SonicOS 7
DPI-SSL

管理ガイド

SONICWALL®

内容

1

DPI-SSL について

ⓘ **補足:** DPI-SSL は、暗号化された HTTPS トラフィックやその他の SSL ベースの IPv4 と IPv6 のトラフィックの検査を実現する個別にライセンスされる機能です。

トピック:

- DPI-SSL の使用
- 導入シナリオ
- DPI SSL のカスタマイズ
- アプライアンスモデル別の接続数

DPI-SSL の使用

トピック:

- サポートされる機能
- セキュリティ サービス

サポートされる機能

セキュア ソケット レイヤの精密パケット検査 (DPI-SSL) は、SonicWall の精密パケット検査技術を拡張して、暗号化された HTTPS トラフィックおよびその他の SSL ベースのトラフィックを検査できるようにするものです。SSL トラフィックを透過的に復号化して脅威をスキャンし、脅威や脆弱性が見つからなかった場合には再度暗号化して送信先に送信します。

暗号化された HTTPS およびその他の SSL ベースのトラフィックを DPI-SSL で分析することによって、セキュリティ、アプリケーションの制御、データ漏洩の抑止を強化できます。DPI-SSL サポートは、次のとおりです。

- Transport Layer Security (TLS) ハンドシェイク プロトコル 1.2 およびそれより前のバージョン – TLS 1.2 通信プロトコルは、DPI-SSL 配備でのファイアウォールとサーバとの間の SSL 検査/復号化時にサポートされます (これまで、TLS 1.2 のサポートはクライアントとファイアウォール間に限られていました)。SonicOS はその他の領域でも TLS 1.2 をサポートしています。
- SHA-256 – 再署名されたすべてのサーバ証明書は、SHA-256 ハッシュ アルゴリズムによって署名が行われます。

- Perfect Forward Secrecy (PFS) – 通知された暗号スイートでは、Perfect Forward Secrecy ベースの暗号やその他のより強力な暗号が弱い暗号よりも優先されます。その結果、クライアントやサーバは、より強力な暗号をサポートしていない場合を除き、弱い暗号をネゴシエートしないことが見込まれます。

DPI-SSL は SSL トンネル上でのアプリケーション レベルの帯域幅管理もサポートします。アプリケーション ルールの HTTP 帯域幅管理ポリシーは、アプリケーション ルールに対してDPI-SSL を有効にしているときに HTTPS でアクセスするコンテンツにも適用されます。

クライアントとサーバの両方の DPI-SSL をアクセス ルールによって制御できます。

トピック:

- ローカル CRL のサポート
- TLS 証明書状況要求拡張機能
- SSH X11 転送の遮断
- ECDSA 関連暗号のサポート
- 独立して動作する DPI-SSL および CFS HTTPS コンテンツ フィルタ
- 復号化されたパケットに保持される元のポート番号

ローカル CRL のサポート

証明書失効リスト (CRL) は、予定された有効期限になる前に発行元の証明書認証機関 (CA) が取り消した、もはや信頼されないデジタル証明書のリストです。このリストについて CA に連絡する際の問題は、ブラウザが CA のサーバに到達したかどうか、または攻撃者が失効チェックをバイパスするために接続をインターセプトしたかどうかを確認できないことです。

ローカル CRL は、通常の CRL (つまり、オンライン CRL) を基準に決まります。通常の CRL の場合、クライアントは CRL 配布ポイントから CLR をダウンロードする必要があります。クライアントが CRL をダウンロードできない場合、既定では、クライアントは証明書を信頼します。通常の CRL とは異なり、ローカル CRL は、DPI-SSL のインポート メモリに失効した証明書のリストをローカルに保持して、証明書が失効しているかどうかを確認します。

この機能の詳細については、テクニカル サポートにお問い合わせください。

TLS 証明書状況要求拡張機能

DPI-SSL は、新しい TLS 証明書状況要求拡張機能 (正式には OCSP stapling) をサポートします。この拡張機能をサポートすることにより、既に確立されているチャンネルを通じて証明書状況情報が DPI-SSL クライアントに配信されるため、オーバーヘッドが削減され、パフォーマンスが向上します。

SSH X11 転送の遮断

ⓘ | **補足:** X11 転送には、有効な SonicWall DPI-SSH ライセンスが必要です。

X は、Unix ワークステーション用の一般的なウィンドウ システムです。X を使用すると、ユーザは、ユーザのローカル ディスプレイでウィンドウを開くリモート X アプリケーションを実行できます (逆の場合は、リモート ディスプレイでローカル アプリケーションを実行します)。ファイアウォールおよび管理者がリモート接続を遮断した後にリモート サーバが外部にある場合、ユーザはまだ SSH トンネリングを使用すればローカル マシンで X ディスプレイを取得

できます。したがって、ユーザはファイアウォール上のアプリケーションベースのセキュリティ ポリシーを迂回し、セキュリティ リスクを引き起こすことができます。アプリケーションと X サーバの間の X プロトコル セッションはネットワークを介して送信されている間は暗号化されないため、X11 プロトコル接続を SSH 接続経由でルーティングして、セキュリティと強力な認証を提供できます。この機能は X11 転送と呼ばれます。SSH クライアントは、SSH サーバに接続するときに X 転送を要求します（クライアントで X 転送が有効になっていると仮定）。サーバがこの接続で X 転送を許可している場合、ログインは正常に進行しますが、サーバは舞台裏で特別な手順を実行します。ターミナル セッションの処理に加えて、サーバはリモート マシンで実行されるプロキシ X サーバとして自身を設定し、プロキシ X ディスプレイを指すようにリモート シェルで DISPLAY 環境変数を設定します。X クライアント プログラムは、実行されるとプロキシに接続します。プロキシは実際の X サーバと同様に動作し、SSH クライアントにプロキシ X クライアントとして動作するよう指示し、ローカル マシンの X サーバに接続します。SSH クライアントとサーバは協力して、2 つの X セッション間の SSH パイプを介して X プロトコル情報をやり取りします。X クライアント プログラムは、ディスプレイに直接接続されているかのように画面に表示されます。DPI-SSH X11 転送は、次のクライアントをサポートしています。

- Cygwin 用の SSH クライアント
- Putty ·secureCRT
- Ubutu の SSH
- CentOS の SSH

DPI-SSH X11 転送は、次の SSH サーバをサポートしています。

- Fedora
- Ubuntu

SSH X11 転送では、ルート モードとワイヤ モードの両方がサポートされます。対象が

- ワイヤ モードでは、DSSH X11 転送は保護（直列トラフィックのアクティブ DPI）モードでのみサポートされます。
- ルート モードでは、制限はありません。

SSH X11 転送でサポートされる接続の最大数は、DPI-SSH と同じです。1000.DPI-SSH。

ECDSA 関連暗号のサポート

DPI-SSL クライアントは ECDSA（楕円曲線デジタル署名アルゴリズム）暗号をサポートしています:

- TLS_ECDHE_ECDSA_WIATH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

独立して動作する DPI-SSL および CFS HTTPS コンテンツ フィルタ

DPI-SSL および CFS HTTPS コンテンツ フィルタは、同時に有効にでき、次のように機能します。

- DPI-SSL クライアント検査が無効になっている場合、コンテンツ フィルタ サービスは HTTPS 接続をフィルタリングします。

- DPI-SSL クライアント検査が有効になっているが、コンテンツ フィルタ オプションが選択されていない場合、コンテンツ フィルタ サービスは HTTPS 接続をフィルタリングします。
- DPI-SSL クライアント検査が有効で、コンテンツ フィルタ オプションが選択されている場合、CFS は HTTPS 接続をフィルタリングしません。

復号化されたパケットに保持される元のポート番号

暗号化接続の DPI-SSL/DPI-SSH 接続の場合、復号化されたパケットは送信先ポートが 80 と表示されます (HTTPS の場合)。復号化されたパケットがパケット キャプチャ/Wireshark で確認されると、元のポート番号を保持するようになりました。ポート番号の変更はパケット キャプチャにのみ適用され、実際のパケットまたは接続キャッシュには適用されません。

セキュリティ サービス

DPI-SSL を使用できるセキュリティ サービスおよび機能は、次のとおりです。

ゲートウェイ アンチウイルス	コンテンツ フィルタ
ゲートウェイ アンチスパイウェア	アプリケーション ファイアウォール
侵入防御	

配備方針

DPI-SSL の主な配備シナリオには次の 2 つがあります。

- **クライアント DPI-SSL**: 装置の LAN 上のクライアントが WAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。DPI-SSL に対する除外は、コモンネームまたは種別を基準にして行うことができます。
- **サーバ DPI-SSL**: リモート クライアントが WAN 経由で接続して装置の LAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。

プロキシ配備

DPI-SSL はプロキシ配備をサポートしています。プロキシ配備では、すべてのクライアント ブラウザがプロキシ サーバにリダイレクトされますが、装置はクライアント ブラウザとプロキシ サーバの間に存在します。このシナリオでは、ドメインが仮想ホスティング サーバに含まれる場合や、同じサーバ IP を複数のドメインで使用できる一部のクラウド配備内でのドメイン除外など、すべての DPI-SSL 機能がサポートされます。

また、通常のデータ センター サーバ ファームでは、サーバ上の SSL 処理の負荷を軽減するために、前面に負荷分散装置やリバース SSL プロキシを配置しています。サーバの前面に位置して復号化を行っている負荷分散装置の場合、通常、装置には負荷分散装置の IP しかわかりません。負荷分散装置は、内容を復号化し、この接続の割り当て先となる特定のサーバを決定します。今回、DPI-SSL には IP ベースの除外キャッシュを無効にするためのグローバル ポリシー オプションが用意されました。IP ベースの除外キャッシュがオフになっていても、除外は機能し続けます。

DPI SSL のカスタマイズ

ⓘ **重要:** NetExtender SSL VPN ゲートウェイを DPI SSL IP アドレス除外リストに追加してください。NetExtender トラフィックは PPP によってカプセル化されており、このようなトラフィックを SSL VPN によって復号化しても意味のある結果は得られません。

一般には、装置を通過するありとあらゆるトラフィックを保護することが DPI-SSL のポリシーです。この点がセキュリティのニーズに合わせて、DPI-SSL では処理の対象をカスタマイズすることができます。

DPI-SSL には、DPI の処理から除外される組み込み (既定) ドメインのリスト (データベース) が付随します。このリストへの追加はいつでも行うことができ、追加したエントリはどれでも削除できます。また、DPI 処理の対象としての組み込みエントリの除外と包含を切り替えることもできます。DPI-SSL では、コモンネームまたは種別 (バンキング、医療など) によってドメインを除外したり含めたりすることもできます。

ただし、コモンネームと種別のどちらによるものかに関係なく、除外されたサイトは、装置を回避してクライアント マシンにダウンロードされるエクスプロイト キットや、無防備なクライアントに偽りのサイト/証明書を提示する中間者の乗っ取りによって今後悪用されうるセキュリティ上のリスクになる可能性があります。こうしたリスクを回避するために、DPI-SSL では除外されるサイトを除外前に認証することができます。

ネットワーク内での HTTPS 接続の割合が増え、新しい https サイトが現れてくるので、最新バージョンの SonicOS であっても、組み込み/既定除外の完全なリストを用意することはまず不可能です。新しいクライアント アプリケーションに特有の実装やサーバ実装が原因で DPI-SSL によるインターセプトが発生した場合、一部の HTTPS 接続はエラーになるので、シームレスなユーザ エクスペリエンスを実現するためには、装置上でのこうしたサイトの除外が必要になる場合があります。SonicOS は、このような失敗した接続のログを保持しています。こうした接続エラーは、トラブルシューティングを行ったり、信頼できるエンティティを除外リストに追加したりするために使用できます。

サイトの除外/包含に加えて、DPI-SSL では、グローバルな認証ポリシーとグローバルなポリシーに対するきめ細かな除外ポリシーの両方を用意しています。例えば、接続の認証を行うためのグローバル ポリシーでは、信頼できる新しい CA 証明書や、安全性の高いプライベート (または企業にとってローカルな配備の) クラウド ソリューションの自己署名サーバ証明書など、基本的に安全な接続が遮断される可能性があります。管理者は、きめ細かいオプションを使用して、グローバル認証ポリシーから個々のドメインを除外できます。

同じサーバ (証明書) でサポートされるドメインのリストに含まれているドメインに対して除外を設定できます。つまり、サーバ証明書によっては複数のドメイン名が含まれているものがありますが、1 つのサーバ証明書が対象としているすべてのドメインを除外することなく、これらのドメインのうち 1 つだけを除外したい場合があります。例えば、`youtube.com` を除外して、他のすべてのドメイン (`google.com` など) を除外せずに済ませることができます。`*.google.com` は、`youtube.com` がサブジェクト代替名拡張の下での代替ドメインとしてリストされているサーバ証明書のコモンネームであるにもかかわらずです。

装置モデル別の接続

ハードウェア モデルとそのクライアント DPI-SSL 検査実行のための最大同時接続数については、以下のプラットフォーム データシートを参照してください。SonicWall TZシリーズ。

当社の製品シリーズの詳細については、SonicWall リソースのページを参照してください。最大接続数 (DPI SSL) など、ハイエンド、ミッドレンジ、エントリ レベル、および仮想ファイアウォールの詳細情報を「**By Product Series (製品シリーズ別)**」ドロップダウン メニューで検索します。

2

DPI-SSL/TLS クライアントの設定

トピック:

- 復号化サービス > DPI-SSL/TLS クライアント
- DPI-SSL 状況の表示
- DPI-SSL/TLS クライアントの配備

復号化サービス > DPI-SSL/TLS クライアント

ⓘ | **ヒント:** DPI-SSL の詳細については、「DPI-SSL について」を参照してください。

DPI-SSL 状況の表示

「**DPI-SSL ステータス**」セクションには、現在の DPI-SSL 接続数、ピーク接続数、最大接続数が表示されます。

DPI-SSL/TLS クライアントの配備

一般に、DPI-SSL/TLS クライアントの配備シナリオは、LAN 上のクライアントが WAN 上のコンテンツを参照するときに HTTPS トラフィックを検査するために使用します。このシナリオでは、ファイアウォールは検査対象のコンテンツに対する証明書と秘密鍵を所持していないのが普通です。装置は、DPI-SSL 検査を実行した後で、リモートサーバから送信された証明書を書き直し、新規に生成したこの証明書に署名します。これには、クライアント DPI-SSL の設定で指定した証明書が使用されます。既定では、これはファイアウォールの認証局 (CA) の証明書ですが、別の証明書を指定することもできます。証明書の信頼のエラーを防ぐために、ユーザに対しては、ブラウザの信頼済み証明書の一覧にこの証明書を追加するよう指示する必要があります。

トピック:

- 一般設定の構成
- 再署名認証局の選択
- 除外と包含の設定
- コモンネームによる除外/包含
- クライアント DPI-SSL の例

一般設定の構成

トピック:

- SSL クライアント検査を有効にする
- ゾーンの DPI-SSL クライアントを有効にする
- ゾーンの DPI-SSL サーバを有効にする

SSL クライアント検査を有効にする

SSL クライアント検査を有効にするには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」に移動します。
2. 「**一般**」を選択します。

3. 「**SSL クライアント検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
4. 検査を実行するサービスを 1 つ以上選択します。既定では何も選択されていません。
   - **侵入防御**
   - **ゲートウェイ アンチウイルス**
   - **ゲートウェイ アンチスパイウェア**
   - **アプリケーション ファイアウォール**
   - **コンテンツ フィルタ**
5. 復号化/インターセプトされた接続についてサーバの認証を行うには、「**復号化された接続で常にサーバを認証する**」を選択します。有効にすると、DPI-SSL によって以下のような接続が遮断されます。
   - 信頼できない証明書を使用するサイトへの接続。
   - Client Hello のドメイン名が、この接続のサーバ証明書に照らして検証できない場合。

このオプションは、既定では選択されていません。このオプションを選択すると、「**期限切れ CA を許可する**」が使用可能になります。

ⓘ **重要**:このオプションは、高いレベルのセキュリティが必要な場合にのみ有効にします。遮断された接続は、接続エラー リストに表示されます(「*接続エラーの表示*」を参照してください)。

ⓘ **ヒント**:このオプションを有効にする場合は、「**CFS 種別基準の除外をスキップする**」オプション(「*コモンネームの除外/包含*」を参照)を使用して、このグローバル認証オプションから特定のドメインを除外します。これは、信頼できるサイトのあらゆるサーバ関連エラーをオーバーライドするのに役立ちます。

6. 期限切れまたは中間の CA を許可するには、「**期限切れ CA を許可する**」を選択します。このオプションは、既定では選択されていません。これを選択しないと、Client Hello のドメイン名が、この接続のサーバ証明書に照らして正当であると確認できない場合、接続は遮断されます。
7. 除外のためにサーバ IP アドレスベースの動的キャッシュの使用を無効にするには、「**複数の異なるサーバ**

ドメインをファイアウォールが単一のサーバ IP と見なす配備。例: プロキシ セットアップ」を選択します。このオプションは、既定では選択されていません。

このオプションは、装置がクライアント ブラウザとプロキシ サーバの間に存在する場合を含め、すべてのクライアント ブラウザがプロキシ サーバにリダイレクトされるプロキシ配備で役に立ちます。ドメインが、前面に負荷分散装置を配置したサーバ ファームの一部として、または、同じサーバ IP を複数のドメインで使用できるクラウド配備内で、仮想ホスティング サーバに含まれる場合のドメイン除外など、すべての DPI-SSL 機能がサポートされています。

そのような配備では、装置から見えるすべてのサーバ IP がプロキシ サーバの IP になっています。そのため、プロキシ配備では、IP ベースの除外キャッシュを無効にしておく必要があります。このオプションを有効にしても、SonicOS が除外を実行する機能に影響はありません。

8. 既定では、DPI-SSL の接続制限を超える新しい接続はバイパスされます。接続制限を超えた場合に、新しい接続が破棄されずに復号化をバイパスできるようにするには、「接続制限を超えたときに、復号化なしの SSL を許可 (バイパス) する」チェックボックスをオンにします。このオプションは、既定では選択されています。

DPI-SSL の接続制限を超える新しい接続が確実に破棄されるようにするには、このチェックボックスをオフ (無効) にします。

9. 新しい組み込みの除外ドメイン名を監査したうえで除外のために追加するには、「除外に追加される前に、新しいビルトイン除外ドメイン名を監査する」チェックボックスをオンにします。このチェックボックスは、既定ではオンになっていません。

このオプションを有効にすると、組み込みの除外リストが変更されるたびに (例えば、新しいファームウェア イメージやその他のシステム関連動作のアップグレード)、そうした変更を知らせる通知用ポップアップ ダイアログが「**復号化サービス > DPI-SSL/TLS クライアント**」ページの上に表示されます。新しい変更の内容を検査/監査し、組み込みの除外リストに対する新しい変更のうち任意のもの、一部、またはすべてを許可または拒否することができます。この時点で、実行時除外リストは更新され、新しい変更が反映されます。

このオプションを無効にすると、SonicOS は、組み込み除外リストに対する新しい変更すべての許可および追加を自動的に行います。

10. コモンネームまたは種別の除外ポリシーの適用前にサーバの認証を必ず行うには、「**除外ポリシーを適用する前に、常にサーバを認証する**」チェックボックスをオンにします。このオプションは、既定では選択されていません。有効にすると、DPI-SSL によって以下のような除外された接続が遮断されます。
    - 信頼できない証明書を使用するサイトへの接続。
    - Client Hello のドメイン名が、この接続のサーバ証明書に照らして検証できない場合。

これは、除外ポリシーの適用前にサーバ接続を認証する場合に便利な機能です。このオプションを有効にすると、装置は、接続に対する除外を無分別に適用したり、その結果として除外サイトや除外対象種別に属するサイトについてのセキュリティ ホールを生み出したりすることがなくなります。これは、バンキング サイトが種別として除外されている場合に特に重要です。

サーバ証明書と Client Hello でのドメイン名の両方を検証したうえで除外ポリシーを適用することで、SonicOS は信頼できないサイトを拒否したり、ある主のゼロデイ攻撃の発生を潜在的に阻止したりできます。SonicOS の実装では、「信頼だけでなく検証も」というアプローチを採用しており、除外ポリシーの基準に適合するドメイン名をまず検証するようにし、それによって無防備なクライアントによるフィッシングや URL リダイレクト関連の攻撃を防止しています。

ⓘ **重要:** サブジェクト代替名拡張における代替ドメインを除外する場合は、このオプションを有効にすることをお勧めします。

ⓘ **ヒント:**このオプションを有効にする場合は、「**CFS 種別基準の除外をスキップする**」オプション（「*コモンネームの除外/包含*」を参照）を使用して、このグローバル認証オプションから特定のドメインを除外します。これは、信頼できるサイトのあらゆるサーバ関連エラーをオーバーライドするのに役立ちます。

11. 「適用」をクリックします。

ゾーンの DPI-SSL クライアントを有効にする

ゾーンの DPI-SSL クライアントを有効にするには、以下の手順に従います。

1. 「**オブジェクト | 一致オブジェクト > ゾーン**」に移動します。
2. 設定するゾーンの「**編集**」アイコンを選択します。「ゾーンの編集」ダイアログが表示されます。
3. 「**SSL クライアント検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
4. ゾーンの設定を終了します。
5. 「**OK**」をクリックします。
6. DPI-SSL クライアント検査を有効にする各ゾーンに対して、ステップ 2 からステップ 5 を繰り返します。

ゾーンの DPI-SSL サーバを有効にする

ゾーンの DPI-SSL サーバを有効にするには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > サーバ SSL**」に移動します。

ⓘ **ヒント:**DPI-SSL/TLS サーバの設定については、「*DPI-SSL/TLS サーバの設定*」を参照してください。

2. 「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
3. 1 つ以上の検査種別を選択します。
4. 「**適用**」を選択します。
5. 「**オブジェクト | 一致オブジェクト > ゾーン**」に移動します。
6. 設定するゾーンの「**編集**」アイコンを選択します。「ゾーンの編集」ダイアログが表示されます。
7. 「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。
8. ゾーンの設定を終了します。
9. 「**OK**」をクリックします。
10. DPI-SSL サーバ検査を有効にする各ゾーンに対して、ステップ 6 からステップ 8 を繰り返します。

再署名認証局の選択

再署名証明書は、その認証局の証明書がファイアウォールによって信頼されている場合のみ、元の証明書の署名認証局を置き換えます。認証局が信頼されていない場合、証明書は自己署名になります。証明書エラーを避けるために、DPI-SSL によって保護されているデバイスによって信頼されている証明書を選択してください。

ⓘ **補足:** DPI SSL 認証局（CA）による証明書の要求/作成については、ナレッジ ベースの記事「DPI-SSL 証明書再署名を目的とした DPI-SSL 認証局（CA）による証明書の要求/作成方法（SW14090）」を参照してください。

再署名証明書を選択するには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
2. 「**証明書**」を選択します。

3. 「**証明書**」ドロップダウン メニューから使用する証明書を選択します。既定では、DPI-SSL は、既定の SonicWall の DPI-SSL CA 証明書を使用して、検査したトラフィックを再署名します。

   ⓘ **補足:** 求める証明書が表示されない場合は、「**デバイス | 設定 > 証明書**」ページでその証明書をインポートできます。

4. 選択した証明書をファイアウォールにダウンロードするには、(**ダウンロード**) リンクを選択します。「**ファイル名を開く**」ダイアログが表示されます。

   ⓘ **ヒント:** 利用可能な証明書を表示するには、「(**証明書の管理**)」リンクをクリックして、「**デバイス | 設定 > 証明書**」ページを表示します。

   a. 「**ファイルを保存する**」ラジオ ボタンが選択されていることを確認してください。

   b. 「**OK**」をクリックします。

ファイルがダウンロードされます。

5. 「**適用**」をクリックします。

ブラウザへの信頼の追加

再署名認証局による証明書の再署名を正しく行うためには、ブラウザがこの認証局を信頼する必要があります。この信頼は、ブラウザの信頼できる CA のリストに再署名証明書をインポートすることによって確立できます。お使いのブラウザの指示に従って、再署名証明書をインポートしてください。

除外と包含の設定

既定では、DPI-SSL を有効にすると、それが装置上のすべてのトラフィックに適用されます。DPI-SSL 検査を適用するトラフィックを、以下のようにカスタマイズできます。

- 「**除外/包含**」リストで、除外/包含するオブジェクトとグループを指定します。
- 「**コモンネーム**」除外では、指定したホスト名が除外されます。

- 「**CFS 種別基準の除外/包含**」では、指定した種別が CFS 種別に基づいて除外または包含されます。

このカスタマイズにより、同じサーバ（証明書）でサポートされるドメインのリストに含まれているドメインに対する代替名の個別の除外/包含が可能になります。大量のトラフィックを処理する配備において、DPI-SSL が CPU に及ぼす影響を軽減し、DPI-SSL 検査の同時接続が最大数に達するのを防ぐために、信頼できる送信元を除外することが有効となる場合があります。

ⓘ **補足:** Google ドライブ、Apple iTunes、または証明書がピン留めされたその他任意のアプリケーションの使用時にファイアウォールで DPI-SSL が有効になっている場合、こうしたアプリケーションはサーバに接続できない可能性があります。アプリケーションが接続できるようにするには、関連するドメインを DPI-SSL から除外します。例えば、Google ドライブが機能するようにするには、以下のドメインを除外します。

```
.google.com

.googleapis.com

.gstatic.com
```

Google のすべてのアプリケーションは 1 つの証明書を使用しているので、これらのドメインを除外すれば各種 Google アプリケーションが DPI-SSL をバイパスできるようになります。
あるいは、クライアント マシンを DPI-SSL から除外します。

トピック:

- オブジェクト/グループの除外/包含
- コモンネームによる除外/包含
- CFS 種別基準の除外/包含の指定
- コンテンツ フィルタ
- アプリケーション ルール

オブジェクト/グループの除外/包含

DPI-SSL クライアント検査をカスタマイズするには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
2. 「**オブジェクト**」を選択します。

3. 「**アドレス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

   ⓘ **ヒント:**「**包含**」ドロップダウン メニューは、指定する除外リストの微調整に使用できます。例えば、「**除外**」ドロップダウン メニューで「Remote-office-California」というアドレス オブジェクトを選択し、「**包含**」ドロップダウン メニューで「Remote-office-Oakland」というアドレス オブジェクトを選択します。

4. 「**サービス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

5. 「**ユーザ オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

6. 「**適用**」をクリックします。

コモンネームによる除外/包含

除外リストに信頼されたドメイン名を追加できます。信頼されたドメインを組み込みの除外データベースに追加すると、DPI-SSL が CPU に及ぼす影響が軽減され、装置で DPI-SSL 検査対象の同時接続が最大数に達するのを防ぐことができます。

トピック:

- DPI SSL 既定の除外の状況の表示
- コモンネームの除外/包含
- 個別コモンネームの削除
- 接続エラーの表示
- 既定の除外を手動で更新する

DPI SSL 既定の除外の状況の表示

ファイアウォールは、MySonicWall の DPI SSL 既定の除外データベースの更新を定期的にチェックし、「DPI-SSL 既定除外状況」セクションにデータベースの最新の状況を表示します。「*既定の除外を手動で更新する*」で説明されているように、ファイアウォール上のデータベースを手動で更新できます。

既定の除外の状況を表示するには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント サーバ**」に移動します。
2. 「**コモンネーム**」を選択します。
3. 「**DPI SSL 既定の除外状況**」までスクロールします。

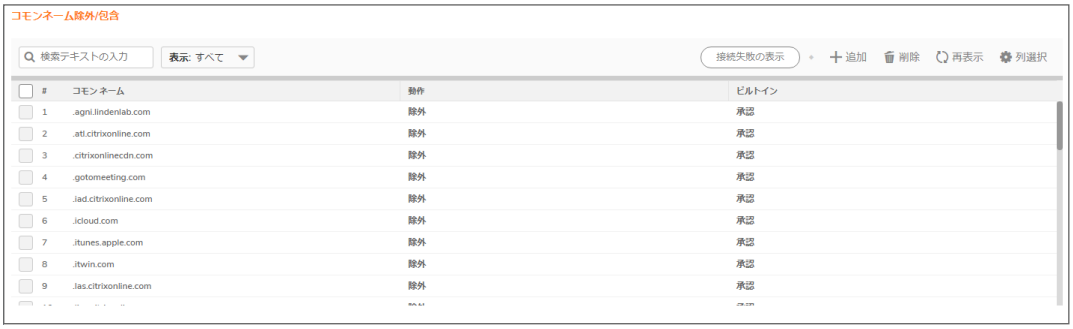
既定除外タイムスタンプ	既定の除外データベースが更新された日時。

最終確認	ファイアウォールが既定の除外データベースをチェックした日時。

コモンネームの除 外 /包 含

コモンネームによってエンティティを除外/包含するには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
2. 「**コモンネーム**」を選択します。
3. 「**コモン ネーム:**」までスクロールします。**除外/包含**。



4. 以下のオプションを選択することで、コモンネームの表示を制御できます。
   - **表示** オプション:
     - **すべて** – すべてのコモンネームを表示します。
     - **既定** – 既定のコモンネーム (「**ユーザ定義**」のものを除く) を表示します。
     - **ユーザ定義** – 管理者が追加したコモンネームのみを表示します。
5. 既定では、すべての組み込みコモンネームが承認されています。組み込みコモンネームの承認は、以下の操作によって拒否できます。
   a. コモンネームの「**構成**」列にある「**このビルトイン名を拒否する**」アイコンをクリックします。確認メッセージが表示されます。

   b. 「**OK**」をクリックします。

「**拒否**」アイコンが「**承認**」アイコンになり、「**ビルトイン**」列の「**承認**」が「**拒否**」になります。

ⓘ | **ヒント**: 組み込みのコモンネームは変更も削除もできませんが、拒否したり許可したりすることはできます。

拒否されたビルトイン コモンネームを許可するには、以下の手順に従います。

   a. 該当する「**このビルトイン名を受け入れる**」アイコンをクリックします。確認メッセージが表示されます。

   b. 「**OK**」をクリックします。

6. 個別コモンネームを追加するには、「**+ 追加**」をクリックします。「**コモンネームの追加**」ダイアログが表示されます。

   a. フィールドに 1 つ以上のコモンネームを追加します。複数のエントリがある場合は、カンマまたは改行文字で区切ります。

   b. 「**動作**」の種別を指定します。

      - **除外**（既定）
      - **CFS 種別基準の除外をスキップする**
      - サーバを認証することによって接続が遮断される場合にこのドメインのサーバの認証を見合わせるには、「**サーバの認証をスキップする**」を選択します。このオプションは、サーバが信頼されたドメインである場合にのみ有効にします。

   c. DPI-SSL は、ある接続がインターセプト（包含）されるか除外されるかを、ポリシーまたは設定に基づいて動的に決定します。DPI-SSL によって接続のドメイン名が抽出されると、同じサーバ/ドメインに対する以降の接続で除外情報が使用できるようになります。

      動的な除外キャッシュ（サーバ IP 基準とコモンネーム基準の両方）の使用を**有効**または**無効**にするには、「**除外ポリシーの適用前にサーバを常に認証する**」ドロップダウン メニューからオプションを選択します。既定では「**グローバル設定を使用する**」が選択されています。

   d. 「**適用**」をクリックします。

      「**コモンネーム除外/包含**」テーブルが更新され、「**ビルトイン**」列が「**個別**」になります。「**除外ポリシーの適用前にサーバを常に認証する**」オプションが選択されている場合は、「**ビルトイン**」列の「**ユーザ定義**」の隣に**情報**アイコンが表示されます。

      情報アイコンをマウスでポイントすると、どの個別属性が選択されていたかがわかります。「**接続エラー リスト**」を使用して追加されたコモンネームの場合、情報アイコンによって以下のエラーの種別が示されます。:

      - **CFS 種別による除外をスキップ**
      - **サーバ認証をスキップ**
      - **サーバの認証に失敗**

- **クライアント ハンドシェイクに失敗**
- **サーバ ハンドシェイクに失敗**

エントリを削除するには、「**設定**」列の**削除**アイコンを選択します。

7. フィルタを指定してコモンネームを検索できます。
   a. 「**フィルタ**」フィールドに、名前を name:mycommonname という構文で指定して入力します。
   b. 「**フィルタ**」をクリックします。
8. 「**適用**」をクリックします。

個別コモンネームの削除

個別コモンネームを削除するには、以下の手順に従います。

1. 以下のいずれかを実行します。
   - 「**設定**」列で、個別コモンネームの**削除**アイコンを選択します。
   - 「**除外**」で名前を選択したうえで、「**削除**」をクリックします。
   - 「**すべて削除**」を選択すると、すべてのコモンネームが削除されます。確認メッセージが表示されます。「**OK**」をクリックします。
2. 「**適用**」をクリックします。

接続エラーの表示

SonicOS は、最近の DPI-SSL クライアント関連の接続エラーのリストを保持しています。これは以下の点で有効性の高い機能です。

- DPI-SSL によってエラーになった接続をリスト表示
- エラーになった接続を監査可能
- 不具合のあるドメインを自動的に除外するしくみを提供

ダイアログには、実行時の接続エラーが表示されます。接続エラーは、以下の理由のいずれかによって発生する可能性があります。

- クライアントとのハンドシェイクの失敗
- サーバとのハンドシェイクの失敗
- Client Hello 内のドメイン名の検証の失敗
- サーバの認証の失敗（サーバ証明書の発行者が信頼できない）

このエラー リストは実行時にのみ利用可能です。エラーごとにログに記録される数値は、1 つのエラー種別でバッファ全体の領域を超過することがないように、制限されています。

接続エラー リストを使用するには、以下の手順に従います。

1. 「**接続失敗の表示**」をクリックします。「**接続失敗リスト**」ダイアログが表示されます。

   このリストの各エントリには、次の項目が表示されます。

   - **クライアント アドレス**
   - **サーバ アドレス**
   - **コモンネーム** – 接続に失敗したドメインのコモンネームです。このエントリは、自動除外リストに追加する前に、インラインで編集できます。
   - **エラー メッセージ** – この接続の除外について適切な判断ができるように、接続に関連付けられたコンテキスト情報を提供します。

2. 除外リストにエントリを追加するには、以下の手順に従います。
   a. 項目を選択します。
   b. エントリを編集します。
   c. 「**除外**」をクリックします。
3. エントリを削除するには、以下の手順に従います。
   a. エントリを選択します。
   b. 「**消去**」を選択します。
4. すべてのエントリを削除するには、「**すべて消去**」をクリックします。
5. 終了したら、「**閉じる**」をクリックします。

既定の除外を手動で更新する

環境が閉じている場合、または既定の除外を手動で更新する場合は、www.MySonicWall.com から既定の除外データベースをダウンロードしてインポートできます。

既定の除外を手動で更新するには、以下の手順に従います。

1. www.MySonicWall.com から既定の除外データベースをインポートします。
2. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
3. 「**既定の除外を手動で更新する**」セクションまでスクロールします。

4. 「**除外のインポート**」を選択します。「**除外ファイルのインポート**」ダイアログが表示されます。

5. 「**ファイルの追加**」をクリックします。「**ファイルのアップロード**」ダイアログが表示されます。
6. ダウンロードした既定の除外データベース ファイルを開きます。
7. 「DPI-SSL 既定除外状況」セクションで、「**コモンネーム除外/包含**」テーブルと、ファイアウォールで使用されている既定のデータベースの状況が更新されます。

CFS 種別基準の除外/包含の指定

コンテンツ フィルタ種別によってエンティティを除外/包含できます。

CFS 種別基準の除外/包含を指定するには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
2. 「**CFS 種別基準の除外/包含**」を選択します。

リストの状況は、ビューの一番上にあるアイコンで示されます。緑のアイコンはコンテンツ フィルタがライセンスされていることを示し、赤いアイコンはライセンスされていないことを示します。

3. 選択した種別を含めるか除外するかを選択するには、次のどちらかを選択します。
   - **除外**（既定）
   - **包含**

既定では、すべての種別の選択が解除されています。

4. 必要に応じて、ステップ 3 およびステップ 4 を繰り返して、他方のリストを作成します。
5. 包含/除外する種別を選択します。すべての種別を選択する場合は、「**すべての種別を選択**」をクリックします。
6. また、ドメインのコンテンツ フィルタ種別情報が DPI-SSL で利用可能でない場合に接続を除外するために、「**コンテンツ フィルタ種別を使用できない場合に接続を除外する**」チェックボックスをオンにすることもできます。このオプションは、既定では選択されていません。

   ほとんどの場合、HTTPS ドメインの種別情報は、ファイアウォール キャッシュにおいてローカルで利用可能です。種別情報がローカルで利用可能でない場合、DPI-SSL は、クライアントまたはサーバ通信を遮断することなく、種別情報をクラウドから取得します。まれに、DPI-SSL が判断を行うための種別情報が利用可能でない場合があります。既定では、そのようなサイトが DPI-SSL で検査されます。
7. 「**適用**」をクリックします。

クライアント DPI-SSL の例

トピック:

- コンテンツ フィルタ
- アプリケーション ルール

コンテンツ フィルタ

HTTPS および SSL ベースのトラフィック上で SonicWall のコンテンツ フィルタの実行に DPI-SSLを使用するには、以下の手順に従います。

1. 「**ポリシー | セキュリティ サービス > コンテンツ フィルタ**」に移動します。
2. 「コンテンツ フィルタ種別」としてドロップダウン メニューで「SonicWall CFS」が選択されていることを確認します。
3. 「**グローバル設定**」セクションまでスクロールします。

4. 「**コンテンツ フィルタ サービス (CFS) を有効にする**」を選択します。
5. 「**適用**」をクリックします。
6. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
7. 「**一般**」を選択します。

8. 「**SSL クライアント検査を有効にする**」チェックボックスをオンにします。
9. 「**コンテンツ フィルタ**」チェックボックスをオンにします。
10. 「**適用**」をクリックします。
11. HTTPS プロトコルを使用して、遮断されるサイトに移動し、適切に遮断されることを確認します。

> ⓘ **補足:** DPI-SSL 上のコンテンツ フィルタで HTTPS アクセスを初めて遮断したときには、空白のページが表示されます。ページを更新すると、ファイアウォールの遮断ページが表示されます。

アプリケーション ルール

アプリケーション ファイアウォール ルールによってフィルタするには、「**ポリシー | DPI-SSL > クライアント SSL**」ページと「**ポリシー | ルールとポリシー > アプリケーション制御**」ページの両方で、それらを有効にする必要があります。

1. 「**ポリシー | DPI-SSL > クライアント SSL**」ページに移動します。
2. 「**一般**」を選択します。

3. 「**SSL クライアント検査を有効にする**」チェックボックスをオンにします。
4. 「**アプリケーション ファイアウォール**」チェックボックスをオンにします。
5. 「**適用**」をクリックします。
6. 「**ポリシー | ルールとポリシー > アプリケーション制御**」ページに移動します。
7. 「**アプリケーション ルールのグローバル設定**」セクションまでスクロールします。
8. 「**アプリケーション制御を有効にする**」を選択します。このオプションは、既定では選択されていません。
9. ポリシーの動作として「ページの遮断」を設定し、Microsoft Internet Explorer ブラウザを遮断するように、HTTP クライアント ポリシーを設定します。
10. 「**適用**」をクリックします。
11. Internet Explorer から HTTPS プロトコルで任意のウェブサイトにアクセスし、遮断されることを確認します。

3

DPI-SSL/TLS サーバの設定

トピック:

- 復号化サービス > DPI-SSL/TLS サーバ
- DPI-SSL/TLS サーバ設定について

復号化サービス > DPI-SSL/TLS サーバ

ⓘ | **補足:** DPI SSL については、「DPI-SSL について」を参照してください。

通常、サーバ DPI-SSL の配備シナリオは、リモート クライアントが WAN 経由で接続してファイアウォールの LAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。サーバ DPI-SSL では、アドレス オブジェクトと証明書のペアリングを設定できます。アドレス オブジェクトへの SSL 接続を検出した装置は、ペアリングされた証明書を提示し、接続するクライアントと SSL のネゴシエーションを行います。

その後、ペアリングでサーバがクリアテキストと定められている場合は、サーバの元の (NAT 再割付後の) ポートに対して標準の TCP 接続が行われます。ペアリングがクリアテキストと定められていない場合、サーバへの SSL 接続がネゴシエーションされます。これにより、接続のエンドツーエンドの暗号化に対応できます。

ⓘ | **補足:** この配備方針では、ファイアウォールの所有者が元のコンテンツ サーバの証明書と秘密鍵を所持しています。サーバの元の証明書を装置にインポートし、サーバ DPI-SSL の UI で、サーバ IP アドレスとサーバ証明書の適切な割付を作成する必要があります。

DPI-SSL/TLS サーバ設定について

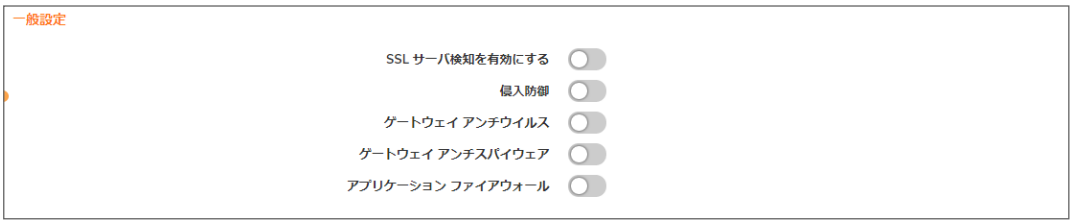
トピック:

- DPI-SSL/TLS サーバの一般設定
- 除外と包含の設定
- サーバと証明書のペアリングの設定

DPI-SSL/TLS サーバの一般設定

サーバ DPI-SSL 検査を有効にするには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > サーバ SSL**」ページに移動します。



2. 「**一般設定**」セクションまでスクロールします。
3. 「**SSL サーバ検査を有効にする**」を選択します。
4. 検査を実行するサービスを 1 つ以上選択します。

- **侵入防御**
- ゲートウェイ アンチウイルス
- **ゲートウェイ アンチスパイウェア**
- **アプリケーション ファイアウォール**

5. 「**適用**」をクリックします。
6. 「**SSL サーバ**」セクションにスクロールして、DPI-SSL 検査を適用するサーバを設定します。「*サーバと証明書のペアリングの設定*」を参照してください。

除外と包含の設定

既定では、DPI-SSL を有効にすると、装置のすべてのトラフィックに適用されます。包含/除外リストを設定すると、DPI-SSL 検査を適用するトラフィックをカスタマイズできます。**包含/除外**リストでは、オブジェクトまたはグループを指定できます。大量のトラフィックを処理する配備において、DPI-SSL が CPU に及ぼす影響を軽減し、DPI-SSL 検査の同時接続が最大数に達するのを防ぐために、信頼できる送信元を除外することが有効となる場合があります。

DPI-SSL サーバ検査をカスタマイズするには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > サーバ SSL**」ページに移動します。
2. 「**包含/除外**」セクションまでスクロールします。

3. 「**アドレス オブジェクト/グループ**」の「**除外**」から、DPI-SSL 検査から除外するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」に設定されています。
4. 「**アドレス オブジェクト/グループ**」の「**包含**」から、DPI-SSL 検査に含めるアドレス オブジェクト/グループを選択します。既定では、「**包含**」は「**すべて**」に設定されています。

   ヒント:「**包含**」は、指定した除外リストを微調整するために使用できます。たとえば、「**除外**」から Remote-office-California アドレス オブジェクトを選択し、「**包含**」から Remote-office-Oakland アドレス オブジェクトを選択します。
5. 「**ユーザ オブジェクト/グループ**」の「**除外**」から、DPI-SSL 検査から除外するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」に設定されています。
6. 「**ユーザ オブジェクト/グループ**」の「**包含**」から、DPI-SSL 検査に含めるアドレス オブジェクト/グループを選択します。既定では、「**包含**」は「**すべて**」に設定されています。
7. 「**適用**」をクリックします。

サーバと証明書のペアリングの設定

サーバ DPI-SSL の検査では、トラフィックに対して DPI-SSL 検査を実行する各サーバへのトラフィックの署名にどの証明書を使用するかを指定する必要があります。

サーバと証明書のペアリングを設定するには、以下の手順に従います。

1. 「**ポリシー | DPI-SSL > サーバ SSL**」ページに移動します。
2. 「**SSL サーバ**」セクションまでスクロールします。

3. 「**+ 追加**」をクリックします。「**SSL サーバの設定**」ダイアログが表示されます。

4. 「**アドレス オブジェクト/グループ**」で、DPI-SSL 検査を適用するサーバに対応するアドレス オブジェクト/グループを選択します。
5. 「**SSL 証明書**」で、サーバへのトラフィックの署名に使用する証明書を選択します。この証明書は、トラフィックで DPI-SSL サーバ検査が実行された各サーバのトラフィックに署名するために使用されます。詳細情報の参照先は次のとおりです。

- 装置への新しい証明書のインポートについては、「再署名認証局の選択」を参照してください。
- Linux **証明書の作成**。

  ⓘ | **ヒント:**(証明書の管理)リンクをクリックすると、「**デバイス | 設定 > 証明書**」ページが表示されます。

6. SSL オフロードを有効にするには、「**平文**」を選択します。サーバと証明書のペアリングを追加するとき、「**平文**」オプションを使用すると暗号化されていないデータをサーバに送信できます。このオプションは、既定では選択されていません。

   ⓘ | **重要:**この設定が適切に動作するためには、このサーバに対する NAT ポリシーを「**ポリシー | ルールとポリシー > NAT ルール**」ページで作成し、オフロード サーバに対するトラフィックを SSL ポートから非 SSL ポートに割り付ける必要があります。トラフィックは、443 以外のポートに送信する必要があります。例えば、SSL オフロードで HTTPS トラフィックを使用している場合、適切な動作のためには、トラフィックをポート 443 からポート 80 に再割付する受信 NAT ポリシーを作成する必要があります。

7. 「**追加**」を選択します。

4

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます https://www.sonicwall.com/ja-jp/support。

サポート ポータルでは、次のことができます。

- ナレッジベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする https://community.sonicwall.com/technology-and-support。
- ビデオ チュートリアルを視聴する。
- 次のサイトにアクセスする https://mysonicwall.com。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートに連絡するには、次の URL にアクセスします https://www.sonicwall.com/ja-jp/support/contact-support。

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS DPI-SSL 管理ガイド
更新日 - 2021 年 1 月
ソフトウェア バージョン - 7
232-005440-10 Rev A

エンドユーザ製品契約

SonicWall エンドユーザ製品契約を参照する場合は、以下に移動してください https://www.sonicwall.com/ja-jp/legal。

オープン ソース コード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、"SonicWall Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035