Revolutionary Protection for Company Intranets

Maintaining data protection is one of the greatest challenges companies are facing today, because no one wants to risk a bad image due to media reports of data having been stolen from the company. Yet companies are still concentrating on protecting themselves from access from outside the company, although statistics have repeatedly shown that a large part of the spying is taking place from within the local network. This is where a maximum of protection is needed that can be implemented with only a minimum of effort and without interrupting internal workflows.

Network Access Control (NAC) solutions support the company in this task. The ARP-GUARD solution, in particular, can be implemented easily and quickly because it requires no changes to existing network structures. It learns on its own which devices are on the network, and produces a graphic overview of the network including all existing switches and routers.

By simply defining an appropriate set of rules, the company can implement its own network security policy easily, flexibly and clearly. Together with VLAN management, it is possible to clearly represent and enforce a group management and assignment system. Automatically generated notifications of a diversity of events keep the administrator always informed of network activities and possible security breaches.

Altogether, this ensures that the internal network is protected against unintentional or undesirable access and against layer 2 attacks.

ARP-GUARD Features:

- Network Access Control
- MAC address, 802.1X and RADIUS authentication
- Inventorying
- Graphical topological representation to aid visualization
- Central administration of multiple sites
- Independence of switch manufacturers
- VLAN management
- No client installation
- IPv6 support
- RADIUS server
- Individual reporting
- Ticket system for guests with self registration
- DHCP monitoring

ARP-GUARD Add-Ons:

- Endpoint
- Captive Portal
- Cluster

ARP-GUARD available as:

- Appliance
- Virtual Appliance
- Software
  - Linux
  - Windows (Sensor)

ARP-GUARD’s architecture is designed such that it can be used by small, medium-sized as well as large companies. Regardless of the company’s size or what its needs are, there is only one management level from which ARP-GUARD is centrally configured and operated. Depending on need, sensors can also be implemented for load balancing or for managing external areas.

This makes the product highly scalable, which enables it to be used to protect large corporations, to balance loads or to guarantee highest availability by using clusters.
RADIUS Server
ARP-GUARD can also rely on its proven architecture for RADIUS applications. The sensor serves as a RADIUS cache and dispatch, and can thus ensure high availability. Moreover, ARP-GUARD also contains a fully implemented RADIUS server that works specifically with the various EAP protocols and thus supports 802.1X.

Endpoint Security
The ARP-GUARD Endpoint add-on uses the WMI protocol, among other methods, to determine the current security status of a Windows client. Further possibilities include evaluating traps, and monitoring the communication between the AV server and the client. In no case is it necessary to install software on the end device.

Captive Portal
The Captive Portal add-on lets you control network access for guest or external components, such as smartphones and notebooks, both in your LAN and WLAN. Using a set of dynamic firewall rules, you can control access at all times, and limit it to what is absolutely necessary.

High Availability
ARP-GUARD provides the possibility to set up layer 2 or layer 3 clusters. Even mixed configurations of virtual appliances and physical appliances are no problem at all.

Fingerprinting
The development of fingerprinting function for ARP-GUARD initially searches for keys/certificates on the end devices, and then saves these as reference values in its database. If the identical device is again active on the network, a public key or certificate is again downloaded from the end device and compared with the reference value. If they do not agree, the device can be taken out of the network.

<table>
<thead>
<tr>
<th>ARP-GUARD</th>
<th>ACCESS</th>
<th>ACCESS+</th>
<th>FINANCE</th>
<th>PREMIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventories</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Permissions management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual port locking/VLAN assignment</td>
<td>without VLANs</td>
<td>Yes</td>
<td>without VLANs</td>
<td>Yes</td>
</tr>
<tr>
<td>Identifying and blocking unknown devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic VLAN assignment/VLAN management</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Protection from internal attacks</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MAC-based RADIUS</td>
<td>without VLANs</td>
<td>Yes</td>
<td>without VLANs</td>
<td>Yes</td>
</tr>
<tr>
<td>RADIUS with user data/certificates</td>
<td>without VLANs</td>
<td>Yes</td>
<td>without VLANs</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphical display of topology</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Software Modules

Network Access Control (NAC)
- Central port security system
- MAC address, 802.1X and RADIUS authentication
- Ticket system for guests with self registration

VLAN management
- Both static and dynamic VLAN management
- Guest access and quarantine area for intranet protection

Layer 2 IPS
- Protection from the dangers of:
  - Man-in-the-middle-attacks
  - ARP poisoning
  - MAC flooding
  - MAC spoofing
  - IP spoofing

Network overview
- Up-to-date inventories
- List of all end devices
- Log of addresses / assignment changes
- Graphical representation of the topology