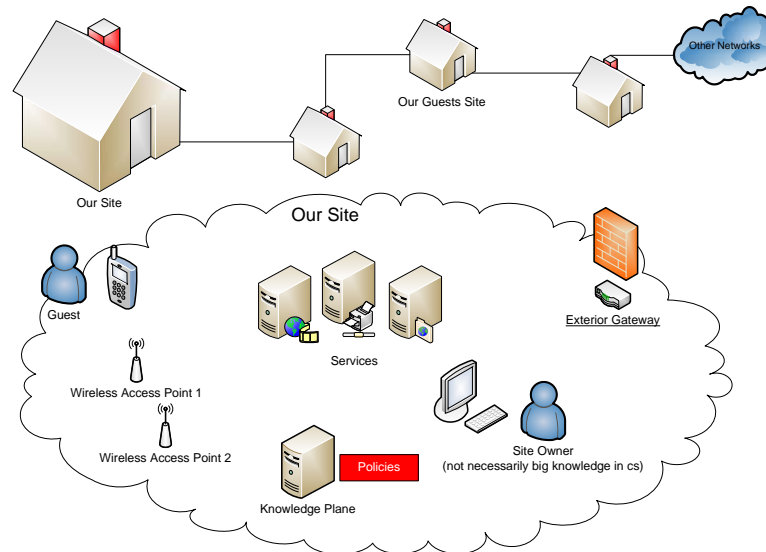




Secure Auto-Managing Networks



Motivation

Rechnernetze finden sich heutzutage in nahezu allen Lebensbereichen. Es sind sehr viele unterschiedliche Geräte auf verschiedene Arten aneinander angebunden oder gerade noch nicht verbunden, da entsprechende Möglichkeiten (noch) fehlen.

Es ist zu erwarten, dass in Zukunft noch deutlich mehr Geräte der unterschiedlichsten Art verbunden sein werden. Dies betrifft nicht nur professionelle Umfelder sondern insbesondere auch Häuser und ähnliches, die nicht unter Verwaltung von speziell ausgebildeten Administratoren stehen.

Das Eingliedern von heterogenen Geräten in ein zukünftiges gemeinsames Netz muss daher so geschehen können, dass kein Eingriff vom Benutzer erforderlich ist, der tiefer gehendes Wissen über die Komponente, das Netzwerk oder ähnliche technische Details erfordert.

Zu diesem Zweck wird eine standardisierte Architektur benötigt, die Wissen über im Netzwerk befindliche Komponenten besitzt und diese derart konfiguriert, dass das Netz in gewünschter Weise funktioniert.

In „gewünschter Weise“ bedeutet hier insbesondere auch, dass Sicherheitsziele im Netz durchgesetzt werden, also beispielsweise sichergestellt wird, dass ein Hausbesucher, der das WLAN zum Zugriff auf das Internet verwendet, nicht die Garagentorsteuerung manipulieren kann.

Aufgabenstellung

Konkrete Aushänge folgen demnächst hier und auf der Website. Bei Interesse für das Thema gerne einfach kurz melden. Kontaktdaten siehe unten.

Voraussetzungen

Kenntnisse in den Bereichen Netzwerkkonfiguration, Netzsicherheit, Objektorientierte Programmierung, Client-/ Server-Programmierung, C++, Java

Stichworte

Self Configuration, Knowledge Plane, Policy Based Management

