Forefront Threat Management Gateway (TMG) *und* Forefront Unified Access Gateway (UAG)

Die perfekte Lösung

KEMP

3KV a member of HPI group

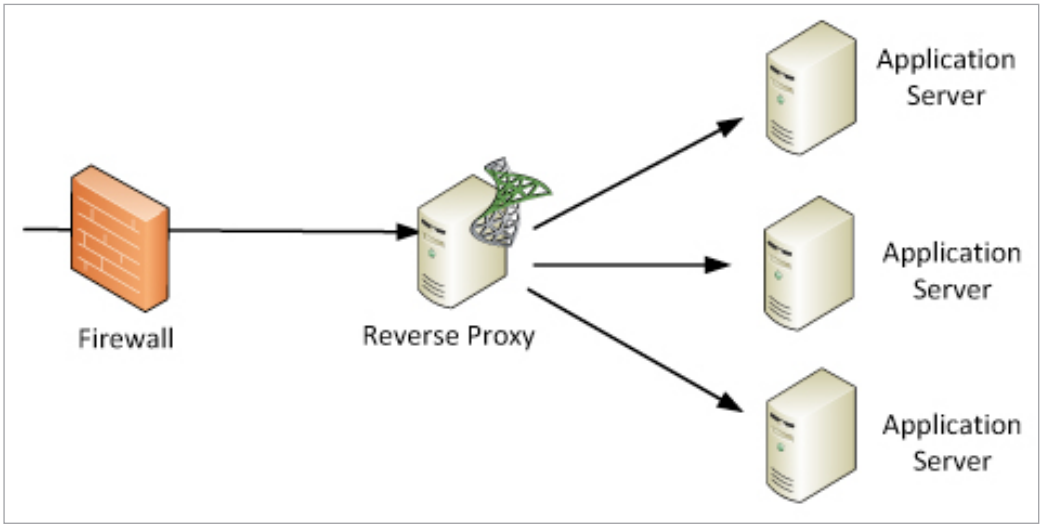
Das Problem

Die Abkündigungen seitens Microsoft von **Forefront Threat Management Gateway (TMG)** und **Forefront Unified Access Gateway (UAG)** sind ein herber Einschnitt und bedeuten für viele Kunden eine Neuorientierung bezüglich des Themas Reverse Proxy, denn beide Produkte wurden in der Praxis als Reverse Proxies eingesetzt.

Bevor auf die Alternativen eingegangen wird betrachten wir zunächst einmal die Grundfunktionen eines Reverse Proxy.

Grundfunktionen eines Reverse Proxies

Ein Reverse Proxy nimmt Anfragen von einer Firewall an. Bei diesen Anfragen handelt es sich um HTTP / HTTPS Traffic. Die Anfrage wurde auf der Firewall schon nach schädlichem Inhalt überprüft. Der Reverse Proxy prüft die angefragten Server und URLs auf ihre Richtigkeit und präsentiert ein Formular zur Eingabe der Credentials. Diese Credentials werden Prä Authentifiziert. Sind die Credentials korrekt wird die Anfrage an den jeweiligen Applikations Server weitergeleitet.

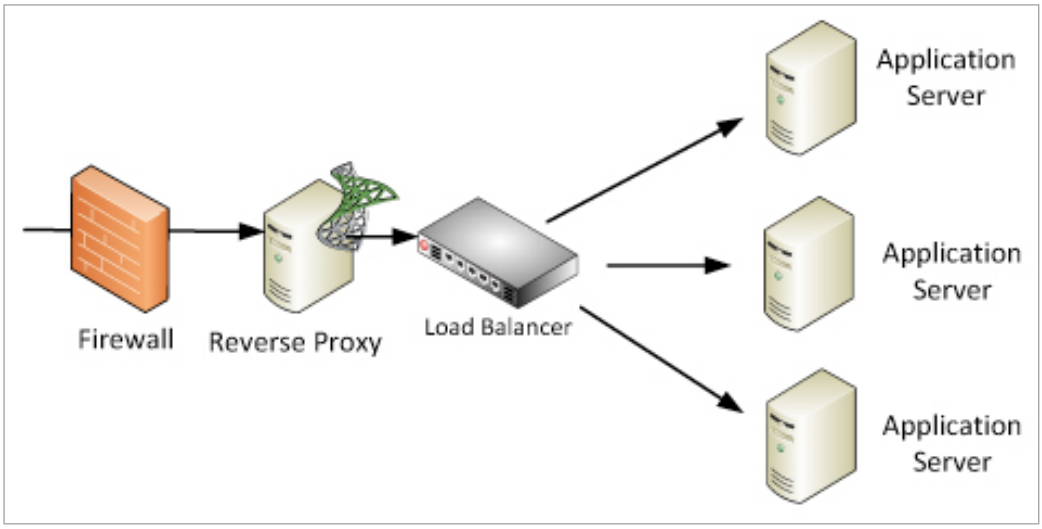


Ein Reverse Proxy ist dabei so platziert, dass er selbst kein Mitglied einer Domäne ist und die Abfrage nach der Korrektheit der Credentials per LDAP an einen Domain Controller gerichtet wird. Dazu werden vom Reverse Proxy eigene Eingabe Formulare verwendet.

Des Weiteren existieren auf einem Reverse Proxy Regeln zu den erlaubten FQDN der Applikations Server und deren URLs, die ebenfalls überprüft werden.

Um in die Netzwerkpakete „hineinschauen" zu können arbeitet ein Reverse Proxy im Layer 7 Modus und terminiert bei HTTPS die SSL Verbindung am Reverse Proxy, um diese dann wieder verschlüsselt an den Applikations Server durchzureichen.

Bei größeren Installationen und einer hohen Anzahl von Anfragen werden diese in der Regel über einen Loadbalancer weitergeleitet, der die Lastverteilung auf die Applikationsserver übernimmt.



Eines muss an dieser Stelle noch klar vermittelt werden:
Ein Reverse Proxy ist KEINE Firewall und ersetzt auch nicht eine Firewall.

Reverse Proxies werden also immer im Zusammenspiel mit Firewalls eingesetzt, je nachdem wie die Netzwerktopologie sich darstellt (Perimeter Netzwerk, Front End / Back End Firewall, …).

Bei der Fülle an Angeboten zu Reverse Proxies ist es müßig, Vergleiche im Einzelnen aufzulisten. Allerdings seien an dieser Stelle zwei neue Funktionalitäten der Microsoft Windows 2012 R2 Server kurz beleuchtet, die Reverse Proxy Funktionalitäten beinhalten und durchaus Beachtung finden.

Es handelt sich dabei um die Features IIS Application Request Routing (IIS ARR) und IIS Webapplicationproxy (IIS WAP). Beide Features stehen nur mit Windows Server 2010 R2 zur Verfügung, erfordern also grundsätzlich den Einsatz eines Windows 2012 R2 Servers (IIS ARR) oder von zwei Windows 2012 R2 Servern (IIS WAP). WAP benötigt Windows ADFS (Active Directory Federation Services) für die Prä Authentifizierung, deshalb werden für diese Konfiguration 2 Windows 2012 R2 Server benötigt.

IIS ARR wird auf einem Windows Server 2012 R2 installiert, der nicht Member einer Active Directory Domäne ist. Die Installation von IIS ARR ist relativ einfach. IIS ARR eignet sich eher für kleine Umgebungen. IIS ARR hat allerdings einen gravierenden Nachteil, es kann keine Prä Authentifizierung!

Für IIS WAP braucht es zwei Windows 2012 R2 Server, einen für ADFS der Domain Member ist und einen für den WAP, der nicht Domain Member ist. IIS WAP beherrscht Prä Authentifizierung, die Konfiguration ist allerdings sehr aufwendig und fehlerträchtig und auch die Fehlersuche, wenn in diesem Konstrukt etwas nicht funktioniert, ist sehr aufwendig.

Beide also nicht unbedingt elegante und leicht zu konfigurierende und zu bedienende vollwertige Alternativen.

Die Lösung

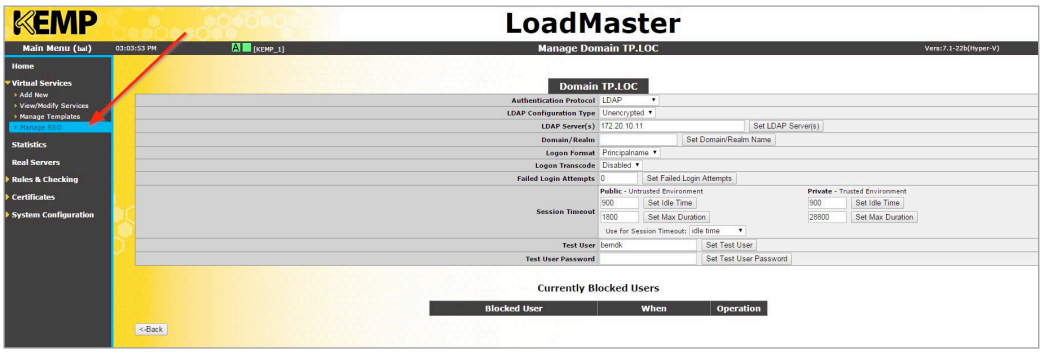
Nach der Abkündigung von TMG und UAG besannen sich natürlich die verschiedenen Hersteller von Loadbalancern auf die Möglichkeiten, diese Funktionalitäten in den Loadbalancern nachzubilden. Denn es ist natürlich geschickt, eine derartige Funktion in einem Loadbalancer zu haben, den man in vielen Fällen sowieso benötigt und womit man sich weitere Installationen erspart.

Bei den **Loadbalancern der Firma KEMP Technologies** wird die Web Proxy Funktionalität durch das Edge Security Pack (ESP) nachgebildet. Das ESP ist fester Bestandteil der Kemp Loadbalancer Funktionen, muss also nicht extra geordert werden.

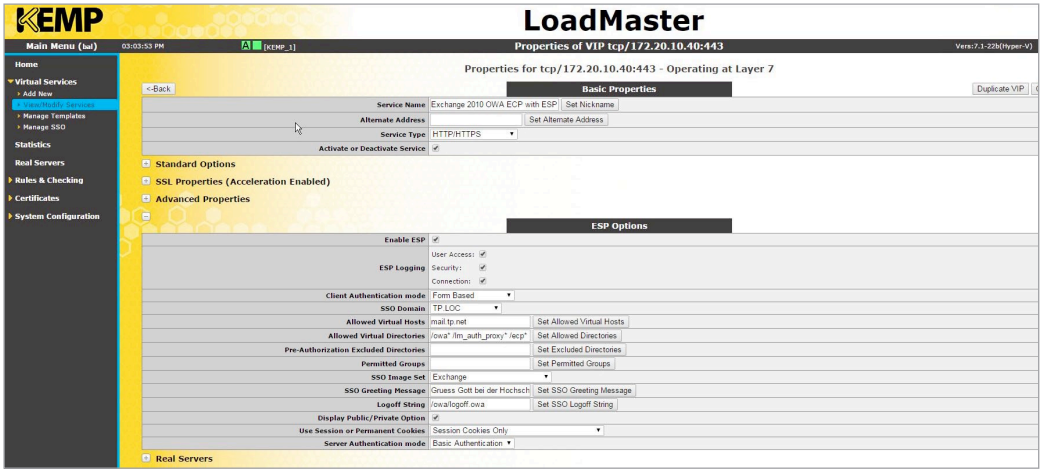
ESP wird per Virtual Service aktiviert. Um das ESP an einem Virtual Service nutzen zu können muss allerdings der SSL Traffic für diesen Virtual Service am Loadbalancer terminiert werden. Das ESP bietet verschiedene Optionen:

» Single Sign On
» Abfrage User Credentials per LDAP gegen einen Domain Controller
» Beschränkung Zugriff auf bestimmte Server und URLs
» Formular basierte Anmeldung
» Logging der Zugriffe

Single Sign On Optionen:



ESP Settings:



Für weitere Informationen stehen wir Ihnen gerne persönlich zur Verfügung.

3KV a member of HPI group

3KV GmbH Central Tower Munich Landsberger Straße 110 80339 München Germany

Phone: +49 (0)89 800 656-0 Fax +49 (0)89 800 656-66 info@3kv.de www.3kv.de