Redesign Swisscom NAC Service

Studiengang: MAS Information Technology
Betreuer: Mathias Engel
Experte: Christof Dubach (Swisscom)

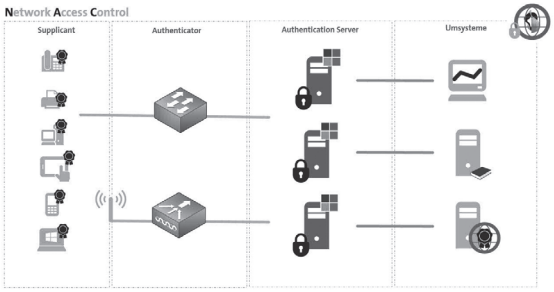
Durch die Neuentwicklung des internen Windows 10 Mitarbeiternotebooks traten zunehmend Integrationsschwierigkeiten mit dem bestehenden Radius Server auf. Um die Weiterentwicklung nicht zu gefährden, wird der bestehende Radius Server durch einen Microsoft Network Policy Server (NPS) ersetzt. Der Network Access Control (NAC) Zugriffsschutz zur Netzwerkinfrastruktur kann mit den neuen Clients so wieder gewährleistet werden.

Umfeld

Das Umfeld des Swisscom NAC Services umfasst einen Radius Server Cluster von 6 physikalischen Servern, welche zusammen über 40 000 Clients schweizweit am firmeneigenen Netzwerk authentisieren. Die Clients befinden sich an über 330 Standorten und verbinden sich täglich mit mehr als 2 400 Access Points (AP) und 1 800 Access Switches. Unter all diesen Clients sind Windows 7 & 10 Notebooks, Apple MAC Books und iPads, so wie IP-Phones, welche sich mittels Zertifikat authentisieren, um Zugriff auf die firmeneigenen Ressourcen zu erhalten. Der NAC Service beinhaltet sowohl die kabelgebundene, wie auch die Wireless Anbindung.

Problemstellung

Der aktuell eingesetzte Radius Server zeigt einige Integrationsschwierigkeiten mit dem Authentisierungsverfahren der Windows 10 Clients. Diese können sich nicht mehr authentisieren. Weiter existiert kein End2End Monitoring Tool. Das bedeutet, dass im Fehlerfall sämtliche Log-Files auf jedem Radius Server einzeln analysiert werden müssen. Historisch bedingt wurden die Radius Server auf den Access Switchen schweizweit in verschiedener Reihenfolge konfiguriert, damit alle Radius Server gleichmässig mit den Requests ausgelastet werden.



Vorgehen

Durch die Erfahrung von bereits realisierten Kunden NAC Lösungen, wurde im Voraus beschlossen, dass der neue Radius Server mit einem Microsoft NPS Cluster realisiert wird. Intern war die Vorgabe, dass sich alle bestehenden Clients, ohne Anpassungen der Authentisierungsmechanismen, am Firmennetzwerk anmelden können. Das Projekt enthielt ein umfangreiches Konzept, welches die Ausgangslange sehr detailliert beschrieb. In einem Proof of Concept (PoC) wurden alle möglichen Authentisierungsmethoden der bestehenden Clients auf dem neuen NPS Radius Server getestet und verifiziert. Nach Abschluss der erfolgreichen Tests wurden die produktiven virtuellen NPS Radius Server hochgefahren. Durch das Analysieren und Optimieren der Access Switch Konfigurationen konnte ein Loadbalancing der Radius Requests konfiguriert werden. Dies ergibt eine Vereinheitlichung der Access Switch Konfiguration und dennoch eine gleichmässige Auslastung der Radius Server. Bevor alle Swisscom Standorte migriert werden, wurden einzelne Standorte als Pilot auf den neuen NPS-Radius Server umgeschaltet. Abschliessend werden nun schweizweit alle Swisscom Standorte auf den neuen NAC Service migriert.

Stefan Mathys

Resultat

Da die bestehenden Umsysteme, wie die Certificate Authority (CA) und das Active Directory (AD), die für die Authentisierung nötig sind, ebenfalls bereits auf Microsoft Servern basieren, harmonisierten diese hervorragend mit den neu eingesetzten NPS-Radius Servern. Sämtliche Projektziele konnten realisiert und eingehalten werden. Durch die Integration in das bestehende Monitoring und dem Logging Tool SPLUNK (www.splunk.com) wurde eine zentrale Stelle eingesetzt, welche sämtliche Events aller Radius Server und zusätzlich aller Netzwerkkomponenten gemeinsam aufzeigen kann. Somit konnte eine End2End Sicht für den Authentisierungsprozess geschaffen werden.