Sophos PCI DSS v2 Firewall Rules

Note: if the existing firewall configuration is fairly simple, it is recommended that you start fresh, using the new Virtual Terminal Default – PCI 2.0 policies and configure that as necessary, following the Firewall_Config_New.docx guide instead.

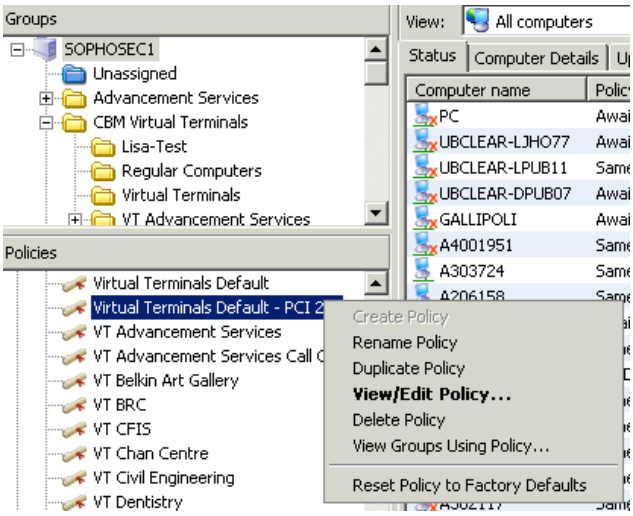
Block by default is *always* the required default rule for the firewall policies. Inbound/Outbound traffic is compared first to against LAN, Global Rules, or Applications rules before it is blocked by default.

Any changes that differ from the default settings shown here MUST be documented down. Please follow the suggested documentation format at the end of this document.

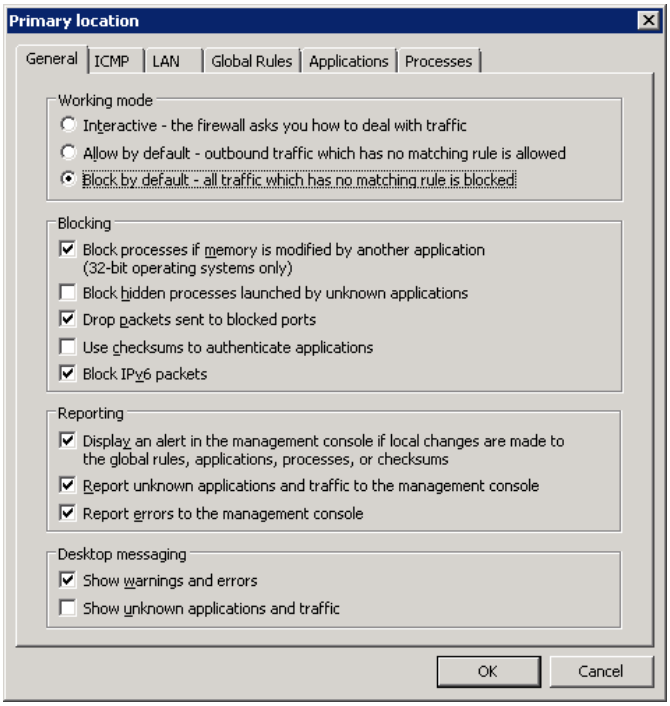
*Listing & explanation of allowed UBC Adminstrative IP space can be found here: http://www.it.ubc.ca/service_catalogue/internet_telephone/network_management/ubc_ip_addy_list.html

Recommended steps

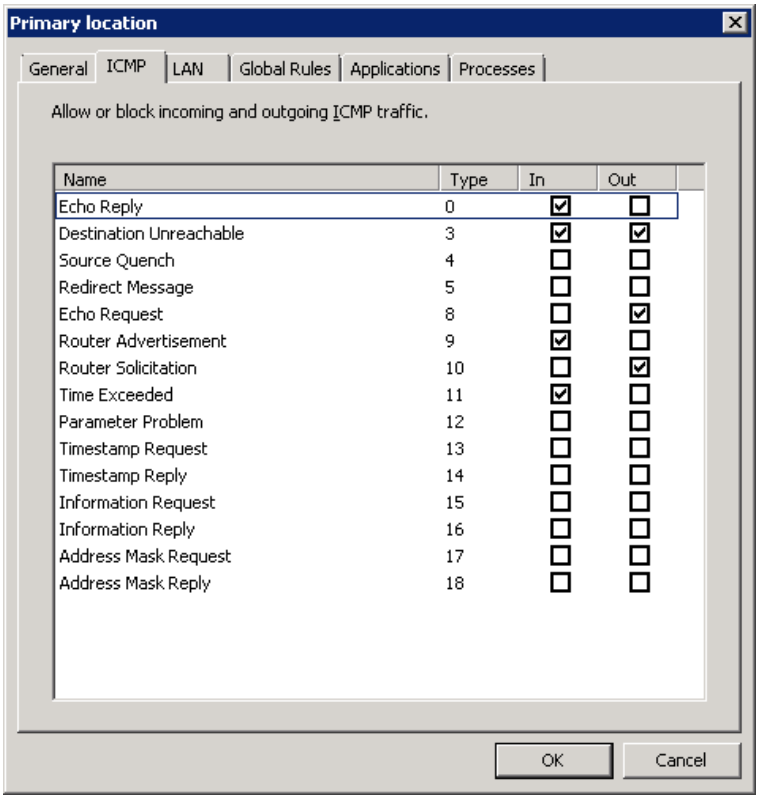
1) Open up the firewall policy that has been custom created for your group. (It should NOT be Virtual Terminal Default or Virtual Terminal Default – PCI 2.0, if it is, see the Firewall_Config_New.docx guide instead).



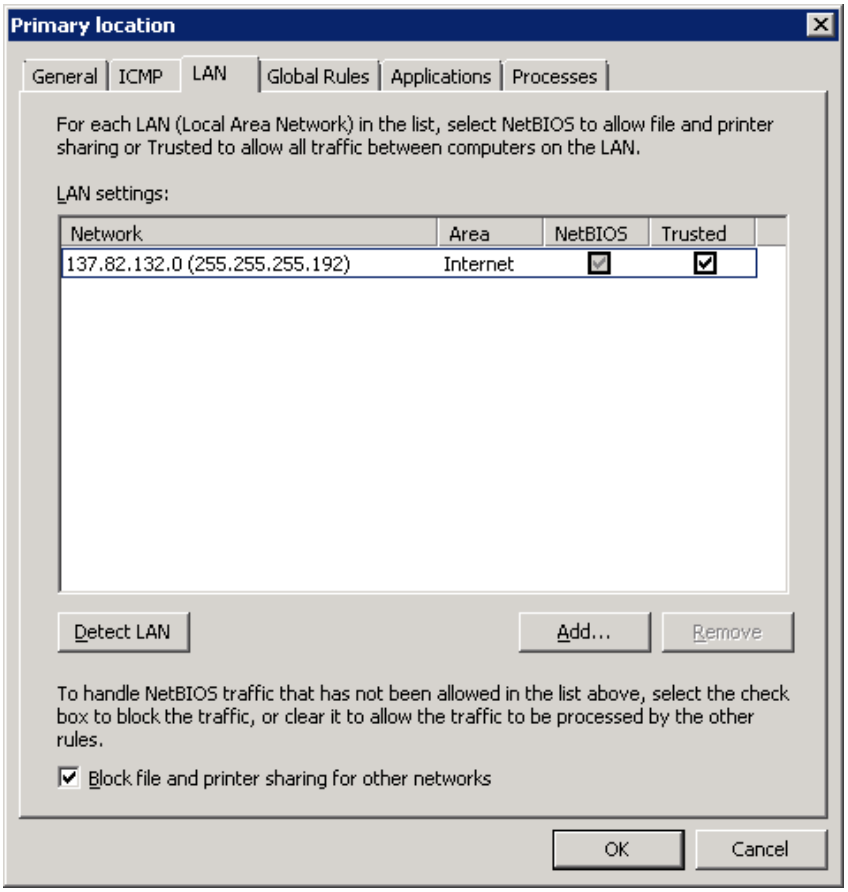
2) Ensure that this is the default General setting.



3) Ensure this is the default ICMP setting.

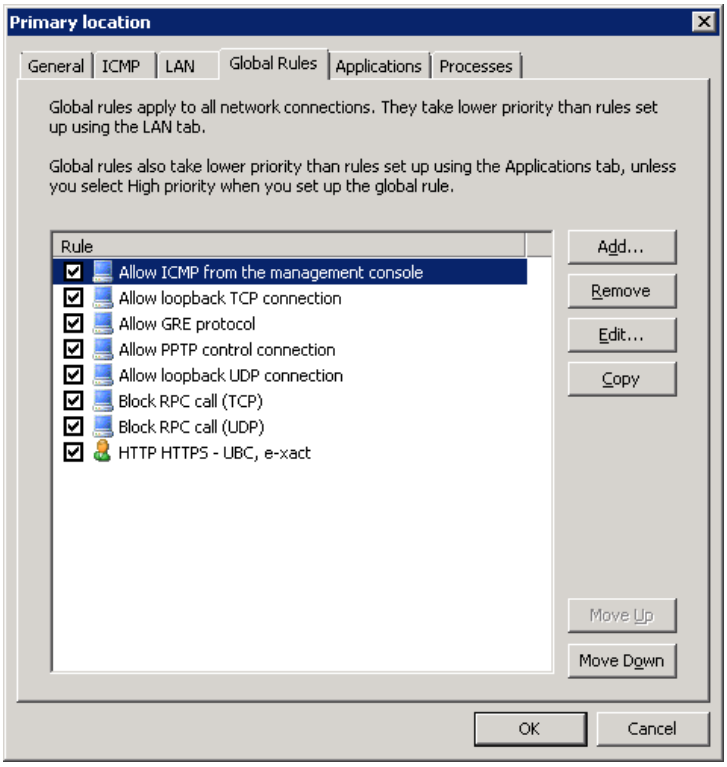


4) This is should be the default LAN rules:



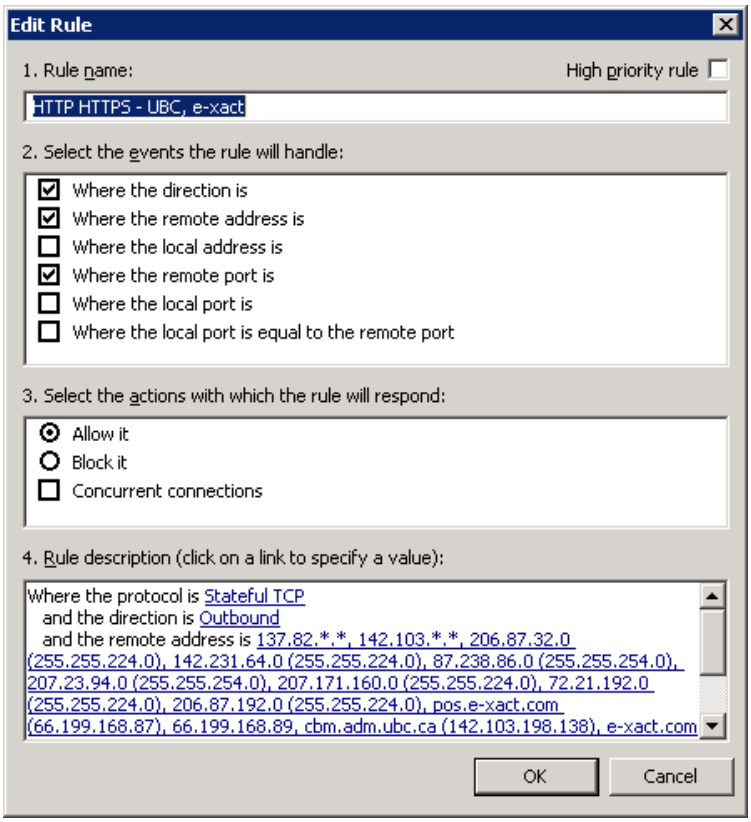
a. 137.82.132.0 subnet of the Sophos Enterprise Console sophosec1.it.ubc.ca.
b. Now re-examine each remaining entry:
    i. Moving forward, only NetBIOS required IP addresses should be placed here. **Trusted** should *not be turned on* as enabling it will allow all traffic between that IP address and the local computer.
    ii. Only allow departmental file servers if absolutely necessary. Note adding in a file server may result in the file server and other computers on the network being included/considered as part the Cardholder Data Environment.
    iii. Printers are NOT to be included here. If you have any printers added here, they will need to be removed. Printers should be handled by the printer policy (step 6 – Spoolsv.exe) under Application tab. It will allow printer usage as long as the printer has been installed via IP or DNS on the local computer. If you find this is not working then please let us know.
    iv. Document all difference between the default LAN rules and what is remaining.

5) This is now the default Virtual Terminal Global Rules:



Notice there is a new rule added – HTTP HTTPS – UBC , e-xact.

<u>You need to add this new rule to your Global Rules:</u>



a. this rule restricts traffic to UBC & e-Payment (e- xact). The allowed IP addresses are:

- UBC administrative IP address space (exclude wireless and ResNet)
- pos.e-xact.com
- e-xact.com
- cbm.adm.ubc.ca

137.82.*.*
142.103.*.*
142.231.64.0 (255.255.224.0) (/19)
206.87.32.0 (255.255.224.0) (/19)
206.87.192.0 (255.255.224.0) (/19)
207.23.94.0 (255.255.254.0) (/23)
pos.e-xact.com (66.199.168.87, 66.199.168.89)
e-xact.com (205.210.42.167)
cbm.adm.ubc.ca
72.21.192.0 - 72.21.223.255 255.255.224.0 (/19)
207.171.160.0 - 207.171.191.255 255.255.224.0 (/19)
87.238.86.0 - 87.238.87.255 255.255.254.0 (/23)

for stateful outbound traffic to HTTP (TCP 80) and HTTPS (TCP 443) ports.

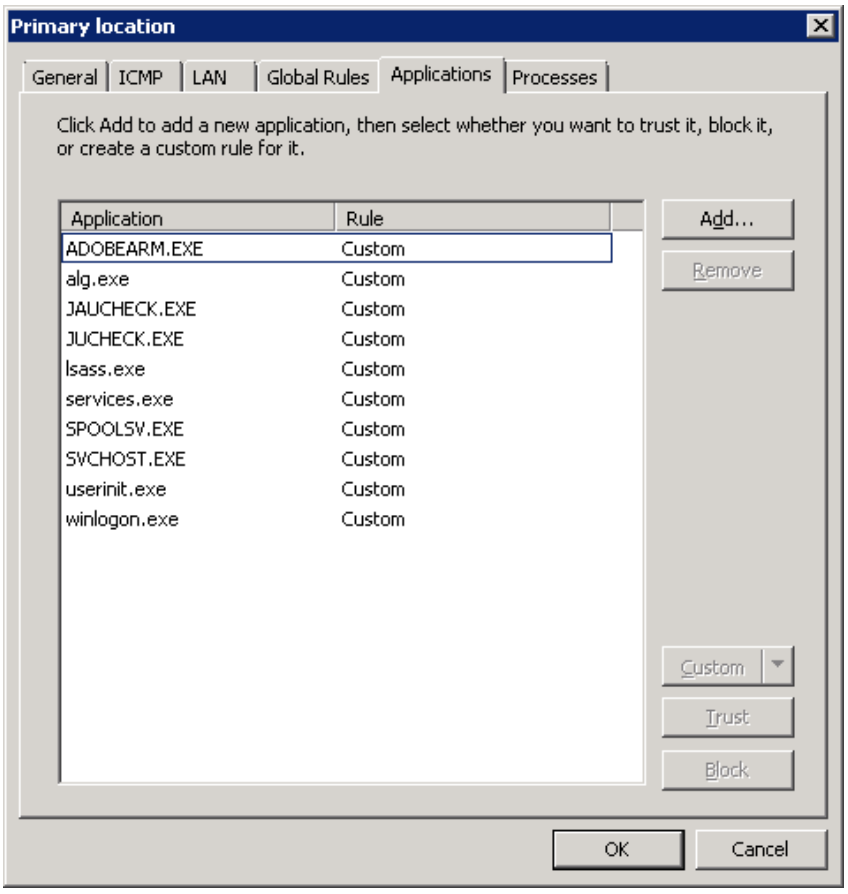
b. You are permitted to allow other websites if the merchant requires them. Create a new for the other websites.

Note: Google, Hotmail and Facebook are NOT permitted. The list of websites will be subject to review by UBC IT. Document the list and submit it back to UBC IT for review.

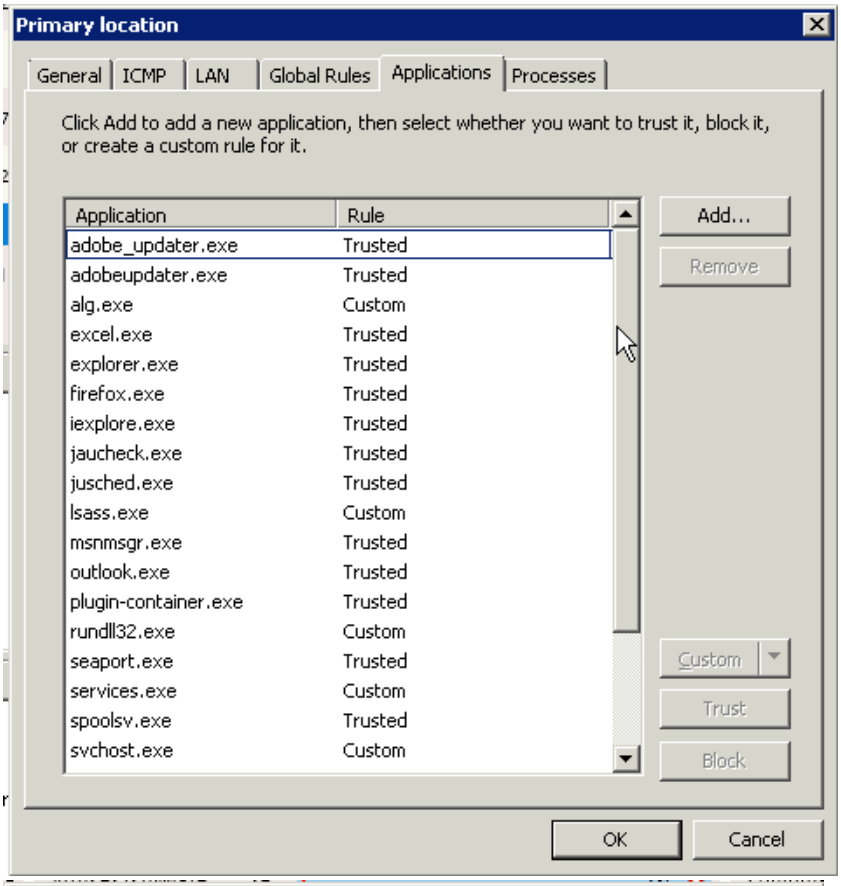
c. Any differences between the default Global Rules and your Global Rules will need to be documented.

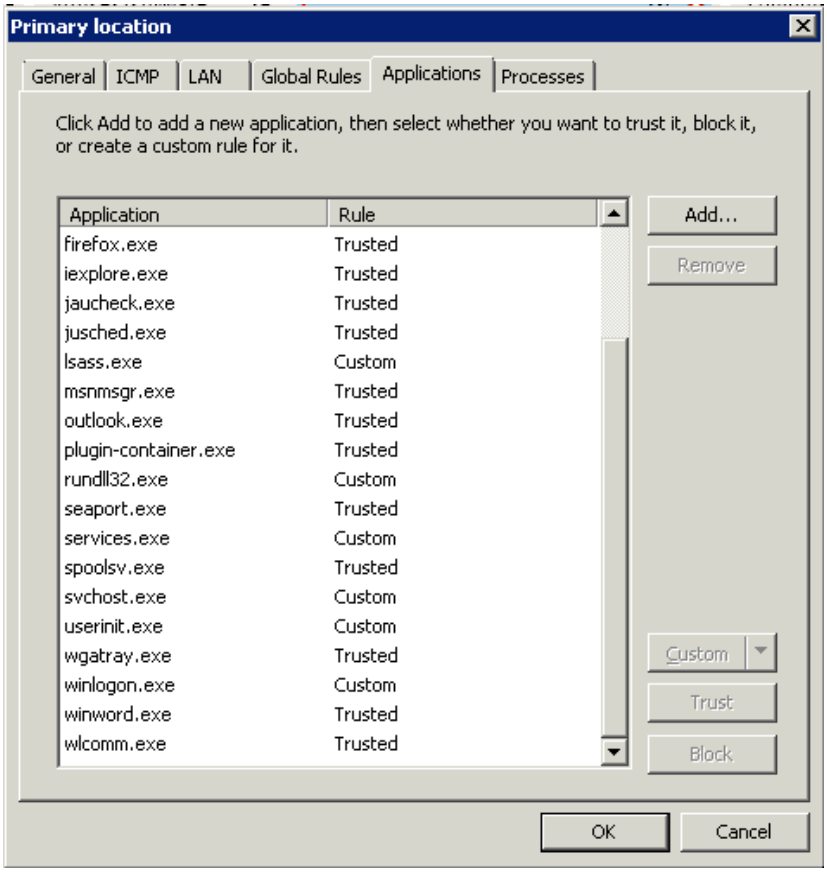
Remember: Any application on the local computer can access these IP address ranges and ports/protocols under yours and the UBC/e-xact global rules.

6) This is the new default Virtual Terminal Applications rules:

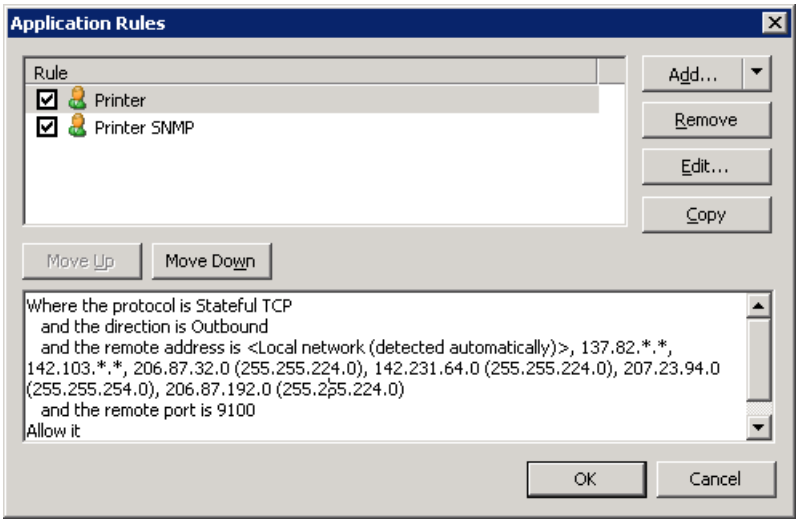


This was the old Virtual Terminal default:





a. The new default rules are now quite stripped down, to only allow Adobe, Java, miscellaneous Microsoft services (update, DNS, etc.) and printer traffic to pass through. **Note that that spoolsv.exe is no longer set to 'trusted'—instead a custom rule set has been created it. You need to add in the following modification for spoolsv.exe for printer traffic.** Note you need to install the printer via IP or DNS.



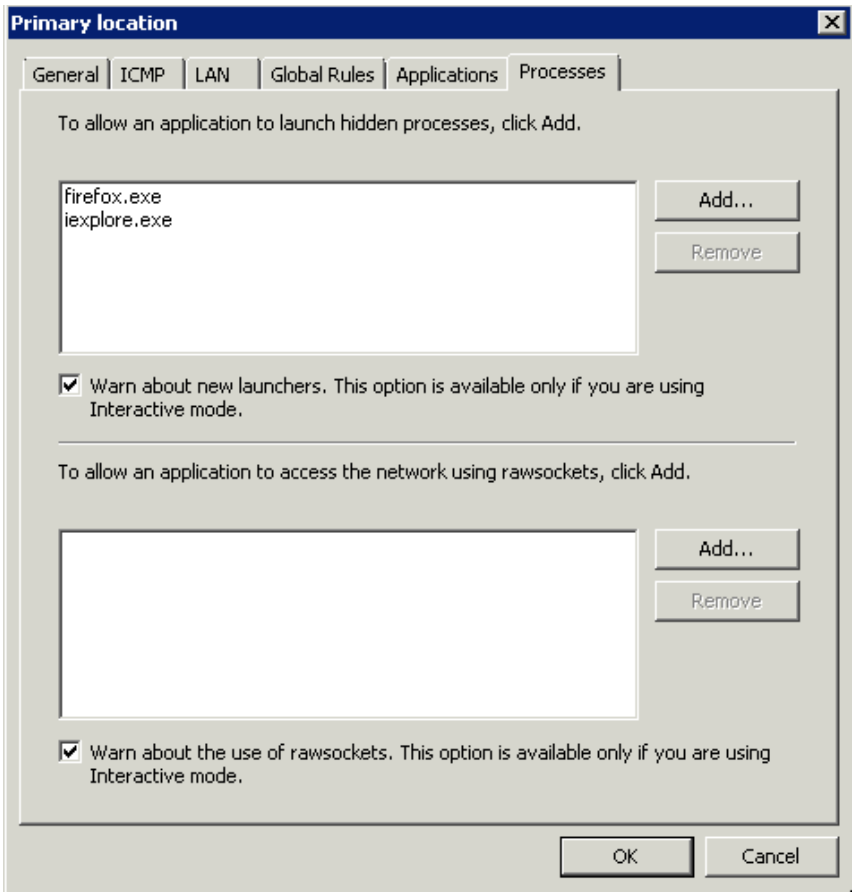
b. Remove as much unnecessary application rules from your existing rules as possible. **MSN Messenger and any browser application or instant messenger rules will need to be removed, eg firefox.exe, iexplorer.exe, etc. If you do not remove them, it will negate the Global rule of allowing only web traffic to approved websites.**

i. Best practice to remove the unnecessary application rule is to remove the application rule and then test the application to see if it still works.

c. Any rule that was not part of the new Virtual Terminal default will need to be documented.

d. We should not be using 'trusted'. Do custom rule sets whenever possible.

7) This should be the default Processes tab:



8) Configurations for optional applications for remote administration.

Remote administration to be white listed only to your department's IT administrative computer's IP addresses or at most, UBC administrative IP address space. Do not open up to the general Internet. Again document down this change.

Examples:

Teamviewer Service

Limit IP address range to required range for remote administration for your group. Create a new Global Rule for this.

E,g,

Where the protocol is Stateful TCP

and the direction is Inbound

and the remote address is 137.82.182.*

and the remote port is 443, 5938

Allow it

Remote Desktop RDP

Limit IP address range to required range for remote administration for your group. Create a new Global Rule for this.

e.g.

Where the protocol is Stateful TCP

and the direction is Inbound

and the remote address is 137.82.182.*

and the remote port is RDP 3389

Allow it

Documentation format:

File Servers	
Name	**IP Address**

Applications	**Note: HTTP 80 or HTTPS 443 to UBC IP Address Space already allowed**		
Name	**Client side executables (.exe files, etc.)**	**Server IP Addresses or Range**	**Ports**

External Non UBC Websites	
URL or IP Address range	**Ports (if not HTTP 80 or HTTPS 443)**