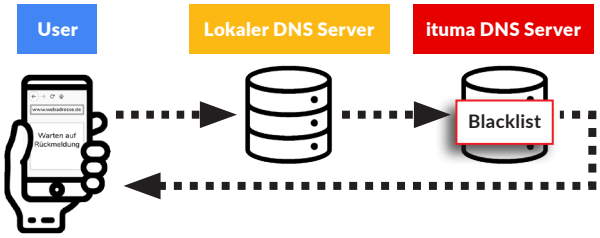
ITUMA **WIFI CONTENT FILTER**

Der von der ituma GmbH bereitgestellte Content-Filter verhindert Zugriffe auf unerwünschte Inhalte. Die Konfiguration via DNS-Server ist skalierbar und kann individuell auf Ihre Bedürfnisse angepasst werden.

Vereinfachte Funktionsweise:

DNS Anfragen der mobilen Endgeräte zur Auflösung der Internetadressen werden an den DNS-Service des Content Filters weitergeleitet. Alle bei diesem eintreffenden Anfragen prüft der Server gegen eine lokal vorgehaltene Liste (Blacklist) von Domainnamen.



Filterung und Rückmeldung

Wenn die angefragte Domain nicht auf der Blacklist geführt wird, leitet der Server die DNS Anfrage an den nächsten höher gelegenen DNS Server weiter. Die zurückgelieferte Internetadresse wird regulär an das anfragende Endgerät zurückübermittelt, sodass dieses den Verbindungsaufbau zum gewünschten Ziel initialisieren kann.

Wenn die angefragte Domain nicht auf der Blacklist geführt wird, leitet der Server die DNS Anfrage an den nächsten höher gelegenen DNS Server weiter. Die zurückgelieferte Internetadresse wird regulär an das anfragende Endgerät zurückübermittelt, sodass dieses den Verbindungsaufbau zum gewünschten Ziel initialisieren kann.

Eine direkte Angabe der DNS-Server ist auch möglich. Um den Dienst aber nicht frei im Internet zu betreiben, werden dabei die Zugriffe auf die Source-IP der jeweiligen Lokalität beschränkt (sofern hier statische IPs existieren).

DNS basiertes Filtern

DNS wird verwendet, um zu einer URL die IP und dadurch die Lokalisation im Internet zu ermitteln. Über die IP-Adresse wird dann der hinter der URL bereitgestellte Content gefunden.

Aufgrund der hohen Anzahl existierender Domains sind deren Auflösungen auf eine Vielzahl von Servern hierarchisch verteilt. Kann ein DNS-Server die Adresse nicht auflösen, wird die Anfrage zum nächst höhergelegenen DNS-Server weitergeleitet.

Sofern jedoch der Domainname aufgrund von unerwünschtem Inhalt in der Liste geführt wird, beantwortet der Service die Anfrage je nach Konfiguration dahingehend, dass

- die eigene IP des DNS-Servers anstatt der wahren IP an den Client zurückgeliefert wird oder
- eine fiktive IP-Adresse zurückgeliefert wird.

Kleinhülsen 29 | 40721 Hilden | Germany
E-Mail: kontakt@ituma.eu | Tel: +49 2103 280 99 0

Sicherheit

DNS Anfragen sind im Allgemeinen unverschlüsselt. Auf Wunsch erfolgt die Anbindung des Gateways zum Content Filter mit SSL-Verschlüsselung oder über eine dedizierte VPN-Verbindung.

Aktualität

Die eingesetzte Blacklist basiert auf der „Ultimate Hosts Blacklist“ mit aktuell über 1,7 Mio. Einträgen sowie der „StevenBlack/hosts with the porn extension“ mit über 88.000 Einträgen. Die Blacklist wird täglich aktualisiert.

Gefilterte Inhalte

Alle Inhalte gemäß der Ultimate Hosts Blacklist werden gefiltert. Filterung nur einzelnen Kategorien ist nicht möglich. Sie können über eine zusätzliche Blacklist eigene Einträge hinzufügen oder wieder löschen.

Verhalten individueller Apps

APPs, die versuchen eine gesperrte Adresse im Internet zu erreichen, werden keine Antwort erhalten, da die Anfragen durch den Content Filter nicht beantwortet werden. Ausnahmen sind APPs, die einen Browser simulieren und versuchen, eine unverschlüsselte Webseite aufzurufen. Diese werden die lokale Webseite des Content Filters zeigen. Alle anderen Anwendungen werden in einen Timeout laufen.
Andere Streamingdienste von Apps sind von dem Content Filter nicht betroffen.

Auswirkungen des Content Filters auf die User-Experience

Wenn die angefragte Domain nicht auf der Blacklist geführt wird, verhält sich der Content Filter transparent und für den Nutzer ist keine Beeinflussung feststellbar.

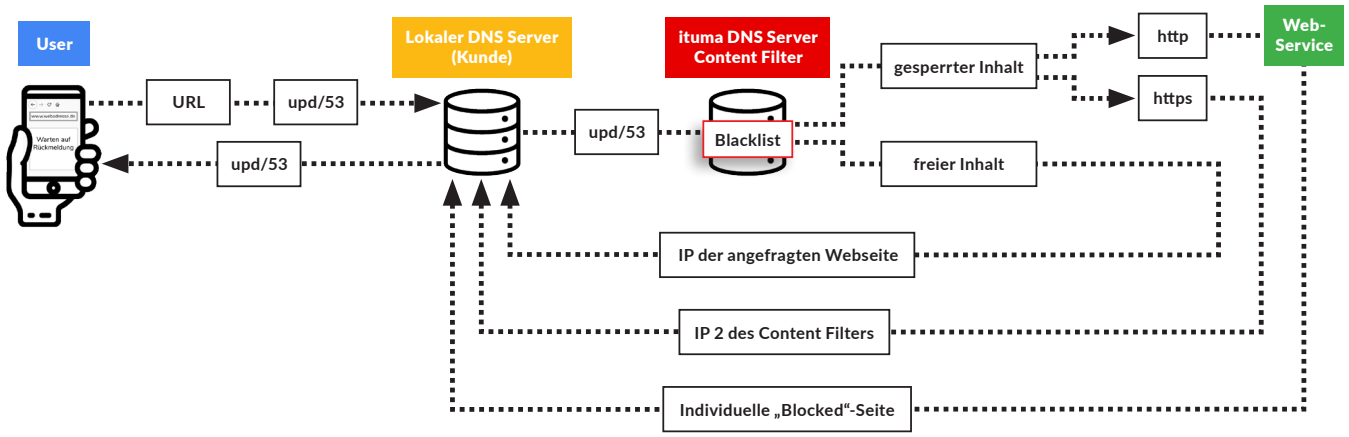
Sofern jedoch der Domainname aufgrund von unerwünschtem Inhalt in der Liste geführt wird, ist der Einfluss des Content Filters für den Nutzer abhängig von der Applikation und dem angefragten Dienst:

- Wenn vom Nutzer eine http-Adresse angefragt wurde, kann eine individuell gestaltete Rückgabeseite eingesetzt werden.
- Bei Anfrage einer https-Adresse erhält der Nutzer entweder
  - nach einer von seinem Endgerät abhängigen Zeitspanne eine Timeout-Meldung (wenn vom Server die IP-Adresse des DNS-Servers zurückgesandt wurde)

  oder
  - eine von seinem Endgerät abhängige Meldung, dass die Verbindung nicht hergestellt werden konnte (wenn vom Server eine fiktive IP-Adresse zurückgesandt wurde).

Die Verzögerung mit/ohne Filter bewegt sich im Millisekundenbereich (~20ms → ~50ms).

Beispiel: Konfiguration mit Kunden-Gateway



Der Content Filter besitzt eine zweite IP. Auf dieser werden alle Anfragen mit gesperrtem Inhalt direkt beendet. Dadurch laufen die Anwendungen auf dem Client schnell in einen Timeout und eine entsprechende Meldung wird beim User angezeigt. Parallel läuft ein Webservice, durch den für HTTP Anfragen eine individuelle Nachricht anzeigt werden kann.

Kleinhülsen 29 | 40721 Hilden | Germany
E-Mail: kontakt@ituma.eu | Tel: +49 2103 280 99 0