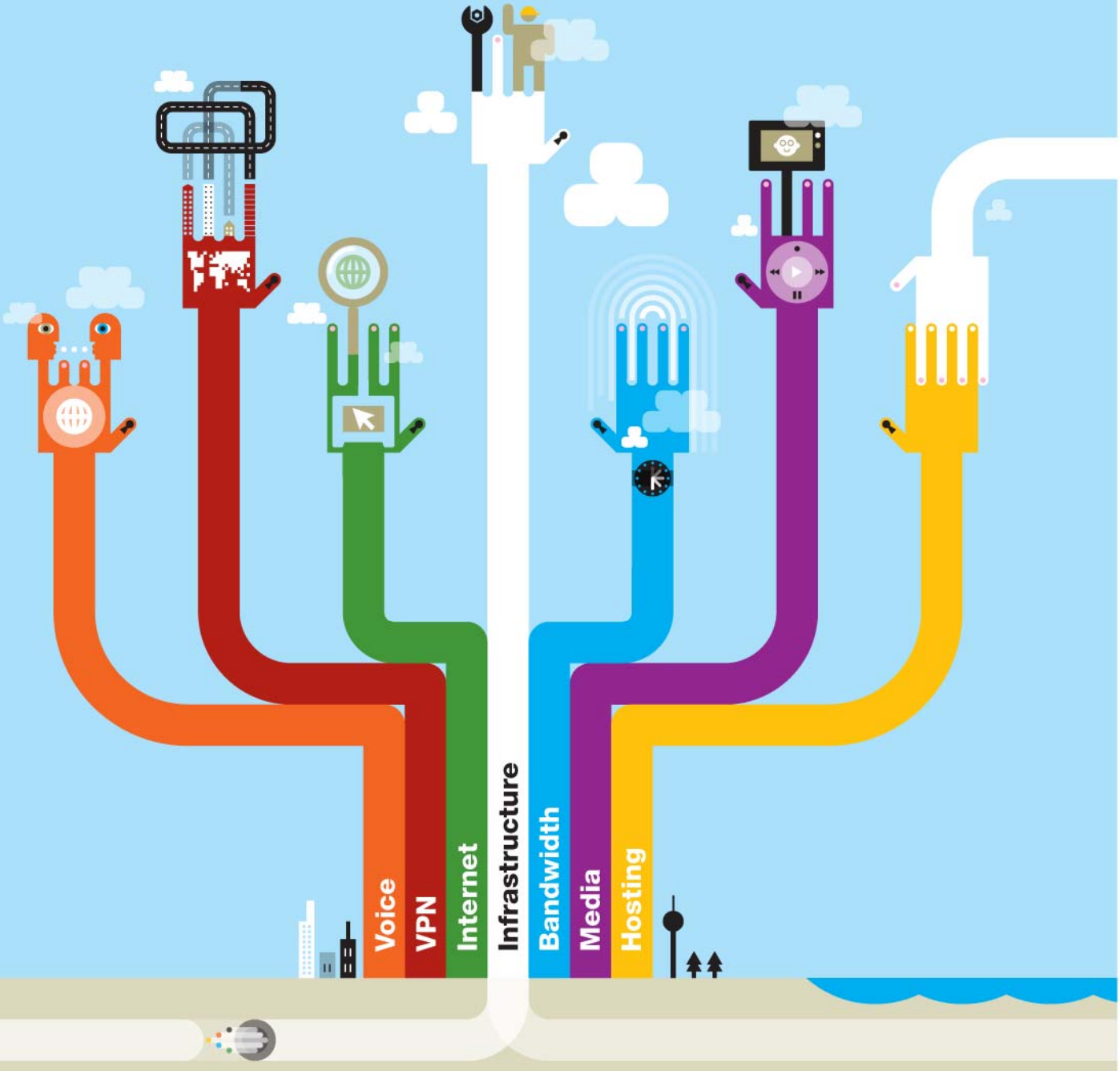
interoute
from the ground to the cloud

Customer Service Description
Next Generation Network Firewall



Interoute, Walbrook Building, 195 Marsh Wall, London, E14 9SG, UK
Tel: +800 4683 7681 Email: info@interoute.com

www.interoute.com

Contents

Contents

1 Introduction 3

2 An Overview 3

3 The Next Generation Network Firewall Service 4
Technical Service Details 4
Customer Requirements 5
Reporting 5

4 Commercials, Service Levels and Support 9
Pricing 9
Billing Options 9
Ordering 9
Service Support 10

5 Non Standard Options 10

1 Introduction

This document outlines the Next Generation Network Firewall Service and value proposition for you and our customers. It is intended to answer all the questions you are likely to encounter on a sales call or from your customer. Should you need any further clarification, please contact our Security Services Product Manager.

2 An Overview

The internet is now an enterprises primary tool for communication, research and customer interaction. Interoute provides firewalls to our customers to protect their enterprises from attacks. Historically this has been by controlling the TCP ports or opportunity for connectivity over the internet.

Today's Cybercriminals and malware producers are very sophisticated and rarely attempt direct port attack or control of an enterprises resources. The attack vectors taken by Cybercriminals today have a tendency to "poison" the web applications that enterprises users may be accessing. This means there is now a very real need to be able to monitor these web applications and secure the enterprise from any threat they may bring at the web application level

Enterprises increasingly need greater information on the performance of their network edge devices. Not only for their own peace of mind but also for compliance purposes. Therefore the provision of a firewall device that does not provide information easily and in a configurable format is no longer acceptable to the growing needs of enterprises.

Interoute is very aware of these growing requirements not only for the enterprise and its need for compliance but also the changing vectors of potential attack.

To this end Interoute is making available to its customers a Next Generation Network Firewall Service. The service comprises of a Checkpoint firewall based upon throughput and deployed within our Data Centres associated with the customers Internet access. The service platform will allow the customer to be able to access live information on what is happening at the firewall and also provide reports on line, via email or output as PDF and other formats.

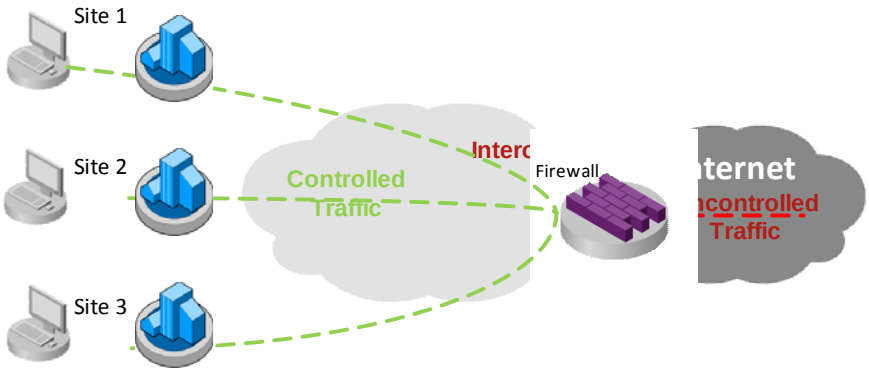
Interoute SOC will provide the support to the customer on the implementation of the customers firewall policy and the maintenance, support of the device and changes as required.

3 The Next Generation Network Firewall Service

Next Generation Network Firewalls are an important part of protecting any organisation from Internet threats.

Firewalls provide a central point for traffic control based on a rich variety of traffic characteristics:

- IP address – source or destination control
- Port Number – source or destination control
- Domain – DNS integration to simplify access to otherwise difficult to define resources
- Application Type – using deep packet inspection to control web applications
- Outbound IPv4 Network Address Translation and native IPv6 access to the Internet.
- Controlled Remote Access to Enterprise networks.



Technical Service Details

Interoute Next Generation Network Firewall Service enforces a specific policy to allow, block and detect traffic at the boundary to the Internet creating an internal secured zone. Two DMZ zones for Internet facing hosts and Corporate Wireless access are also reserved and external remote access is configured with software token authorisation at installation to provide a complete solution for all access needs.
The default configuration allows for outbound IPv4 NAT and native IPv6 access to the Internet.
Complete visibility and reporting of the network boundary provided by the firewall is available from real-time access to monthly and ad-hoc reporting.
Deployment in line with an Interoute supplied Internet Service is the only supported solution as it achieves the highest degree of protection and manageability. The firewall has the following additional features:

SSL VPN

Provides wide device support for remote access further secured by software tokens

Web Application Visibility and Control

Visibility and Control for Web apps, Web 2.0

Interoute structured methodology for the implementation and operation of firewall services has been developed by our security professionals with extensive experience in network firewalls. The high-level methodology is as follows:

Firewall Setup

Configure management, tuning, monitoring and alerting variables

Install recommended rule set

Settling-in process

Implement firewall rules specific to the customer environment

Post installation process

Enable alerting and reporting

Our structured approach means that the firewall is introduced into your network in a controlled fashion, ensuring that it is tuned correctly and will not block your connectivity and user traffic.

Customer Requirements

Interoute Network Firewall is deployed to protect the internal, privately addressed network and requires the following Customer information to provide full service:

- Mail Server information and other “inbound” rules
- Contact email address for reporting and service management
- Contact for management of software tokens
- Target machine for deployment of management software (see notes)

This information will require the full disclosure by the customer at time of order. The Next Generation Network Firewall Service Data Capture Form (DCF) will need to be submitted at time of order.

Interoute will be responsible for all aspects of the firewall configuration management, including:

- Maintenance and modification of the Firewall.
- Platform updates, with patches and version upgrades applied on a monthly basis. The specific time of the update will be agreed with the customer.

Reporting

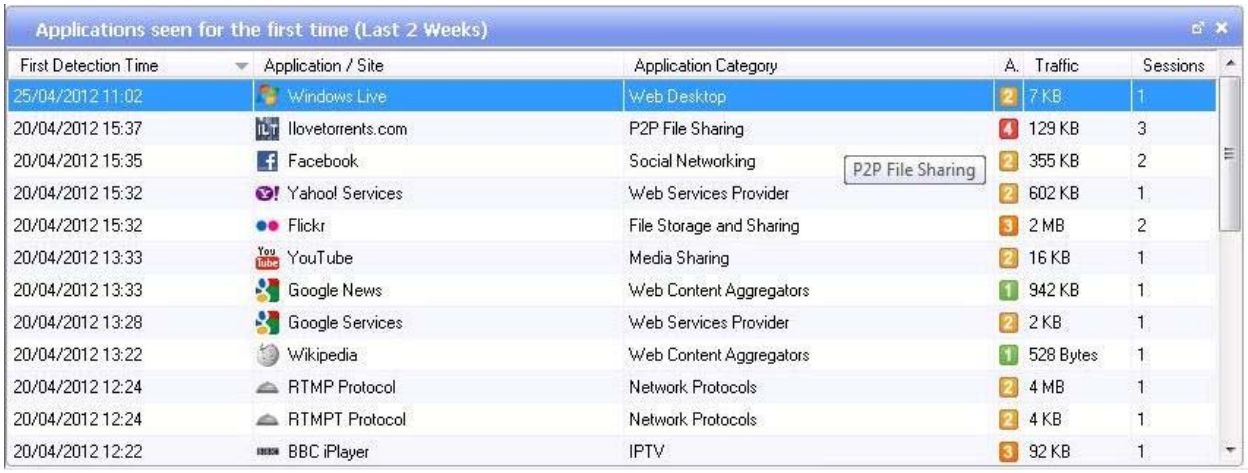
Interoute will provide you with a monthly firewall report that includes the following information relative to your specific Next Generation Network Firewall service:

- Top Services

- Top Sources
- Top Rules
- Top Applications
- Security Event information

One of the major benefits of the Next Generation Network Firewall Service from Interoute is that it provides our customers with a view of their firewalls directly. This means that real-time access to the firewall management environment can provide enhanced network reporting and visibility showing:

Application usage and risk:



First Detection Time	Application / Site	Application Category	A.	Traffic	Sessions
25/04/2012 11:02	Windows Live	Web Desktop	2	7 KB	1
20/04/2012 15:37	Ilovetorrents.com	P2P File Sharing	4	129 KB	3
20/04/2012 15:35	Facebook	Social Networking	2	355 KB	2
20/04/2012 15:32	Yahoo! Services	Web Services Provider	2	602 KB	1
20/04/2012 15:32	Flickr	File Storage and Sharing	3	2 MB	2
20/04/2012 13:33	YouTube	Media Sharing	2	16 KB	1
20/04/2012 13:33	Google News	Web Content Aggregators	1	942 KB	1
20/04/2012 13:28	Google Services	Web Services Provider	2	2 KB	1
20/04/2012 13:22	Wikipedia	Web Content Aggregators	1	528 Bytes	1
20/04/2012 12:24	RTMP Protocol	Network Protocols	2	4 MB	1
20/04/2012 12:24	RTMPT Protocol	Network Protocols	2	4 KB	1
20/04/2012 12:22	BBC iPlayer	IPTV	3	92 KB	1

Firewall rules and usage:

No.	Hits	Source	Destination	VPN	Service	Action	Track
1	2K	Internal4 Internal6	Any	Any Traffic	Any	accept	Log
2	112	Any	Internal6	Any Traffic	echo-request6 neighbor-advertisement neighbor-solicitation	accept	Log
3	6	JumpHost	Win7Client	Any Traffic	Remote_Desktop_Protocol	accept	Log
4	0	Any	Internal4	RemoteAccess	Any	accept	Log
5	0	Any	Mailserver	Any Traffic	smtp	accept	Log
6	78K	Any	Any	Any Traffic	Any	drop	Log

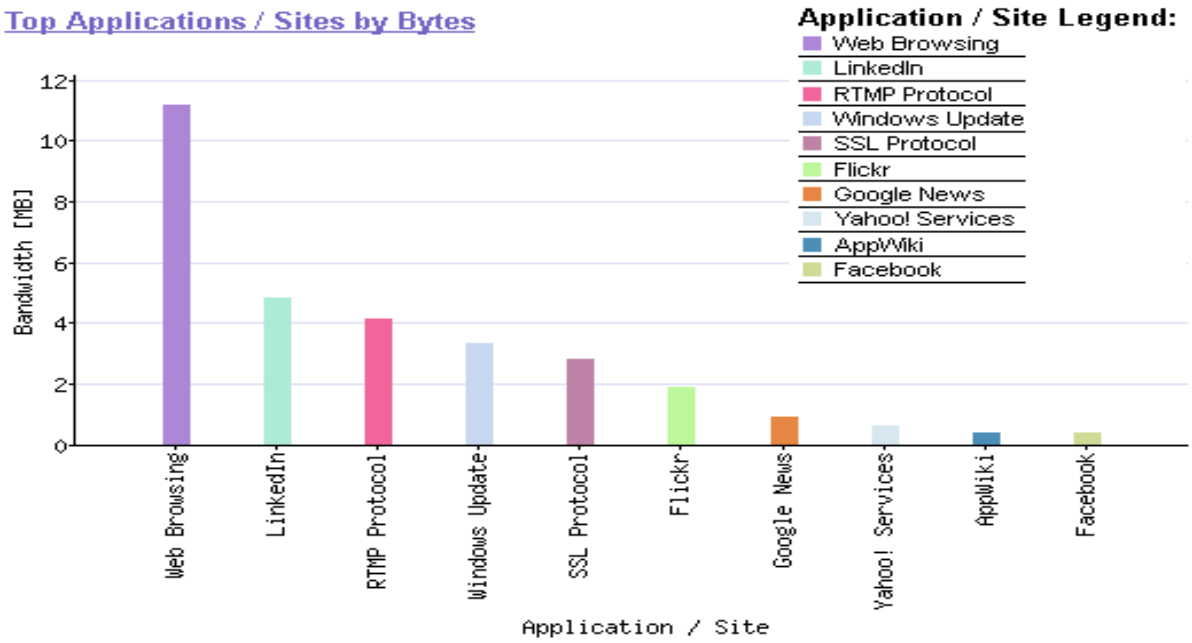
Application rules and usage:

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
1	14		Any	Internet	Facebook Games BBC iPlayer	Block	Log
2	2K		Any	Internet	Any Recognized	Allow	Log

Firewall logs:

Time			Service	Source	IPv6 Source	Destination	IPv6 Dst.	Rule
15:32:27		TCP	http	10.0.46.71		216.218.228.114		1
15:32:27		TCP	http	10.0.46.71		216.218.228.114		1
15:32:28		TCP	http	10.0.46.71		216.218.228.114		1
15:32:34		TCP	FW1_lea	10.0.46.69		10.0.46.70		1
15:32:34		TCP	FW1_lea	10.0.46.69		10.0.46.70		1
15:32:41		i..			2001:1478:a:a0...		2001:1478:a:a0...	1
15:32:46		i..			fe80::20c:29ff:f...		2001:1478:a:a0...	2
15:32:55		TCP	http		2001:1478:a:a0...		2001:470:1:18::...	1
15:32:55		TCP	http		2001:1478:a:a0...		2001:470:1:18::2	1
15:32:55		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:32:55		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:32:55		TCP	http	10.0.46.71		77.67.29.33		1
15:33:00		TCP	http		2001:1478:a:a0...		2001:470:1:18::2	1
15:33:00		TCP	http		2001:1478:a:a0...		2001:470:1:18::2	1
15:33:01		TCP	http	10.0.46.71		216.218.228.114		1
15:33:01		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:33:01		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:33:01		TCP	http	10.0.46.71		216.218.228.114		1
15:33:02		TCP	http	10.0.46.71		216.218.228.114		1
15:33:02		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:33:03		UDP	domain-udp		2001:1478:a:a0...		2001:1478:a:a0...	1
15:33:03		TCP	http	10.0.46.71		216.218.228.114		1
15:33:04		TCP	http	10.0.46.71		216.218.228.114		1
15:33:04		TCP	FW1_lea	10.0.46.69		10.0.46.70		1
15:33:04		TCP	FW1_lea	10.0.46.69		10.0.46.70		1
15:33:04		TCP	http	10.0.46.71		216.218.228.114		1
15:33:06		TCP	http	10.0.46.71		216.218.228.114		1

Top Applications/Sites



The technology of the Next Generation Network Firewall Service simplifies network security management by enabling administrators to schedule regular reports without constant manual intervention or reference to Interoute SOC.

Multiple reporting schedules can be maintained, making it flexible enough to meet the most demanding reporting needs. These reports can be automatically distributed to specific users via email or uploaded to FTP or Web sites. These reports can be generated in HTML or PDF formats.

With automatic report generation, we enable organisations to efficiently capture security and network intelligence on an ongoing basis. Customers can also generate reports for overall security performance analysis or auditing.

Performance Statistics

Interoute will monitor the firewall and in the event that the appliance does not responding to a poll, or in the event of an error condition being identified, will investigate and remediate to return the firewall to normal service. Interoute also captures health status generated by the installed firewall to a centralised management system that provides command, control and monitoring capabilities.

Supported Service Options

- CIR selectable from 1Gbps through to 10Gbps (up to 40Gbps and more available as a custom order)
- Virtual Firewall appliances for those customers with VMware hosted in an Interoute data centre with up to 500Mbps CIR. **Note: Application Control not available on this platform.**
- Fully managed service with customer access to customer specific areas of management platforms
- Custom alerting and reporting available as a professional services engagement
- Nominated user name and password access to management and reporting platform.
- Read only access of the management platform via proprietary software tool
- SSL support integrated into the platform which allows SSL connection for users regardless of device.
- Bundled Remote Access Software Tokens (5) to support, more available as separately purchasable option
- Clustering for High Availability

Unsupported Service Options

Interoute has specified firewall performance and features very carefully based on testing and experience. Some firewall features increase load/complexity to a point where throughput and stability can be compromised so the following are not supported in the standard product:

- Inbound NAT to user services (e.g. Web Server); the publicly addressed DMZ zone provides this function

- IPsec VPN (available in special use cases but replaced by more functional SSL VPN)

Security Servers

Features other than Firewall/NAT, Web Application Control, SSL VPN/Mobile Access

Support of end-user devices used for Remote Access and Management Access.

Product Codes

Interoute Next Generation Network Firewalls are selected by a specifying a committed information rate.

Sizing	Committed Information Rate	Product Code
Small	1Gbps	CON-CPAP-SG2207
Medium	3Gbps	CON-CPAP-SG4407
Large	10Gbps	CON-CPAP-SG12207
Virtual	Up to 500Mbps	CON- CPSG-P107

4 Commercials, Service Levels and Support

Pricing

The Interoute Next Generation Network Firewall Service is a service based upon throughput which is equivalent to the throughput of the internet service provided. The service includes the costs for management, management interface and reporting portal.

Billing Options

The following Billing plans are available for the Symantec.cloud Services offered by Interoute:

- An initial non-recurring charge
- A monthly fixed rate charge for the term of the contract

The non-recurring charge is a fixed fee that is payable on a per customer basis. It is important to note that the non-recurring charge is payable on acceptance of order and not refundable.

Ordering

The service is ordered via an order form and standard terms and conditions. For the order to progress a Data Capture Form will be required at time of order. A “clean” order and DCF should take around 10-20 working days to be provisioned depending on equipment availability.

Service Support

All the services are supported by Interoute Security Operations Centre. The normal hours of operation are 08:00 to 18:00 daily. The Security Operations Centre will support customer calls and liaise during these hours. Outside of these hours the Security Operations Centre is covered by rota staff.

5 Non Standard Options

Any required customer solution that requires deviation from the standard topology for installation will be treated as a bespoke service. Bespoke services are satisfied via the submission of a Customer Design Document via your account manager of account System Engineer.

Notes:
Management Software Requirement:

Management Software Console Requirements

This table shows the minimum hardware requirements for console applications:

Component	Windows
CPU processor	Intel Pentium Processor E2140 or 2 GHz equivalent
Memory	1024MB
Available Disk Space	900MB
Video Adapter	Minimum resolution: 1024 x 768