**Purpose**

The purpose of this document is to set out the technical implementation parameters for each of the Highways England sites for purposes of remote access, monitoring and limited administration of their AV equipment to enable enhanced and pro-active response to fault conditions.

This has been produced to give an overview of the specific site setups and a suggested head end solution. It is the responsibility of the bidder (External Supplier ES) to provide their own detailed solution and include any additional elements they feel is needed to provide a working solution.

**Scope**

The Scope will be limited to the following details.

The provision and configuration of a Headline network configuration suitable to manage the system and access each client site.

Per site network topology and expected communications protocols.

It should be noted that some of the addressing used may change when reaching the implementation stage, but this should only be treated as a logical addressing change, methodologies and protocols will remain the same.

**Assumptions**

Each site networking equipment/switching to be provided by NRTS.

External Supplier (ES) supplied gateways are VLAN capable.

**Method**

A review of each of the Highways England sites included in this project (Northeast RCC, Northwest RCC, West Midlands RCC, Southwest ROC, East Midlands RCC, East RCC & Southeast RCC) was completed in consultation with the relevant manufacturers to ascertain potential equipment communication strategies and possibilities.

This information was then compiled into a limited per site diagram alongside communication parameters for review.

Where multiple elements share the same configurations, or are repeated, cabling has been omitted from network layouts for clarity. They are however included in informational tables for port calculations.

**External Supplier (ES) Suggested Headend**

The suggested headend network consists of redundant public WAN connections across 2 x Cisco ASR 9k Series security gateways interconnected with multiple fibre backbone switches to provide the basis of the network.

There is provision of an OpenVPN access cluster with PKI support to terminate connections from our client sites and to manage the encryption and certificate requirements for such connections.

The monitoring headend is a cluster of Debian servers running custom metric and dashboard software. Onsite gateway components will return data gathered to this location via the OVPN access cluster.

The Engineering WS cluster is a VMWare deployment of Windows 10 Machines for use of the field engineers only. Access to these machines needs to be strictly controlled and audited on a per-week basis.

Engineer access to client data, or to client sites is granular and enforced on a minimum-required per device basis. Such rules are applied and monitored via the ASR gateways.

There is a headend management system – this system is for device management and security control of the appliances, switches and gateways only.

The physical location of these components is to be detailed by the External Supplier (ES) and within a Tier 4 datacentre which is ISO27001, 14001 and PCI DSS compliant. Additionally, the infrastructure equipment is deployed within secure caged areas of all data halls and buildings utilised.

**Highways Onsite Service Provider Appliance**

We have broken out the logical layout of the monitoring systems as this will remain consistent from site to site and will be abbreviated in the per-site drawings.



The external supplier (ES) Gateway appliance comprises several inbuilt services used to provide the remote monitoring and control capabilities. These are;

**OpenVPN access client** – this will establish an outbound tunnel back to the Headend using the following parameters;

**TLS** Yes, Authentication & Encryption

**DH Key** 2048-bit

**Encryption** AES-256-GCM

**Digest** SHA-256

**Cert Re-Key** 43,200s

**Data Collection Service** – this will communicate with LAN connected/interfaced devices to gather metrics and monitoring information. This information will be aggregated and delivered back to the Headend. Devices are configured here on a per site basis.

**Connection Firewalling Service** – based on iptables rules this service will allow/disallow/NAT connections between segments where required. Configurations for these rules are suggested in the per-site below.

**Field Engineer Access –** Generates an easy to review onsite dashboard for a visiting engineer to employ quick diagnostics.

**Onsite Admin –** Device and firewall administration

**CXS –** Command Execution Service. If enabled, this will allow selected commands to be executed on permitted devices. Examples: *Re-sync video input, projector 1. Reset wall controller.*

This service requires command-acknowledgement meaning that the External Service (ES) provider engineer can request an execution which must be approved by another Field or otherwise authorised engineer before it will complete.

**Interconnect**

For the sake of completeness, we have shown multiple physical connections for each of the LAN/WAN connections we would attempt communication with. These connections can however be combined onto one link as the appliances are VLAN capable should this be preferred.

**Outbound Connectivity Requirements**

We have revised the service offering to a dial-back methodology. We found this to be more compatible with many of our clients who lacked the inhouse capability to provide multiple public addresses.

The appliance will establish outbound communication as follows;

**Destination:** Subnet range supplier to specify. (Single IP can be specified prior to GL)

 Port: TCP/UDP single port – will be specified per appliance/site

 ICMP Echo + Reply (Proto 1)

**Inbound Connectivity Requirements**

Only in response to outbound traffic. No direct inbound routing required.

**Client Network Connectivity**

Connectivity towards ‘Device Lan’ – this is a new LAN comprising all devices to be monitored.

Connectivity towards CCTV LAN – NATTED, one IP address required.

**Northwest RCCNetworking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

Main Control Room 7 x RJ-45 on new Device LAN.

Silver Command 6 x RJ-45 on same Device LAN as Main Control Room.

IP Pool TBD – Suggested 172.X.Y.Z/27 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | NEC Display | 21:22 TCP | Device Control Telnet/SSH | No |
| ESGW | Projector | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |
| ESGW | DDS-02 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**Northeast RCC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

RCC Main Control 17 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/27 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | Mit Projector | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**East Midlands RCC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

RCC Main Control 15 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/27 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | Mit Projector | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**West Midlands RCC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

RCC Main Control 16 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/27 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | Barco OV | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | Barco BCM | TBD | BCM Control | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**East RCC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

RCC Main Control 25 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/26 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | Mit Projector | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**Southeast RCC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

RCC Main Control 25 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/26 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | Mit Projector | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**Southwest ROC**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

ROC Main Control 26 x RJ-45 on new Device LAN.

IP Pool TBD – Suggested 172.X.Y.Z/26 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | NEC Display | 21:22:80 TCP | Device Control Telnet/SSH/HTTP | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |

**Test Environment**

****

**Networking Requirements**

Comms 1 x WAN Capable Port, 1 x CCTV LAN Port, 1 x Device LAN Port. (Or VLAN)

Test Area 2 x RJ-45 on new Device LAN, 1 x with PoE Class 2 if possible.

IP Pool TBD – Suggested 172.X.Y.Z/28 allowing for future growth.

DHCP Yes. To support engineering connections – will be provided by ESGW.

**Firewalling Policies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Src** | **Dst** | **Port** | **Desc** | **Encryption** |
| ESGW | rPi Display Emulator | 21:22:80 TCP | Emulate connected display/projector | No |
| ESGW | CCTV Control PC | 5900 | PC VNC | Yes |
| ESGW | DDS-01 | 21:80 | Device Interface/Status Telnet/HTTP | No |