LimRAD Auth Platform

Network Access Control (NAC)

NAC product carries out the activities to control and manage the access of users and computers to the corporate computer network. For this purpose, it realizes real-time identification, authorization and device health checks of the devices starting from the first access point to the corporate network during the entire working time.

The security and authorization of the users and computers at the first access to the corporate network are performed using the world standard 802.1x (AAA) technology in this regard. Policy Manager Radius server, one of our products, is used to provide this service.

Policy Manager Radius server responds to industry standards without using open source code, with a completely new architecture and coding that conforms to industrial standards, by obtaining high performance with low hardware resources in standard or hardware manufacturers attributes in networks such as wired, wireless, VPN, APN. is a new generation Radius Server.

Authentication is done from MS AD, LDAP, PostgreSQL, MySQL, MSSQL, JSON-API, Oracle or internal local user identity databases for authorization checks at the time of connecting devices to the corporate network. After authentication, Network Access Control (NAC) provides authorization info with "Role", "Downloadable-ACL", "VLAN", and / or manufacturer-specific data on the type it can support the access device.

After the devices are bought with the appropriate authorization to the corporate network, they are constantly checked for health (Device Posturing). Rules for this health check can be defined specifically for the needs and policies of the institution. These rules include whether the device is included in the domain, the current status of the anti-virus program on the device, the operating system updates, the rules about the hardware such as USB, camera installed on the device, applications or services installed on the device, registry) checks can be made regarding the presence of keys and / or their values.

In accordance with the defined rules, devices detected as unhealthy in accordance with the corporate policy can be automatically quarantined. How to apply the quarantine can be defined through the management interface.

Key Features

- Redundant Virtual Appliance architecture
- Multiple roles and service rule architecture
- Dynamic and continuous device health check
- Able to create device health rules in line with the institution's policies
- Multiple hardware manufacturer support
- Multiple database support as authentication sources.

  MS Active Directory
  LDAP
  Oracle
  MSSQL
  PostgreSQL
  MySQL
  JSON-API
- Advanced reporting features
- Consolidated Log feature, forwarding log to external syslog servers
- Supported virtualization platforms: VMware vSphere Hypervisor (ESX / ESXi), Microsoft Hyper-V, CentOS KVM and Amazon AWS

General Features

- Delivered as Hyper-V, CentOS KVM and Amazon AWS virtual image, can be installed quickly. Related settings are made on the web interface by giving the IP address with the quick setup wizard over the console.

- 802.1x, Captive Portal, MAC address authentication features

- Available health control components
    * Domain membership
    * Antivirus application status
    * OS version (version number, 64 bit control)
    * Upto date status of the operating system
    * Installed applications and versions
    * Installed services and operational states
    * Existence and values of keys in device registry
    * Existence of defined critical files

- Consolidated advanced recording feature is provided through the web interface

- Can access user verification by accessing multiple user databases simultaneously

- It has a high performance and high flexibility to meet the different demands of the institutions

- Designed to use low hardware resource and can work as a virtual server.

- Developed in accordance with international standards, has multi-manufacturer support.

- There is no hardware dependency.

- It has full control over the devices with its agent structure.

- It can transmit authentication information to integrated with external systems like firewalls. (Network SSO)

Difference Features

LimRAD Auth Platform developed from scratch without using any open source code projects.

LimRAD can work in redundant architecture and is designed to ensure business continuity. All setup and management is provided from the web portal interface instead of complex command lines.

Since network and user traffic does not pass through it, it can authenticate from the central data. With different and dynamic levels of authority, multiple management roles can be provided on a single server, depending on the level of authority.

With its flexible structure, it can collect information from different sources and automatically detect devices on the network and add them to the device database.

Can make device / user security group, organizational unit or device based network authorization.

It has low hardware resource usage with its scalable multithreading architecture.

It can provide service from the smallest businesses to large scale enterprises, distributed telecommunication service providers.

It does not allow disruption in your business continuity as it is located in the central authentication position.

It support full flexibility with creation of any number of device access rules and enforcement rules and their combinations.

With the information such as access device, time, device type, location, user name on which the access is made, users can be separated and authenticated accordingly. For example, request coming as *@company1.com can be directed to one authentication source, requests coming as *@company2.com can be directed to another one. It provides high flexibility with data regular expression matching infrastructure it uses.

With support of multiple hardware manufacturers, it eliminates your hardware brand dependencies. Can work with all industry standard manufacturers.

Up to 50,000 users can be simultaneously verified on a single virtual appliance with capacity to be increased while operating (*).

Protocol Features

- Radius AAA
- Radius CoA
- WMI
- SSH, Telnet
- SNMP
- Captive Portal (Hotspot) (**)
- EAP
- EAP MD5
- EAP GTC
- EAP PEAP
- EAP TLS (v1,0-v1,1-v1,2)
- EAP TTLS
- PAP
- MSCHAPv2, MSCHAP
- CHAP
- Windows Machine Authentication
- SMB v2/v3
- SYSLOG integration
- Certificate Authority (CA)
- Secure communication with HTTPS
- OTP Server
- SMS Gateway
- SMTP Relay

- If the necessary hardware resource and license are provided

** It is seperately licensed and the module starts working when the license is included in the system.

Supported User Information Databases

- Microsoft Active Directory
- LDAP
- Oracle
- PostgreSQL
- MSSQL
- MySQL
- Local DB
- Microsoft Azure Active Directory
- JSON API

RFC Standards

- RFC 2246
- RFC 2548
- RFC 2759
- RFC 2865
- RFC 2866
- RFC 2869
- RFC 2882
- RFC 3079
- RFC 3576
- RFC 3579
- RFC 3580
- RFC 3748
- RFC 4017
- RFC 4346
- RFC 4514
- RFC 4518
- RFC 4849
- RFC 5216
- RFC 5246
- RFC 5280
- RFC 5281
- RFC 7231

IP V6 Features

- Web and CLI based management.
- Authentication and authorization for IPv6
- Syslog, DNS, NTP, IPv6 integration

802.1x L2 AUTHENTICATION

LOCAL – GENERAL SPECIFIC NETWORKS

USER DEVICES

USER INFORMATION CORPORATE INFORMATION STORE

- MS, Active Directory
- MSSQL, MYSQL, PostgreSQL, Oracle
- LDAP
- Local

LimRAD AUTH PLATFORM

USER EVALUATION AND IMPLEMENTATION

- User access rule determination
- Establishing a service relationship
- Making user authentication
- Determining the suitability of the defined rules
- Applying the return rule set according to the appropriate rule control
- Transmission of relevant Radius Attributes to the Access Device (VLAN, Role)
- Keeping records and / or transmitting to related servers
- Keeping Account Information, keeping it associated with the user

ACCESS DEVICES

- Switch
- Wireless Access Point
- Wireless Controller
- APN server
- VPN Server
- Firewall
- Any device that supports Radius protocol

USER NETWORK ACCESS REQUEST TRANSLATED TO RADIUS STANDARD

LİMATEK SİSTEM TEKNOLOJİLERİ SANAYİ TİCARET A.Ş.
ODTU Technopolis Gallium Block No: BK12 06800 Çankaya/ANKARA
0312 287 76 73