CCP Colt IP Access Service Description

1 Overview

Colt IP Access provides you with a dedicated permanent access to the public Internet and a range of features such as access circuits, DNS, Managed Router and SMTP relay. In addition, a range of security and communication options are available.

Colt in Asia provides partner IP Access including network access via 3rd party as per customer requests.

The Service includes installation, configuration and management.

The following Add-ons are available, regional restrictions apply.

- Colt Managed Dedicated Firewall
- Colt Managed Virtual Firewall
- Colt IP Domain
- Colt Workforce Mobility

2 Technology platform

Colt IP Access sites can be directly connected to our wholly owned and managed city and long-distance fibre-optic infrastructure. Protected circuits are available in both the city and long-distance sections of our network as an option. They ensure high resilience by providing an alternative path in case of failure.

3 Network access

Colt IP Access Services can be provided:

- on-Net using our fibre end-to-end (for premises directly connected to our network)
- on-Net using secure 3rd party leased fibre in Asia
- off-Net using Colt's Unbundled Local Loop (ULL) digital subscriber line (DSL) services
- off-Net using contended (default) or uncontended (on customer request and where available) third-party other licensed operator (OLO) tail
- third party DSL

Colt IP Access services are installed during business hours. Business hours are 8.30 AM to 5.30 PM local time, Monday to Friday, excluding public or bank holidays. If you request installation of your Service outside of business hours this may be subject to additional installation charges.

4 Features

Depending on the geographical region, the following features are available as standard with the Colt IP Access Service. Regions are Colt Europe (EU), Japan (JP), Singapore (SG).

Feature	Description	Region
Provider-aggregated IP addresses	A range of fixed, dedicated provider-aggregated IP addresses is provided	EU,JP, SG
Provider-independent IP addresses	You can use provider-independent IP addresses with most of the access technologies	EU
Online performance reporting	Online service performance and service management reports are available as part of the IP Access service.	EU, JP
Billing	We offer fixed or usage-based billing for IP bandwidth usage. The billing model is 95% peak percentile with a sample taken every 5 minutes.	EU

5 Options

The following options may be available, depending on the specific implementation you require.

Feature	Description	Region
Managed Router	We can supply, install, configure, manage and maintain the router on your premises as part of the Service. Following new technology developments we may at our own discretion choose to install a Virtual CPE instead of a physical device on site, but in either case you will not have to provide your own CPE router or layer-3 routing function. If you do not select the managed router option you must provide your own CPE router or layer-3 routing function.	EU
Unmanaged Router	We can supply and install an unmanaged router on your premises as part of the Service. You will be responsible for the management/configuration, Colt will replace the hardware if it fails.	EU, SG
Resilient dual access	For business-critical Internet access services, it is possible to provide two separate CPEs connected via two separate access circuits. In addition, a resilient access with a third-party ISP can be provided.	EU

DSL Backup	We can protect the primary access circuit using a separate DSL circuit for backup purposes.	EU
Network Address Translation (NAT)	You can select NAT with a managed router.	EU, JP
Dynamic Host Configuration Protocol (DHCP)	We can provide DHCP services with a managed router.	EU
Router configuration views and Event Viewer	Read-only access to router configuration and events information is available via a secure website.	EU
SNMP read-only access	Provides visibility for the optional managed CPE router which terminates the IP access circuit at your site.	EU
Border Gateway Protocol-4 (BGP-4) feed	We can provide a BGP-4 feed for most access technologies (containing all or part of the BGP routes of the Internet). The BGP feed will periodically consume bandwidth on the access circuit.	EU, JP
SMTP mail relay/backup	SMTP mail relay and SMTP mail backup services are available.	EU
Domain Name System (DNS)	Colt offers recursive or authoritative DNS services.	EU, JP

In addition, a range of complementary Services can be provided with the baseline Service:

Feature	Description	Region
Colt IP Domain	Enables you to register additional domain name(s)	EU, JP
Colt IP Guardian* DDoS Monitoring and Mitigation Service	Provides enhanced protection against distributed denial of service attacks (DDoS)	EU, JP

* If the size of a DDoS attack is such that the integrity of the Colt IP/MPLS network is threatened and other Colt customers could be affected, we will discard all traffic destined for your IP address under attack in order to maintain the integrity of the Colt network (“black holing”).

For customers connected to other providers in addition to Colt (multi-homed customer): If traffic on another provider’s network due to an attack on the customer is redirected to the Colt IP/MPLS network we will be entitled to drop all the BGP sessions announcing the customer in order to protect the Colt IP/MPLS network.

With the exception of Colt Singapore, we have upgraded our Internet Service to support the IPv6 protocol. If you choose to use this new protocol you have the option of either using it exclusively or in combination with the existing IPv4 protocol. Use of IPv4 and IPv6 on the same line is referred to as a “dual-stack” service.

Colt Managed Dedicated Firewall (Europe)

The service includes a dedicated firewall device, separate from the router. Keeping firewalling features separate, with purpose-built hardware platform and security specific operating system enables higher performances.

The firewall is located on your premises and is installed and remotely managed by us and configured with your chosen security policy and firewall rule set.

Colt Managed Dedicated Firewall (MDF) is available in four different variants to match a wide range of service and performance needs.

Colt Managed Dedicated Firewall includes all the features available with Router-based Firewall. In addition, a high-availability configuration is available for enhanced resilience and the firewall can be aware of the VLANs (Virtual LANs) you may set-up (not available on the entry level variant).

With the exception of the entry level variant, all variants of the Colt Managed Dedicated Firewall are proactively monitored. We will monitor a range of parameters on your service including appliance availability, network throughput, CPU or memory utilisation. For each parameter we set a warning threshold. If the threshold is exceeded, we will investigate the cause, notifying you of the ongoing actions.

Web-based reporting is provided and includes details of the security policy deployed, firewall performance and activity statistics and an events viewer with configurable reporting intervals.

Options

Colt MDF can be provided with the following optional deep inspection capabilities as a chargeable extra:

Signature based intrusion protection - Identifies and blocks traffic at the transport layer based according to a database of known traffic profiles and behaviours that correspond to an attack (deep inspection signatures). The deep inspection capability available on the MDF platform is limited by the number of signatures in the database and therefore will not provide as comprehensive a level of protection as a dedicated stand-alone Intrusion Prevention System.

Colt Managed Virtual Firewall (Europe)

The service provides firewall features such as stateful packet filtering on IP address and port numbers, network IP address translation and screening of the protected networks, as well as basic logging. -

Managed Virtual Firewall is a fully managed service delivered from a shared infrastructure managed and hosted by Colt. You will be provided with a single virtual firewall instance on the shared hardware platform which will be fully separated from other customer firewall instances on the same platform by virtualisation technology. As a shared platform Colt remains responsible for all hardware-related issues. The service includes the following standard features

- Implementation of firewall policy as approved by you
- Log file retention
- Security functions and addressing

Static and dynamic network address translation (NAT) is supported.

Log files will be retained for events for not less than the last seven eight days through a secure portal on a rolling 30 days basis. This data can also be downloaded as a comma separated variable (CSV) file. The URL of the secure portal will be mentioned in your welcome kit.

Optional:

Any issues highlighted by the information contained in the log file should be addressed through the service modification process to initiate any security action.

You have the responsibility for reviewing the log data and deciding whether or not further action should be taken. Any additional change or modification requested by you will be charged by us, should it fall outside the standard features aforementioned.

Rules applicable to all Firewall types

It is expected that you have an existing security policy outlining the security parameters that will be used as the basis of the configuration of your Colt Router Based, Managed Virtual or Managed Dedicated Firewall. You are responsible for the security policy and implemented firewall rule set and for ensuring that your security policy and rule set meet your security requirements. (The firewall rule set is the technical implementation of the relevant parameters defined within the security policy).

As a result, you are responsible for any adverse effects (including any external attacks) that may be due to the security policy or rule set you provided for implementation. Our time and efforts to restore your services as a result of such an attack may incur additional Charges.

You are responsible for configuring VLANs at your premises.

Colt IP Domain (Europe)

We can register a domain name on your behalf, subject to availability. Two types of domain names can be registered:

- Country specific domain extensions (example: .de, .fr, and .it)
- Generic top level domains (example: .com, .org, .net)

The IP Domain - Registration service includes:

- Initial registration of your domain
- On going administration of your domain - charges may apply

We provide one (1) free domain name registration with the IP Access service. This domain name is limited to:

- A country specific domain extension from an extended Colt country]; or
- One of the following generic top level domains: com, org, net, biz, info, mobi, eu, asia

Colt Workforce Mobility (Europe)

Workforce Mobility enables end users to connect to your corporate network through a secured connection over the internet. Internet access to the end users has to be provided by you.

The following encryption options for securing the user's internet connection are available:

- Secured Socket Layer (SSL) encryption with different user access roles

You can authenticate user access requests using either:

- Our authentication systems and online portal
- Your authentication systems (Colt will forward all access requests to your servers)

You will need to provide all end-user support for the software and hardware provided as part of the Workforce Mobility Service. Our service provision and assurance is available only to your technical department and we will not provide support directly to your end-users.

Colt IP Guardian

Colt IP Guardian provides enhanced protection from Distributed Denial of Service (DDoS) attack.

If the size of a DDoS attack is such that the integrity of the Colt IP/MPLS network is threatened and other Colt customers could be affected, we will discard all traffic destined for your IP address under attack in order to maintain the integrity of the Colt network (black holing).

For Customers connected to other providers in addition to Colt (multi-homed Customer): If traffic on another provider's network due to an attack on the customer is redirected to the Colt IP/MPLS network we will be entitled to drop all the BGP

sessions announcing the Customer in order to protect the Colt IP/MPLS network.

Colt IP Guardian is available in three variants:

- Continuous – this is the default variant of the Service and provides continual and automatic mitigation against attack. You may call the Colt helpdesk to manually stop or amend the mitigation process but traffic will always be automatically redirected when an anomaly is detected.
- On-Demand - this variant of the service is the same as the Continuous variant, except that it also gives you the ability to manually activate and deactivate mitigations via the Colt portal. By default this is coupled with the same automated protection provided by the Continuous variant, but you have the option to turn this automatic protection off so that mitigations will not occur unless you manually start them. Alerts will be sent via email. Please note mitigations must not be run on a permanent basis. You should only start a mitigation when you genuinely believe that you are being attacked and should stop it once you believe the attack is over. Colt reserves the right to either cancel the service or amend the charges if this rule is not being adhered to. You have to activate and deactivate mitigations via the Colt portal, which should also be used to track progress of existing mitigations.
- Emergency Implementation – existing Colt IP Access customers who have not already purchased either the Continuous or the On-Demand variants listed above may contact us to request an emergency implementation of the service, usually in the midst of an attack or when an attack is imminent. The service is provided for a fixed duration and subject to a fixed, non-recurring charge as specified on the implementation form. As the service is provided on an emergency basis it does not include any long-term analysis of your normal traffic patterns and this may result in a greater risk of false positives than would be the case for the Continuous or On Demand standard services.