



Customer
Service

Service Description

Internet



Document Control

Status	Drafted for digital.nsw.gov.au
Author's Name Position	Matt Duniam Network Architect
Category (Sub-Category)	ICT (Telecommunications)
Summary	Service Description for Fixed Data under the Telecommunications Purchasing Arrangements

Revision record

Please note significant document changes with a version increment of 1.0. Minor administrative changes, where the meaning or intention of the document is not altered should increase by an increment of 0.1.

Version	Date	Author	Summary of changes
1.0	19/12/2017	Matt Duniam	Release version
1.1	December /2018	Matt Duniam	Minor corrections following RFP clarifications. Released as part of RFx101331
2.0	02/06/2019	Matt Duniam	Updated to include more granular details on parameters. Released as part of RFx133881
2.1	06/04/2020	Matt Duniam	Minor update for digital.nsw.gov.au

Copyright



This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License. Terms for use can be found at <https://www.customerservice.nsw.gov.au/copyright> and the applicable license for use is at <http://creativecommons.org/licenses/by-nd/4.0/>.

© State of New South Wales through Department of Customer Service, 2020.

Table of Contents

Document Control	2
1. Service Tower Description	4
2. Service Category – Internet Uplink and Access	5
2.1 Core Internet Uplink	5
2.2 Internet Access	6
2.3 Peering Access	8
3. Service Category – Internet Uplink and Access Add-ons	10
3.1 Internet Firewall	10
3.2 DNS Hosting	11
3.3 Web Content Filtering	13
3.4 Email Protection	14
4. Glossary	17

1. Service Tower Description

Internet Services enable secure access to the Internet for users and applications. Internet services are typically presented to the Government Data Centres however they may be required at any Eligible Customer location.

These services are expected to continually evolve as technology changes and the security and bandwidth demands related to Internet services escalates, especially with the continual move to public Cloud.

It is expected that individual services will be consumed from different Suppliers, therefore services should be delivered in a modular fashion to facilitate that. Eligible Customers, or a designated third party, are expected to aggregate Internet Services from various Suppliers and any integrations with other towers, services and devices in their environment.

The services within this catalogue must meet the requirements for Internet Services defined in the Requirements Schedule and comply with the Common Services Catalogue.

This catalogue defines the minimum set of base services required by the customers and provides a generalised overview of their current states.

2. Service Category – Internet Uplink and Access

2.1 Core Internet Uplink

Service Overview

This Service is where an Eligible Customer requires high speed Internet access at a location, and the Eligible Customer requires the Supplier to:

- Monitor and proactively manage availability, capacity and performance.
- Provide an Ethernet termination point.

This service is characterised by its high speed, guaranteed bandwidth and high availability. It is suitable for Data Centre or Core sites.

This Service provides connectivity to the Internet as per Figure 1 below.

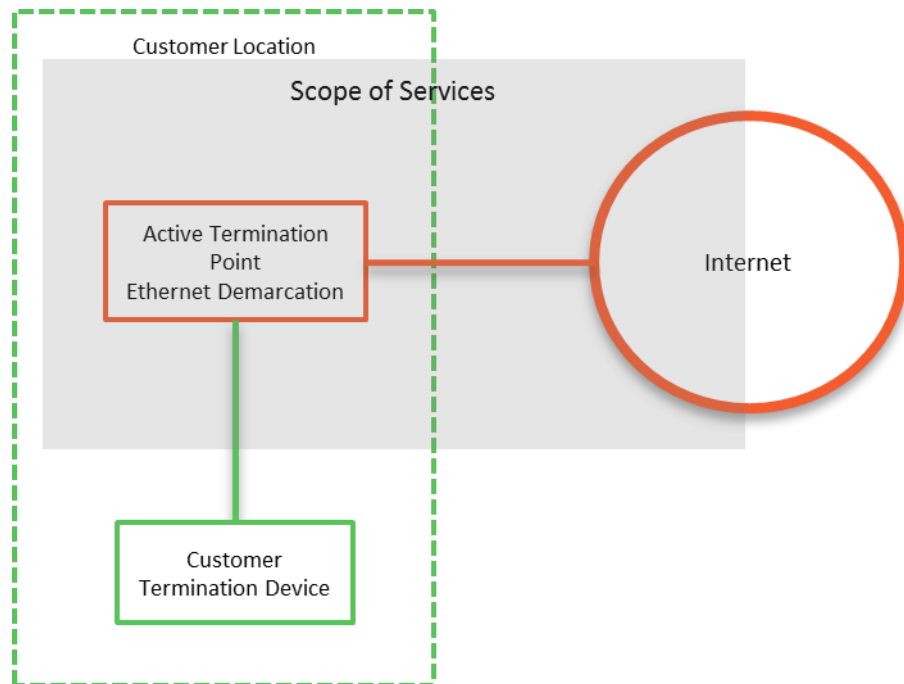


Figure 1: Core Internet Uplink

The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.

Services will be differentiated by the access network that is used, in terms of:

- Type; head-end, tail
- Physical layer; satellite, fixed wireless, copper, fibre
- Provider; respondents, NBN, 3rd party
- NBN Traffic Class; TC4, TC2, Enterprise Ethernet

<p>Service Deliverables</p>	<p>The Base Service will provide:</p> <ul style="list-style-type: none"> • Connectivity to the Internet for International and National carriage. • The Service should provide a range of Eligible Customer selectable bandwidths. <ul style="list-style-type: none"> ○ The bandwidth through the Supplier network should be guaranteed i.e. uncontended. ○ Outside the Supplier network the bandwidth is expected to be best efforts; however, the expectation is that the contracted bandwidth is available for most of the time. • Full proactive management of the Service, including monitoring and proactive response for capacity and availability. • A standards-based Ethernet termination to connect to Eligible Customer equipment. • Basic Denial of Service protection. <p>Service Options that Eligible Customers are interested in, and could also be provided are:</p> <ul style="list-style-type: none"> • A CPE device to act as a gateway and connect directly to the Eligible Customer LAN. • Advanced Denial of Service protection. • Traffic engineering, to control traffic allocation of bandwidth for different application types.
------------------------------------	---

<h2>2.2 Internet Access</h2>	
<p>Service Overview</p>	<p>This Service is where an Eligible Customer requires Internet access at a location, and the Eligible Customer requires the Supplier to:</p> <ul style="list-style-type: none"> • Monitor and proactively manage availability and capacity. • Provide an Ethernet termination point. <p>This service is characterised by its lower of QoS, compared to Core Internet Uplink, and contended bandwidth tiers. This service is suitable for access sites.</p> <p>This Service provides connectivity to the Internet as per Figure 1 below.</p>

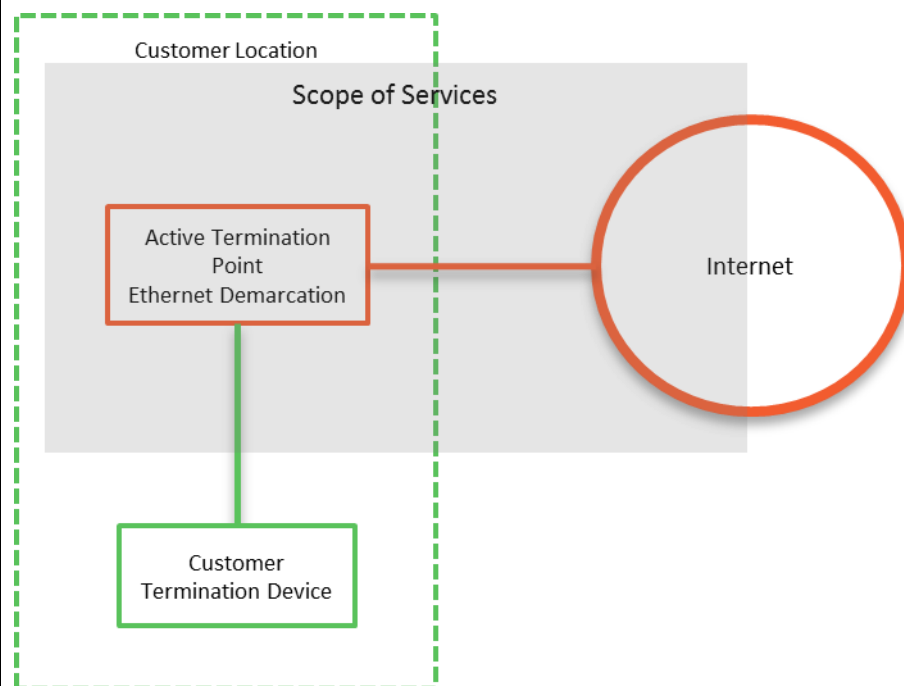


Figure 2: Internet Access

The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.

Services will be differentiated by the access network that is used, in terms of:

- Type; head-end, tail
- Physical layer; satellite, fixed wireless, copper, fibre
- Provider; respondents, NBN, 3rd party
- NBN Traffic Class; TC4, TC2, Enterprise Ethernet

Service Deliverables

The Base Service will provide:

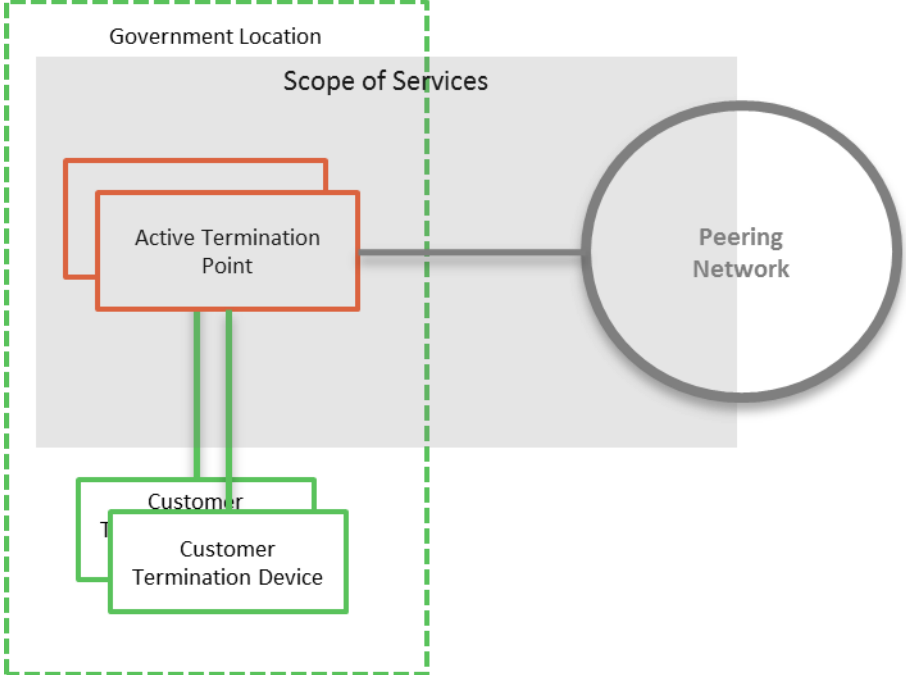
- Connectivity to the Internet for International and National carriage.
- The Service should provide a range of Eligible Customer selectable tiers. Each tier will have its own bandwidth and performance criteria.
 - Bandwidth within the Supplier network may be contended or uncontended, depending on the Service tier.
 - Outside the Supplier network the bandwidth is expected to be best efforts; however, the expectation is that the contracted bandwidth is available for most of the time.
- Full proactive management of the Service, including monitoring and proactive response for capacity and availability.
- A standards-based Ethernet termination to connect to Eligible Customer equipment.
- Basic Denial of Service protection.

Service Options that Eligible Customers are interested in, and could also be provided are:

- A CPE device to act as a gateway and connect directly to the Eligible Customer LAN.
- Advanced Denial of Service protection.

	<ul style="list-style-type: none"> • Traffic engineering, to control traffic allocation of bandwidth for different application types.
--	--

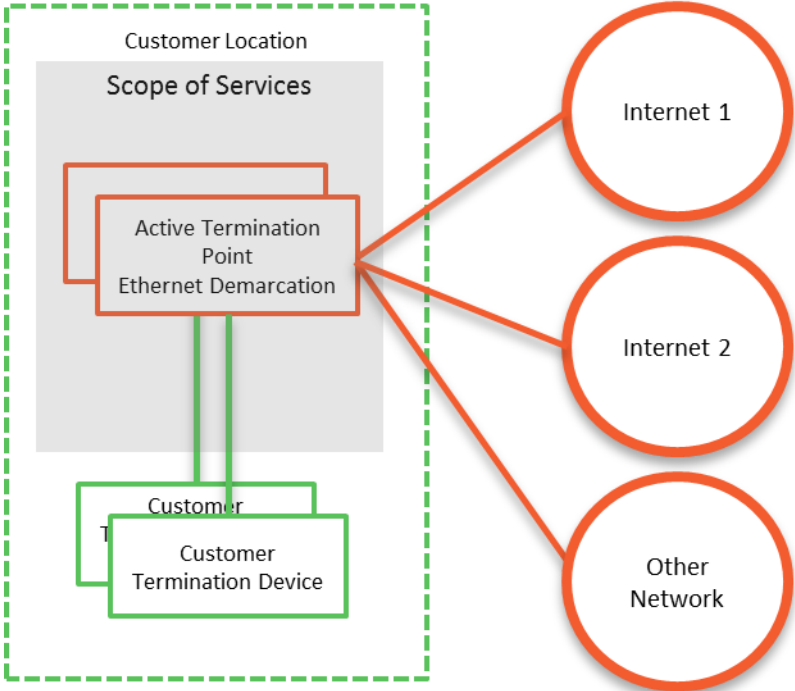
2.3 Peering Access

Service Overview	<p>This Service is where an Eligible Customer requires direct, uncontended access to content providers or subscriber aggregation organisations, and the Eligible Customer requires the Supplier to:</p> <ul style="list-style-type: none"> • Provide access to a Peering network • Monitor and proactively manage availability and capacity. • Provide an Ethernet termination point. <p>This Service provides connectivity to Peering as per Figure 3 below.</p>  <p style="text-align: center;"><i>Figure 3: Peering Access</i></p> <p>The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.</p>
-------------------------	---

Service Deliverables	<p>The Base Service will provide:</p> <ul style="list-style-type: none"> • Connectivity to the Peering Network, and reachability to all Open Peering organisations on the Peering Network. • The Service should provide a range of Eligible Customer selectable bandwidths. • Full proactive management of the Service, including monitoring and proactive response for capacity and availability.
-----------------------------	---

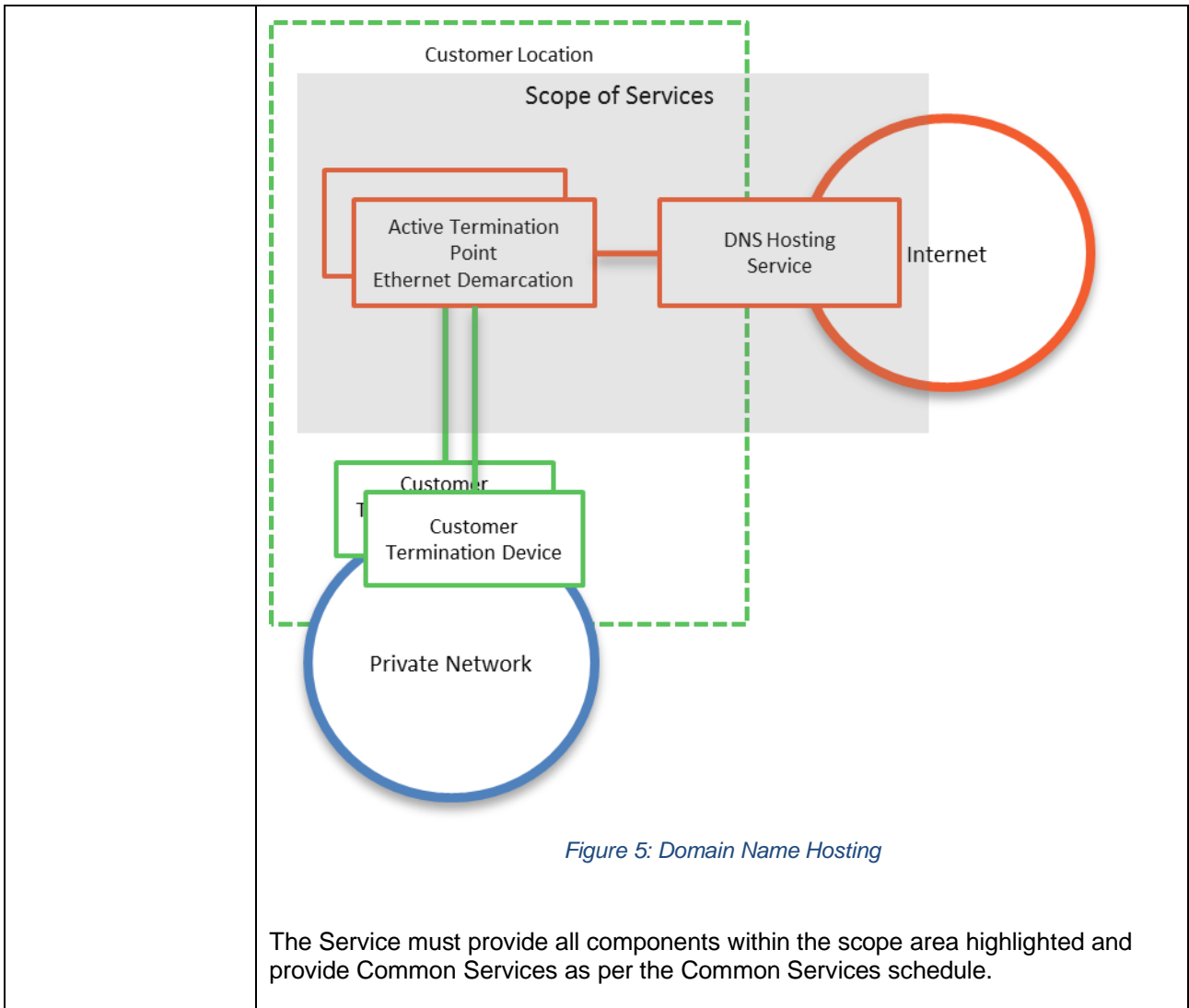
	<ul style="list-style-type: none">• A standards-based Ethernet termination point to connect to Eligible Customer equipment. <p>Service Options that Eligible Customers are interested in, and could also be provided are:</p> <ul style="list-style-type: none">• Selective Peering with organisations on the Peering Network, typically via a separate logical network and with point-to-point routing.• Restricted/Closed peering with organisations, typically on via dedicated connectivity and not via the Peering Network.
--	---

3. Service Category – Internet Uplink and Access Add-ons

3.1 Internet Firewall	
<p>Service Overview</p>	<p>This Service is where an Eligible Customer requires a managed firewall service to provide protection from the Internet, and the Eligible Customer requires the Supplier to:</p> <ul style="list-style-type: none"> • Provide the Firewall as a managed service. • Monitor and proactively manage availability, capacity, and performance. • Provide an Ethernet termination point. • Connect to one or multiple upstream Internet or other network providers. <p>This Service provides connectivity between Untrusted networks and the Eligible Customer Termination Devices as per Figure 4 Error! Reference source not found. below.</p>  <p style="text-align: center;"><i>Figure 4: Internet Firewall</i></p> <p>The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.</p>
<p>Service Deliverables</p>	<p>The Base Service will provide:</p>

	<ul style="list-style-type: none"> • The ability to terminate multiple networks, and control the traffic flow between networks. • Full proactive management of the Service and interconnection points, including monitoring and pro-active response for capacity, availability, security, and performance. Significant events must also be proactively logged and diagnosed. • Grey level diagnostics, to determine which interconnecting Supplier needs to take ownership of an incident or problem. • A standards-based Ethernet termination point at each Data Centre to connect to Eligible Customer equipment. • The ability to apply firewall policies based on Eligible Customer requirements. • The ability to alert and/or filter traffic based on known behaviour. <p>Service Options that Eligible Customers are interested in, and could also be provided are:</p> <ul style="list-style-type: none"> • Enhanced monitoring and alerting of behaviour patterns i.e. not reliant on signatures. • Workflow and Audit management. • Enhanced Unified Threat Management, such as sandboxing and scanning for malicious content.
--	---

<h2 style="margin: 0;">3.2 DNS Hosting</h2>	
<p>Service Overview</p>	<p>This Service is where an Eligible Customer requires Domain Name Hosting to support reachability of their applications, and the Eligible Customer requires the Supplier to:</p> <ul style="list-style-type: none"> • Host domain names. • Monitor and proactively manage availability, capacity, and performance. • Provide access to the service over the Internet. <p>This Service provides Domain Name Hosting as per Figure 5 below. Where internal DNS services are provided a termination is required at the Data Centres. For external hosting, the Service could be provided entirely from the Internet.</p>



<p>Service Deliverables</p>	<p>The Base Service will provide:</p> <ul style="list-style-type: none"> • The ability to host domain names and provide reachability for domain name resolution from the Internet. • Full proactive management of the Service, including monitoring and proactive response for capacity, availability, and performance. • A standards-based Ethernet termination point at each Data Centre to connect to Eligible Customer equipment, where internal DNS services are provided. <p>Service Options that Eligible Customers are interested in, and could also be provided are:</p> <ul style="list-style-type: none"> • Advanced DNS resolution, for example DNS load balancing algorithms • Internal DNS resolution services • IP address Management, and automated DNS record updates
------------------------------------	--

3.3 Web Content Filtering

Service Overview

This Service is where there are many Eligible Customer devices that need to access the Internet and require protection to ensure that the devices are not compromised and that the Internet sites being accessed are in line with the Eligible Customer policies.

The Eligible Customer require the Supplier to:

- Monitor and proactively manage availability, capacity, security, and performance of the Service.
- Provide filtered connectivity to the Internet, including the Internet Access.
- Provide connectivity for Eligible Customer devices from the Internet and from an interconnection at the Government Data Centres.

This Service provides connectivity to the Internet as per Figure 6 below.

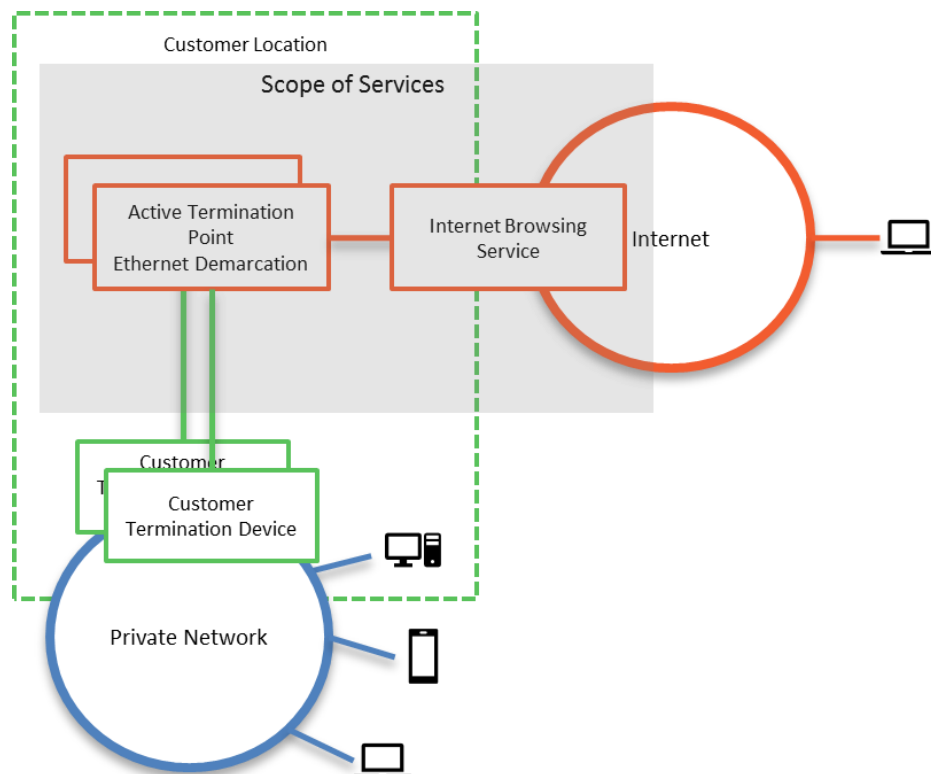


Figure 6: Internet Browsing

The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.

Service Deliverables

The Base Service will provide:

- Internet Access for Eligible Customer devices connecting to the Service. The Service should provide a range of Eligible Customer selectable bandwidths.
- The ability for Eligible Customer devices to connect to the Service via their Private Network or via the Internet.

	<ul style="list-style-type: none"> • Full proactive management of the Service and interconnection points, including monitoring and pro-active response for capacity, availability, and performance. • A standards-based Ethernet termination at each location to connect to Eligible Customer equipment. • The ability to apply security policies based on Eligible Customer requirements, with policies able to be applied for the organisation, group, and individual. • The ability to alert and/or filter traffic based on known behaviour, malicious content, and content type. • The ability to prevent or allow access to web sites, based on categories, white lists, or black lists. • The ability to prevent or allow access to web sites (URL filtering), based on categories, white lists, or black lists. <ul style="list-style-type: none"> • The filtering policy will be based on the group that the users belong to. • There are potentially many distinct groups with different policy lists. <p>Service Options that Eligible Customers are interested in, and could also be provided are:</p> <ul style="list-style-type: none"> • Cloud Access Security Brokerage
--	--

<h3>3.4 Email Protection</h3>	
<p>Service Overview</p>	<p>This Service is where the Eligible Customer has devices that need to send and receive emails over the Internet and require protection to ensure that the devices are not compromised and that the emails being sent and received are in line with the Eligible Customer policies.</p> <p>The Eligible Customer require the Supplier to:</p> <ul style="list-style-type: none"> • Monitor and proactively manage availability, capacity, and performance of the Service. • Provide filtering of email content to and from the Internet, and provide the Internet Access. • Provide connectivity for Eligible Customer Email platforms to the Internet from interconnection points at the Eligible Customer’s location(s). <p>This Service provides connectivity to the Internet for Email as per Figure 7 below.</p>

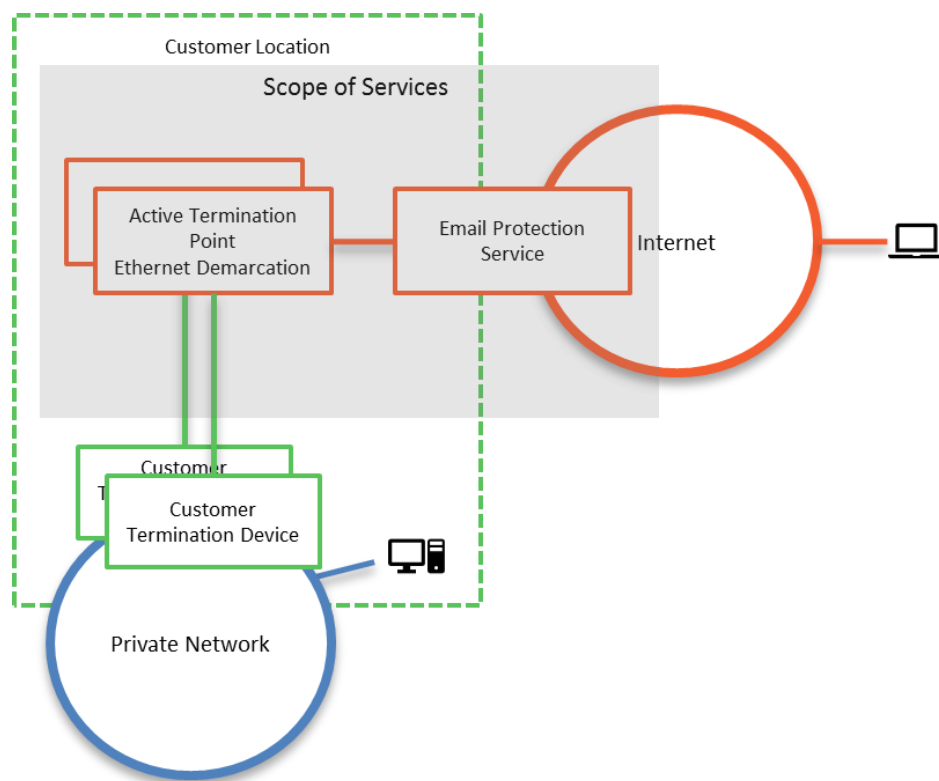


Figure 7: Email Protection

The Service must provide all components within the scope area highlighted and provide Common Services as per the Common Services schedule.

Service Deliverables

The Base Service will provide:

- Internet Access for third-party email hosts connecting to the Service. The Service should provide a range of Eligible Customer selectable bandwidths.
- The ability for Eligible Customer Email platforms to connect to the Service via their Private Network.
- Full proactive management of the Service and interconnection points, including monitoring and pro-active response for capacity, availability, and performance.
- A standards-based Ethernet termination point at each Data Centre to connect to Eligible Customer equipment.
- The ability to apply security policies based on Eligible Customer requirements, with policies able to be applied for the organisation, group, and individual.
- The ability to alert and/or filter traffic based on known behaviour, malicious content, and content type.
- The ability to prevent or allow access to domains, based on categories, white lists, or black lists.
- The ability to detect and quarantine unsolicited email, and to provide a mechanism for the users to view quarantined email and release the email if required.

Service Options that Eligible Customers are interested in, and could also be provided are:

	<ul style="list-style-type: none">• Hold and release of email, based on policies• Classification of emails, through user prompts and rules
--	---

4. Glossary

Term or short form	Long-form	Definition
aaS	as-a-Service	An item, or grouping of items, made available to a customer as a service
Active Termination		Where the Service Provider provide a device that terminates the service at a site and enables end-to-end management.
ADSL	Asymmetric Digital Subscriber Line	
APN	Access Point Name	A gateway between a mobile network and another network, such as the Internet or a Private WAN.
bps or bit/s	Bits per second	
BYO	Bring your own	
CAB	Change Advisory Board	
Circuit		For data connections, a circuit a path that data transverses between two points. A circuit is a component of a Service.
CMS	Configuration Management System	
Contract Authority		The central entity that is accountable and responsible for the Head Agreements of the TPAs
CoS	Class of Service	
		TPA Release Version
CSI	Continual Service Improvement	
Customer		NSW Government Agency, or any organisation procuring services from the Service Catalogues.
CPE	Customer Premise Equipment	A device that is used by Service Providers to terminate services at a site.
Customer Termination Device		A Customer device that is connected to the Provider's equipment
DHCP	Dynamic Host Control Protocol	
DISS	Digital Information Security Strategy	
DoS (or DDoS)	Denial of service (or distributed denial of service)	An attack that attempts to make a service unavailable by overwhelming it with traffic from multiple sources.
DWDM	Dense Wavelength Division Multiplexing	
Error		A design flaw or malfunction that causes a failure of one or more IT services or other configuration items.
Event		A change of state that has significance for the management of a service.

Term or short form	Long-form	Definition
Gateway device		A layer 3 device at a site that acts as the sites router, to transmit packets to the WAN. Host devices have a gateway device configured, typically via DHCP.
Gbps or Gbit/s	Giga (billion) bits per second	
Grey Area Diagnostics		The process to proactively diagnose in-scope services and interconnections to help identify the cause of an incident or problem. The result is to identify that the cause of the incident or problem: <ul style="list-style-type: none"> - Is caused by in-scope services - Is not caused by in-scope services - Could be caused by in-scope services, and further diagnostics are required
ICT	Information and Communications Technology	
ICT Risk Management		Information Communication Technology (ICT). The NSW Digital Information Security Policy mandates a risk-based approach to securing information, based on the ISO 27001 standard. DFSI has implemented a framework in line with the policy, with ICT risks being managed through an Information Security Management System (ISMS).
Incident		An unplanned interruption to a service or a reduction in the Quality of a service. Failure of a configuration Item that has not yet impacted service is also an Incident.
IP	Internet Protocol	
IPSLA	Internet Protocol Service Level Agreement	Cisco IOS feature that allows for the collection of network performance information.
ISM	Information Security Management	
ISMS	Information Security Management System	
ISO	International Standards Organisation	
ITSM	IT Service Management	
IVR	Interactive Voice Response	
kbps or kbit/s	Kilo (thousand) bits per second	
Known Error		A Problem that has a documented root cause and workaround.
Location, Site		A Customer site or location is a place where services are to be delivered. Depending on the service, this may not necessarily be a physical building.
MACD	Move, Add, Change or Delete	

Term or short form	Long-form	Definition
MAN	Metropolitan Area Network	
Mbps or Mbit/s	Mega (million) bits per second	
MNO	Mobile Network Operator	Provider of wireless/mobile communications services that owns or controls all the elements necessary to sell and deliver services to an end user, e.g. radio spectrum, wireless network infrastructure, back haul, billing, customer care, provisioning systems and repair capabilities.
MVNO	Mobile Network Operator	Provider of wireless/mobile communications services that does not own the wireless network infrastructure over which it provides services to its customers. Instead they enter a business agreement with a MNO to obtain bulk access to network services at wholesale rates. They do have their own customer service, billing systems, marketing, and sales personnel.
MPLS	Multi-Protocol Label Switching	
MTU	Maximum Transmission Unit	
NBN	National Broadband Network	
NBN Co		The entity responsible for the design, build and operation of the NBN
NFV	Network Function Virtualisation	
NIVR	Network Interactive Voice Response	
OADM	Optical Add-Drop Multiplexer	
Operational Risk		Risks associated with business-as-usual activities at the Division / Business Unit / Related Entity level that is normally managed within that area, unless the level of risk requires a review by the DFSI Executive and/or Secretary.
OSS	Operational Support System	
OTT	Over-the-top	
Passive Termination		Where the Service provider provides a physical termination point which can't be monitored.
PE	Provider Edge	
Peering		The exchange of data directly between Content Providers and Customers, rather than via the Internet.
Performance		A measure of what is achieved or delivered by a system, person, team, process or service
POI	Point of Interconnect	
POP	Point of Presence	

Term or short form	Long-form	Definition
Priority		The value given to an Incident, Problem or Change to indicate its relative importance in order to ensure the timeframe within which action, such as Response and Resolution, is required.
Private Data Network		A network or networks that utilises private infrastructure to deliver physically or logically private services
Problem		A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.
Public Data Network		A network or networks that utilises publicly available, shared infrastructure such as mobile networks or the Internet
Public Holidays		All NSW public holidays as gazetted, except for Bank Holidays specific to only banks and financial institutions as per the Retail Act.
QoS	Quality of Service	
RACI	Responsible, Accountable, Contributor, Informed	
Resolver Group		Specialised groups that have the knowledge and skill to solve an Incident or Problem.
R-OADM	Reconfigurable Optical Add-Drop Multiplexer	
Root Cause		The underlying or original cause of an incident or problem.
RSP	Retail Service Provider	
Sandboxing		A security mechanism for separating untested or untrusted programs or code to mitigate system failures or software vulnerabilities from spreading.
Satellite		Satellite based connectivity to deliver NBN connectivity
SDN	Software Defined Network	
SD-WAN	Software Defined Wide Area Network	
SD-WANaaS	SD-WAN-as-a-Service	
Service Window		Service window is defined as the timeframe within which service availability and service management (incident response, incident resolve) are measured and managed.
Significant Event		This is an event that materially impacts a Customer, and is likely to be a P1 or P2.
SIP	Session Initiation Protocol.	
SLA	Service Level Agreement	

Term or short form	Long-form	Definition
SoR	Statement of Requirements	
TDM	Time Division Multiplexing	
TPA	Telecommunications Purchasing Arrangements	
User		A person who uses a service on a day-to-day basis.
VIP	People with critical roles within an organisation, and identified to Service Providers.	
VNF	Virtual Network Function	
VPN	Virtual Private Network	
WAN	Wide Area Network	
WoG or WofG	Who of government	All Clusters and Agencies within the NSW Government.

Strategic Sourcing | ICT / Digital Sourcing | Department of Customer Service

Address: Level 23, McKell Building, 2-24 Rawson Place, Sydney NSW 2000

E-mail: Strategic.Sourcing@customerservice.nsw.gov.au

