

TrustPort WebFilter

TrustPort WebFilter ist der effektive Weg, Ihren Zugang zum Internet zu verwalten. Das Aufrufen von unerwünschten Webseiten kann blockiert werden, spezielle Webseiten werden nach Prüfung der Inhalte gemäß Ihren Vorgaben individuell behandelt.

Aufzeichnung besuchter Webseiten

Kontrolle des Zugriffs auf unerwünschte Inhalte

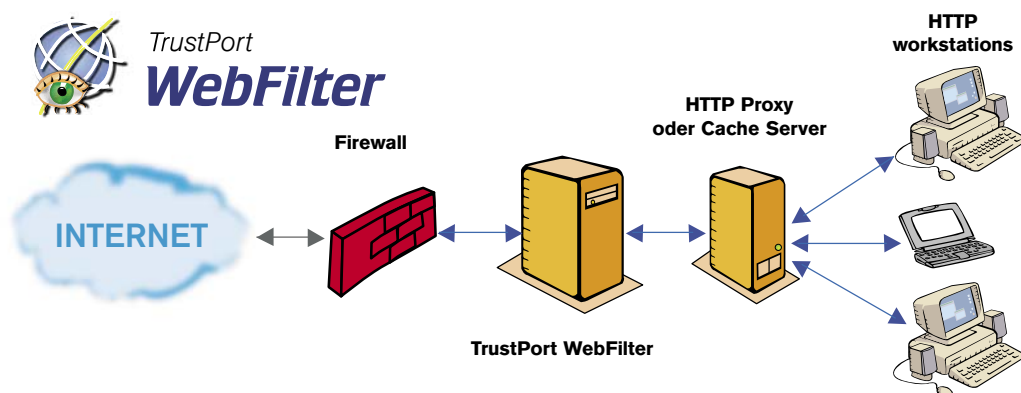
Blockade von verbotenen Webseiten

Überwachen von nicht arbeitsrelevanten Aktivitäten



Effektivere Nutzung der Arbeitszeit
Produktivere Nutzung der Internet Verbindungen

Schutz vor Internet-Schädlingen
Schutz der Firmendaten



Web Filterung = Erhöhung des Sicherheits-Levels = Reduktion von Supportkosten

Die Funktionen von TrustPort WebFilter

Funktionen

- Erlaubt oder blockiert den Zugriff der Nutzer auf speziellen Webseiten.
- Anwenden von White/Black Listen (erlaubte oder blockierte Adressen).
- Einrichten von direktem Zugriff oder Ablehnung ohne Anwendung der Filter für bestimmte Nutzer.
- Zu den verschiedenen Einstellmöglichkeiten des TrustPort Webfilters gehören:

Block – wenn eine Internet Adresse unter Block definiert ist, erfolgt kein Zugriff.

Permit – wenn eine Internet Adresse unter Permit definiert ist, wird die Seite angezeigt (Nützlich für Firmen, die Zugriff nur auf bestimmte Bereiche (Domains) erlauben und andere Inhalte blockieren möchten).

Monitor – die Kategorien der besuchten Webseiten werden permanent angezeigt.

Filter Einstellungen

- **High Level Filter** – Kann den Zugriff auf bestimmte Webseiten verhindern und untersucht den Inhalt der Internet Adresse, pro aufgerufene Seite oder die komplette Domain.
- **Rule Based Filter** – der Standard, wird regelmäßig über automatische Updates aktualisiert.
- **User defined Filter** – Benutzerdefinierter Filter, gibt dem Nutzer die Möglichkeit, exakte Adressen und Domains einzugeben, die blockiert werden sollen. Geeignet für große Datenmengen.
- **Heuristic Filter** – analysiert den Seiteninhalt. Kommt zur Anwendung, wenn keiner der vorher genannten Filter fündig wird. Webseiten oder komplette Orte werden im Inhalt

pro-aktiv analysiert und kategorisiert. Das Resultat wird für künftige Zugriffe gespeichert, um erneute Analysen überflüssig zu machen. Der heuristische Filter kann separat ein- oder ausgeschaltet werden.

- **Time Filter** – arbeitet mit der Standard Funktion, dem User und dem Heuristic Filter, und bietet die Einstellmöglichkeit zwischen aktivem Modus und Monitor (überwachendem, passivem) Modus.

Informationen über Nutzerverhalten

- Verbindungsprotokolle enthalten Kennungen oder Nutzernamen gemäß ihrem autorisierten Zugang.
- TOP 15/Kategorien (die meistbesuchten Seiten pro Kategorie).
- TOP IP/Nutzer pro Kategorie (die meistbenutzten Computer und meist aktiven Nutzer pro individuelle Kategorie).

Beispiele für die Kategorien der angezeigten Informationen

- Diskussionsgruppen.
- Dating Seiten.
- Filme, Musik, und andere Multimedia Inhalte.
- Aggressive oder gewalttätige Inhalte.
- Sexuelle Inhalte.
- Server mit Inhalten, welche gegen Urheberrecht verstoßen.

Weitere Angebote

- Monitoring und Reporting können über eine Vereinbarung erweitert werden.
- Bei Bedarf kann die Applikation auf die speziellen Anforderungen des Kunden zugeschnitten werden.
- Das Produkt kann ausgegliedert über Fernwartung von TrustPort konfiguriert, bedient und gemanagt werden.
- Ergänzender Schutz Ihres Systems, kann einfach durch die voll kompatiblen Antivirus und Antispam Module von TrustPort ergänzt werden.



Systemanforderungen

Server – Minimale Anforderungen

- Windows 2000, Windows 2003 Server, Windows 2008 Server.
- Internet Explorer 6 oder höher.
- Pentium IV oder höher.
- 1024 MB RAM, mehr Speicher erhöht die Performance.
- 10 GB freier Festplattenspeicher.
- Ein Server, wo die Applikation installiert werden kann.

Client – Minimale Anforderungen

(funktionierender Internet Browser)

- Internet Explorer 6 oder höher.
- Mozilla 1.6 oder höher.
- FireFox 2.0 oder höher.