BQ

European tech company deploys Cisco Meraki wireless, security, and switching for unified management of distributed locations

- Leading European tech company with 1,200 employees & offices in Europe and Asia
- Cloud-based Dashboard provides centralised management of distributed locations
- Offices connected and sharing resources using self-healing Site-to-Site VPN

BQ is a leading European technology company. Smartphones, tablets, 3D printers and PrintBots are a few of their products. With offices in Europe and Asia, over 1,200 employees, and a product presence in over 50 countries, BQ's vision is to create and distribute technology that educates, inspires, open doors, breaks down barriers, and is accessible for everyone. BQ also considers itself to be an educational company, dedicated to helping people understand technology, encouraging its use, and inspiring others to create it.

With BQ's philosophy revolving around a commitment to education in technology, the Do-It-Yourself philosophy, and the Open Source Initiative, Director of IT Mario Fernández wanted a powerful network infrastructure which reflected these ideals and would support the company's on-going global initiatives. "We realised it was necessary for all teams to be connected on a single network and to manage them from a single location. In an increasingly international company, we needed a high level of flexibility and the capacity for customisation."

BQ chose Cisco Meraki as the ideal solution for optimising the management of its entire network, enabling them to configure the network easily and tailor it to their needs. According to Mario Fernández, "getting new BQ offices up and running is now extremely easy thanks to Meraki. Centralised cloud management enables us to control our entire network from a single panel, without having to develop a system ourselves. It has already been done, so all we have to do is use it".

Using the centralised dashboard for unified management, BQ deployed Meraki Security Appliances, Switches, and Access Points to their various locations. Without having to be on-site, the IT team can manage each of the remote locations via the dashboard, have visibility into network usage, and implement changes as needed.

Using the automatic site-to-site VPN built-into the MX Security Appliances, Mario is able to connect each of the separate locations together. He can even link pre-existing, non-Meraki VPN peers into the same network, thereby making the sharing of resources between sites seamless. The self-healing nature of the VPN connections on the MX devices means they will stay updated in dynamic IP environments. Additionally, BQ is using the traffic shaping and per-client bandwidth limits to regulate how the network is being used, enabling fair network usage amongst all of its employees.

To ensure the security of the network, Mario has implemented a series of security measures, including malware detection, intrusion detection and prevention powered by Sourcefire's SNORT technology, and even content filtering. Each of these features is easily enabled with the simple click of a button or by selecting categories to block, like adult content, phishing, and hacking. Aside from preventing access to certain content, the MX can prioritise certain types of mission-critical traffic and even pair VLAN routing with more granular group policies. These group policies are designed to provide more customised settings for particular users, devices, and even traffic types.

The Meraki Layer 2 and Layer 3 access switches provide BQ with per-port customisation depending on the individual needs of each locations. Access policies can be enabled on each port which requires users to enter their 802.1X credentials for wired access. Due to the unified dashboard, Mario and the IT team can seamlessly move through the dashboard, clicking into each port and identifying the device or Meraki access point connected, providing greater insight into how each network is used throughout the greater organisation.

"Monitoring the use of broadband in each network enables us to act rapidly to prevent any loss of service. In a matter of clicks, we can block a user, apply a content filtering policy, and limit the broadband for different applications."

– Mario Fernández, Director of IT

From the network core to the end user devices, the IT team can have complete control. Whether employee, guest, or vendor, users are routed to one of 15 SSIDs per network that has been completely customised for their group. Mario has then defined per-device bandwidth restrictions, Layer 7 firewall limitations, and traffic shaping rules tailored to the company's requirements. One of the greatest benefits of the Meraki solution is that all of these configurations require simple selections from drop-down menus or fill in the blank. The IT team does not need additional training nor do they need to utilise complex command line to achieve their results.

BQ is in full expansion, which means opening new offices. Thanks to Meraki, BQ can expand its network without any problems and can

continue to manage each of the distributed sites from one location. This centralisation allows for greater efficiency and effectiveness, as well as enabling each of the various offices to share information quickly and securely.

Director of IT Mario Fernández explains, "the security policies can be used as templates and tailored to each network. On adding a new device to that network, it is instantly configured". The Meraki interface is highly detailed and intuitive, and includes tools for supervision, remote diagnostics, and detection of potential incidents, all of which enables BQ to detect any issues with ease. Together with its Anti-malware system, this guarantees the security of BQ's activities and protects against external threats. "Monitoring the use of broadband in each network enables us to act rapidly to prevent any loss of service. In a matter of clicks, we can block a user, apply a content filtering policy, and limit the broadband for different applications," Mario concludes.