Securing Cost Savings for Scottish Police

Single communications infrastructure improves inter-force collaboration and supports CESG security standards

EXECUTIVE SUMMARY

CUSTOMER NAME
- Scottish Police Services Authority

LOCATION
- Glasgow, Scotland

INDUSTRY
- Public Sector – Government

COMPANY SIZE
- 1,600 employees

BUSINESS CHALLENGE
- Establish a nationwide shared services network infrastructure
- Introduce dynamic data encryption capability
- Enable delivery of national policing applications
- Standardise technology platforms

NETWORK SOLUTION
- Cisco foundation networking technologies
- Cisco virtualisation architecture
- Cisco borderless networks architecture

BUSINESS VALUE
- Foundation for centralised services which will improve collaboration between Scottish police forces
- Streamlined deployment of applications
- Cost savings and efficiencies for policing
- Data encryption for enhanced information security

CUSTOMER PROFILE

Digital communications enrich our world but can also open the door to social ills such as terrorism, fraud and identity theft. The Scottish Police Services Authority (SPSA) is entrusted with establishing a consistent and effective national service provision in a number of discrete areas:

- Realise efficiencies through sharing of resources and best practices
- Enable economy of scale
- To support and allow police forces to focus on operational policing

Inaugurated in April 2007, the SPSA is a non-departmental public body that manages police information systems, forensic services and training on behalf of Scotland's eight police forces and wider criminal justice community. It provides one of the world's only independently-accredited crime scene to court forensic services; manages information systems used by more than 50 agencies across the UK; and trains over 8,000 police officers every year through the Scottish Police College. It also maintains the Scottish Crime and Drug Enforcement Agency. It has over 1,600 staff and an overall budget of over £100 million.

ORGANISATIONAL CHALLENGE

Before the SPSA was established, police forces in Scotland managed IT systems independently of one another, and each force was responsible for its own technology systems, software applications and data repository.

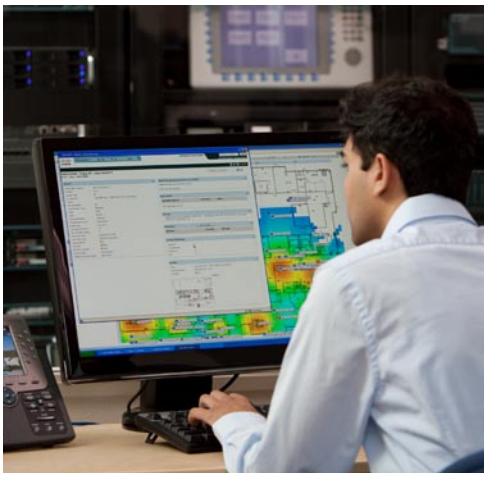
In 2006 the Association of Chief Police Officers in Scotland (ACPOS) agreed that a shared services infrastructure was needed to reduce administrative overheads and increase resources available for front line policing. The SPSA was created by the Scottish Government to consolidate common functions such as forensics, training, technology systems and ICT assets.

A centralised data network called Scottish Police Network (SPN), hosting applications and serving information from two data centres East and West, was started in April 2008. Using Multiprotocol Label Switching (MPLS) to run secure connections between all police forces and agencies in Scotland, a change in legislation during the deployment of the SPN presented some additional challenges for the project team.

The UK Government's Communications Electronic Security Group (CESG), which defines the data security standards that all government agencies must adhere to, introduced regulations that the original plans for the SPN would not meet. New legislation required all data marked 'RESTRICTED' or above in the CESG classification system to be encrypted if being sent over a public communications network.

Billy McMath, Head of Technical Services, SPSA,explains "We'd spent a lot of time and effort on building the network but when the CESG issued the new directive, it completely changed the game for us. Suddenly our WAN was not suitable for information of a certain security level because it didn't have data encryption capability."

To address the changes, the SPSA adopted CESG recommendations for a cryptographic hardware solution involving the use of point-to-point devices. However the hardware was not compatible with the design of the SPN and proved difficult to manage and scale.



NETWORK SOLUTION

SPSA came up with an alternative that would enable it to dynamically establish and collapse encrypted point-to-point connections on the fly. The software-based solution involved fitting all Cisco routers with CISCO DES/3DES/AES/SSL VPN Encryption/Compression cards and incorporated an encryption accelerator module to maintain data processing performance.

The SPSA Information Services division manages some 21,000 handheld radios, 12,000 desktop computers and laptops across over 250 sites. It uses Cisco ISR routers to link police sites and Catalyst 6500 Series Switches as the core switches in the two data centres. Cisco Catalyst 3100 and 2800 Series Ethernet Blade Switches provide resilient connectivity within its two data centres.

Cisco MDS 9000 Series Multilayer Switches are used to deploy the storage area network that distributes critical policing applications to all sites. ACE devices ensure application load balancing across the two data centres while Global Site Selectors ensure load balancing across the wide area network.

Cisco's ONS 15400 Series Multiservice Platform supports a Cisco Dense Wavelength Division Multiplexing (DWDM) solution between the two data centres to improve availability and redundancy. Cisco DWDM is also used to partition fibre optic cabling into separate fibre channel and ethernet connections.

BUSINESS BENEFITS

Having established the shared services network the SPSA embarked on a programme to centrally host key police applications, while decommissioning local variants. This was scheduled to support the ACPOS business change programme and the first application to be migrated was HOLMES (Home Office Large Major Enquiry System) – a national investigation management system used by all UK police forces. The eight separate HOLMES instances were replaced by a single version to be used by all Scottish forces.

Seven further applications are already at different stages in moving onto the shared services network, including the National Custody System – being rolled out as a single integrated custody management system for all Scottish forces. Already, some forces are benefiting from the National Infrastructure providing new Firearms Licensing Management Systems as part of national

PRODUCT LIST

DATA CENTRES
- **Cisco Data Centre**
- **Cisco Firewall Services Modules (FWSM)**
- **Cisco ACE Modules**
- **Cisco Global Site Selectors**
- **Cisco IOS**
- **Cisco Works**

ROUTING AND SWITCHING
- **Cisco Catalyst 6500 Chassis Switches**
- **Cisco IOS Routers**
- **Cisco Catalyst 3800 and 2800 Routers**
- **Cisco PoE Switches**
- **Cisco MDS 9000 Fiber Channel Switches**
- **Cisco ONS 15400 Series Multiservice Platform**

convergence and all forces have benefited from the National Infrastructure supporting a very successful project to rationalise back office services for the Safety Camera Partnership, enabling centralised processing of fines for driving offences. The network will also support a new single integrated Command and Control system for the whole of Scotland.

Centralisation has improved operational efficiency and enhanced disaster recovery provisions. It also enables a more sustainable and cost effective approach by reducing the requirement for separate servers.

Billy McMath says that the deployment of applications and storage of data using a national infrastructure has enabled the SPSA to help streamline policing procedures in Scotland: "Having a single technology platform makes it much easier to support operational standards across the forces and be consistent in analysing performance data."

Improved network security management ensures better intrusion prevention. Cisco's Security Monitoring, Analysis and Response System aggregates all network threat notifications and alarms that exhibit a trend into a single incident and prioritises each by severity. The SPSA Security team can now spot anomalous behaviour from inside the organisation as well outside.

Most recently, the software approach to network encryption successfully leverages the existing infrastructure, making it significantly cheaper than hardware based solution. It also meets CESG requirements as well as network outage response targets. Redundancy in the network is supported by the Global Site Selectors, which redirect traffic between data centres in the event of failover.

Billy McMath says, "We're proud of the technological advances the SPSA has introduced and the underlying infrastructure is a key part of that."

"We're proud of the technological advances the SPSA has introduced and the underlying infrastructure is a key part of that."

Billy McMath, Head of Technical Services , SPSA

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

The Print Consultancy (01483 771211) / Feb 09

Printed in the UK