SONICWALL™

コンテンツ・フィルタリング・サービス& コンテンツ・フィルタリング・クライアント

有害で非生産的な Web コンテンツへのアクセスをブロックする強力な保護および生産性向上ソリューション

教育機関、企業、および政府機関において、インターネット接続可能なコンピューターを IT 部門から学生、従業員、職員に支給する場合、たとえそのコンピューターを組織内の Web 利用ポリシーが適用されているファイアウォール内で使用する場合であっても、非常に大きなリスクが伴います。不適切/危険/違法な情報や画像が含まれたサイトへのアクセスに、インターネット接続が使用される場合はなおさらです。そういったサイトにはマルウェアが仕込まれていることもあり、そうと知らずにダウンロードしてしまったため機密情報が盗まれてしまうという事態もあり得ます。

特に学校には、不適切で有害な Web コンテンツから生徒を守る責任があります。また、学校や図書館が eRate（学校図書館や公立図書館のインターネット接続料を割引にする米国の補助金制度）を受給するには、児童をインターネットから保護する法律（CIPA: Children's Internet Protection Act）に適合したコンテンツ・フィルタリング・ソリューションをインストールすることが法律で義務付けられています。企業や政府機関の場合、従業員や職員による Web アクセスを制限しなければ、法的責任を問われる可能性があることは言うまでもなく、非生産的なネットサーフィンによる生産性の著しい低下が生じる可能性があります。

SonicWall 統合脅威管理および次世代ファイアウォール（NGFW）上で動作する、SonicWall コンテンツ・フィルタリング・サービス（CFS）は強力な保護および生産性向上ソリューションで、教育機関、企業、図書館および政府機関向けに、他に類を見ないコンテンツフィルタリング機能を提供します。SonicWall CFS を使用する組織は、学生や従業員がファイアウォール内で IT 部門支給のコンピューターからアクセスできる Web サイトを制御できます。

SonicWall CFSは、要求された Web サイトを、何百万ものレーティング済み URL、IP アドレスおよび Web サイトが格納されたクラウド上の膨大なデータベースと照らし合わせます。CFS には、56 を超える予め定義されたカテゴリについて、個人やグループの ID ごと、または時間帯別に、サイトへのアクセスを許可または拒否するポリシーを作成して適用する管理者用ツールがあります。また CFS では、SonicWall ファイアウォール上で Web サイトのレーティングを動的にローカルにキャッシュできるため、ほぼ即時の応答時間を実現しています。

ファイアウォールの外側で使用するノートパソコンには、SonicWall コンテンツ・フィルタリング・クライアントが、有害で非生産的な Web コンテンツのブロック制御に関する拡張機能を提供し、安全性、セキュリティおよび生産性上の懸念を解消します。クライアントは、SonicWall ファイアウォールによって自動的に展開され、プロビジョニングされます。このコンテンツ・フィルタリング・クライアントは、ローミングデバイスの Web ベースのアクセスを制御するツールを IT管理者に提供するほか、そのデバイスがネットワークのファイアウォールに再接続すると内部ポリシーの適用対象になるよう自動的に切り替えるように設定することもできます。クライアントの管理と監視は、クラウド上にあるポリシーおよびレポート作成用の強力なエンジンを使って行われ、このエンジンへのアクセスは、ファイアウォールのインターフェイスからシームレスに実施されます。有効期限の過ぎたクライアントがインターネットへアクセスするために内部ネットワークへの接続を試みた場合、その接続は拒否され、ユーザには是正措置の手順が記されたメッセージが送付されます。

メリット:

- クラス最高レベルの保護
- きめ細やかなコンテンツフィルタリング制御
- 動的にアップデートされるレーティングアーキテクチャ
- アプリケーショントラフィック分析
- 使いやすい Web ベースの管理
- ハイパフォーマンスな Web キャッシュ機能とレーティングアーキテクチャ
- IP ベースの HTTPS コンテンツフィルタリング
- 拡張性やコスト効率に優れたソリューション
- ローミングデバイス用のコンテンツ・フィルタリング・クライアント

特徴とメリット

きめ細やかなコンテンツフィルタリング機能により、管理者は予め定義されているカテゴリのすべて（またはカテゴリの組み合わせ）をブロックしたり、帯域制御を適用したりできます。管理者はユーザレベル認証（ULA）およびシングルサインオン（SSO）を適用してユーザ名とパスワードによるログオンを強化できます。CFS では、Java™、ActiveX®、Cookie など、害を及ぼすおそれのあるコンテンツをブロックできるうえ、授業中や営業時間中といった時間帯でのスケジュールフィルタリングも可能です。さらに、IM、MP3、ストリーミングメディア、フリーウェアなど、帯域を消費するファイルをフィルターにかけて排除することで、パフォーマンスを向上させます。

動的にアップデートされるレーティングアーキテクチャは、要求されたすべての Web サイトを、数百万の URL、IP アドレス、ドメイン情報をカテゴリ分けした高精度のデータベースに照らし合わせます。SonicWall のファイアウォールはリアルタイムでレーティングを受け取り、個々のレーティングをローカルのポリシー設定と照合します。このアプライアンスは、管理者がローカルに設定したポリシーに基づいて要求を許可または拒否します。

アプリケーショントラフィック分析スイートには、SonicWall Global Management System（GMS®）および SonicWall Analyzer が含まれており、いずれもブロックされた Web サイトおよびユーザが訪問したサイトを含め、ファイアウォールを通って送信されたデータのリアルタイム分析および履歴分析を実施します。

使いやすい Web ベースの管理は、柔軟なポリシー設定とインターネットの利用状況の完全制御を可能にします。管理者は、個人ユーザ、グループ、または特定のカテゴリタイプに対して、複数のカスタムポリシーを適用できます。ローカルの URL フィルタリング制御機能により、特定のドメインやホストの許可または拒否が可能です。不適切で非生産的なコンテンツをより効率よくブロックするために、管理者はフィルタリングリストの作成やカスタマイズも可能です。

ハイパフォーマンスな Web キャッシュ機能とレーティングアーキテクチャにより、管理者はカテゴリごとにサイトを容易に、自動的にブロックできます。URL のレーティングは SonicWall ファイアウォール上でローカルにキャッシュされるため、頻繁に訪問するサイトの場合、以降のアクセスに要する応答時間はほんの一瞬です。

IP ベースの HTTPS コンテンツフィルタリングにより管理者は暗号化された HTTPS 接続による Web サイトへのユーザアクセスを制御できます。HTTPS のフィルタリングは、暴力、差別、オンラインバンキング、ショッピングといった不適切/非生産的な情報や画像を含んだ Web サイトのカテゴリ別のレーティングに基づいて行われます。

拡張性とコスト効率に優れたソリューションは、SonicWall のファイアウォールからコンテンツのフィルタリングを制御するため、ハードウェアを追加する必要もなく、専用のフィルタリングサーバーを別途展開する費用もかかりません。

ローミングデバイス用のコンテンツ・フィルタリング・クライアントは、内部の Web 利用ポリシーの適用を拡張して、ファイアウォールの外側にあるデバイスについて、不適切で非生産的なインターネットコンテンツをブロックできるようにします。デバイスがインターネットに接続する際、接続が確立される場所に関係なく、セキュリティと生産性にかかわるポリシーが必ず適用されます。

SonicWall コンテンツフィルタリングのソリューションアーキテクチャ

SonicWall ファイアウォール経由で展開および管理される SonicWall コンテンツ・フィルタリング・サービスにより、IT 管理者は、ファイアウォールの内側にある IT 部門支給のエンドポイントデバイスが LAN、無線 LAN、または VPN 経由で、不適切で非生産的な Web サイトにアクセスするのを防止する、インターネット利用ポリシーを作成して適用できます。

ファイアウォールの外側にあるローミングデバイスについては、SonicWall コンテンツ・フィルタリング・クライアントによって、デバイスがインターネットに接続する際には必ず、接続が確立される場所に関係なく、セキュリティと生産性にかかわるポリシーを拡張できます。SonicWall ファイアウォールの実施機能を使用して展開を簡素化し、クライアントの管理および監視は、ポリシーおよびレポート作成のための強力なエンジンを使って行われます。

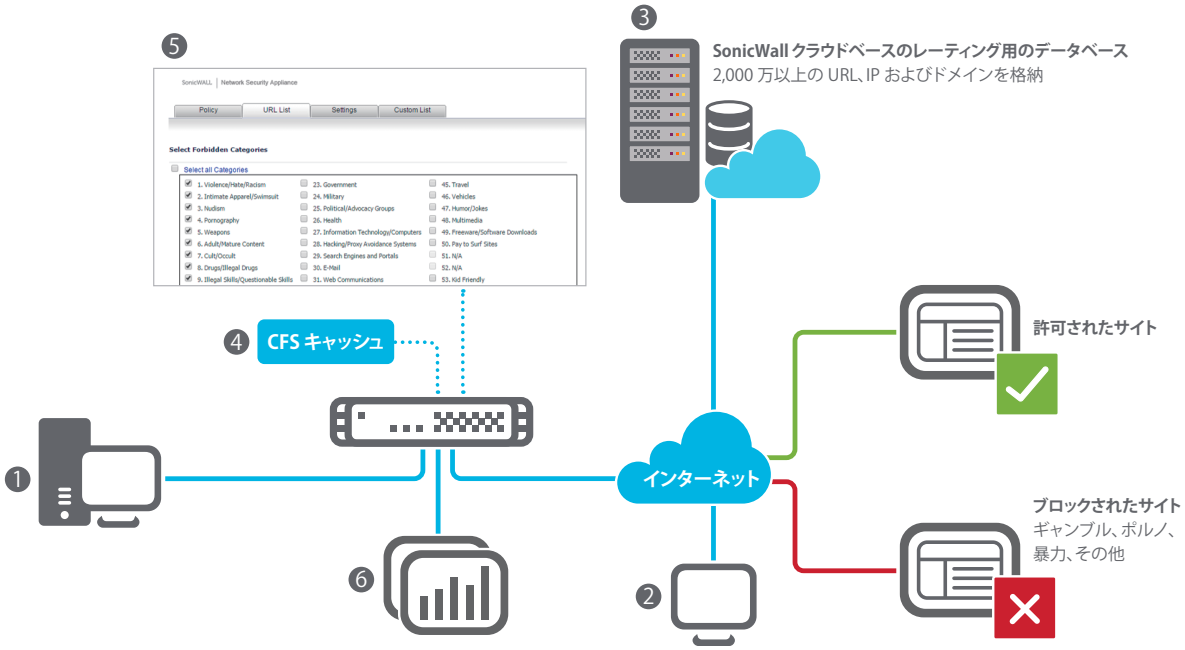
SonicWall Analyzer または SonicWall Global Management System（GMS）を使用することで、IT 管理者は Web の利用状況に関するリアルタイムレポートと履歴レポートを作成できます。

当社について

創設後25年以上にわたり、SonicWallはこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、Eメールセキュリティまで、SonicWallは自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約200の国と地域に100万台を超えるセキュリティデバイスを持つSonicWallは、お客様が自信を持って未来を受け入れられるようにします。

	コンテンツ・フィルタリング・サービス・プレミアム	コンテンツ・フィルタリング・クライアント
カテゴリ	56 以上	56 以上
ユーザ / グループポリシー	✓	✓
動的なレーティング	✓	✓
レポート作成	Analyzer* および GMS*	✓
Web サイトのキャッシュ機能	✓	✓
セーフサーチの適用	✓	✓
IP 範囲ごとの CFS ポリシー適用	✓	✓
利用可能: • TZ Series • NSA Series • E-Class NSA Series • SuperMassive 9000 Series • SuperMassive E10000 Series	✓ ✓ ✓ ✓ ✓	Windows、Chrome OS または Mac OS 搭載のエンドポイントデバイス。 SonicWall ファイアウォール経由で展開。
YouTube for Schools	✓	✓
HTTPS コンテンツフィルタリング	✓	✓
スケジュール設定によるフィルタリング	✓	✓
コンテンツフィルタリング用データベース	動的にアップデートされるベース。2,000 万以上の URL、IP、ドメインを格納	
サポート対象のファームウェアバージョン / オペレーティングシステム	SonicOS 5.x 以降	ファイアウォール – Gen5: SonicOS 5.9.0.4 以降、Gen6: SonicOS 6.1.1.6 以降 ノートパソコン - Microsoft Windows 7/8/10、Windows Server 3/Server 8/ Server 12、Chrome OS、Mac OS 10.8 以降

Analyzer および GMS はオプションです (別売)。



1. ファイアウォールの内側にいる SonicWall CFS ユーザ
2. ファイアウォールの外側にいるローミング中の CF クライアントユーザ
3. SonicWall CFSレーティング用の分散データベース
4. 許可されたサイトのレーティングのローカルキャッシュ
5. URL ポリシーを設定して、不適切または非生産的な Web サイトをブロック
6. SonicWall Analyzer または GMS を使用して、リアルタイム/履歴レポートを作成

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-ContentFilteringSvc-US-KJ-29434-D1

SONICWALL™