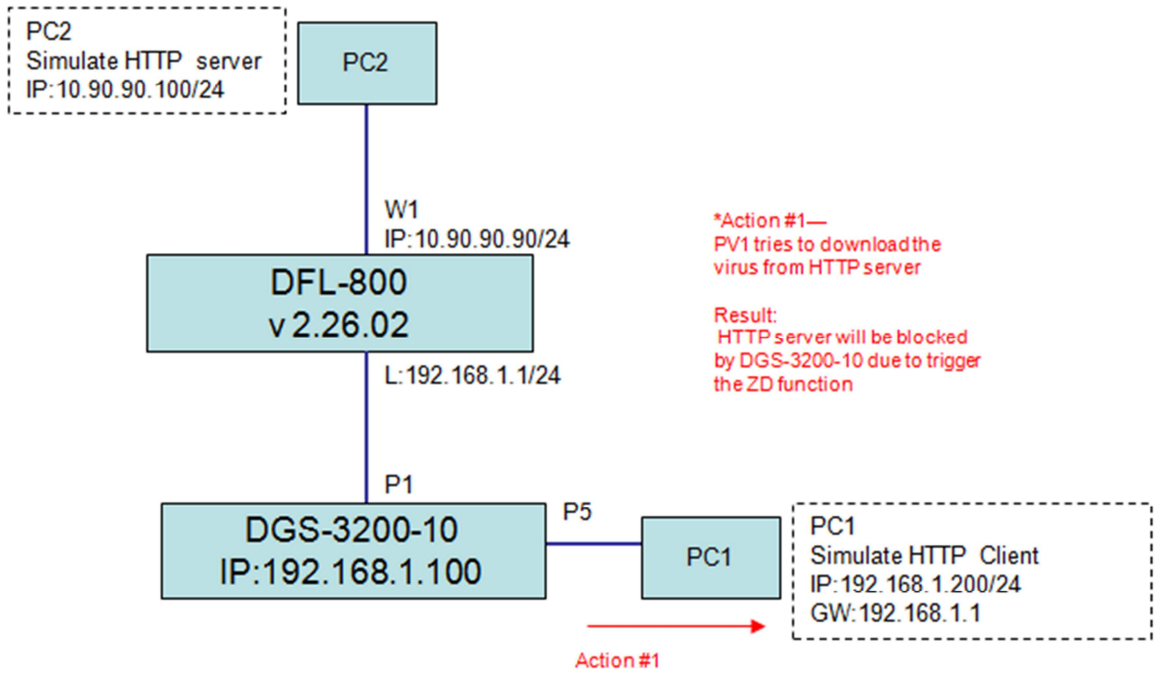
Since ZoneDefense blocking state in the switches is a limited resource, the administrator has the possibility to configure which hosts and servers that should be blocked at the switches when a virus has been detected.
For the Security Gateway to know which hosts and servers to block, the administrator has the possibility to specify a network range that should be affected by a ZoneDefense Block. All hosts and servers that are within this range will be blocked.

Note that. Below are the implied rules for HTTP antivrius feature:
1.Downloads (server to client) are scanned.
2.Uploads (client to server) are not scanned.

For FTP antivirus feature:

FTP transfers are scanned both during uploads and downloads.

[Topology]



[Configuration]

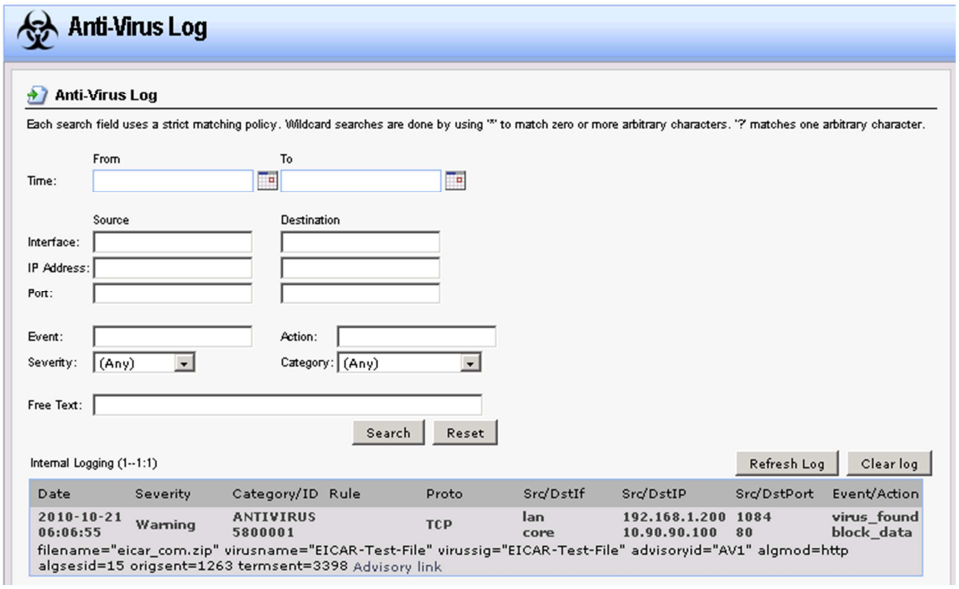
```
##############################################################################
##########
set Interface Ethernet wan1 DHCPEnabled=No
set Address IP4Address InterfaceAddresses/wan1_ip Address=10.90.90.90
set Address IP4Address InterfaceAddresses/wan1net Address=10.90.90.90/24

add ZoneDefenseSwitch dgs-3200-10 IP=192.168.1.100 SNMPCommunity=private Enabled=Yes
SwitchModel=DGS-32XX

add ALG ALG_HTTP http-av Antivirus=Protect ZDEnabled=Yes ZDNetwork=all-nets
add Service ServiceTCPUDP http-av-enable DestinationPorts=80 Type=TCP ALG=http-av
```

add IPRule Action=NAT SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet DestinationInterface=wan1 DestinationNetwork=all-nets Service=http-av-enable Index=1 LogEnabled=Yes Name=http-av-enable-with-zd
##
##########

[Test result]
1. Check the Firewall logs via WebUI. Go to "status"-->"anti-virus".



2. Check the ZoneDefense via WebUI. Go to "status"-->"ZoneDefense".

3. Check the ACL on the Switch:

##
####

DGS-3200-10:4#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:190
Total Used Rule Entries :10

Access Profile ID: 3 Type : IP
==========
==========
Owner : ACL
MASK Option :
Source IP MASK
255.255.255.255

Access ID : 1 Mode: Deny
Ports : 1-10

65.54.87.210
==========
==========

Access ID : 2 Mode: Deny
Ports : 1-10

63.80.138.26
==========
==========

Access ID : 3 Mode: Deny
Ports : 1-10

65.54.87.224
==========
==========

Access ID : 4 Mode: Deny
Ports : 1-10

63.80.4.64
==========
==========

Access ID : 5 Mode: Deny
Ports : 1-10

65.54.87.181
==========
==========

Access ID : 6 Mode: Deny
Ports : 1-10

63.80.138.9
==========
==========

Access ID : 7 Mode: Deny
Ports : 1-10

209.84.13.126

```
================================================================
====================

Access ID : 8           Mode: Deny
Ports     : 1-10
---------------
65.54.87.171
================================================================
====================

Access ID : 9           Mode: Deny
Ports     : 1-10
---------------
8.26.193.125
================================================================
====================

Access ID : 10          Mode: Deny
Ports     : 1-10
---------------
10.90.90.100
================================================================
====================
Unused Entries: 190


DGS-3200-10:4#
################################################################
####
```