ITT NMRN WAN and Firewalls – Supplier Questions and Answers

Q. Can you please send me a list of the CLI's? One for each address.
A. There aren't any as they are all fibre lines.

Q. Are you looking for an internet breakout for this MPLS? If so how much bandwidth will you require?
A. Yes we are and would to a degree be led by yourselves. What would the normal amount be? I'd suggest 400Mbps as a minimum if that works.

Q. Would you be looking at backup connectivity for any of the head office or key sites? You have mentioned back up in your document are the backup lines in the list below?
A. It would be good to have some backup broadband circuits at each of the sites that we could use in the event of a fibre outage, yes. At Portsmouth Historic Dockyard we have the 10/100Mbps Virgin Media line as our current backup, but as stated this would also need to increase and ideally be used in an Active/Active scenario.

Q. If you are having internet breakout.   Do you require a single firewall (single point of failure) or 2 firewalls to secure the internet breakout?
A. We would go for 2 firewalls for some resiliency, but presumably these would sit at the MPLS level with each site below these? We are open to suggestions on how this can be interpreted.

Q. On the P2P that go back to Portsmouth, is it the Portsmouth Historic Dockyard or National Museum of the Royal Navy?

A. These go back to the National Museum of the Royal Navy.

Q. Management of firewall. Are NMRN planning to supply their own firewall, or access to manage the Cloud Firewall. If supplying own, where is this to be situated?
A. I am assuming we will need one firewall in the cloud which will ultimately control access to the MPLS if that is the solution proposed. You may also propose a firewall at each of our sites as well as part of the supplied routers.

Q. Management of Firewall – expand on what Admin they are planning to cover?
A. Not sure I entirely understand the question, but this is primarily for us to have visibility of the rules created and to allow us access to implement new rules or block existing ports if required.

Q. SDWAN can remove centralised Firewall and breakout with policy, plus the SRX estate or it replacement. Is there any identified need for WAN optimisation and any QoS?
A. Potentially there is, at the moment our main 100Mbps line at the NMRN is hitting saturation and so we have switched on some QoS rules which are being worked through. We of course hope that an increase in bandwidth will resolve some of these issues, but without full visibility of what the other organisations are doing on their networks, some control is required.

Q. What is the current breakout from the Elite MPLS, not detailed in the ITT.
A. We currently have 1Gbps 1:1 out from the vSRX.

Q. What failover option are NMRN considering? FTTC, 4G?
A. We are open to options on this. I don't think 4G will work at some of our sites because of locations and signal strengths, a regular office broadband circuit would be useful with the exception of the NMRN as detailed in the ITT, where we already have a fibre backup connection with Virgin Media.

Q. For the new DR location, would a 1Gbps or 100/100 P2P assist?
A. I don't think we'll get P2P due to the geographic location, but happy to be told otherwise. 1Gbps would be great if within budget.

Q. Graphing – is this to be reported on request or periodically provided. Also, is it a load/capacity report or is health/stability also to be reported ?
A. Ideally both to be reported on, but mainly load / capacity. Periodically would be useful, but also on request. We would like visibility so we didn't need to request them, we could login and see utilisation easily.

Q. Define parameters for alerts? Outage or 10%+ degradation?
A. Outage mainly on this one.

Q. Portsmouth Dockyard – Active/Active – in order to provide a recommendation on the two connections, is it possible to have usage reports? This will determine the overall bandwidth needed in the event of a problem and BAU can be delivered.
A. Yes I can supply these in the form of Cacti graphs. What sort of date range are you thinking of? The 10Mbps Virgin line isn't currently used so won't have any traffic across it.

Q. Portsmouth Dockyard – Would NMRN accept these two circuits route to alternate Fibre Exchanges?
A. Yes that would be fine.

Q. Royal Marine site – would a rolling 30 day ADSL be acceptable?
A. Yes it would if it simplified the setup in the short term, but as outlined in the ITT this isn't necessarily in scope.

Q. Would each organisation need their own VRF in an MPLS, with secure partitioning?
A. Not necessarily from a security point of view, but as listed in the tender we do forward traffic from Wi-Fi radios at the remote sites to a central controller in Portsmouth on its own subnet, so we would potentially need it for that.

Q. Are there any specific security elements needed to be considered within the Firewall?
A. Not really, the standard firewall rules will apply and the ability to block certain ports, IPs or protocols. We would be copying existing rules across from our current firewall as well.

Q. The copper line at HMS Victory – does this need to be part of the MPLS and do you have the CLI for this circuit?

A. It doesn't need to be a part of the MPLS, no. The CLI is 02392 863832 and the full address is HMS VICTORY, 2 dock, HMNB Portsmouth, Hants, PO1 3PZ.

Q. The tender states that PHD has 2 circuits, are failover links desired for all the sites?

A. Yes they are and we are open to suggestions on how to achieve this. In some locations 4G would be an option, but signal strength at one or two sites wouldn't work out. A standard office broadband connection would be the minimum.

Q. I wanted to ask if you want us to perform onsite installs for the hardware or if you are happy for us to pre-program the routers and ship them to site for you to install?

A. Happy to install them ourselves with some remote support if required.

Q. Does there need to be any site to site VPN or client to site SSLs or equivalent?

A. There doesn't, of course allowing for the fact that we need some sort of internal MPLS / SD-WAN link between our sites.

Q. The tender references a desire to bring firewall management back in-house. Do you have a preference on, or expertise to, a particular firewall manufacturer?

A. No specific manufacturer, no. As long as there is some support available from your team or some initial training that can take place, that would all help.

Q. It is assumed that all sites are connected into MPLS, are all these utilising the Elite Ltd centralised managed firewall?

A. They are. The only site that isn't in the MPLS is HMS Victory, simply because it doesn't need to be, and FAAM which is connected to the MPLS via VPN.

Q. What is the current specification of the Elite Ltd internet breakout service?

A. We currently have 1Gbps 1:1 out from the vSRX.

Q. Do any sites have a localised internet breakout service? If yes provide details

A. No, although we would like to consider this as part of this tender as a backup.

Q. The site description suggests PHD is a backup circuit for NMRNP, can we assume these are the same physical locations?

A. They are, although different buildings which are connected with 1Gbps internal fibre.

Q. Is Quality of Service required on the circuits?

A. Ideally yes, we are having some issues currently which have required QoS. Moving forward this will be a useful control, particularly at NMRNP, as we don't have full control or visibility of customers networks.

Q. What voice solution is currently in use and where are the IP PBX located?

A. We use the 3CX phone system which is hosted in Portsmouth.

Q. What internet connection does the guest WiFi utilise?

A. Ultimately it will be the Portsmouth connection as that is where the controller for the Wi-Fi is and so the requests will go out from there. But the radios are routed back to Portsmouth across the MPLS, so to a degree will be using the internet breakout at all locations.

Q. Will co-managed firewall comply with DSS requirements, where we will retain responsibility for backup and maintenance of the device an NMRN retain ownership of the device configurations?

A. Yes as I understand it, because we need to have visibility of rules created. They don't deem it sufficient if we ask for a rule and you say it is done, if we can't actually verify that.

Q. Why are there P2P links, is there a technical reason?

A. No, when they were installed this was a cost effective option to get 100Mbps to those sites, so if there is an alternative then we are happy to consider that.

Q. What site resiliency is currently in position for network connectivity?

A. None other than at the Portsmouth site and see comment above.

Q. What are the requirements of the firewall?

A. Some QoS as mentioned above and the usual port / protocol rules to block / allow appropriate traffic. We don't have any particular in-house expertise on one brand of firewall, so are happy to go with your suggestion as long as we have the option of some remote support or some initial training to guide us through.

Q. What centralised internet breakout size is required?

A. TBC once I know what we currently operate on.

Q. Will the existing WIFI controller be retained? Can we replace this but retain functionality? Is this currently Juniper also?

A. Yes it will be as this is managed by a 3rd party. The WiFi is Ruckus.

Q. I would like to see if there is a network diagram available illustrating the current setup?

A. Unfortunately we don't have anything which is up-to-date at this stage. Happy for you to produce something and we can verify it.

Q. Does the circuit install cost come out of the circuit budget indicated?

A. Yes it would need to.

Q. What is the likely start date for this project and expected delivery timescale?

A. The contract award and final confirmation is on the 10th December, so we would look to move as quickly as possible after that date. We don't have a timescale in mind, we'd of course need to approach it in a sensible manner and ensure we have minimal downtime on any circuits.

Q. Is there any wayleave or known installation issues experienced as part of previous circuit installs at any site?

A. We only required one wayleave previously and that was at the Portsmouth site for the Virgin media connection. All other sites have been straightforward installs I believe.

Q. How much is the current quarterly cost for the internet breakout circuit? It is assumed this cost forms part of the National Museum Royal Navy's existing circuit budget.

A. We aren't billed for this separately, it forms part of our overall costs, I assume broken out across each circuit.

Q. WAN monitoring – Would you like this on a working week, 7 day week and or 24/7 basis for the purposes of escalation support? Alternatively we can cost these as options

A. Really this is twofold. Firstly a 'live' view to see current traffic levels to monitor the links and for any saturation if it occurs. Secondly just the basic monitoring for up / down on the circuits.

Q. WAN Security – Would you like security services provided as standard on the firewalls (regardless of MPLS or SDWAN) to provided additional security benefits? Alternatively we can cost these as options.

A. Yes please, the minimum would be a firewall either on the internet breakout or configurable on the SD WAN at each circuit.

Q. P2P Links – Will you requiring routing between subnets from the P2P links? If no, routers are not required. If yes they will be required.

A. Yes we will as we need to route not only our local subnets back to the main network, but also subnets like the Wi-Fi which need routing back to Portsmouth.

Q. Do you know what firewall you would like to / intend to use? I am assuming you are supplying this?

A. No we aren't supplying it. The aim was for the suppliers to put one in, either at the internet breakout on an MPLS if that is what is proposed, or I assume one at each site as part of the router in the event of an SD WAN being the proposed solution? No preference over model either, as long as we can have some support if needed around config if it is something we are unfamiliar with.

Q. On contracts finder the value is stated as £110,000, but from reading the documents it states that "Our overall aim is to stay well within our existing budget, ideally achieving some savings". The existing budget is - £11,964 a quarter over 3 years £143,568. Could you advise if the £110K is a fixed number for the maximum cost?

A. No I'm happy to work over the £110k cost if it is for the right solution.

Q. "Where we have two connections into Portsmouth Historic Dockyard we would like to use an Active / Active setup to maximise our investment in the backup connection. Note that the connections terminate into different buildings but are linked via gigabit fibre." Please confirm you can provide a Layer 2 connection for the relevant failover mechanism to operate across?

A. Yes, I can confirm we provide this.

Q. "At Portsmouth Historic Dockyard we have 6 separate businesses all sharing the connection . We present each business with a port on our WAN VLAN which they then connect to their own router and manage their own network from. This means that we have a requirement for a minimum of 32 public IPs for various devices that each of these businesses run, with the scope to increase this if required." Please confirm you are comfortable with a 1:1 NAT scenario on a cloud firewall to facilitate this?

A. Yes I think we are. So in effect all traffic will be forwarded to each public IP? It would then be the responsibility of the tenant to firewall and filter their traffic from there?

Q. "We also require one additional public IP for a CCTV system at HMS Caroline, Belfast." Please confirm you are comfortable with a 1:1 NAT scenario on a cloud firewall to facilitate this?

A. Yes, although as per above presumably we would need to supply a firewall to filter out other unnecessary traffic?

Q. "Explosion Museum - 100Mbps (P2P to Portsmouth) and RNSM 100/100Mbps (P2P to Portsmouth)." Please confirm you are comfortable with these sites being part of the MPLS network rather than have P2P circuits?

A. Yes, no problem with that.

Q. "All sites offer public WiFi which is routed back to a controller in Portsmouth. This is via a separate VLAN and subnet which is sent back across the MPLS. We would need to maintain this capability moving forward." Please confirm the bandwidth required at each site for this WiFi VLAN?

A. We don't have a specific value at present. The Wi-Fi is managed by a 3rd party and so each connection has a bandwidth limit applied to it anyway. It's difficult to put a figure on this, currently it doesn't cause us any problems.

Q. "Currently our DR solution resides in another building at Portsmouth Historic Dockyard, but there is a desire to move this to FAAM and so the connection from NMRNP to FAAM will need to be sufficient enough to take replica increments from our production environment overnight, via VEEAM backup. This amounts to, on average, around 60GB per night but can be as high as 200-300GB on occasion." Please confirm if you would like this DR replication traffic to be part of a VRF shared by just these two sites, and if so, how much bandwidth is required on the VLAN?

A. Happy for it to be included as a VRF. I'd be open to suggestions about how much bandwidth is required. My main concern would be latency across the link, but it was more about it ensuring we had the capacity to work with between the two sites.

Q. I assume you are looking for it to be a full security solution, not just a NAT / Stateful solution? Do you have current details of the IP Addressing / VLANS / Routing internally? Apart from the phones, I am somewhat unaware of what you have done recently. We will look to mirror what you currently have, than the changeover should be much easier – Again, we are quoting to do the lot – config routing against your current design, etc rather than just install of the lines?

A. Happy if it is ongoing support and yes to a full security solution for the WAN. Our details of current addressing and routing is ok, just not all documented. Yes to getting it all configured to mirror what we have currently. Portsmouth is the most complex as you would expect, the other sites are simpler with just a couple of different subnets.

Q. Just a quick question regarding the link between NMRNP and PHD. Is this a direct private fibre between internal switches and is it Layer 2 or 3 via a VLan trunk?

A. It is a direct private fibre between internal switches at layer 2, but is across a VLAN trunk currently.