CCP Colt IP Access
Descripción de los servicios

1 Descripción general

Colt IP Access proporciona un acceso permanente dedicado a Internet y una gama de funcionalidades como circuitos de acceso, DNS, Managed Router y SMTP relay. Además, hay una gama de opciones de comunicación y seguridad disponibles.

Colt en Asia proporciona IP Access de partner que incluye acceso de red a través de terceros conforme a las solicitudes de los clientes.

El Servicio incluye instalación, configuración y gestión.

Los siguientes complementos están disponibles. Se aplican restricciones regionales.

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

2 Plataforma tecnológica

Las sedes de Colt IP Access pueden conectarse directamente a la infraestructura de fibra óptica de larga distancia y metropolitana de propiedad y gestión total de Colt. Los circuitos protegidos están disponibles, como opción, tanto en las secciones de larga distancia como metropolitanas de la red de Colt. Garantizan una elevada fiabilidad y ofrecen una ruta alternativa si se produce un fallo.

3 Acceso a la red

Los servicios Colt IP Access se pueden proporcionar:

- On-Net, con fibra de Colt extremo a extremo (para oficinas conectadas directamente a la red de Colt)
- On-Net mediante fibra contratada de terceros segura en Asia
- Off-Net, utilizando servicios de Digital Subscriber Line (DSL) de desagregación del bucle local (ULL) de Colt
- Off-Net, utilizando circuitos de otros operadores con licencia (OLO) con contención (predeterminado) o sin contención (a petición del Cliente y donde esté disponible)
- DSL de terceros

Los servicios de Colt IP Access se instalan durante el horario comercial. El horario comercial de Colt es de 8:30 a 17:30 hora local, de lunes a viernes, días festivos NO incluidos. Si el Cliente solicita que se instale el Servicio fuera del horario comercial, la instalación puede suponer unos costes de instalación adicionales.

4 Funcionalidades

Según la región geográfica, las siguientes funcionalidades están disponibles como estándar con el servicio Colt IP Access. Las regiones son Colt Europa (UE), Japón (JP), Singapur (SG).

Funcionalidades	**Descripción**	**Región**
Direcciones IP agregadas por el proveedor	Se ofrece una gama de direcciones IP dedicadas y agregadas por el proveedor	UE, JP, SG
Direcciones IP independientes del proveedor	Se pueden utilizar direcciones IP independientes del proveedor con la mayor parte de las tecnologías de acceso	UE
Informes de rendimiento online	Los informes sobre el rendimiento online y la gestión del Servicio se incluyen como parte del servicio IP Access.	UE, JP
Facturación	Se ofrece facturación por uso o facturación fija para el uso de ancho de banda IP. El modelo de facturación es el percentil máximo del 95 % con una muestra tomada cada 5 minutos.	UE

5 Opciones

En función de la implementación específica que el Cliente necesite, las opciones siguientes pueden estar disponibles.

CCP Colt IP Access
Descripción de los servicios

Funcionalidades	Descripción	Región
Router gestionado	Colt puede proporcionar, instalar, configurar, gestionar y realizar el mantenimiento del router en sus instalaciones como parte del Servicio. Gracias a los nuevos desarrollos tecnológicos, Colt puede ahora optar por instalar un CPE (equipo en las dependencias del Cliente) virtual en lugar de un dispositivo físico en la sede, si así lo cree conveniente. En cualquier caso, el Cliente no tendrá que proporcionar su propio router CPE o función de enrutamiento de nivel 3. Si la opción seleccionada no incluye un router gestionado, el Cliente deberá proporcionar su propio router CPE o función de enrutamiento de nivel 3.	UE
Router no gestionado	Colt puede suministrar e instalar un router no gestionado en las instalaciones del Cliente como parte del Servicio. El Cliente será responsable de la gestión/configuración y Colt sustituirá el hardware si falla.	UE, SG
Resilient Dual Access	Para los servicios de acceso a Internet imprescindibles para la empresa, se pueden proporcionar dos CPE independientes y conectados mediante dos circuitos de acceso separados y routers PE. También se puede proporcionar un acceso flexible con un ISP de terceros.	UE
Protección de capa 2 para servicios On-Net	Los circuitos locales IP Access estándar no están protegidos; en otras palabras, no tienen una ruta de backup de capa 2. Está disponible como complemento y proporciona una ruta de fibra de backup de capa 2 pero no incluye redundancia de PE o CPE.	UE
DSL Backup	Colt puede proteger el circuito de acceso primario mediante un circuito DSL independiente con fines de backup.	UE
Conversión de direcciones de red (NAT)	Puede seleccionar NAT con un router gestionado.	UE, JP
Protocolo de configuración de host dinámico (DHCP)	Colt puede proporcionar servicios DHCP con un router gestionado.	UE
Vistas de configuración del router y visor de eventos	A través de un sitio web seguro está disponible el acceso de solo lectura a la información de configuración del router y a la información de eventos.	UE
Acceso SNMP de sólo lectura	Proporciona visibilidad para el router CPE gestionado opcional que termina el circuito de acceso IP en la sede del Cliente.	UE
Datos de Border Gateway Protocol-4 (BGP-4)	Colt puede proporcionar datos BGP-4 para la mayoría de las tecnologías de acceso (que contengan todas o parte de las rutas BGP de Internet). Los datos BGP consumen periódicamente ancho de banda en el circuito de acceso.	UE, JP
SMTP Mail Relay/backup	Los servicios SMPT Mail Relay y backup están disponibles.	UE
Domain Name System (DNS)	Colt ofrece servicios DNS recursivos o autoritativos.	UE, JP

Además, se puede proporcionar una variedad de servicios complementarios con el servicio básico:

Funcionalidades	Descripción	Región
Colt IP Domain	Permite registrar nombres de dominio adicionales	UE, JP
Colt IP Guardian*	Proporciona una protección mejorada contra ataques distribuidos de denegación de servicio (DDoS)	UE, JP
Managed Dedicated Firewall	Proporciona un firewall de gestión física para las instalaciones del Cliente	UE
Colt Managed Virtual Firewall	Ofrece una funcionalidad del firewall sencilla y rentable en el backbone IP de Colt	UE

*Si el tamaño del ataque DDoS es de tal envergadura que la integridad de la red IP o MPLS de Colt se ve amenazada y otros Clientes de Colt pueden verse afectados, Colt descartará todo el tráfico destinado a su dirección IP que esté siendo atacada para mantener la integridad de la red de Colt (enrutamiento con reglas de filtrado).

Para los Clientes conectados a otros proveedores además de Colt (Cliente Multi Homing): si, debido a un ataque contra el Cliente, el tráfico en la red del otro proveedor se redirige a la red IP/MPLS de Colt, Colt tiene la potestad a dejar caer todas las sesiones BGP que anuncian al Cliente para proteger la red IP/MPLS de Colt.

Con la excepción de Colt Singapur, Colt ha actualizado el servicio de Internet para que sea compatible con el protocolo IPv6. Si el Cliente prefiere utilizar este protocolo, tiene la opción de utilizarlo de manera exclusiva o en combinación con el protocolo IPv4 existente. El uso de los protocolos IPv4 e IPv6 en la misma línea se conoce como servicio de doble pila.

Colt Managed Dedicated Firewall (MDF) (Europa)

El Servicio incluye un dispositivo de firewall dedicado, separado del router. Además de las funciones del firewall, la plataforma de hardware diseñada expresamente y el sistema operativo de seguridad permite un mayor rendimiento.

El firewall se ubica en las instalaciones del Cliente, Colt lo instala y gestiona de forma remota, y se configura con la política de seguridad y el conjunto de normas del firewall que el Cliente elija.

Colt Managed Dedicated Firewall (MDF) está disponible en cuatro opciones que cubren un gran número de necesidades de servicio y rendimiento.

Colt Managed Dedicated Firewall incluye todas las funciones disponibles con Router-Based Firewall. Asimismo, la configuración de alta disponibilidad ofrece una mejor redundancia, de modo que el firewall puede advertir los LAN virtuales (VLAN) que configure (no disponible con la opción de nivel de entrada).

Excepto la opción del nivel de entrada, todas las opciones de Colt Managed Dedicated Firewall se supervisan de forma proactiva. Colt supervisa diversos parámetros del Servicio, como la disponibilidad del equipo, el rendimiento de red, la CPU o la utilización de memoria. Para cada parámetro Colt establece un umbral de aviso. Si se ha excedido el umbral, Colt investigará el motivo y notificará al Cliente las acciones a seguir.

Se proporcionan informes basados en web y se incluyen detalles acerca de la política de seguridad empleada, el rendimiento del firewall y las estadísticas de actividades y el visor de eventos con intervalos de informes configurables.

Opciones

Colt MDF se puede proporcionar con las siguientes funcionalidades de inspección opcionales, como opción extra facturable:

Detección de intrusiones basada en firmas: identifica y bloquea el tráfico en la capa de transporte en función de una base de datos de perfiles y actividades de tráfico conocidos que corresponden con un ataque (firmas profundas de inspección). La funcionalidad de inspección profunda disponible en la plataforma MDF está limitada por el número de firmas de la base de datos y, por lo tanto, no proporciona un nivel de protección completo, como el de un sistema de prevención de intrusiones dedicado independiente.

Colt Managed Virtual Firewall (Europa)

El Servicio proporciona funcionalidades de firewall como, por ejemplo, el filtrado de paquetes por dirección IP y por números de puerto, la conversión de direcciones de red IP, el rastreo de las redes protegidas o un registro básico.

Managed Virtual Firewall es un servicio completamente gestionado que se presta en una infraestructura compartida gestionada y alojada por Colt. El Servicio proporciona una única instancia de firewall virtual para la plataforma de hardware compartida, completamente independiente del resto de instancias de firewall del Cliente residentes en la misma plataforma gracias al uso de la tecnología de virtualización. Dado que se trata de una plataforma compartida, Colt sigue siendo responsable de cualquier

cuestión relacionada con el hardware. El Servicio incluye las siguientes funcionalidades estándar:

- Implementación de la política del firewall aprobada por el Cliente
- Retención del archivo de registros
- Funciones de seguridad y direcciones

La conversión de direcciones de red dinámica y estática (NAT) también se admite.

Los archivos de registro de eventos de los últimos siete días se mantendrán en un portal seguro por períodos de treinta días sucesivos. Estos datos también se pueden descargar en forma de archivo de variables separadas por comas (CSV). La URL del portal seguro se comunicará al Cliente en la documentación de bienvenida al servicio.

Opcional:

Los problemas identificados por la información contenida en el archivo de registro se abordarán a través del proceso de modificación del servicio para iniciar una acción de seguridad.

El Cliente es responsable de revisar los datos de registro y decidir si necesita alguna corrección. Colt facturará los cambios o modificaciones adicionales que solicite el Cliente si no están incluidos en las funcionalidades estándar descritas anteriormente.

Normas aplicables a todos los tipos de firewall

Se espera que el Cliente cuente con una política de seguridad que establezca los parámetros de seguridad que se utilizarán como base de la configuración del servicio Colt Router Based Firewall, Managed Virtual Firewall o Managed Dedicated Firewall. El Cliente es el responsable de la política de seguridad y la normativa del firewall, y de asegurarse de que se cumplan los requisitos de seguridad. (El conjunto de normas del firewall es la implementación técnica de los parámetros relevantes definidos en la política de seguridad).

En consecuencia, el Cliente es responsable de cualquier efecto adverso (incluidos ataques externos) que pueda deberse a la política de seguridad o la normativa de la implementación. El tiempo y esfuerzos de Colt para restaurar el Servicio como resultado de un ataque puede implicar cargos adicionales.

El Cliente es responsable de configurar VLAN en sus instalaciones.

Colt IP Domain (Europa)

Colt puede registrar un nombre de dominio por cuenta del Cliente, sujeto a disponibilidad. Pueden registrarse dos tipos de nombre de dominio:

- Extensiones de dominio específicas de países (por ejemplo: .es, .fr o .it)
- Dominios genéricos de nivel superior (por ejemplo: .com, .org, .net)

El servicio de registro IP Domain incluye:

- Registro inicial del dominio
- Administración del dominio (puede implicar algún cargo adicional)

Colt proporciona un (1) registro de nombre de dominio gratuito con el servicio IP Access. El nombre de dominio tiene las limitaciones siguientes:

- Una extensión de dominio específico de un país desde un país extendido de Colt; o bien,
- Uno de los dominios genéricos de nivel superior siguientes: com, org, net, biz, info, mobi, eu, asia

Colt Workforce Mobility (Europa)

Workforce Mobility permite a los usuarios finales establecer una conexión segura con su red corporativa a través de Internet. El acceso a Internet de los usuarios finales debe proporcionarlo el Cliente.

Están disponibles las siguientes opciones de cifrado para proteger la conexión a Internet del usuario:

- Cifrado Secured Socket Layer (SSL) con diferentes perfiles de acceso de usuario.

El Cliente puede autenticar las solicitudes de acceso de los usuarios mediante:

- Los sistemas de autentificación y el portal online de Colt.
- Los sistemas de autentificación del Cliente (Colt reenviará todas las solicitudes de autenticación a los servidores del Cliente).

El Cliente deberá facilitar a sus usuarios finales toda la asistencia necesaria con el software y el hardware proporcionado como parte del servicio Workforce Mobility. La prestación de Servicio y su aseguramiento solo está disponible para el departamento de TI del Cliente y no se proporciona asistencia directamente a los usuarios finales del Cliente.

Colt IP Guardian

Colt IP Guardian ofrece protección reforzada contra ataques de denegación de servicio distribuido (DDoS).

Si el tamaño del ataque DDoS es de tal envergadura que la integridad de la red IP o MPLS de Colt se ve amenazada y otros Clientes de Colt pueden verse afectados, Colt descartará todo el tráfico destinado a la dirección IP del Cliente que esté siendo atacada para mantener la integridad de la red de Colt (enrutamiento con reglas de filtrado).

Para los Clientes conectados a otros proveedores además de Colt (Cliente Multi Homing): si, debido a un ataque contra el Cliente, el tráfico en la red del otro proveedor se redirige a la red IP/MPLS de Colt, Colt podrá dejar caer todas las sesiones BGP que anuncian al Cliente para proteger la red IP/MPLS de Colt.

Colt IP Guardian está disponible en dos versiones:

- Servicio estándar: IP Guardian mitiga los ataques automáticamente por defecto (la mitigación automática se encuentra "activada"). El Cliente puede confiar plenamente en la mitigación automática. Además Colt le da la posibilidad de activar y desactivar manualmente las mitigaciones mediante el portal de Colt.
  También tiene la opción de solicitar a Colt que desactive la mitigación automática durante la prestación del Servicio o posteriormente mediante las incidencias de asistencia para que no se produzcan mitigaciones, a menos que las inicie manualmente.
  Si opta por desactivar la mitigación automática e iniciar/detener las mitigaciones manualmente, el Cliente no debe ejecutar mitigaciones de manera permanente. Debe iniciar la mitigación de manera manual únicamente cuando tenga la certeza de que está siendo víctima de un ataque y debe detenerla cuando el ataque haya cesado. El portal Colt IP Guardian debe utilizarse para realizar el seguimiento del progreso de las mitigaciones existentes.
  Colt se reserva el derecho de cancelar el Servicio o modificar los cargos si no se observa esta regla.
- Implementación de emergencia: los Clientes de Colt IP Access existentes que no hayan adquirido IP Guardian estándar pueden contactar con Colt para solicitar una implementación de emergencia del Servicio, generalmente ante la amenaza de un ataque o si un ataque es inminente. El Servicio se proporciona por un período de tiempo limitado y está sujeto a un cargo fijo no periódico en el formulario de implementación. Dado que el servicio se proporciona en caso de emergencia, éste no incluye ningún análisis posterior de su tráfico y puede derivar en un mayor número de falsas alertas positivas.