Barracuda CloudGen Firewall and macmon

Cloud-generation security with advanced endpoint security and extended network access control (NAC)

Advanced Threat Protection & sandboxing

Barracuda Advanced Threat Protection (BATP) is an integrated cloud-based service available on Barracuda CloudGen Firewall that augments the URL Filter, IPS, and regular antivirus features. It combines multiple layers of threat detection with machine-learning techniques and a sandbox-based detonation of any file that is not conclusively analyzed by the preceding layers. Although the cloud-based service is the fastest in the industry, delays in downloads of a minute are sometimes unacceptable, so customers may opt for the "Deliver first, then scan" functionality that passes the file to the client instantly before the final verdict. In the unlikely case that a download turns out to be malicious, the information is automatically passed to macmon NAC for instant network segregation of the client machine that is now likely infected.

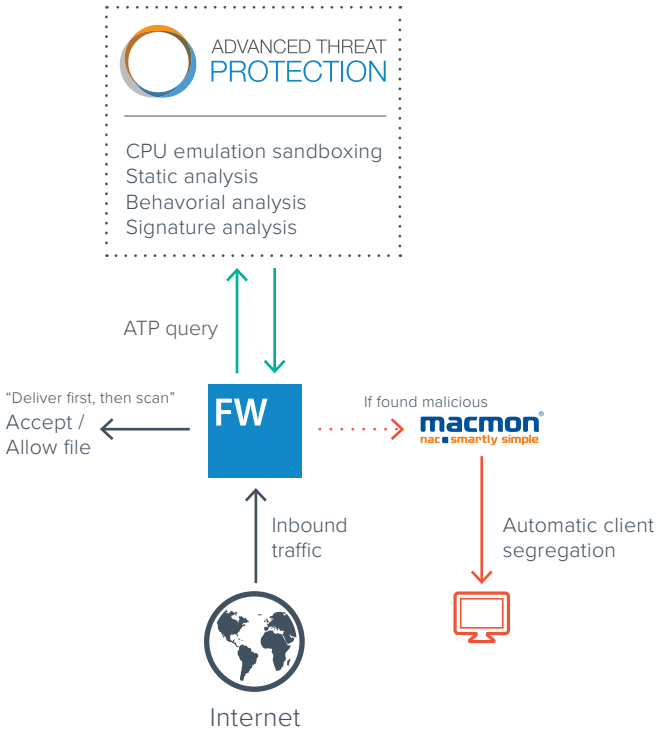

Figure 1 - Advanced Threat Protection with macmon integration

Botnet & spyware detection

As a result of extending protection across multiple threat vectors, BATP leverages a powerful global threat intelligence network that ingests vast amounts of diverse threat information from over 50 million deployed collection points around the world.

BATP therefore has one of the world's most complete information sets of command and control servers for botnets, ransomware, and spyware.

In case Barracuda CloudGen Firewall detects a client device talking to one of these botnet or spyware command servers, the endpoint device can be considered compromised. This information is conveyed automatically to macmon NAC for instantaneous network segregation and alerting.

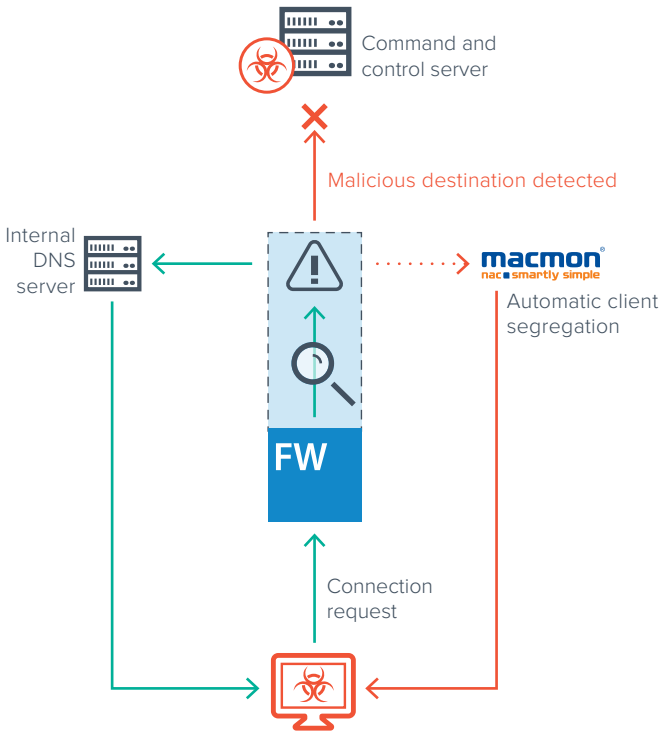

Figure 2 - Bot & spyware protection with macmon integration

Automatic group-based security enforcement

macmon NAC reports detected or changed endpoint devices to Barracuda CloudGen Firewall for automatic security enforcement. With macmon NAC, communication policies between devices are based on both network segments and group membership. Security group membership is updated automatically by the macmon NAC device detection, resulting in a policy that is always up to date. This also applies to guest and BYOD devices. The integration ensures that only macmon NAC-authorized devices are allowed to access the internet or dedicated internal resources, to enforce even more stringent security levels, or to adjust available bandwidth by application. In this way, for example, mobile guest devices may be permitted to download a firmware update, but the download speed is adjusted for background downloads so consumed bandwidth does not affect production applications.

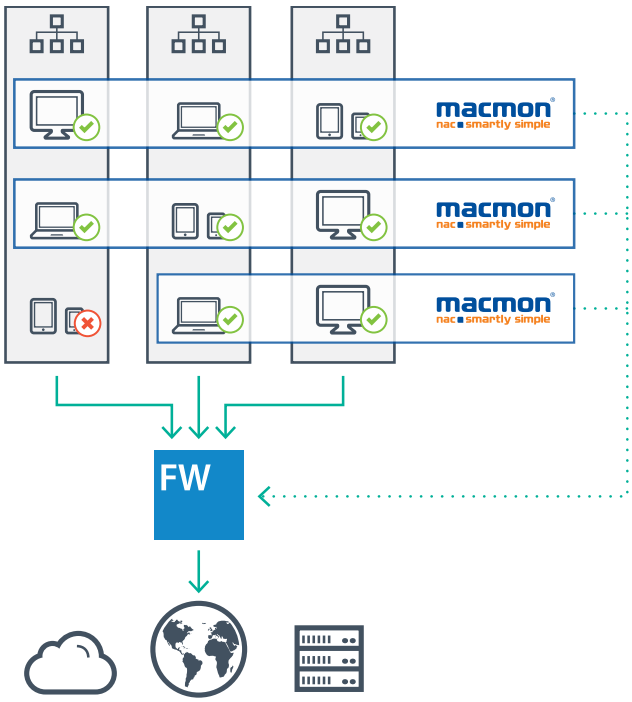

Figure 3 - Automatic group-based security enforcement

Device discovery and network visibility

Barracuda CloudGen Firewall and macmon actively exchange both IP and MAC addresses and topology information to regain network status and device visibility even across complicated networks or multiple DMZs. This makes the graphical topology display the ideal choice for regaining detailed control of networks. Graphical filtering of device properties allows for the easy detection of configuration errors. For example, all switches that recognize a specific VLAN are simply highlighted and selected – at the same time, devices that are not (yet) can be easily determined.

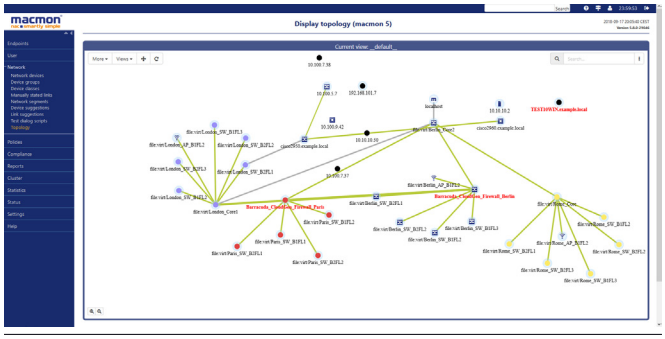

Figure 4 - macmon's graphical display topology

Requirements

Integration requires Barracuda CloudGen Firewall release 7.2.3 or later and macmon Premium Bundle.

More information

Barracuda Campus:
https://campus.barracuda.com/doc/73718914/

macmon secure GmbH:
https://www.macmon.eu

Barracuda
Your journey, secured.

macmon®
nac smartly simple

Offering every company a flexible and efficient NAC solution which can be implemented with minimal effort, adding considerable surplus value for network security. macmon secure is a member of the Trusted Computing Group and actively involved in related research projects.

For additional information, please visit www.macmon.eu.