A lot of people post on NetPro that they want to permit or restrict by domain names on a PIX/ASA firewall. You can't just type in deny packetpros.com, but using the MPF you can block them. Here's how we block two sites; packetpros.com and nortel.com.

```
regex Block_Packetpros ".packetpros.com"
regex Block_Nortel ".nortel.com"

access-list inside_mpc extended permit tcp any any eq www
access-list inside_mpc extended permit tcp any any eq https
!
class-map type regex match-any Block_Domains
 match regex Block_Packetpros
 match regex Block_Nortel
class-map type inspect http match-all Block_These_Domains
 match request header host regex class Block_Domains
class-map inspection_default
 match default-inspection-traffic
class-map httptraffic
 match access-list inside_mpc
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
 policy-map type inspect http http_inspection_policy
 parameters
protocol-violation action drop-connection
 class Block_These_Domains
  drop-connection
 policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
```

```
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map inside-policy
 class httptraffic
  inspect http http_inspection_policy
!
service-policy global_policy global
service-policy inside-policy interface inside
```

Let’s verify it’s working properly.

I tried to go to www.packetpros.com. It failed and here is what is in the log.

```
%ASA-7-609001: Built local-host outside:75.50.95.75
%ASA-6-302013: Built outbound TCP connection 2399 for outside:75.50.95.75/80 (75.50.95.75/80) to inside:192.168.50.5/4316 (172.30.30.248/50162)
%ASA-5-304001: 192.168.50.5 Accessed URL 75.50.95.75:/
ASA-4-507003: tcp flow from inside:192.168.50.5/4316 to outside:75.50.95.75/80 terminated by inspection engine, reason – disconnected, dropped packet.
ASA-6-302014: Teardown TCP connection 2399 for outside:75.50.95.75/80 to inside:192.168.50.5/4316 duration 0:00:00 bytes 0 Flow closed by inspection
%ASA-7-609002: Teardown local-host outside:75.50.95.75 duration 0:00:00
%ASA-7-609001: Built local-host outside:75.50.95.75
%ASA-6-106015: Deny TCP (no connection) from 192.168.50.5/4316 to 75.50.95.75/80 flags PSH ACK on interface inside
%ASA-7-609002: Teardown local-host outside:75.50.95.75 duration 0:00:00
```

As you can see the inspection engine dropped the connection. Not too bad is it? If you need to add a new domain to block, just add a regular expression for it and add it to the class map.

```
regex Block_Avaya ".avaya.com"

class-map type regex match-any Block_Domains
 match regex Block_Avaya
```