**Configuration Management Record**

| **Date** | **Component**  (firewall / IDS/IPS, etc) | **Action**  (Add, remove, change) | **Modifier**  (administrator, IT) | **Name** | **Old Setting** | **New Setting** | **Reason** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 21/6/2023 | Firewall | Change | Project Manager Giuseppe Raciti  0438 221 782 | pfSense - Windows | **Automatic Update**: Disabled | Automatic Update: Set to update every 24 hours | The firewall was not updating automatically. |
| 26/06/2023 | IDS/IPS | Change | Project Manager Giuseppe Raciti  0438 221 782 | Snort - Linux | **Home Network address** : Any | 192.168.1.0/24 | The network address was not set to monitor the traffic on the server NIC |
| 28/06/2023 | IDS/IPS | Change | Cloud Engineer  Mark Byrne  0457 532 233 | Snort - Windows | **Home network address**: Any | 192.168.0.0/24 | The network address was not set to monitor the traffic on the server NIC |
| 28/06/2023 | IDS/IPS | Change | Cloud Engineer  Mark Byrne  0457 532 233 | Snort - Windows | All - Snort.conf file | External network address:  !$HOME\_NET  Set RULE\_PATH to C:\snort\rules  Set PREPROC\_RULE\_PATH to c:\snort\preproc\_rules  Set WHITE\_LIST\_PATH to c:\snort\rules  Set BLACK\_LIST\_PATH to c:\snort\rules | These are the key changes to enable the snort.conf file to be set up correctly on Windows. |
| 29/06/2023 | IDS/IPS | Change | Cloud Engineer  Mark Byrne  0457 532 233 | Snort - Windows | All - Snort.conf file | Set config logdir: to c:\snort\log  Set dynamicpreprocessor directory to C:\snort\lib\snort\_dynamicpreprocessor  Set dynamicengine to C:\snort\lib\snort\_dynamicengine\sf\_engine.dll  Included specific rule path $RULE\_PATH\community.rules | These are the key changes to enable the snort.conf file to be set up correctly on Windows. |
| **Date** | **Component**  (firewall / IDS/IPS, etc) | **Action**  (Add, remove, change) | **Modifier**  (administrator, IT) | **Name** | **Old Setting** | **New Setting** | **Reason** |
| 30/06/23 | IDS/IPS | Add | Project Manager Giuseppe Raciti  0438 221 782 | Snort - Linux | # config logdir: | config logdir: /etc/snort/log | No default directory was set for logs |
| 04/07/2023 | Firewall | Change | Project Manager Giuseppe Raciti  0438 221 782 | pfSense - Windows | Disabled | Enable remote logging | Sends log data to Splunk |
| 04/07/2023 | Firewall | Change | Project Manager Giuseppe Raciti  0438 221 782 | pfSense - Windows | N/A | Created Private / public keys | To allow remote SSH connections |
| 05/07/2023 | Firewall | Change | Project Manager Giuseppe Raciti  0438 221 782 | Sophos Antivirus - Linux | Off | Turn on IPS Detection | Feature was turned off |
| 06/07/2023 | Firewall | Change | Project Manager Giuseppe Raciti  0438 221 782 | Sophos Antivirus - Linux | Off | Automatic local backup turn on and set to daily backup at 6am | To save the configuration file to backup to the OneDrive, the backup had to be turned on. |
| 09/07/2023 | Firewall | Change | Server Administrator  Mauricio G. Guerra  0447 768 852 | Sophos XG Firewall | On | Activate DoS protection | To protect Linux Web Server for DoS and DDoS attacks |
| 09/07/2023 | Firewall | Change | Server Administrator  Mauricio G. Guerra  0447 768 852 | Sophos XG Firewall | On | Activate SYN floods / ICMP floods | To prevent SYN / ICMP floods |
| 09/07/2023 | Firewall | Change | Server Administrator  Mauricio G. Guerra  0447 768 852 | Sophos XG Firewall | On | Advanced Threat Protection (ATP) | Will enable behavioral analysis to detect and mitigate advance and zero day threats |
| 11/07/2023 | Antivirus | Change | Cybersecurity Specialist Shaun Heywood 0433108395 | Sophos Endpoint Security and Control | Remove third party security software, On | Remove third party security software, OFF | There may be requirements for additional security platforms |
| 11/07/2023 | Antivirus | Change | Cybersecurity Specialist Shaun Heywood 0433108395 | Sophos Endpoint Security and Control | In the Scan for section – click the checkbox > Suspicious files is turned off | In the Scan for section – click the checkbox > Suspicious files, turns on this setting | We want Sophos to scan for suspicious files |
|  |  |  |  |  |  |  |  |