Wireless LAN Campus

A private Michigan university uses the RAD-Series RADIUS Server to authenticate and control all users attempting to access two different networks: the offsite network through wired connections, and the inside campus network through wireless LAN connections. The university wanted a security solution that would centralize the management of all network users and record all session activity to allow departmental charge-backs.

The RAD-Series software is located at the university, and seamlessly interfaces to the local Internet service provider's Network Access Servers (NASs), authenticating all network users, and allowing the university to easily manage their user database and secure the connections.

Project Overview

The university wanted its local Internet Service Provider (ISP) to be able to access the security software through a firewall in order to send its authentication requests, and thus required that the security software be compatible with and interface to the ISP's network access servers.

The network ties to a LDAP user directory, which runs on a Linux server. The LDAP directory stores all of the users' information about access rights, session time allowances and departmental roles.

Requirements

The university needed an authentication solution with the following requirements:

Network Access Control. User authentication was needed for all people attempting to connect to the network via wireless LAN, dial-up, firewall, and tunnel/VPN access. The university wanted a standards-based solution that would work with existing equipment and databases.

Compatibility with the ISP's Hardware. Since all of the hardware equipment for the dial-in network was located offsite at the university's local ISP, solution compatibility and integration between that network and the university's on-site equipment was a major requirement. The ISP would have to access the security software through the university's firewall, to be granted authentication and access the user directory.

Easy to Use and Maintain. The IT department wanted to manage all network users via a simple, web-based interface – not through a complex command line-interface that the rotating network administrators would not know how to use.

Tight Security. With students and faculty access the network via multiple wired and wireless methods, and the ISP needing to proxy authentication requests to the authentication software to check user's credentials, security and privacy was a major concern.

Reporting Capabilities. The university wanted to figure out which departments were accessing the network most often, and for how long. Therefore, session logging capabilities were required to keep track of this activity, allowing the IT department to monitor network usage and expenses, and implement departmental charge-backs.

Solution & Implementation

The solution is Interlink Networks' RAD-Series RADIUS Server, designed specifically for those seeking an easy-to-use solution to secure their networks from unauthorized users and intruders. The RAD-Series performs three vital functions for network access control:

- **Authentication** - Validates any remote or WLAN user's username and password against a central database or directory to ensure the validity of that user's credentials

- **Authorization** - For each user, the RAD-Series provisions the appropriate policy such as IP address, session limit, or tunnel type, for what that user is authorized to do based on a wide range of criteria including point of access, time, and specific user or group credentials.

- **Accounting** - Logs all remote and WLAN connections, including user names and connection duration, for use in tracking, auditing, or billing.

The IT department installed and configured the RAD-Series software in minutes, and then worked with the ISP to direct its access requests to the software for authentication. The university set up a firewall to enhance security, and configured it to allow the ISP's authentication requests to come through in order to access the university's Linux server running the RAD-Series software.
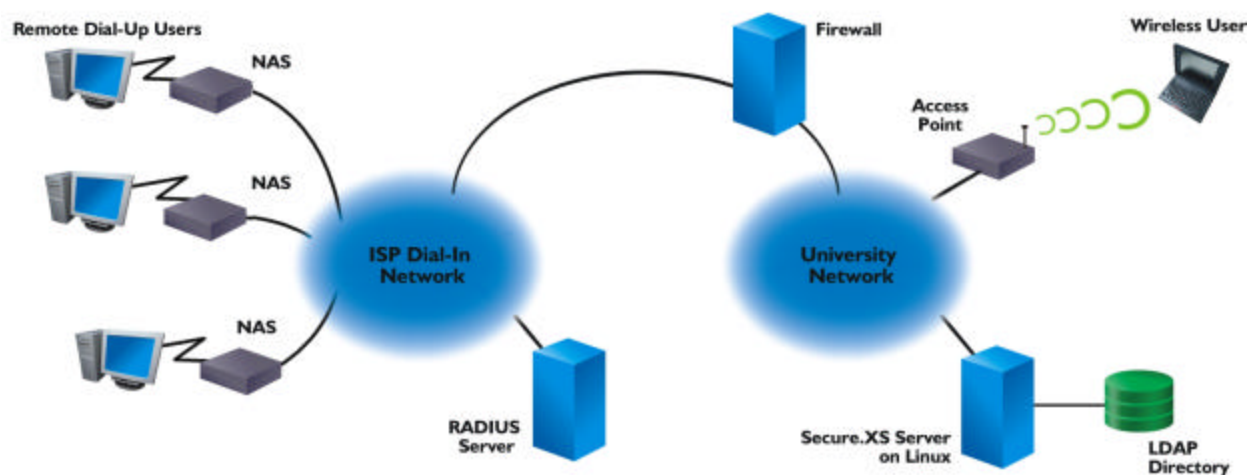
Why the RAD-Series RADIUS Server?

The university chose the RAD-Series software because of its excellent cost-to-benefit ratio, along with its ability to meet all of the requirements with the following benefits:

802.1x Strong Authentication. The RAD-Series authenticates wireless LAN users upon attempting to connect to the network by checking their credentials via strong 802.1x authentication – a Layer 2 security

method – and authorizing network and VLAN access. The RAD-Series authenticates all users, regardless of how they are connecting, simplifying and centralizing the administration. The 802.1x strong authentication also thoroughly addresses the security requirement.

Multi-Vendor Support & Compatibility. The RAD-Series is a standards-based, non-proprietary solution that is compatible with any RADIUS-based equipment such as network access servers, VPNs, firewalls, and WLAN access points and switches. There's no need to get locked into one manufacturer to ensure network security compatibility. The ISP's network access servers configured instantly to the software, and vice-versa.

Web-Based Server Administrator. Managing network users is easy with The RAD-Series' web-based graphical user interface, which allows administrators to simply set-up and maintain multiple servers from their preferred Web browser. User profiles and software operation can be configured and monitored remotely.

Event and Session Logging. The RAD-Series' built in session manager generates comprehensive activity records. It logs all network access activity, providing a security audit trail, accounting data for departmental charge-back, and important information for network diagnostics and service level management.

Graduation

The result is a combination of wired and wireless users securely accessing two separate networks, while the university's IT department can easily control these users and manage the network – including access points and databases – through the RAD-Series user interface. The university found an easy-to-use authentication solution that met all of its requirements and came in under budget.