CCP Colt IP Access
Descrizione del Servizio

1 Descrizione del Servizio

Colt IP Access fornisce un accesso dedicato permanente alla rete Internet pubblica, con una serie di funzionalità quali circuiti di accesso, DNS, router gestito e SMTP relay. Sono inoltre disponibili varie opzioni per la sicurezza e la comunicazione.

Colt in Asia offre IP Access da partner, compreso l'accesso alla rete mediante terza parte, in base alle richieste del Cliente.

Il Servizio include l'installazione, la configurazione e la gestione.

Sono disponibili le seguenti opzioni aggiuntive, ma la disponibilità dipende dall'area geografica.

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

2 Piattaforma tecnologica

I siti Colt IP Access possono essere connessi direttamente all'infrastruttura in fibra metropolitana e a lunga distanza, completamente gestita e di proprietà di Colt. Nella rete Colt i circuiti protetti sono disponibili come opzione sia nella connessione in area metropolitana che in quella a lunga distanza. Tali circuiti garantiscono un'elevata protezione fornendo un percorso alternativo in caso di guasto.

3 Accesso alla rete

I Servizi Colt IP Access possono essere forniti:

- On-Net utilizzando la connessione in fibra ottica end-to-end di Colt (per le sedi collegate direttamente alla rete Colt)
- On-Net utilizzando connessioni sicure in fibra noleggiata da terze parti in Asia
- Off-Net, utilizzando i servizi Digital Subscriber Line (DSL) dell'Unbundled Local Loop (ULL) di Colt
- Off-Net, utilizzando code condivise (opzione predefinita) o non condivise (su richiesta del Cliente e in base alla disponibilità) di terzi operatori autorizzati (OLO, Other Licensed Operator)
- DSL di terzi

I Servizi Colt IP Access vengono installati in orario d'ufficio. Per orario d'ufficio si intende dalle 8.30 alle 17.30 ora locale, dal lunedì al venerdì, a esclusione delle festività pubbliche. Su richiesta, e a pagamento, è possibile effettuare l'installazione fuori dall'orario di ufficio.

4 Caratteristiche

A seconda della posizione geografica, le caratteristiche elencate di seguito sono disponibili come standard con il servizio Colt IP Access. Le regioni geografiche sono Colt Europa (EU), Giappone (JP), Singapore (SG).

Caratteristica	Descrizione	Regione
Indirizzi IP aggregati dal provider	Viene fornita una serie di indirizzi IP, statici e dedicati, aggregati dal provider	EU, JP, SG
Indirizzi IP indipendenti dal provider	È possibile utilizzare indirizzi IP indipendenti dal provider con la maggior parte delle tecnologie di accesso	EU
Reportistica sulle prestazioni online	Il Servizio IP Access comprende report online sulle prestazioni e la gestione del Servizio.	EU, JP
Fatturazione	Per l'utilizzo dell'ampiezza di banda IP, è possibile scegliere tra fatturazione fissa o a consumo. Il modello di fatturazione è 95% picco percentile con un campione prelevato ogni 5 minuti.	EU

5 Opzioni

Possono essere disponibili le seguenti opzioni, a seconda dell'implementazione specifica richiesta dal Cliente.

Caratteristica	Descrizione	Regione
Router gestito	Come parte del Servizio, Colt può fornire, istallare, configurare e gestire il router presso la sede del Cliente. Sulla base degli sviluppi tecnologici, Colt può decidere di istallare, a propria discrezione, un CPE virtuale anziché un dispositivo fisico in sede. Tuttavia, in entrambi i casi, il Cliente non è tenuto a fornire il router CPE o la funzionalità di routing di livello 3. Se non si seleziona l'opzione del router gestito, il Cliente è tenuto a fornire il router CPE o la funzionalità di routing di livello 3.	EU
Router non gestito	Come parte del Servizio, Colt può fornire e istallare un router non gestito presso la sede del Cliente. Il Cliente è responsabile della gestione/configurazione e Colt sostituirà l'hardware in caso di guasto.	EU, SG

Dual access con ridondanza	Per i Servizi di accesso Internet di importanza critica, è possibile fornire due CPE distinti collegati tramite due circuiti di accesso separati. Può inoltre essere fornito un accesso ridondante tramite un ISP terza parte.	EU
Backup DSL	Colt può proteggere il circuito di accesso primario mediante un circuito DSL separato a scopo di backup.	EU
Network Address Translation (NAT)	Il Cliente può scegliere la NAT con un router gestito.	EU, JP
Dynamic Host Configuration Protocol (DHCP)	Colt può fornire servizi DHCP con un router gestito.	EU
Visualizzazione della configurazione del router e visualizzatore di eventi	È disponibile l'accesso in sola lettura alle informazioni di configurazione del router tramite un sito Web protetto.	EU
Accesso SNMP in sola lettura	Fornisce visibilità al router opzionale CPE gestito che termina il circuito IP Access presso la sede del Cliente.	EU
Feed Border Gateway Protocol-4 (BGP-4)	Per la maggior parte delle tecnologie di accesso si può richiedere un feed BGP-4 (che contiene tutti o parte degli instradamenti BGP di Internet). Il feed BGP consuma periodicamente ampiezza di banda nel circuito di accesso.	EU, JP
SMTP Mail Relay/Backup	Sono disponibili servizi di SMTP Mail Relay e SMTP Mail Backup.	EU
Domain Name System (DNS)	Colt offre servizi DNS ricorsivi o autorevoli.	EU, JP

Con il servizio di base possono inoltre essere forniti vari servizi complementari:

Caratteristica	Descrizione	Regione
Colt IP Domain	Consente di registrare nomi di dominio aggiuntivi	EU, JP
Colt IP Guardian*	Offre una maggiore protezione dagli attacchi DDoS (Distributed Denial of Service)	EU, JP
Servizio DDoS Monitoring e Mitigation		

* Se le dimensioni di un attacco DDoS fossero tali da minacciare l'integrità della rete IP/MPLS Colt e danneggiare altri Clienti di Colt, Colt provvederà a scartare tutto il traffico destinato all'indirizzo IP del Cliente sotto attacco per mantenere l'integrità della rete Colt ("*black holing*").

Per i Clienti collegati ad altri provider oltre a Colt (Clienti multi-homed): se, a causa di un attacco, il traffico sulla rete di un altro provider viene reindirizzato sulla rete IP/MPLS Colt, Colt si riserva il diritto di scartare tutte le sessioni BGP di comunicazione al Cliente al fine di proteggere la rete IP/MPLS Colt.

Fatta eccezione per Colt Singapore, Colt ha aggiornato i propri Servizi Internet in modo da supportare il protocollo IPv6. È possibile decidere di utilizzare questo nuovo protocollo in maniera esclusiva o congiuntamente al protocollo IPv4. L'uso di IPv4 e IPv6 sulla stessa linea consente la creazione di un servizio definibile "dual stack".

Colt Managed Dedicated Firewall (Europa)

Questo Servizio comprende un dispositivo firewall dedicato, separato dal router. Mantenendo separate delle funzioni di firewall, con una piattaforma hardware appositamente costruita e un sistema operativo specifico per la sicurezza, è possibile ottenere prestazioni superiori.

Il firewall è ubicato presso la sede del Cliente ed è installato e gestito da remoto da Colt e configurato con la politica di sicurezza e le regole di firewall scelte dal Cliente.

Colt Managed Dedicated Firewall (MDF) è disponibile in quattro diverse varianti adatte a un'ampia gamma di servizi ed esigenze.

Colt Managed Dedicated Firewall comprende tutte le funzioni disponibili con Router-Based Firewall. Inoltre, è disponibile una configurazione di alta disponibilità per una ridondanza migliore e il firewall può essere a conoscenza delle VLAN (LAN virtuali) impostate dal Cliente (non disponibile nella variante del livello base).

Con l'eccezione della variante del livello base, tutte le varianti di Colt Managed Dedicated Firewall sono monitorate in modo proattivo. Colt monitora una serie di parametri sul servizio del Cliente, inclusa la disponibilità dell'apparecchiatura, il rendimento della rete, la CPU o l'utilizzo della memoria. Per ciascun parametro viene stabilita una soglia di allarme. In caso di superamento di questa soglia, Colt indagherà la causa e notificherà al Cliente le azioni intraprese.

Viene fornita la reportistica basata sul Web che comprende dettagli della politica di sicurezza adottata, le statistiche di performance e attività del firewall e un visualizzatore di eventi con intervalli di reporting configurabili.

Opzioni

Colt MDF può essere fornito con funzionalità di ispezione approfondita opzionali a pagamento:

Protezione contro le intrusioni basata su firma - Identifica e blocca il traffico a livello di trasporto in base ai dati presenti in un database di profili di traffico conosciuti e comportamenti corrispondenti a un attacco (firme per ispezioni approfondite). La funzionalità di ispezione approfondita della piattaforma MDF è limitata dal numero di firme presenti nel database e, di conseguenza, non fornirà un livello di protezione completo quanto un sistema di protezione dalle intrusioni dedicato.

Colt Managed Virtual Firewall (Europa)

Il Servizio offre funzioni di firewall quali il filtraggio dei pacchetti in modalità "stateful" sull'indirizzo IP e i numeri di porta, la traduzione dell'indirizzo IP di rete e il monitoraggio delle reti protette, oltre ad attività di registrazione di base. -

Managed Virtual Firewall è un servizio completamente gestito, fornito da un'infrastruttura condivisa, gestita e ospitata da Colt. Nella piattaforma hardware condivisa, viene resa disponibile al Cliente una singola istanza di firewall virtuale, la quale, grazie alla tecnologia di virtualizzazione, è pienamente separata da altre istanze di firewall presenti nella stessa piattaforma. Colt è responsabile dei problemi relativi all'hardware della piattaforma condivisa. Il Servizio include le seguenti funzioni standard:

- Implementazione delle politiche del firewall approvate dal Cliente
- Mantenimento dei file di registro
- Indirizzamento e funzioni di sicurezza

Viene supportata la tecnologia NAT (Network Address Translation) statica e dinamica.

I file di registro saranno mantenuti per almeno sette/otto giorni dall'evento, tramite un portale sicuro che contiene dati relativi agli ultimi 30 giorni. Questi dati si possono inoltre scaricare sotto forma di file CSV (Comma Separated Variable). L'URL del portale sicuro si trova nel kit di benvenuto.

Opzionale:

Ogni problema evidenziato dalle informazioni contenute nel file di registro deve essere gestito tramite il processo di modifica del Servizio, al fine di attivare interventi relativi alla gestione della sicurezza.

Il Cliente ha la responsabilità di esaminare i dati di registro e decidere se è necessario o meno prendere ulteriori misure. Qualsiasi modifica o variazione aggiuntiva richiesta dal Cliente, qualora non rientri nelle funzioni standard di cui sopra, sarà addebitata al Cliente.

Regole applicabili a tutti i tipi di Firewall

Si presume che il Cliente disponga di una politica di sicurezza in cui sono definiti i parametri di sicurezza da utilizzare come base della configurazione del Colt Router Based, Managed Virtual o Managed Dedicated Firewall. Il Cliente è responsabile delle politiche di sicurezza e delle regole firewall implementate, nonché di garantire che la politica di sicurezza e le regole soddisfino i requisiti specifici. (Con il termine regole firewall si intende la realizzazione tecnica dei parametri pertinenti definiti nella politica di sicurezza).

Pertanto, eventuali effetti negativi (compresi gli attacchi esterni) dovuti alla politica o alle regole di sicurezza fornite per l'implementazione sono responsabilità del Cliente. Il tempo dedicato da Colt per ripristinare i servizi del Cliente a seguito di tali tipi di attacchi può essere soggetto ad ulteriore addebito.

Il Cliente è il solo responsabile della configurazione delle VLAN presso la propria sede.

Colt IP Domain (Europa)

Colt può registrare per conto del Cliente un nome di dominio, in base alla disponibilità. È possibile registrare due tipi di nomi di dominio:

- Estensioni di dominio specifiche per paese (esempio: .de, .fr e .it)
- Domini di livello superiore generici (esempio: .com, .org, .net)

Il Servizio IP Domain – Registration comprende:

- La registrazione iniziale del dominio del Cliente
- L'amministrazione continuativa del dominio del Cliente; questo servizio può essere soggetto ad addebito

Colt fornisce una (1) registrazione nome dominio gratuita con il Servizio IP Access. Questo nome di dominio è limitato a:

- Un'estensione di dominio specifica per paese da un paese Colt; oppure
- Uno dei seguenti domini di livello superiore generici: com, org, net, biz, info, mobi, eu, asia

Colt Workforce Mobility (Europa)

Workforce Mobility consente agli utenti finali di collegarsi alla rete aziendale del Cliente attraverso una connessione Internet protetta. L'accesso Internet agli utenti finali dovrà essere fornito dal Cliente.

Sono disponibili le seguenti opzioni di crittografia per la protezione della connessione a Internet degli utenti:

- Crittografia SSL (Secured Socket Layer) con diversi ruoli di accesso utente

Il Cliente può autenticare le richieste di accesso degli utenti utilizzando:

- I sistemi di autenticazione e il portale online di COLT
- I sistemi di autenticazione del Cliente (Colt inoltrerà tutte le richieste di accesso ai server del Cliente)

Il Cliente è responsabile per il supporto agli utenti finali relativo a software e hardware forniti con il Servizio Workforce Mobility. La fornitura del Servizio di Colt e la

relativa assistenza sono disponibili solo per il reparto tecnico del Cliente, Colt non fornisce assistenza diretta agli utenti finali del Cliente.

Colt IP Guardian

Colt IP Guardian offre una protezione avanzata dagli attacchi DDoS (Distributed Denial of Service).

Se le dimensioni di un attacco DDoS fossero tali da minacciare l'integrità della rete IP/MPLS Colt e danneggiare altri clienti di Colt, provvederemo a scartare tutto il traffico destinato all' indirizzo IP del Cliente sotto attacco per mantenere l'integrità della rete Colt (*black holing*)

Per i Clienti collegati ad altri provider oltre a Colt (Clienti multi-homed): se, a causa di un attacco, il traffico sulla rete di un altro provider viene reindirizzato sulla rete IP/MPLS Colt, avremo il diritto di scartare tutte le sessioni BGP di comunicazione al Cliente al fine di proteggere la rete IP/MPLS Colt.

Colt IP Guardian è disponibile in tre varianti:

- Continuous - Si tratta della variante predefinita del Servizio, in grado di garantire la mitigazione automatica e costante degli attacchi. Sebbene il Cliente abbia la possibilità di contattare l'helpdesk di Colt affinché intervenga per interrompere o correggere manualmente il processo di attenuazione, il traffico sarà sempre reindirizzato automaticamente in caso di rilevamento di un comportamento anomalo.
- On Demand - Questa variante del Servizio presenta le stesse caratteristiche della variante Continuous, a eccezione del fatto che consente di attivare e disattivare manualmente i processi di mitigazione tramite il portale Colt. Come impostazione predefinita, fornisce anche la stessa protezione automatizzata garantita dalla variante Continuous, che, qualora necessario, il Cliente può disattivare affinché i processi di mitigazione vengano eseguiti esclusivamente tramite attivazione manuale. Gli avvisi e le notifiche verranno inviati tramite e-mail. I processi di mitigazione non devono essere attivi su base permanente. È necessario avviare un processo di mitigazione solo quando si ha la certezza di essere soggetti ad un attacco in un determinato momento, e sarà opportuno arrestare il processo quando si ritiene che l'attacco sia terminato. Qualora non ci si attenga scrupolosamente a tale criterio, Colt si riserva il diritto di annullare il Servizio o di rettificarne il costo. È necessario attivare e disattivare i processi di mitigazione tramite il portale Colt, che permette anche di monitorare l'avanzamento dei processi di mitigazione già in corso.
- Emergency Implementation - I Clienti con Colt IP Access esistenti che non hanno ancora acquistato le varianti Continuous o On-Demand menzionate possono contattare Colt per richiedere la variante Emergency Implementation del Servizio mentre un attacco è in corso o in procinto di verificarsi. Il servizio viene fornito per una durata prestabilita ed è soggetto a una tariffa fissa non ricorrente, in linea con quanto specificato nel modulo di implementazione. Poiché il Servizio viene fornito in base al verificarsi di condizioni di emergenza, non include alcuna analisi di lungo termine dei normali schemi di traffico e ciò potrebbe comportare un rischio maggiore di falsi positivi rispetto alle varianti Continuous e On Demand del Servizio.