

## Secure Content Management: Sicherheit und Effizienz für moderne Unternehmensnetzwerke

*Themen: Der Bedarf an sicheren Inhalten,  
aktuelle technologische Entwicklungen,  
Lösungsalternativen und  
Anwendungsbeispiele*

### INHALT

Die Bedeutung von Secure Content Management	2
- Unbegrenzter Zugriff	
- Die Risiken	
So funktionieren Secure Content Management- Lösungen	4
- Site Blocking im Vergleich zu Content- Monitoring	
- Lösungsarchitekturen	
Evaluierung der Lösungen	6
- Integration von Content Management und Firewalls	
- Standalone-Appliances	
- Wichtige Funktionen und Vorteile	
Anwendungsbeispiele	12
- Kleine Unternehmen	
- Mittlere Unternehmen	
Resümee	13

*Egal, ob es sich um kleine Firmen oder um große globale Organisationen handelt – immer mehr Unternehmen verlassen sich heute auf das Internet, um rasch und unkompliziert auf Informationen und Ressourcen zuzugreifen. Doch angesichts der Risiken, die auf ihre internen Netzwerke und Daten lauern, stehen diese Unternehmen vor einer Vielzahl enormer Herausforderungen. Diese Risiken können in unterschiedliche Kategorien unterteilt werden. Hierzu zählen Angriffe auf Daten und Netzwerke sowie der Missbrauch von Ressourcen durch autorisierte Benutzer. Außerdem gilt es, das Netzwerk effizient zu verwalten und rechtlichen Problemen vorzubeugen, die sich daraus ergeben können, dass Benutzer am Arbeitsplatz mit ungeeigneten Inhalten konfrontiert werden. Einige Bedrohungen fallen gleichzeitig unter mehrere Kategorien. Dies gilt beispielsweise für Viren, Phishing-Programme, Spyware und andere externe Bedrohungen, die Netzwerk-Administratoren zusätzliche Arbeit bereiten, unnötig Bandbreite beanspruchen und rechtliche Probleme verursachen können. Auch eine missbräuchliche Nutzung von Instant Messaging- und Peer-to-Peer-Anwendungen kann zu Problemen führen und die Produktivität beeinträchtigen.*

*Das vorliegende Whitepaper behandelt neue Technologien, mit denen sich der Zugriff auf Netzwerkressourcen steuern lässt. Daneben wird Content Filtering mit alternativen Methoden zum Sperren bestimmter Websites verglichen und es werden umfassende Secure Content Management-Architekturen vorgestellt. Für Benutzer, die sich für Content Management-Lösungen interessieren, vergleicht dieses Dokument integrierte Lösungen mit Standalone-Appliances und beschreibt wichtige Funktionen für beide Optionen. Anwendungsbeispiele machen deutlich, welche Vorteile ein Secure Content Management-System unterschiedlichen Organisationen zu bieten hat. Parallel dazu werden die Anforderungen von Unternehmen im Hinblick auf Netzwerkschutz, Produktivität, Administration und rechtliche Haftungsspflichten erläutert.*

*Die im Whitepaper behandelten Informationen geben die gesammelten Erfahrungen des SonicWALL® Research & Development Teams wieder und sollen aufzeigen, in welchen Anwendungsbereichen sich die SonicWALL Secure Content Management-Lösungen sinnvoll einsetzen lassen. Die SonicWALL-Lösungen, die im Schlussabschnitt aufgeführt sind, werden auf der SonicWALL-Website detailliert beschrieben: <http://www.sonicwall.com>.*

## Die Bedeutung von Secure Content Management

### Unbeschränkter Zugriff

Mit der zunehmenden Nutzung des Internets erhöhen sich auch die Risiken des unkontrollierten Zugriffs auf Websites. Wenn Mitarbeiter bewusst oder unabsichtlich Websites mit ungeeigneten, illegalen oder gefährlichen Inhalten aufrufen, leidet darunter nicht nur die Produktivität – es können auch rechtliche Probleme auftreten. Darüber hinaus kann die Netzwerk-Performance beeinträchtigt werden, was sich negativ auf das Geschäft auswirken kann. Auch zunehmende Sicherheitsrisiken wie Trojaner und Würmer können die Geschäftsabläufe empfindlich stören.

### Die Risiken

#### Produktivitätsverluste bei Mitarbeitern

Durch Sperren des Zugangs auf ungeeignete Websites können Unternehmen übermäßiges privates Surfen im Internet verhindern und Bandbreite sparen. Eine Umfrage von SonicWALL und dem Partnerunternehmen Cerberian<sup>1</sup> hat ergeben, dass von den befragten Mitarbeitern:

---

<sup>1</sup> 2004 Umfrage zur Internetnutzung von Cerberian und SonicWALL vom 26. Mai 2004 (Cerberian ist ein Anbieter von Application Services und URL-Filtering-Lösungen)

- 16 % mindestens einmal am Arbeitsplatz bewusst Websites mit pornografischen Inhalten aufgerufen haben
- 40 % Kollegen beim Surfen auf Websites mit pornografischen Inhalten beobachtet haben
- 32 % Kollegen beim Aufrufen von Glücksspiel-Websites beobachtet haben
- 91 % Kollegen beim Online-Shopping beobachtet haben
- 85 % Kollegen beim Surfen auf Sport-Websites beobachtet haben
- 55 % mehr als 10 % der Arbeitszeit mit privatem Surfen verbringen, also ca. vier Stunden pro Woche oder auf das Jahr gesehen rund 9 Arbeitstage (siehe Abb. 1).

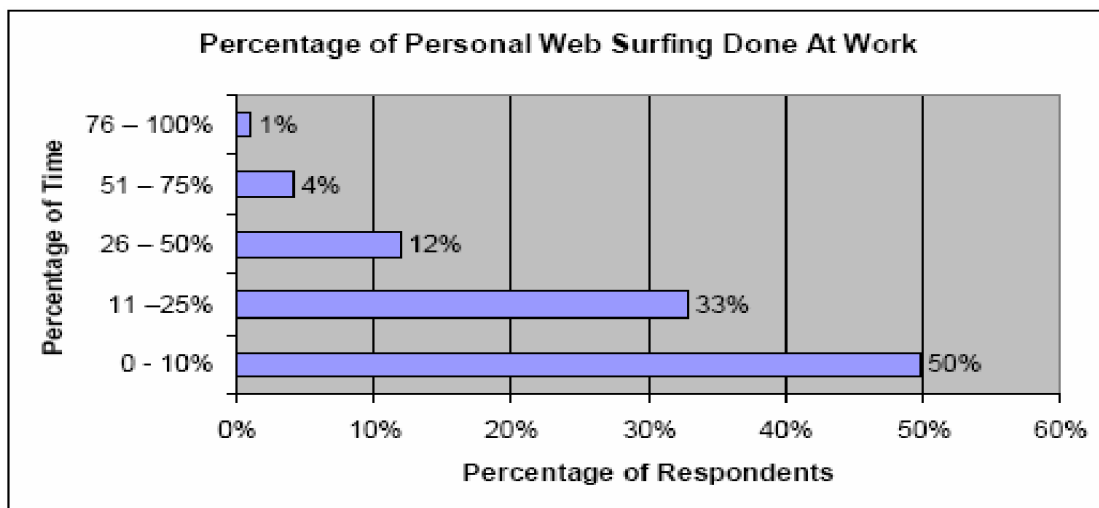


Abb. 1. Anteil der mit privatem Surfen am Arbeitsplatz verbrachten Zeit (Quelle: SonicWALL und Cerberian)

### Rechtliche Risiken

Mitarbeiter, die Websites mit Inhalten wie Pornografie oder Gewalt bzw. Sites mit verhetzenden Inhalten aufrufen, können schwerwiegende rechtliche Probleme verursachen. Im Rahmen einer Studie der Employment Law Alliance (ELA) aus dem Jahr 2004 gaben 24 % der befragten Mitarbeiter an, dass sie oder ihre Kollegen am Arbeitsplatz pornografische Websites besuchen, an Sex-Chats teilnehmen oder anderen Aktivitäten in Verbindung mit Sex im Internet nachgehen.<sup>2</sup> Unternehmen müssen sich deshalb vor rechtlichen Problemen schützen, die z.B. dadurch entstehen können, dass Mitarbeiter wiederholt mit anstößigen Inhalten auf den Computern von Kollegen oder in ihrem Arbeitsumfeld konfrontiert werden.

Auch Peer-to-Peer-Netzwerke und File Sharing bergen Haftungsrisiken. So kann es etwa zu folgenschweren Klagen aufgrund von Urheberrechtsverletzungen kommen. Die Recording Industry Association of America (RIAA) bekam vor kurzem eine Million Dollar Schadensersatz von einer Organisation zugesprochen, bei der urheberrechtlich geschützte Musikdateien im Unternehmensnetzwerk gefunden

<sup>2</sup> "Sex in the Workplace," Employment Law Alliance, Steve Hirschfeld, Februar 2004

wurden.<sup>3</sup> Wenn Mitarbeiter über das Firmennetzwerk illegal Musikdateien oder Filme herunterladen, können Unternehmen wegen Urheberrechtsverletzung zur Verantwortung gezogen werden.

### Hacker-Angriffe und Datenschutzverletzungen

Instant Messaging, Peer-to-Peer-File Sharing und Multimedia-Downloads machen Unternehmen anfällig für Backdoor-Angriffe. Nach Angaben des IT-Sicherheitsunternehmens TruSecure, enthielten 45 % der kostenlosen Dateien, die über die Tauschbörse Kazaa heruntergeladen wurden, Viren, Trojaner oder Backdoor-Programme.<sup>4</sup> Die neueste Bedrohung stellen über Instant Messaging und Peer-to-Peer-Netzwerke verbreitete Viren dar, bei denen Benutzer dazu aufgefordert werden, mit Malware infizierte JPEG-Bilder herunterzuladen und anzusehen.<sup>5</sup> Außerdem können Dateien, die automatisch heruntergeladen werden, wie beispielsweise Java-Applets und ActiveX-Skripte, Datenschutzverletzungen ermöglichen. Mithilfe dieser Skripte lesen Hacker Cookies, die beim Besuch von Websites auf den Desktop-Computern von Mitarbeitern abgelegt wurden. Cookies können persönliche Informationen über Mitarbeiter, wie beispielsweise Surfverhalten oder Kaufgewohnheiten, offen legen.

## So funktionieren Secure Content Management-Lösungen

Content Security-Lösungen steuern den Zugriff auf bestimmte Websites anhand von klar definierten Kriterien. Dabei wird der Internetzugriff per URL-Adresse oder Content-Kategorie (wie beispielsweise Sex oder Glücksspiel) überwacht. Einfache Content Management-Lösungen können feststellen, wie Inhalte übermittelt werden (beispielsweise über Java-Applets oder ActiveX-Skripte) und entsprechende Zugriffsberechtigungen festlegen. Mit komplexeren Content Management-Lösungen lassen sich auch Anwendungen wie Instant Messaging und Peer-to-Peer-Services sperren.

### Site Blocking im Vergleich zu Content-Monitoring

Secure Content Management-Lösungen steuern die Internetnutzung indem sie entweder Websites sperren oder bestimmte Web-Inhalte überwachen. Obwohl sich diese Methoden deutlich voneinander unterscheiden, basieren beide auf der Pass-Through-Filtering-Technologie, d.h. alle angeforderten Websites müssen Internetkontrollpunkte, wie beispielsweise Firewalls, Proxy-Server oder Caching-Appliances passieren. Das Gerät prüft dann jede Anfrage und stellt fest, ob sie zugelassen oder ob sie den Unternehmensregeln entsprechend abgewiesen werden soll.

### Site blocking

Beim Site Blocking werden Websites mithilfe von Filtern, die auf Listen oder URLs basieren, identifiziert und gegebenenfalls gesperrt. Einige Lösungen arbeiten mit so genannten Weißen Listen, die nur Websites zulassen, die in der Liste aufgeführt sind. Ein Einzelhandelsunternehmen könnte beispielsweise eine Weiße Liste erstellen, die neben der Firmenwebsite nur einschlägige Websites mit Informationen zum Versand oder zu Lieferanten enthält. Andere Lösungen arbeiten mit Schwarzen Listen, die den Zugriff auf alle Websites mit Ausnahme der in der Liste genannten Sites zulassen. Schwarze Listen werden von Unternehmen bevorzugt, deren Mitarbeiter einen umfangreicheren Zugriff benötigen. Bei dieser Methode wird die URL-Datenbank in Kategorien, wie beispielsweise "Gewalt" oder "Drogen", eingeteilt, so dass Netzwerk-Administratoren bestimmte Kategorien gezielt sperren können.

Wie effektiv Site Blocking ist und wie gut es sich verwalten lässt, hängt von verschiedenen Faktoren ab:

---

<sup>3</sup> *Electronic Musician*, April 2002

<sup>4</sup> "2003/2004 Trends and Predictions in Network Security", *TruSecure*, Dezember 2003

<sup>5</sup> "FaceTime Warns Enterprises of New JPEG Virus Propagating Via Instant Messaging and Peer-to-Peer Networks", *FaceTime Communications*, September 2004

- **Größe der Datenbank.** Je nach Größe der Datenbank können unterschiedlich viele Websites indiziert, bzw. in die Liste aufgenommen werden.
- **Häufigkeit der Aktualisierung.** Es entstehen ständig neue Sites, und viele bestehende Sites wechseln regelmäßig die URL-Adressen. Die meisten Site Blocking-Lösungen aktualisieren ihre Datenbanken täglich und laden jeden Abend automatisch neue URLs herunter.
- **Einteilung in Kategorien.** Bei der Definitionen von Kategorien muss sehr sorgfältig vorgegangen werden: Sie müssen fein genug abgestuft sein, um den Zugang zu bestimmten Websites effektiv zu unterbinden und gleichzeitig den Zugriff auf zulässige Sites nicht zu blockieren.

Eine grundlegende Einschränkung von Site Blocking besteht darin, dass die Methode ausschließlich auf HTTP-basierten Internet-Verkehr abzielt. Instant Messaging, E-Mail-Anhänge, Peer-to-Peer-Anwendungen und andere Applikationen, die ebenfalls Sicherheitsgefahren enthalten können, werden nicht berücksichtigt.

### Content Monitoring

Die einfachste Methode bei der Überwachung von Webinhalten funktioniert über das Sperren von Stichwörtern. Hier werden keine URLs gesperrt, stattdessen wird der eingegebene Text mit einer benutzerdefinierten Liste an Wörtern und Wendungen verglichen. Stimmt der Text mit den gesperrten Wörtern oder Wendungen überein, filtert oder blockiert die Lösung die Daten oder beendet unter bestimmten Umständen sogar die Anwendung. Ein Nachteil dieser Methode ist, dass eigentlich unproblematische Seiten möglicherweise gesperrt werden, weil sie eines oder mehrere der indizierten Wörter enthalten. So könnte beispielsweise eine Website zum Thema Brustkrebs gesperrt werden, weil sie das Wort "Busen" enthält.

Komplexere Content Monitoring-Lösungen analysieren nicht nur einzelne Wörter auf einer Website, sondern prüfen auch den Kontext und andere Daten, wie beispielsweise HTML-Tags. Mit diesen Informationen können erweiterte Content Monitoring-Lösungen Websites genauer analysieren und besser unterscheiden, ob Inhalte gesperrt werden sollen oder nicht.

Content Monitoring bietet außerdem den Vorteil, dass damit nicht nur Websites überwacht und gefiltert werden können, sondern auch Inhalte, die über Chatrooms, Instant Messaging, E-Mail-Anhänge und Windows-Anwendungen übermittelt werden.

### Lösungsarchitekturen

Content Management-Software kann in Netzwerk-Geräte wie beispielsweise einen Proxy-Server, eine Caching-Appliance oder eine Firewall integriert werden oder auf einem speziellen Microsoft Windows-, Linux-, oder UNIX-Server integriert werden. Die drei gängigsten Methoden unterscheiden sich hinsichtlich der Effizienz, der Kosten und des Verwaltungsaufwands.

#### Client-Lösungen

Client-Lösungen werden auf dem Desktop installiert und sind am besten für die private Nutzung in Kombination mit einer Kinderschutzsoftware geeignet. Client-Software-Lösungen enthalten eine Management-Oberfläche und eine Datenbank mit gesperrten Websites. Die Datenbank-Updates können von den Eltern über das Internet heruntergeladen werden. Zu den führenden Anbietern von Client-Lösungen gehören Zone Labs, Net Nanny® und Internetdiensteanbieter wie Microsoft® MSN und AOL®.

#### Standalone-Lösungen

Standalone-Lösungen bestehen aus dedizierten Datenbank-Servern für die Definition von Regeln sowie aus einem separaten Gateway oder einer Firewall, die für die Einhaltung der Content Management-Regeln zuständig ist. Eine solche Lösung lässt sich leichter verwalten als eine clientbasierte Lösung, weil Regeln

nur einmal definieren werden müssen und anschließend auf allen Desktops angewendet werden können. Bei den meisten Standalone-Lösungen müssen jedoch zusätzlich zur Content Management-Software noch zwei separate Hardware-Geräte gekauft und verwaltet werden. Außerdem muss je nach Bedarf zusätzlicher Speicher angeschafft werden, wenn der verfügbare Speicherplatz für die Regel-Datenbank nicht mehr ausreicht. Zu den führenden Anbietern von Standalone-Lösungen gehören SonicWALL®, Websense und SurfControl®.

### Integrierte Lösungen

Integrierte Lösungen kombinieren Verwaltungs- und Verarbeitungsfunktionen in einem einzigen Gateway oder einer Firewall; dadurch lassen sich die Ausgaben für Anschaffung und laufenden Betrieb senken. Wird das Gateway oder die Firewall allerdings gleichzeitig für Antiviren- und Intrusion Prevention-Services verwendet, kann dies die Leistung beeinträchtigen. Zu den wichtigsten Anbietern von integrierten Content Filtering-Lösungen gehören SonicWALL®, Symantec™ und WatchGuard®.

## Evaluierung der Lösungen

Je nachdem, welche Anforderungen an die Sicherheitsfunktionen, die Performance und die Verwaltbarkeit der Lösung gestellt werden, sollten sich Geschäftskunden zwischen einer integrierten Lösung und einer Standalone-Appliance entscheiden. Beide Alternativen können Internet Content Management mit Funktionen zum Schutz vor dynamischen Bedrohungen kombinieren und so das Netzwerk vor Viren, Spyware, Würmern, Instant Messaging und Peer-to-Peer-Anwendungen schützen.

Standalone- und integrierte Lösungen basieren gleichermaßen auf einer Rating-Architektur sowie einer Datenbank mit Millionen von bewerteten Websites und Domänen. Versucht ein Benutzer auf eine Website zuzugreifen, wird geprüft, ob die URL in der Master Rating-Datenbank aufgeführt ist. Die Datenbanken können vom Anbieter der Content Filtering-Lösung verwaltet und an mehreren Standorten zur Verfügung gestellt werden, um eine effiziente Performance und hohe Verfügbarkeit zu gewährleisten. Beim Anfordern einer Website wird eine Bewertung ausgegeben und mit den Content Filtering-Regeln, die der Administrator definiert hat, verglichen. Wenn die Anforderung zulässig ist, wird dem Benutzer die Seite angezeigt. Ist der Zugriff auf eine Website nicht erlaubt, erhält der Benutzer eine Nachricht mit dem Hinweis, dass die Site entsprechend den Regeln gesperrt ist.

### Integration von Content Management und Firewalls

Lösungen, die Content Filtering-Funktionen in eine Firewall integrieren, sind kostengünstig und ideal für Unternehmen mit kleinen bis mittelgroßen Netzwerken geeignet. Der Content Filtering-Dienst kann hierbei entweder in eine bestehende Firewall integriert oder zusammen mit einer neuen Firewall-Lösung installiert werden. In der Regel stellt ein solcher Dienst eine ständig aktualisierte, umfassende Datenbank mit Millionen von Websites, Domänen und IP-Adressen zur Verfügung. Der Verwaltungsaufwand hierfür ist minimal, so dass Unternehmen die Administration selbst übernehmen oder aber bei ihrem IT-Serviceanbieter outsourcen können.

### Standalone-Appliances

In größeren Unternehmen, die umfassendere Kontrollmöglichkeiten benötigen, gewährleistet eine Standalone Content Filtering Appliance maximalen Schutz vor den immer komplexeren Bedrohungen aus dem Internet. Zwar muss bei dieser Option zusätzliche Hardware angeschafft werden, aber dank der unkomplizierten Installation und Handhabung bieten Standalone-Appliances interessante Vorteile: Die Appliance kann in jedes Netzwerk integriert werden, ohne dass bestehende Hardware oder Software neu konfiguriert werden muss. Außerdem sind solche Appliances eine erschwingliche Alternative, um Firewalls ohne Upgrade zu aktualisieren und neue Funktionen hinzuzufügen. Eine Standalone-Appliance kann zudem Internet Content Management mit Echtzeit-Gateway Anti-Virus- und Anti-Spyware-Funktionen kombinieren,

ohne das Budget zu belasten. Hochwertige Produkte zeichnen sich durch eine umfangreiche Funktionspalette und ein optimales Preis-Leistungs-Verhältnis aus. Standalone-Appliances bieten neben einfachen Website-Zugriffskontrollmöglichkeiten und den genannten Vorteilen folgende Pluspunkte:

- **Nahtlose Integration.** Die Appliances lassen sich problemlos in nahezu jedes Netzwerk integrieren und mit allen bestehenden Firewalls kombinieren. Plug & Play beschleunigt die Installation: Die Lösungen können ohne großen Aufwand in das Netzwerk eingebunden werden, ohne dass zusätzliche Server oder Hardware nötig sind.
- **Dynamic Rating Engine.** Dank integrierter Funktionen können neue URLs dynamisch bewertet werden. Mit Echtzeit-Analysen von Webinhalten, Kontextinformationen für indizierte Wörter, HTML-Tags und anderen Daten werden Ratings und Kategorien festgelegt, so dass der Web-Zugriff entsprechend den festgelegten Regeln sofort freigegeben oder gesperrt werden kann. Neue Bewertungen können für weitere Anfragen automatisch zu einer Master Rating-Datenbank hinzugefügt werden.
- **Schutz vor Angriffen.** Mithilfe der Deep Packet Inspection-Technologie werden Viren, Würmer, Trojaner, Spyware, Phishing-Angriffe, bösartiger Code und andere Angriffe abgeblockt, bevor sie das Netzwerk infizieren. Die Appliances können den Netzwerk-Datenverkehr über eine Vielzahl an Ports und Protokollen wie HTTP, SMTP, POP3, FTP und NetBIOS scannen und neutralisieren.
- **Verbesserte Bandbreitennutzung und erweiterte Sicherheit zur Vermeidung rechtlicher Probleme.** Die Applikationen bieten Kontrollmöglichkeiten zur Verwaltung von Instant Messaging-, Peer-to-Peer- und Multimedia-Anwendungen.
- **Management- und Reporting-Funktionen.** Dank integriertem Support können Netzwerk-Administratoren alle Benutzer über eine einzige Benutzeroberfläche verwalten, haben aber gleichzeitig die Möglichkeit, individuelle Kategorien und URL-Rating-Listen zu erstellen, was eine feinere Einstellung der Filterregeln ermöglicht (siehe Abbildung 2). Erweiterte Reporting- und Analysetools mit benutzerdefinierten Reports ermöglichen zudem einen detaillierten Einblick in die Netzwerknutzung.

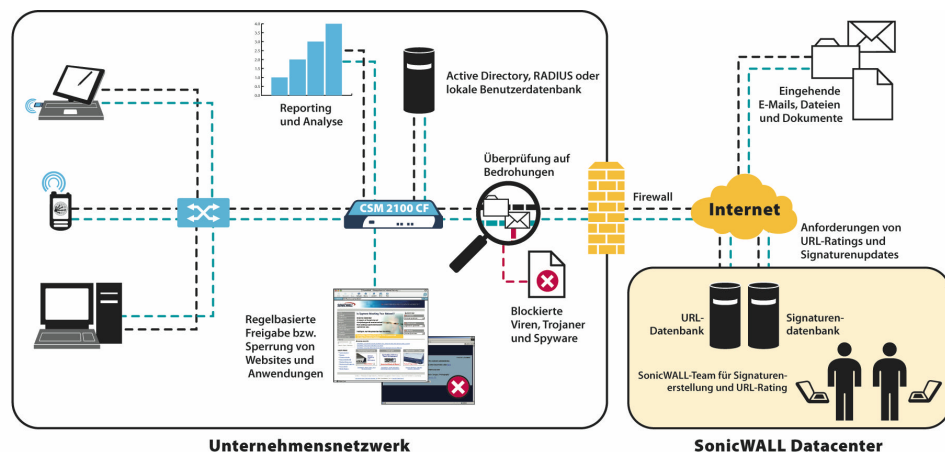


Abb. 2. SonicWALL CSM 2100 CF

## Wichtige Funktionen und Vorteile

Egal, ob ein Kunde für sein Netzwerk eine integrierte Content Management-Lösung oder eine Standalone-Appliance ins Auge fasst – hochwertige Lösungen lassen sich daran erkennen, dass sie mehrere der in diesem Kapitel beschriebenen Features aufweisen und die drei wichtigsten funktionalen Anforderungen an eine Secure Content Management-Lösung abdecken: Schutz vor Bedrohungen, Sicherstellen der Mitarbeiterproduktivität und Vermeidung rechtlicher Probleme. Gleichzeitig sollten sie sich gut skalieren und einfach verwalten lassen. In Tabelle 1 am Ende dieses Kapitels werden die Funktionen nach Kategorien zusammengefasst.

### Regel-Verwaltung

Funktionen zur Regel-Verwaltung bieten Unternehmen umfassende Content Management-Kontrollmechanismen. Der Netzwerk-Administrator hat dabei die Möglichkeit, Regeln für bestimmte Sites außer Kraft zu setzen. Administratoren können Websites, die eigentlich als unzulässig bewertet wurden, wieder freigeben, indem sie ihnen die Kategorie "zugelassene Domäne" zuweisen. Einem Web-Design-Team kann beispielsweise der Zugriff auf bestimmte Online-Shopping-Sites gewährt werden, damit die Mitarbeiter interaktive E-Commerce-Lösungen und Oberflächen-Designs recherchieren können.

Gleichzeitig sollte der Administrator befugt sein, eine Website als "gesperrte Domäne" zu kennzeichnen, die in keine Problemkategorie fällt. Beispielsweise können so Sportseiten zur Liste der gesperrten Domänen hinzugefügt werden, damit bei beliebten Sport-Veranstaltungen die Mitarbeiterproduktivität nicht leidet.

Content Management-Lösungen lassen sich zudem auch so konfigurieren, dass bestimmte Benutzer und Gäste die Möglichkeit haben, Filterregeln außer Kraft zu setzen, um auf gesperrte Sites zuzugreifen. Mithilfe einer vordefinierten Kombination aus Benutzernamen und Kennwort, die mit einer entsprechenden Berechtigung versehen ist, kann der ungefilterte Webzugang noch erweitert werden. Alternativ kann der Administrator auch ein individuelles Konto einrichten.

Hochwertige Content Management-Lösungen bieten außerdem die Option, mehrere Regeln für unterschiedliche Filter-Anforderungen festzulegen. Dadurch kann der Administrator ganz flexibel Benutzergruppen im Netzwerk individuelle Regeln zuweisen. Auf diese Weise könnten z.B. einem Supply Chain Manager andere Regeln als einem Verwaltungsangestellten zugewiesen werden oder es ließen sich für verschiedene Abteilungen eines Unternehmens unterschiedliche Regeln definieren. Netzwerk-Administratoren sollten auch die Zeiträume bestimmen können, in denen bestimmte Content-Regeln eingesetzt werden. So könnte eine Firma bestimmte Filterregeln während der normalen Arbeitszeiten aufrechterhalten und diese für Mitarbeiter, die am Abend länger bleiben, außer Kraft setzen.

### Individuelle Rating-Kategorien

Mit dieser Funktion können Netzwerk-Administratoren beliebige Kombinationen von Kategorien sperren und bei Bedarf anpassen, wenn sich die Filterregeln einer Organisation ändern. Nach einer Anpassung durch den Administrator sollte die Content Management-Lösung sofort die neuen Regeln anwenden. Außerdem sollten Administratoren individuelle Rating-Kategorien erstellen und Regeln festlegen können, mit denen benutzerdefinierte Unterkategorien blockiert bzw. zugelassen werden können.

### Integrierte Dynamic Rating Engine

Ruft ein Benutzer eine neue URL auf, für die es in der Master Rating-Datenbank noch keine Bewertung gibt, können Appliances mit einer integrierten Dynamic Rating Engine die Seite zur Analyse und Klassifizierung in Echtzeit abfragen. Kann die Rating Engine die Website nicht eindeutig bewerten und kategorisieren, sollte die Site in die Kategorie „Andere“ eingeordnet und entsprechend gekennzeichnet werden, damit sie später vom Netzwerk-Administrator noch einmal geprüft werden kann.

## Gateway Anti-Virus und Anti-Spyware Protection

Umfassende Secure Content Management-Lösungen kombinieren Enterprise Class-Filtering mit Echtzeit-Gateway Anti-Virus- und Anti-Spyware-Funktionen. Mithilfe von Deep Packet Inspection und einer dynamisch aktualisierten Signaturendatenbank lassen sich Netzwerke umfassend schützen und Bedrohungen neutralisieren, bevor sie das Netzwerk infizieren. Statt Ports einfach nur zu sperren, gleichen hochwertige Lösungen die heruntergeladenen, als E-Mail-Anhang verschickten und komprimierten Dateien mit einer umfassenden Signaturendatenbank ab, um Viren, Würmer, Trojaner, Spyware, Keylogging- und Phishing-Angriffe sowie bösartigen Code zu blockieren. Deep Packet Inspection bietet beispiellosen Netzwerkschutz und reduziert die Dateien, die fälschlicherweise als infiziert identifiziert und gesperrt werden, auf ein Minimum. Um die Effizienz der Antiviren- und Anti-Spyware-Software zu ermitteln, prüfen Sie, inwiefern die verfügbaren Features (z.B. Deep Packet Inspection-Funktionen) folgende Anforderungen erfüllen:

- Verarbeitung (unbegrenzt) großer Dateien
- Verarbeitung tausender gleichzeitiger Downloads
- Verarbeitung komprimierter Dateien (erfordert Technologie zum Dekomprimieren und Scannen von Dateien auf Paketebene)
- Häufig aktualisierte Signaturendatenbanken (um neue Angriffe durch neue Bedrohungen zu verhindern)
- Zugriff von Drittanbietern auf Signaturendatenbanken (offene Lösungen erlauben die Zusammenarbeit mehrerer Anbieter bei der Erkennung von Bedrohungen)

## Umfassender Schutz

Secure Content Management-Lösungen müssen Kontrollmöglichkeiten und Zugriffsbeschränkungen auf mehreren Ebenen aufweisen, um Netzwerke hinreichend vor Bedrohungen zu schützen. Firewalls und Gateways wehren Angriffe – und dabei vor allem externe Bedrohungen – an vorderster Front ab, bieten aber keinen ausreichenden Schutz vor internen Bedrohungen und missbräuchlicher Netzwerknutzung. Daher müssen weitere Methoden zur Kontrolle und Prüfung des Datenverkehrs auf Paketebene im gesamten Netzwerk eingesetzt werden.

## Anwendungskontrollen

Sicherheitslösungen sollten mehrere Filterfunktionen mit Intrusion Prevention-Technologie für Anwendungen und Protokolle enthalten. Auf diese Weise lässt sich das Downloaden von Peer-to-Peer-, Instant Messaging- oder Multimedia-Anwendungen effektiv sperren.

## Integration von Active Directory

Durch die Integration mit Microsoft® Active Directory®-Software lassen sich Regeln entsprechend der organisatorischen Hierarchie festlegen und alle Benutzer über eine einheitliche Oberfläche mit Single Sign-On verwalten. Wechselt ein Benutzer in eine andere Abteilung oder wird die Firma umstrukturiert, sollte die Content Management-Lösung in der Lage sein, alle Regeln automatisch gemäß den in Active Directory eingegebenen neuen Rollen zu aktualisieren.

## Intelligentes URL-Parsing

Dank intelligentem URL-Parsing können Content Management-Lösungen den Status von URLs auf der Grundlage der gesamten URL bestimmen, und nicht nur anhand der Domänen- und Pfadanteile. Dies garantiert zusätzlichen Schutz, da Benutzer keine gesperrten Seiten aus dem Zwischenspeicher aufrufen können.

### Anmeldung mit Benutzernamen und Passwort (ULA)

Administratoren müssen für die Einhaltung der im Unternehmen geltenden Netzwerk-Sicherheitsbestimmungen sorgen. Dazu müssen sie in der Lage sein, jedem Benutzer ein eigenes Zugangsprofil mit genau definierten Berechtigungen und Prioritäten zuzuweisen. Sicherheitslösungen sollten darüber hinaus ULA unterstützen. Auf diese Weise kann das Netzwerk so konfiguriert werden, dass sich alle Benutzer mit ihrem Benutzernamen und Passwort anmelden müssen. ULA greift auf bestehende Authentifizierungsdatenbanken wie RADIUS und Active Directory zurück.

### Webbasiertes Reporting

Sicherheitslösungen sollten optionale Reporting-Pakete enthalten, die sich einfach mit der Content Management-Lösung verknüpfen lassen und detaillierte Reports zu Internetnutzung und Content Filtering liefern. Mit einem integrierten erweiterten Reporting- und Analysetool können Administratoren individuelle Reports erstellen, die ein detailliertes Bild der Netzwerknutzung liefern.

Tabelle 1. Hauptfunktionen von Content Management -Lösungen und unterstützte Aufgabenbereiche

Funktionen	Schutz vor Bedrohungen	Optimierung der Produktivität	Vermeidung von rechtlichen Problemen	Vereinfachte Verwaltung
Gezielte regelbasierte Kontrollen				
Manuelle Umgehung von Regeln				
Erstellung individueller Rating-Kategorien				
Dynamic Rating Engine				
Viren- und Spyware-Schutz: Sperren von Ports Deep Packet Inspection	 	 	 	
Schutz verschiedener Netzwerkebenen: Firewalls und Gateways Packet Inspection	 	 	 	
Anwendungssteuerung				
Integration von Active Directory				
Intelligentes URL-Parsing				
Anmeldung von Benutzern mit Usernamen und Passwort (ULA)				
Webbasiertes Reporting				

## Anwendungsbeispiele

Die folgenden fiktiven Beispiele zeigen, wie Unternehmen vom Einsatz von Content Management-Lösungen profitieren können und welche Lösung für die einzelnen Szenarien empfehlenswert sind.

### Kleine Unternehmen

#### Schilling & Söhne GmbH

*Schilling & Söhne ist ein kleines Familienunternehmen mit 30 Mitarbeitern. Die Firma benötigt eine Content Management-Lösung, um die begrenzte Netzwerk-Bandbreite optimal für geschäftsrelevanten Internetverkehr nutzen zu können. Außerdem möchte das Unternehmen den Zugriff auf Online-Shopping- und Sport-Websites während der Arbeitszeit sperren, um so Produktivitätsverlusten vorzubeugen. Schilling & Söhne hat kein Budget für einen eigenen Netzwerk-Administrator und braucht eine Lösung, bei der nach der Installation keine weitere Verwaltung nötig ist.*

#### Empfehlung

Für diesen Kunden ist eine integrierte Content Management-Lösung am besten geeignet. Kleine Unternehmen sollten darauf achten, dass ihre Lösung folgende Leistungen bietet:

- Unkomplizierte Installation und Verwaltung. Die Lösung sollte alle gängigen Firewalls unterstützen und Regeln und Updates automatisch auf alle Benutzer anwenden.
- Skalierbarkeit zur reibungslosen Netzwerkerweiterung. Soll ein neues Gebäude oder eine neue Benutzergruppe ins Netzwerk eingebunden werden, sollte sich die Erweiterung ohne großen Aufwand mit zusätzlichen Appliances realisieren lassen.
- Detaillierte Regelverwaltung. Jede Abteilung oder Geschäftsstelle sollte individuelle Regeln festlegen können, die auf der Funktion der Mitarbeiter sowie auf weiteren Klassifizierungsmerkmalen basieren.
- Unterstützung für die Umgehung von Filterregeln. Bestimmte Benutzer, wie etwa Mitarbeiter in leitenden Positionen, sollten uneingeschränkten Zugriff auf Internetsites haben.
- Automatisches Sperren gefährlicher Seiten. Downloads von Java- und ActiveX-Komponenten sowie Cookies müssen bei Bedarf gesperrt werden können, um die Sicherheit und den Datenschutz zu erhöhen.

### Mittelgroße Unternehmen

#### Notar- und Anwaltskanzlei MRB

*Eine größere Kanzlei mit einem Hauptbüro und mehreren kleinen Niederlassungen beschäftigt insgesamt 1000 Mitarbeiter. Die Firewall am Hauptstandort wehrt Angriffe auf das Netzwerk ab, bietet aber keine Antiviren- oder Filterfunktionen. Die Kanzlei benötigt zusätzlich noch eine High-End-Content Security Management-Lösung, um die Firewall zu entlasten und so die Bandbreite besser nutzen zu können. Daneben soll die Lösung zusätzliche Funktionen bieten, beispielsweise Schutz vor Viren und Spyware sowie die Möglichkeit, Peer-to-Peer-File Sharing und Instant Messaging zu sperren. Das Unternehmen legt außerdem Wert auf eine zentralisierte Verwaltung, um Regeln firmenweit festzulegen, verteilen und anwenden zu können. Da nur begrenzte IT-Ressourcen zur Verfügung stehen, sollte die Lösung unkompliziert in der Bereitstellung und Verwaltung sein.*

## Empfehlung

Bei diesem Kunden empfiehlt sich der Einsatz einer komplexeren Content Management-Lösung. Mittelgroße bis große Unternehmen sollten darauf achten, dass ihre Lösung folgende Leistungen bieten:

- Alle gängigen Funktionen von hochwertigeren Content Management-Appliances bei gleichzeitig extrem niedrigen Kosten
- Nahtlose Integration mit bestehenden Firewall-Geräten unterschiedlicher Anbietern für eine optimale Ausnutzung bestehender Investitionen
- Umfassendes Content Management ohne Beeinträchtigung der Netzwerk-Performance
- Schutz vor ungeeigneten Webinhalten – selbst bei noch nicht bewerteten URLs (eine integrierte Dynamic Rating Engine bewertet neue Sites, sobald sie online sind)
- Sperren von Peer-to-Peer-File Sharing und Instant Messaging für eine verbesserte Bandbreitennutzung und zur Vermeidung rechtlicher Probleme, die sich aus dem Download von urheberrechtlich geschützten Dateien ergeben können
- Nutzung von Deep Packet Inspection sowie einer dynamisch aktualisierten Signaturendatenbank zum umfassenden Schutz vor Bedrohungen wie Viren, Würmern, Trojanern, Keylogging- und Skript-Angriffen, Spyware und anderem böswilligem Code
- Detailliertes Reporting zu Netzwerknutzung und Content-Zugriff, so dass Administratoren die Regeln entsprechend anpassen können
- Integration mit Active Directory für minimalen administrativen Aufwand

## Resümee

Secure Content Management-Systeme stellen für moderne Unternehmen ein wesentliches Instrument dar, um die Mitarbeiterproduktivität zu verbessern und rechtlichen Problemen durch Internetmissbrauch vorzubeugen. SonicWALL bietet zwei Lösungen, mit der sich die wechselnden Anforderungen moderner Unternehmen hinsichtlich Performance, Flexibilität und Kosten erfüllen lassen:

- Der SonicWALL Content Filtering Service (CFS) eignet sich für kleine und mittelgroße Organisationen, die eine kosteneffiziente integrierte Content Management-Lösung mit minimalem Verwaltungsaufwand benötigen.
- SonicWALL Content Security Manager 2100 Content Filter (CSM 2100 CF) bietet durch die Kombination von Internet Content Management-Funktionen mit dynamischem Gateway Anti-Virus- und Anti-Spyware-Schutz umfassendes Content Security Management.

Da beide SonicWALL-Lösungen nur ein lokales Gerät erfordern und als Abo vertrieben werden, können sie zu einem außerordentlich niedrigen Preis angeboten werden.

Ausführliche Informationen über SonicWALL Content Management-Lösungen erhalten Sie unter: <http://www.sonicwall.com/products>