WLAN NAC mit PacketFence

Fachgebiet: Networking and Security
Betreuer: Marcel Wälti
Experte: Mathias Engel (advact AG)
Industriepartner: Post CH AG

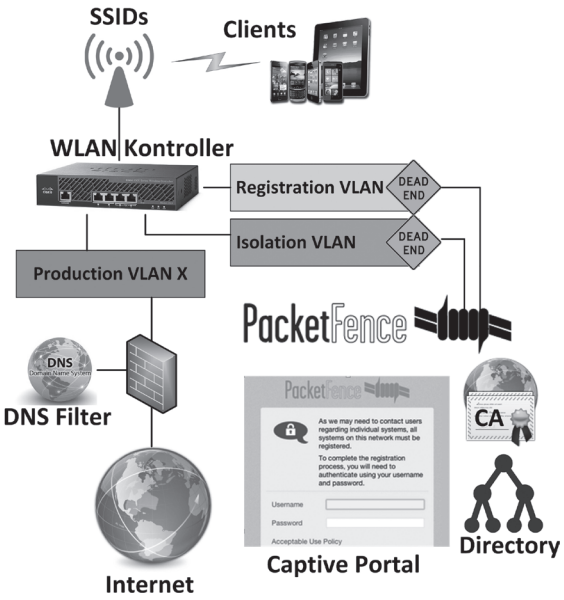
Aufgrund der stetig wachsenden Anzahl mobiler Geräte werden WLAN-Netze immer stärker beansprucht. Die Authentifizierungs- sowie Filtersysteme kommen an ihre Leistungsgrenzen. Im Rahmen dieser Arbeit wurden die Gäste-WLANs der Post CH AG rundum erneuert. Die bestehende Authentifizierungslösung wurde durch die OpenSource NAC Software (Network Access Control) PacketFence abgelöst. Die alten HTTP-Filtersysteme wurden durch eine Lösung auf Basis von DNS ersetzt.

Umfeld

Post IT betreibt in jedem Bürogebäude des Konzerns ein Gäste-WLAN für interne und externe Mitarbeiter. Dieses Netz wird hauptsächlich für firmeneigene Smartphones und Tablets sowie für private Geräte verwendet. Für Demogeräte in Poststellen als auch für Gäste in Postfinance Filialen wird ebenfalls ein Internetzugang zur Verfügung gestellt.

Problemstellung

Der festgestellte Trend der stetig wachsenden Zahl mobiler Geräte hat dazu geführt, dass die bestehende Authentifizierungs- und Filterlösung mit dem Ansturm von Geräten nicht mehr zurechtkam. Die sich häufenden Beschwerden bewogen schliesslich dazu, das Projekt «WLAN Improvement» ins Leben zu rufen. In einer Evaluation vier möglicher Lösungen konnte sich die OpenSource Software PacketFence durchsetzen.



PacketFence Übersicht

Das Ziel der Master Thesis war es, PacketFence als neue Authentifizierungslösung fürs Gäste-WLAN einzuführen.

Vorgehen

Nachdem das umfangreiche Konzept, welches unter anderem auch Authentifizierung mittels Active Directory, Zertifikaten und SMS Nachrichten beinhaltet, durch das Sicherheits- und Architekturteam abgenommen wurde, konnte mit dem Bau der Netze und Systeme begonnen werden. Vordefinierte Tests halfen dabei, die Funktionalität der Lösung auf den gewünschten Stand zu bringen. Mit der Fertigstellung der Installations- und Betriebsanleitung sowie der Schulung des Betriebs- und Helpdesk-Teams konnte die neue Lösung schrittweise den Endbenutzern kommuniziert werden.

Resultate

Sämtliche Ziele konnten erreicht und PacketFence damit erfolgreich eingeführt werden. Mehr als 7000 Geräte verwenden bereits die neue Lösung. Dank der gewählten «out of band» Architektur, bei der der Verkehr nicht durch PacketFence selbst fliesst, kommt es trotz grosser Nutzerzahlen zu keinerlei Performance-Einbussen. Der bestehende Proxy-Filter wurde durch eine selbst entwickelte Filterlösung auf Basis von DNS abgelöst. Als Datenquellen kommen neben externen Dienstleistern auch selbst generierte «Blacklists» zum Zug. Das System arbeitet schnell und zuverlässig. Im Vergleich zum alten Filter können so rund Fr. 40 000 pro Jahr an Lizenz- und Wartungskosten eingespart werden.

Fazit

Das positive Feedback der Benutzer bestätigt die gewählte Lösung. Sie ist performant, kostengünstig und stabil und somit bestens für die Zukunft gerüstet.

Ausblick

Bereits jetzt zeichnen sich erste neue Bedürfnisse ab, die mit PacketFence erfüllt werden könnten. Die Einführung von IPv6 im Gäste-WLAN ist bereits im Gange.

Lukas Reusser