Einführung neue Zonen Firewalls mit IPS Service

Studiengang: MAS Information Technology

Durch die erweiterten Anforderungen eines Kundennetzwerks wurde unser ICT Unternehmen beauftragt eine Optimierung im Bereich der Zonen Firewalls konzeptionell zu erarbeiten und umzusetzen. Dabei wird das Firewall Produkt von Cisco mit FortiGate erneuert und ein IPS Service auf einzelnen Zonen Firewalls aufgebaut. Zusätzlich soll dabei evaluiert werden, was es für zusätzliche Ansätze auf Netzwerkebene gibt, die mit einem IPS korrelieren können.

Umfeld

Unser ICT Unternehmen betreibt ein umfangreiches Netzwerk eines Kunden in Form von Managed Services. Netzwerkdienste im Bereich WAN, LAN, WLAN und Security werden zur Verfügung gestellt. Die zentrale Drehscheibe von diesem Netzwerk ist der Netzübergang zum Internet, wo alle Zonen Firewalls angeschlossen sind. An den Zonen Firewalls sind verschiedene Netzwerkzonen mit entsprechenden Sicherheitsstufen von Netzkunden angeschlossen. Die Zonen Firewalls schützen diese Netzwerkzonen mit einem Regelwerk.

Problemstellung

Um einen erweiterten Funktionsumfang in Betracht auf Performance und IPS abdecken zu können soll das Cisco Firewall Produkt durch eine FortiGate Firewall Lösung ersetzt werden. Dabei muss die Cisco Firewall Regel Syntax Migration automatisiert auf FortiGate Syntax erfolgen. Die neuen Zonen Firewalls müssen ins dynamische Routing zum Internetübergang aufgenommen werden, wo unter anderem die Problematik von zwei verschiedenen Default Routen zu zwei Web Proxy Diensten zu lösen ist. Eine Lese- und Schreibberechtigung für Netzkunden mit Administratorenrechten auf den Zonen Firewalls muss erarbeitet sowie ein Pilot soll umgesetzt werden.
Der IPS Service soll Netzwerkzonen mit höheren Sicherheitsstufen schützen und intern auf den Zonen Firewalls aufgebaut werden. Dabei müssen folgende Problemstellungen für das IPS behandelt und gelöst werden:

- Funktionsweise IPS Feature im FortiOS
- Anwendung welcher IPS Verfahren und Schutzmechanismen?
- Was ist pro Netzwerkzone zu schützen und welche Signaturen sollen aktiviert sein?
- Was gibt es für zusätzliche Schutzmöglichkeiten im Netzwerkbereich, die mit dem IPS korrelieren können?

Daneben soll ein Penetration Test aufzeigen, ob das neue Firewall Produkt gehärtet ist oder ob es Schwachstellen aufweist, die ausgenutzt werden können.

Lösungskonzept und Realisierung

Für die Migration des Firewall Regelwerks von Cisco Syntax auf FortiGate Syntax bietet FortiGate die Applikation «FortiConverter» an. Der FortiConverter deckt nicht alle Anforderungen für den automatisierten Wechsel ab, wodurch zusätzlich mit «vb.net» ein Migrations-Tool entwickelt wurde.
Das dynamische Routing wird mittels eBGP von den Kundennetzen (MPLS VPNs) über die Zonen Firewalls bis zum Internetübergang realisiert. Über eBGP werden die internen Netzwerkzonen propagiert. Vom Internetübergang erfolgt die Verteilung einer Default Route mittels OSPF. Damit die zwei verschiedenen Web Proxy Dienste von den Zonen Firewalls über zwei Default Routen im Internetübergang angesprochen werden können, werden zwei VRFs erstellt.
Entsprechende TACACS+ Attribute Values (AV) werden von einem Identity Server zur FortiGate gesendet, um ein eingeschränktes User Profil dynamisch zuweisen zu lassen und die Lese- und Schreibberechtigung für Firewall Administratoren von Kunden einzugrenzen.
Der Zonen Firewall Pilot wurde erfolgreich umgesetzt und der Penetration Test war zufriedenstellend.
Das Network IPS (NIPS) wird auf den Zonen Firewalls inline geschaltet und soll bösartige Verbindungsversuche aktiv blockieren. Das IPS im FortiOS wird mit einem signaturbasierten und ratenbasierten Schutz aufgesetzt. Die IPS Engine in der FortiGate muss immer pro Firewall Regel aktiviert werden. Während dem Pilot wird das IPS zuerst im Monitoring Mode eingeschaltet. Dabei werden alle Signaturen aktiviert und die Alarmmeldungen via syslog auf einem Remote Server gesammelt. Mit ELK sollen die IPS Logging Daten ausgewertet werden um zu bestimmen, welche IPS Signatur-Kategorien in Zukunft scharf geschaltet werden sollen. Als erweiterten Schutz in Korrelation mit einem IPS kann ein SIEM in Betracht gezogen werden.

Schlussbetrachtung

FortiGate überzeugt als neue Zonen Firewall Lösung. Erweiterte Funktionen müssen auf dem System im CLI angepasst werden. Das GUI kann für einfachere Konfigurationen verwendet werden. Etwas speziell ist die IPS Handhabung, wo pro Firewall Regel definiert werden muss, welche IP Pakete zur IPS Engine weitergeleitet werden sollen.

Thomas Imboden

Marcel Ritschard