

ScanSource Europe organises WLAN Gaming Party to prove strength of Motorola AirDefense

The WLAN Gaming Party, held in Brussels in October, attracted over 80 enthusiastic gamers from Belgium, France and the Netherlands. They played a variety of state-of-the-art games in a wireless network built up with Motorola's wireless solutions. Simultaneously, a group of international hackers attempted to take down the WLAN. ScanSource suggested this initiative to Motorola in order to challenge the rich performance and security specifications of Motorola's AirDefense Enterprise Wireless Intrusion Prevention System, RFS6000 Wireless Switch and AP7131 Access Point. "These Motorola wireless products are designed to stop any form of intrusion," said Phil Boyd, partner services director at ScanSource Europe. "If we are recommending these products to our customers to ensure 100 per cent

A 60-hour non-stop WLAN Gaming Party, organised by ScanSource Europe and Motorola Enterprise Mobility Solutions, threw up some interesting challenges to Motorola's AirDefense Enterprise Wireless Intrusion Prevention System.

security, then we wanted to give them the most intensive testing possible."

The event was supported by 15 backroom staff from ScanSource and Motorola. Food and drinks were provided throughout the event (burgers, chips, pizza, and even croissants in the mornings, with plenty of coffee for the nocturnal gamers). All the participants stayed, played and slept on site for the whole 60 hours. Around 100 computers were attached to the network, from high-spec quad core CPUs to more standard PCs. Everyone was offered wireless or wired connection to the network. At the beginning all participants were on wireless;

Connection to the network was via a USB WiFi 'n' adaptor. Registration and connection to the network proceeded smoothly, taking only 5 to 10 minutes per person. The games were organised into tournaments, with an IBM server running the gaming servers for the different games, which included Counter-Strike, Quake 3, UT, Wii (Mario Kart), PS3 (FIFA 2010), Poker and Trackmania. The event was sponsored by 16 companies who offered a range of prizes for the winning teams, including a Netbook PC, headsets, memory sets, memory coolers and keyboards.

Intensive real-life environment

by the end of the event over half of them had preferred to stay on the wireless network despite the possibility to switch to cable.

"The WLAN event provided an intensive real-life environment to thoroughly test our network skills and hardware," said Boyd. "Testing the WiFi with so many operating systems and users who wanted to be able to utilise the network 24 hours per day created a variety of challenges. >>



At the WLAN Gaming Party, over 80 enthusiastic gamers from Belgium, France and the Netherlands played a variety of state-of-the-art games in a wireless network built up with Motorola's wireless solutions.

<< However, our support team met them all head on and delivered a highly successful event. We achieved all the goals we set and obtained large amounts of technical data which are still being analysed.” Some of these challenges were associated with the different operating systems of the gamers. Windows XP, Windows Vista and Linux were the most common, but one gamer was already running the new Windows 7, and some were still using Win2000. In addition, some gamers didn't have a USB 2.0 interface, so a compatible USB key had to be provided.

Other issues were linked to the network infrastructure. The clients were installed using the latest driver available on the FTP. There was a latency issue (2000-3000 ms ping every minute) that came back on all Windows operating systems, although different solutions were found for each of them. WLAN optimiser and script were made available on the intranet, but the absence of a procedure



on how to install, configure and use these led to certain difficulties. At the beginning of the event, there was some instability with the mesh network and the nine Access Points, so the Motorola team had to reconfigure the entire wireless network.

As to the security of the network, none of the hackers succeeded in breaching the Motorola AirDefense Enterprise Wireless Intrusion Prevention System. “We were delighted but not surprised

to see our products come through this tough examination,” said Patrick Groot Nuelend, product marketing manager EMEA at Motorola. “With IT systems holding and transmitting more and more sensitive information, it was absolutely essential that we clearly demonstrated that serious hackers are unable to intrude our wireless networks. We did this, and gained significant feedback that will enable us to further enhance our products in the future.” ●

FURTHER PRODUCT INFORMATION

Motorola's AirDefense Enterprise Wireless Intrusion Prevention System is designed to provide complete protection against wireless threats, policy compliance monitoring, robust performance monitoring and troubleshooting, and location tracking in an appliance that can scale to meet the needs of the largest global organisations. AirDefense uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g/n) wireless traffic in real time for the highest level of security, rogue mitigation and policy enforcement. With a real-time view of all WLAN traffic, AirDefense Enterprise also enables network administrators to remotely troubleshoot problems, identify and respond to network mis-configurations, and monitor network availability. AirDefense Enterprise provides tools to proactively monitor WLAN network performance, investigate problem areas and troubleshoot connectivity issues remotely. Remote troubleshooting improves wireless availability, reduces downtime and drastically reduces expensive site visits.

The RFS6000 Wireless Switch provides an integrated wireless LAN communication platform that enables the delivery of highly secure mobile voice and data services inside and outside the enterprise. Designed for medium to large enterprises, the RFS6000 simplifies and reduces the cost associated with converged solutions through a comprehensive feature set that delivers the best in class performance, security, scalability and manageability required to meet the needs of the most demanding mission critical business applications.

The AP-7131 Access Point delivers the throughput, coverage and resiliency required to build an all wireless enterprise. The tri-radio modular design provides support for high-speed wireless voice and data services, mesh networking and non-data applications such as Intrusion Prevention Systems. The fully DFS compliant 802.11n AP-7131 offers speeds up to 600 Mbps (per AP), six times the bandwidth of an 802.11a/g access point. An AP-7131 can function as either as a stand-alone access point or as a wireless switch adopted access point for centralised management.