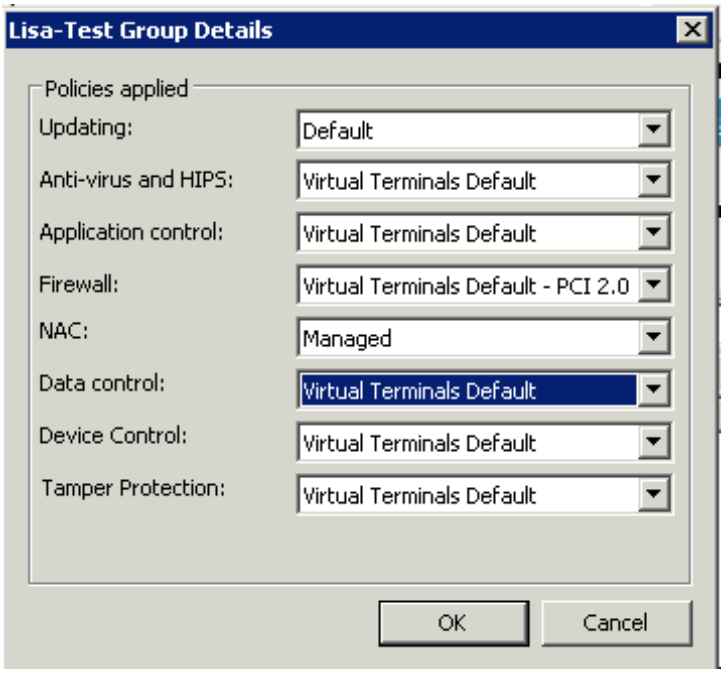
Sophos PCI DSS v2 Firewall Rules

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.

If you have an existing custom firewall setting and would like to edit that, instead of starting from the new default rules, please see **Firewall_Config_Existing.docx.**

Recommended steps

1) Ensure that the group policies are set the following (right click the group folder and select View/Edit Group Policy)



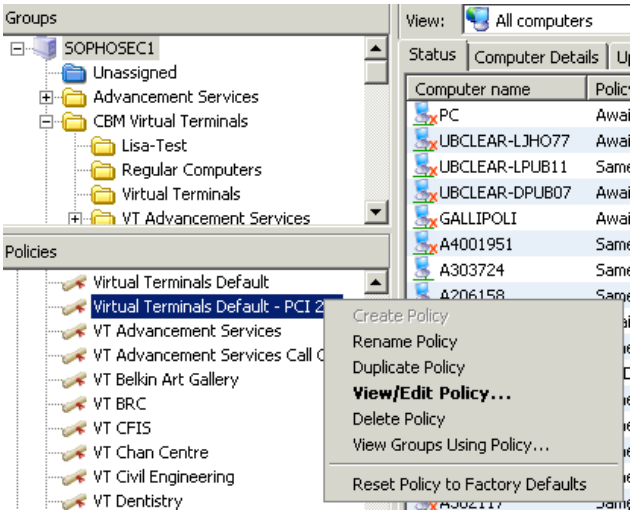
2) If the user needs access to a printer, ensure that the printer is installed via IP or DNS on the local computer and try a test page. Note: You should NOT have to have to modify the firewall rule to allow printer use. If you find this is the case, please let us know. The firewall policy allows SPOOLSV.exe to send outbound traffic via TCP 9100 and UDP 161 SNMP to local network and UBC administrative IP space for network printing.
3) This default policy will allow all application (including web browsers) access to UBC administrative IP address space (excluding wireless and ResNet) and e-Payment.
4) Ensure that the web browser does allow traffic through to www.ubc.ca and https://cbm.adm.ubc.ca/cbmadmin/function/administercbm

---- NOTE--- if you are configuring a stand-alone computer, you should be able to stop here. If not, (ie, file servers need to be added, other website access needs to be granted, etc.) then move on below to customize the new default Sophos Firewall configurations for your group.

If you are allowing RDP usage, you must limit the IP Range for remote administration. Please continue onwards to the next steps below.

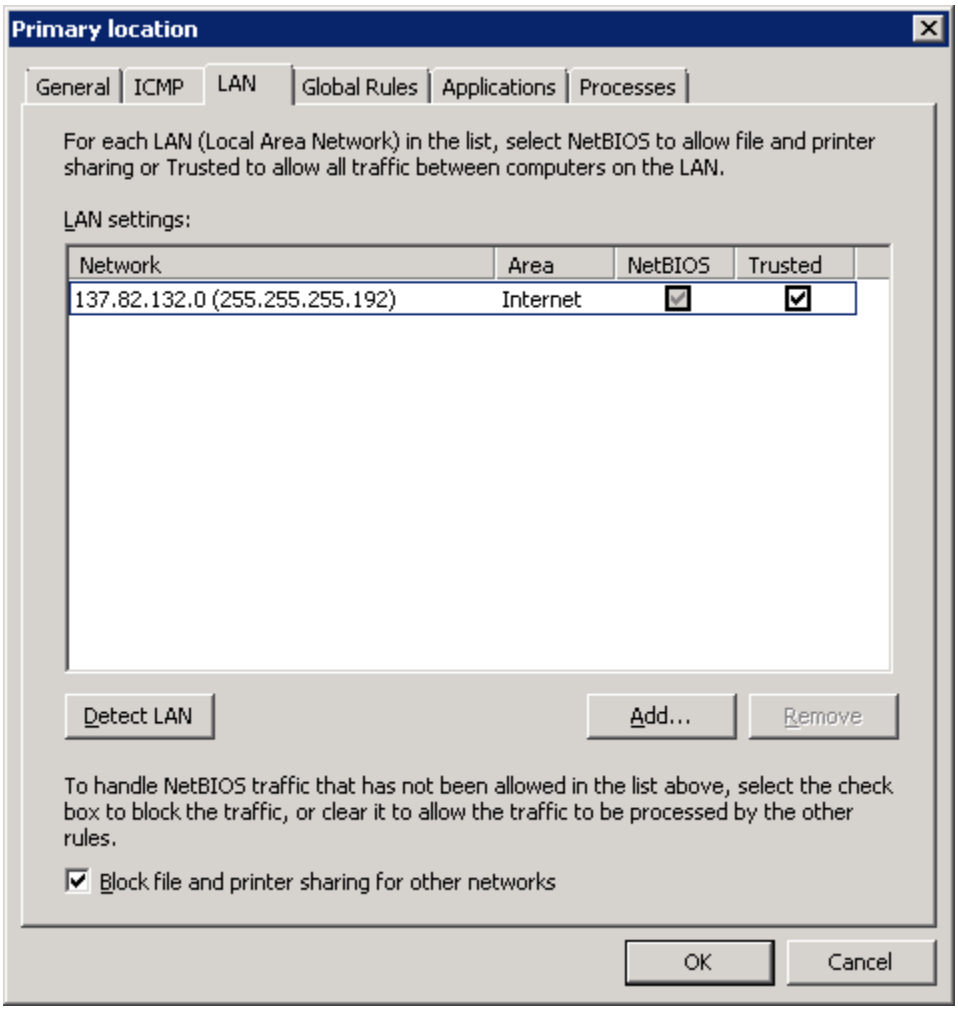
For every change you make, you need to DOCUMENT down the change with an explanation of what it is. Please use the example documentation format on the last page.

1) Make a copy of the "Virtual Terminals Default – PCI 2.0" firewall policies:



a. **Make sure you apply the policy you just created to your group!**

2) **<u>Adding in file servers:</u>**



Only NetBIOS required IP addresses should be placed here.

Trusted should *<u>not be turned on</u>* as enabling it will allow all traffic between that IP address and the local computer.

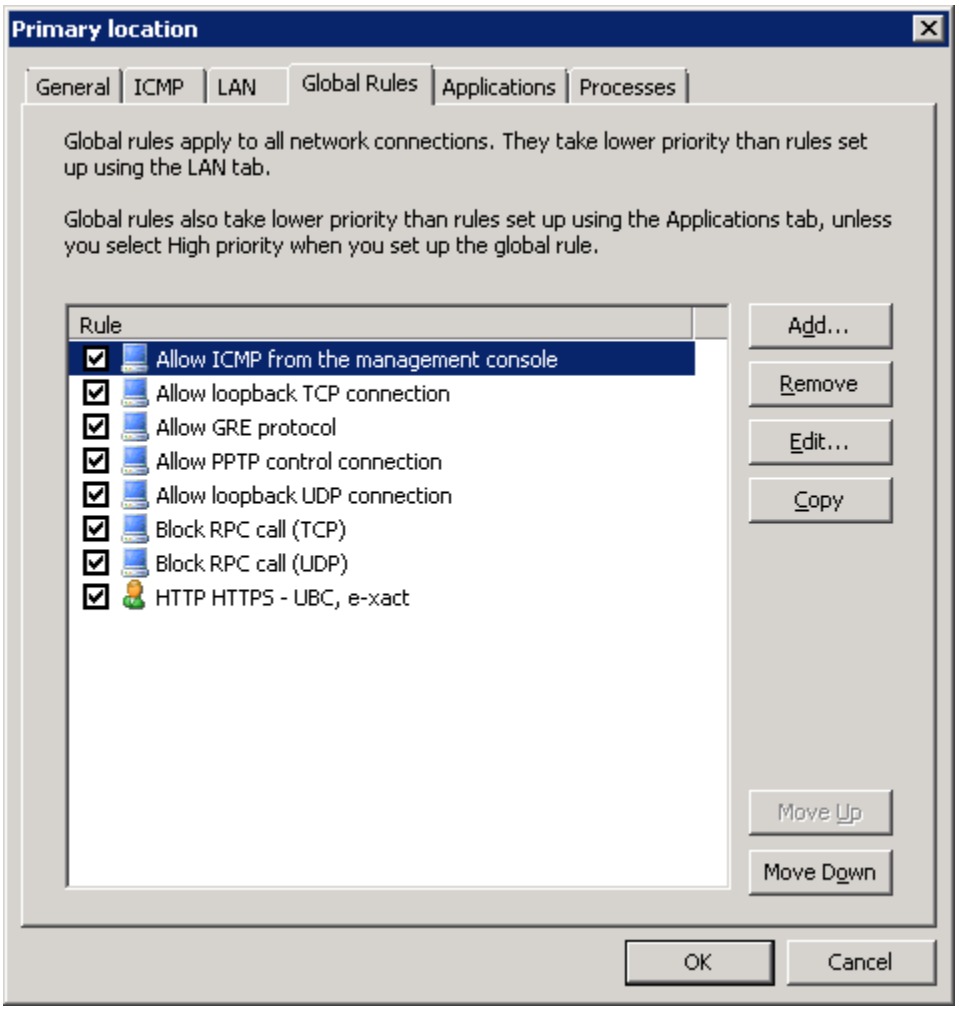
Current IP address is the subnet of the Sophos Enterprise Console sophosec1.it.ubc.ca.

Only allow departmental file servers if absolutely necessary.

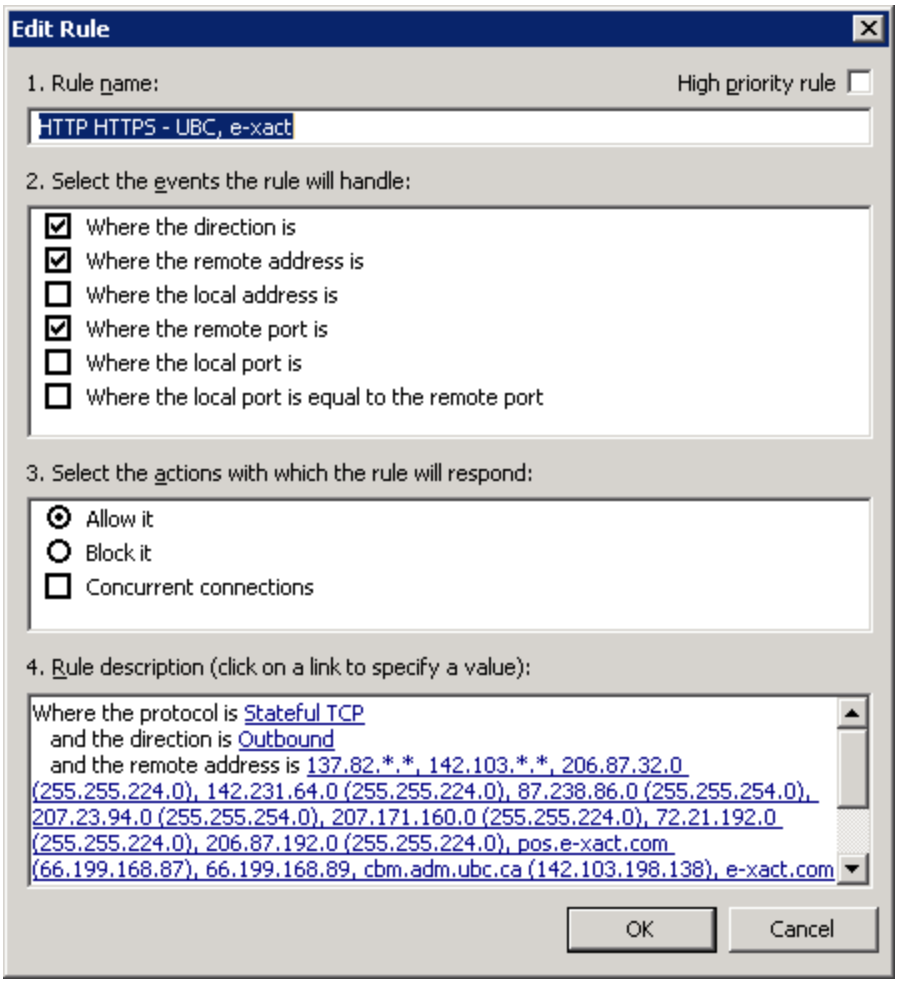
Printers are NOT to be included here. If you have any printers added here, they will need to be removed. The default setting should allow printer usage as long as the printer has been installed via IP or DNS on the local computer. If you find this is not the case, please let us know. The default Virtual Terminal PCI 2.0 firewall policy allows SPOOLSV.exe to send outbound traffic via TCP 9100 and UDP 161 SNMP to local network and UBC administrative IP space for network printing.

Note adding in the file server may result in the file server and other computers on the network being included/considered as part the Cardholder Data Environment.

3) Allowing access to websites other than UBC ones and e-Payment (e-xact.com):



Add in a new Global Rule under the Global Rules window.

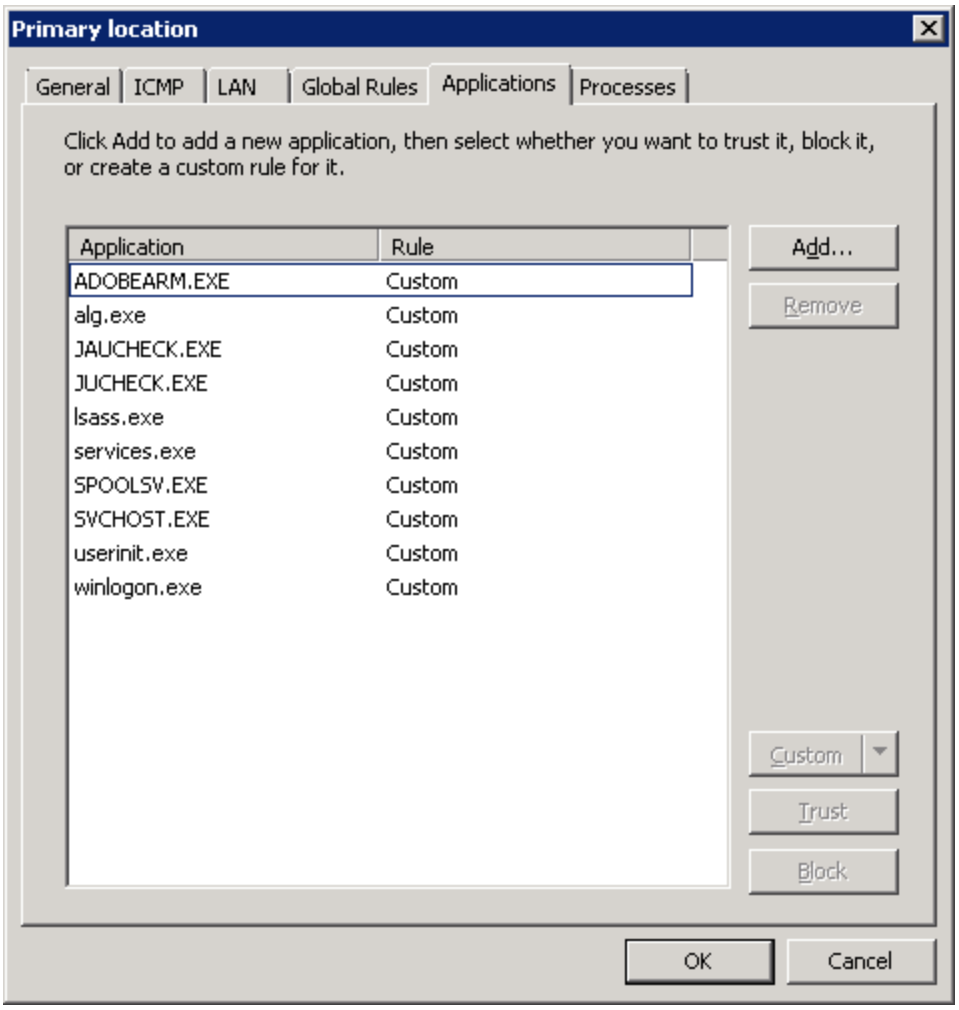


The above is the rule created for allowing UBC and e-xact (e-Payment) traffic only. Use this as an example of how a new rule for other websites should be created.

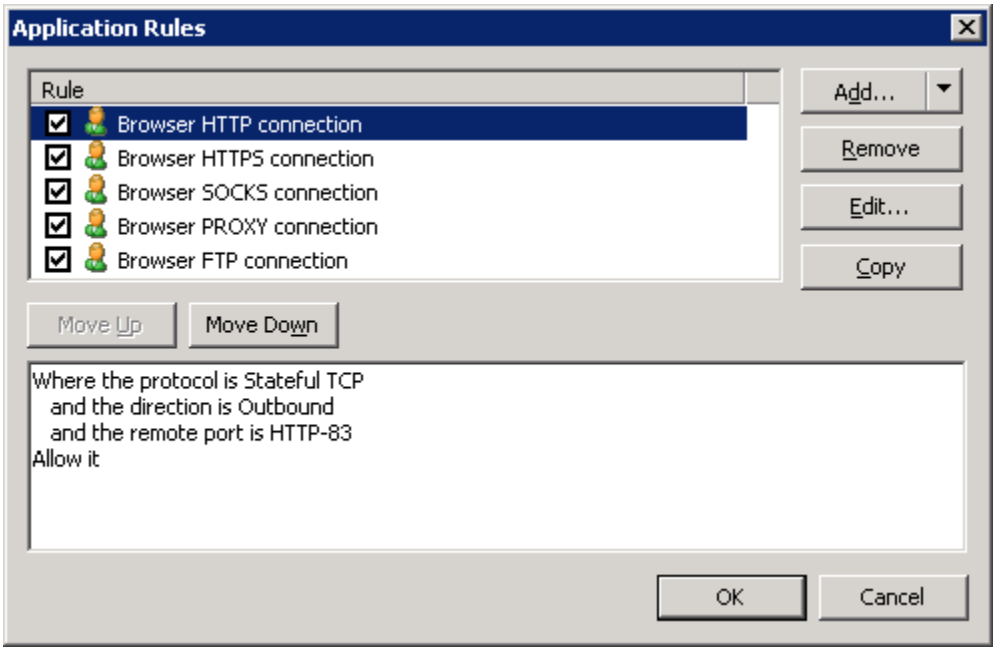
Note: Google, Hotmail and Facebook are NOT permitted. The list of websites will be subject to review by UBC IT. Document it down (last page of this file) and submit it back to UBC IT for review.

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.

4) Allowing applications to communicate to outside resources



Add in a new rule for the application that is blocked by the firewall here. By default we have allowed Adobe, and Oracle java updates to pass through the firewall. (Adobearm.exe, jaucheck.exe, jucheck,exe)



You need to configure it according to what the application requires. The above is an example of one that communicates over HTTP or HTTPS to numerous IP addresses (e.g. Akamai) for software patches and updates. 'Trusted' rules need to be avoided as much as possible.

5) 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.

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)**