SICUNET
SMART & SIMPLE

Neptune Embedded Browser Access Control System - FAQs for the IT Professional

What is the Neptune Network Appliance / Hardware?

Our controller is an embedded, browser managed network appliance that is designed to support physical security of a facilities via a fast and intuitive embedded HTML5 web interface it's primary use is to inform control who, what, where and when access events occur . The system manages any physical device that the system designer chooses to control such as door locking hardware, device management such as fans, pumps, pullies …. In addition, the system is designed to monitor and inform the status of these devices. The hardware and software configured and managed over a network using most internet browsers. The system can manage 60 transactions per second, using its Quad Core processor with 64 Bit processing. Neptune offers additional system configurations that support up to 150 transactions per second with significant system capacities for scaling options.

The access control software runs on an industry standard Linux Ubuntu operating system and requires no server or software to be installed on local PC's or other browser enabled devices. As a browser managed system, our technology ensures compatibility with network equipment, smart devices, and computers. As a native IP network appliance, we do not require any additional gateways, communication wiring or add on adapters to be installed. Our system's Gigabit auto sensing network connection is responsive while ensuring secure connectivity.

All the hardware is similar in design, using identical software and is uniquely designed to perform the function of a "server" or a "client". In this design each device contains all the capabilities of the system and with database redundancy. When installed, a controller is configured as a server, or a client and no special hardware or software is required. Our market leading online licensing feature enhancement and system scaling allows you to grow or add capabilities when needed. It is fast and easy to turn an enhanced feature on or add additional clients to the system to manage more doors.

All communication between devices is encrypted and secure. Whether stored on the panel, SD Card and or FTP Server system data, event logs, user data are encrypted and secure.

How does Neptune and its hardware leverage the network?

Many customers choose to leverage the company's network infrastructure to interconnect and manage their Physical Access Control System. Leveraging an existing network lowers the cost of installation and improves performance when compared to other communication methods.

How does Neptune interconnect multiple panels?

Our controllers are designed to interconnect and control access for one or many doors or devices. When controllers are added to a network / system the hardware automatically sets itself an IP address in the zeroconf address space. The expansion controller then multicasts for a server controller at a specific IP address and port and presents our Unique Identifier (UID) to let it be known as an expansion controller. The Server controller then responds to establish the system interlink.

Expansion controllers can be statically or dynamically addressed. Typically, the server is assigned a static IP address and clients are configured for DHCP. However, the systems clients could be configured statically should the network administrator prefer.

These panels are designed to be interconnected on the secure side of a local LAN or WAN.

Neptune Embedded Browser Access Control System - FAQs for the IT Professional

How does Neptune interconnect with Cloud services?

Our controllers are designed to interconnect to the cloud for enhanced features such as mobile credential issuance and database synchronization. Our system interlinks panel to panel, mobile app, credential server and cloud via SSL with AES 256-bit encryption layer. Depending on the mail service we may also add TLS to pass data to an SMTP server.

Encryption Standards and Protocol

Network security and encryption is something we do not take lightly. We deploy the latest security encryption and protocols available. We have had and will continually perform PEN tests to ensure our standards and cyber protection practices are sound and up to date.

- □ SSL Encryption and Authentication for the browser to the controller
- □ HTTPS - Hypertext Transfer Protocol Secure
- □ SSH Authentication and Encryption between the server and the expansion hardware “clients”. The system administrator has the option to upload a private / corporate key.
- □ AES 256 Advanced Encryption Standard – data packets Users, Logs, Systems settings…
- □ In addition to the use of industry IT security standards, our system adds a secondary encryption require that only our hardware / ecosystem is capable of decoding and visually displaying the data that is produced and communicated by our system. This is proprietary to our system and is an added protection because the data is specific to our system use only.

To ensure our systems are secure, Sicunet performs and uses a variety of services to test the product for Cyber Security (PEN Testing). As a security provider, we take network security seriously and provide periodic security updates as required.

System Set up Information Requirement Checklist

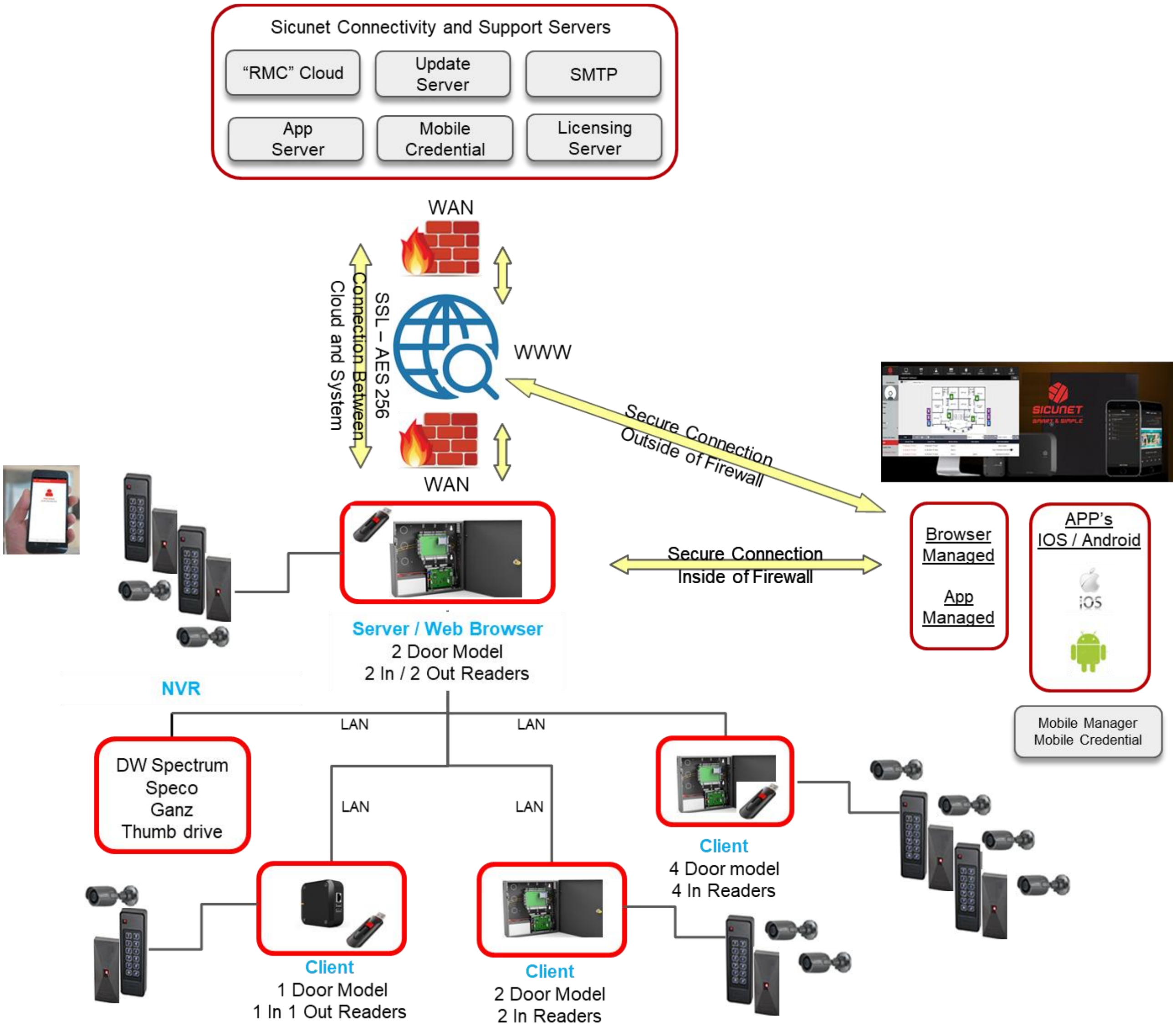
- □ DNS (Domain Name Server) IP address (Static for the server, Static or DHCP for the clients)
  Note: IP Address should be configured inside the firewall.
- □ Gateway IP Address, if any
- □ Subnet mask and IP addresses for the server and clients
- □ E-Mail relay server address or name
- □ E-Mail address name for Neptune and setup on the email server to accept the mail for the eNc relay
- □ NTP (Network Time Protocol) server name (s) if the network has no internet access.

Neptune Embedded Browser Access Control System - FAQs for the IT Professional

Network Port Usage Table

	TCP Port Description and Function		
Port	Direction	Service	URL | Address
20000	In Bound	Between the server and client	
6000, 6001	In Bound	If the server and the client are in different network, open these ports at server side	
9000-9100	In Bound		
80	In Bound	Between the server and browser. If the server and browser are in the same network you do not need to configure these ports.	Internal to LAN / WAN, Server Static IP, Clients - Optional Static or DHCP
443			
587	Outbound	SMTP (email)	Clients email configuration
9000, 9400, 9600	Outbound	Mobile App	link.remote-manager.net
9500	Outbound	Mobile Credentials – TCP Socket	cloud.sicunet.com
9900	Outbound	Cloud - Remote Management Cloud "RMC"	remote.sicunet.com
2021	Outbound	Software Updates - update.remote-manager.net	update.remote-manager.net
554	In Bound	RTSP Port for NVR - Video Streaming	Varies by vendor
8081	In Bound	RESTful API	
Note: Each port is tied to a system function. If you are not using the function the port does not need to be accessible.			

Eco System Overview


Sicunet Connectivity and Support Servers
"RMC" Cloud
Update Server
SMTP
App Server
Mobile Credential
Licensing Server
WAN
SSL – AES 256
Connection Between
Cloud and System
WWW
Secure Connection
Outside of Firewall
WAN
Secure Connection
Inside of Firewall
Browser Managed
App Managed
APP's
IOS / Android
iOS
Mobile Manager
Mobile Credential
Server / Web Browser
2 Door Model
2 In / 2 Out Readers
NVR
LAN
LAN
DW Spectrum
Speco
Ganz
Thumb drive
LAN
LAN
Client
4 Door model
4 In Readers
Client
1 Door Model
1 In 1 Out Readers
Client
2 Door Model
2 In Readers