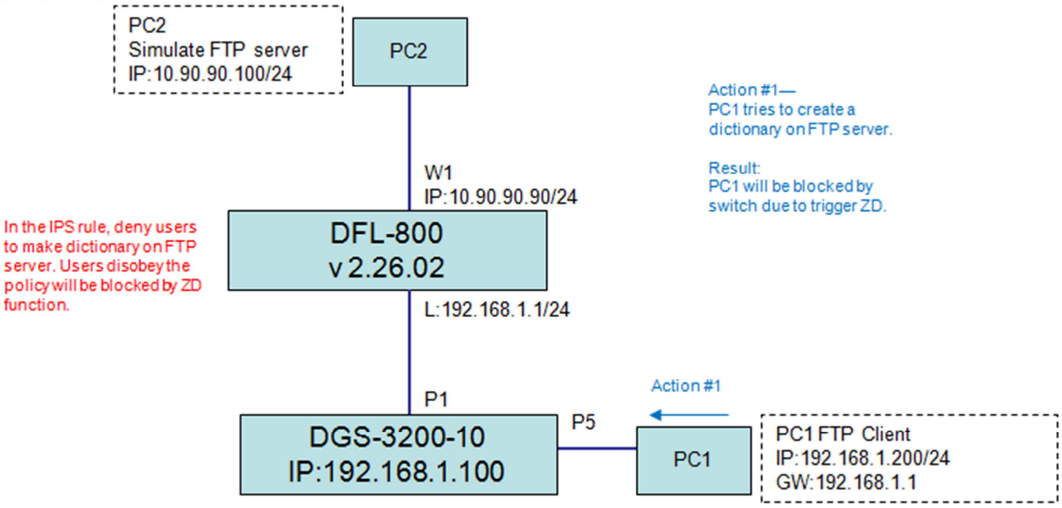
[Background]

The IPS is used for detecting the traffic from OSI layer 5~ layer 7, administrators are able to prevent the intrusion from internet or intranet by setting up the IDP rules.
IPS with ZoneDefense feature is able to block some internal or internet intended users to breach the service servers.
The current example is trying to block the users who are intended to make the dictionary on the FTP server.

[Topology]



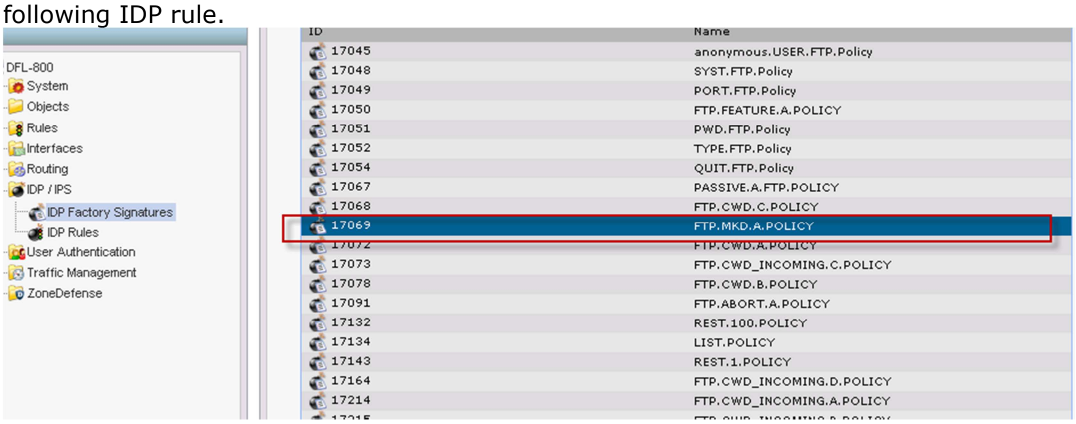
In the IPS rule, deny users to make dictionary on FTP server. Users disobey the policy will be blocked by ZD function.

Action #1— PC1 tries to create a dictionary on FTP server.

Result: PC1 will be blocked by switch due to trigger ZD.

[Configuraion]

STEP1. Find the signature we want to apply via WebUI and then copy the string for creating the following IDP rule.



ID	Name
17045	anonymous.USER.FTP.Policy
17048	SYST.FTP.Policy
17049	PORT.FTP.Policy
17050	FTP.FEATURE.A.POLICY
17051	PWD.FTP.Policy
17052	TYPE.FTP.Policy
17054	QUIT.FTP.Policy
17067	PASSIVE.A.FTP.POLICY
17068	FTP.CWD.C.POLICY
17069	FTP.MKD.A.POLICY
17072	FTP.CWD.A.POLICY
17073	FTP.CWD_INCOMING.C.POLICY
17078	FTP.CWD.B.POLICY
17091	FTP.ABORT.A.POLICY
17132	REST.100.POLICY
17134	LIST.POLICY
17143	REST.1.POLICY
17164	FTP.CWD_INCOMING.D.POLICY
17214	FTP.CWD_INCOMING.A.POLICY

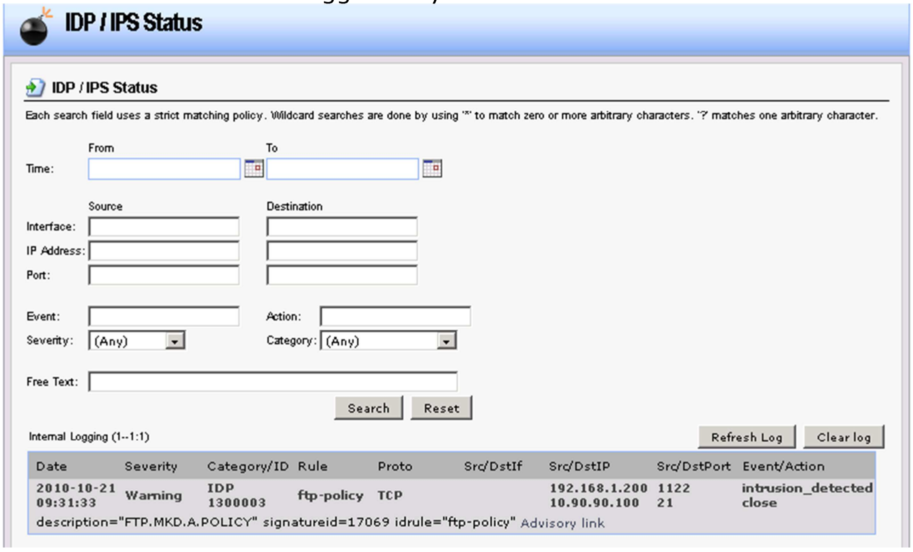
STEP2. Create rules via CLI.

```
###########################################################
set Interface Ethernet wan1 DHCPEnabled=No
set Address IP4Address InterfaceAddresses/wan1_ip Address=10.90.90.90
set Address IP4Address InterfaceAddresses/wan1net Address=10.90.90.0/24

add IDPRule SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet
DestinationInterface=wan1 DestinationNetwork=all-nets Service=ftp-passthrough Name=ftp-policy

cc IDPRule 1(ftp-policy)
add IDPRuleAction Action=Protect Signatures=FTP.MKD.A.POLICY LogEnabled=Yes
ZoneDefense=Yes BlackList=No
// The string FTP.MKD.A.POLICY was copied from STEP1.
cc

add ZoneDefenseSwitch dgs-3200-10 IP=192.168.1.100 SNMPCommunity=private Enabled=Yes
```

SwitchModel=DGS-32XX
##

[Result]

1. Check if the PC1 was triggered by IPS rule via WebUI. Go to Status-->IDP/IPS Status.



IDP / IPS Status

IDP / IPS Status

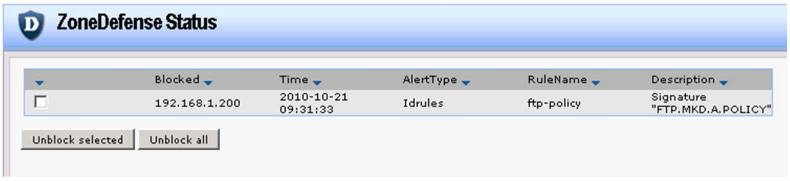
Each search field uses a strict matching policy. Wildcard searches are done by using "*" to match zero or more arbitrary characters. '?' matches one arbitrary character.

Internal Logging (1--1:1)

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2010-10-21 09:31:33	Warning	IDP 1300003	ftp-policy	TCP		192.168.1.200 10.90.90.100	1122 21	intrusion_detected close

description="FTP.MKD.A.POLICY" signatureid=17069 idrule="ftp-policy" Advisory link

2.Check if the ZoneDefense was triggered via WebUI. Go to "Status"-->"ZoneDefense"



ZoneDefense Status

	Blocked	Time	AlertType	RuleName	Description
□	192.168.1.200	2010-10-21 09:31:33	Idrules	ftp-policy	Signature "FTP.MKD.A.POLICY"

3.Check if the ACL was built on Switch.

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

Access Profile Table

Total Unused Rule Entries:199
Total Used Rule Entries  :1


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
---------------
192.168.1.200
==========================================================
==================
Unused Entries: 199
```

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

4. Now the PC1 (192.168.1.200) shall not be able to access anywhere.