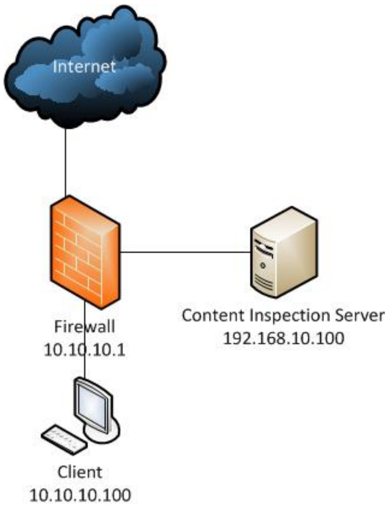
USING NETLINKS FOR CONTENT INSPECTION

MATT MCKINLEY

1. Scenario

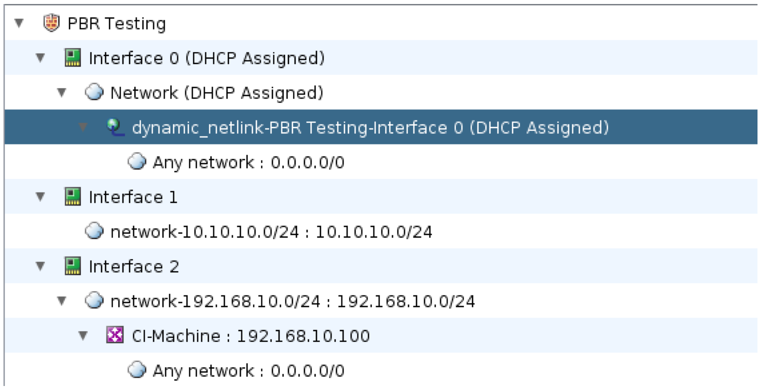
In the McAfee NGFW, sending packets to an external content inspection sever is possible through the use of the built-in CIS redirection service. This, however, only supports the redirection of HTTP. For other services, such as HTTPS, another method must be used. The following details the use of netlinks as a way of sending essentially anything for external inspection. In the use case requested by the customer, the original source IP of the connection was to be preserved.



2. Configuration

The following are the steps to perform in configuring this solution. There are other ways to configure it, but this is the simplest incarnation:

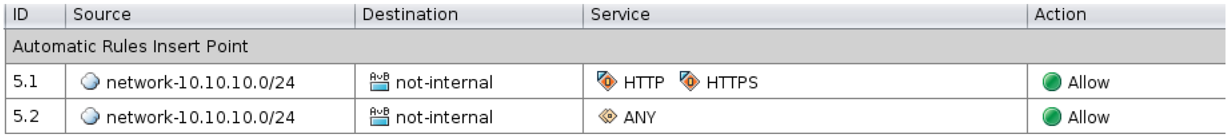
2.1. **Configure the Routing.** Configure the routing. Note that the Content Inspection machine is configured as a router and set as the firewall default route. The actual route that all other traffic will use is configured as the netlink.



- PBR Testing
  - Interface 0 (DHCP Assigned)
    - Network (DHCP Assigned)
      - dynamic_netlink-PBR Testing-Interface 0 (DHCP Assigned)
        - Any network : 0.0.0.0/0
  - Interface 1
    - network-10.10.10.0/24 : 10.10.10.0/24
  - Interface 2
    - network-192.168.10.0/24 : 192.168.10.0/24
      - CI-Machine : 192.168.10.100
        - Any network : 0.0.0.0/0

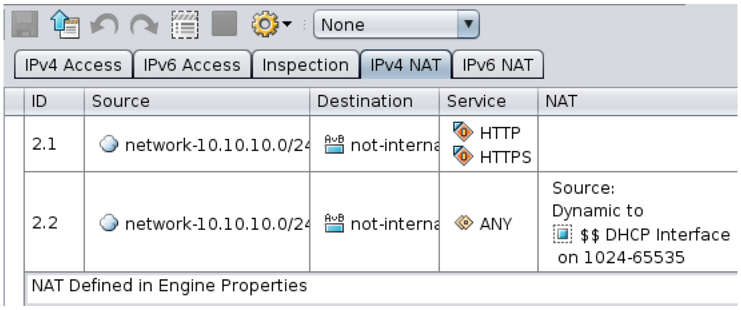
Date: June 9, 2015.

2.2. Configure the Policy. Below are the access rules. Note that the HTTP/HTTPS rule is not actually needed, but is still there for rule counter purposes.



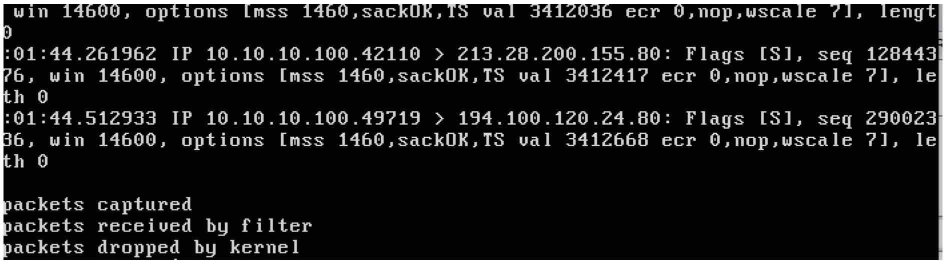
ID	Source	Destination	Service	Action
Automatic Rules Insert Point				
5.1	network-10.10.10.0/24	not-internal	HTTP HTTPS	● Allow
5.2	network-10.10.10.0/24	not-internal	ANY	● Allow

2.3. Configure NAT. Now, configure the NAT rules. Note that the rules at the top are ”no NAT” for HTTP and HTTPS. By default, as per the routing, services that are not NATed to anything take the default route of the firewall, which is set as the Content Inspection Server. In this figure, you can see that all other services are being NATed to the IP address of the external interface, which uses a netlink.



ID	Source	Destination	Service	NAT
2.1	network-10.10.10.0/24	not-interna	HTTP HTTPS	
2.2	network-10.10.10.0/24	not-interna	ANY	Source: Dynamic to $$ DHCP Interface on 1024-65535
NAT Defined in Engine Properties				

2.4. Testing the Configuration. When packets are not NATed, such as in the case here, the packets use the default route of the firewall, which is set to the address of the content inspection server. When packets arrive at that address, they have not been NATed, and the original source address is preserved. The test client machine is 10.10.10.100 and the tcpdump was taken from the CIS. Note that the source address is preserved. Here is a screen capture of a tcpdump running on the test machine, 192.168.10.100:



```
 win 14600, options [mss 1460,sackOK,TS val 3412036 ecr 0,nop,wscale 7], lengt
0
:01:44.261962 IP 10.10.10.100.42110 > 213.28.200.155.80: Flags [S], seq 128443
76, win 14600, options [mss 1460,sackOK,TS val 3412417 ecr 0,nop,wscale 7], le
th 0
:01:44.512933 IP 10.10.10.100.49719 > 194.100.120.24.80: Flags [S], seq 290023
36, win 14600, options [mss 1460,sackOK,TS val 3412668 ecr 0,nop,wscale 7], le
th 0

packets captured
packets received by filter
packets dropped by kernel
```