

Background

Borlänge Municipality is a Swedish borough in Dalarna County in central Sweden with a population of approximately 47,000 people. The municipality is the largest employer in the region with some 3,700 employees and local government officials.

Borlänge Municipality is a dynamic organisation, continually developing their operations and services. Recognising the benefits that remote network access technology could deliver in terms of improving communications across the organisation and improving service delivery in the community, the municipality saw it as a vital development to provide remote access/mobile working facilities for employees and officials. They had previously already deployed various remote access systems. For example, external suppliers were using RAS dial up to access key systems on the network and provide on-line support and maintenance. However, these systems proved inflexible, slow and costly, and network admission was difficult to control. Borlänge needed an alternative remote access solution that would address the issues of the existing system and provide a platform for expansion in the future.

Requirement

Remote/mobile access: Borlänge needed a system that would give employees and officials the flexibility to work anywhere as if they were in the office, with access to the network resources and services they needed from their own laptops, home pc's, and PDA's.

Network access control and network security: One of the key issues with their existing remote access system was how to restrict access on a needs-only basis. To ensure that applications and data on the network were protected from unauthorised access, the Borlänge IT team needed a solution that would give them control over the level of access granted to each user.

Easy-to-use: As they were planning to provide remote access to employees and groups based across the municipality, they needed a solution that could also be managed centrally, that would be easy for employees to use thus minimising the need for extra support, and which could be easily expanded to include more groups and add more functionality in the future.

Solution

Borlänge Municipality identified that the network security solution developed by AppGate would address all their requirements. An AppGate Security Server was installed behind their firewall, replacing all their previous network access products with one comprehensive system.

....continued overleaf...

"The AppGate technology is a dream. It's easy to set up and maintain and I have full control over everything - it's up to me what happens. I wouldn't change it for anything!"



Christer Hammarstrom
Technical IT Manager
Borlänge Municipality

"The support I get from AppGate is marvellous. Right from the start they worked closely with me to ensure that everything worked smoothly, and they still continue to provide me with lots of help and advice."

Christer Hammarstrom
Technical IT Manager
Borlänge Municipality



In a world with fewer borders, the demand for network security changes from security at the perimeter, to security at the source. AppGate is the leader in this space, with a solution that protects applications, protects communication and secures end point devices. The AppGate solution supports all types of transmission, fixed, wireless and mobile and is easily integrated into any customer environment. AppGate has customers in 19 countries, many from market segments like defense, government and Fortune 500 companies.

Solution continued ...

The AppGate solution integrated seamlessly with the existing infrastructure. Using accounts and roles defined centrally in Novell Directory Services, the AppGate server's authorisation system allowed the Borlänge team to define powerful rules for what applications and services should be available to each user. The laptops and PC's of all employees needing access to critical applications were installed with AppGate's Personal Firewall, and the Client Check functionality ensures that remote devices have and are running the latest antivirus update before any connection is allowed.

Employees are now able to connect securely to the network regardless of their location. Those working from home can use their own PC's to access the applications and services they need, and using AppGate's Secure Print functionality, they can print documents locally rather than having to go into the office. Employees working in social care can use their PDA's to access email and the intranet while they are out working in the community, and IT support teams are able to provide remote desktop support regardless of their location, using their PDA's and laptops to do system checks and server maintenance.

The flexibility of the AppGate solution has also made it easy for other groups to use the network. Branch offices based around the municipality that previously had no access to the intranet, and the neighbouring borough in the county of Säter that needed to use the common administration system, can all now easily connect to the network without the need for a leased line or IP-SEC VPN solution.

"The AppGate technology is a dream", said Christer Hammarstrom, Technical IT Manager for Borlänge Municipality. "I have full control over everything and I wouldn't change it for anything!"

Future

The flexibility of the AppGate solution is allowing Christer Hammarstrom and his team to roll out additional functionality one step at a time. Currently they are testing remote access by mobile phone and will be looking to roll it out across the organization, leveraging wireless access points that have already been installed.

Tips and Tricks

Access control is critical when diverse groups of users need to be able to connect to defined network resources securely.

The AppGate solution splits Network Access Control into two parts. The rules engine harvests information, which is then combined using Boolean statements into access rules. An example for IN_OFFICE might be: 'user is an employee AND operating system is XP AND device is connected via the WLAN'.

If IN_OFFICE is true then the user is offered the OFFICE Role. This is the second part of Network Access Control.

A Role defines exactly what network access is permitted on a server-by-server, port-by-port basis. So at one extreme, a 3rd party might have access to webserver1:80 only, while the OFFICE role might connect users to the mail server, intranet, CRM system and ERP system.

By controlling exactly what users have access to, security is optimised for the network.

