SPECIFICATIONS

Virtualisation platforms
Virtual appliances are supported on
- VMware
- Microsoft Hyper-V
- KVM

Supported operating systems
- Linux, Red Hat
- DOMOS
- CentOS
- Microsoft (Sensors)

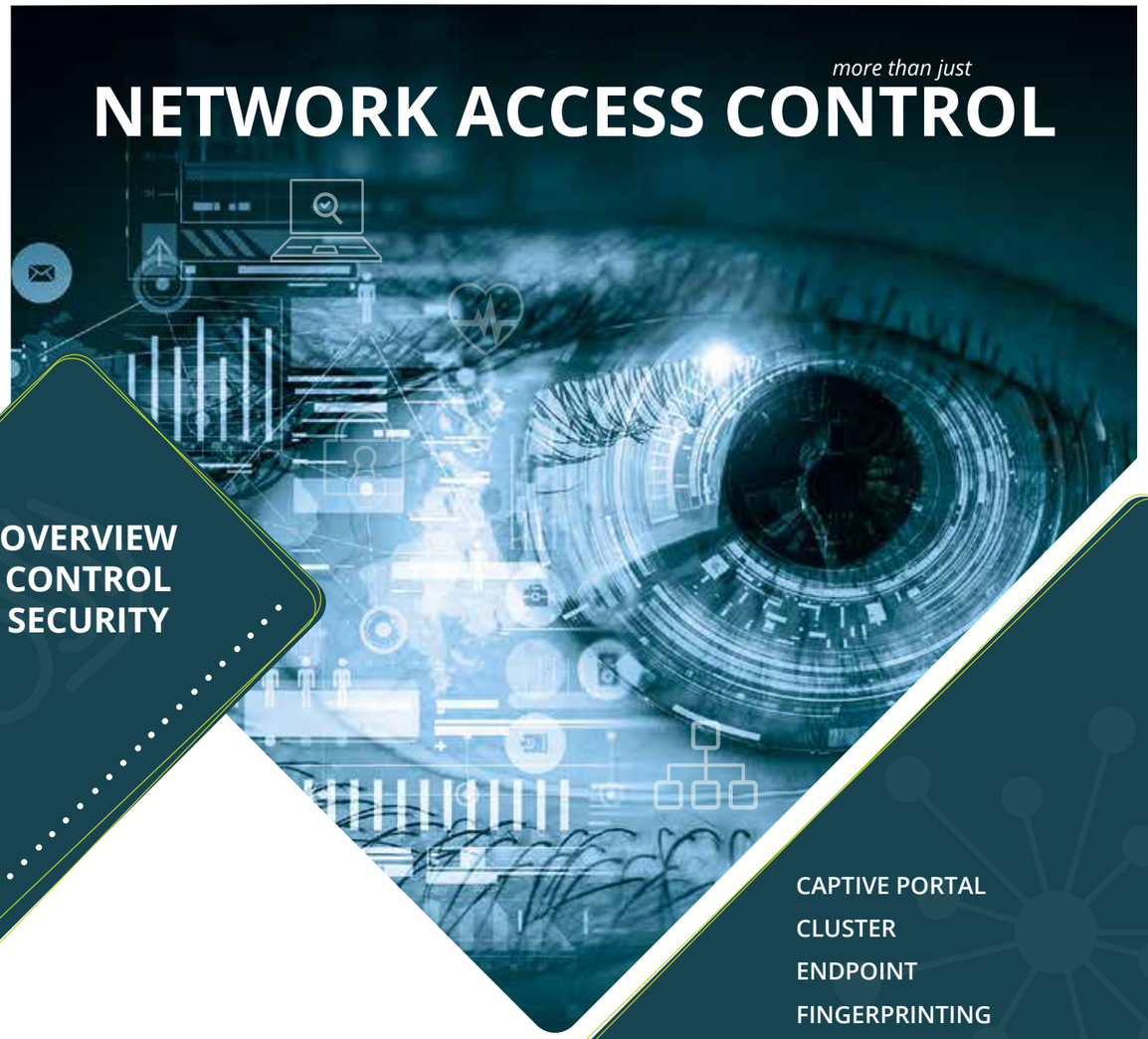
Authentication methods
- MAC-based RADIUS
- EAP
- SNMP
- 802.1X

Protocols
- RADIUS
- SNMP
- SSH
- Telnet
- DHCP
- LDAP
- HTTPS
- Kerberos
- WMI

Supported browsers
- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Internet Explorer
- Microsoft Edge

ISL Internet Sicherheitslösungen GmbH Alte Wittener Str. 70 44803 Bochum +49 234 976672-0 www.arp-guard.com

ARP GUARD by ISL



OVERVIEW
CONTROL
SECURITY

CAPTIVE PORTAL
CLUSTER
ENDPOINT
FINGERPRINTING
DEVICE DETECTION
SENSOR MANAGEMENT SYSTEM
VLAN MANAGER
ACCESS PROTECTION

ARP-GUARD is our established Network Access Control (NAC) solution, which – unlike complex and costly network applications – can also be easily implemented in heterogeneous and large networks. Access protection quickly and clearly identifies known and unknown devices regardless of manufacturers or technologies, before they are granted access to the network. In addition to standard access protection, the solution also acts as a central instance that bundles security-related information, recognises and reports anomalies in the network and remedies them immediately.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

THE ARP-GUARD SOLUTION IN DETAIL

DEVICE DETECTION AND INVENTORY

ARP-GUARD communicates with the entire network infrastructure and quickly registers all systems in the network. Every end device becomes visible, and sources of interference can quickly be localised and eliminated. What's more, the solution represents the entire architecture in a graphic topology. This makes network planning easier and, in particular, also provides for the transparency required by audits and reviews.

ACCESS PROTECTION

The central management and regulation of all network access allows for comprehensive control. Unknown devices are recognised and reported in real time. Once a device has been clearly identified, it is subject to the established further procedure. From immediate port shutdown to relocation to a special Virtual Local Area Network (VLAN), any desired action can be defined and managed in the rules for the entire network.

NETWORK SEGMENTATION WITH VLAN MANAGER

With VLAN management, segmentation in VLANs is easy to implement and convenient to manage. As a result, sensitive areas are additionally protected, public areas are clearly delimited from internal areas, and guests and service providers are only granted special access. Instead of manual setup on the individual switch ports, devices are automatically assigned to the associated VLAN as specified in the rules. Employees who move, travel or work in other locations always take their environment with them.

FINGERPRINTING

The combination of different authentication methods, such as MAC-based RADIUS and 802.1X, offers security and flexibility. We supplement these methods with ARP-GUARD fingerprinting, which captures various properties, such as cryptographic certificates and keys, in order to identify devices clearly and with certainty.

SENSOR MANAGEMENT ARCHITECTURE

Its special sensor management architecture makes ARP-GUARD multi-client capable and enormously scalable. The use of sensors enables the effective integration of any number of locations. Umbrella management makes it possible to manage decentralised, large network environments. Like an umbrella, a central set of rules spans the entire network – simply and automatically! Users, roles, rights and policies are synchronised, but sensors can also be used decentrally.

ARP-GUARD ADD-ONS

CAPTIVE PORTAL – GUEST ACCESS AND BYOD

The Captive Portal add-on regulates the network access of guest and third-party components like smartphones and notebooks. Targeted network access can be defined for third-party devices in any environment and controlled at any time by a dynamic firewall rule set – even across locations thanks to the sensor management architecture. Bring your own device (BYOD) is therefore easy to implement, and private devices are only given access that is explicitly approved by rules.

NETWORK INTEGRITY ON ALL END DEVICES

The ARP-GUARD endpoint feature provides valuable support for the implementation of compliance requirements. During authentication, it is checked whether end devices meet the security guidelines and comply with security-relevant details such as status, antivirus or patch level of the operating system. If a device does not meet the guidelines, it is isolated and, for example, updated in a quarantine VLAN. Devices only gain access to the network areas after they have been checked or adapted.

HIGH CLUSTER AVAILABILITY FOR SENSITIVE IT AREAS

With simple software and hardware, the cluster add-on enables server replication for increased reliability and scalability for critical IT systems.

ARP-GUARD AT A GLANCE

- Device detection and inventory
- Graphic representation of the network infrastructure
- Centralised control and monitoring of network access
- Central definition and enforcement of guidelines in real time
- Network segmentation
- LAN/WLAN network integrity down to the end devices
- Unique fingerprinting for clear device identification
- End device compliance check
- Regulation of guest access and BYOD
- Reduced IT administration effort through automation
- Independent of manufacturer and technology
- Supports ISO/IEC 27001, DIN EN 80001-1, PCI/DDS
- German-language support

YOUR ADDED VALUES

SIMPLE IMPLEMENTATION

The successful basic installation already achieves a significantly higher level of security, which can be gradually further expanded. Integration into the existing infrastructure is seamless and trouble-free, and does not require any changes or further investment.

AVAILABLE OPTIONS

ARP-GUARD management is provided both as a virtual and a physical appliance. For cluster installations, there is also the additional option of mixed operation. In addition, sensors can also be installed directly on the company's own servers.

CROSS-SECTOR STRENGTHS

ARP-GUARD is used in all domains. In addition to industry, trade, healthcare, government agencies, education and research, the solution is today indispensable especially in the financial sector, one of the most security-sensitive industries. The flexibility, architecture and functionality of ARP-GUARD make it ideal for critical infrastructures. As a matter of course, ARP-GUARD complies with the security requirements of ISO 27001, DIN EN 80001-1 and PCI/DSS, and is certified for providing IT baseline protection.

A BLEND OF METHODS FOR MORE SECURITY AND FLEXIBILITY

ARP-GUARD covers the entire range of authentication options. From the 4.0 version, the different features have matured into a perfect symbiosis that is state of the art. The licence enables mixed operation of SNMP, MAC-based RADIUS and 802.1X with the same feature set. A later migration from SNMP to 802.1X is also easily possible.

SERVICE & SUPPORT

Enjoy first-level support provided by our qualified and experienced ARP-GUARD partners.
www.arp-guard.com/kontakt/vertriebspartner

You also benefit from our comprehensive range of services spanning from software subscription (access to all minor and major releases, updates and new versions) and third-level support (manufacturer support for customer-specific optimisation and adaptation) to technical training.