Proof of Concept für eine neue Firewall & WEB-Proxy Lösung

Studiengang: MAS | Vertiefung: MAS Information Technology

Im Rahmen eines öffentlichen Ausschreibeverfahrens wird im Bereich Netz- Zugangssysteme ein Produktewechsel fokussiert. Betroffen sind Next Generation Firewall von Check Point und WEB-Proxy von Blue Coat. Um zu prüfen, ob die heutigen und künftigen Anforderungen dem neuen Produkt von Fortinet entsprechen, soll ein Proof of Concept durchgeführt werden.

Ausgangslage

Das ISC-EJPD betreibt eine eigene Informatik Infrastruktur und bietet individuelle Fachanwendungen mit erhöhten Anforderungen in Sicherheit, Verfügbarkeit und Softwareentwicklung an.
Um eine langfristige Sicherung der beschaffungsrechtlichen Grundlage zu erreichen, wurde eine Ausschreibung für die ganze Bundesverwaltung durchgeführt. Der **Zuschlag gilt bis 2032** und die One-Vendor-Strategie will mit dem **Produkt Fortinet** umgesetzt werden.

Zielsetzung

In einem **PoC** soll nun geprüft werden, ob die heutigen und künftigen Anforderungen mit dem neuen Produkt Fortinet umgesetzt werden können. Es sollen **Parameter & Features getestet** werden und weitere **Erkenntnisse** und **Empfehlungen** abgegeben werden.

Vorgehen

Die **Situationsanalyse** zeigte die heutige hochverfügbare Check Point Firewall Lösung in einem aktuellen und guten Zustand. Ebenso die WEB-Proxy Landschaft von Blue Coat im Web Security Bereich. Die genutzten Features für eine solche Umgebung sind Voraussetzung dazu. Diese gelten nun als **Anforderungen** für das neue Produkt Fortinet.

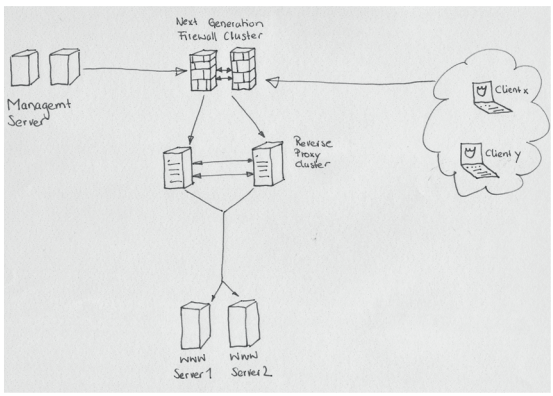
Lösung

Der Aufbau der virtuellen Fortinet Appliances konnte mithilfe des Testkonzeptes realisiert werden. Parallel zum Aufbau wurden **Smoketests** durchgeführt, die bereits zu Beginn das Vorhaben ins Wanken brachten. Für das FortiWeb (Reverse Proxy) Management **fehlte** die **Proxy Einstellung**. Die Umgehungslösung führte nun zumindest eine Online Lizenzvalidierung durch. Kurz darauf wurde ein Incident an die PoC Verantwortlichen adressiert, dass das CSIRT Kommunikationsverbindungen vom FortiManager zu FortiGuard blockiert. **Nicht konforme HTTP** Abfragen waren die Ursache dafür. Weitere Parameter & Features wurden mit einem negativen wie positiven Ergebnis getestet.

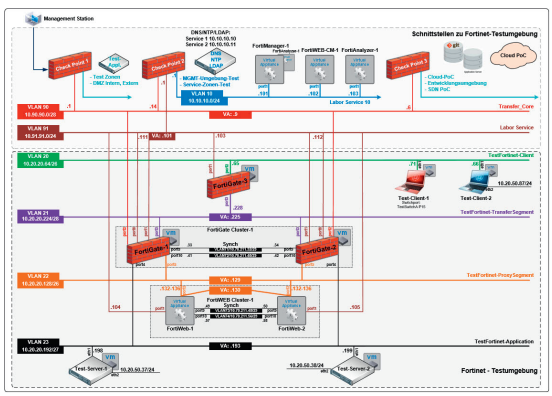
Fazit

Eine wichtige **Erkenntnis** ist, dass das ISC-EJPD eine aktuelle Security Umgebung hat, die aber in Zusammenhang mit Ihrer Grösse in Richtung Automatisierung gehen muss.
Daher die **Empfehlung** eine Automatisierung anzustreben, die wir uns für eine allfällige Produkte Migration auch gleich zu nutzen machen können.
Die **Konsequenzen** aus dem PoC sind die Ausarbeitung von Lösungen für die Fehlerklassen 3 und 4. Mit dem **Ausblick** in die nächste Phase «Pilot» zu starten.

Bruno Heiniger



Entwurf einer möglichen Testumgebung



Aufgebaute virtualisierte Fortinet Testumgebung