

Service Description:

TNP Cloud Connect is a user-friendly, high-quality, free to use wireless service that gives public & visitors access to the internet. The solution is a secure, high-capacity system that utilises existing infrastructure rather than overlaying additional wireless equipment and is compatible with all device types such as smart phones, tablets and PCs.

The service is accessed through an easy-to-use portal and made available to all users through either social media login or text message allowing for an accurate audit trail.

Compliance is achieved by segregating visitor and staff traffic and enabling monitoring for misuse of the service.

The solution is completely scalable and not restricted to a limited number of locations served or access points, safeguarding against additional costs that may arise from usage and capacity limits. It can be delivered using a Cloud based or an on premise authentication and filtering infrastructure allowing flexibility for high availability and truly scalable architecture.

Benefits

- ➔ User registration based on social-media authentication (Facebook, Twitter, LinkedIn) or text message based registration.
- ➔ Multiple, customisable landing pages/portals
- ➔ Responsive interface for mobile devices.
- ➔ Compliant and auditable.
- ➔ Requires user identification, acceptance of AUP and logs all accesses from the network.
- ➔ Web traffic is filtered to avoid unsuitable content.
- ➔ Bulk traffic such as bit torrent can be limited in available throughput to avoid causing network slow-downs for other users.
- ➔ Overall traffic rate limits and per-user limits can be configured if desirable.
- ➔ Fully monitored.
- ➔ Configurable user session times

Core and Supplementary Components

The core component of this service allows the customer to form a secure tunnel from their wireless infrastructure across the internet to the TNP CloudConnect platform. Included with the service is a high-availability pair of encryption endpoints/CPE to form this tunnel.

Per Site

This element is for the initial setup of the solution including installation and 6 hour fix SLA of a pair of IPSec endpoint devices to establish a secure tunnel from your wireless guest network to our cloud solution. This is priced per site, but normally this would only need to be located at the site of the wireless controller installation which would normally be the datacentre. If wireless controllers are located split across two datacentres, then a HA or multisite deployment would be required. There is no limitation on the number of buildings served or APs.

Portal Charge per 1,000 concurrent users

The solution is sized based on blocks of 1,000 concurrent users and 100Mb of bandwidth usage. The user limit is not a hard limit; our solution will allow more but we can't guarantee the service if this is exceeded. You can, however, request we set a hard limit if desirable. Additional 1,000 blocks can be added to an existing system as required, so this doesn't need to be sized for long term expectations.

Custom Portals

Multiple web redirect portals can be configured to be supported, these can have different look and feel to the portal, or different web filtering configurations. These are configured by adding multiple VLANs to the IPSec handover devices allowing the customer to configure SSID or Location to VLAN mapping.

A basic configuration and look & feel to the web redirect landing page (background colour, logo, text) is included, where a bespoke design is required, TNP will provide templates and can work with the customers own web design team.

SMS Charges

SMS usage should be fairly low as normally users would be pushed to use social media logins primarily. SMS credits can be purchased in blocks.

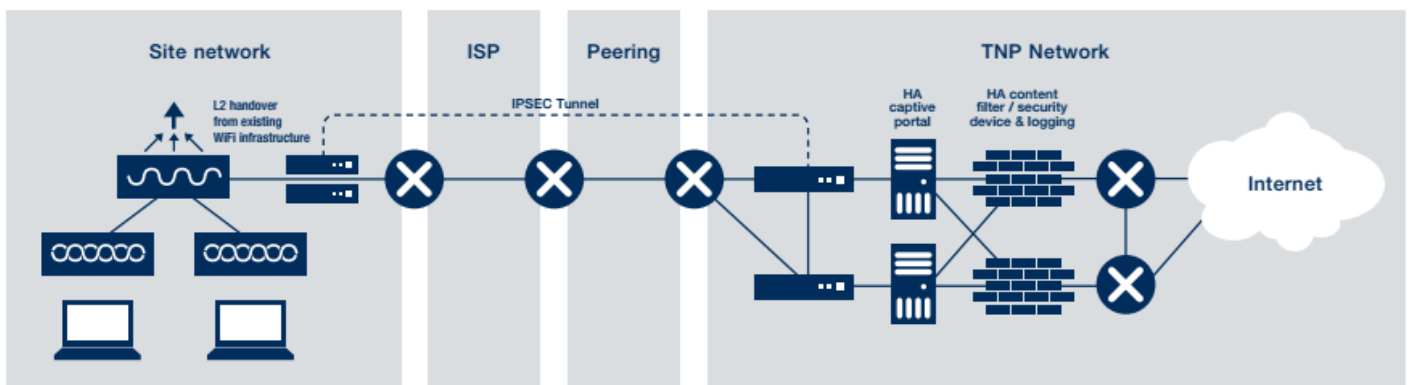
Virtual Internet Connection

Where an organisation wishes to securely segment traffic away from their primary Internet connection to meet either compliance, segregation or constraints from an existing provider, a virtual Internet connection can be provided via a port on the provided IPSec endpoints. This virtual Internet connection will then run over the secure tunnel to the TNP core, providing isolation from any existing provider and IP addressing. A single, static and unfiltered IP address will be provided for the customer to undertake their own firewalling & distribution.

Service Features

- ➔ Base capacity of 1,000 concurrent users/100Mb/s of traffic
 - Upgradable in blocks of 1,000 concurrent users
- ➔ Pair of HA encryption endpoints/CPE
- ➔ Fully Managed Service
 - Managed installation
 - Customer Management Centre – centralised fault reporting
 - Service Level Agreement and Maintenance Levels as noted in the SLA below

Infrastructure



Lead Times

The standard provisioning lead time for the Services is up to 35 working days subject to survey and the type/amount of work required to enable the service. TNP will make an assessment at the initial planning stage to determine exact lead time.

Billing

TNP will bill for the services in advance on an annual basis.

Conditions on the Customer

This solution is for a customer network based in the UK.

Outline Implementation Plan

Stage	Timescale
Contract Award	
Kick-off meeting	+1 week
Order equipment	+1 week
Technical Requirements review ➔ Confirm number of VLANs ➔ Confirm SSID(s) ➔ Confirm RF-level traffic shaping (if required) ➔ Confirm public & private IP addressing for NTE & tunnel endpoint ➔ Confirm available datacentre space & power ➔ Confirm portal customisations required	+2 weeks
Equipment delivery & pre-stage	+4 weeks
Portal wireframes/proofs approval	+6 weeks (subject to timely confirmation from customer)
Physical/Remote-hands Installation ➔ Commission VPN tunnel ➔ Test to directly-connected laptop ➔ Customer to configure test SSID and restrict broadcast to testing area.	+8 weeks
Soft Launch ➔ Final approval and installation of portal ➔ Customer to make visitor wifi SSID available in restricted area	+10 weeks
Full Launch ➔ Customer to make visitor SSID fully available	Once Customer is happy with soft launch

Service Level Agreement

The SLA and associated support is provided to the purchasing organisation and its IT staff. End-user support is not a component of this service

General Provisions

TNP will provide support and advice, under this SLA, on matters relating to:

- ➔ Availability of the Services
- ➔ Quality of the Services
- ➔ Provisioning
- ➔ Essential downtime
- ➔ Customer support
- ➔ Complaints handling
- ➔ Accurate and timely invoices

TNP acknowledges that failure to meet the Service Level Thresholds as set out in this SLA will result in Service Credits being due to the Customer.

Service Levels

The following Service Level Performance Criteria apply:

- ➔ **Availability.**
 - Network Availability of 99.5%
 - Service Desk Availability of 99%

- ➔ **Incident Resolution.** With a time to restore Service to a customer as set out below.
- ➔ **Quality.** TNP commits to answering all calls within 60 seconds and responding to every properly reported fault within one working hour (including emails) of notification to the TNP CMC (Customer Management Centre).
- ➔ **Provisioning.** TNP commits to provisioning the Services in accordance with the Implementation Plan.

Service Maintenance Level and Agreed service time

Service Maintenance for the Services has an Agreed Service Time of Monday to Friday (excluding Bank Holidays) 08:00-18:00.

Severity Levels

The following Severity Levels apply:

Severity 1 - The Services are Unavailable across the entire Customer's estate

Severity 2 - The Services are Unavailable at one of the Customer's sites

Severity 3 - The Services are Unavailable to an individual user

Severity 4 - All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Customer or in any other way not attributable to TNP.

Incident resolution times

The Service Maintenance Level for the Services is subject to the following Incident Resolution Times:

- ➔ Severity 1 – 6 working hours
- ➔ Severity 2 - End of Next Working Day
- ➔ Severity 3 – Five Working Days
- ➔ Severity 4 (Indicative Only) – One Month

Service level Thresholds

The following Service Level Thresholds apply:

- ➔ Availability Service Level Threshold - Services - Not applicable
- ➔ Availability Service Level Threshold- Service Desk = 99%
- ➔ Incident Resolution Service Credit (39 or less incidents per Service Period) = No more than 2 Incidents are Resolved in excess of the max Incident Resolution Times
- ➔ Incident Resolution Service Credit (40 or more incidents per Service Period) = $(0.25 \times (95-PC) + 2.5)$ to a maximum of 5%
- ➔ Quality Service Credits – Service Desk
 - Calls Answered within 60s = $(0.25 \times (90-PC) + 2.5)$ to a maximum of 5%
 - Email Responded to within 1 day = $(0.083 \times (95-PC) + 2.5)$ to a maximum of 5%
 - Abandoned Calls = $(0.25 \times (95-PC) + 2.5)$ to a maximum of 5%

Service Failure Thresholds

The following Service Failure Thresholds apply:

- ➔ Availability Service Failure Threshold – Services - Not applicable
- ➔ Availability Service Failure Threshold- Service Desk = 95%
- ➔ Incident Resolution Service Failure Threshold (39 or less incidents per Service Period) = 5 or more Incidents are Resolved in excess of the max Incident Resolution Times
- ➔ Incident Resolution Service Failure (40 or more incidents per Service Period) = 85%
- ➔ Quality Service Failure Threshold – Service Desk
 - Calls Answered within 60s = 80%
 - Email Responded to within 1 day = 60%
 - Abandoned Calls = 85%

Critical Service Failure Definition

- ➔ A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Failure Threshold on three (3) occasions in any six (6) consecutive Service Periods.
- ➔ In the event of a Critical Service Level Failure, the Customer shall be entitled to terminate the Contract for material Default.

Service Credits

Where the level of performance of TNP in the provision by it of the Services during the Contract period fails to meet the applicable Service Level Threshold then Service Credits are available and calculated using the formulae set out below. Service Credit payments are subject to the Service Credit Caps indicated as a maximum percentage.

Service Credit Due (£) = Contract Charge (£) x Service Credit (%)

- ➔ Availability Service Credit– Services - Not applicable
- ➔ Availability Service Credit - Service Desk = $(5 \times (99-PC) + 5)$ to a maximum of 25%
- ➔ Incident Resolution Service Credit (39 or less incidents per Service Period) = 2.5% payable for 3 incidents in breach of the Service Level Threshold in any Service Period to a maximum of 5% payable when 4+ incidents are in breach of the Service Level Threshold in any Service Period
- ➔ Incident Resolution Service Credit (40 or more incidents per Service Period) = $(0.25 \times (95-PC) + 2.5)$ to a maximum of 5%
- ➔ Quality Service Credits – Service Desk
 - Calls Answered within 60s = $(0.25 \times (90-PC) + 2.5)$ to a maximum of 5%
 - Email Responded to within 1 day = $(0.083 \times (95-PC) + 2.5)$ to a maximum of 5%
 - Abandoned Calls = $(0.25 \times (95-PC) + 2.5)$ to a maximum of 5%

Where *PC* is the Achieved Service Level Performance Criteria (%) for a Service Period.

Service Period

The Service period is defined as the recurrent period of one month during the term of the Service provision.

Service Level Guarantee Exclusions

The following items (which are not exhaustive) will either temporarily 'stop the clock' for the purposes of the Service Level Guarantee or prevent payment of Service Credits:

- ➔ TNP or its contractors are unable to gain access to the end user premises or carry out any work
- ➔ The incident is the result of a failure of third party equipment
- ➔ Access is not available when required by TNP
- ➔ Customer fails to respond in a timely fashion to an enquiry from TNP
- ➔ Customer fails to accept first appointment offered by TNP
- ➔ There is action by the Operator, end user or a third party which prevents TNP from completing its obligations
- ➔ There is Scheduled or Emergency Maintenance service interruption
- ➔ The fault is the subject of an inaccurate fault report
- ➔ The fault is due to Force Majeure
- ➔ Delay in the acceptance of necessary infrastructure build out charges for installations, upgrades or remedial works

TNP may suspend the Service from time to time for necessary technical reasons and network upgrades. Scheduled Maintenance will be published to a designated contact at organisations with 2 weeks advance notice. In extreme circumstances where a loss of Service is likely without intervention, emergency maintenance for an identified purpose may be carried out where two weeks' notice is not possible.

Escalation Levels

If the Customer is at any time unhappy with the level of quality of support provided by the TNP CMC or with any aspect of the Service, the escalation path below will apply:

Escalation Level 1 – CMC Agent

Escalation Level 2 – CMC Manager

Escalation Level 3 – Managing Director

Working Time Definition

The Working Day is defined as Monday to Friday excluding Bank Holidays

Working Hours are defined as: The period from 08:00 to 18:00 on Working Days.

Service Delivery Definition

The Services will only be deemed to have been delivered once the service has been handed over to the Customer.

Incident Resolution and Service Unavailable Definitions

Subsequent to Services commencement, where the Customer believes the quality of the Service is not acceptable:

- ➔ an Incident will be raised with the TNP CMC
- ➔ TNP will investigate the Incident
- ➔ Subsequent to the investigation, if
 - a fault is found, the Incident is Resolved as any other Incident
 - a fault is not found and the Customer still believes the quality of the Services is unacceptable, TNP will evidence to the Customer that the Services comply with relevant Standards
- ➔ In the event that a fault is not found and TNP cannot evidence to the satisfaction of the Customer that the Services comply with relevant Standards, the Service will be deemed Unavailable from the time that the Incident was first raised with the TNP CMC and the Incident Resolution Time will be accordingly measured from that time.

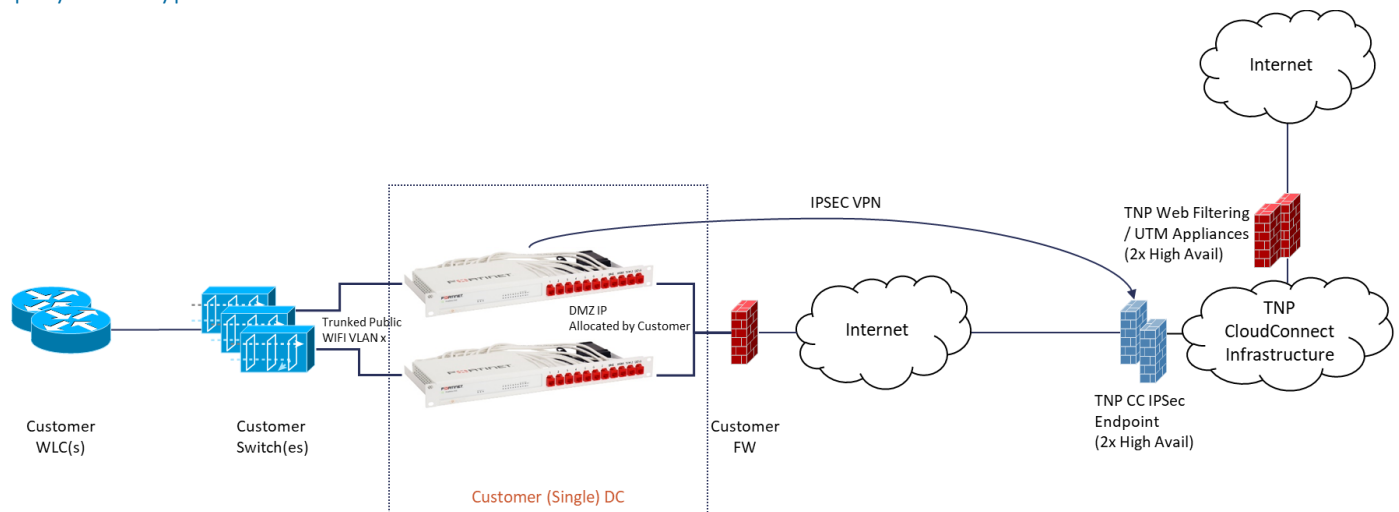
Price Card

Item	Installation / One-Off	Rental per Annum unless stated
Standard Deployment: HA pair of IPSec endpoints installed in a single location	£1,500	£700
HA Deployment: HA pair of IPSec endpoints installed across two locations	£1,500	£1,100
Multisite Deployment: HA pairs of IPSec endpoints installed in two separate locations	£3,000	£1,400
Portal Charge per 1,000 concurrent users	-	£2,950
Custom Portals: Additional portal handover VLAN	-	£500
Bespoke landing page design liaison per-portal	£725	
SMS and WhatsApp Charges: Priced in blocks • 100,000 • 50,000 • 25,000 • 10,000 • 5,000 • 1,000	£3,872 £1,995 £1,150 £484 £302 £66	-
Virtual Internet Connection • 100Mb/s • 200Mb/s • 300Mb/s • 400Mb/s • 500Mb/s • 600Mb/s • 700Mb/s • 800Mb/s • 900Mb/s • 1Gb/s	-	£760 £1,060 £1,510 £2,140 £2,940 £3,900 £5,030 £6,330 £7,790 £9,420

As an illustration, if you required a 2,000 concurrent user portal, 100,000 SMS credits, no additional custom portals and delivery into a single site, it would cost as follows:

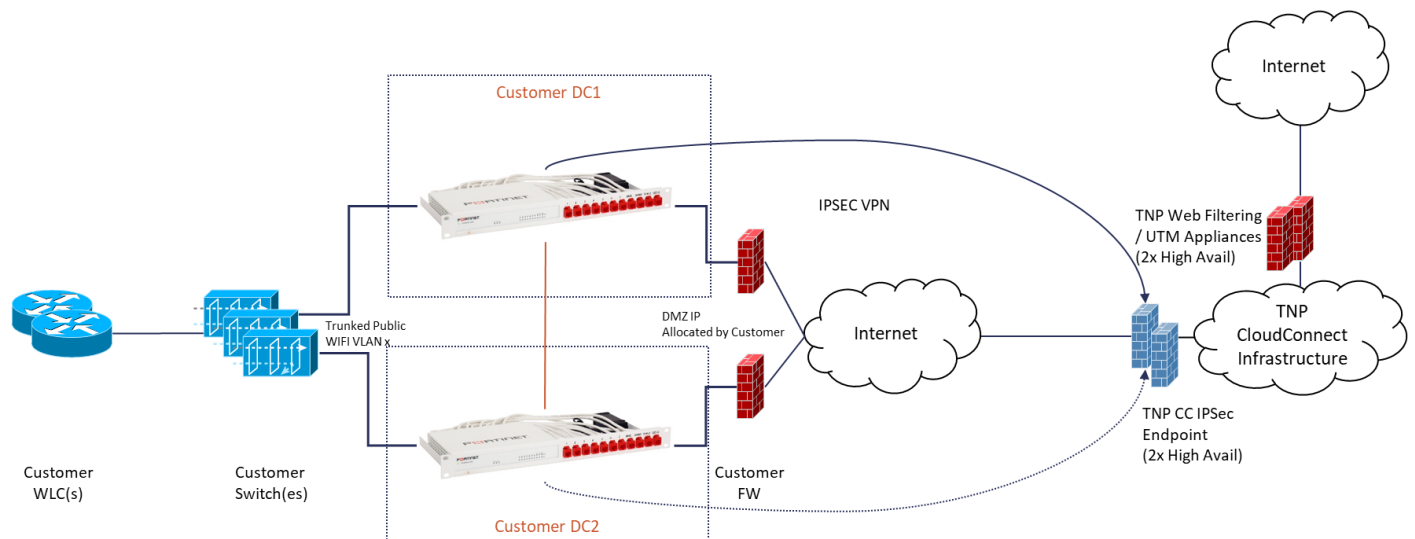
	Qty	Item Price	Line Total
Per site installation	1	£1,500.00	£1,500.00
100,000 SMS Credits	1	£3,872.00	£3,872.00
Total Installation/One-off			£5,372.00
2,000 concurrent user portal	2	£2,950.00	£5,900.00
Per site Rental/SLA charge	1	£700.00	£700.00
Total Rental per annum			£6,600.00

Deployment Types



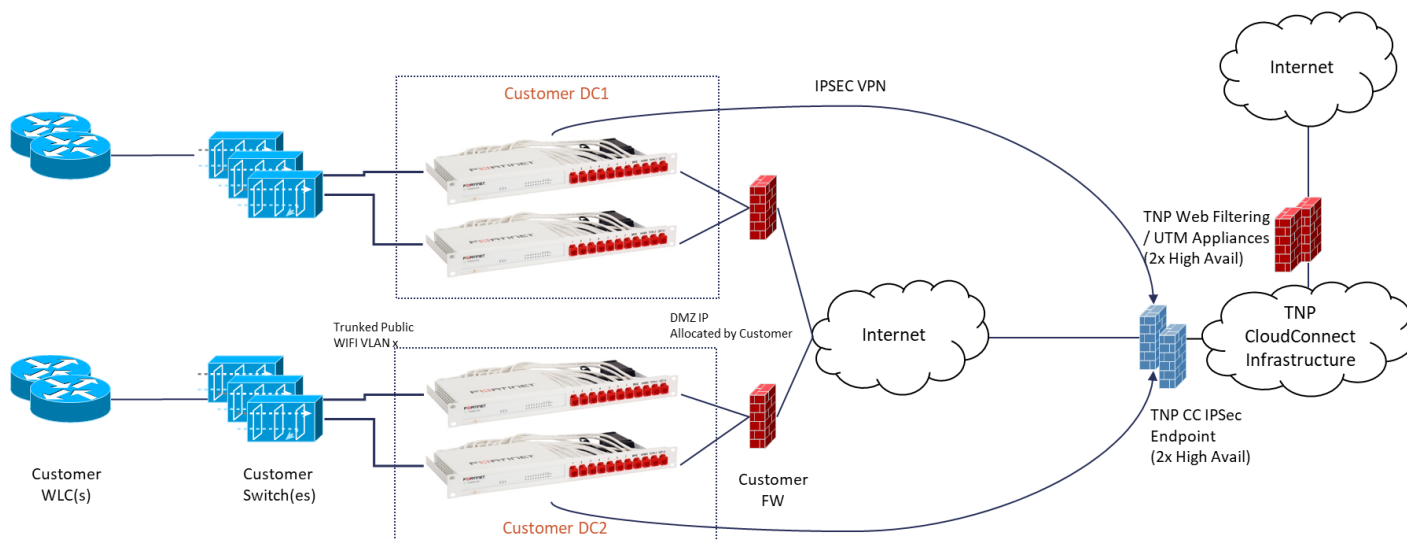
- DMZ uplink to firewall must share same L2 subnet
- One VLAN per-filter profile or portal is required, VLAN IDs can be allocated by customer.
- Fortigate HA managed by TNP
- Outbound NAT rules are required on customer firewall to permit IPsec VPN.
- Customer network connections 1000BASE-T

Title: Cloud Connect Standard Deployment	
Customer: TNP	
Drawn: IA	
Date: 03/01/2019	



- DMZ uplink to firewall must share same L2 subnet
- Customer firewalls must be in HA pair, same subnet required to be maintained.
- LAN-side switches and WLCs must be shared L2 between DCs
- Customer-provided fibre pair (single or multimode) required between DCs for Fortigate HA link.
- One VLAN per-filter profile or portal is required, VLAN IDs can be allocated by customer.
- Fortigate HA managed by TNP
- Outbound NAT rules are required on customer firewall to permit IPsec VPN.
- Customer network connections 1000BASE-T

Title: Cloud Connect HA Deployment	
Customer: TNP	
Drawn: IA	
Date: 03/01/2019	



- DMZ uplink to firewall must share same L2 subnet per-DC
- LAN-side switches and WLCs must be same L2 subnet within DCs
- Clients and APs should normally be pinned to the same WLC. In a failover scenario, client reauthentication may be required as the client will roam to another controller.
- One VLAN per-filter profile or portal is required, VLAN IDs can be allocated by customer.
- Fortigate HA managed by TNP
- Outbound NAT rules are required on customer firewall to permit IPsec VPN.
- Customer network connections 1000BASE-T

Title: Cloud Connect MultiSite Deployment	
Customer: TNP	
Drawn: IA	Date: 03/01/2019