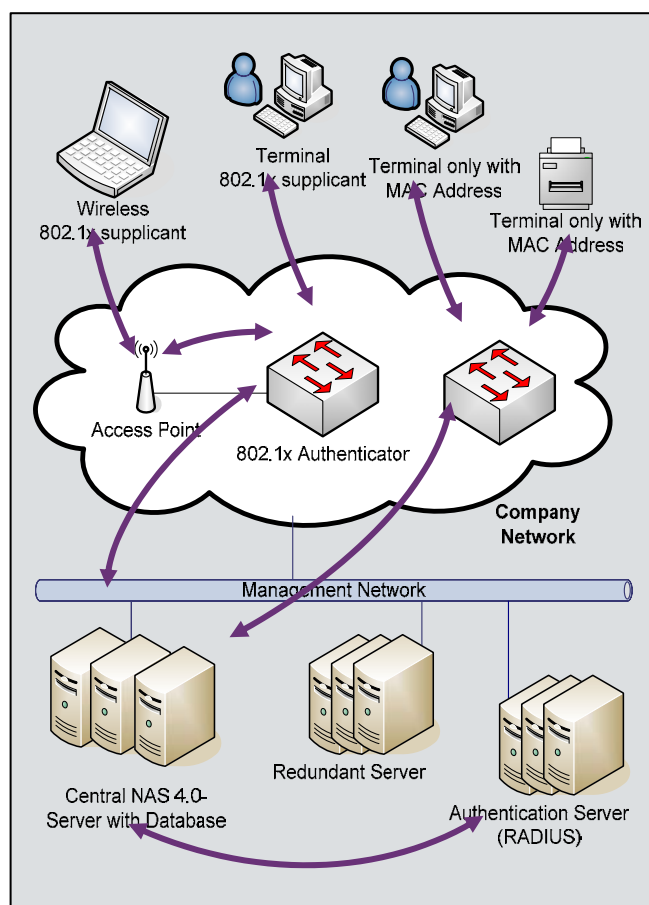




USP Network Authentication System™

Secure the Network Perimeter without compromises

Security measures inside the corporate network boundary were a perfect no-go until very recently. Especially access ports on the network access infrastructure were considered secure since they are on the company premises and are not publicly accessible. The threat from viruses, worms and other malware demands re-thinking this assumption. In meeting rooms, offices, and training facilities devices can get connected without having passed any checks and can cause considerable damage.



How the USP Network Authentication System™ works.

THE SITUATION.

The problem of unauthenticated network access is well known. Standard bodies have reacted and have defined the IEEE 802.1x standard that makes access control possible. The USP Network Authentication System™ (NAS) supports the IEEE 802.1x standard

and enables simultaneously an authentication based on the MAC hardware-address. United Security Providers' NAS is a broad solution for network access control, which supports any network device.

THE OFFER.

The USP Network Authentication System™ authenticates based on certificates over IEEE 802.1x or the MAC hardware-address every device connected to corporate network. Unknown devices are detected and blocked or moved to a quarantine or guest area automatically, based on the current policy set through the NAS GUI. Alerts on negative authentication results, i.e. on illegitimate devices are handed to your existing network monitoring solutions. Established processes are used, ensuring incidents are handled by your appropriate organizational units (e.g. Incident Response Teams). Devices in the quarantine area are offered remediation support to be able to successfully enter the production environment.

The statement of health protocol IF-TNCCS-SOH enables the gathering of additional information about devices. SOH-messages notify the NAS about the actual status of virus protection and the operating system. According to policy stored in the NAS various actions can be taken, for example moving the device into a quarantine area. The following operating systems will support SOH:

- Microsoft Windows XP SP3 (available end 2007)
- Microsoft Windows Vista



USP Network Authentication System™

THE PROJECT PLAN.

The NAS gets integrated into your environment to be monitored. For the development of the solution and processes, as well as for the integration into existing processes our well proven approach will be used.

Step 1: Information gathering

Your network, your systems and your process framework are analysed in depth, using the existing documentation. Interfaces to your (potentially existing) inventory database, to the monitoring systems (for logging and alerting) and to the network devices get specified as a part of the tetrad NAS integration framework.

Step 2: Policy and Design

The policy specifies the requirements devices have to fulfill to be permitted into the network fully authorised and how devices are treated if they do not comply with these requirements. For network ports in 'public' areas, like meeting rooms, a lower security setting can be selected. In return, access to internal IT-systems can be limited. If necessary, definitions within the directory and the Certificate Authority (CA) for the release and distribution of machine-certificates are extended. The network design is supplemented with secured segments and solutions for the redundancy of vital components such as NAS, Active Directory and RADIUS server.

Step 3: System- and Process Integration

The NAS gets set up on a testing server and is integrated into your environment. The interfaces are activated. Missing processes are defined and implemented, existing processes are adapted. In the pilot stage the NAS is run in «permissive mode», meaning only logging and alerting are activated, no ports will be blocked. Using the logged data, the complete process chain for inventorying devices not present in the database and for handling negative authentication (devices that cannot be found in the database) is tested. Once processes are established, the NAS can be switched to «restrictive mode», i.e. illegitimate devices will be cut off from the network.

Step 4: Optimization

Based on the results of Step 2 the optimization potential is analysed. Possible measures can improve the quality of the inventory data or selective configuration of your network infrastructure. Your systems and processes are adapted accordingly.

THE BENEFITS.

The NAS can be integrated quickly and at low cost into your network. The protection of your network infrastructure and of all systems using it can be improved substantially at once. By eliminating the threat of illegitimate devices connecting to the corporate intranet your operational risk is reduced drastically. Moreover, the NAS can recognize devices of a wide variety of manufacturers and can determine their physical location. Devices that do not conform to the policy for network access can be identified, blocked automatically, and removed physically. The direct link to the inventory system enforces a current and accurate inventory database.

SECURITY IS OUR BUSINESS.

In today's competitive environments, security and operational freedom are often contradictory to each other. We surmount this challenge on behalf of our customers because we consistently aim our expertise towards current and future security requirements. United Security Providers unites leading Swiss IT security specialists under a single roof, and our international network of partners assures access to our solutions for clients all over the world. This strategy guarantees true world-class service quality.

United Security Providers – protecting what matters.

Louis Oetiker

United Security Providers
Bahnhofstrasse 4 · Postfach · CH-3073 Gümligen

Fon +41 31 959 02 02 · Fax +41 31 959 02 59
louis.oetiker@united-security-providers.ch
www.united-security-providers.ch