

ARP-GUARD Captive Portal Add-On

Mit dem Captive Portal Add-On haben Sie die Möglichkeit, den Netzwerkzugang von Gast- oder Fremdkomponenten wie zum Beispiel Smartphones oder Notebooks sowohl im LAN als auch im WLAN zu regeln. Dabei können Sie den Zugriff durch den Einsatz eines dynamischen Firewall-Regelwerkes jederzeit kontrollieren und auf das Nötigste einschränken. Selbst Bring Your Own Device (BYOD) ist leicht und übersichtlich mit dem Captive Portal Add-On realisierbar.



Die Funktionsweise

Das ARP-GUARD Captive Portal Add-On leitet einen unbekanntes Netzwerk-Client automatisch beim Verbinden über einen Access Point oder per Netzwerkdose auf das Captive Portal Login um. Auf dem Captive Portal Login wird eine Authentifizierung anhand von Benutzernamen und dem dazugehörigen Passwort oder per MAC-Adresse durchgeführt; dabei wird entweder auf die ARP-GUARD Datenbank oder per LDAP/LDAPS auf die AD (Active Directory) zugegriffen.

Nur wenn eine erfolgreiche Authentifizierung stattgefunden hat, gewährt der ARP-GUARD den Zugang zum Netzwerk bzw. zum Internet. Je nach Konfiguration der Richtlinien im Regelwerk des ARP-GUARD Management-Systems kann der jeweilige Netzwerk-Client den Zugriff auf bestimmte Ports, Protokolle, Dienste, einzelne Server bis hin zu Netzwerksegmenten erhalten.

Im Falle eines Besuches durch einen SAP Consultant kann dieser mit seinen vom ARP-GUARD erstellten Zugangsdaten oder durch das Erlernen der MAC-Adresse seines Clients nur den direkten Zugang auf das SAP-System erhalten. Dank der Sensor-Management Architektur geschieht dies auch standortübergreifend.

ARP-GUARD Features:

- Network Access Control
- MAC-Adresse, 802.1X, RADIUS-Authentisierung
- Inventarisierung
- Zentrale standortübergreifende Administration
- Switch-Hersteller unabhängig
- VLAN-Management
- Ohne Client-Installation
- IPv6 Support
- RADIUS-Server
- Individuelles Reporting
- Gästeticket-System mit Selbstregistrierung

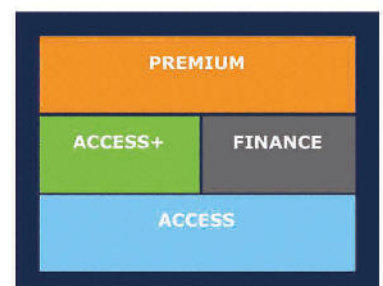
Weitere Add-Ons:

- Endpoint
- Cluster

Erhältlich als

- Appliance
- Virtuelle Appliance
- Software
 - Linux
 - Windows (nur Sensor)

Software Module

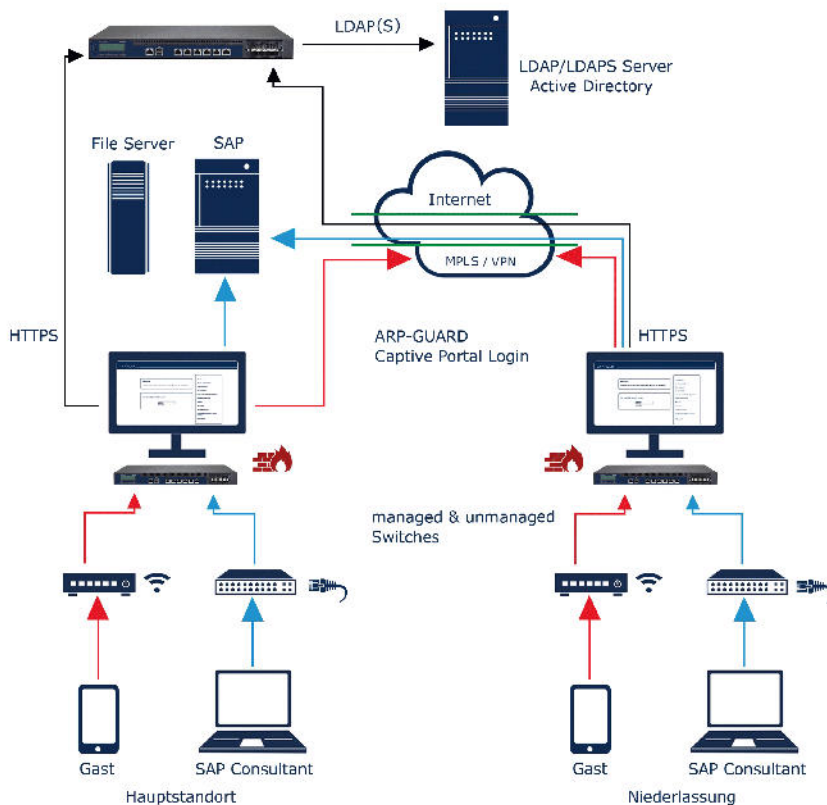


Das ARP-GUARD Management-System setzt automatisch anhand des Benutzers oder der MAC-Adresse des Clients auf dem jeweiligen Sensor die dynamischen Firewall-Regeln, so dass nur der vom Administrator vorkonfigurierte Zugriff auf das Netzwerk für diesen Benutzer oder die Benutzergruppe erfolgen kann.

Ein Mitarbeiter aus der eigenen Unternehmensgruppe, der z.B. als Besucher einer ausländischen Tochtergesellschaft im eigenen LAN willkommen ist, kann sich am Captive Portal anmelden und erhält damit per LDAP bzw. LDAPS einen Zugang zum Netzwerk, ohne dass administrative Aufwendungen erforderlich werden.

Auch BYOD lässt sich mit dieser Technologie realisieren, da private Endgeräte über das Firewall-System nur auf solche Ressourcen zugreifen, die explizit für diesen Fall freigegeben worden sind. Das Captive Portal ist zu allen Modulen erhältlich und wird nach gleichzeitig angemeldeten (concurrent) Benutzern lizenziert.

ARP-GUARD Management-System



Funktionsumfang

- Gäste-Accounts erstellen
- Berechtigung über Rollensystem/Regelwerk
- RADIUS-Authentifizierung anhand von Gäste-Accounts
- Gäste-Tickets erstellen per E-Mail/Ausdruck
- Login mit zusätzlicher PIN-Eingabe
- Selbstregistrierung der E-Mail oder SMS
- Anzahl der MACs pro Gast/ E-Mail Domain begrenzen
- Portal Login mit LDAP/LDAPS
- Automatischer VLAN-Wechsel (Gäste-VLAN)
- MAC Adressen lernen
- Eigenes Portal-Design
- Voucher (Zeitraumbegrenzung)
- Überprüfung eigener AGB's
- LAN
- WLAN
- Serien-Tickets erstellen (Vordruck)
- Konfiguration von Server und Portal über GUI
- Gezielter & beschränkter Netzwerkzugang (Netzwerksegmente, Server, Protokolle, Dienste etc.)
- Automatische Umleitung auf das Portal
- MAC Authentifizierung (unmanaged Switches)
- Verteilte Sensor-Management Architektur
- BYOD für LAN und WLAN
- DHCP Server oder DHCP Relay
- Anpassung an vorhandene Routing Struktur
- Verteilte dynamische Firewall