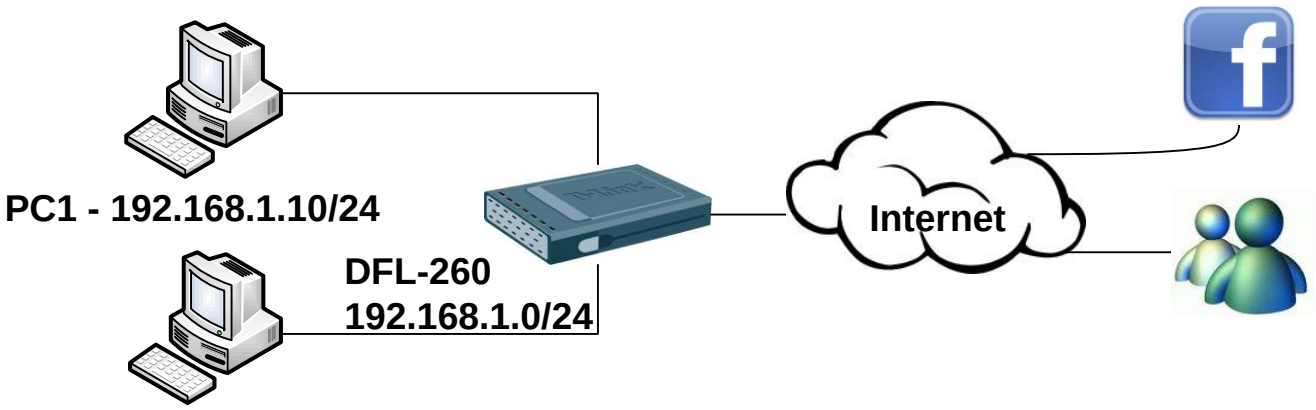
How to set up IDP to block MSN messenger and use WCF to block Facebook

[Issue]

PC1 can access Facebook and use MSN.

PC2 can't access Facebook and use MSN.

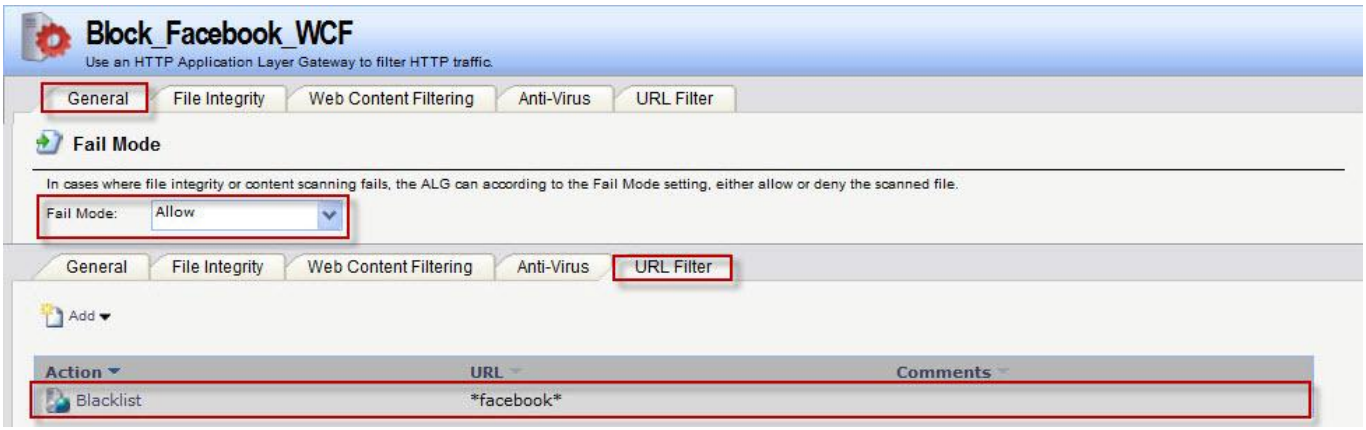
[Topology]



[Setup DFL-260]

1. Objects > address Book > InterfaceAddresses

2. Objects > ALG with AV/WCF

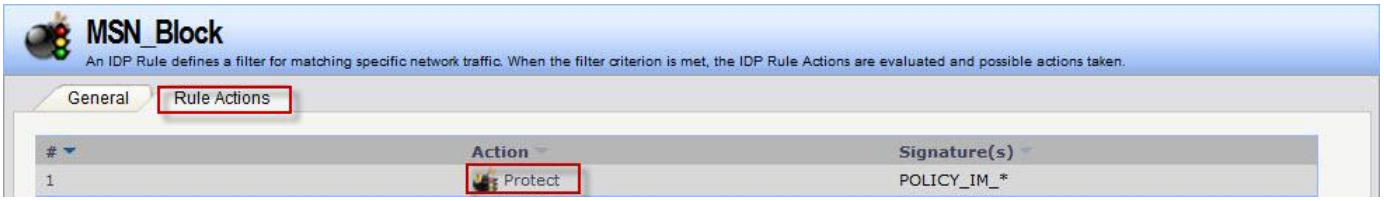


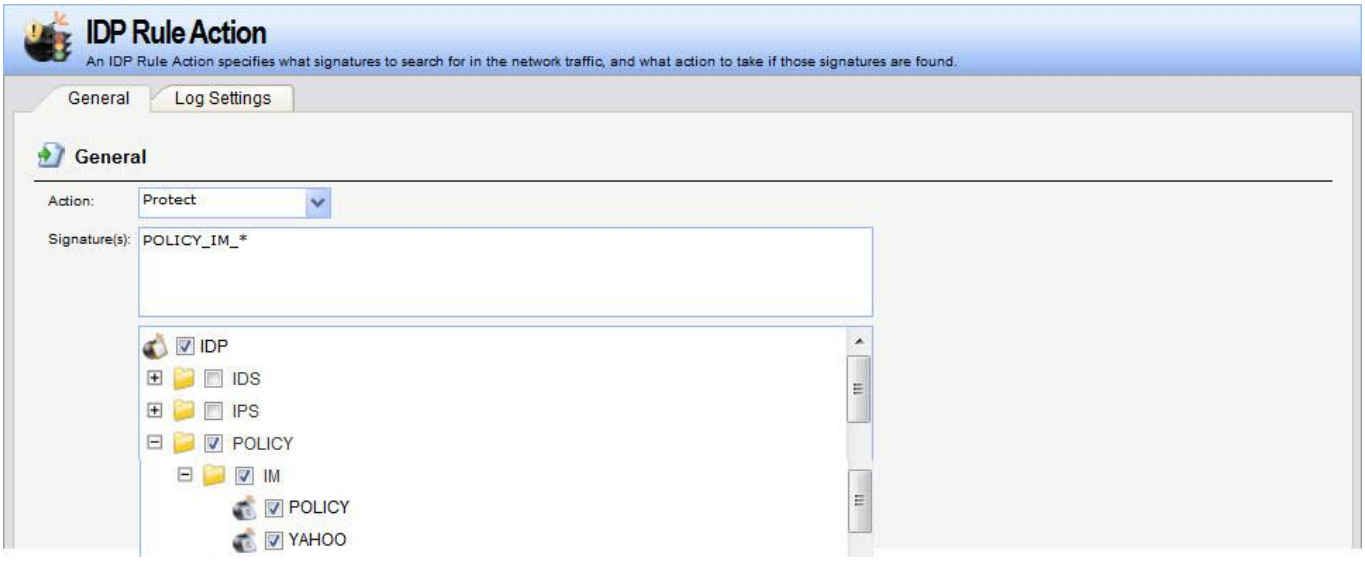
3. Objects > Services

4. IDP / IPS > IDP Rules

   Create an IDP Rules to block PC2 use MSN messenger.

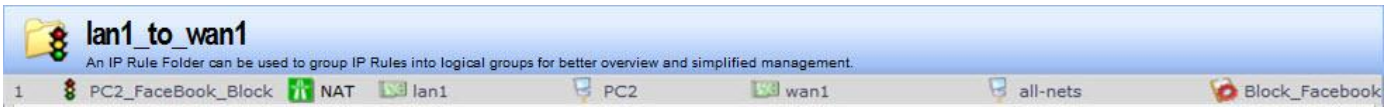
   When you finish the rule then click it (ex: MSN_Block). In Rule Actions page create a new IDP Rule action.





5. Rules > IP Rules

   We only need to create trigger rule for detection PC2 traffic.



[Test]

1. PC2 trying login MSN messenger will see “Error code 80072745 on sign in”.
2. PC2 access Facebook will see this block page.

3. PC1 can access Facebook and login MSN messenger.

[Firewall Log]

1. When PC2 login MSN messenger can see this log in firewall.

2011-08-12 18:35:48	Warning	IDP 1300003	MSN_Block	TCP	192.168.10.20 64.4.9.190	56314 1863	intrusion_detected close	
description="Version.Request.MSN.Messenger8.Policy" signatureid=55908 idrule="MSN_Block"								

2. When PC2 access Facebook can see this log in firewall.

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2011-08-12 18:38:34	Info	CONN 600005	PC2_FaceBook_Block	TCP	lan1 core	192.168.10.20 69.171.228.39	56337 80	conn_close_natsat close
conn=close connnewsrcip=192.168.11.193 connnewsrcport=35693 connnewdestip=69.171.228.39 connnewdestport=80 origsent=867 termsent=1672 conntime=1								
2011-08-12 18:38:34	Info	ALG 200002						alg_session_closed
algmod=http algsesid=193								
2011-08-12 18:38:34	Notice	ALG 200126		TCP	lan1 core	192.168.10.20 69.171.228.39	56337 80	request_url block
categories="blacklist" audit=off override=no origsent=747 termsent=84 url="www.facebook.com/" algname=Block_Facebook_WCF algmod=http algsesid=193								
2011-08-12 18:38:34	Info	ALG 200001		TCP	lan1 core	192.168.10.20 69.171.228.39	56338 80	alg_session_open
algmod=http algsesid=194 origsent=92 termsent=44								
2011-08-12 18:38:34	Info	CONN 600004	PC2_FaceBook_Block	TCP	lan1 wan1	192.168.10.20 69.171.228.39	56338 80	conn_open_natsat
conn=open connnewsrcip=192.168.11.193 connnewsrcport=36063 connnewdestip=69.171.228.39 connnewdestport=80								
2011-08-12 18:38:34	Info	ALG 200001		TCP	lan1 core	192.168.10.20 69.171.228.39	56337 80	alg_session_open
algmod=http algsesid=193 origsent=92 termsent=44								
2011-08-12 18:38:34	Info	CONN 600004	PC2_FaceBook_Block	TCP	lan1 wan1	192.168.10.20 69.171.228.39	56337 80	conn_open_natsat
conn=open connnewsrcip=192.168.11.193 connnewsrcport=35693 connnewdestip=69.171.228.39 connnewdestport=80								

END