

# ***NETWORK ACCESS CONTROL***

Netzwerkzugriff nur für bekannte Geräte!

Gastzugänge

VLAN-Management

MAC-based, 802.1x

Unbekannte Geräte

Captive-Portal



***NAC*** Appliance  
*network access control*

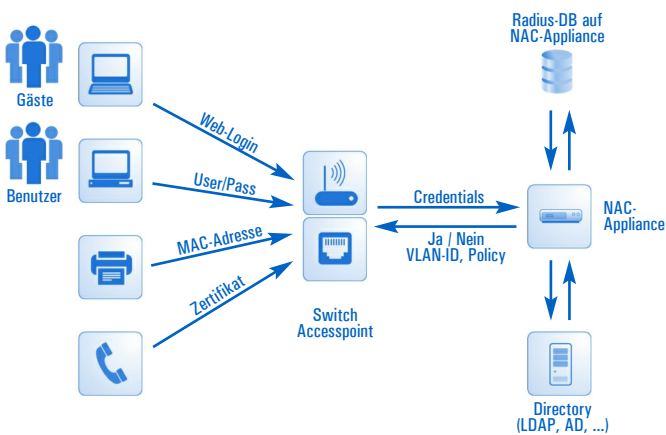


**Thomas-Krenn.AG**<sup>®</sup>  
Die Server-Experten



## EINBINDUNG VON GÄSTEN

**Gesicherter Zugriff von Gästen** – Fast jedes Unternehmen kennt die Situation, dass Gäste, Lieferanten, Dienstleister oder Kunden „schnell mal“ einen Internetzugang benötigen. Die Realisierung dieses Wunsches über das lokale Unternehmensnetzwerk birgt jedoch verständlicherweise enorme Risiken. Unsere NAC-Appliance realisiert einen sicheren und eingeschränkten Gästezugang mit Hilfe von Quarantänesegmenten und dem Captive-Portal-Modul (CaPo).



## RISIKO UNBEKANNTE GERÄTE

**Erkennen und Abwehren fremder Geräte** – Sobald ein Client mit einem lokalen Netzwerk verbunden ist greifen die meisten Sicherheitsmechanismen wie externe Firewalls, Virens Scanner oder Proxies nicht mehr. Ohne geeignete Schutzmechanismen kann somit ein infizierter oder mit böswilligen Absichten ausgestatteter Rechner problemlos im internen Firmennetzwerk agieren und beträchtliche Schäden verursachen. Daher müssen solche Geräte erkannt und am Netzwerkzugang gehindert werden. Unsere NAC-Appliances ermöglichen dies mit Hilfe von MAC- oder 802.1x-basierter Authentifizierung.



	Basismodelle			Erweiterungsmodule			
	NA-2500	NA-2500-V	NA-2500-X	MAC unlimited	802.1x unlimited	CaPo unlimited	proNetworking
Appliance	Hardware	Virtuell	Virtuell				
System/CPU	Dual-Core Atom	VMWare ab 4	Xenserver ab 5.6				
Abmessungen	19" 1U						
Ethernet Ports	2 RJ45 10/100/1000	2 V-NICs	2 V-NICs				
NAS (Switches, APs)	5	5	5	unlimited	unlimited		
MAC-based Auth	✓	✓	✓				
MAC-Supplicants	50	50	50	unlimited			
802.1x-based Auth	⊘	⊘	⊘		✓		
802.1x Supplicants	⊘	⊘	⊘		unlimited		
CaPo Instanzen	1	1	1			5	
CaPo User	25	25	25			unlimited	
CaPo Gäste	25	25	25			unlimited	
CaPo LDAP	⊘	⊘	⊘			✓	
CaPo Firewall	✓	✓	✓				
Externer Radius	⊘	⊘	⊘	✓	✓	✓	
Advanced Reporting							✓
VLAN							✓
Bonding/Teaming							✓
High-Availability							✓
Network-Debugging							✓
Loghost-Anbindung							✓

## VLAN MANAGEMENT

**Dynamische Verwaltung von Segmenten** – Für registrierte Endgeräte definieren Sie in der Oberfläche das zu diesem Client zugehörige VLAN. Nach erfolgter Authentifizierung wird das Netzwerkgerät dann automatisch diesem VLAN zugeordnet. Dynamische VLAN-Verwaltung ist in der NAC-Appliance standardmäßig bei MAC- und 802.1x-basierter Authentifizierung enthalten.

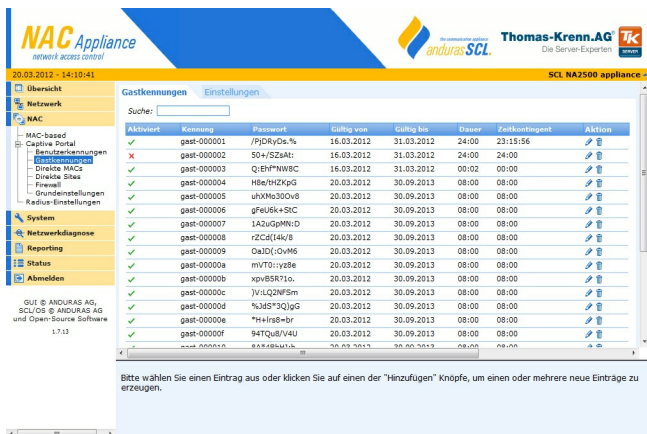
**Quarantänesegmente** – Optional können unbekannte Clients in sogenannte Gast- oder Quarantänesegmente verwiesen werden. Dort stehen dann eingeschränkte Netzdienste zur Verfügung, durch die das restliche Netzwerk nicht gefährdet wird.

# Wie ist es um unbekannte Geräte in Ihrem Unternehmensnetzwerk bestellt?

## FLEXIBLE ANBINDUNG

**Active-Directory, LDAP und Radius** – Neben der Authentifizierung gegen die lokale Radius-Datenbank ist die Einbindung von externen LDAP-Servern oder Active-Directory-Umgebungen möglich. Auch die Anbindung eines bereits vorhandenen Radius-Server ist möglich.

**Externer Syslog-Server** – Für eine zentrale Vorhaltung der Protokoll-dateien kann ein externer Syslog-Server an die NAC-Appliance ange-bunden werden.



## MOBILE GERÄTE (WLAN)

**Trend zu mobilen Geräten** – Die Anzahl an mobilen Geräte in Unternehmen steigt stetig an. Ob es sich hierbei nun um Laptops, Smartphones oder Gästerechner handelt, die Herausforderung ist immer die gleiche: Wie bindet man diese mobilen Geräte sicher in das lokale WLAN-Netz ein? Die NAC-Appliance unterstützt Sie hierbei mit den Techniken der 802.1x basierten Authentifizierung und der web-basierten Anmeldung (Captive Portal).

## MAC-BASIERTE AUTHENTIFIZIERUNG

**Erkennung registrierter MAC-Adressen** – Netzwerkgeräte werden anhand ihrer MAC-Adresse identifiziert. Der zugehörige Network Access Server (NAS), z.B. ein Switch oder AccessPoint, authentifiziert diese Geräte dann an der NAC-Appliance. Ist die MAC-Adresse bekannt und an der NAC-Appliance hinterlegt, dann erhält das Gerät Zugriff auf das Netzwerk. Optional übermittelt die NAC-Appliance auch VLAN-Informationen an den NAS. Somit können Netzwerkgeräte auch dyna-misch den gewünschten VLAN-Segmenten zugewiesen werden.

## 802.1X-BASIERTE AUTHENTIFIZIERUNG

**Anmelde- oder zertifikatbasierte Authentifizierung** – In Fällen kri-tischerer Netzwerkbereiche wie WLAN oder hochsensiblen lokalen Netzwerken bietet die Authentifizierung per MAC-Adresse keinen aus-reichenden Schutz. Hier empfiehlt sich der Einsatz einer 802.1x-basier-ten Authentifizierung. Mit Hilfe des im 802.1x Standard spezifizierten Extensible Authentication Protocol Over LAN (EAPOL) stehen verschie-dene anmelde- oder zertifikatsbasierte Authentifizierungsmöglichkeiten zur Verfügung. Ebenfalls können Netzwerkgeräte wieder dynamisch den gewünschten VLAN-Segmenten zugewiesen werden.

## CAPTIVE-PORTAL AUTHENTIFIZIERUNG

**Authentifizierung per Web-Portal** – Mit Hilfe der NAC-Appliance erhalten Sie eine automatisierte Möglichkeit Gäste in Ihrem Netzwerk zu verwalten. Ihre Gäste-Rechner gelangen sowohl per WLAN als auch per Netzkabel automatisch in ein Gastsegment. Dort werden diese dann per Weboberfläche gebeten sich am so genannten Captive-Portal anzumelden. Die zugehörigen Anmeldedaten haben Sie zuvor an der NAC-Appliance generiert oder sie werden direkt von externen Authentifizierungsdiensten wie z.B. LDAP abgefragt. Nach erfolgreicher Anmeldung stehen Ihren Gästen dann die von Ihnen freigegeben Ressourcen zur Verfügung. Sie definieren dabei gewünschte Zeitkontingente und Zugriffszeiten sowie die Beschränkung der Dienste, die Sie für Ihre Gäste vor-gesehen haben.

## VERFÜGBARE PLATTFORMEN

Hardware-Appliance



XenServer  
Virtual-Appliance

**CITRIX®**  
**XenServer**

VMWare  
Virtual-Appliance

**vmware**

**Thomas-Krenn.AG®**  
Die Server-Experten



**Thomas-Krenn.AG**  
Speltenbach-Steinäcker 1  
D-94078 Freyung  
[www.thomas-krenn.com](http://www.thomas-krenn.com)

 **anduras**  
intranet security AG

**ANDURAS AG**  
Messestraße 3  
D-94036 Passau  
[www.anduras.de](http://www.anduras.de)