Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

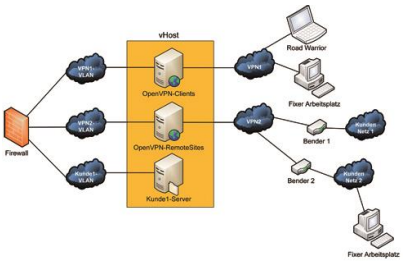
InIT Institut für angewandte
Informationstechnologie

Secure Access Remote Site

Diplomierende
Kevin Lapagna
Peter Zürcher

Dozent
Marc Rennhard

Diese Arbeit beschreibt die Konzeption und Erstellung einer OpenVPN Infrastruktur, deren Verwaltung komplett über eine eigens dafür entwickelte Webapplikation erfolgt. Die Resultate der Arbeit werden dafür verwendet, eine bereits bestehende VPN Infrastruktur der Young Solutions AG abzulösen. Youngsolutions setzt dieses VPN ein, um ihren Kunden und den eigenen Mitarbeitern einen sicheren Zugriff auf die Server-Systeme in ihren Rechenzentren zur Verfügung zu stellen. Dieser Service wurde eingerichtet, da youngsolutions ihren Kunden virtuelle Server und Dienste zur Verfügung stellt, die auf Systemen laufen, welche nicht direkt über das Internet verfügbar sein dürfen. Mittelfristig werden für diese Produkte signifikant mehr Nutzer erwartet. Der Verwaltungsaufwand der Umgebung, die bis anhin nicht automatisiert ist, skaliert bei den erwarteten Nutzerzahlen jedoch nicht mehr. Da in diesem Fall auch die Übersicht über die Konfiguration nicht mehr gegeben ist, kann die Effektivität und damit die Sicherheit des Systems nicht mehr gewährleistet werden.



Schema der logischen Netzstruktur. Die einzelnen Netze werden mit VLANs gebildet und über eine Firewall miteinander verbunden.

Das neue Verwaltungswerkzeug soll dafür sorgen, den Administrationsaufwand für den Betrieb auf ein Minimum zu beschränken. Dazu wurde eine gesamtheitliche Benutzer-, Zugriffs- und Zertifikatsverwaltung mit Ruby on Rails realisiert. Um die Benutzerführung zu vereinfachen, wurde der Grossteil der Interaktionen mit Ajax, unter Verwendung des JavaScript-Frameworks jQuery, umgesetzt. Ebenfalls wurden die nötigen Schnittstellen, die für eine automatisierte Anpassung des Firewallregelwerks und die Konfiguration der VPN-Server sorgen, erstellt und integriert. Dabei wird die in der Arbeit benutzte pfSense Firewall über das Web-Interface mit einer XML-Datei konfiguriert, während die OpenVPN-Server mit SSH angesprochen werden.

Ausschnitt aus der Benutzeroberfläche der Web-Applikation. Die Userdaten, Zugriffsberechtigungen und Zertifikate können über diese Ansicht verwaltet werden.

Zusätzlich wurde ein Embedded-System konzipiert, welches die Anbindung ganzer Kundennetze in die VPN Infrastruktur ermöglicht. Der erstellte Prototyp ist ein passiv gekühlter Mini-Computer mit einem ALIX-Systemboard. Nebst dem Aufbau des VPN Tunnels kann das Gerät als Router und Wireless-LAN Access Point verwendet werden.

Die Anforderungen wurden während der Arbeit alle erfolgreich umgesetzt. Die für nach der Arbeit geplante Integration der Lösung in das produktive Umfeld sollte mit geringem Aufwand möglich sein.