

# Notouch

Issue 2 : Spring 2009

www.networksfirst.com



## Moving towards a holistic approach to networking

Even the tough times produce their own unique set of opportunities. For example, we are already seeing how the 'big players' are halting recruitment and looking to outsource network support which previously they could have managed internally.

We are also seeing a market growth in a more holistic approach to network support. More and more businesses now understand the importance of seeing their network as a whole entity and therefore accepting the recognition that support must also be integrated into whole network infrastructure.

This approach is, quite rightly, being encouraged by the manufacturers who appreciate that every component needs to be looked at to make up the whole network. Interestingly, this is resulting in us developing a much closer working relationship with many of the leading manufacturers and we are strategically realigning ourselves accordingly. Ever more manufacturers are looking for ways to further improve the services wrapped around their

product portfolios and are recognising that high quality value add service partners are vital not only in retaining customers but in winning new ones.

This year, Networks First will be investing a lot of extra effort into building strategic alliances with key manufacturers and looking at new strategies to help us deliver a more holistic service in an affordable, innovative and effective way. All of which will help us to focus on our key aim: how we can improve margins not only for us but also for you, our partners.

To help us develop the right services to meet your needs not only now but in the future, we would like to ask all our partners to provide us with valuable feedback on what you need from us to make 2009 a successful year for you. We will shortly be issuing our latest market survey but in the meantime feel free to give me a call. Many thanks and I look forward to hearing your views...

Peter Titmus, MD, Networks First

## Networks First developing customer portal



'Firecrest' to provide partners with an interactive tool and access to real time information.

Networks First's new customer portal, Firecrest, has now entered its pilot testing phase. The interactive tool will provide partners with access to real time information at the touch of a button.

Developed by Networks First's own internal IT development team following a significant investment, the portal gives partners secure visibility of live information regarding all of their interactions and activities. Benefits include a more efficient interaction with the service desk as well (continues on page 3)

## New vendor manager keeps manufacturer support strong

We are delighted to announce that Bill Rhodes has taken up the role of Vendor Manager at Networks First to ensure that our partners are aware of every opportunity available to them whilst providing a powerful multivendor, mixed technology proposition to their customers.

By having the manufacturers' full and proactive support for our services we are able to identify manufacturer opportunities that you can adopt as part of your Business Development plan.

As a best of breed organisation, Networks First

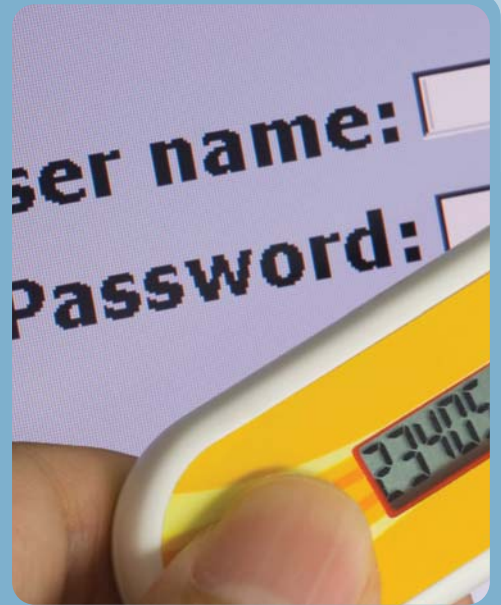


believes an integral part of any solution is the delivery of seamless support. Therefore every solution that we deliver on your behalf aims to build on, and enhance, the manufacturers' offerings. We work hard to make sure that all the leading manufacturers are happy to work with us, so that together we can provide a unique quality of service to your customers.

Bill Rhodes says, "Recent changes to the economy have brought with it a focus on the importance of renewing network security and efficiency. The market is increasingly looking to their service supply partners to provide an enhanced proposition that meets critical business needs. We are working with the manufacturers to identify and provide this extra value that will enable you to differentiate the solution that you are able to offer your customers."

# Do Local Authorities need to beef up their security? *I should CoCo!*

Paul Lewis, Network Consultant



An important deadline is looming for Local Authorities. The Government is requiring them all to connect to the Government Connect Secure Extranet or GCSx network, which has its very own Code of Connection or CoCo. The deadline for signing up as compliant to the various security control measures it contains is **31st March 2009**.

## What is the GCSx?

The GCSx is a Wide Area Network (WAN) provided by Cable & Wireless, under contract to the Government. The aim is to provide robust and secure inter-connection for the networks of Local Authorities, critical Government bodies, and other approved organisations.

GCSx, for instance, provides secure gateways to the NHS (N3), the Government Secure Extranet (GSX), the Criminal Justice Extranet (CJX) and the Police National Network (PNN).

Critically, the GCSx and interconnected networks are approved to carry sensitive information, such as personal data and that classed as restricted. This will help bodies adhere to their duties under the Data Protection Act.

As a single network, from a single vendor, it should also be much easier to define and monitor Service Levels on the platform, which is not the case with most Internet-based connectivity, even when it is adequately secured (for example using encrypted IPSec tunnels).

## What are the key compliance requirements?

There are lots of requirements covering all areas of ICT security, though some are recommended rather than mandatory. One of the main stumbling blocks affecting Authorities is the mandate that remote workers accessing the networks must authenticate strongly, using a two-factor process.

## What is Two-Factor Authentication?

Authentication is the process of confirming that someone is who they claim to be. Two-factor

authentication insists that a user requiring a service (in this case, remote connection to the network) provides two different pieces of verifiable evidence concerning their identity:

**Something they know** - usually a passcode or PIN  
**Something they have** - this is usually a small token device, though these days there are a number of alternatives, including biometrics (almost what they are, rather than what they have!)

The key idea is that, if just one of the criteria is compromised (for example a token is lost, or someone has obtained a password or PIN by social engineering), access security is not compromised.

If you think about it, this is a process we all know - and mostly trust - for accessing our money through a cashpoint - you're stuck without both your bankcard and its PIN.

In IT terms, two-factor authentication has been around for a long time, but it has not been implemented by many organisations despite the proven security benefits; primarily because of cost. Many organisations are now starting to realise that these costs are, relatively speaking much lower, as the same system can now be used to authenticate multiple services, including IEEE 802.1x Wired and Wireless LAN authentication, Dial-up, IPSec and Secure Sockets Layer (SSL) VPN network access. Strong authentication is also proving invaluable for securing management access to key IT systems such as server, switch and firewall administrator logins.

Far and away the leading vendor for two-factor authentication systems is RSA Security (now a division of storage giant, EMC) - in fact RSA's pedigree in the Security arena means that virtually all systems incorporating encryption technologies for instance, are underpinned by RSA technology.

## RSA Authentication Manager and SecurID authenticators

RSA's system is based around its Authentication Manager (formerly known as ACE/Server). This acts as the central two-factor authentication system to which points of network access, such as VPN concentrators, Firewalls or Wireless Access

Points, are referred when receiving connection requests. Traditional hardware tokens, such as those commonly seen on key-rings, are still the most popular authenticator. However, increasing use is now being made of newer alternatives including software on smart-phones or PDAs, which does the same job, without requiring a dedicated device.

In addition to its two-factor capabilities, Authentication Manager also incorporates the widely deployed and proven Steel-Belted RADIUS software. RADIUS (Remote Authentication Dial In User Service) software is often an intermediate port-of-call for remote access authentication, before referral to a two-factor authentication system - providing additional authorisation and accounting features. This means that the full deployment requirements for secure remote access can be delivered with a single solution.

Another relatively recent RSA development is the availability of Authentication Manager in a dedicated, hardened appliance format, making it simpler and easier to deploy and maintain.

RSA has understood the challenges Councils face in meeting CoCo requirements and have responded with special pricing for two-factor authentication services, in this vertical space, available until the CoCo deadline at the end of March.

## How Networks First can help

In addition to our proven skills in core aspects of networking, we have a long history of working with RSA's SecurID 2-factor authentication system. Not only can Networks First help advise Authorities in choosing the right blend of authenticators for their users' needs, but can also provide fully managed deployments, including the key role of integrating the system with numerous access technologies from many different vendors, including Cisco and Check Point. We can also, of course, provide tailored and responsive support services to keep the network and its security system working into the future.

# Networks First makes website more user friendly



Networks First is proud to announce the launch of its brand new corporate website and would like to take this opportunity to briefly introduce a few of the upgrades which we hope will make for a more user friendly and interactive experience.

Firstly, the new navigation menu allows users to browse the site and find information far more quickly and easily than before. The website now

includes an audio listening facility to allow visitors to hear up-to-date information on our services, partners and accreditations.

And finally, the new 'hot topic' voting panel asks partners to give their views on industry topics.

We hope you like the changes and would welcome any feedback following your next visit!



## A healthy connection

Networks First is pleased to announce that it has successfully completed the NHS Connecting for Health Information Governance Statement of Compliance process. This means it has now officially become a Commercial Third Party (CTP) organisation for connection to the NHS N3 network.

As you probably already know, N3 provides fast, broadband networking services to the NHS, offering reliability and value for money. The high-speed network makes it possible to deliver the reforms and new services needed to improve patient care.

Based on the international standard for 'Information Security Management', ISO 27001 (formerly BS7799), the rigorous approval process involved Networks First responding to a series of qualified security and technology based criteria, as well as the support of a named sponsor within the Healthcare market.

Derek Dale, Networks First's Service Director says, "Networks First's approval to join the N3 network demonstrates our ability to meet the most stringent security requirements and will enable us to start working more closely with partners in further extending our Swift Vision / Swift Plus portfolio of services into the NHS. Joining the N3 network will mean that Networks First will now be able to connect with numerous NHS units across the UK in the safest and most secure method possible."

To find out more, please contact your account manager.

## Best Companies – Shining stars

Networks First has been awarded two stars at the prestigious Best Companies Awards 2009.

The Best Companies awards not only aim to recognise industry leading organisations operating in the UK but also help organisations identify their strengths and weaknesses whilst providing benchmarks and guidance to help improve performance.

It rates companies equally across eight key factors within the workplace: Leadership, My Company, Personal Growth, My Manager, My

Team, Giving Something Back, Fair Deal and Wellbeing.

Peter Titmus comments: "This is only our second year of entering the Best Companies Place to Work so we are delighted to have already achieved the two star status. Winning two stars is recognition of our employees' commitment to Networks First and we hope to continue to develop and deliver a rewarding workplace. I firmly believe that delivering service excellence begins by focusing on employee engagement."

(from front page)

as the ability to view incident reports and statistics online, providing partners with an immediate overview of their customers' incidents to ensure they are fully empowered to deal with any network issues quickly and effectively. Future versions of Firecrest will also allow users to view quotes, orders and contracts online.

Peter Titmus comments: "Networks First's goal is to become the partner of choice in delivering Network Support Services. But being the partner of choice isn't just about providing a pricing model

that meets with expectations, it's about going that extra mile to be responsible, responsive and reliable. To do that, we need to be continually improving our services. It is for this reason that we have decided to invest heavily in developing new technologies that will allow us to lead the field in service support.

"The launch of Firecrest is the next step in achieving complete transparency with our partners. It's a solution that fully embraces our philosophy of a true partnership – providing

partners with the information that they require as soon as they require it."

"Networks First is currently working with a number of partners to test each element and following in-depth evaluation and feedback from this pilot process, we will be rolling Firecrest out to all of our partners."

If you are interested in joining the pilot process, please contact your Networks First account manager.

# Skills snapshot – here's what we can do!

In the past 18 months Networks First has increased the number of vendors it works with and wants to keep partners aware of the company's full skills capabilities. The table below demonstrates the vendors and associated skills and accreditations the company holds.

If you have any questions about the skills Networks First holds for any of the manufacturers, please do not hesitate to contact your account manager.

Manufacturer & Accreditation	LAN	WAN	IPT	WLAN	Security	RNM (Remote Network Monitoring)
<b>3Com</b>	✓	✓	TE	TE	TE	TE
<b>Aruba</b>	NA	NA	NA	✓	NA	NA
<b>Avaya</b>	TE	TE	✓	NA	NA	✓
<b>Brocade</b> (formerly known as Foundry Networks)	✓	NA	NA	✓	NA	✓
<b>CA (Spectrum)</b>	NA	NA	NA	NA	NA	✓
<b>Cisco – Silver</b>	✓	✓	✓	✓	✓	TE
<b>Dell</b>	✓	NA	NA	NA	NA	NA
<b>Enterasys – Gold</b>	✓	✓	NA	NA	NA	NA
<b>Extreme – ESP</b>	✓	NA	NA	✓	NA	TE
<b>HP Procurve</b>	✓	NA	NA	✓	NA	TE
<b>Juniper (Netscreen)</b>	NA	NA	NA	NA	✓	✓
<b>Mitel</b>	NA	NA	✓	NA	NA	✓
<b>Nokia Checkpoint</b>	NA	NA	NA	NA	✓	NA
<b>Nortel – SSP</b>	✓	✓	TE	✓	TE	NA
<b>Packeteer</b>	NA	✓	NA	NA	NA	NA

✓ – Formal Accreditation  
TE – Trained or Experienced Personnel  
NA – Technology not available from the manufacturer

**3Com** – Networks First has 14 trained 3Com engineers

**Aruba** – Networks First has Aruba wireless capabilities for site survey and commissioning

**Avaya** – Networks First has skills to design and install IP Office

**Brocade** (formerly known as Foundry Networks) – Networks First has skills in design and commissioning of Foundry Networks

**CA Spectrum** – is used for our high end remote network monitoring service

**Cisco** – Networks First has been a Cisco Silver Partner for five years

**Dell (PowerConnect)** – Networks First has skills in the installation and commissioning of Dell PowerConnect

**Enterasys** – Networks First is an Enterasys Gold partner

**Extreme** – Networks First has been an Extreme partner since 2000

**HP Procurve** – Networks First has seven accredited engineers

**Mitel** – Networks First has the highest number of Mitel 3300 engineers in the channel

**Nokia Checkpoint** – Networks First has five Checkpoint trained engineers

**Nortel Networks** – Networks First has consultancy skills in Nortel Networks and has been an SSP for three years

**Packeteer** – Networks First has skills in the installation and commissioning of Packeteer

## Feedback

We're keen to hear your feedback on our newsletter and would welcome any ideas for content or your thoughts on the layout and style. Please contact the editor at : [editor@networksfirst.com](mailto:editor@networksfirst.com)

### Contact details:

Networks First  
Number One, Paper Mill Drive,  
Church Hill South, Redditch B98 8QJ  
Tel: 0845 850 5577 Fax: 0845 850 5577  
Email: [editor@networksfirst.com](mailto:editor@networksfirst.com)