

Large Telecommunications Company

Industry: **Telecommunications**
Application: **Securing WLAN Campus**
Product: **Array SPX**

Challenges

- Provide a unique access point for guests and employees
- Consolidate guest and employee access while staying in compliance with internal security policies
- Allow guests to use IPSec clients when required to connect to their home offices
- Provide employees with a similar end-user experience to the one they have now

Solution

- Virtualization - Providing a unique access point for guests and employees
- Network separation (Virtual Routing and VLAN support)
- Support for IPSec over L3
- L3 standalone client

Results

- Allows for the integration of any APs in the wireless network, regardless of their security capabilities
- The ability to use different wireless cards
- Easy to set up, deploy, and maintain
- Increased productivity as employees are able to remotely access company information and applications
- Convenient access from wireless networks and PDAs
- Increased security and superior reliability for Vodafone's remote access system

The world's leading mobile telecommunications company picks Array for its WLAN campus secure access solution.

The Company provides an extensive range of mobile telecommunications services, including voice and data communications, and is the world's largest mobile telecommunications company, with a significant presence in Continental Europe, the United Kingdom, the United States and the Far East through the Company's subsidiary undertakings, associated undertakings and investments.

As of December 2004, based on the registered customers of mobile telecommunications ventures in which it had ownership interests at that date, the Company had approximately 151.8 million customers, excluding paging customers, calculated on a proportionate basis in accordance with the Company's percentage interest in these ventures.

The Issue

The Company offers wireless access to employees (VF corporate network) and guests (Internet) via two separate networks. The employee network uses L2 security provided by CISCO's LEAP solution and in the past has been exposed several times as well as causing complete dependency on the AP. The Company quickly realized the need to move away from that dependency without compromising security.

The Company was also looking to consolidate the security mechanism for guest access with employee access. However in order for this type of consolidation to pass through their security policy there had to be a way to completely isolate one network from the other.

Requirements:

- Provide a unique access point for guests and employees.
- Consolidate guest and employee access while staying in compliance with their internal security policies.
- Allow guests to use IPSec clients when required to connect to their own home offices.
- Provide employees with a similar enduser experience to the one they have now.

The Array Solution

The Company deployed an Array SPX5000 cluster behind the Access Points. Utilizing the SPX and Access Points support for VLAN, separate networks are defined for employees, guests and management purposes. This provides the required separation on the unsecured side of the network. Utilizing VLANs on the inside interfaces in combination with Virtual Routing provides all the necessary separation on the secured side.

The solution allows employees to utilize the L3 standalone client, which maintains a similar end-user experience to the one they currently have. Guests use the standard web interface which is integrated with a "Scratch Card" system that is already in place.

The Array Solution

Architecture

To secure a wireless deployment the Array SPX is placed behind the Wireless Access Points, separating the secured network from the AP's network.

The Array SPX meets the two major needs for secured wireless access, authentication so that only authorized users can access secured resources and encryption so that data cannot be "hijacked" from the air. Therefore, with this architecture all security features on the APs can be disabled.

Virtual Portals

The Array SPX may be configured with one or more virtual portals depend on the number of different communities that will utilize the wireless access. Virtual portals may be configured for different departments or even for guest access.

Browser Access Vs Client Access

Users may access the Array SPX services through their web browsers; however wireless access usually requires just full L3 access. In order to provide for a more seamless user experience, Array offers a standalone L3 client; this client can be pre-installed and pre-configured by users so that a single click will allow for wireless connectivity. The client can also be by common utilities that are used to identify whenever a PC is disconnected from a wired network.

Guest Access

One of the advantages offered by using the Array SPX to secure WiFi communication is the ability to provide both network access (to the corporate network) and Internet access using the same APs.

Regular employee access usually requires access to the corporate network, and through the corporate network employees may access the Internet. Guest access on the other hand should not under any circumstances allow for access to the corporate network, and should provide direct connection to the Internet.

The Array SPX allows for the implementation of such access modes using the same set of APs. On the front-end, different virtual portals are configured for guest and employee access. On the backend, virtual routing is used to assure that guests access the Internet directly without passing through the corporate network. The following diagram shows a typical Array SPX based wireless deployment for both employees and guests.

In conclusion, utilizing the Array SPX for securing WiFi access presents several benefits. It allows for the integration of any APs in the wireless network, regardless of their security capabilities. It also allows for the use of different wireless cards; although wireless security standards were recently accepted, different vendors still have major interoperability issues.

Winning Factors

- Virtualization - Providing a unique access point for guests and employees.
- Network Separation (mainly Virtual Routing and VLAN support) - Without these capabilities it would have not been possible to consolidate guest and employee access while staying in compliance with their internal security policies.
- Support for IPSec over L3 allowing guests to use IPSec clients when required to connect to their own home offices.
- L3 Standalone client - Providing employees with a similar end-user experience to the one they have now.

