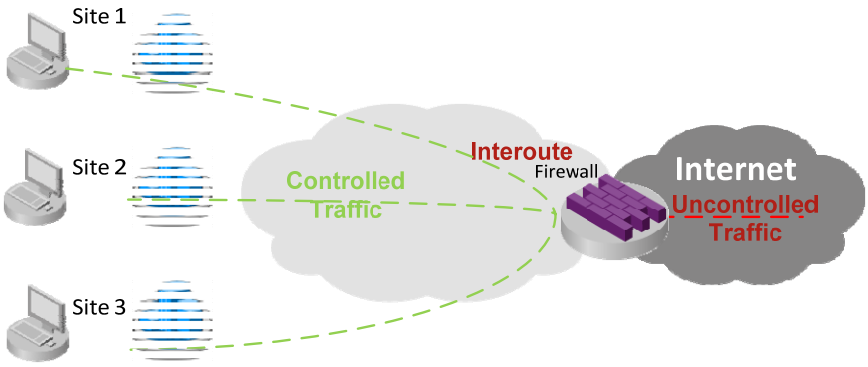
Next Generation Network Firewall



Overview

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

Next Generation 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

Next Generation Firewalls also play a key role on IPv4 networks providing outbound Network Address Translation to the Internet and controlled Remote Access to corporate networks.

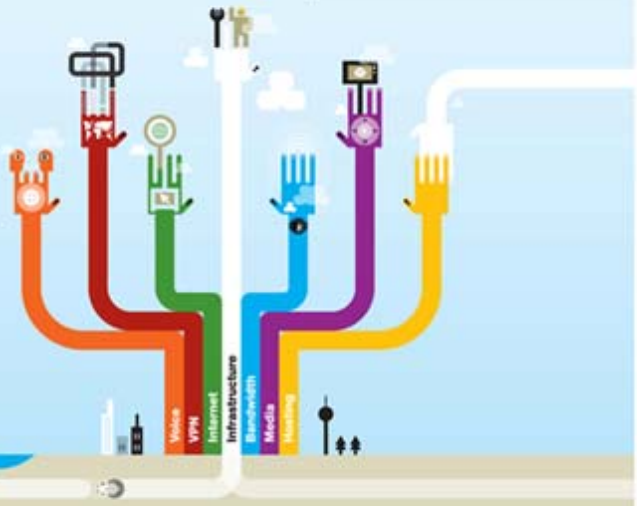
Technical Service Details

Interoute Next Generation Network firewall 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 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, standard 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 production traffic.

Customer Requirements

Interoute Next Generation Network Firewall is deployed to protect the internal, privately addressed network and requires the following 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

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.

Supported Service Charges

The Interoute Next Generation Network Firewall service is billed as a combination of Non-Recurring Charges (NRC), and Monthly Recurring Charges (MRC).

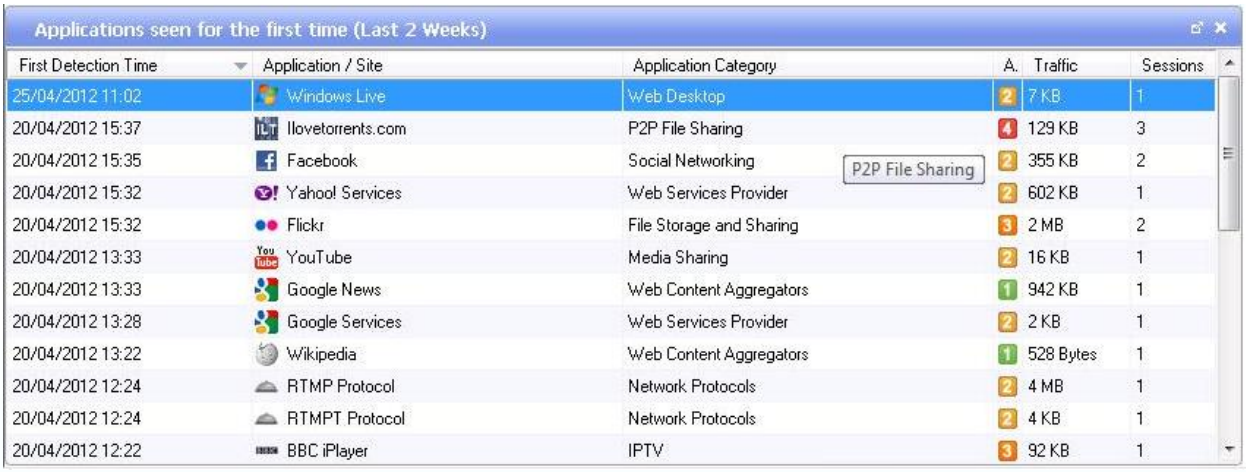
Reporting

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

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

Interoute also provides real-time access to the firewall management environment to provide enhanced network reporting and visibility showing:

Application usage and risk:



Applications seen for the first time (Last 2 Weeks)

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

P2P File Sharing

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

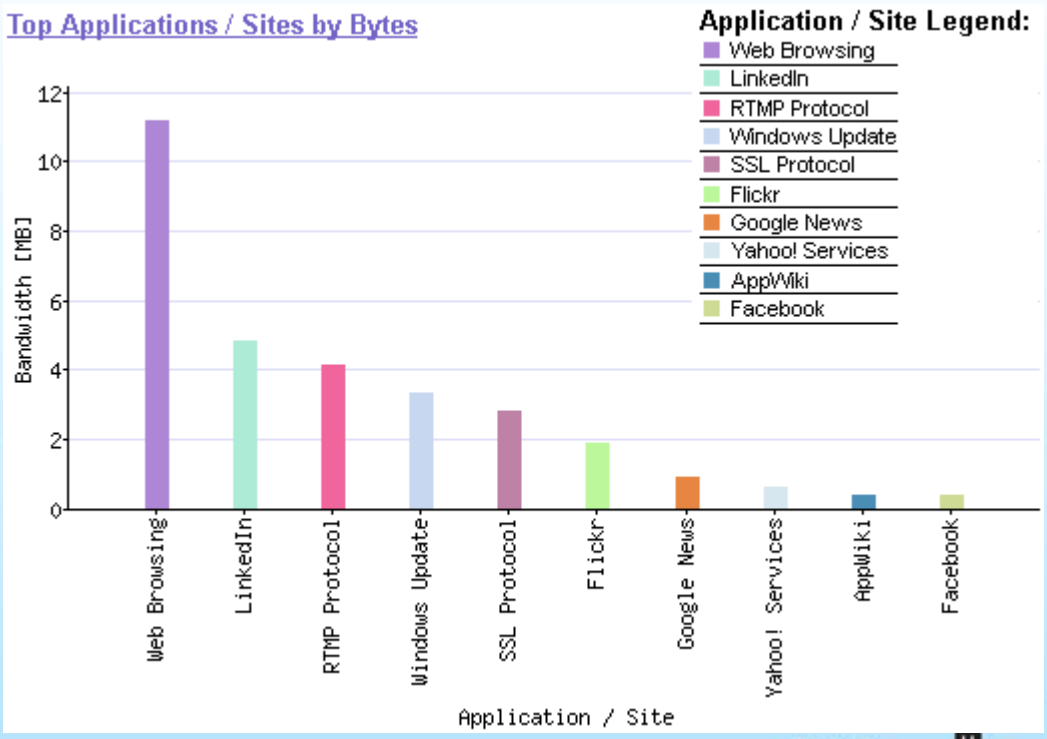
Application rules and usage:

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

HTML reports delivered by email:



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
- 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-SOC-VEN205

How to order

Order through an Interoute Account Manager.

More information

For product enquiries please consult the Security Services Product Manager.