

## Case Study: IEEE 802.1x für LAN und WLAN

### Branche

Chemische Industrie

### Projekthinhalte

In einem Industriepark LAN mit vier ansässigen Firmen und insgesamt mehr als 10.000 Nutzern wurden die Unternehmensnetze logisch getrennt. Gleichzeitig wurde eine deutliche Erhöhung der Netzwerksicherheit für LAN und WLAN insbesondere gegen unzulässigen Zugang von „innen“ durch einen effektiven Schutz der Netzwerkzugänge erreicht. Dazu wurden VLANs zur logischen Separation der Netze und IEEE 802.1x zur dynamischen Konfiguration und zur Absicherung des Zugangs über LAN und WLAN verwendet. Die vorhandenen flexiblen Unternehmensstrukturen mit mobilen Mitarbeitern werden nun durch eine hochflexible Netzwerkinfrastruktur unterstützt, die sich dynamisch an neue Gegebenheiten anpassen lässt. LAN und WLAN wurden dabei nahtlos integriert, um überall das für den Arbeitsprozess und für die Umgebung optimale Medium bereitstellen zu können.

Im Hintergrund arbeiten redundant ausgelegte und damit hochverfügbare RADIUS-Proxy-Server, die anhand der Anfrage zunächst erkennen, zu welcher der beteiligten Firmen der Client gehört und dann seine Anmeldung an die jeweiligen firmenspezifischen RADIUS-Server weiterleiten. Anschließend findet dort eine Prüfung der Anfrage gegen den jeweiligen Verzeichnisdienst statt. Ist der Client bekannt und zugelassen, wird er automatisch dem richtigen VLAN zugewiesen und gelangt damit, unabhängig an welchem Ort auf dem Campus er sich mit dem Multi-Client LAN verbindet, sicher und automatisch in das Intranet der eigenen Firma.

Bei den Komponenten setzte das Projekt auf Cisco-Switches und überwiegend auf Software-Komponenten, die die bereits im Einsatz befindlichen Microsoft-Systeme von Hause aus mitbringen, d.h. den Microsoft IEEE802.1x-Supplicant und den IAS RADIUS-Server. Da IEEE 802.1x jedoch ein offener Standard ist, werden von der gesamten Architektur auch andere Verfahren und Komponenten unterstützt, womit das gesamte Konzept herstellerunabhängig bleibt. Damit sind die beteiligten Firmen weiterhin frei in der Wahl eigener alternativer Authentifizierungs-Methoden und selbst eine künftige Rechneranmeldung mit Smart-Cards – ein besonders sicheres Verfahren – oder auch andere 2-Faktor-Authentifizierungsverfahren können mit dem System umgesetzt werden.

Zum weiteren Gesamtkonzept der rt-solutions.de gehörte darüber hinaus ein eigenes, logisch abgetrenntes Gast-VLAN mit beschränkten Zugriffsrechten. Ein solches Gast-VLAN ermöglicht es zum einen, allen Rechnern, die noch nicht auf den neuen Standard umgestellt sind, weiterhin Netzwerkkonnektivität zu behalten und sorgt zum anderen dafür, dass auch Rechner externer Mitarbeiter auf die für sie notwendigen Netzwerk-Ressourcen zugreifen können.

Mit gründlichen Tests und durch Unterstützung beim Rollout sowie bei der Etablierung der neuen Netzwerkmanagement- und Helpdesk-Prozesse sorgte rt-solutions.de für einen reibungslosen Ablauf der schrittweisen, weltweiten Umstellung der ca. 11.000 Ports, welche die Netzwerkqualität und -sicherheit vom ersten Augenblick an garantierte.

Wesentliche Rahmenbedingungen für den Erfolg des Projektes waren:

- ▶ Reibungslose und für die Benutzer transparente Migration
- ▶ Berücksichtigung von nicht 802.1x-fähigen Legacy-Geräten
- ▶ Robuste, flexible und hochverfügbare Netzwerkstrukturen
- ▶ Anbindung an den vorhandenen Verzeichnisdienst (Active Directory)
- ▶ Einbindung in die bestehende Netzwerkmanagement-Lösung (HP OpenView)
- ▶ Zugangskonzept für Gäste und Externe
- ▶ Kostengünstige, wiederverwendbare Lösung

### **Zeitraumen und Aufwand**

Das Konzept und die Implementierung wurden in 2005 mit einem Aufwand von 200 PT durchgeführt.

### **Eingesetzte Technologien**

- ▶ IEEE 802.1x mit EAP-PEAP
- ▶ RADIUS
- ▶ LAN, WLAN
- ▶ VLANs (IEEE 802.1q)
- ▶ PKI/Zertifikate

### **Fazit**

Das System läuft produktiv. Das Projekt wurde im Zeit- und Budgetrahmen erfolgreich umgesetzt. Das Ergebnis stellt heute eines der größten produktiven Netze mit dynamischer VLAN-Zuweisung und gesichertem Zugang auf Basis von IEEE 802.1x dar.