

Broadband

Technical specification

Contents

Introduction	3
Service overview	4
Functional requirements	4
Connection options	5
High level design	6
Virtual Broadband	8
Broadband use cases	9

Introduction

Heathrow has been the busiest international hub airport in the world for the past decade, handling more than 70 million passengers on an annual basis.

In order to successfully cater for such an extraordinary high volume of traffic, the airport operation must be based on firm technical foundations, providing a reliable, uninterruptable service. The IT infrastructure at Heathrow has been built to meet this challenging criteria, and is being constantly upgraded to adopt the latest innovations and standards. It has proven to be well designed and able to handle business as usual operations, as well as to cope with the unexpected events.

Now, all Heathrow airport tenants whether they are airlines, retailers or support service companies can benefit from this powerful IT infrastructure, which has been built for airport operations. Modern, resilient, built for the airport by the airport – the IT services portfolio, using the Heathrow common IT infrastructure, is constantly evolving to bring our customers the products they need to benefit their business.

The Broadband service offers an end-to-end network solution providing a wide range of options for connection to the internet. Utilising the existing fibre and cable infrastructure, Broadband can be delivered in an affordable and flexible manner, and depending on the service option selected, is capable of providing internet connectivity to multiple customer locations across the airport, as well as integration with the wireless networks. The cross campus connectivity is securely routed between dedicated customer networks to create a private environment.

Service overview

The Broadband service has been designed to provide high speed and resilient access to the public internet from virtually any location within the airport campus. Multiple connection options are available to support the various requirements of airport tenants.

Functional requirements

The fundamental functional requirements for the Broadband internet were identified by the customers in three options:

1. Direct connection to the internet; where tenants can deploy their own routing equipment at their airport demise, without a requirement for an airport provided VLAN/VPN.
2. Access to a Heathrow airport wireless LAN (WLAN) with a direct connection to the internet, enabling connection to the customer's headquarters or 3rd parties (typically credit card processing companies). Deploying its own routing equipment at the premises, without a requirement for its own VLAN/VPN (virtual local area network/private network).
3. Connection to the internet via a Heathrow Managed LAN/WLAN solution, where a VLAN/VPN is provisioned across the Heathrow campus, and internet connection is provided at a central location. Tenants still need to provide their own routing equipment and firewalls.
4. A fully managed solution as per item 3, but where there is no requirement to provide tenants routing or firewall equipment as this is provisioned by Heathrow as virtual firewalls.

Service overview

Connection options

There are a number of service options for Broadband.

Broadband Light

Ideal for a single location such as an office or retail store, this option is delivered as a separated connection via an Ethernet RJ45 port. Customers will need to provision their own router and firewall for connection to the internet. Heathrow Wireless LAN can be optionally connected to the same router via a second RJ45 connection using bridged mode.

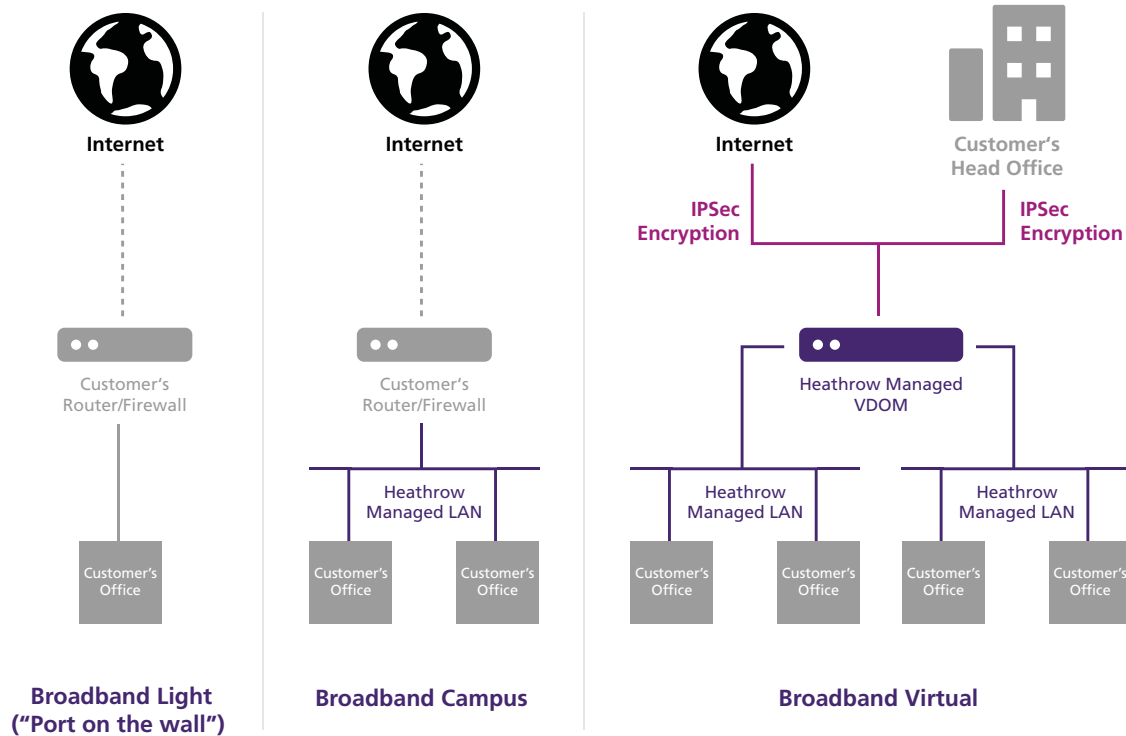
Broadband Campus

Ideal for using a common internet connection to serve multiple locations at Heathrow. This option is intended for customers with a Heathrow Managed LAN. Customers will need to provision their own router and firewall typically located in one of Heathrow's 'meet me' communications rooms.

Broadband Virtual

For customers who do not want to have physical firewalls and routers. This option makes use of virtual firewalls provisioned by Heathrow. Typically used to provide an IPSec (internet protocol secure) connection between customers Heathrow locations and head office.

How the options work



High level design

The options and features made available were chosen based on analysis of the requirements gathered from tenants across the Heathrow airport. The service is operated on the existing infrastructure and builds upon a standard VPN deployment on the existing hardware, while making use of some additional new features to provide the required solution. The main focus was to shorten delivery times, while effectively reducing costs. This is only achievable if the multitudes of separate connections to the internet are consolidated into a single (but resilient) pipe which all customers use.

The Broadband solution is capable of the following features and modes of operation:

- 1) A single ISP (internet service provider) resilient connection to their backbone.
- 2) A resilient Heathrow virtual firewall provides
 - Public to private IP addressing translations.
 - Overloading customers to a single address for general internet access.
 - 1-to-1 address translation for inbound access.
 - DHCP (Dynamic Host Configuration Protocol) service for customer WAN router interfaces.
 - Connectivity to private Broadband VPN solution.
 - Connectivity to private customer managed VPN solutions.
- 3) Hub and spoke deployed VPNs
 - Hub VPN providing access to the internet (connected to the above firewall).
 - Spoke VPNs in each domain to provide routed separation from customers on the Heathrow infrastructure.
- 4) Perimeter security - MAC and IP ACLs (Dynamic Host Configuration Protocol) to hide one customer router from another on the same subnet.
- 5) Optional WLAN service provisioning using new WLAN bridge mode standards dedicated to customers.

High level design – continued

For the external connectivity, service shall utilise the WAN terminated on Cisco routers, one in the Terminal 5 and Terminal 3 data comms. These links provide a resilient and load balanced solution, with fully managed fail over between their circuits in Terminal 5 and Terminal 3.

For the connectivity within the airport campus, customers have multiple options to choose from:

- Connect from the demise to the WAN aggregation point through the Heathrow cabling (using the passive infrastructure service); this is the separated connection option
- Connect from the demise to the WAN aggregation point through the Heathrow active infrastructure (using the Managed LAN service); this is the managed connection option

Each of the above options are based on creating virtual local area networks for each customer accessing the internet. With each option there is the ability to interconnect the broadband with the Heathrow wireless network (using the WLAN service).

In all instances, the individual customers VLANs are securely separated from each other.

For the internet access distribution within a customer's demise, customers are expected to use their own network devices, in accordance with their best practices and internal policies.

The customer's router acts as a gateway for connection to their services and sits within the Broadband end-to-end design. There are a number of conditions that need to be adhered to when deciding on the router:

- The router needs to be a layer 3 (routing) device only, and no layer 2 (switching) device will be allowed.
- No Wi-Fi capabilities are to be enabled in order to combat interference of conflict with any other campus WLAN device.
- All managed service routers need to be housed in Heathrow meet-me comms room and within the confines of WAN Aggregation infrastructure.
- Un-managed service router may be stored within customer premises.

The Broadband service at its initial release will allow for customer's Broadband router to use the DHCP (Dynamic Host Configuration Protocol) to obtain an IP Address for internet connection. The provisioned port will give access to the internet via a private IP addressed VPN, with a head end firewall for translating the privately IP allocated customer Broadband routers with a public IP address.

Exceptionally high resiliency of the Broadband service is ensured on multiple infrastructure levels:

- Dual external connectivity.
- Redundancy of the Heathrow active infrastructure equipment.
- Fully meshed cabling.

Virtual Broadband

To accommodate future capacity and current high demand a re-design of the solution was undertaken providing an alternative method which allows the public IP addresses to be directly allocated out to either the customer broadband firewall/router for unmanaged customers or to a Firewall VDOM for managed customers (regardless of which domain the customer was based in). In essence, a Virtual Broadband solution.

To achieve the requirement a new solution has been developed which makes use of the following key routing technologies to in effect bridge the public IP subnets to each domain and each customer.

Unmanaged customers

- A common Broadband VPN is deployed across the Heathrow Campus.
- The same subnet/s and VLAN are then deployed to each Heathrow domain.
- Static host routes are then used to over-ride the normal Address Resolution Protocol (ARP) process on the router interfaces and route traffic across the Multi Protocol Label Switching (MPLS) network between subnets which are the same.

Managed customers

1. Due to the issue of connecting to a common VLAN from different VDOMs, separate specific customer Broadband VPNs will be created.
2. For managed customers the static routes will then be exported/imported between the main Broadband VPN on the WAN aggregation domain and the specific customer Broadband VPN.

The solution has the following key benefits over the existing solution:

1. We are able to allocate out the public IP address directly, there is no need to perform private to public NAT (Network Address Translation).
2. The customer will be pointed directly at the relevant CE (Customer Edge) router HSRP (Hot Standby Router Protocol) address for the relevant public subnet they are part of, there is no need to configure policy based routing to load share between the links going out to the internet.
3. The solution in effect means that there is no need to provide a firewall for unmanaged customers.
4. For managed customers separate VLANS will be getting used at the firewall for each customer so there is no need to implement transparent VDOMS and VDOM to VDOM interlinks.

Broadband use case

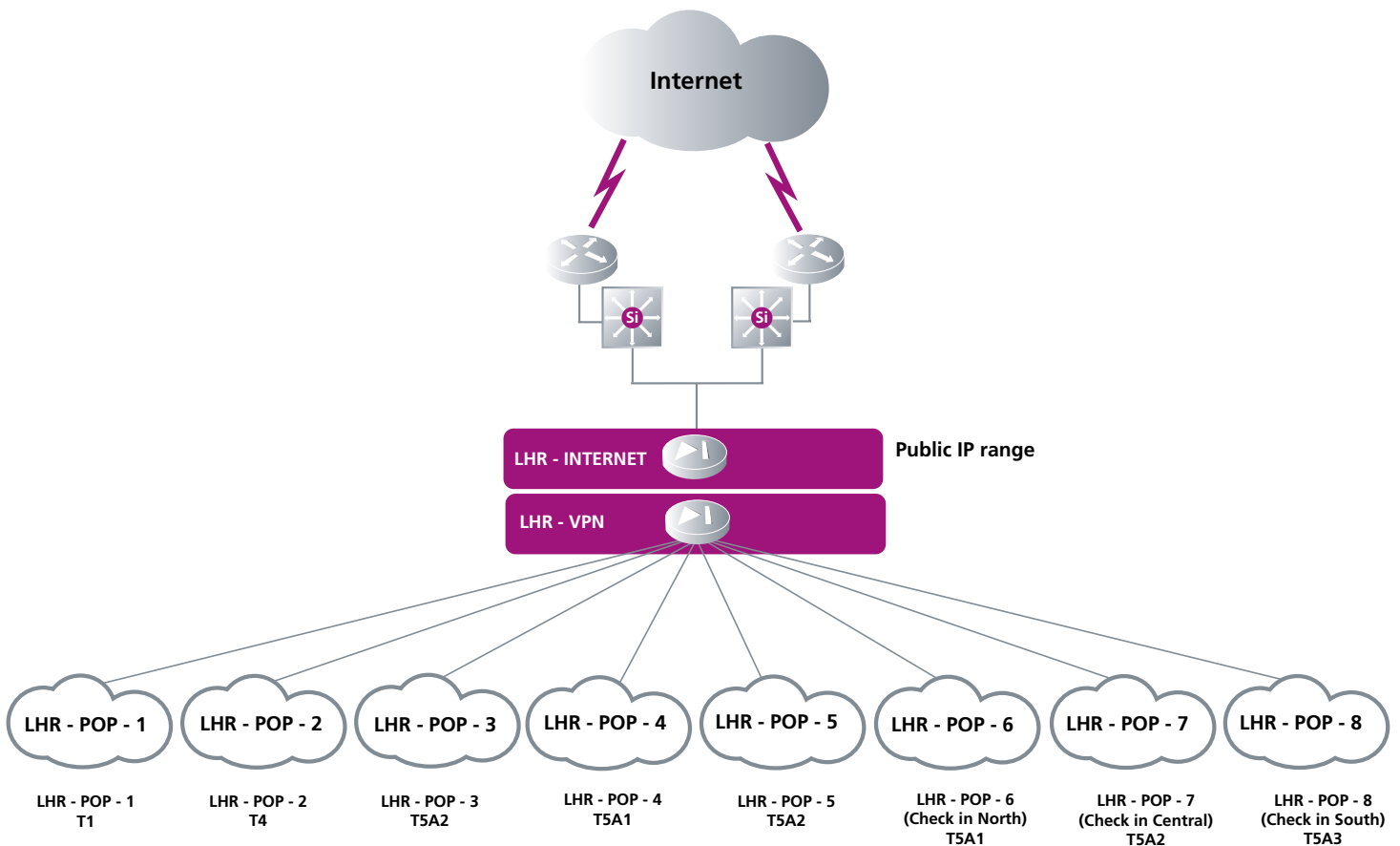
Pop-up Retail stores, Terminal 5

Heathrow Retail had a desire to provide pop-up sites across Heathrow for their customers making use of the retail space. A flexible solution was needed that could be ramped up and down based on the customer requirements.

There are 8 retail units across the Heathrow campus. The pop-up units are used for retailers and other marketing companies to demo their merchandise or services. These units have a high churn of companies making use of them so the network design was adaptable to accommodate individual requirements with little or no additional network design each time a new company makes use of the experiential sites.

For Broadband connectivity to be implemented the design was deployed on the third party firewalls (Broadband) as a managed VPN solution. Each site had their own VPN (individually named) and was isolated from other Heathrow VPNs. A new VDOM on the third party firewalls was used for all the units to allow connectivity to the 3rd party internet solution. The VPNs will be allowed to communicate with each other via the firewall if the customer desired this.

A network topology of this design is as follows:



Pop-up Retail stores, Terminal 5 – continued

The following were network requirements for this solution:

- 8 new isolated VPNs one for each pop-up unit.
- Connection to third party internet firewalls, using a single new VDOM.
- Provide internet access controlled via a standard set of policies that can be adjusted for the individual customer purposes.
- Provide detailed survey of each site with recommendations on any new physical infrastructure requirements.
- Provide a standard deployment model for each pop-up site, i.e. outlet configuration profile.

Conclusion:

A full design is completed prior to the implementation which specifies and sets out all the technical information that will be required. This includes such items as topology diagram, scope of works and logical configuration.

The SITA deployment team ensured that all configuration work is completed, in parallel to the 3rd party logical configuration on their own routers.

End to end connectivity is verified with the SITA technical teams to ensure that Broadband connectivity is achieved.

The pop-up retail Units are now fully functional and provide a function in which the various concessionaires who utilise them are able to use the broadband service to connect to back-end services and on store devices.

Virtual Broadband use case

SITA was asked to look at delivering a managed firewall Broadband solution for retail customers. The primary objective would be to provide a centralized resilient internet connection with a logically separate managed firewall for each retail customer. The main focus was to deliver IPSEC (Internet Protocol Security) tunnels across the internet to customer remote sites and to route any customer Internet traffic via a customer proxy server.

The IPSEC tunnels would be used to provide site to site communication between the customer office at Heathrow and the customer central/HQ office. 'Any to Any' communication would be permitted between the customer sites across the tunnel.

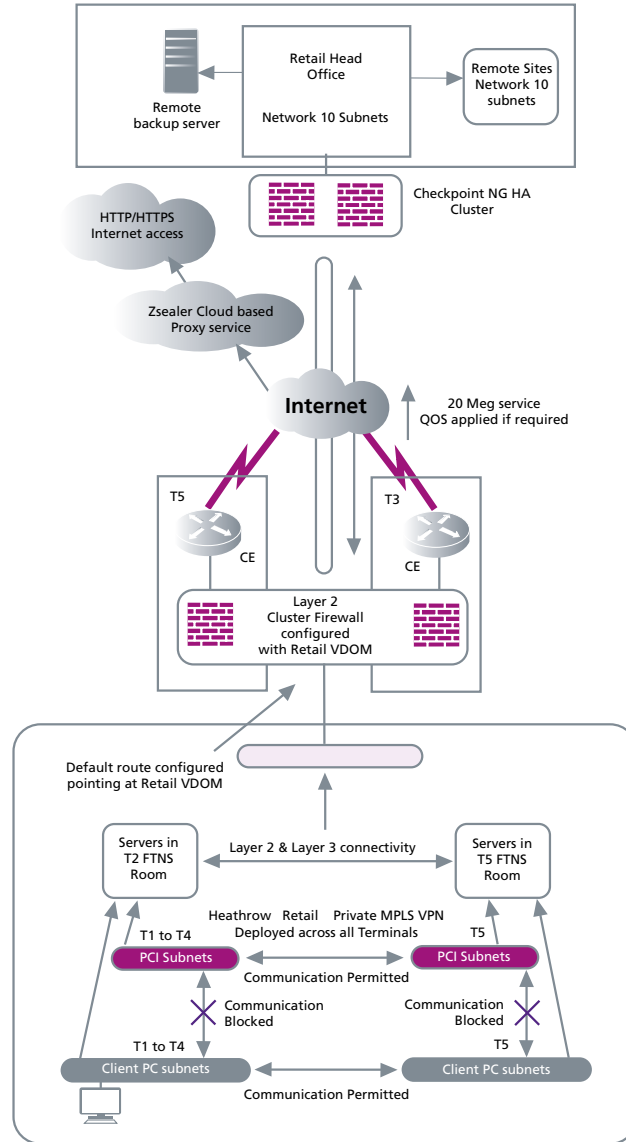
The Managed Broadband service provides the following advantages to customers over having to implement their own Internet connections:

- A single resilient central Internet outlet point which is reachable from all terminals. Currently many retail customers have to implement separate internet connections in each Terminal.
- The need to not have to manage and support the internet pipes and firewalls at Heathrow, as well as not having to buy the firewalls. Dealing with ISP or firewall problems can prove difficult for retail customers whose primary focus is not IT, and having to visit Heathrow to deal with issues can prove costly both in terms of resource and down time. SITA have a dedicated on site IT extranet team with a wealth of experience in both implementing and supporting internet and IPSEC connectivity.

The following general requirements were required by the retail customer:

1. A fully resilient internet connection using separate physical hardware and using separate Internet pipes going out of Heathrow from different physical locations.
2. 20 meg of dedicated bandwidth.
3. Secure site to site communication via an IPSEC tunnel between a number of private IP subnets located throughout the main retail unit network and all IP subnets deployed at Heathrow.
4. Separation within a VPN in terms of security between different IP subnets used for different functions. For example - the tills and PC's should be on different VLANS. Tills should be able to communicate with other tills but not with PC's. Till's should not be able to communicate with the internet.
5. Full routing between any subnet in any terminal to any other subnet in any other terminal at Heathrow where desired. So essentially cross campus communication between devices where required.

A network topology for this deployment is provided below:



Conclusion

The Virtual Broadband methodology has created a new and expansive way of supplying customers an internet connection with an almost logical configuration, deployed and managed by SITA engineers. With many customers spread across the airport this type of connection offers flexibility and effortless communication campus wide without the need of separate connections.

With predominantly all of the end to end connection managed and supported by SITA, this has now offered customers' peace of mind knowing that their service availability will remain constant at all times.

Contacts

Contact: 0208 745 6565

Email: Heathrow@sita.aero

Contact Address: Compass Centre, Nelson Road, Hounslow, Middlesex, TW6 2GW

Legal Notice

Heathrow Airport Common Infrastructure Policy (CIP) and Heathrow Airport Limited reserves all of its rights and remedies in respect of the CIP including but not limited to those rights relating to scope, application and enforcement. The rights and remedies set out in the CIP are in addition to, and not exclusive of, any rights or remedies provided by law.

This document and the information contained therein are confidential and remains the property of Heathrow Airport Limited. The document may not be reproduced or the contents transmitted to any third party without the express written consent of Heathrow Airport Limited. This document and information contained therein is subject to contract.