



Interoute GCloud 10 Service Definition

SD-WAN – Enterprise Edge

Proposal Date: 23rd May 2018

ENGINEERED FOR
THE AMBITIOUS

interoute
interoute.com

VERSION HISTORY

Version	Date	Title	Author
V0.1	23 rd May 2018	GCloud 10 – Service Definition – Enterprise Edge	Interoute

All quotes, offers or proposals are (i) made based on Interoute's standard terms and conditions (ii) subject to contract, survey and availability; and (iii) only valid for a period of 30 days from the date of this message.

CONFIDENTIALITY STATEMENT

© Interoute 2018

This document contains information proprietary to and/or considered confidential by Interoute. Except as otherwise provided no part of this document may be reproduced, stored or transmitted in any form or by any means whether graphic, electronic or mechanical, including photocopying, recording, taping or storage in any information retrieval system, for any purpose, without prior written permission of Interoute.

Interoute is a trading name of Interoute Communications Limited, registered in England number 04472687, registered address: Interoute, 31st Floor, 25 Canada Square, Canary Wharf, London E14 5LQ.

Nothing within this document may be construed as an offer to supply goods or services except where explicitly stated. All sales are subject to contract.

Interoute and GTT

On Monday 26th February 2018, it was announced GTT had reached a definitive agreement to purchase 100% of the shares of Interoute. The acquisition is expected to close in the second half of 2018 as it is subject to customary regulatory clearances.

GTT Communications, Inc., is a publicly traded company on the New York Stock Exchange (NYSE: GTT) that provides multinational clients with connectivity to the cloud through a comprehensive suite of cloud networking services, including wide area networking, internet, optical transport, managed services and voice services.

Once the acquisition is complete the combination of Interoute and GTT will bring additional resources, deeper geographic reach and enhanced technical skills. This will enable us to provide you with products and services in more places than ever before. The combined company will bring together Interoute's depth and reach in Europe with GTT's fast-growing, global cloud networking business and dense connectivity footprint in North America.

As the transaction progresses towards completion over the coming months, Interoute will continue to run as an independent business, with no material changes. And as we enter this next stage of our development we will remain dedicated to serving you and supporting your business with the services it needs to thrive. Our business is joining with another like-minded, customer focused service provider that will enable us to extend our ability to support the best company's in the world, with advanced infrastructure and solutions, from the Ground to the Cloud.

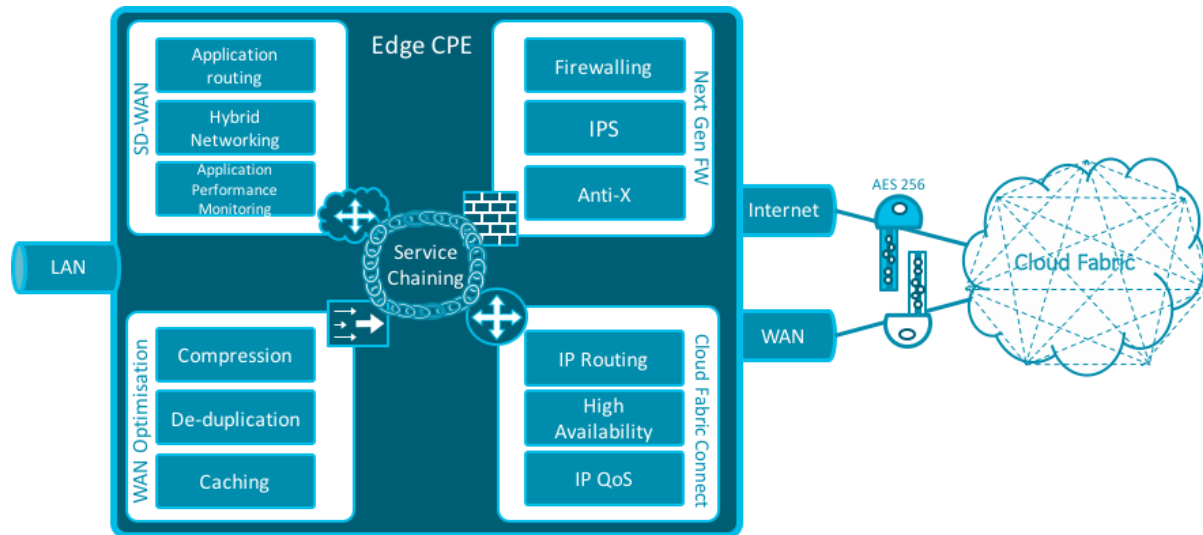
Contents

1.	Product Overview	5
1.1	Service Options	6
2.	SD-WAN Service	7
2.1	Service Overview	7
2.1.1	Benefits	8
2.2	Architecture	9
2.2.1	Virtual Appliance	9
2.2.2	Cloud Gateways	9
2.2.3	Central Management & Orchestration	9
2.3	Standard Features	9
2.3.1	Tunnel Bonding	9
2.3.2	Dynamic Path Control	10
2.3.3	Path Conditioning	10
2.3.4	Application Visibility and Control	10
2.3.5	Business Intent Overlays	10
2.3.6	Quality of Service (QoS)	11
2.3.7	In-flight data encryption	11
2.3.8	At-rest data encryption	11
2.3.9	Integrated firewall	11
2.3.10	Software as a Service (SaaS) application optimisation	11
2.3.11	Network service and features	12
3.1	WAN Optimisation (Optional Service)	12
3.2	Cloud Fabric	13
2.5.1	Fast path routing	14
2.5.2	Cloud peering & Direct Connections	14
2.6	Gateways	15
2.6.1	WAN Optimisation Gateway	15
2.6.2	Enhanced Internet Overlay Performance & 3 rd Party Network Integration	16
2.6.3	Regional Next Generation Firewall Hubs	16
2.6.4	Hybrid network integration points	16
3.	Next Generation Firewall Service	17
3.1	Service Overview	17
3.2	Architecture	17
3.3	Standard Features	17
4.	Interoute Edge Devices	19

5.	Service Delivery and Operating Models	20
5.1	Device Implementation	20
5.2	Standard Changes	20
5.3	Managed Service Model	22
5.3.1	Roles and Responsibilities	22
5.4	Self Service Model Interfaces	23
	5.4.1 Next Generation Firewall	23
	5.4.2 Direct Management	23
5.5	SD-WAN Reporting	24
5.6	Firewall reporting	28
5.7	Professional Services	28
6.	IP Network Connectivity	29
6.1	Network Requirements	29
7.	Service Availability & Coverage	30
7.1	Delivery complexity levels	30
7.2	Service Availability Tables	30
8.	Professional Services	33
8.1	Project Management	33
	8.1.1 Migration Approach	33
	8.1.2 Migration Method	34
8.2	Service Management	34
	8.2.1 Operational Support for Interoute's Unified ICT Portfolio	35
	8.2.2 Operational Management	35
	8.2.3 Network Operating Centre (NOC)	38
9.	Virtual Data Centre Service Management	40
9.1	VDC vTools	41
9.2	Escalation Process	42
9.3	Defined Service Requests and Events	43
9.4	Escalation Summary	44
9.5	VDC Solution Architecture: Resiliency	44

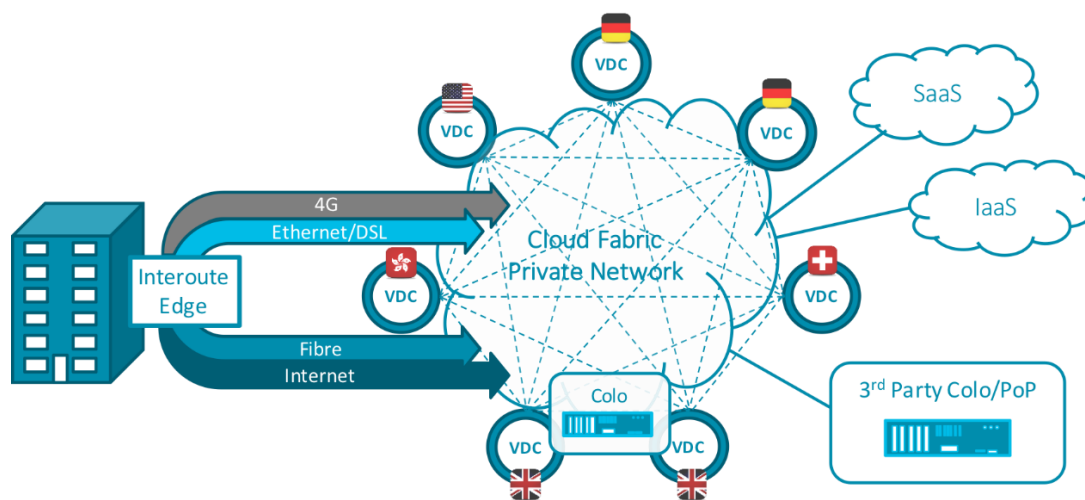
1. Product Overview

Interoute Enterprise Edge is a software defined platform approach to WAN endpoints. It leverages virtualisation and cloud technology to provide multiple flexible services such as SD-WAN, Next Generation Firewall and IP routing. Interoute Edge can also replace traditional CPE routing devices, offering flexibility and a future-proof platform for service delivery.



Edge Platform Overview.

Interoute Edge connects customers into Interoute’s Cloud Fabric – a global, Software-Defined intelligent backbone. Cloud Fabric offers flexibility of access networks and provides reliable and high-performance connections between Edge sites and cloud applications, regardless of underlying connectivity. Interoute’s Virtual Data Centre IaaS platform is also directly integrated for an end-to-end cloud and network infrastructure solution.



Flexible access & cloud integration.

Edge devices are simply connected to access networks and are managed and controlled via Interoute’s “My Services” portal.

1.1 Service Options

Service	Availability
SD-WAN	Standard
WAN Optimisation	Optional
Next Generation Firewall	Optional

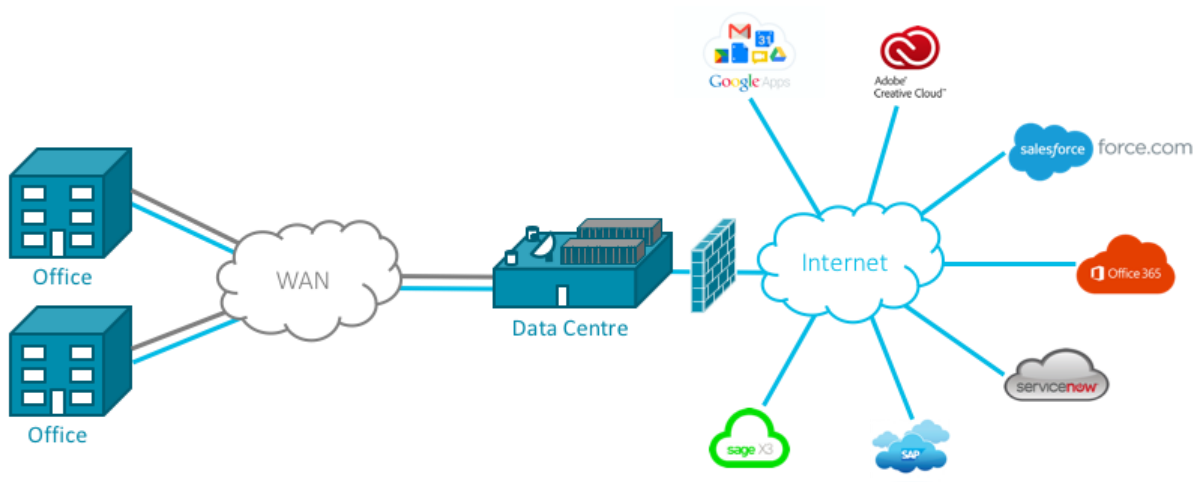
2. SD-WAN Service

2.1 Service Overview

Traditional networks were designed to deliver applications from a central datacentre, with low latency from each site. As applications move to the cloud, traffic can take an indirect route, resulting in poor performance.

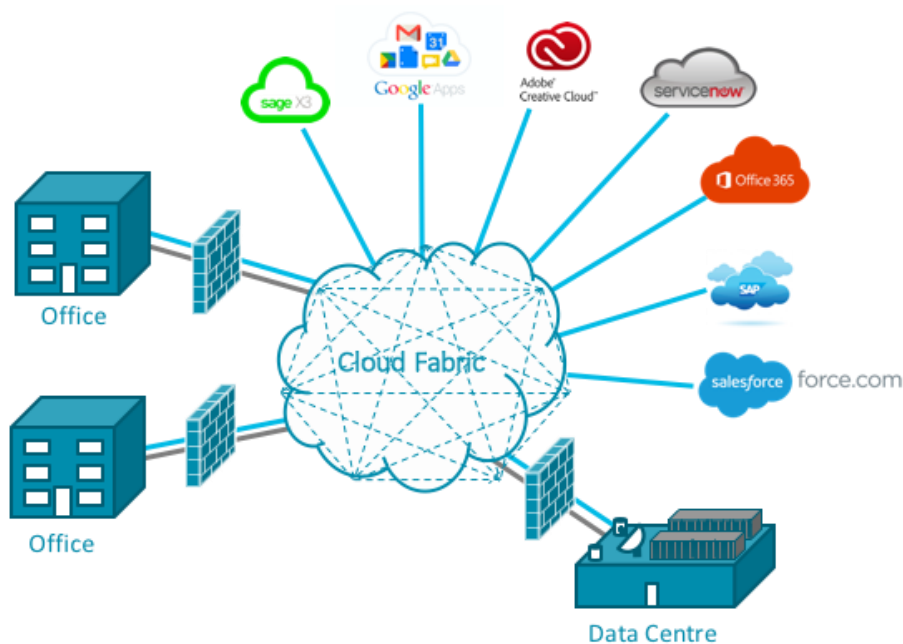
Interoute's Edge Access product optimises access to applications in the data centre and the cloud.

SD-WAN offers benefits over traditional router appliance-based WANs. It provides a software defined overlay to traditional networks which abstract the connectivity access mechanism and provides an application connection approach. Logical application connections can also be built over multiple access types (such as a private WAN and Internet circuits) as well as load-balanced across multiple circuits.



Traditional WAN design

The SD-WAN model de-centralises the traditional network perimeter and reduces the distance between users and resources. Policies can be defined based on application or user requirements to achieve the most effective and efficient path. The service can offer simplification, performance and cost benefits for branch office connections, especially when delivering connections to cloud applications.



Hybrid SD-WAN design

2.1.1 Benefits

Faster access to applications

- With Interoute Edge Access, all application traffic takes the most suitable route.
- Part of the Enterprise Digital Platform, our unique Cloud Fabric binds together all your locations with cloud providers on our low-latency network backbone and delivers application performance aware routing.
- Unlike other SD-WAN solutions, Interoute controls the network routing and uses the fastest route, not the lowest cost.

Lower network costs

- The hybrid networking approach enables the use of low-cost, high-bandwidth internet circuits together with business-critical connections.
- Dynamic Path Control directs and optimises traffic over both access types on the optimal, best performing path for the application.
- Integrated network acceleration reduces the bandwidth requirement.

Reliable and secure connections

- Our unique cloud fabric adapts with demand to deliver predictable and reliable connections.
- Business intent policies deliver application-defined QoS.
- Edge Access resolves complications of assembly of data from multi paths and out-of-sequence packets.
- All data is encrypted in-flight using AES 256, whether using a private network or the internet.

2.2 Architecture

2.2.1 Virtual Appliance

The SD-WAN service is built on virtual appliances installed on the physical Edge device. Overlay policies and dynamic path control facilitate the use of multiple IP connections simultaneously. They dynamically adapt the use of the underlying IP networks based on policy, availability and performance of application connections.

2.2.2 Cloud Gateways

Edge gateways, which are deployed in Interoute's Virtual Data Centre platform provide cloud-based connections between segregated access networks. This capability abstracts the underlying access networks into one logical, blended network domain and enables all Edge devices to communicate over any of the available access networks. This capability enables:

- Different access networks to function as backup connections in the case of a failure or service degradation. For example, private connections can failover to Internet connections.
- Policies to be applied on a per application basis to prefer different access networks. For example, cloud applications to prefer Internet, whereas privately hosted ERP prefer private networks.
- The active use of all available network access investments.

2.2.3 Central Management & Orchestration

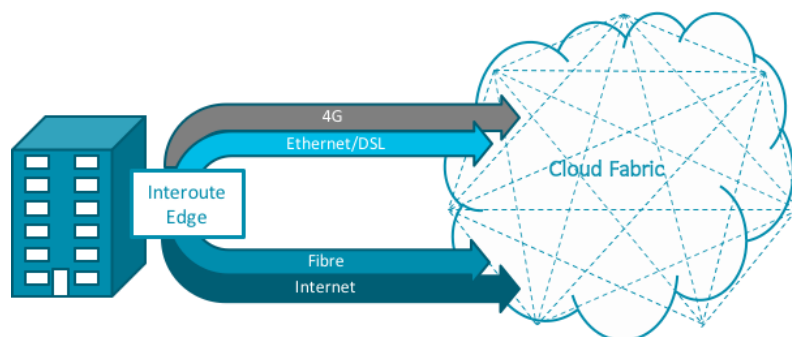
Within "My Services", a centralised orchestration platform manages and controls the configuration of SD-WAN services and gateways within a single logical domain per SD-WAN.

2.3 Standard Features

This section describes the standard technical features of the SD-WAN service.

2.3.1 Tunnel Bonding

Configured from two or more physical WAN transport services, bonded tunnels form a single logical overlay connection, aggregating the performance of all underlying links. If a link fails, the remaining transport links continue to carry all traffic avoiding application interruption.



Any access type

2.3.2 Dynamic Path Control

Dynamic Path Control (DPC) is a key feature of the SD-WAN service. DPC provides real-time traffic steering over any access link based on policies. In the event of an outage or brownout, DPC automatically fails-over to the secondary connection in less than one second.

DPC enables the full utilisation of all circuits at each location. Enabling the simultaneous use of multiple WAN links has traditionally been difficult because of limitations in routing protocols.

DPC eliminates the active/standby configuration, improving the reliability and performance for branch office applications. The traffic engineering decision is made by DPC, not layer-three routing, intelligently routing or load balancing traffic across the available links. This allows what was a standby line to be brought online without the complexity of pure IP routing.

Policies can be applied that make more intelligent decisions about how the access links are used and which path is used by each application. For example, a user can create policies that would route their most critical traffic such as VoIP, video conferencing and ERP traffic to always use the private WAN, while the rest of the traffic is load balanced.

2.3.3 Path Conditioning

Path Conditioning overcomes the adverse effects of dropped and out-of-order packets that can occur across the network, especially on less reliable access circuits, such as LTE, broadband or satellite.

Path Conditioning improves performance and reliability of access networks. Path Conditioning complements DPC by overcoming the effects of dropped and out-of-order packets on connections.

Path Conditioning is achieved by using the following techniques:

- **Adaptive Forward Error Correction (FEC).** The SD-WAN service uses packet-level FEC to reconstitute lost packets at the far end of a WAN link, avoiding delays that come with multiple round-trip retransmissions. This enables WANs to easily recover from packet loss, regardless of the reason. The solution dynamically adjusts FEC in response to changing link conditions to minimise overhead.
- **Real-time Packet Order Correction (POC).** The SD-WAN service re-sequences packets across all IP flows on the far end of a WAN link to avoid retransmissions that occur when packets arrive out of order.

2.3.4 Application Visibility and Control

The SD-WAN service identifies applications on the first packet to deliver SaaS and trusted web application traffic directly to the Internet while directing unknown or suspicious traffic to the data centre firewall or IDS/IPS. First packet application identification is especially important when branches are deployed behind Network Address Translation (NAT); the correct path must be selected based on the first packet to avoid session interruption.

2.3.5 Business Intent Overlays

Business Intent Overlays (or BIOs) are used by SD-WAN service to categorise and steer the traffic across any available links, similarly to how VLANs are deployed in an internal network to isolate and control the various types of traffic. Each Business Intent Overlay supports applying specific traffic policies such as intended routing topologies, WAN optimisation or compression, QoS features and so on, which are used to steer the traffic dynamically in accordance with the policy.

2.3.6 Quality of Service (QoS)

The SD-WAN service offers up to six QoS queues. The QoS scheme is the same as that used across all other Interoute connectivity products ensuring seamless interworking with standard MPLS/VPN CPE.

Each queue is set based on the customers need with a maximum and minimum percentage of the total bandwidth. QoS is honoured for both pass-through traffic which is routed into the underlay network (typically an MPLS/VPN) or overlay networks.

2.3.7 In-flight data encryption

The SD-Wan service uses 256-bit AES encryption to secure all WAN traffic in an overlay tunnel. All enterprise data in-flight across the SD-WAN encrypted tunnel fabric (SD-WAN overlay) is secured without any performance degradation.

2.3.8 At-rest data encryption

The SD-WAN service encrypts any data stored at rest on the virtual appliance with AES-128.

2.3.9 Integrated firewall

A firewall provides segregation between public and private networks, or between different sections of the internal corporate network.

Firewall Modes

The firewall modes enable the selection of the basic level of security at each location. These can be deployed in three different 'firewall' modes, each with different properties as described below:

Stateful: this permits only LAN to WAN pass-through traffic so allows users on the LAN to browse the Internet for example. It also allows all traffic sourced from an SD-WAN service IPsec tunnel (site to site SD-WAN traffic) or to an IPsec SD-WAN service tunnel.

Hardened: Enables direct deployment of SD-WAN on the Internet. No unauthorised outside traffic is allowed to enter the site. If a packet is not in the encrypted tunnel it is denied access and immediately dropped. Interfaces set this way only allow tunnelled traffic from other SD-WAN service devices and allow no traffic to breakout locally to the Internet. **Hardened is the default option for Internet connected sites.**

Allow All: this permits completely unrestricted WAN to LAN and LAN to WAN communication for both tunnel and un-tunnelled traffic. This is not normally recommended for Internet connected sites. **Allow all is the default option for privately connected sites.**

***Note:** This integrated firewall is separate from the Next Generation firewall service.*

2.3.10 Software as a Service (SaaS) application optimisation

SaaS optimisation is a unique feature of the SD-WAN service. It delivers real-time updates on the best performing path to reach hundreds of Software-as-a-Service (SaaS) applications (including Salesforce and Office 365), ensuring users connect to their applications in the fastest, most intelligent way available. By constantly aggregating and exchanging metrics about SaaS providers across the entire Interoute network and delivering real-time updates to the Edge devices on the optimal, best performing path. The Edge devices then use this data to measure packet loss, latency and other metrics from their locations to the different cloud

services, always ensuring that local users are connected to their cloud applications in the fastest and most efficient way.

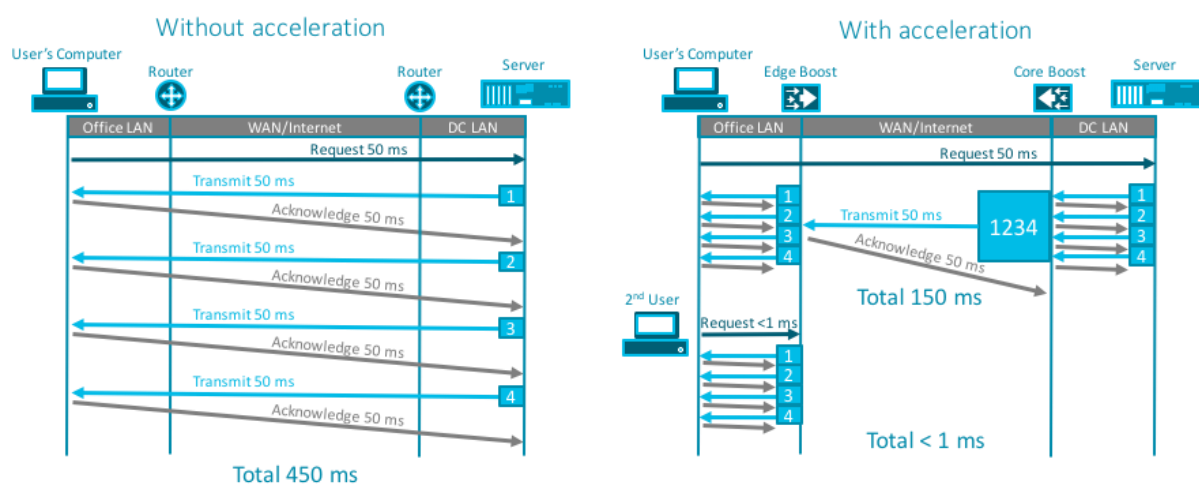
2.3.11 Network service and features

This section defines the supported network services and features:

- Static Routes
- BGP
- IPv4
- DHCP
- DHCP Relay
- SNMP
- Netflow
- QoS (6 levels)

3.1 WAN Optimisation (Optional Service)

WAN optimisation provides additional performance for specific locations and applications. This is of importance where physical distance between the user and the application degrades performance. For example, where sites are remote from the data centre or for cloud applications. In these scenarios, performance has less to do with available bandwidth, but rather network latency – the time it takes to send and receive data packets.



WAN optimisation overview.

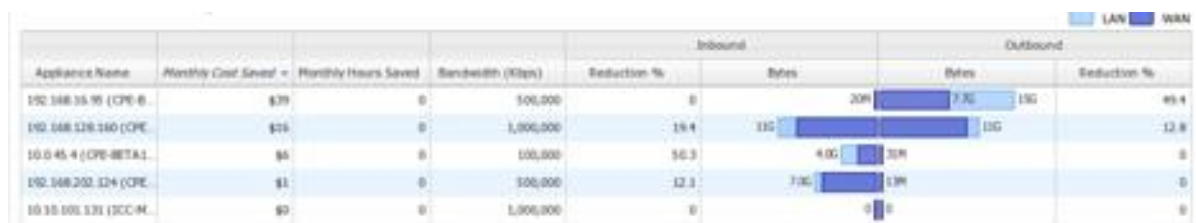
WAN optimisation achieves this using latency mitigation and data reduction techniques.

Network optimization

Network optimization uses TCP optimisation to reduce the effects of jitter and network latency. Commonly-used protocols like TCP or SMB/CIFS are chatty in nature and stop transmitting while waiting for far end acknowledgement – this behaviour dramatically reduces performance particularly in environments with high latencies. The optimisation technology used by SD-WAN service allows for LAN-like responsiveness regardless of the actual latency on the WAN circuit.

Bandwidth optimization

SD-WAN service's bandwidth optimization feature uses de-duplication and compression to more effectively use the available bandwidth, dramatically reducing WAN bandwidth requirements and increasing response speeds by locally serving traffic requests.



Appliance Name	Monthly Cost Saved	Monthly Hours Saved	Bandwidth (Kbps)	Reduction %	Inbound Bytes	Outbound Bytes	Reduction %
192.168.15.15 (CPE-B)	\$39	0	100,000	0	20M	7.7G	99.4
192.168.116.140 (CPE)	\$26	0	1,000,000	19.4	11G	13G	12.8
10.0.45.4 (CPE-BETA1)	\$0	0	100,000	50.3	4.0G	20M	0
192.168.202.124 (CPE)	\$1	0	100,000	12.1	7.7G	1.3M	0
10.10.100.131 (CCO-M)	\$0	0	1,000,000	0	0	0	0

Reporting optimised bandwidth

Note: Encrypted application traffic will not be de-duplicated or compressed unless a certificate/public and private key are available and supplied by the customer.

3.2 Cloud Fabric

Interoute's software defined Cloud Fabric provides a single, private global backbone. It delivers fast performance, consistently low latencies and minimal packet loss for connected sites.



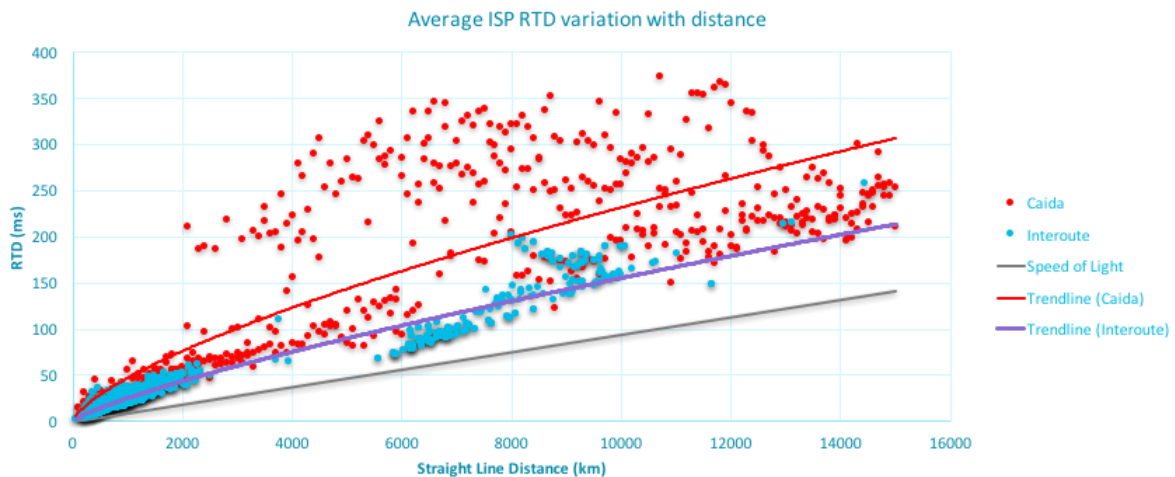
Cloud Fabric Backbone

2.5.1 Fast path routing

Cloud fabric is configured for fastest path routing, not lowest cost connections. The backbone vastly outperforms most internet connections with predictable and consistent latency. The graphic below shows the round-trip delay (RTD) of connections over a distance. Three sets of data are represented:

1. The grey line is the speed of light, which is a theoretical limit of performance.
2. The red dots and trend line represent latencies of commodity internet connections. The data is taken from the Centre for Applied Internet Data Analysis (CAIDA), an independent 3rd party.
3. The blue dots and purple trend line is the RTD between all points of presence two points on the Interoute backbone.

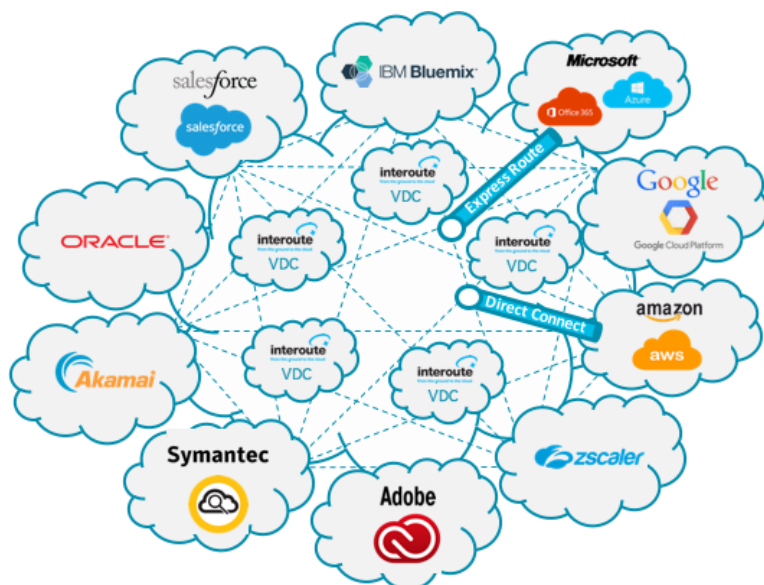
The data demonstrates the varied performance and inconsistency of typical internet connections, whereas the Interoute backbone enjoys predictable and better performing connections.



Average ISP RTD variation with distance

2.5.2 Cloud peering & Direct Connections

Cloud Fabric provides multiple on-net routes to major cloud provider destination. Connections do not traverse 3rd party IP networks using uncontrolled routing policies. We peer directly and control the routing.



Cloud Peering

Cloud Direct

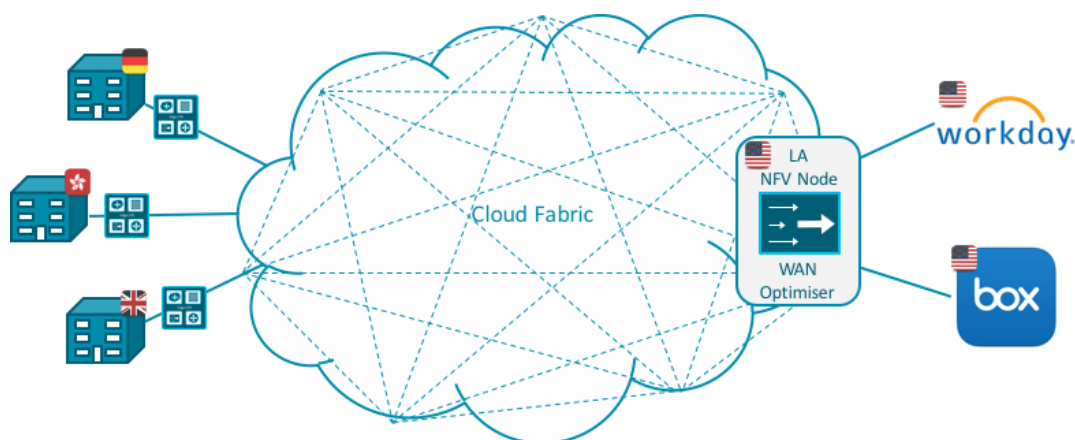
Direct connections to cloud providers such as Microsoft and AWS are available using dedicated private network connections. For more information, see the Cloud Direct product pages.

2.6 Gateways

Gateways can be deployed on Interoute's VDC (global IaaS platform) to connect into Cloud Fabric at strategic locations, including Europe, North America and ASIA-PAC to enhance the SD-WAN service.

2.6.1 WAN Optimisation Gateway

Provisioning cloud gateways with WAN optimisation capabilities enables the extension of WAN optimisation services to virtual sites within the SD-WAN. This can provide particular advantages to aggregate site connections into remote cloud services, optimising traffic over large distances for maximum benefit.



Cloud WAN Optimisation Gateway Architecture

2.6.2 Enhanced Internet Overlay Performance & 3rd Party Network Integration

Sites connecting to a wider SD-WAN using independently-sourced access circuits can connect into a regional cloud gateway. In doing so, they benefit from Interoute's Cloud Fabric, with assured high throughput on our low-latency global backbone.

2.6.3 Regional Next Generation Firewall Hubs

Regional hubs can be used for centralised delivery of Next Generation firewalls. This approach complements deployments where Next Generation firewall services are not deployed on Edge devices and "hardened" SD-WAN security policy is in place.

2.6.4 Hybrid network integration points

Cloud gateways provide integration points for public and private access circuits into one logical overlay hybrid network. This extends Dynamic Path Control, Path Conditioning and Business Intent Overlay functionality into regional hubs within the cloud. Available at multiple locations across the globe. It enables public and private access connections to effectively be utilised as backup circuits to each other, despite connecting to different access networks.

3. Next Generation Firewall Service

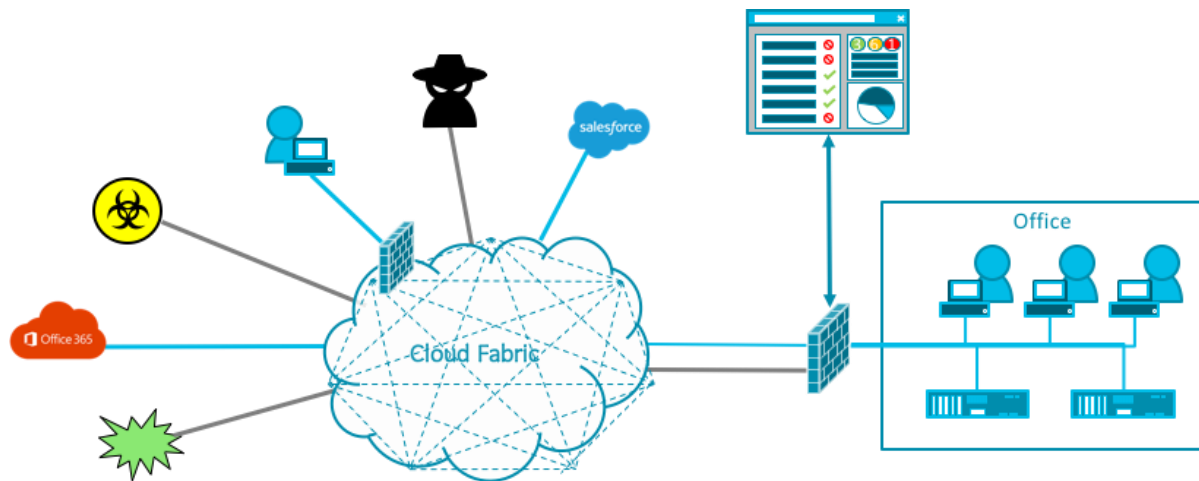
3.1 Service Overview

Next Generation Firewalls have heightened application-detection capabilities which enable application aware rule sets to be implemented. In addition, they include several additional security capabilities that were previously the domain of separate dedicated systems, such as Intrusion Prevention, URL filtering, Anti-virus and anti-malware. This heightened application awareness and Unified Threat Management (UTM) approach provides a more stringent defence against a broader range of attacks.

3.2 Architecture

The Next Generation firewall platform leverages virtual appliances installed on the Interoute Edge devices. Traffic is passed through the firewall and inspected using the advanced UTM capabilities.

An optional centralised orchestration platform manages and controls the configuration of next generation firewall services. Firewall policies can be managed and pushed to multiple Edge devices as a single group.



Central firewall management

3.3 Standard Features

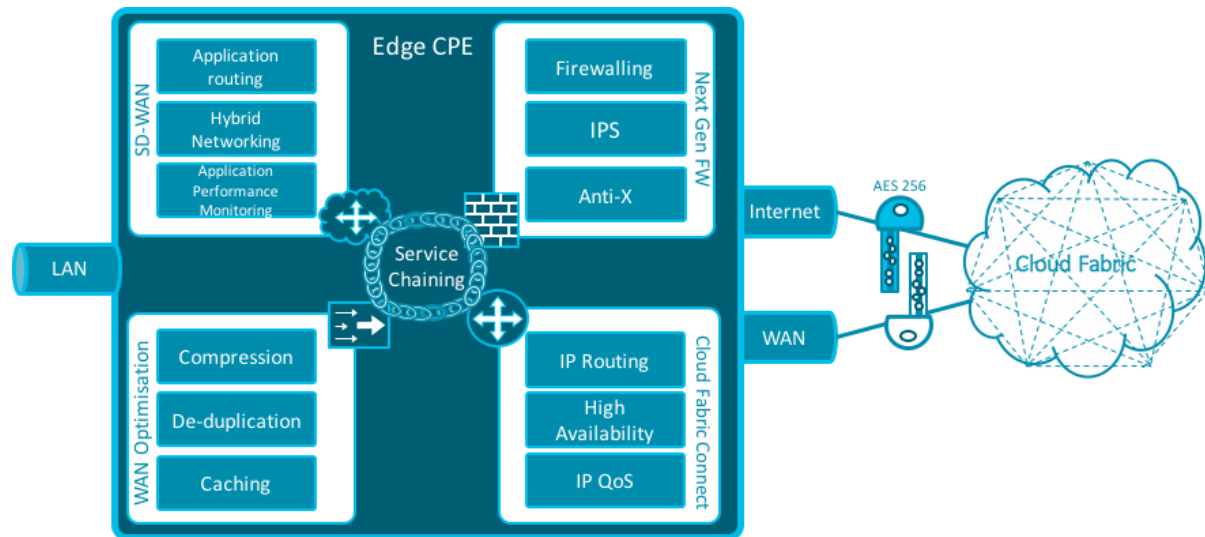
This section describes the technical features of the Next Generation Firewall service.

Features		Description
	Stateful packet inspection	Apply Standard policy based upon ports & protocols
	Application Awareness	Provide richer and more accurate traffic classification based on Vendor's application ID database
	Intrusion Prevention System	Block or Alert against known threat signatures, such as network and application layer vulnerability exploits, buffer overflows, DoS attacks and port scans.

	Features	Description
Security	Anti-Virus & Malware protection	Malicious code protection blocks millions of known malware variants, including those hidden within compressed files as well as known PDF viruses
	Command & Control Prevention	Prevent access to known command & Control servers, Use command and control App-ID™, behavioural botnet report, DNS sinkholing, and passive DNS to quickly correlate unknown traffic, suspicious DNS, and URL queries with infected hosts. Apply global intelligence to intercept and sinkhole DNS queries for malicious domains.
	File Blocking	Enable rules to block specific file types
	URL filtering	Set policies for acceptable web usage based on categories. This feature provides a fully integrated, customisable URL filtering engine which allows administrators to apply simple web-browsing and control policies that safeguard the enterprise from a full spectrum of legal regulatory, and productivity risks.
	Zero-Day threat Prevention (Sandboxing)	Unknown or targeted malware (e.g. advanced persistent threats) hidden within files can be identified and analysed by across multiple operating systems and application versions which directly observes and executes unknown files in a virtualized sandbox environment. The feature monitors more than 420 malicious behaviours and, if malware is found, a signature is automatically developed and delivered in as little as 15 minutes. All major file types are supported by including: PE files; Microsoft Office .doc, .xls, and .ppt; Portable Document Format (PDF); Java Applet (jar and class); and Android Application Package (APK).
Management	Logging & log export	Log firewall events and export logs to an external location for long-term storage and Analysis
	Reporting	Generate regular reports on firewall events, user activity, top threats, Geo-Location etc. choose from standard templates or create custom reports from a flexible management GUI
	SNMP read-only	Provide read-only access for external customer SNMP management system
	Rule Scheduling	Configure selected rules to run only at certain times
Network	Outbound NAT	Allow large RFC1918 internal private address space to share small public subnet as per established best practice

4. Interoute Edge Devices

Interoute Edge devices are physical x86 devices, typically deployed in customer offices or data centres. They provide the CPU, RAM and storage capacity which is used to support the virtualised services to the site in which they are deployed. Edge devices also include physical network interfaces for connecting to physical networks, such as WAN, LAN, Internet.



Virtualised CPE

5. Service Delivery and Operating Models

Interoute offers several management models by service. Customers can mix and match options.

Service	Managed Service Model	Self Service Model
SD-WAN	Y	N
SD-WAN with WAN Optimisation	Y	N
Next Generation Firewall	Y	Y

5.1 Device Implementation

Edge devices are shipped by Interoute for installation at the customer's site. Edge devices require a suitable physical environment for operation which is physically secure, has appropriate space and power and meets the environmental requirements.

The physical installation process is simple and can be performed with minimal technical experience. Devices must be installed in a suitable location and physically connected to power and network connections according to the installation guide. Installations can be performed either by an Interoute engineer or by the customer.

Services delivered by Interoute are either installed "over the wire" using secured network access connections or can be pre-staged before installation.

5.2 Standard Changes

SD-WAN Standard Changes

Changes		Change
IP Networking Controls	Networking	<ul style="list-style-type: none">Edit Deployment (for BYOI circuits)Add/edit/remove LAN interface/sub interface addressingEdit Subnet Sharing rulesAdd/Remove/Edit static LAN routes
	DHCP	<ul style="list-style-type: none">Configure Local DHCP Server/Relay
	LAN Routing	<ul style="list-style-type: none">Add/Remove/Edit VRRP ConfigurationAdd/Remove/Edit BGP Configuration
	QoS Policies	<ul style="list-style-type: none">Add/edit/remove QoS policies. Automatically created policies may not be edited/removed
SD-WAN Controls	Application Identification	<ul style="list-style-type: none">Add/Edit/Remove ACL for BIO traffic classification.
	Shaping	<ul style="list-style-type: none">Edit local shaper configuration
	Applications and SaaS	<ul style="list-style-type: none">Add/Edit/Remove User-Defined application based on L4 criteria.Add/Edit/Remove Group definitionSpecify whether SaaS services should be optimised/advertised from a given SaaS gateway & Edit RTT recalculation Interval.
	Business Intent Overlays	<ul style="list-style-type: none">Add/delete/edit SD-WAN routing policy (BIO)Apply/Remove One or more BIOs from a defined set of appliancesEdit the SD-WAN wide definition of local breakout traffic.

	Templates	<ul style="list-style-type: none"> Request creation/application of a template comprised of other listed configuration items on this sheet. The template may be applied to any subset of the appliances constituting the SDWAN.
Security Management	Integrated Firewall Mode	<ul style="list-style-type: none"> Select the firewall mode that is deployed at each location.
	SSL Certificates & optimisation	<ul style="list-style-type: none"> Add/Delete customer certificates for non-SaaS traffic Add/Delete CA certificates Add/Delete customer certificates for SaaS traffic
	Thresholds – Crossing Alerts	<ul style="list-style-type: none"> Add/Edit/Remove alarms based on supported criteria
	SNMP	<ul style="list-style-type: none"> Enable/Disable SNMP on the LAN Edit SNMP Community String Add/Edit/Remove SNMP Trap Receivers
	Netflow	<ul style="list-style-type: none"> Enable/disable Netflow Set Flow timeout Select Interface type & direction to sample Add/edit/remove Netflow collector details

Next Generation Firewall Standard Changes

Configuration	Change
Patching	<ul style="list-style-type: none"> Loading of additional patches onto one (1) Firewall Device or HA Pair Interoute will implement critical and security patches by default as a standard part of the managed service so this only refers to non-essential patches to be implemented at customer request.
Firewall Rules	<ul style="list-style-type: none"> Modification or addition of firewall policy rules Rules can be defined as: stateful firewall (Traditional port/protocol firewall rules), Application (Based on Palo Alto AppID), URL filtering (category-based) or IDS/IPS thresholds or policies in-line with the standard features of the service. For the avoidance of doubt, one line on the policy document or change request form is considered to be one rule.
Log Dump	<ul style="list-style-type: none"> Execution of a log dump request, for a specific time period of no more than five (5) hours in duration
Reporting	<ul style="list-style-type: none"> Enabling of standard firewall reports on any given firewall Any change to the format or content of the reports
SNMP Read-Only	<ul style="list-style-type: none"> Enabling SNMP read-only on the firewall for a customer-managed SNMP management system

5.3 Managed Service Model

The service is available as a managed service. Managed services are controlled and operated by Interoute's engineers. Customers can provide Interoute with configuration requirements according to the standard options available for the service. Access is provided to Interoute's "My Services" portal to raise and track tickets for change, support and information requests as well as view invoices, and service management information.

5.3.1 Roles and Responsibilities

		Responsible	Accountable	Consulted	Informed
Service Requirements	Service selection and options	Customer technical representative	Customer	Interoute Sales Engineer	Interoute Account Manager
	Supplying technical pre-requisite information and configuration options (data capture forms)	Customer technical representative	Customer	Interoute Sales Engineer	Interoute Account Manager
Implementation	Installation of service and configuration of options	Interoute	Interoute	Customer	Customer
	Implementing service monitoring	Interoute	Interoute	Customer	Customer
	Basic testing	Interoute	Interoute	Customer	Customer
	Testing & Accepting the service	Customer	Customer	Interoute	Interoute
Operation	Monitoring the service and reacting to alarms	Interoute	Interoute	Customer	Customer
	Incident Management	Interoute	Interoute	Customer	Customer
	Problem Management	Interoute	Interoute	Customer	Customer
Change Control	Applying critical & security updates	Interoute	Interoute	Customer	Customer
	Supplying change requirements	Customer	Customer	Interoute	Interoute
	Implementation of standard changes	Interoute	Interoute	Customer	Customer
Service Management	Creation and delivery of standard service management reports	Interoute	Interoute	Customer	Customer

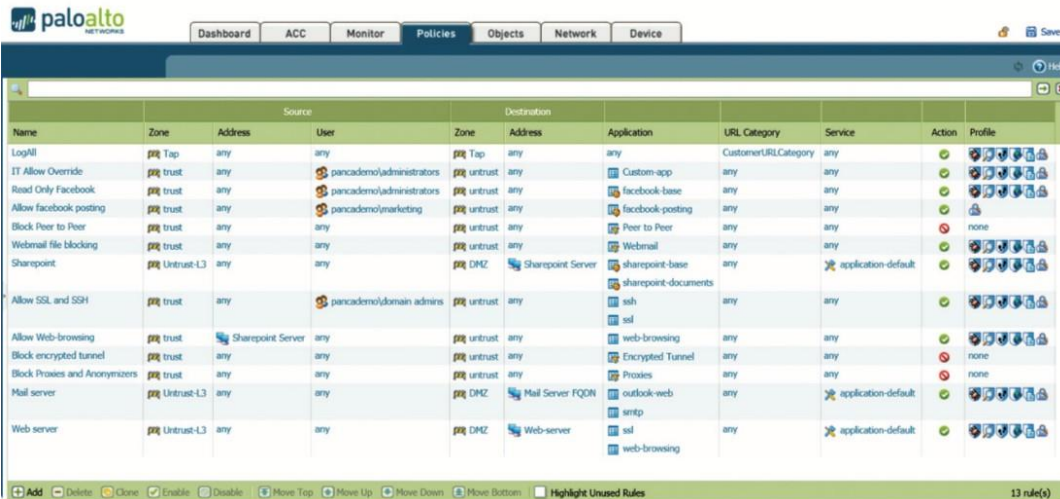
5.4 Self Service Model Interfaces

5.4.1 Next Generation Firewall

For remote management of the firewalls the customer can opt to manage the firewalls individually, or to deploy optional additional centralised management software.

5.4.2 Direct Management

The Next-Generation Security Platform can be managed individually via a command-line interface (CLI) or through a full-featured browser-based interface.



The screenshot shows the Palo Alto Networks management interface with a table of firewall rules. The table has columns for Name, Zone, Address, User, Zone, Address, Application, URL Category, Service, Action, and Profile. The rules are listed in the table, including LogAll, IT Allow Override, Read Only Facebook, Allow facebook posting, Block Peer to Peer, Webmail file blocking, Sharepoint, Allow SSL and SSH, Allow Web-browsing, Block encrypted tunnel, Block Proxies and Anonymizers, Mail server, and Web server.

Name	Zone	Address	User	Zone	Address	Application	URL Category	Service	Action	Profile
LogAll	any	any	any	any	any	any	any	any	allow	default
IT Allow Override	trust	any	pancademo/administrators	untrust	any	Custom-app	any	any	allow	default
Read Only Facebook	trust	any	pancademo/administrators	untrust	any	facebook-base	any	any	allow	default
Allow facebook posting	trust	any	pancademo/marketing	untrust	any	facebook-posting	any	any	allow	default
Block Peer to Peer	trust	any	any	untrust	any	Peer to Peer	any	any	deny	none
Webmail file blocking	trust	any	any	untrust	any	Webmail	any	any	allow	default
Sharepoint	Untrust-L3	any	any	DMZ	Sharepoint Server	sharepoint-base	any	application default	allow	default
Allow SSL and SSH	trust	any	pancademo/domain admin	untrust	any	ssh	any	any	allow	default
Allow Web-browsing	trust	Sharepoint Server	any	untrust	any	web-browsing	any	any	allow	default
Block encrypted tunnel	trust	any	any	untrust	any	Encrypted Tunnel	any	any	deny	none
Block Proxies and Anonymizers	trust	any	any	untrust	any	Proxies	any	any	deny	none
Mail server	Untrust-L3	any	any	DMZ	Mail Server FQDN	outlook-web	any	application default	allow	default
Web server	Untrust-L3	any	any	DMZ	Web-server	smtp	any	application default	allow	default

User Interface

Panorama Central Management

For large-scale deployments, the customer can use Palo Alto Panorama to globally deliver visibility, policy editing, reporting, and logging features for all of the Edge firewalls as well as any other self-managed hardware and virtual appliance Palo Alto firewalls in the customer network. Panorama provides the same level of contextual control over global deployment as is provided over a single appliance directly.



Central Management

Panorama Features	Description
Template Stacking	Develop multi-level policy template hierarchy based on a single global template, make changes at template level rather than firewall level
Management Access Segmentation	Use a combination of role-based access and Device Group Hierarchy to provide granular, devolved administration
Configuration Import	Import existing firewall configuration into Panorama. Easy transition of pre-production to production without re-typing configuration
Management tools and APIs:	Web Based User Interface, Powerful command-line interface and Complete XML-based REST API
Log forwarding	Configurable syslog, SNMP, email forwarding of all logs/events
3rd Party Integration	Configuration management: Tufin, Firemon, AlgoSec Log collection: Splunk, Q1, RSA

5.5 SD-WAN Reporting

Customers can view and generate reports for the SD-WAN service within the MyServices portal. A reporting platform provides network wide visibility and reporting capabilities as detailed below.

Health dashboard

The health dashboard provides a high-level view of the network health, based on configured thresholds. Filters are available for packet loss, latency and jitter. Each block represents one hour and uses colour coding to display the most severe event among the selected filters. Clicking a block displays a pop-up with specifics about that event, what value triggered it, and any additional threshold breach during the same hour.

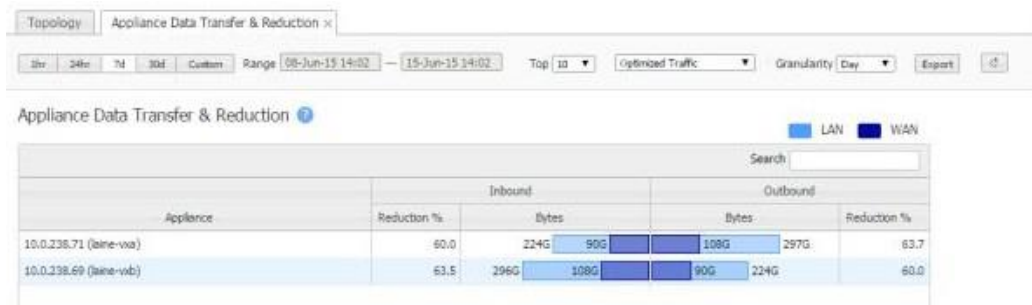


Health Dashboard

- Green = normal operation
 - Orange = marginal
 - Red = needs immediate attention
 - Aqua = warning (an alarm level)
 - Grey = no data available
- Health dashboard

Data Transfer & Reduction

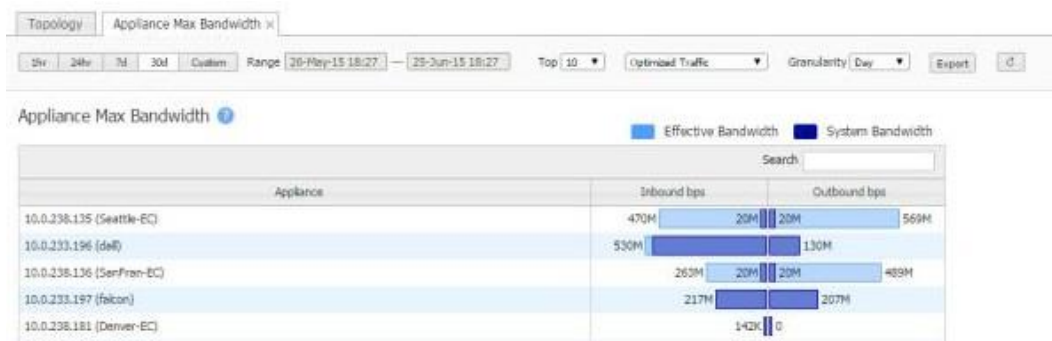
The Data Transfer & Reduction chart lists the top devices based on the total volume of inbound and outbound traffic before reduction. It shows how many bytes the service saved when transferring data, aggregated over a selectable time period.



Data transfer & reduction report

Max bandwidth

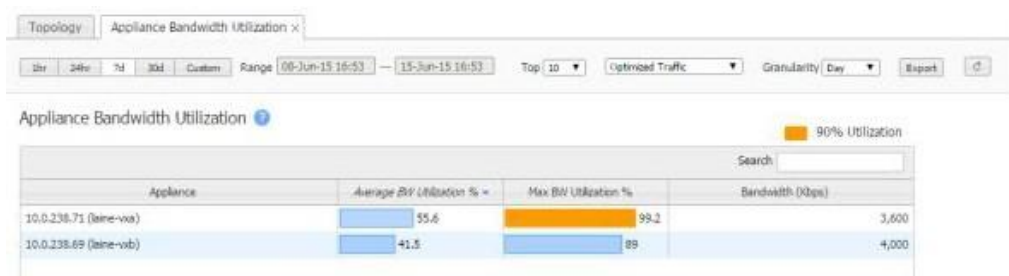
The Appliance Max Bandwidth chart lists the top devices by the peak throughput (in either direction), within a selected time period. It compares the system bandwidth of the device to the effective bandwidth it's providing.



Max Bandwidth report

Bandwidth Utilisation

The Appliance Bandwidth Utilisation chart lists the top devices by the average percent of available bandwidth used.



Bandwidth utilisation report

Bandwidth Trends

The Appliance Bandwidth Trends chart shows bandwidth usage over time.



Bandwidth trends report

Top devices by packet

The Appliance Packet Count chart lists the top devices according to the sum of the inbound and outbound LAN packets, showing how much traffic was sent.

The screenshot shows the 'Appliance Packet Count' table for the range 16-Jun-15 01:40 to 16-Jun-15 02:21. The table lists the top 10 devices by packet count, showing LAN and WAN packet counts and maximum packet rates (pps).

Appliance	Inbound				Outbound			
	LAN Packets	LAN Max pps	WAN Packets	WAN Max pps	LAN Packets	LAN Max pps	WAN Packets	WAN Max pps
10.0.238.69 (lane-vb)	1,644,369	7,211	1,027,453	583	1,819,747	12,137	1,032,899	574
10.0.238.71 (lane-va)	1,730,602	6,144	1,067,136	581	1,829,467	16,041	1,001,768	633

Top devices by packet report

Application reduction

Application reduction charts show which applications have sent the most bytes.

The screenshot shows the 'Application Reduction' table for the range 16-Jun-15 01:48 to 16-Jun-15 02:29. The table lists the top 10 applications by byte count, showing LAN and WAN byte counts and reduction percentages.

Application	Inbound		Outbound	
	Reduction %	Bytes	Bytes	Reduction %
grutella	72.8	1.5G	419M	73.5
datadomain	60.5	1.1G	420M	60.3
adl	33.7	637M	636M	33.8
unassigned	24.6	560M	556M	24.2
3par	50.4	499M	513M	51.1

Application reduction report

Application Pie Charts

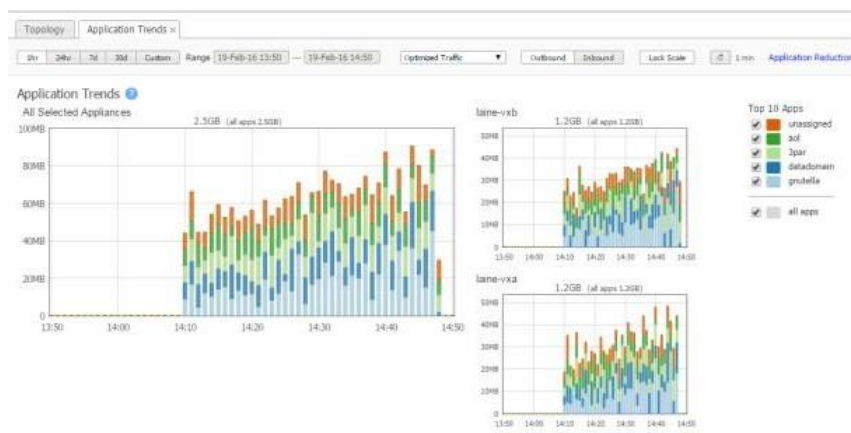
Application pie charts show what proportion of the bandwidth an application consumes on the LAN and on the WAN. Charts also identify any saved bandwidth by optimisation features.



Application use of network report

Application trends

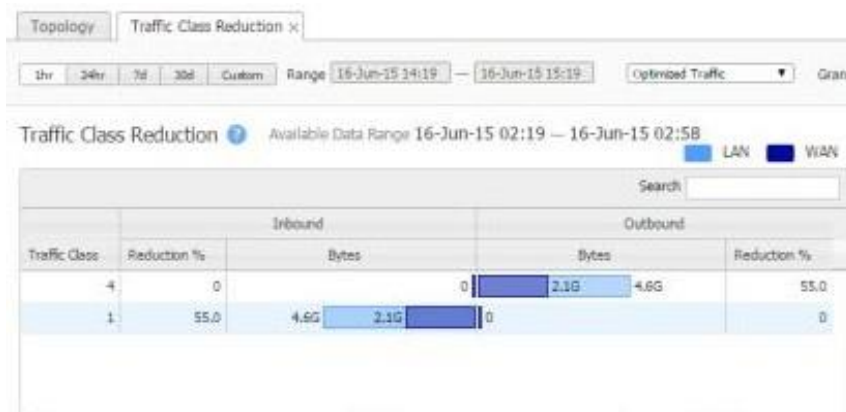
Application trend reporting shows what proportion of traffic each application use over time.



Application trends report

Traffic Class reduction

Traffic Class Reduction shows which applications have sent the most bytes



Traffic class reduction report

5.6 Firewall reporting

If the customer has selected the optional firewall service then additional Firewall-specific reporting is available as a standard feature but this is not enabled by default. If the customer has selected the self-service option then they will be able to view and configure firewall reports via the management console. If the customer has selected the managed model then reports can be enabled upon request, and if the customer is unable to specify the required report format then Interoute will provide a default report format that the customer can modify at a later date via the standard change process.

5.7 Professional Services

In addition to the service models, Interoute can provide additional professional services, on an ad-hoc basis. These services can include a broad array of further engineering and consultancy-type services, such as:

- Engineering
- Project Management
- Service Management
- Network Discovery
- Security Audit
- Migration
- Policy Authoring
- Penetration testing

6. IP Network Connectivity

Edge devices are physically connected to IP networks using commodity IP network connections. Typically, multiple access networks are connected to the Edge device, such as Internet and VPN (MPLS) as well as the internal LAN network. Interoute's Cloud Fabric connector is installed as a virtual appliance on the Edge device. The Cloud Fabric connector delivers IP routing services and services required for management, operation and integration.

Interoute offers a full range of Internet and private network products as well as offering support for Internet connectivity sourced by the customer – Bring Your Own Internet (BYOI).

6.1 Network Requirements

Interoute SD-WAN service is designed to be a fully functional CPE which can be directly connected to access circuits. Each SD-WAN device must have a copper Ethernet RJ-45 presentation for both LAN and WAN connections.

Circuit presentation	Separate CPE required
Ethernet RJ-45 10/100/1000	No
All other interface types	Yes

LAN Requirements - In order for LAN-side support of failover in resilient device configurations (including HA and cold standby) all connected LAN devices must accept *gratuitous ARP updates*.

WAN requirements - There are two main connectivity sourcing scenarios for all the SD-WAN service sites

Interoute Supplied Access - When Interoute supplies the Internet access or MPLS VPN the access circuits will always meet the technical requirements required for a successful deployment.

Customer Supplied Access - When the customer supplies local Internet connectivity (e.g. Bring Your Own Internet or BYOI), the following technical requirements must be delivered from the customer supplied services:

Technical Requirements	
Physical Circuit presentation	Circuits must be presented to the Edge device as defined above.
Performance requirements	Uncontended connections with fixed bandwidth.
IP Address requirements	Interoute requires a minimum of one useable IP address for each logical circuit (or /30 subnet). A /29 subnet with 6 useable IP addresses is recommended to allow for future services.
NAT requirements	<p>Only static NAT is currently supported by the SD-WAN service devices. This means the following ports must be kept permanently open and the device can forward the ports below to the private IP address of the SD-WAN service device.</p> <p>Ports:</p> <p>500 /UDP</p> <p>4500 /UDP</p>
Firewalling requirements	To enable the SD-WAN functionality the SD-WAN service devices need to have completely unfiltered egress access towards the Internet.

7. Service Availability & Coverage

Interoute can service customers in all countries with few exceptions (such as embargoes countries). However, Interoute defines 5 levels of delivery complexity by country, which can have an impact on such areas as:

- Delivery lead times due to customs.
- Import duties which may be payable by the customer.
- Requirement for transfer of ownership of hardware.
- Individual export licenses and pre-shipment inspections.
- Level of customer involvement required for the import process.

7.1 Delivery complexity levels

Level 1 – No documentation is required. Devices can be shipped from the Brussels warehouse with only a Requisition. The customer will not be involved in any import clearance.

Level 2 – A Shipping invoice will need to be prepared. The customer might be involved in the Import if they will be importing but the clearance process in these countries is straight forward and quick.

Level 3 – Type approvals are required to be prepared by the customer before shipping, with an approved invoice and confirmation of ready to ship & import. Interoute will provide assistance with the type approvals of the device.

Level 4 – A shipping invoice is required. The customer must also act as the Importer of Record and be prepared for managing the customers import clearance process. This is likely to involve some registrations at customs or obtaining import permit by the IOR (Importer of Record).

Level 5 - The customer needs to prepare with Import customs procedures as for Level 4, but also Interoute need to obtain either Individual Export License or Pre-Shipment Inspection. It could take from 2-3 weeks to several months to prepare the documentations.

7.2 Service Availability Tables

The following tables define the availability and complexity of Edge service deliveries.

Africa					
Algeria	4	Gabon	4	Niger	5
Angola	4	Gambia	5	Nigeria	4
Benin	5	Ghana	4	Rwanda	4
Botswana	5	Guinea	4	Sao Tome and Principe	5
Burkina	5	Guinea-Bissau	5	Senegal	4
Burundi	5	Ivory Coast	4	Seychelles	5
Cameroon	4	Kenya	4	Sierra Leone	5
Cape Verde	5	Lesotho	5	Somalia	5
Central African Republic	5	Liberia	5	South Africa	2
Chad	4	Libya	5	South Sudan	5
Comoros	5	Madagascar	4	Sudan	5
Congo	5	Malawi	5	Swaziland	5
Congo, Dem Rep	4	Mali	3	Tanzania	4
Djibouti	5	Mauritania	5	Togo	5
Egypt	4	Mauritius	4	Tunisia	4
Equatorial Guinea	5	Morocco	4	Uganda	4
Eritrea	5	Mozambique	4	Zambia	4
Ethiopia	4	Namibia	5	Zimbabwe	5

Asia					
Afghanistan	5	Japan	2	Philippines	4
Bahrain	3	Jordan	4	Qatar	3
Bangladesh	4	Kazakhstan	5	Saudi Arabia	3
Bhutan	5	Korea, North	Embargoed Korea, South	Singapore	2
Brunei	5	Kuwait	3	Sri Lanka	3
Burma (Myanmar)	5	Kyrgyzstan	4	Syria	Embargoed
Cambodia	5	Laos	5	Taiwan	3
China	4	Lebanon	4	Tajikistan	5
East Timor	5	Malaysia	3	Thailand	3
Hong Kong	5	Maldives	5	Turkmenistan	5
India	3	Mongolia	4	United Arab Emirates	2
Indonesia	3	Nepal	5	Uzbekistan	4
Iran	Embargoed	Oman	4	Vietnam	3
Iraq	5	Pakistan	4	Yemen	5
Israel	3				

Europe					
Albania	3	Germany	1	Norway	2
Andorra	1	Greece	1	Poland	1
Armenia	3	Hungary	1	Portugal	1
Austria	1	Iceland	2	Romania	1
Azerbaijan	3	Ireland	1	Russia	5
Belarus	5	Italy	1	San Marino	1
Belgium	1	Kosovo	3	Serbia	3
Bosnia and Herzegovina	3	Latvia	1	Slovakia	1
Bulgaria	1	Liechtenstein	1	Slovenia	1
Croatia	1	Lithuania	1	Spain	1
Cyprus	1	Luxembourg	1	Sweden	1
Czech Republic	1	Macedonia	3	Switzerland	2
Denmark	1	Malta	1	Turkey	2
Estonia	1	Moldova	3	Ukraine	3
Finland	1	Monaco	1	United Kingdom	1
France	1	Montenegro	3	Vatican City	1
Georgia	3	Netherlands	1		

North & Central America					
Antigua and Barbuda	5	Dominican Republic	3	Netherlands Antilles	4
Bahamas	5	El Salvador	3	Nicaragua	4
Barbados	5	Grenada	5	Panama	3
Belize	5	Guatemala	3	Saint Kitts and Nevis	5
Canada	2	Haiti	5	Saint Lucia	5
Costa Rica	2	Honduras	3	Saint Vincent & Gren	5
Cuba	Embargoed Dominica	Jamaica	5	Trinidad and Tobago	5
Antigua and Barbuda	5	Mexico	3	United States	2

8. Professional Services

8.1 Project Management

Interoute’s Professional Services portfolio is designed to customise and complement the experience for Public Sector customers who purchase any of the Unified ICT suites of solutions.

Public Sector Clients are able to take full advantage of our professional set of services ranging from to ITIL aligned operational management to project management through to customised service and technical assistance – services brought to you by our highly skilled and motivated team.

Interoute Project Management offers a skilled and credible advocate who will work collaboratively to successfully deliver the ICT Solution in a professional, consistent & controlled manner using Interoute Project Methodology (IPM) based on PRINCE2®.

For a Unified ICT service project to be successful for both parties, there has to be the right level of communication, information and understanding from all parties.

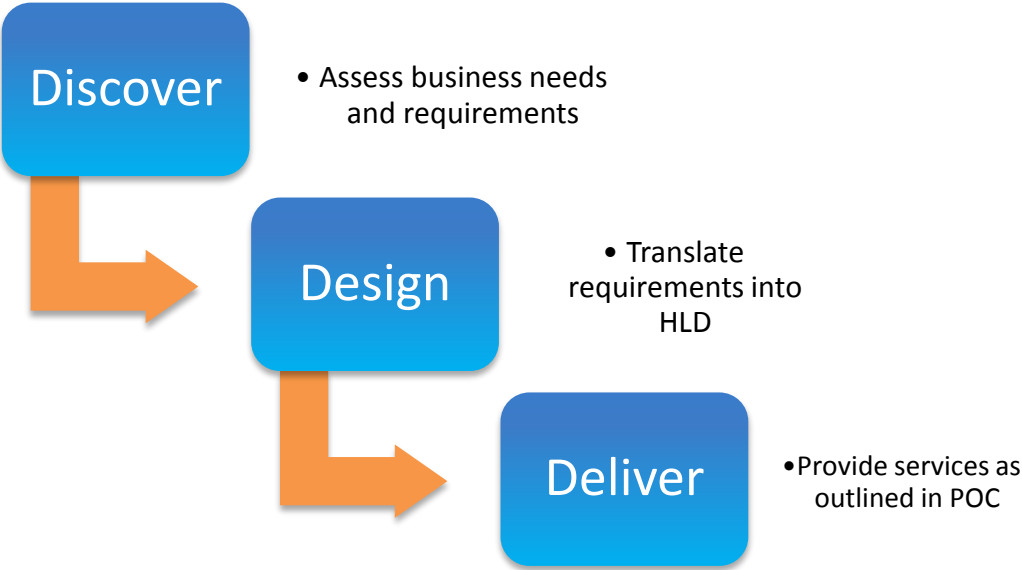
Assigned contact points within Interoute, who understand the Public Sector and the overall ICT strategy, ensuring that Public Sector clients receive the full benefit of our Unified ICT Services without having to understand the entire Interoute organisation.

Interoute’s approach to Project Management recognises that Public Sector clients require robust and flexible planning to ensure that any service deployment, solution transition, or optimisation, is fulfilled with the highest degree of accuracy and detail, accounting for time, cost, quality and risk at all times.

Interoute Project Managers provide a single point of contact, access to Interoute leadership and will oversee the handover to Interoute support of the new Interoute Unified ICT Services

8.1.1 Migration Approach

Interoute migration services are designed to ensure a seamless journey for our customers onto the Virtual Data Centre (VDC). The migration project would be run utilising our proven consultative methodology. Each stage is designed to ensure that services are transitioned onto the VDC using the appropriate approach for each individual application. The Interoute process consists of three phases:



Discover

During the discovery phase Interoute captures information regarding the existing infrastructure; server and network architecture, security considerations through to SQL deployments. This information is documented and used to create a high level design. The next part of the discovery would be post proposal and would involve Interoute working with the customer to further understand the applications, dependencies, infrastructure and risks.

Design

The purpose of the design phase would be to create a final low level design and migration project plan. Interoute would use the information captured to date and the output from the discovery workshops and feed these into the final design and plan.

Deliver

Once the final design and project plan has been agreed the project to migrate the customer on to the Interoute VDC would begin. The project would be collaborative and require Interoute to work closely with the customer and their 3rd party suppliers to ensure a successful migration.

8.1.2 Migration Method

Interoute offer different approaches for our customers to migrate from their existing environments into the Interoute VDC. Each approach can be applied to all or part of an environment and in many cases Interoute would recommend a mixture of the below.

Interoute as part of the discovery phase would work with its customers to agree the best approach for each individual application. Using our migration experience and knowledge of our platforms to provide a consultative service.

New build

The new build migration would entail provisioning a new virtual machine on the Interoute VDC, installing the relevant applications and then migrating data from existing environments.

Server Replication

Server replication requires the installation of our Hypervisor Agnostic Migration Toolset onto the virtual or physical servers in the existing environment. These would then be replicated over a secure connection (preferably Interoute's fibre network) into the Interoute VDC. The new virtual machines would then be brought online and tested on the VDC before being handed over as a live service.

Export and Import

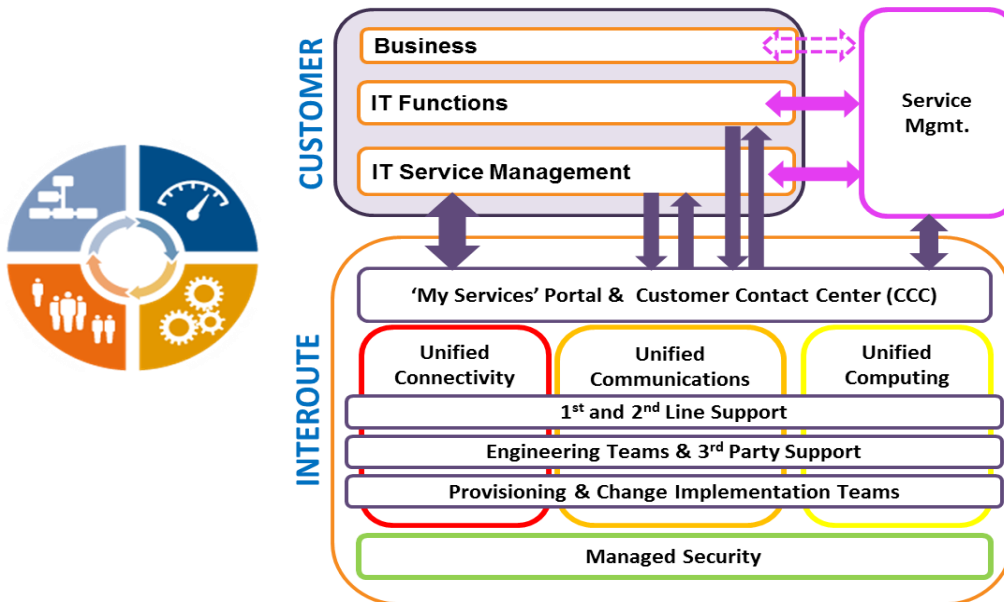
This option would be used to migrate servers that were either not connected or unable to be connected to the Interoute network for migration. Interoute would again utilise our migration tool set to capture an image of the server export this to removable media, this would then be transferred to Interoute and imported as an Image on the VDC. This would then be used to provision a new copy of the server in the VDC which would be tested and then handed over.

Lift and Shift

For legacy applications or appliances that are not suitable for virtualisation Interoute provides colocation. The underlying servers would usually be physically moved from the existing customer data centres in to the Interoute colocation facility.

8.2 Service Management

This section details the key Support areas that underpin Interoute's Product Portfolio and provide the foundational layers across which Service Management operates.



8.2.1 Operational Support for Interoute's Unified ICT Portfolio

Interoute's Unified ICT Product Portfolio is powered by an extensive operational management structure across the organisational footprint.

This structure exists not only to ensure that your services are delivered to expectations, but to do so with a focus on continual improvement in the efficiency and effectiveness of our operational teams supporting them.

Using the ITIL framework to govern our processes and form the basis of our Service Management enables us to demonstrate the service quality you require, while keeping our solutions and their management focussed on providing exactly what your business requires.

Our ITIL processes are followed throughout the organisation, from our centralised Operations Centres to our Local Data Centre Operations to ensure consistency in this quality across every aspect of our solutions.

8.2.2 Operational Management

Our operational teams work to ITIL aligned processes in their day to day duties. Their focus is on fault resolution and request fulfilment activities, managing any service or platform affecting failures, from notification through to resolution and targeted against your service metrics. This forms the base level of Service Management included with our product sets.

The Customer Contact Center (CCC) and My Services portal are the points of contact for all requests, trouble tickets and coordination of fault resolution activity. The key activities always performed include:

- Ticket Handling
- Customer Notifications
- Executing Requests
- Planned Works Notification

Interoute operates two fully diverse operation centres, each with a Customer Contact Centre (CCC) and Network Operating Centre (NOC), in Prague – Czech Republic (primary site) and Sofia – Bulgaria (backup site). These facilities are operational 24 hours a day, 7 days a week. To ensure business continuity the two operations centres both act as a disaster recovery site for each other in case of major incidents where Interoute is not able to provide support from that site. ISO 20000 (Quality) and ISO 27001 (Security) are applied to our Central Operations and Data Centre Operations to ensure these standards are adopted consistently across the support organisation. These are industry best practices recognised by the International Standards Organisation (ISO) that deliver quality and secure IT outsourced IT solutions.

Fault Resolution

Interoute’s approach to incidents and events enables us to detect and manage event conditions that may occur throughout your IT environment delivering and supporting our services, while ensuring you are kept notified.

Event notifications can arise through alarms on our own monitoring system, or via contact from Customers or other parties, where they can raise incidents at our CCC (Customer Contact Centre), as appropriate.

Incidents are raised in our Service Management tool and allocated to the appropriate resolver group for action. All operational teams are aligned to deliver the service metrics defined in our Product Portfolio.

“My Services” (Interoute Customer Portal)

Interoute provides you with greater control in managing the relationship with Interoute and the associated products and services, with our web portal, Interoute’s “My Services”, positioned as your first line of support and information



Through “My Services”, Interoute enables you to:

- Speed up communication
- Efficiently share key information (technical, numbers, results)
- Increase service control
- Decrease operational management overheads
- Obtain an inside view into system management and performance.

The Graphical User Interface (GUI) for “My Services” is adaptive, so that when your users log in, each user is presented with different menu options according to the access privileges and/or services they are subscribed to.

“My Services” is a browser-based product with a series of reporting screens and fault logging options. Ease of navigation is central to its design, to ensure even first-time users can quickly locate their desired function, meeting their requirements with minimal delay.

Once successfully logged in, the user is provided with a homepage with customisable preference options to ensure that the tool matches the user’s individual requirements. From here, they can select the functions pertinent to their needs.

Functionality handled through the “My Services” portal includes:

- Secure Customer Login;
- Services List;
- Trouble Tickets;
- Order Tracking;
- Service Changes;
- Invoices;
- Performance monitoring;
- Customising views to show key detail as required.

Customer Contact Centre (CCC)

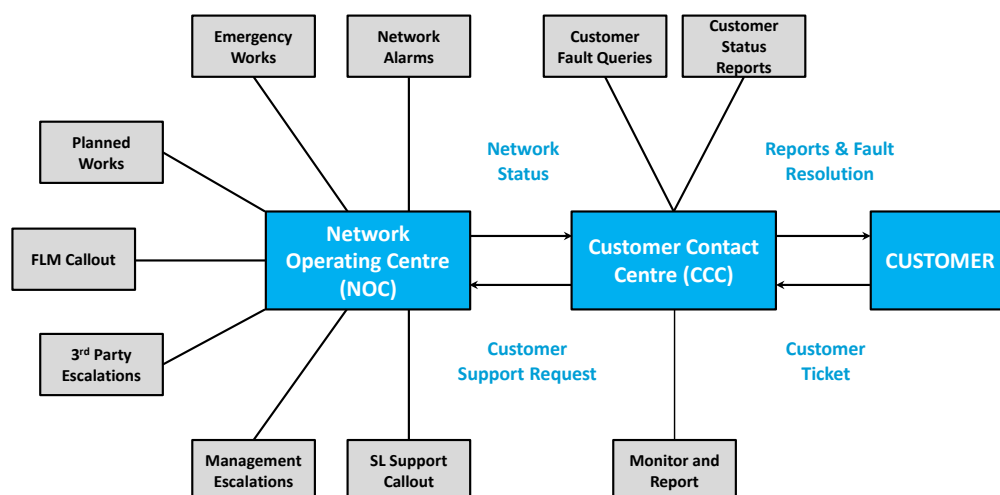
Interoute provides customer support on a 24x7 basis from the CCC and can be contacted via My Services, telephone, and email.

The CCC is our call centre providing a single point of contact for customers and coordination of fault resolution activity.

The primary purpose of the CCC is to manage ticket life cycle through to resolution within the service levels, and comprises of the following key activities:

- Opening tickets in response to calls from customers;
- Managing resolution through the NOC;
- Providing regular updates to customers until the ticket is closed;
- Proactively informing customers of possible disruptions where the NOC has detected a problem through its management systems for managed services;
- Proactive ticket handling;
- Arranging customer/contractor site access;
- Planned works notifications.

Our Customer Contact Centre (CCC) works very closely with the Network Operating Centre (NOC), as illustrated in the diagram below. When an incident is logged, the Network Operating Centre (NOC) will provide regular updates during the life of the incident directly to the CCC. The CCC will continue to inform the customer until the incident is resolved.



INFORMING OUR CUSTOMERS | The NOC liaises regularly with the CCC to ensure that you are informed with progress reports and anticipated time to repair.

The CCC can easily be contacted by an International toll free 0800-number, a Direct Dial In number, an online web portal (My Services), or email. Our CCC team is multilingual with the majority of European languages supported: English, French, German, Italian, Spanish, Swedish, Portuguese, Dutch, Czech, Greek, Polish, Bulgarian, Russian,

Hungarian, Norwegian and Romanian. We also have Arabic speakers within the operations centre, however if they are not available when required Interoute will engage the services of a translation service.

8.2.3 Network Operating Centre (NOC)

Interoute operates multiple operation centres; two of which are fully diverse with centres based in Prague and Sofia; each has a Customer Contact Centre (CCC) and Network Operating Centre (NOC). Bracknell (UK) is a CAS(T) accredited NOC and PNOC delivering and managing secure UK Public Sector Network services, whilst retaining sovereign management of a partitioned UK network. The NOCs are responsible for the first level of troubleshooting on IP, Transmission or Voice incidents. The NOCs manage the Interoute network tasked with responsibility for:

- Proactive Network Monitoring;
- Effective management of technical and network resource;
- Technical analysis and troubleshooting;
- Third Party management and Planned Works management.

Prague

- Primary Active Centre for Network, Video & Data Centre Surveillance;
- 2nd line Hosting, Security, Voice, Video, TX, IP support;
- 3rd Line Hosting, Security, Voice, Video, TX, IP support;
- Primary Service Desk;
- Incident Management and request fulfilment for Premium and Full Service Plus customers;
- Clearsign support desk;
- Primary Provisioning & Activation Centre;
- Operations Change Control;
- Quarterly Operational Continuity drills.

Sofia

- Secondary Centre for Network Surveillance;
- Extension to the 2nd line Hosting, Security, Video, Voice, TX, IP support;
- Incident Management and request fulfilment for Full Service customers;
- Extension of the Provisioning & Activation Centre;
- Quarterly Operational Continuity drills.

Prague and Sofia NOCs are in charge of ensuring Proactive Network Monitoring, which enables us to monitor the network work and the hosted systems continuously to guarantee both the connection and uptime.

Bracknell

- CAS(T) / IL2 Accredited Security NOC;
- Provisioning NOC for UK Secure connectivity services;
- Security cleared personnel providing 1st line support in English language;
- PNOC and 2nd and 3rd line support;
- Incident Management and Request Fulfilment for all IL2+ projects;
- Partitioned network management and UK Sovereign NMS data repository.

The Bracknell NOC is backed-up by active CAST(T) disaster recovery sites in Central London.

1st, 2nd & 3rd Line Support

The NOC liaises regularly with the CCC to ensure that our customers are kept informed with progress reports and anticipated time to repair. The NOC engineers form these specialist teams:

- First Line Technical Support is based in Prague and Sofia, the first line team is made up of our 24/7 NOC. The Prague based support team is responsible for IP, Transmission, Video and Voice and is made up of 22

first line engineers, 4 lead engineers and 3 third party (OLO) specialists. First line teams follow an extensive internal training and development program;

- Second Line Technical Support is based in both Prague and Sofia and comprises 8 engineers with vendor specific technical certifications. When the NOC/SHOC needs extra technical expertise to resolve an incident they can engage second line support. Updates on incidents provided by second line support will be communicated to the customer by CCC;
- Third Line Technical Support is provided by Interoute's Prague based Network engineering group which is made up of 26 engineers across IP, transmission and voice disciplines.

Ensuring Consistent Service

The NOC function of the network is duplicated and the core is fully resilient. Sites with backup are connected to 2 PEs (core IP devices). NNIs to MPLS partners are duplicated. Central Firewalls have a cold standby in case of hardware failure.

Planned Works

Interoute aims to perform all major Planned Works (PW) during a weekend, with our preferred maintenance window of Saturday 23:00 GMT - Sunday 05:00 GMT. Due to the size of our network and obligations to other customers, it is not always possible to put PWs within this window however every effort is made to do so. Thorough checks are performed to avoid collisions on protected services, so that the primary and spare paths on the Interoute network are not hard down at the same time.

All Interoute PW notifications are emailed with a minimum of 14 days' notice before the actual PW window - this is not always guaranteed by third party suppliers as they may have a different SLA. The majority of our PWs do not exceed 4 hours downtime, typically ranging from 10 minutes to 2 hours. Extensive work, such as a fibre reroute, may require the entire 6 hour PW window to allow full preparation and testing of the work, to ensure the change is successful and long-lasting.

All maintenance notifications (Scheduled and Emergency) are sent with an explanation of the type of work and the location. Our PW team is available if further information is required about a PW, with contact details on the notification email. Interoute will notify the customer when the PW is about to commence, when it has been completed, and will provide progress updates during the PW as appropriate.

9. Virtual Data Centre Service Management

Interoute understands that our customers may require a managed Virtual Data Centre (VDC) service. VDC Managed allows a customer to focus on the delivery and configuration of their applications without the usual headaches associated with infrastructure and operating system management. The service provides 24x7 monitoring, maintenance and support for each system giving a customer the peace of mind that their systems are being looked after by a team of experts.

VDC Self Care

VDC Self Care is the baseline self-service support level for Interoute VDC. Interoute provides an on-demand infrastructure product, which is implemented and supported by the customer using the user interface, API and tools provided by Interoute. Interoute provides user documentation, “how to” guides, and white papers at our Knowledge centre as well as Live Chat.

Live Chat Is an instant messaging service for advice and assistance with VDC, staffed by Interoute engineers. Interoute provides 24/365 support for the VDC platform that provides the virtual hardware for the customer’s deployment as well as support for the VDC user interface. Interoute does not provide support for services deployed on VDC, those remain the responsibility of the customer.

VDC Assist

VDC Assist provides implementation and operational assistance functions and is designed to augment the customer’s technical expertise for creating and maintaining resources in the customer's VDC. VDC Assist provides two options for services.

VDC Assist: Implementation assistance

VDC Assist offers pre-packaged professional services such as building virtual architectures of virtual machines, networks and storage volumes to support particular use cases (for example, web server clusters or database clusters).

VDC Assist: Operational assistance

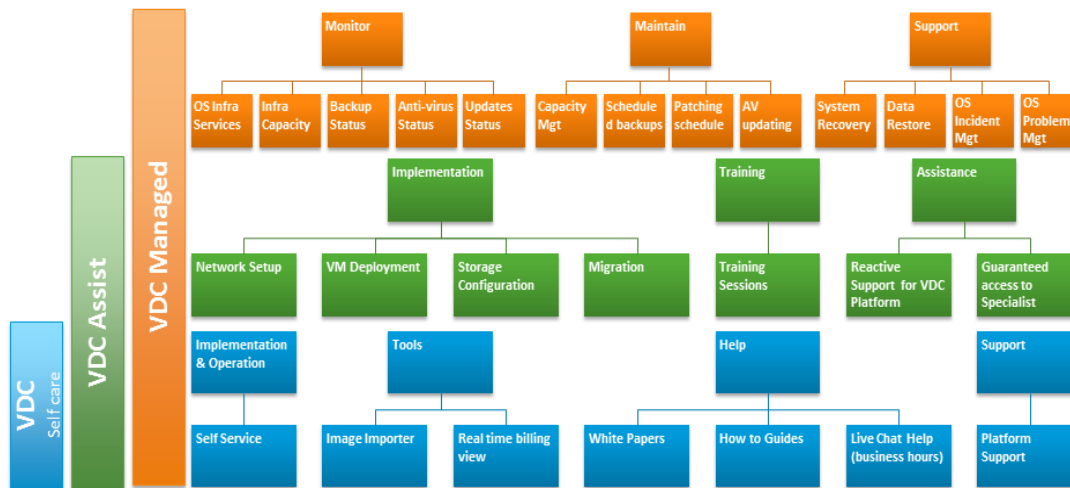
VDC Assist offers assistance with day-to-day operation of the Virtual Data Centre platform, through access to VDC specialists available during business hours. Customers may choose from token-based assistance, subject to a capped number of requests that can be made per month or an unlimited service, with an uncapped number of requests and prioritised assistance.

VDC Managed

VDC Managed provides a managed implementation of virtual machines, networks and storage. In addition Interoute support the day-to-day operation of these elements by providing monitoring of server connectivity, operating system administration, and infrastructure capacity, according to an agreed pre-defined schedule. Interoute maintains the environment by implementing system update patches, anti-virus updates, and managed system and data backup. Incident management is provided to restore data and recover VMs to the state of a standard Interoute build plus any changes that have been made to the system state.

Managed Web, Application & Databases Services

The VDC Managed service can be extended to cover Application Servers and Databases operating in the Interoute VDC environment or can be taken as a stand-alone service for Interoute VDC Self Care customers. The portfolio includes web, application and database servers from Microsoft, Oracle and the open-source community. Our position as both an Oracle Premier and Microsoft Gold partner complements our open source capability to provide a comprehensive set of services to our customers, backed by the vendors. In addition our support teams hold an impressive range of certifications including MCIPT, MCTS, MCDBA, MCP, MCSE, OCP, OCA and OCM.



9.1 VDC vTools

Interoute vTools provides a virtualised toolkit built into VDC that provides Monitoring, Anti-Virus, Patching and Backup for your Windows and Red Hat virtual machines. Interoute vTools provides simplified administration through our VDC GUI with a dashboard view on all virtual machines under vTools management. Interoute vTools utilises the same management tools set provide as part of our VDC Managed service.



Monitoring Service

The Monitoring component of the vTools option provides a standard set of monitoring features that are customisable by the end user to appropriately configure the level of alerting and tune to ensure that only the most relevant faults are alerted.

vTools Monitoring features;

- Simple view of % of CPU use for all CPU's in a Virtual Machine.
- Simple view of % of RAM use for RAM in a Virtual Machine.
- Simple view of % of Disk space for all disks in a Virtual Machine.
- View of the status of Core System Services for the operating system.
- Customer configurable thresholds.
- Customer configurable alerting notification.
- AV configured and applied notification.
- Server Patch status.



Anti-Virus

The Anti-Virus component of the vTools option provides Anti-Virus cover on a machine where appropriate.

vTools Anti-Virus features;

- Automatic distribution of Anti-Virus Signatures.
- Customer configurable exclusions.
- Alerting on Security Threat.



Patch Publishing

The Patch Publishing component of the vTools option publishes patches to a server on behalf of the customer.

vTools Patch Publishing features;

- Automatic push of critical and security patches to customer server.
- Customer has the option to deploy patch or reject.



Backup

The Backup component of the vTools option provides a standard backup tool for server and application backups.

vTools Backup features:

- File level backup included as standard.
- Disk-to-Disk level backup and restore.

- Customer can view backup history.
- Customer can perform a restore of data.
- Customer can initiate a one-time backup job.
- Daily Backup retention 14 days.
- Weekly Backup retention 4 weeks.
- Optional - Monthly Backup retention, up to 7 years.
- Optional - Customer can request physical copy of data backups.

9.2 Escalation Process

Interoute has clearly defined and documented escalation procedures for all service affecting faults which can occur during the operational phase. A copy is provided at service handover.

The customer may escalate any reported problems if they are not satisfied with the progress of the fault resolution, or if response and repair times have not been achieved. If you wish to escalate the problem to a member of the management team, then a Customer Contact Centre agent will record the escalation and pass to the next appropriate management level of the Operation Centre team. The CCC will directly liaise with you for any service affecting issues (including incident tickets, outages or proactive corrective/preventative maintenance).

From the start of any fault you will be updated periodically in line with the SLA. Escalation would be made by telephone based on the timeframes below. If contact is not established immediately, alternate numbers will be used. Escalations will be progressed to next managerial level through the Escalation Matrix¹ based on ticket age and priority. The first level for escalation is always Service Assurance Manager (M1). Escalation levels, roles, and timings are detailed below for In Hours (effectively extended business hours) and Out Of Hours (all other times), according to defined fault categories.

The **ECS** escalation levels and the corresponding contacts are as follows:

During Working Hours Mon-Fri 08:00 - 19:00 CE(S)T					
Level	Name and Contact Details	Escalation Time			
		Incidents			Requests
		Critical	Major	Standard	Standard
M1	SAM , ECS Service Assurance	2 hour	4 hour	48 hour	24 hours
M2	Manager, ECS Service Assurance	4 hour	8 hour	96 hour	48 hours
M3	Senior Manager, ECS Technical Services & Support	8 hour	12 hour	1 x week	72 hours
M4	VP, ECS Operations	12 hour	24 hour	n/a	n/a

Outside Working Hours - Rota Basis - (Mon-Fri 19:00 – 08:00 Sat-Sun 24x7 CET)					
Level	Name and Contact Details	Escalation Time			
		Incidents			Requests
		Critical	Major	Standard	Standard
M1	Operations Shift Manager	2 hour	4 hour	48 hour	24 hours
M2	On Duty Senior Manager	4 hour	8 hour	96 hour	48 hours
M3	On Duty Director	8 hour	12 hour	1 x week	72 hours

Your incident ticket will be automatically escalated according to the above escalation matrix and you can always contact the Interoute CCC to receive confirmation about the escalation level of your incident ticket, or to request an escalation. This information will be also visible on the My Services web portal.

Level 0 - Service Desk - In order to meet this requirement the Service Desk runs a real time Incident & Request wallboard that notifies agents before the timer expires. Performance against this KPI is measured by using metrics within the Incident/request ticket such as the time stamp of the first ‘customer update’ activity recorded by a customer service agent. Interoute strives to provide a fast response to any incident or request logged with the Service Desk within 30 minutes.

Level 1 - Escalation Manager - Our Escalation Managers ‘Service Assurance Managers’ (M1) are assigned to all escalations. The M1 is the first level of escalation and is the coordinator of the escalation until resolution including the creation of RFO (Reason for Outage), if required. The Customer Support Agent would ‘own’ the incident, and the Service Assurance Manager (SAM) would co-ordinate investigation and resolution.

Level 2 - Head of Customer Services - Our Head of the Customer Contact Centre will become involved either at the request of the escalation manager or the customer to ensure the escalation is progressing appropriately and support the Escalation Manager accordingly.

Level 3 – Director of Customer Services - Our Director of the Customer Contact Centre will become involved either at the request of the escalation manager or the customer to ensure the escalation is progressing appropriately and support the Escalation Manager accordingly.

Level 4 - The VP of Operations Centres - Our VP for Operations Centres is responsible for escalating levels across their peer level selected tenderer contacts and internal senior authority level.

9.3 Defined Service Requests and Events

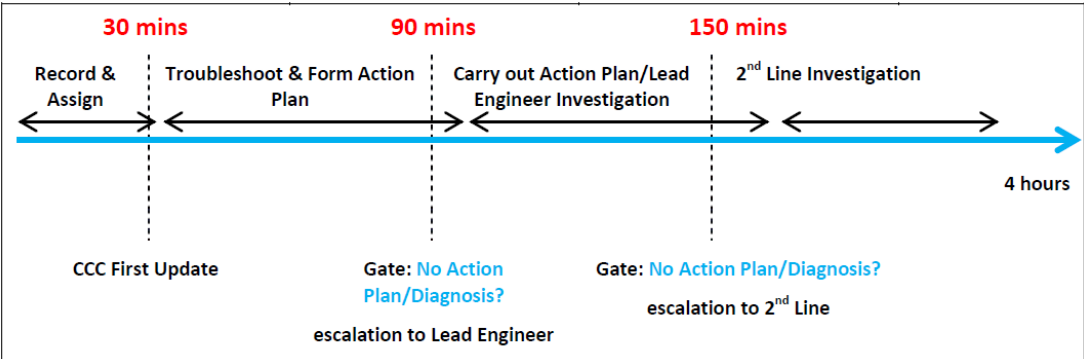
Interoute separates faults into 3 defined fault categories:

Category and availability	Issue	Level 1 (Generalist)	Level 2 (Specialist)	Level 3 (Vendor)	Resolution Target
Priority 1 24x7	Monitor failure (ICMP, HTTP, etc.)	15 mins	1 hours	4 hours	2 hours
	Monitored Service failure				
	Emergency restore request	See RPO & RTO Service Level Objectives			
Priority 2 24x7	Managed device reboot request	30 mins	2 hours	N/A	2 hours
	Managed device Service restart request		4 hours	8 hours	8 hours
	Monitor response time violation				
Priority 3 Business Hours	Standard restore request	N/A			Next Working Day
	Security policy change				
	Capacity warning				
	Virtual device change request				
	Standard restore request				
Priority 4 Business Hours	Information request	N/A			Two Working Days
	User admin request				

Depending on the severity of the failure Interoute engages the relevant fault diagnosis and resolution activities. The principle for these however remain the same; raise an incident ticket, contact the affected parties, identify the problem, initiate escalation procedure, issue fault status updates, resolve the issue and monitor progress of the faulty service.

9.4 Escalation Summary

- 24/7 Management and technical experts on call for network and customer incidents;
- Escalation is based on timelines or at Interoute’s Operational Management request;
- Matrix technical teams to resolve within SLA;
- Dedicated Escalation Manager for all Incidents escalated to M1 and above;
- Escalation Manager acts as strong customer advocate.



EXAMPLE CRITICAL TICKET | for a hard down service with a restoration SLA of 4 hours. ‘Suspend’ time is excluded.

9.5 VDC Solution Architecture: Resiliency

Interoute recommends that a customer deploys services across multiple VDC zones to provide resiliency within their service. A Customer can deploy their servicers either using active/active or active/passive balancing across zones ensuring continuity of service in the event of a disaster. All covered by a 99.99% SLA.

In addition to the multi zone deployment options customers can take advantage of the Affinity groups built into the Interoute VDC. Virtual Machines that belong to an affinity group are guaranteed to be deployed across multiple physical hosts providing a layer of resiliency within the individual zone for all virtual machines that make up a service.