**Tender for the Implementation and Management of NGN Network & Voice Services**

**(SD-WAN, WAN, LAN, WLAN, UC & CC)**

**Tender Notice period ends 2nd June at 9am**

**If you wish to be included in this tender, you must confirm to the NGN contact your expression of interest via email.**

**If your interest to participate is not made to the NGN main contact provided on the front page of this tender document before the Tender Notice period end date, then you will not be able to participate in this tender event.**

**NGN Contact: Harriet Wilkes**

**Email: hwilkes@northerngas.co.uk**

**COMPANY INTRODUCTION**

## **Company overview**

Northern Gas Networks Limited (NGN) is the company responsible for distributing gas to homes and businesses across the North of England. As part of the restructuring of the gas distribution business in England, NGN successfully acquired the North of England gas Distribution Network (DN) and took control of the assets on 1st June 2005. NGN has been responsible since then for the transportation of gas to the North of England via 36,000Km of pipelines.

The DN is located in the North of England and extends south from the Scottish border to South Yorkshire and has coastlines on both the East and West sides of the region. The DN contains a mixture of large cities such as Newcastle, Middlesbrough, Leeds and Bradford and a significant rural area including North Yorkshire and Cumbria. The area covers around 6.7 million inhabitants and has approximately 2.5 million customers. The DN is supplied via 23 off takes from the national Transmission System.

**Northern Gas Networks Geographic Area**

|  |  |
| --- | --- |
|  |  |
| No. | Location |
| 1 | North Tyne |
| 2 | Cumbria |
| 3 | Wear |
| 4 | Tees |
| 5 | North Riding |
| 6 | Bradford |
| 7 | Leeds |
| 8 | East Riding |
| 9 | Pennines |
|  |  |



## **NGN Core Values**

NGNs dream is to become the UK’s most loved, admired and respected company, and to establish a reputation for doing business really well through a united and empowered team that is mind-blowingly great. We recognise the important role that our supply chain partners have in supporting NGN to achieve our dream.

Our dream lies at​​ the centre everything we do and has been translated into a **unique set of values** that reflect and reinforce our culture

* Trailblazing
* Intellectually Curious
* Community Focused
* Empowered
* Heartfelt
* Happy

Every member of our team is passionate about the contribution they make to our growing reputation as a pioneering, effective, conscious and enlightened business that is focused on changing the way that things are done.

We expect our suppliers to share our vision and values and our way to support NGN in achieving our goals.

**PROCUREMENT INFORMATION**

**Procurement Act 2023 / Procurement Regulations 2024**

This procurement is being conducted in accordance with The Procurement Act 2023 / Procurement Regulations 2024 using the Competitive Flexible Procedure.

## **NGN Contact**

**ALL COMMUNICATIONS MUST BE SENT VIA THE NGN’S PROCUREMENT PORTAL MARKET DOJO.**

During the period of this Tender process, no contact must occur between any member of your organisation's staff and any member of NGN other than through the designated contact points. The only exception to this rule is where organisations already have staff working on NGN business, in which case their staff should be instructed not to discuss the project with NGN employees.  
NGN reserves the right at its sole discretion to exclude any organisation (or third party working for any organisation) found to be in breach of these contact requirements.

## **Procurement Process**

The procurement process will be managed electronically via NGN’s Procurement Portal Market Dojo.

All communication will be managed through Market Dojo.

All tender response must be uploaded electronically.

Tender questions should be answered in the requested format, i.e. text or attachment, and word counts adhered to where applicable. If a question requires an attachment upload as your response and you have multiple attachments, please upload these as a Zip file. If you experience any technical difficulties, please contact the person named in this document. Responses should not be submitted via the messaging portal. Suppliers should note that if they persistently fail to follow this instruction, and answers are not readily available in the correct format then this may result in failing to achieve a score in the relevant section.

Suppliers should avoid uploading responses on the last day of any stage of the tender in case of technical difficulties as NGN will not reopen an event after it has closed.

Suppliers may save documents in Market Dojo throughout the process but must ensure that it is submitted in full before the closing date.

NGN cannot access or determine whether Suppliers have submitted a bid until after the event has closed as our process is a totally sealed bid process. It is your responsibility to ensure that you submit your bid on time.

Responses must be submitted within the timeframe stated in Market Dojo

**Central Digital Platform**

**Registration: It is important to make sure that your organisation registers onto the**[**Central Digital Platform (CDP)**](https://www.find-tender.service.gov.uk/Search)**. NGN will be unable to award a contract with your organisation without a valid unique supplier ID (PPON number)**

**IMPORTANT NOTE: If at any point during the procurement event or through the lifecycle of an awarded contract your organisation or any Subcontractors are placed on the Government lead debarment list it is at NGN’s discretion as to whether we exclude a bidder from participating or terminate an ongoing contract.**

**Procurement Plan**

A tender process will be carried out under the Competitive Flexible Procedure. It is anticipated that the strategy will be in line with the below

A diagram of a process

AI-generated content may be incorrect.

If supplementary stages are required throughout the process, or stages noted in the strategy defined above are no longer required, it is at NGN’s discretion to include or remove stages. Please note that any additional stages added could result in the following changes to scoring -

* an enhancement of scores awarded in previous stages OR
* an additional award criteria OR
* Score from previous stage + score from additional stage added together.

The impact that any additional stage has on scoring will be clearly communicated to all bidders and will not be refined following submission of tender stages.

### **Contract Basis**

The initial period of any contract(s) resulting from this procurement will be 3 years.

The length of the contract may be extended by NGN for a further 5x1-year periods to give a maximum duration of 8 years.

All prices shall be fixed for the initial 3-year term. For any price increases at the point of extending, your price increase mechanism must be clearly highlighted in your commercial response during the RFP.

A copy of the Contractual Agreement has been provided. Bidders should note that the challenges will be scored based upon risk and NGN reserve the right to reject any bidders who propose high risk challenges, or a material change to the contract. Please see Contract Challenges Scoring Guidance below.

During the RFP you should state any major Contract Challenges that you have relevant to the proposed draft agreement and state your proposed amendments in the 'Contract Challenges Matrix' provided. By proposing no challenges, you are confirming that you accept the proposed draft Agreement.

**Bidders must raise all challenges to the proposed Terms and Conditions during the RFP stage and submit the Contract Challenges Matrix as part of their tender return, NGN will not consider any challenges raised at a later stage. NGN reserves the right to disqualify those bidders who raise high risk contract challenges or suppliers who raise contract challenges at a later stage. NGN reserves the right to revoke conditional award and conclude terms instead with the next highest scoring bidder.**

**** ****

## **Evaluation Criteria**

The evaluation criteria for the PQQ and RFP stages of this procurement process are outlined below.

It is at the discretion of NGN to change the weightings/criteria or add additional sub criteria/weightings to the PQQ or RFP if there is a need to do so before the submission deadline of the relevant stage. Any changes to the evaluation criteria will be communicated to all Bidders.

**Conditions of Participation Evaluation**

This section is made up of Pass/Fail questions. Suppliers who pass all questions will automatically be invited to submit responses to PQQ questions.

Suppliers who fail any Conditions of Participation questions will be rejected from this tender.

## **PQQ Evaluation Criteria**

PQQ responses will be assessed against the criteria set out below.

Each section will have weighted questions and weightings are detailed in Market Dojo.

|  |  |  |
| --- | --- | --- |
| Section Ref | Criteria | Weighting |
| Section 1 | PQQ Guidance | NA - Information for Bidders |
| Section 2 | Cyber Security and IT | 20% |
| Section 3 | Supplier Financials | 3% |
| Section 4 | Responsible Procurement | 10% |
| Section 5 | Health and Safety | 3% |
| Section 6 | Business Continuity | 4% |
| Section 7 | PQQ Specific Questions Pass/Fail | Pass/Fail |
| Section 8 | PQQ Specific Questions Weighted | 60% |
|  | Total | 100% |

Suppliers who pass all mandatory and (to the satisfaction of NGN) all discretionary questions will then be assessed against the scoring criteria and the top 4 scoring suppliers will then progress through to tender stage.

Please note, if a successful supplier does not wish to take part in the RFP, then the next highest scoring supplier will be invited to bid.

### **RFP Evaluation Criteria**

The award will be based upon price and quality, and it is the intent that the award will be based on the Most Advantageous Tender.

The RFP evaluation assessment will be as follows:

**RFP Assessment 1 (100%)**

The evaluation criteria is split 40% commercial, 60% non-commercial. The individual scores for each section and question will be indicated against the questions in Market Dojo.

The assessment of price will be carried out independently of the quality assessment and scored against the methodology stated in the evaluation criteria document.

**RFP Assessment 2 – Presentation**

Following Assessment 1 it is anticipated that the top 3 scoring suppliers will be shortlisted to a presentation stage.

All suppliers will receive notification to detail whether they have been shortlisted to presentation and suppliers who do not progress though should note they will not receive detailed feedback until the assessment summaries are issued following the award decision.

During the presentation suppliers will be asked to present their solution in its entirety based on their RFP response. This will either be in person or via Teams.

During the presentation you may be asked to clarify points that were picked up in your RFP response. Following the presentation the score awarded against the RFP non-commercial questions may be adjusted accordingly.

**Final Assessment**

The scores from Assessment 1, Assessment 2 and BAFO price scores will be combined to arrive at the final scores for each supplier.

NGN will award this contract to the highest scoring bidder and we intend to award the contract to 1 company.

The assessment of price will be carried out independently of the non-commercial assessment and scored against the methodology stated above.

**Important Note**

**If the difference between the first and second highest scoring bidder is less than 3% NGN reserves the right to award the tender to the bidder who provides the lowest price tender unless there are exceptional reasons.**

### **Scoring Methodology**

For qualitative questions NGN will score on the following basis

|  |  |
| --- | --- |
| **Points** | **Interpretation** |
| **9-10** | **Excellent** –Overall the response demonstrates that the bidder exceeds all areas of the requirement and provides all of the areas evidence requested in the level of detail requested. This, therefore, is a detailed excellent response that meets all aspects of the requirement leaving no ambiguity as to whether the bidder can meet the requirement. |
| **6-8** | **Good** -Overall the response demonstrates that the bidder meets all areas of the requirement and provides all of the areas of evidence requested, but contains some trivial omissions in relation to the level of detail requested in terms of either the response or the evidence. This, therefore, is a good response that meets all aspects of the requirement with only a trivial level ambiguity due the bidder’s failure to provide all information at the level of detail requested. |
| **3-5** | **Adequate** - Overall the response demonstrates that the bidder meets all areas of the requirement, but not all of the areas of evidence requested have been provided. This, therefore, is an adequate response, but with some limited ambiguity as to whether the bidder can meet the requirement due to the bidder’s failure to provide all of the evidence requested. |
| **1-2** | **Poor** – The response does not demonstrate that the bidder meets the requirement in one or more areas. This, therefore, is a poor response with significant ambiguity as to whether the bidder can meet the requirement due to the failure by the bidder to show that it meets one or more areas of the requirement. |
| **0** | **Unacceptable** - The response is non-compliant with the requirements of the ITT and/or no response has been provided. |

### **Evaluation Panel**

NGN’s team to perform the evaluation of this tender process comprises the following:

This list may change throughout the duration of the Tender

|  |  |
| --- | --- |
| Name | Department |
| Gurpreet Singh | 3iG |
| Nathan Best | 3iG |
| Patrick Wreglesworth | 3iG |
| Lisa Adamson | 3iG |
| Alex Hayden | 3iG |
| Charlotte Hughes | 3iG License |
| Harriet Wilkes | Procurement |
| Alexander Walsh | Legal |

## **Tender Timetable**

|  |  |
| --- | --- |
| **Description of Event** | **Date** |
| Issue Tender Notice  *Conditions of Participation and PQQ live on this date* | 6th May 2025 |
| Tender Notice end date | 2nd June 9am |
| Conditions of Participation end date | 2nd June 5pm |
| PQQ end date | 9th June 9am |
| Evaluation of PQQ submissions | 9th June – 23rd June 2025 |
| Notification to successful/unsuccessful bidders | 24th June 2025 |
| Issue RFP | 25th June 2025 |
| Deadline for supplier clarification questions | 2nd July 2025 |
| Deadline to circulate all suppliers Clarification questions | 7th July 2025 |
| RFP end date | 16th July 2025 |
| Evaluations & Clarifications | 17th July – 31st July 2025 |
| BAFO | WC 4th August 2025 |
| Presentations | WC 4th August 2025 |
| Final Evaluations | 11th August – 15th August 2025 |
| Issue Assessment detailing outcome | 18th August 2025 |
| Standstill Period | 18th August – 26th August 2025 |
| Contract Negotiations | September 2025 |
| Contract signed | September 2025 |
| Transition/Implementation period start | |

***Please note the above timetable is indicative and may be subject to change.***

### **Tender specific Scope of Requirements**

It is at the discretion of NGN to amend requirements of the scope if there is a need to do so. Any changes to the scope will be communicated to all Bidders.

*Please note that substantial amendments will not be made.*

### 2. Introduction

# **Introduction of The NGN Network Service**

In 2022, NGN embarked on a network transformation program aimed at modernizing its infrastructure through the implementation of a Software Defined Wide Area Network (SD-WAN) architecture. The tender for this significant project was awarded to FourNet and their carrier provider, Virtual1, who were tasked with implementing and managing the NGN SD-WAN network service.

The primary objective was to enhance control, security and visibility of the organisation’s increasing internet-consuming services, while maintaining the flexibility to integrate interfacing sites into our network in an agile manner.

The key deliverables of SD-WAN design included:

* Implementation of a single-vendor (Fortinet) SD-WAN solution, comprising Fortinet FortiSASE and Fortinet Secure SD-WAN services.
* Provide a hybrid network solution that integrates both SD-WAN and MPLS technologies, enabling NGN to leverage private Quality of Service (QoS) routing via MPLS, whilst utilising secure SD-WAN routing over the internet.
* Refreshing existing Wide Area Network (WAN), Local Area Network (LAN) and Wireless Local Area Network (WLAN) hardware with Fortinet devices (FortiGates NGFW, FortiSwitches and FortiAPs). Increasing compatibility, visibility, management and network security across the NGN network landscape.
* Implementation of a new WAN with increased bandwidth capacity to enhance the growing demands of our operations.
* Implementing resilient circuits to ensure High Availability (HA) of connectivity at all NGN sites, maintaining continuous and reliable communication.
* Establish a centralised internet breakout from FourNet’s cloud service platform to ensure the secure routing of authorised NGN infrastructure applications and services across the WAN.
* Enabling direct internet access (DIA) from all NGN sites to alleviate WAN congestion and enhance network latency for internet-based services.
* Deployment of Fortinet FortiAuthenticator to rigorously enforce Identity and Access Management (IAM) protocols, specifically 802.1x, for client devices interfacing with the NGN network. This initiative will ensure compliance with dynamic port policies and enhance network security.
* Provide connectivity to partner locations, to enable NGN and its affiliates to securely share private data.
* Deliver a co-managed service, granting NGN comprehensive visibility to monitor the SD-WAN network and Fortinet services hosted within NGN (FortiAuthenticator) and Cloud Services (FortiGaurd, FortiManager, FortiAnalyser and ESP Monitoring).

**Introduction of The NGN Voice Service**

As part of the network transformation programme, NGN also opted to modernise and implement a new voice service, replacing our legacy on-premises EoSL MITEL unified comms (UC) and contact center (CC) solution. FourNet implemented a modernised UC and CC service, utilising their cloud service platform, alongside interfacing into Nice CXOne CCaaS solution.

The key objective was to utilise cloud-based telephony to the greatest extent possible. Mitigating risks associated with power outages, restricted access to physical buildings, and hardware failures.

The key deliverables of UC and CC design included:

* Fully secure and integrated UC and CC voice service with our SD-WAN architecture.
* The solution being cloud-based and accessible globally, providing robust and flexible communication capabilities.
* The UC being built on MS Teams Telephony, enabling NGN to use our existing Microsoft Teams licenses, as part of NGNs wider MS O365 E5 license agreement. This will allow NGN to cater for business stakeholders that require a traditional land line number.
* Integration of MS Tiger Prism into the UC solution, helping NGN to manage and analyse communication data effectively, providing insights into usage patterns and assist in ongoing optimisation of the UC services.
* Configuration of Gamma SIP Trunk Call Manager (STCM) to enhance the UC and CC services, providing HA and resilient communication infrastructure, whilst supporting NGN Business Continuity Management (BCM) processes.
* Integration of the Nice CXOne InContact Omnichannel CC platform, including configuration of the following services:
  + CXOne Automatic Contract Distributor (ACD)
  + CXOne Admin
  + CXOne Digital First Omnichannel
  + CXOne Email
  + CXOne MAX Agent Softphone
  + CXOne Studio

NGN operate out of 17 locations all interconnected via Multiprotocol Label Switching (MPLS) circuits to various partner data centers, NGN on-premises IT infrastructure and AWS cloud services (IaaS).

NGN AWS cloud services host our business applications and services, this also includes our critical national infrastructure services. NGN are increasingly reliant on cloud-based SaaS applications including key interfacing into Microsoft (MS) and SAP services.

NGN on-premises IT infrastructure provides a small footprint of management services within various NGN locations.

For video conferencing, NGN employs several systems including MS Teams Meeting Rooms and Clickshare. Furthermore, NGN operates a digital signage streaming services across all NGN sites.

### 3. Scope

## 3.1 Scope

The existing network and voice service management contracts are approaching renewal with our current service provider. In this tender process, NGN is interested in exploring implementing a new network and voice solution. This will also include providing NGN with a comprehensive service for the management of the implemented network and voice services.

NGN requests that suppliers participating in this tender provide proposals that build upon the existing network and voice technology stacks currently in place. However, NGN is also open to considering alternative technologies. To be considered, these proposed alternatives must demonstrate an equivalent or superior solution in terms of architecture and security best practices, while also adhering to the timelines outlined in this tender process.

The aim of continuing to build on improving service expectations, along with enhancing and optimising these services in alignment with our future business strategies.

The successful supplier will be responsible for the comprehensive solution implementation and management of NGN’s network and voice services. The scope includes, but is not limited to:

* Wide Area Network (WAN)
* Software-Defined Wide Area Network (SD-WAN)
* Next Generation Firewalls (NGFW)
* Local Area Network (LAN & WLAN)
* Cloud Services
* Voice Unified Comms (UC)
* Voice Contact Centre (CC)

The successful supplier will also need to demonstrate the capability to:

* Ensure a seamless transition of network and voice management services, with minimal disruption to NGN operations.
* Deliver complete reliable and high-quality managed service.
* Innovate and propose enhancements to services, as part of the on-going contract.
* Strong understanding and experience of managing critical network and voice services, within a heavily regulated or safety critical environment.

By participating in this tender process, NGN seeks to identify a supplier who can not only meet our current needs but also foster continuous improvement and innovation in our network and voice services.

**Please Note** - Suppliers participating in this tender must ensure that their proposed network and voice services can be successfully implemented within the stipulated timeline as outlined below:

* **Voice Services (UC and CC) – 30-06-2026**
* **Network Services (WAN, SDWAN, NGFWs, Cloud Services, LAN, WLAN) – 29.08.2026**

Below is a high overview of each managed service, along with a granular breakdown of the expected scope of requirements. Including specific points that must be considered by the potential supplier when responding to this tender.

### **3.1.1 Wide Area Network**

The WAN equipment at NGN sites currently comprises of the below:

|  |  |  |
| --- | --- | --- |
| Hardware Vendor | Type | Model |
| Juniper | Service Gateway | NFX150 |
| Juniper | Service Gateway | SRX340 |

Virtual1 provides an underlay network to each location via dual fibre ethernet circuits to facilitate the SD-WAN overlay network which FourNet have deployed. This also includes leveraging the existing infrastructure between Virtual1 and FourNet to provide connectivity from each location into FourNet’s cloud service platform, where FourNet host additional services that NGN utilise.

Each circuit is configured with a single primary DIA service and a single primary layer-3 VPN (MPLS). Security, failover mechanisms, traffic engineering and traffic steering is provided by the FourNet SD-WAN solution.

External and other traffic profiles (as determined by the SD-WAN policies) utilise the DIA services being provided by Virtual1.

A single MPLS VRF has been configured on the Virtual1 core to facilitate traffic profiles (as determined by the SD-WAN policies) which include site-to-site, site-to-AWS, and site-Cloud-Service-Platform traffic.

Virtual1 provide FourNet a mix of Direct Internet Access (DIA) and MPLS services that will allow them to provide hybrid SD-WAN/MPLS WAN services to NGN. All access services provided by Virtual1 are delivered as standalone primary services with no managed active/passive or active/active configuration – all security, failover mechanisms, traffic engineering and steering are provided by the FourNet supplied Fortinet Secure SD-WAN appliances.

Virtual1 do not filter routes within end-user MPLS Virtual Routing Forwarding (VRF), they advertise all connected subnets, routed subnets, plus link and management subnets to the FourNet FortiGate over each BGP peer.

The WAN network topology and physical configuration overviews, including illustrations is in appendix section:  
[3.1 NGN WAN Physical Configuration](#_5.1_NGN_Site)

A full list of NGNs connecting sites, including current carrier and resiliency types is in appendix section: [3.2 NGN Site Connectivity](#_3.2_NGN_Site)

**Scope - WAN:**

Potential suppliers must thoroughly address and consider the following requirements:

* The potential supplier is expected to provide NGN WAN underlay to all NGN sites as specified within section [3.2 NGN Site Connectivity](#_3.2_NGN_Site_1). It is imperative that the WAN links uphold, at a minimum, the current speeds and resiliency that are being provided. Ideally the supplier should enhance the WAN undelay options where feasible.
* Each NGN site will be equipped with resilient links operating within a HA configuration, specifically active/active, to ensure optimal bandwidth utilisation across both links. The underlay links may encompass various types, including MPLS, DIA, FTTC, FTTP, or other relevant services.
* The potential supplier must detail how they propose to migrate the existing WAN connectivity within FourNet’s cloud service platform into their own centralised environment.
* Clearly outline their strategy for ensuring a seamless and efficient transition from the current WAN service. It is imperative that continuity is maintained and disruptions to NGN services are minimised throughout this process.
* The potential supplier should offer scalable network solutions that can grow with the organisation’s needs. This includes the ability to add new locations, increase bandwidth, and integrate additional services without compromising performance or reliability.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract.

### **3.1.2 Software-Defined Wide Area Network (SD-WAN)**

The SD-WAN has been meticulously configured to optimise traffic routing within NGN. This optimisation is achieved through the implementation of SLAs that outline the management of traffic. Specifically, any traffic accessing the web or cloud infrastructure will be directed over the primary DIA link, while traffic destined for the on-premises environment will be routed via the primary MPLS link. This strategic configuration aims to reduce latency and alleviate the load on the central ISP.

The SD-WAN has been built to interconnect groups of connections, thereby providing a consistent service across various links. These links are consolidated into SD-WAN zones, which comprises physical or virtual interfaces. These interfaces can offer services that can be monitored through health checks and evaluated using SLAs.

The SD-WAN Zone are illustrated in appendix section: [3.3 SD-WAN Zones](#_3.3_SD-WAN_Zone)

The SD-WAN rules consist of application-specific or route-specific traffic identification criteria, which are measured using SLAs. There is always a default rule that will utilize all members of the SD-WAN configuration, serving as a fallback for any traffic not matched by the rulesets defined.

The selection of the circuit is contingent upon the specific service being accessed and the applicable ruleset. Certain rules are designed to optimise the use of maximum bandwidth, while others prioritise stability by employing consistent paths.

An implicit rule will ensure load balancing between both circuits based on the source IP address. Consequently, the source will maintain a consistent external IP address for outbound traffic.

A full list of NGNs SD-WAN Rules is in appendix section: [3.4 SD-WAN Rules](#_5.4_SD-WAN_Rules)

**Scope – SD-WAN:**

Potential suppliers must thoroughly address and consider the following requirements:

* Support the implementation of SLAs that outline the management of traffic, including:
  + Directing web or cloud traffic over DIA links to reduce latency and alleviate load on the central ISP.
  + Routing on-premises traffic via the MPLS links.
* Ensure a reliable and consistent service, including:
  + Offer the ability to interconnect groups of connections through SD-WAN zones, comprising physical or virtual interfaces.
  + Provide monitoring of services through health checks and evaluation using SLAs.
  + Support application-specific or route-specific traffic identification criteria.
* Must be able to support and implement routing and optimization rules effectively, including:
  + Implement default rules that utilize all members of the SD-WAN configuration, serving as a fallback for unmatched traffic.
  + Enable circuit selection based on the specific service being accessed and the applicable ruleset.
  + Optimise the use of maximum bandwidth through specific rules.
  + Prioritise stability by employing consistent paths for certain traffic types.
* Maintain efficient load distribution and source IP consistency, including:
  + Ensuring load balancing between circuits based on the source IP address.
  + Maintaining a consistent external IP address for outbound traffic from the source.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract

### **3.1.3 FortiGate Next Generation Firewall (NGFW)**

The FortiGate NGFW equipment at NGN locations currently comprises of the below:

|  |  |  |
| --- | --- | --- |
| Hardware Vendor | Type | Model |
| Fortinet | Physical | Fortinet FortiGate FG80F-POE – Desktop Firewall |
| Fortinet | Physical | Fortinet FortiGate FG200F – DC Firewall |
| Fortinet | Virtual | Fortinet FortiGate VM04 – Cloud Firewall |

A full hardware specification for the above equipment is in appendix section: [3.4 FortiGate NGFW Model Specification](#_3.4_FortiGate_NGFW)

The FortiGate NGFW are configured in HA (Active-Standby) design. The primary and secondary FortiGate NGFWs are configured in HA mode, ensuring that any changes are automatically synchronised between the two. The system continuously monitors the heartbeat, and in the event of a failure in the primary firewall, the secondary firewall will assume the primary role. This transition will remain in place until a manual failback is initiated, ensuring that the link is stable beforehand.

An illustration of the FortiGate NGFW HA design is in appendix section: [3.5 FortiGate NGFW HA Design Description](#_3.5_FortiGate_NGFW)

The FortiGate NGFWs are configured to provide DNS services for web filtering by utilising DNS lookups or a Captive Portal. The DNS service operates in recursive mode on specific interfaces, ensuring that DHCP settings direct DNS requests to the FortiGate NGFWs for Captive Portal setup. The FortiGate NGFW hosts a DNS database, managing Captive Portal DNS lookups from clients that receive the DHCP-assigned DNS addresses, and redirects them to the appropriate DNS Zone/URL when they attempt to browse.

DHCP is enabled on interfaces on the FortiGate NGFWs, the server can provide or relay DHCP requests defines as server or relay mode. These modes are enabled on the specific interfaces with specific templated DHCP ranges.

Each FortiGate NGFW is configured to use dynamic routing; however, there is still a requirement for static routes for Default, Cloud Services and MPLS traffic. Administrator settings for the FortiGate’s are used to see the administration port for remote access, the certificate and additional settings for which the FortiGate can be used to be administered.

FortiGate NGFW Policies and objects are configured and maintained from the FortiManager to maintain central configuration. They are 3 policies used throughout the NGN network. Each of these policies are made up of policy objects which are centrally maintained on the FortiManager. When making changes to the policies via manager, they must be pushed to the referenced FortiGate’s. The reason so few policies can be used is due to this centralisation, and due to policy ID’s being specifically targeted to individual FortiGate’s.

**Scope – FortiGate NGFW:**

Potential suppliers must thoroughly address and consider the following requirements:

* Ensure any proposed solution incorporates NGFW, with core functional requirements embedded in as part of any solution configuration. This includes but not limited to; Firewall capabilities, Intrusion Prevention System (IPS), Application Control, URL Filtering, SSL/TLS Inspection, Threat Intelligence and Endpoint Protection.
* To ensure optimal network performance and reliability, the evaluation of data throughput requirements, the capacity to handle concurrent sessions, and overall system stability are critical considerations. Furthermore, maintaining minimal latency, effectively managing network loads, and ensuring efficient capacity management are essential aspects of the network infrastructure.
* Ensure seamless network integration and full compatibility with an SD-WAN architecture. This includes robust interoperability with SaaS and cloud providers (AWS and Azure), in addition to third-party enterprise tools.
* NGFW policy and objects must be configured and maintained centrally on allowing for streamlined policy management and ensures consistency across the network environment.
* It is imperative that the NGFW uphold, at a minimum, the current design requirements being provided. Ideally the supplier should look at opportunities to enhance the NGFW services where feasible.
* The potential supplier is required to clearly outline their strategy for ensuring a seamless and efficient transition from the FourNet managed FortiGate NGFW services. It is imperative that continuity is maintained and disruptions to NGN services are minimised throughout this process.
* Continuous monitoring of the heartbeat between devices is critical. In the event of a failure, a secondary device should seamlessly assume the primary role until a manual failback is initiated, ensuring a stable and reliable network.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract.

### **3.1.4 Local Area Network (LAN & WLAN)**

The LAN and WLAN equipment at NGN 16 locations currently comprises of the below:

|  |  |  |
| --- | --- | --- |
| Hardware Vendor | Type | Model |
| Fortinet | Switch | Fortinet Switch 248E-FPOE |
| Fortinet | Switch | Fortinet Switch 224D-FPOE |
| Fortinet | Redundant Power Supply | FortiNet RPS 740 |
| Fortinet | AP | Fortinet FortiAP FAP-432F |

A full hardware specification for the above equipment is in appendix section: [3.6 LAN & WLAN Model Configuration](#_3.6_LAN_&)

**FortiSwitches (LAN):**

The FortiSwitches are connected to both FortiGate NGFWs through dual connections in a split link configuration, designed in an Active/Passive setup. Should the primary link experience a failure, the secondary link will immediately become active, thereby minimising any disruption to connectivity. Each FortiSwitch is interconnected with its neighbour through an inter-switch link, and an additional inter-chassis link is configured between the first and last member to enhance resiliency. In the event of a failure of a FortiSwitch within a branch LAN stack, connectivity to the remaining FortiSwitches is maintained, ensuring minimal disruption to NGN end-users.

FortiSwitch templates are held on the FortiManager and used to ensure the FortiSwitches meet the configuration build standard set out in the template each time the configuration is updated.

FortiAuthenticator services are deployed as a configuration to the FortiSwitches to enforce authentication services onto LAN, including Captive Portal and RADUIS for 802.1X certificate and LDAP authentication.

**FortiAPs (WLAN):**

The FortiAPs are designed to leverage WiFi6 architecture, providing enhanced connectivity and performance. They are strategically patched across multiple FortiSwitches within the branch stack to ensure greater resiliency. In instances where FortiAPs are in proximity, they are connected to different FortiSwitches, thereby maintaining coverage in the event of a hardware failure. This approach minimizes disruption to NGN end-users.

FortiAP profiles represent a collection of settings designated for a specific model of access point. These settings encompass the SSID, channel usage, authentication method, radio configuration, and, in certain cases, customization of the access point hardware.

The FortiAP profiles are distributed via FortiManager by assigning them to the respective access points.

FortiAuthenticator services are deployed as a configuration to the FortiAPs to enforce authentication services onto WLAN, including Guest Wireless, Captive Portal and RADUIS for 802.1X certificate and LDAP authentication.

A HLD of the current LAN & WLAN network design is in appendix section: [3.7 LAN & WLAN Design Topology](#_3.7_LAN_&)

A full list of current LAN & WLAN devices installed at each NGN locations is in appendix section[3.8 LAN & WLAN Device List](#_3.8_LAN_&)

**Scope – LAN & WLAN Network:**

The potential supplier will be required to consider the following responsibilities:

* Obtain full-service management of NGN's existing LAN & WLAN services.
* Ensure comprehensive sites surveys are carried out across all NGN sites (excluding third-party datacentres). The survey should detail the LAN and WLAN requirements of the proposed LAN and WLAN services.
* Essential that any proposed solution continues to adopt secure network authentication. This should include but not be limited to, Port-Based Network Access Control (802.1x) Extensible Authentication Protocols (EAP) and Dynamic VLAN assignment. This should also include Radius server integration, Certificate-Based Authentication and Guest access management capabilities.
* Ensure seamless network integration and full compatibility with NGFW and SD-WAN architecture. This includes robust interoperability with hardware, in addition to third-party enterprise tools.
* Ensure optimal network coverage, performance and reliability, the evaluation of data throughput requirements, the capacity to handle concurrent sessions, and overall system stability are critical considerations. Furthermore, maintaining minimal latency, effectively managing network loads, and ensuring efficient capacity management are essential aspects of the LAN and WLAN infrastructure.
* LAN and WLAN policy and objects must be configured and maintained centrally on allowing for streamlined policy management and ensures consistency across the network environment.
* The potential supplier is required to clearly outline their strategy for ensuring a seamless and efficient transition from the FourNet managed LAN & WLAN services. It is imperative that continuity is maintained and disruptions to NGN services are minimized throughout this process.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract.

### **3.1.5 FourNet Cloud Services Platform**

**FortiGaurd:**

The NGN FortiGaurd is deployed within FourNet’s cloud services platform. It enhances the security posture of the NGN network services by overlaying it with Secure Fabric SASE Architecture. Security Profiles utilise the FortiGaurd subscription within cloud services. These security profiles are used within NGN SD-WAN design and configurations to elevate protection. These include, but are not limited to:

* Anti-Virus
* Web & DNS Filtering
* Application Control.
* Intrusion Prevention
* SSL/SSH Inspection
* Application Signatures

**FortiManager:**

The NGN FortiManager is deployed within FourNet’s cloud services platform and is co-managed by both FourNet and NGN. FortiManager operates as a virtual machine, serving as a central management solution for multiple Fortinet devices, including FortiSwitch, FortiAP, and FortiGate within the environment. It employs SSL tunnels to establish a management tunnel, which can be either unidirectional or bidirectional. In a unidirectional state, the tunnel is initiated by either the FortiGate or the FortiManager, contingent upon a valid communication path and the availability of necessary services between the initiator and the recipient.

Furthermore, the FortiManager serves as the solution for template management, policy, and object management. It optimizes the usage of duplicate rulesets, manages the deployment templates for new devices, and facilitates change control management over configurations and assets.

**FortiAnalyser:**

The NGN FortiAnalyser is deployed within FourNet’s cloud services platform and is co-managed by both FourNet and NGN. The FortiAnalyser operates as a virtual machine that utilizes resources independent of the FortiManager. This solution is instrumental in the collection and analysis of logs, with storage being divided between analytical and archival data. Analytical data is retained for 30 days, during which it is used to generate reports, graphs, and graphical dashboards within Fortinet Fabric and FortiView. Furthermore, NGN’s FortiAnalyser is integrated with the FortiManager, enabling centralized management through the FortiManager graphical user interface.

**Virsae Service Management (VSM):**

VSM delivers a service management platform across multi-vendor communication applications. Leveraging big data analytics, artificial intelligence, automation, trending, and reporting. VSM simplifies the management of complex Unified Communications and Contact Centre environments.

The application is a shared front end SaaS Platform delivered from MS Azure, the data collected from the equipment is tenanted and hosted in the UK. Data stored in the cloud is protected with encryption at rest.

MS Azure prevents interaction between data by creating logical and physical separations. Storage is implemented by a shared infrastructure that isolates data through several mechanisms. VSM provides:

* A web portal that simplifies management and automates many manual processes related to data analytics and building reports.
* Detection of alerts in the form of event data. Processing and passing these events across to the FourNet management system.

Virsae has deployed a collector placed within the NGN environment. The VSM collector acts as an aggregator, compresses and encrypts the transport layer and then forwards data from all sources to the Virsae cloud computing service.

The data transmitted to the cloud will only be configuration data only and does not contain any customer or personal data. Virtual machine images (Collectors) contain no customer data, all data is stored in the cloud.

A HLD of the current LAN & WLAN network design is in appendix section: [3.9 Virsae Design Topology](#_3.9_Virsae_Design)

**Scope – Cloud Platform Services:**

Potential suppliers must thoroughly address and consider the following requirements:

* It is imperative that any supplier uphold, at a minimum, the current design requirements being provided. Ideally the supplier should also evaluate opportunities to enhance the cloud service offerings where feasible with their alternative solution proposals.
* Provide a comprehensive strategy that outlines how they will look to migrate the full management of the services being provided by FourNet within their cloud services platform.
* Key consideration should be given to the underlay network build and configuration. Providing insights into how the potential new supplier can replace the services in situ. It is imperative that continuity is maintained and disruptions to NGN services are minimised throughout this process.
* The potential supplier should demonstrate high proficiency in configuring and managing such services outlined, ensuring the Security Fabric SASE Architecture is maintained or enhanced in your proposed solution.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract.

### **3.1.6 Voice Unified Comms (UC) & Contact Centre (CC)**

**MS Teams Telephony Direct Routing:**

The UC has been designed by integrating MS Teams Telephony, enabling NGN to use our existing Microsoft Teams licenses, as part of NGNs wider MS O365 E5 license agreement. This will allow NGN to cater for business stakeholders that require a traditional land line number.

With MS Teams Telephony, NGN stakeholders can securely access the service from any location whilst continuing to benefit from high quality of calls and interactions. The service is provided directly through FourNet’s cloud services platform. The Gamma SIP Trunks are configured in an active/passive design, ensuring a high level of resiliency.

Integration of MS Tiger Prism into the UC solution, helping NGN to manage and analyze communication data effectively, providing insights into usage patterns and assist in ongoing optimization of the UC services.

**Sip Trunk Call Manager:**

The configuration of the SIP Trunk Call Manager (STCM) is to enhance the UC and CC services, providing HA and resilient communication infrastructure, whilst supporting NGN Business Continuity Management (BCM) processes.

The system details all the NGN telephone numbers and where they point to. This is so that in the event of a major incident whereby the CC has a major failure, NGN can continue to operate using the configured business continuity setup. This is achieved through the STCM by diverting call flows to mobile phones.

The business continuity diverts are all pre-configured on the STCM platform and would just require administrators activating/deactivating on request.

This has been setup primarily for the CC system key NGN key business stakeholders, ensuring they are diverted to mobile phones.

**Nice CXone CCaaS:**

NGN has implemented the Nice CXone InContact Omnichannel CC platform. It has been delivered as a CXone Contact Centre as a Service (CCaaS), leveraging the FourNet cloud services platform network services built, as part of the overarching Voice UC network architecture. The key services adopted through the CCaaS are:

* **CXone CCaaS**: This is the core component of the solution, providing the cloud-based contact center functionalities.
* **Agent Interface**: Known as MAX, this interface is designed for agents to handle customer interactions efficiently.
* **Centralized Administration**: This component allows for the centralized management of the contact center, including configuration and administration tasks.
* **CXone Supervisor**: This interface is for supervisors to monitor and interact with agents, ensuring smooth operations and high performance.
* **Call Recording**: This feature enables the recording of calls for quality assurance and compliance purposes.
* **Reporting and Dashboards**: These tools provide insights and analytics on contact center performance, helping in decision-making and strategy planning.
* **CXone Automatic Contact Distributor (ACD)**: This component manages the distribution of incoming contacts to the appropriate agents based on predefined rules.
* **Interactive Voice Response (IVR)**: This system allows customers to interact with the contact center through voice prompts and keypad inputs, streamlining the process of routing calls.
* **Studio**: This is a tool for designing and managing call flows and scripts, enabling customization of the contact center operations.

A HLD of the current voice network design is in appendix section: [3.10 Nice CXone CC HLD Design](#_3.10_Nice_CXone)

**Scope – Voice Unified Comms (UC) & Contact Centre (CC)**

Potential suppliers must thoroughly address and consider the following requirements:

* In the interest of maximising our existing technology stack and commercial licensing agreements, it is imperative that the potential supplier ensures any UC solution continues to utilise MS Teams Telephony Routing.
* It is imperative that any supplier uphold, at a minimum, the current CC requirements as they being provided. Ideally the supplier should also evaluate opportunities to enhance the CC offerings where feasible with their alternative solution proposals.
* It is crucial that any proposed solution includes a robust HA system comparable to the current STCM. Ensuring NGN BCM procedures can be effectively followed in the event of any significant degradation of UC or CC services.
* Provide a comprehensive strategy that outlines how they will look to migrate full management of the voice services (UC and CC) being provided by FourNet within their cloud services platform and Nice CXone partner Cloud Platform.
* Key consideration should be given to the underlay network build and configuration. Providing insights into how the potential new supplier can replace the services in situ. It is imperative that continuity is maintained and disruptions to NGN services are minimised throughout this process.
* The potential supplier should demonstrate high proficiency in configuring and managing UC and CC services, ensuring the Security Fabric SASE Architecture is maintained.
* NGN would like the potential supplier costs for the management of these services to be broken down into non-recurring cost (NRC), that is one-off charges and monthly recurring revenue (MRR) for the duration of the contract.

### 3. APPENDIX

## 3.1 NGN WAN Physical Configuration

A diagram of a computer network

Description automatically generated

The illustration shows the physical network WAN topology, it offers a high-level schematic view of the physical network elements being provided by Virtual1 and FourNet.

Each site is provided with connectivity to the services being provided by FourNet cloud services platform via existing infrastructure in the FourNet data centre campus.

The below illustrations highlight the physical configuration of the various NGN site profiles provisioned, as part of WAN service.

**Standard Sites:**

A diagram of a computer

Description automatically generated

The above illustration provides a lower-level topological view of WAN connections and LAN handoff configuration for all NGN Standard Site services.

Each Standard Site is provided with the following CPE and access services.

|  |  |  |
| --- | --- | --- |
| Primary | Fibre Ethernet | Juniper NFX150 |
| Primary | Fibre Ethernet | Juniper NFX150 |

Each Standard Site access service is configured with a single-link DIA service presenting a public /29, and a single MPLS (External Border Gateway Protocol (eBGP) on the LAN) service handing off on a /30 subnet.

Each MPLS service is delivered within the rack to the FourNet FortiGate NGFW using physical interface on the Virtual1 Juniper. This port is configured as a routed port with a single /30 subnet. Virtual1 configure the first IP in the subnet as the Juniper IP (which is used as the default gateway on the FortiGate devices for this access service). Additionally, an eBGP peer is configured on this connection between the FourNet FortiGate NGFW and Virtual1 Juniper NFX150 to enable dynamic routing updates.

Virtual1 do not filter routes within end-user MPLS VRFs, they advertise all connected subnets, routed subnets, plus link and management subnets to the FourNet FortiGate over each BGP peer.

**Standard Datacentres:**

A diagram of a computer

Description automatically generated

The above illustration provides a lower-level topological view of WAN connections and LAN handoff configuration for all NGN Standard Datacentres services.

Each Datacentre Site is provided with the following CPE and access services.

|  |  |  |
| --- | --- | --- |
| Primary | Fibre Ethernet | Juniper NFX150 |
| Primary | Fibre Ethernet | Juniper NFX150 |

Each Standard Datacentre access service is configured with a single MPLS (eBGP on the LAN) service only, handing off on an /30 subnet. Virtual1 provides Fibre Ethernet access services that terminate in the Datacentre’s Meet Me Room (MMR). These locations are off-net to Virtual1, and they cannot deliver a cross-connect between the MMR and NGN/NGN Partner Rack. NGN provision the required 3rd party cross-connect. This cross-connect terminates on the WAN interface of the Juniper NFX150, which will be hosted within the NGN/NGN Partner Rack.

Each MPLS service is delivered within the rack to the FourNet FortiGate NGFW using physical interface on the Virtual1 Juniper. This port is configured as a routed port with a single /30 subnet. Virtual1 configure the first IP in the subnet as the Juniper IP (which is used as the default gateway on the FortiGate devices for this access service). Additionally, an eBGP peer is configured on this connection between the FourNet FortiGate NGFW and Virtual1 Juniper NFX150 to enable dynamic routing updates.

**Arqiva Datacentres:**

As with the Standard Datacentre deployment, each Arqiva location is provided with a single MPLS (eBGP on the LAN) service only, handing off on an /30 subnet.

Arqiva’s supported deployment has only a single circuit at each location which differs from the resilient services supplied to the Standard Datacentres.

Arqiva treat Braham Street as the primary site and Telehouse North as secondary, and they will prefer/de-prefer paths using BGP. Virtual1 accept and honour these paths based on the BGP information we receive to ensure all traffic is routed to Braham Street under normal operation. The BGP configuration upon the Virtual1 CPE remains consistent with all other deployments in this scenario.

A computer screen shot of a diagram

Description automatically generated

The above illustration provides a lower-level topological view of WAN connections and LAN handoff configuration for the Arqiva Braham Street site only.

The Arqiva Telehouse location is provided with the following CPE and access service.

|  |  |  |
| --- | --- | --- |
| Primary | Fibre Ethernet | Juniper NFX150 |

A diagram of a computer

Description automatically generated

The above illustration provides a lower-level topological view of WAN connections and LAN handoff configuration for the Arqiva Telehouse site only.

As Virtual1 are on-net in this location they provide the services as Network Ports with Virtual1 cross-connects directly from there rack locations into the NGN racks, rather than a Fibre Ethernet access circuit.

The Arqiva Telehouse location is provided with the following CPE and access service.

|  |  |  |
| --- | --- | --- |
| Primary | Network Port & Cross-connect | Juniper NFX150 |

**FourNet Cloud Services Platform:**

FourNet provide and manage several services from within their cloud services platform, these are deployed using the existing infrastructure services held between Virtual1 and FourNet.

A diagram of a virtual network

Description automatically generated

The above illustration provides a high-level topological view of the existing resilient connections between the Virtual1 core and FourNet cloud services platform that is utilised by NGN. Resilience is provided by primary, secondary and tertiary BGP peers in geographically diverse data centres.

**NGN AWS Cloud Services:**

Virtual1 facilitate connectivity to our major public cloud providers by leveraging one of two IaaS partners. This connectivity allows NGN and our end-users private, resilient, on-net, connections into NGN AWS public cloud environment via an MPLS VRF

A logo with a white background

Description automatically generated with medium confidence

Connectivity between Virtual1 and the AWS cloud services is delivered as a layer-3 service, using BGP to provide resilient and dynamic routing updates. The BGP peers are configured directly between the Virtual1 Edge and the AWS cloud platform to form a private MPLS VRF that can in turn be connected to AWS locations or into layer-3 Partner Connects.

Virtual1 have configured connectivity within the Virtual1 Edge and Core and NGN/FourNet have configured the public cloud environment.

Virtual1 do not apply filters to routes within NGNs MPLS VRFs. They advertise all connected subnets, routed subnets, plus link and management subnets within the VRF towards the AWS cloud environment.

In return, the NGN/FourNet advertise all prefixes within the AWS public cloud environment to Virtual1 over each peer, Virtual1 is responsible for propagating routes to these prefixes throughout the MPLS VRF.

**Internet Breakout:**

To ensure Virtual1 can provide fast and resilient Internet transit to NGN, Virtual1 peer with the global carriers, Lumen, Cogent, and Hurricane Electric in multiple locations in both London and Manchester. They also peer with the London Internet eXchange (LINX) and The London Access Point (LONAP) to provide direct connectivity into many other ISPs, Content Delivery Networks (CDNs) and enterprises. Additionally, where possible, they aim to peer directly with the businesses where we see the most traffic.

A diagram of a computer network

Description automatically generated

## 

## 3.2 NGN Site Connectivity

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Location | Postcode | Site Type | Primary Carrier | Secondary Carrier | Resiliency Type |
| Bradford | BD8 9RL | Branch | Virgin  100Mbps/1GB | BT Wholesale  100Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Burradon | NE12 5UJ | Branch | BT Wholesale  100Mbps/1GB | Virtual1  100Mbps/1GB | Carrier-Diverse (Same  Exchange) |
| Cannon Park | TS1 5JH | Branch | Virtual1  100Mbps/1GB | Virgin  100Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Carlisle | CA2 7AF | Branch | BT Wholesale  100Mbps/1GB | TalkTalk  100Mbps/1GB | Carrier-Diverse (Same  Exchange) |
| Ceva Logistics | DL5 6XQ | Branch | N/A | N/A | Partner ISDN |
| Doxford Park | SR3 3XR | Branch | Virtual1  200Mbps/1GB | Virgin  200Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Elland | HX5 9DA | Branch | Virtual1 - Openreach  100Mbps/1GB | Virtual1 - Openreach  100Mbps/1GB | Primary / Failover (RO2) |
| Felnex | LS9 0SR | Branch | CityFibre  100Mbps/1GB | BT Wholesale  100Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Hull | HU5 1SB | Branch | BT Wholesale  100Mbps/1GB | BT Wholesale  100Mbps/1GB | Dual Connections (Same Exchange) |
| Low Thornley | NE21 6LE | Branch | Virtual1  200Mbps/1GB | Virtual1  200Mbps/1GB | Primary / Failover (RO2) |
| Low Thornley NeRV |
| Pontefract | WF8 2JJ | Branch | Virtual1  100Mbps/1GB | Virtual1  100Mbps/1GB | Primary / Failover (RO2) |
| Scarborough | YO11 2YH | Branch | BT Wholesale  100Mbps/1GB | TalkTalk  100Mbps/1GB | Carrier-Diverse (Same  Exchange) |
| Thorpe Park | LS15 8TU | Branch | BT Wholesale  400Mbps/1GB | BT Wholesale  400Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Washington | NE37 3HP | Branch | BT Wholesale  200Mbps/1GB | Virgin  200Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Workington | CA14 4PW | Branch | Virtual1  115Mbps/1GB | N/A | Single FTTP (RO2) |
| York | YO26 6RU | Branch | BT Wholesale  100Mbps/1GB | TalkTalk  100Mbps/1GB | Carrier-Diverse (Same  Exchange) |
| AWS Direct Connect - PRI | SL1 4AX | Public Cloud | Console Connect  1GB | N/A | Cloud Exchange |
| AWS Direct Connect - SEC | E14 2AA | Public Cloud | Console Connect  1GB | N/A | Cloud Exchange |
| National Gas Transmission (CNI) - PRI | GU14 0LH | Partner DC | Virtual1  100Mbps/1GB | Virgin  100Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| National Gas Transmission (CNI) - SEC | SN13 9GB | Partner DC | Vodafone  100Mbps/1GB | Virgin  100Mbps/1GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| National Gas Transmission (Business) - PRI | TW14 0XQ | Partner DC | BT Wholesale  100Mbps/1GB | N/A | Single Fibre Ethernet |
| National Gas Transmission (Business) - SEC | E14 9TR | Partner DC | Virtual1  100Mbps/1GB | N/A | Single Fibre Ethernet |
| Cadent Gas - PRI | TW14 0XQ | Partner VPN | N/A | N/A | N/A |
| Cadent Gas - SEC | E14 9TR | Partner VPN | N/A | N/A | N/A |
| Arqiva - PRI | E1 8EE | Partner DC | Virgin  100Mbps/1GB | N/A | Single Fibre Ethernet |
| Arqiva - SEC | E14 2AA | Partner DC | Telehouse  100Mbps/1GB | N/A | Single NNIs/Cross Connect |
| Cloud Services - Central Internet Break |  | FourNet | 10GB | 10GB | Carrier-Exchange  Diverse (Different  Exchanges) |
| Cloud Services | Central Service | FourNet | N/A | N/A | N/A |

**Site Types:**

Branch - A standard NGN site

Spares - Highlight any resilient standby equipment.

Public Cloud - Amazon Web Services domain, NGN hosted cloud applications (IaaS)

Partner DC - Data Centre (DC) where NGN interconnect with a partners

Partner VPN - NGN partners, connected via VPN rather than with a physical connection.

Cloud Services - Access to FourNet cloud platform (SaaS), hosting several Fortinet applications connected into NGN

**Network resiliency:**

Carrier-Diverse (Different Exchange)

Different carriers, terminating into different exchanges

Carrier-Diverse (Same Exchange)

Different carriers, terminating into the same exchange.

RO2

Connection provided on Openreach circuits, terminating into different exchange. Where available, the circuits will route into the building via different ducts.

Single NNIs

Cabling will be delivered by the DC, routing from between the NGN rack in the DC to carrier rack.

Single Fibre Ethernet  
Single, no resilient fibre ethernet connection.

Single FTTP  
Single, no resilient fibre to the site connection.

Partner ISDN

Single, no resilient Integrated Services Digital Network line, provided by the 3rd party

## 3.3 SD-WAN Zone

|  |  |  |
| --- | --- | --- |
| Virtual-wan-link Type | Physical Interfaces | Gateway |
| DIA1 | Hardware Switch Port1, port3 | ISP1 DIA Gateway |
| DIA2 | Hardware Switch Port2, Port4 | ISP2 DIA Gateway |
|  | | |
| SD-WAN Type | Physical Interfaces | Gateway |
| MPLS1 | Hardware Switch A, port5 | ISP1 MPLS Gateway |
| MPLS2 | Hardware Switch B, port6 | ISP2 MPLS Gateway |

## 5.4 SD-WAN Rules

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Reason | Measurement | Preference |
| FourNet Cloud Services | Internal IP addresses going to Agile Cloud | Max Bandwidth utilisation | MPLS1 - \*, MPLS2 |
| Internal | Internal IP addresses | Lowest Cost link | MPLS1 - \*, MPLS2 |
| Office 365 | Internal going to Office 365 Applications | Best quality link based on Latency | DIA1 - \*, DIA2 |
| Internet | All traffic going to the internet except to RFC1918 and Blacklisted addresses | Maximum bandwidth with link latency to Google DNS | DIA1 - \*, DIA2 |
| Default | All Source IP | load balanced | All |

**Implicit rule:**

Will load balance between both circuits based on the source IP. This means the source will

get a consistent external IP address for outbound traffic.

**Rule 1:**

Is the default internet rule, this is currently balanced across both circuits for the internet, this is

based on maximum bandwidth, and utilises the bandwidth applied to the interfaces. Currently these

are set equal, however the as an example if a new circuit is 400Mbps as opposed to the 200Mbps on

the original. Currently the bandwidths are set as default, so they will be balanced based on usage of

equal cost currently, you will not get the full ratio of balance of a 400Mbps to 200Mbps (2 to 1) as its

currently set as default.

**Rule 2:**

This looks at internal traffic using the MPLS links and is all RFC1918 based traffic for AWS and

site-to-site. This is using Lowest cost based on the SLA’s being performed for Latency, packet loss and

Jitter. Like the Office 365, it will only use 1 link at a time and is good for ensuring a stable link that is

consistent.

**Rule 3:**

Fournet cloud services, this is the Internal Traffic to NGNs FourNet cloud instance. Like the default

internet rule, this uses maximum bandwidth utilisation and will use both links simultaneously.

**Rule 4:**

Looks at Office 365 traffic, this currently selects the best quality link to Office 365, so does not

use bandwidth optimisation, but the most stable link for all traffic. Currently DIA1 link will be used for all

office traffic.

## 3.4 FortiGate NGFW Model Specification

The following is the specification of the Fournet certified Firewall configuration:

Firewall Configuration 1:

A screenshot of a computer

Description automatically generated

Firewall Configuration 2:

A computer screen shot of a computer

Description automatically generated with medium confidence

Firewall Configuration 3:

A screenshot of a computer

Description automatically generated

## 3.5 FortiGate NGFW HA Design Description

## A diagram of a computer network Description automatically generated

The above diagram shows the independent links coming in from each carrier in the majority of sites

The independents links have a reliance on the corresponding FortiGate NGFW, as they utilised a hardware switch to carry the communication over a link to the other FortiGate NGFW.

e.g. DIA 1 – The red link comes in via DIA 1, Juniper 1, and then terminates in firewall 1. Firewall 1 then

has a switched connection to the second FortiGate. This places a reliance on FortiGate 1 to be powered up to

allow the secondary to communicate over the circuit.

Should a HA failover occur, the configuration is replicated to the second FortiGate exactly, meaning IP addresses, MAC addresses etc are identical. If both firewalls are powered up, both circuits will be physically able to communicate to either firewall.

This design decision allows the clear line of demarcation for WAN connectivity, meaning there is no managed switch used on the internet facing communication path.

## 3.6 LAN & WLAN Model Specification

The following is the specification of the Fournet certified Switch configuration:

Switch Configuration 1:

A white box with a white label

Description automatically generated with medium confidence

Switch Configuration 2:

A computer switch with a white box

Description automatically generated with medium confidence

RPS Configuration:

A screenshot of a computer

Description automatically generated

Wireless AP Configuration:

A close-up of a computer device

Description automatically generated

## 3.7 LAN & WLAN Design Topology

Below is a HLD illustration of the LAN & WLAN network design:

A diagram of a computer network

Description automatically generated

Below is illustrates the low-level topology of the NGN LAN configuration:

A diagram of a lan setup

Description automatically generated

## 3.8 LAN & WLAN Device List

The network hardware components listed below are intended to support a resilient single-site deployment.

These are share components across all the NGN environments listed throughout the PQQ document.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | FortiGate Qty | FortiSwitch Qty | RSP Qty | FortiAP Qty | SFP+ Qty | Comment |
| Bradford | 2 | 2 | - | 2 |  |  |
| Burradon | 2 | 2 | - | 5 |  |  |
| Cannon Park | 2 | 2 | - | 4 |  |  |
| Carlisle | 2 | 2 | - | 5 |  |  |
| Ceva Logistics | 1 | 1 | - | - |  |  |
| Doxford Park | 2 | 8 | 4 | 6 | 24 | Switch configuration 1 deployed |
| Elland | 2 | 2 | - | 6 |  |  |
| Felnex | 2 | 2 | - | 6 |  |  |
| Hull | 2 | 2 | - | 5 |  |  |
| Low Thornley | 3 | 3 | 1 | 8 |  |  |
| Low Thornley NeRV |  |  |
| Pontefract | 2 | 2 | - | 4 |  |  |
| Scarborough | 2 | 2 | - | 1 |  |  |
| Thorpe Park | 2 | 11 | 6 | 21 | 30 |  |
| Washington | 2 | 2 | - | 5 |  |  |
| Workington | 1 | 1 | - | 1 |  |  |
| York | 2 | 2 | - | 2 |  |  |
| AWS Cloud Service | 2 | - | - | - |  | VDOMS |
| National Gas Transmission (CNI) - PRI | 2 | - | - | 1 | 1 |  |
| National Gas Transmission (CNI) - SEC | 2 | - | - | 1 | 1 |  |
| National Gas Transmission (Business) - PRI | 1 | - | - | 1 | 1 |  |
| National Gas Transmission (Business) - SEC | 1 | - | - | 1 | 1 |  |
| Arqiva - PRI | 1 | - | - | 1 | 1 |  |
| Arqiva - SEC | 1 | - | - | 1 | 1 |  |
| FourNet Cloud Services | 2 | - | - | - |  | VDOMS |

## 3.9 Virsae Design Topology

Below is a HLD illustration of the Virsae design

A diagram of a computer

Description automatically generated

Below is a low-level illustration of the Virsae design

A diagram of a network

Description automatically generated

## 3.10 Nice CXone CC HLD Design

Below is a HLD illustration of the UC and CC design:

A diagram of a computer network

Description automatically generated

Nice CXOne Contact Centre is provided by FourNet as the service and support partner of Nice. IVR/ACD and CTI systems are hosted by Nice within the Nice AWS Cloud, and Voice with Switching services are hosted within the Nice Private cloud.

Agents are provided with an agent desktop for customer contact agents. The customer contact agent connects directly to the Nice private cloud for system administration and call control.

SIP connectivity is backed off to Fournet for better call control, and cost savings providing the advantages for number porting, PSTN call costs and additional service integrations as part of the FourNet’s cloud services solution.

A diagram of a cloud network

Description automatically generated

The Nice voice solution provides CPAP with BGP route advertisement between the Slough and Manchester FourNet Datacentres.

NGN Have a dedicated SBC with a /29 assignment subnets that is advertised back to Nice CXone. This provides the connection for CX One to reach Gamma for PSTN calls utilising the Fournet interconnects for better call cost flexibility using call plans.

DDIs for the ingress are provided by Fournet utilising Gamma to allow incoming calls.