Network Topology Technical Document

Network security has grown in necessity and complexity. Multiple layers of security or defense in-depth strategies are needed to minimize risk. Network design as well as hardware and software configuration are critical to the security, integrity, availability and recoverability of gaming data.

The start of a practical in-depth defense strategy includes putting public facing servers in a perimeter network. The perimeter network and the local area network should be separated and monitored by devices like:

- Firewalls
- Intrusion Detection/Intrusion Prevention systems (IDS/IPS)
- Unified Threat Management devices

Network traffic should be denied by default and firewalls with packet inspection should be used. A monitoring system that can send the responsible person an alert should also be implemented.

This kind of strategy should also be implemented for other high risk network areas such as a wireless segment, or remote connectivity.

The casino should segment the gaming environment from the rest of the LAN using industry best practices. With the exception of the wireless segment, VLANs may be used to segment the environment that contains gaming data from the rest of the hard wired network. Switches can be used for this type of segmentation. Internal VLAN configuration should include:

- Securing Telnet
- Securing SNMP
- Turning off unneeded services
- Enable and Configure logging
- Disabling unused ports
- Ports that do not need to trunk should have the trunk setting configured to be off
- If possible associate each port to a limited number of MAC addresses
- Explicitly allowing network traffic

Maintaining control over remote connections is an important aspect to network security. Creating unique usernames for each person or company will help ensure that there will be no unauthorized access. The casino should maintain a documented list of people and companies who will access the network remotely Access/system logs should be reviewed on a consistent basis and retained. The information found in logs can be instrumental in troubleshooting or incident remediation.

Remote connections should be secured using encryption and authentication. The encryption must be at least 128 bit and authentication must meet the requirements outlined in the logical security documentation. Logging should be configured on the device that is managing the remote connections. This system log should be reviewed for remote connectivity and required information recorded in the RAMP log.

Virtualizing the IT environment is an option. This type of environment gives a business more flexibility and manageability in managing their networks. However, virtualization creates its own set of requirements. These requirements include:

- The management network and service console must be hardened and segmented from the rest of the virtual environment.
- Virtual machines should be segmented from the hardware running them.
- Access to the hardware should be limited to authorized individuals.
- Passwords should be set for the BIOS
- Passwords should be set for the Bootloader
- Time/Date should be synchronized between the host and guest operating systems
- Resources are limited for Virtual Machines
- Virtual Environment workloads should be monitored

Documenting the following bullet points are an important part to network management. This process can be used as a tool to ensure data security and integrity, analyze trends, help troubleshoot problems, and identify inefficiencies. The following bullet points should be met for network management documentation:

- An inventory of all network components
- A visual diagram of the network
- Policies and procedures to minimize unauthorized access to network components
- List of all 3rd party connections to the network such as a VPN to another company.
- VLANs
- Inter VLAN (if enabled)
- Business justification for allowed network traffic
- Policies and procedures for open ports and documented business justification
- Policies and procedures to identify and remediate unauthorized network connections
- A formal document versioning process should be used
- A change control process should be used
- Testing results
- Management authorization(s)
- An Index of all formal documents
- Vendor best practices or recommendations
- Maintenance and repairs

The casino must document the gaming system versions including modules, collection units, 3rd party programs and Slot Machine Interface Board (SMIB) versions. The versions must be verified against the installation/upgrade notification forms that were sent to the Division prior to the installation or upgrade. Any discrepancies must be reported to the Division via email address stated in the General subsection of this section. This full verification of all gaming system hardware/software must be documented and performed at the completion of each installation/upgrade or annually whichever is sooner.

In order to have an effective environment that meets the needs of the casino, resource requirements for each application and their underlying operating system must be met. Proper configuration of Virtual Workloads is key to keeping the casino operating.

Wireless networks can be utilized by the casino for limited functions. (Please see the section on wireless)

These networks must be segmented from any other part of the LAN. Network traffic traveling into and out of the wireless segment must be monitored and logged.

Documenting policies and procedures for LAN management is necessary in order to ensure that a unified understanding and consistent application of LAN requirements is maintained. Please refer to the documentation section for further clarification.

In addition to the requirements listed above, all documentation must meet the requirements stated in the documentation section.