

Secure 3rd party access for hotel & leisure group

Background

De Vere Group plc, which specialises in hotels and fitness, has two expanding hotel brands: De Vere Hotels & Resorts and Village Leisure Hotels & Leisure Clubs, as well as a rapidly growing health and fitness brand, Greens. Across the group, third party suppliers support key systems such as property management systems, reservations and central office systems. To enable these suppliers to provide on-line maintenance and support, De Vere put in place IPSec VPN and dial-up remote access systems but discovered a number of limitations with these network solutions. So the company needed an alternative secure remote access solution with the flexibility and functionality to enable external suppliers to deliver better, faster service, enable De Vere's own staff to work seamlessly from any location, and support any additional mobile working applications they might introduce in the future.

Requirement

Since De Vere's corporate network was being accessed by a number of external companies, network security was a primary requirement. They needed a solution that would allow them to control 3rd party access, ensuring suppliers would just be able to connect to the applications and systems they needed, not the whole network. In addition, the system would need to be able to support any protocol, not just web based protocols, so that systems and applications could be fully maintained and serviced on-line. However, the solution also needed to simplify connection to the network for the users so that applications and systems, wherever they're located, could be accessed quickly to reduce the time taken for repairs and upgrades.

For De Vere's managers and support staff to be able to work effectively and seamlessly from any location, the remote access solution not only needed to provide full, secure access to corporate applications and data, it would also need to address the challenge faced by the system administrators of how to centrally control network admission and manage usage policies across all businesses in the De Vere group.

Solution

The network security solution developed by AppGate provided a comprehensive solution that addressed all De Vere's requirements and an AppGate Security Server was installed behind the company firewall. Network Defence, an AppGate certified partner specialising in delivering high performance, secure network solutions, lead the project to implement the system, and the installation was completed in just a few days.

....continued overleaf...

"The AppGate technology is amazing. It has delivered exactly what we needed in terms of flexible remote access and network security. And it's been very easy to add more applications. For instance when we added IP telephony - it all just worked!"



Ryan Lynskey
IT Infrastructure Manager
De Vere Hotels & Resorts

"The service from Network Defence and AppGate has been superb. The team listened to us and took time to understand our business, so when we needed some slightly different functionality, they molded the solution to meet our needs and ensured that it worked with our systems."

Ryan Lynskey
IT Infrastructure Manager
De Vere Hotels & Resorts



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 now provides De Vere with granular control of application access so they can decide exactly who can connect, from what device, and what level of access they are permitted. This makes network access for third party suppliers very easy to configure, control and monitor. Suppliers now have single point of access from which they can connect to the appropriate systems on the network. In addition, the AppGate server's ability to tunnel any protocol means they can use remote desktop (RDP), desktop sharing (VNC), file transfer (FTP) and web based protocols to perform remote diagnostics, maintenance and upgrades quickly and efficiently.

To support De Vere's own personnel working remotely, AppGate's Personal Firewall was installed on all corporate laptops. Centrally managed policies and rule-sets ensure that acceptable usage policies are maintained when the laptops are used outside the office, and the 'Client Check' functionality also ensures that they have and are running the latest anti-virus update before any connection is allowed.

Since the AppGate solution was installed, its flexibility and rich functionality has made it easy for new applications to be integrated. When De Vere deployed Cisco's VoIP solution, it was straightforward for Network Defence to integrate it with the AppGate solution and use the AppGate Security Server to secure all VoIP traffic. This installation of VoIP through the application layer VPN was one of the first successfully deployed in the country, and De Vere's IT support team can now take advantage of IP telephony to provide full help-desk support irrespective of where they are working.

Future

The team is planning to equip managers with mobile devices such as PDA's, reducing costs incurred through dial-up connection by providing access to the corporate network through wireless hotspots that are being installed in many of the hotels. In addition, they are looking at leveraging the ability of the AppGate solution to integrate with Microsoft Active Directory to enable all staff to access their corporate email securely over the Internet.

Tips and Tricks

The AppGate solution is well equipped to secure IP telephony traffic for enterprise use.

The IP tunnelling driver gives full bi-directional support for TCP which is used for session setup, and for UDP which is used for voice (rtp) traffic.

The client software allows more than one host to connect to the secure tunnel enabling a soft phone to connect as a separate host with its own MAC address.

The voice traffic routes directly from peer to peer. So for users connected to the AppGate Security Server the voice traffic from their soft phones is secured back to the server. Because the Security Server issues its own set of IP addresses to the IP tunnelling drivers, the users' voice traffic is routed locally and the unsecured traffic is never exposed on the internal LAN. These two factors together guarantee end to end security.

