OctoGate

Content-Filter

Kinder- und Jugendschutz
Filter in Perfektion

OctoGate
EINFACH. SICHER. GESCHÜTZT.

Stand: 04/2016

OctoGate Whitepaper

OctoGate IT Security Systems GmbH
Technologiepark 32
33100 Paderborn

Tel.: +49 5251 18040 0
Fax: +49 5251 18040 39
Email: info@octogate.de
Internet: http://www.octogate.de

Verantwortlicher für den Inhalt: Frank Menne

OctoGate
EINFACH. SICHER. GESCHÜTZT.

Inhalt

OctoGate
EINFACH. SICHER. GESCHÜTZT.

1 OctoGate Content-Filter

OctoGate bietet Unternehmen mit dem Content-Filter eine Lösung bei der die Vorteile klar auf der Hand liegen:

- Vorhaltung von ca. 60 Mio. URLs
- Tägliche automatische Aktualisierung
- Speicherung in einer integrierten SQL Datenbank
- Einfache Auswahl durch 24 verfügbare Kategorien

Thema im Fokus

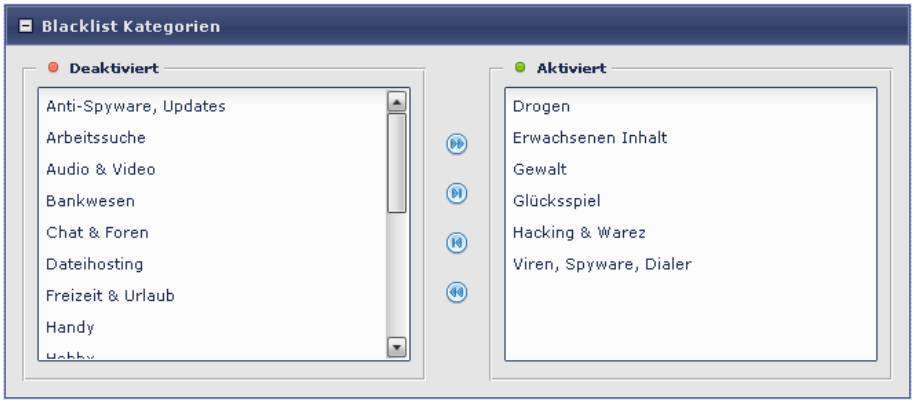
Die Kategorien enthalten zu den Themen zusammengefasste Listen von URLs, welche Sie in der Weboberfläche auswählen können, um den Zugriff auf Internetseiten zu sperren oder freizugeben. Ergänzt werden diese durch manuell definierbare Black- und Whitelisten.

Sie erhalten somit eine einfach zu bedienende Lösung um Inhalte nach Themen sortiert zu filtern oder freizugeben und Ihre individuellen Bedürfnisse zu berücksichtigen. So ist es Ihnen z.B. möglich alle Suchmaschinen zu blockieren und nur die eine von Ihnen gewünschte zu erlauben.

Sie können Filterprofile erzeugen mit denen es Ihnen ermöglicht wird diese Regeln einzelnen Benutzern oder Gruppen zuzuweisen und durch die Nutzung von Pausenfiltern zeitbasiert anzuwenden oder Ausnahmen zu definieren.

1.1 Vorhandene Kategorien

Anti-Spyware/Updates, Arbeitssuche, Audio & Video, Bankwesen, Chat & Foren, Dateihosting, Drogen, Erwachsenen Inhalt, Freizeit & Urlaub, Gewalt, Glücksspiel, Hacking & Warez, Handy, Hobby, Mail, Nachrichten, Onlineshopping, Religion, soziale Netzwerke, Spiele, Suchmaschinen, Viren/Spyware/Dialer, Werbung und Wissenschaft.



OctoGate Content-Filter

Kategorienliste

Kategorie	Beschreibung
Anti-Spyware, Updates	o Software Downloads o Dateidownloads o Filesharing Netzwerke o Wallpapers o Remote Access (kein VPN)
Arbeitssuche	o Arbeit suchen o Jobsuche o Stellenangebote o Arbeitnehmersuche
Audio & Video	o Videos o Filme o Audio/Musik o Bands und kategoriebezogene Downloads o Podcasts o Webradio o WebTV
Bankwesen	o Investments o Aktien o Börse o Kredite o Versicherungen o Banken (nicht auf Online Banking beschränkt)
Chat & Foren	o Kennenlernseiten o Partnerschaftssuche o Freunde finden o Chatanbieter o Blogs o Boards und Communities zu diversen Themen
Dateihosting	o Dateihosting Services
Drogen	o Herstellung von Bier, Wein und Spirituosen o Seiten von Brauereien, Weinkellereien und Brennereien o Drogen (legale und nicht legal) o Tabak sowie Viagra und ähnliche Substanzen
Freizeit & Urlaub	o Humor o Witzige Seiten o Satire o Themen zur Hauseinrichtung o Garten o Pflanzen o Möbel o Dekoration o Wellness

OctoGate Content-Filter

Kategorienliste

Gewalt	o Abstoßend o Extrem blutig o Anleitung oder Aufruf zu Mord o Selbstmord und Gewalt o Ekelerregend o Waffen o Militärische Inhalte o Rassismus und Volksverhetzung o Martial Arts, Kung Fu, Taek won do („aggressive“ Sportarten)
Erwachsenen Inhalt	o Pornographische oder vorwiegend sexuelle Inhalte o Jugend- und Kinderschutz nach deutscher BPjM o Modelagenturen o Model Fan Pages
Glücksspiel	o Gewinnspiele o Lotto o Glücksspiele
Hacking & Warez	o Hacking o Ratgeber zum Thema Hacking o Lizenzverletzende Internetseites o Malware Anleitungen o Systeme überlisten o Abofallen o Dynamische Internetseiten
Handy	o Klingeltöne o Apps o Mobiltelefonhersteller
Hobby	o Sport jeglicher Art o Google o Image Hosting o Haus und Garten o Ratgeber (Kochen, Garten, Pflanzen, Tiere) o Fanseiten o Innenarchitektur o Wohneinrichtungen und ähnliche Kategorien o Clubs und Vereine o Reisen o Buchungsdienste o Reiseinfos o Hersteller von Rollern, Booten, Fahr- und Flugzeugen (inkl. Helikopter)

OctoGate Content-Filter

Kategorienliste

Mail	o E-Mail Anbieter o Webmail
Nachrichten	o News o Nachrichten o Tagesthemen o Prominews o Branchennews
Onlineshopping	o Shoppingseiten o Internet Auktionen o Kleinanzeigen
Religion	o Verschwörungstheorien o Religion o Kult o Okkulte
Soziale Netzwerke	o Soziale Netzwerke
Spiele	o Spiele zum Download o Online Spiele
Suchmaschinen	o Verzeichnisdienste Internetseites o Suchmaschinen
Viren, Spyware, Dialer	o Anonymisierungsproxies und Listen dieser Rechner o Erkennung von Tor-Netzwerken o URL-Umleitungen
Werbung	o Werbedienste o Werbebanner o Internetseiten-Tracker (Surfanalyse)
Wissenschaft	o Lexika o Nachschlagewerke o Übersetzer o medizinische Einrichtungen o gesammelte Informationen o Astrologie o Esoterik o Horoskope o Ideologie o Schulen o Universitäten o Sexualerziehung

Eine Auszug entsprechender Internetseiten finden Sie auch in unserem OctoGate Handbuch unter Kapitel 12.3 Content-Filter-Kategorien

2 Badwords-Filter

Analyse & Prophylaxe

Lassen Sie die OctoGate eine Inhaltsanalyse von aufgerufenen Internetseiten durchführen und auf Basis einer Badwords-Liste filtern:

Sie können einen Schwellwert definieren und eine Liste mit "schmutzigen" Worten denen Sie einen Wert von 1-9 zuweisen. Übersteigt die Summe der Werte der auf einer Internetseite gefundenen schmutzigen Worte den Schwellwert, wird die Internetseite gesperrt. Wir liefern Ihnen eine umfangreiche Liste mit im Alltag bewährten Inhalten als Vorgabe mit.

2.1 SafeSearch

Machen Sie schon im Vorfeld die Suchergebnisse sicherer, indem Sie die OctoGate den **SafeSearch** Filter gängiger Suchmaschinen erzwingen lassen, um anstößige Inhalte gar nicht erst aufzufinden.

3 ICAP

Internet **C**ontent **A**daptation **P**rotocol (ICAP) ist ein Protokoll zur einfachen Weiterleitung von Inhalten für **HTTP**, **HTTPS** und **FTP**-basierte Dienste

Ein ICAP-Client ist im Normalfall ein Proxy, der HTTP(S)/FTP-Anfragen von einem Browser entgegennimmt. Die Daten werden zu einem ICAP-Server gesendet, um dort bearbeitet zu werden. Diese Bearbeitung kann eine Überprüfung der angeforderten Internetseite, ein Virenscan oder ähnliches sein. Der Server sendet eine Antwort zurück, die dann über den ICAP-Client zurück zum Browser geht und dort angezeigt wird.

Für die Weiterleitung werden die HTTP(S)/FTP-Daten in ein ICAP-Paket verpackt und an den Server weitergeleitet. Es wird bei der Weiterleitung zwischen zwei Modi unterschieden. Für die Anfragen gibt es reqmod (Request modification) und für den Inhalt respmod (Response modification). Diese Unterscheidung ermöglicht es beispielsweise Content-Filtern, neben dem Blockieren von nicht gewünschten Anfragen auch noch Bandbreite zu sparen. Anfragen, die bereits im reqmod blockiert werden, verursachen kein weiteres Laden von Internetinhalten, wodurch Bandbreite gespart wird.

Quelle: https://de.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol

4 Virenschutz

Die OctoGate prüft sämtlichen ein- und ausgehenden Datenverkehr auf schädlichen Inhalt. Viren-, Trojaner- und Dialer-Erkennung erfolgt bereits beim Download. Eine mögliche Gefahrenquelle bleibt jedoch bestehen: Durch Wechselspeichermedien wie USB-Sticks, SD-Karten oder externe Laufwerke können Viren an der OctoGate vorbei in das interne Netzwerk gelangen.

Aus diesem Grund bietet Ihnen die OctoGate einen zusätzlichen Virenscanner für alle an ihr angeschlossenen PCs. Dieser Virenscanner lässt sich zentral über die Administrationsoberfläche der OctoGate für alle PCs konfigurieren und bietet die Möglichkeit Wechselspeichermedien zu sperren (ein so genanntes „Device Lock“).

5 HTTPS-Filterung

Scanning SSL-Daten

Web Server haben die Notwendigkeit, die Daten von und zu Clients zu sichern, typischerweise Daten wie z.B. Passwörter, Formulare für persönliche Information wie Bankeingaben etc.

Internetseiten können Datenverschlüsselung unter Verwendung von SSL-Zertifikate ausnutzen. Wenn eine URL mit „https“ anstatt von „http“ beginnt, werden diese Daten nach und von dem Endbenutzer verschlüsselt.

Das bedeutet, dass übermittelte Daten verschlüsselt übertragen werden und der Zugriff unbefugter Personen weitestgehend unterbunden wird. Wenn die Daten an seinem Bestimmungsort ankommen werden diese schließlich entschlüsselt.

Dennoch ist es heute notwendig diese Inhalte ebenfalls nach böswilligen Bedrohungen oder Datenlecks zu scannen. Hiermit sind auch Internetseiten gemeint, die sich fälscherweise als vermeintlich bekannte Internetbankseiten ausgeben.

Auch beim verschlüsselten Datenverkehr können böswillige Inhalte enthalten sein, so dass ein Endbenutzer möglicherweise vertrauliche Information über einen vermeintlich verschlüsselten Kanal sendet. Hierbei besteht das Problem, dass dieser Inhalt nicht gescannt werden kann, da dieser verschlüsselt übertragen wird.

Jedoch können wir unter Verwendung einer sog. „man-in-the-middle“ Funktion diesen Datenverkehr ebenfalls nach böswilligen Inhalten scannen. Mithilfe eines SSL-Zertifikats können wir ein Vertrauensverhältnis zwischen dem Client schaffen und die Verbindung zur aufgerufenen Internetseite herstellen. Dadurch ist der Scanner in der Lage Inhalte zu entschlüsseln, zu scannen und wieder zu verschlüsseln.

5.1 Funktionsweise

Abbildung 1: "Man-In-The-Middle"

Eine Client-Verbindung zu einer sicheren HTTPS-Seite wird abgefangen und durch eine SSL-Gateway Content Inspection Firewall umgeleitet.

Diese Gateway-Firewall sendet sein Zertifikat zusammen mit seinen öffentlichen Schlüssel an den Client. Der Kunde muss diesem Zertifikat vertrauen. Das kann manuell vom Client erfolgen, indem das Zertifikat in der "**Trusted Root Certification Authorities**" installiert wird, oder für alle Clients mithilfe von Active Directory-Gruppenrichtlinien.

Dadurch kann die Gateway-Firewall eine Verbindung zur aufgerufenen Internetseite herstellen und leitet den Datenverkehr, nach eingehender Prüfung der Inhalte, dem Client weiter.

Hinweis: Wenn der Client diesem Zertifikat nicht vertraut, entstehen sog. Zertifikatfehler, da die Zertifikate selbstsigniert sind und nicht von einer bekannten CA (Zertifizierungsinstanz) signiert wurden. Entsprechend zeigen die gängigen Browser beim Aufrufen solcher Internetseiten Warnhinweise an. Zwar ist die Verbindung verschlüsselt, aber mangels Authentifizierung ist unklar, mit wem die (verschlüsselten) Daten austauscht werden.

5.2 Let's Encrypt

Let's Encrypt (englisch, „Lasst uns verschlüsseln") ist eine Zertifizierungsstelle, die Ende 2015 in Betrieb gegangen ist und kostenlose X.509-Zertifikate für Transport Layer Security (TLS) anbietet. Dabei ersetzt ein automatisierter Prozess die bisher gängigen komplexen händischen Vorgänge bei der Erstellung, Validierung, Signierung, Einrichtung und Erneuerung von Zertifikaten für verschlüsselte Internetseiten.

Ziel des Projekts ist es, verschlüsselte Verbindungen im „World Wide Web" zum Normalfall zu machen. Indem unter anderem Zahlung, Webserverkonfiguration, Validierungs-E-Mails und die Sorge um abgelaufene Zertifikate überflüssig werden, sollen Aufwand für Einrichtung und Pflege von TLS-Verschlüsselung deutlich gesenkt werden

Beteiligte

Let's Encrypt ist ein von der gemeinnützigen Internet Security Research Group (ISRG) angebotener Dienst.

Hauptsponsoren sind die Electronic Frontier Foundation (EFF), die Mozilla Foundation, Akamai und Cisco Systems. Weitere Beteiligte sind die Zertifizierungsstelle IdenTrust, die University of Michigan (U-M), die Stanford Law School, die Linux Foundation sowie Stephen Kent von Raytheon/BBN Technologies und Alex Polvi von CoreOS.

Quelle: https://de.wikipedia.org/wiki/Let%E2%80%99s_Encrypt

Ausblick

Es ist davon auszugehen, dass im Jahr 2017 bis zu 90 % der derzeitigen „http"-Verbindungen auf „https" umgestellt werden. Dieser Trend zeigt wiederum die Notwendigkeit auf, die Inhalte der entsprechenden Internetseiten ebenfalls analysieren und scannen zu müssen, um zukünftigen Bedrohungen vorzubeugen.