



## **PRESS RELEASE**

19<sup>th</sup> August 2019

### **barox introduce 'Smart Sticky' Enterprise-class network security**

barox Kommunikation AG, the manufacturer of IT switches designed specifically for the demands of video networks, has introduced 'Smart Sticky' MAC & IP address Enterprise-class network security.

Supporting built-in Cyber security on all barox RY-switches, barox powerful Smart Sticky MAC & IP address learning adds an additional layer of high security.

An easy automatic process via the barox DMS GUI, once configured, barox Smart Sticky learns the dynamic MAC addresses of all connected ports/devices and VLANS, turning them into secure MAC addresses, adding each secure MAC address to the running configuration, and freezing them and their associated IP addresses – making them, 'Sticky'.

Whilst traditional device protection via MAC filtering alone offers simple protection against unwanted network access, it does not, for example, protect against a widespread attack of 'MAC spoofing'. Smart Sticky with its combined MAC and IP address protection provides advanced port and network security with Limit Control settings.

#### **Port security with Limit Control settings**

By learning the Mac and IP address of each and every port, it is not possible for a port to be hijacked. This prevents an 'unknown' device being able to access the network to attack the system for spoofing/phishing, preventing it from being used for malicious attacks. Only devices with a known MAC and IP address will operate on the network.

If non-managed switches are connected to terminal devices at the barox switch, Limit Control can be used to block free IP/Ethernet terminals, and prevent access to the network ports of those non-managed switches.

“barox Smart Sticky provides a very high level of Cyber and physical network protection for use within a wide variety of applications,” says Rudolf Rohr, barox Co-founder & Managing partner. “This is particularly the case where outdoor networks like car parks, would leave devices such as cameras open to threat, where they could be unplugged, and a rogue device plugged in.

“On activation, the barox Smart Sticky function is able to learn the entire MAC and IP address configuration of all ports on a network. In addition, limits can be set to make sure that any unused ports are blocked, to prevent their use and access to the system, whilst active ports are fully protected against unauthorised usage too. Switch rules can also be set to govern specific port IN/OUT TCP streaming, and a White/Blacklist set-up. And furthermore, any changes to network/device configurations need to be authorised to take effect.”

- Ends -

For further information, please contact:

Rudolf Rohr  
Co-founder & Managing partner  
barox Kommunikation AG  
Tel: +41 56 210 4520  
Email: rohr.rudolf@barox.ch

Graeme Powell  
Director of PR & marketing services  
GPM Ltd  
Tel: +44 (0)1765 608851  
Email: graemepowell@gpm.org.uk