Best Practices
WatchGuard Webblocker – Neue Funktionen, die sie kennen sollten

Agenda

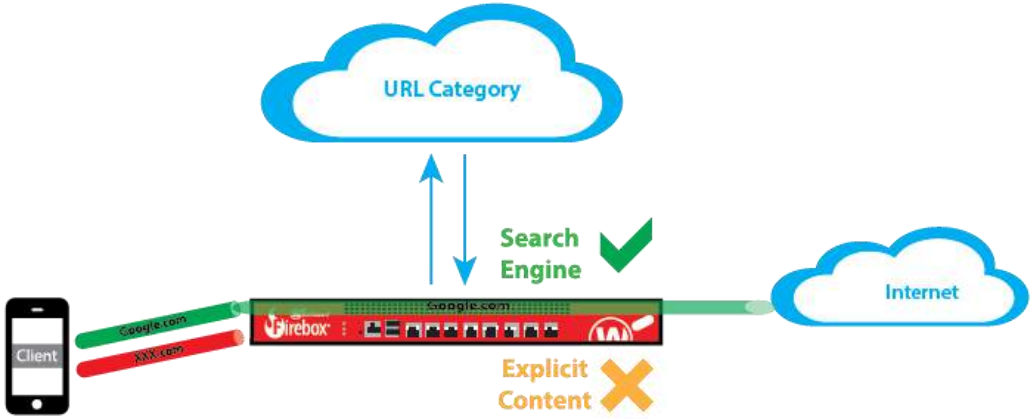
- Grundlegende Funktionsweise des Webblockers
- Verwendung des WatchGuard Webblockers in der WatchGuard Firebox
- Ausflug – Windows Client (!)
- Last, but not least - Demo

Grundlegende Funktionsweise des Webblockers

- **Problemstellung Web-Surfen**
  - Unkontrolliertes Surfen im Internet
    - Verlust von Arbeitszeit
    - Download von nicht gewollten Inhalten
  - Rechtliche Vorgaben
    - Jugendschutz im Arbeitsrecht
    - Geistiges Eigentum / Illegale Inhalte
  - Bedrohungen für interne Infrastruktur
    - Inhalt von Downloads
      - Trojaner
      - Keylogger
      - …

Grundlegende Funktionsweise des Webblockers

- Wenn der Benutzer eine Webseite aufrufen möchte, wird vorher über die Firebox die Datenbank des Webblockers angefragt. Die URL der Webseite wird hochgeladen, mit der Datenbank verglichen und die entsprechende Kategorie zurückgegeben.
- Die Firebox vergleicht den Rückgabewert mit der entsprechenden Richtlinie in der angesprochenen Regel.

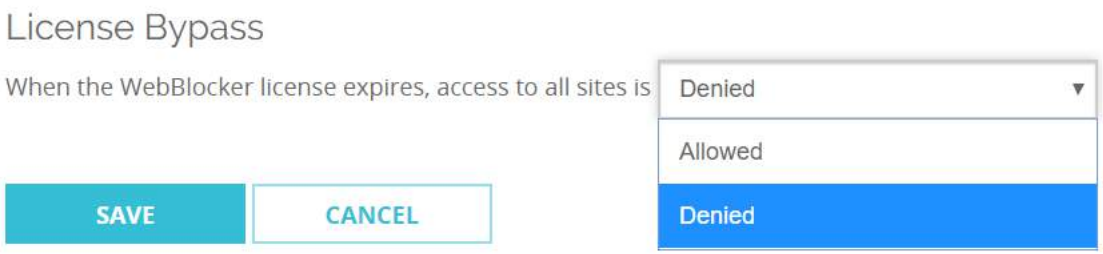


Grundlegende Funktionsweise des Webblockers

- Um den Webblocker-Dienst zu aktivieren, muss *DNS* auf der Firebox konfiguriert werden!
- Wenn keine DNS-Server konfiguriert sind, müssen alle externen Schnittstellen entweder *DHCP oder PPPoE* verwenden.
- Wenn externe Schnittstellen mit einer *statischen IP-Adresse* konfiguriert sind, müssen Sie den DNS-Server manuell konfigurieren, bevor Sie den WatchGuard Webblocker aktivieren können.

Grundlegende Funktionsweise des Webblockers

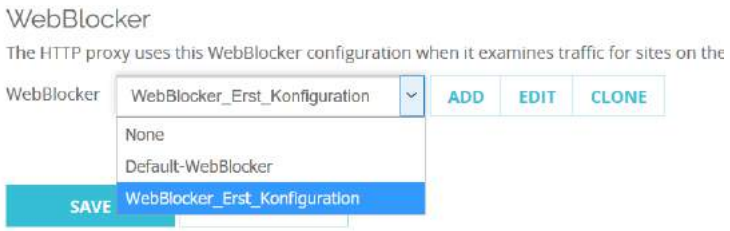
- WatchGuard Webblocker setzt eine gültige Lizenz voraus.
  - Ohne Lizenz wird die Einstellung aus den Webblocker Settings umgesetzt.



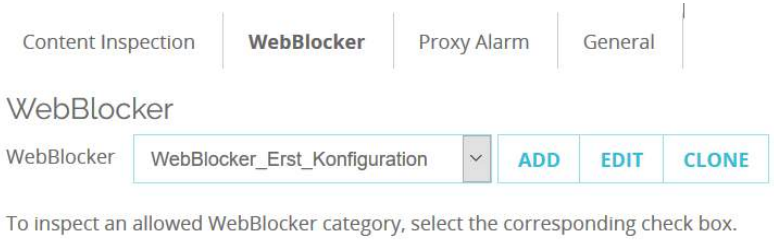
- In *Fireware v11.12 und höher* unterstützt Fireware IPv6 für Proxy-Richtlinien und Abonnementdienste. Webblocker verwendet IPv4 für die Verbindung zum Webblocker Cloud Server. Wenn Ihre Firebox für IPv6 konfiguriert ist und die Webblocker-Konfiguration die Webblocker Cloud für URL-Kategorisierungsnachschlageanforderungen verwendet, müssen Sie das externe Interface sowohl mit einer IPv4- als auch einer IPv6-Adresse konfigurieren.

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- WatchGuard Webblocker ist ein Dienst, der innerhalb des HTTP Proxy eingesetzt wird.
- WatchGuard Webblocker ist auch im HTTPs Proxy auf zweierlei Weise zu verwenden.
  - Innerhalb der zugewiesenen HTTP Proxy Action



  - Als Content Filter Zuweisung im HTTPs Proxy selber



Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- Folgende Aktionen können mit den WatchGuard Webblocker innerhalb des HTTP Proxy Action durchgeführt werden:
  - Allow – Die Webseite wird dargestellt.
  - Deny – Die Webseite wird öffnet sich nicht. Es wird dafür eine Verbots- / Block-Seite dargestellt.
- Seit der *Fireware Version 12.4 oder höher* ist eine weitere Aktion wählbar.
  - Warn - Die Website wird nicht geöffnet. Im Browser wird eine Warnseite angezeigt. Die Benutzer können auswählen, ob sie zur Website wechseln oder zur vorherigen Seite zurückkehren möchten.

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- Des weiteren wurde die Funktion des „Override“ verändert.
- In den Einstellungen der Webblocker Action findet man im Fenster „Categories“ in unteren Bereich die Option „Enable Webblocker Override“.
- Wenn man diese Option auswählt, hat man die Auswahl zwischen zwei möglichen Einstellungen:

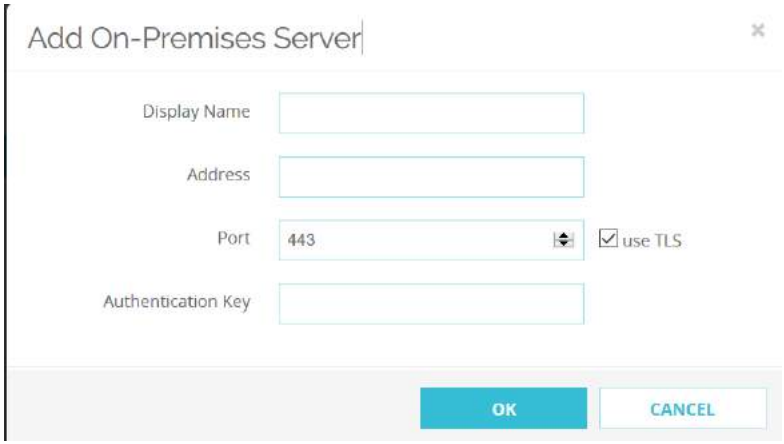
1. *Passphrase* – Erlaubt es, eine Passphrase einzugeben, um die Webblocker-Einstellungen zu überschreiben und Zugriff auf abgelehnte Inhalte zu erhalten.
2. *User Group* – Erlaubt es, die Mitglieder der angegebenen Benutzergruppe sind, die Webblocker-Einstellungen zu überschreiben und Zugriff auf abgelehnte Inhalte zu erhalten.

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- Die Option „Passphrase“ verhält sich genauso, wie die Option „Webblocker local override“ (Advanced Tab) in den Versionen vor Fireware 12.4.
- Bei der Aktivierung der Option „Override“ wird die Richtlinie „WG-Auth-Webblocker“ automatisch erstellt.
- Im der Deny Page (Blockseite) wird ein Bereich eingeblendet, wo der Benutzer die Passphrase oder sein Username und Password eintragen kann.
- Benutzer müssen Firebox-DB oder AD User sein !
- Bei HTTPs muss Content Inspection aktiviert sein, um dies zu ermöglichen. Sonst wird die Webseite geblockt.

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- On-premises Webblocker-Server wird für die Fireware Version 12.2 oder höher angeboten.
- Wenn Sie diese Option auswählen, müssen Sie den On-premises Webblocker-Server auf einer virtuellen VMware- oder Hyper-V-Maschine in Ihrem Netzwerk installieren und die Details zum On-premises Webblocker-Server in den globalen Webblocker-Einstellungen hinzufügen.
- Der On-premises Webblocker-Server ist nicht zu verwechseln mit dem Surfcontrol-Server im WSM!



Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

Global Webblocker Exceptions

- Globale Ausnahmen können von mehreren Webblocker-Actions verwendet werden und eliminieren die Notwendigkeit, dieselben Ausnahmen zu mehreren Actions hinzuzufügen.
- Die globale Ausnahmeliste enthält eine vordefinierte Ausnahme, um Verbindungen zu WatchGuard-Servern zu ermöglichen.
  - In jeder Webblocker-Action geben Sie an, ob die Action die globale Ausnahmeliste prüft.
  - Webblocker prüft immer zuerst die in der Webblocker-Action definierten Ausnahmen.
  - Wenn „Check global exceptions“ markiert ist und eine URL nicht mit den in der Webblocker-Action definierten Ausnahmen übereinstimmt, prüft Webblocker die URL dann gegen die globale Ausnahmeliste.
  - Wenn die URL mit einer globalen Ausnahmeregel übereinstimmt, führt Webblocker die in der Regel definierte Aktion aus.

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- Mit den Webblocker Global Settings können Sie die Cache-Größe und die Dauer der Speicherung von Cache-Einträgen konfigurieren.
- Die maximale Anzahl von Einträgen, die im Webblocker-Cache gespeichert werden können, variiert je nach Gerät und ist nicht konfigurierbar.

WebBlocker Cache Entries	Device Model
8,000	Firebox T10, XTM 2 Series
32,000	Firebox T15, T30, XTM33, XTM330, XTM505, 510, 520, 530
64,000	Firebox T35, T50, T55, T70, Firebox M200, XTM515, 525, 535, 545, XTM810, 820, 830
256,000	Firebox M300, M370, M400, M470, M500, M570, M670, M4600, M5600, XTM1050, XTM2050, XTM850, 860, 870, 1520, 1525, 2520

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

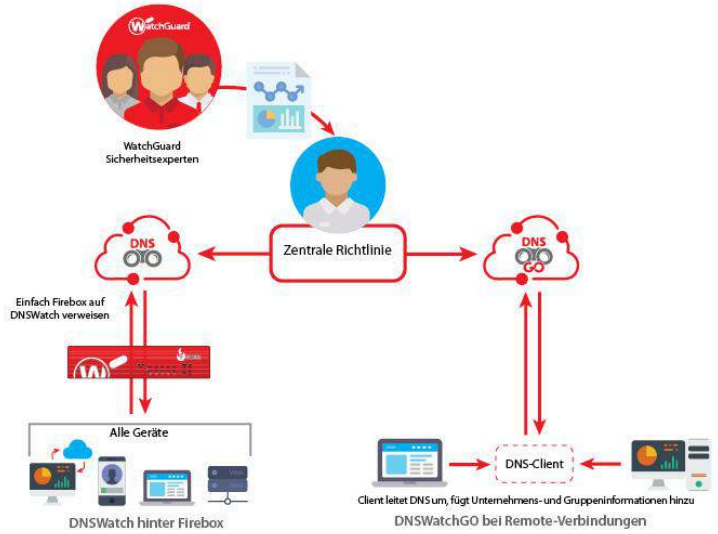
- Best Practice:
  - Um andere Ports als 80 (HTTP) und 443 (HTTPs) zu untersuchen, kann man den WatchGuard Webblocker in einen TCP-UDP Proxy verwenden.
  - Exeptions werden am schnellsten und einfachsten von der WatchGuard Firebox umgesetzt, wenn es sich um „regular expression“ handeln. http://watchguardsupport.force.com/publicKB?type=KBArticle&SFDCID=kA2A00000000EoeKAE&lang=en_US

Verwendung des WatchGuard Webblockers in der WatchGuard Firebox

- Best Practice:
  - Wenn man mehrere Fireboxen verwaltet oder mehr als eine Webblocker-Action auf derselben Firebox konfiguriert hat, können Webblocker-Exeptions von einer Webblocker-Action exportieren und in eine andere Webblocker-Action auf derselben oder einer anderen Firebox importieren werden.
  - In Fireware 12.3 oder höher können auch Webblocker-Exeptions in die und aus der „global exeption list“ in den globalen Webblocker-Einstellungen importieren und exportieren werden. Exeptions können zwischen der globalen Ausnahmeliste und Webblocker-Actions übertragen werden.

Ausflug – Windows Client (!)

- WatchGuard Webblocker wird auch seit neusten in einen anderen WatchGuard Produkt verwendet.
- WatchGuard DNSWatchGo greift als Client Lösung auf die WatchGuard Webblocker Datenbank zu.
- Der Zugriff erfolgt über einen „API call“.
- Die Konfiguration erfolgt über die Cloud.



Demo

Link Sammlung

- Einrichten des On-Premise Webblocker Server

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/webblocker/wb_server_manage_c.html

- Einstellungen von globalen Parameter (z.B. Expetions)

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/webblocker/wb_global_settings_c.html

- Troubleshooting und Best Practice

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/webblocker/webblocker_troubleshoot_c.html

Vielen Dank!