SonicOS および SonicOSX 7 SSL VPN

管理ガイド

SONICWALL®

目次

SSL VPN について **3**
NetExtender について 7
NetExtender 範囲に対するアドレス オブジェクトの作成 7
アクセスの設定 8
プロキシの設定 9
スタンドアロン クライアントのインストール 10
SSL VPN アクセスのためのユーザの設定 10
ローカル ユーザの場合 10
RADIUS、LDAP、TACACS+ ユーザの場合 11
強制トンネル方式アクセスの場合 13
生体認証 14

SSL VPN サーバの動作の設定 **15**
サーバ設定ページ 15
ゾーン上の SSL VPN 状況 15
SSL VPN サーバ設定 15
RADIUS ユーザの設定 16
SSL VPN クライアント ダウンロード URL 17

SSL VPN クライアントの設定 **18**
設定オプションの設定 19
クライアント ルートの設定 19
クライアント設定の指定 20

SSL VPN ウェブポータルの設定 **22**
ポータル設定 22
ポータル ロゴ 設定 23

SSL VPN セッションの表示 **24**
状況ページ 24
ブックマーク ページ 24

仮想オフィスの設定 **25**
仮想オフィス ポータルへのアクセス 25
NetExtender の使用 25
SSL VPN ブックマークの設定 26
IPv6 用のデバイス プロファイルの設定 30

SonicWall サポート **31**
このドキュメントについて 32

3

SSL VPN について

補足: SonicOS/X という表記は、その機能が両方の SonicOS および SonicOSX で使用可能なことを示します。

このセクションでは、SonicWall ネットワーク セキュリティ装置における SSL VPN 機能の設定方法を説明します。SonicWall の SSN VPN 機能は、NetExtender クライアントを使用してネットワークへのリモート アクセスを保護します。

NetExtender は、Windows または Linux ユーザ用の SSL VPN クライアントであり、透過的にダウンロードされます。ネットワーク上で任意のアプリケーションを安全に実行でき、ポイント ツー ポイント プロトコル (PPP) を使用できるようになります。NetExtender によって、リモート クライアントはローカル ネットワーク上のリソースにシームレスにアクセスできます。ユーザは、次の 2 通りの方法で NetExtender にアクセスできます。

- SonicWall ネットワーク セキュリティ装置によって提供される仮想オフィス ウェブ ポータルにログインする
- スタンドアロンの NetExtender クライアントを起動する

各 SonicWall 装置は、最大数の現在のリモート ユーザをサポートしています。詳細については、「SSL VPN の最大同時ユーザ数」を参照してください。

最大同時ユーザ数 (ハードウェア ファイアウォール)

SonicWall 装置モデル	SSL VPN の最大同時接続数
NSa 9650	3000
NSa 9450	3000
NSa 9250	3000
NSa 6650	2000
NSa 5650	1500
NSa 4650	1000
NSa 3650	500
NSa 2650	350
SM 9600	3000
SM 9400	3000
SM 9200	3000
NSA 6600	1500
NSA 5600	1000
NSA 4600	500

SonicWall 装置モデル	SSL VPN の最大同時接続数
NSA 3600	350
NSA 2600	250
TZ600/TZ600P	200
TZ500/TZ500 W	150
TZ400/TZ400 W	100
TZ350/TZ350 W	75
TZ300/TZ300 W/TZ300P	50
SOHO 250/SOHO 250W	25

最大同時ユーザ数 (VMWARE)

VMWare ESXi 装置モデル	SSL VPN の最大同時接続数
10	10
25	25
50	25
100	25
200	50
300	50
400	50
800	50
1600	50

最大同時ユーザ数 (AZURE)

Azure 装置モデル	SSL VPN の最大同時接続数
10	10
25	25
50	25
100	25
200	100
400	100
800	100
1600	100

最大同時ユーザ数 (AWS)

AWS 装置モデル	SSL VPN の最大同時接続数
10	10

AWS 装置モデル	SSL VPN の最大同時接続数
25	25
50	25
100	25
200	50
400	50
800	50
1600	50

最大同時ユーザ数 (AWS – PAYG)

AWS – PAYG 装置モデル	SSL VPN の最大同時接続数
200	50
400	50
800	50
1600	50

最大同時ユーザ数 (LINUX KVM)

Linux KVM 装置モデル	SSL VPN の最大同時接続数
10	10
25	25
50	25
100	25
200	50
300	50
400	50
800	50
1600	50

最大同時ユーザ数 (MICROSOFT HYPER-V)

Microsoft Hyper-V 装置モデル	SSL VPN の最大同時接続数
10	10
25	25
50	25
100	25
200	50
300	50

Microsoft Hyper-V 装置モデル	SSL VPN の最大同時接続数
400	50
800	50
1600	50

SonicOS/X は IPv6 アドレスによるユーザ向けの NetExtender 接続をサポートしています。アドレス オブジェクトのドロップダウン メニューには、事前定義されたすべての IPv6 アドレス オブジェクトが含まれています。

ⓘ **補足:** IPv6 Wins サーバはサポートされていません。IPv6 FQDN がサポートされています。

ⓘ **補足:** 「**デバイス | 設定 > 管理**」ページの「無線コントローラ モード」が「**無線コントローラ**」で、「全機能ゲートウェイ」または「無線なし」に設定されているとき、SSL VPN 接続を利用できます。「無線コントローラ モード」で「無線コントローラ専用」が有効になっている場合、SSL VPN インターフェースは使用できません。

「**ネットワーク | SSL VPN > サーバ設定 > ゾーンの SSL VPN 状況**」の状況表示はすべてのゾーンで停止中となり、SSL VPN ゾーンは編集できません。

トピック:

- NetExtender について
- SSL VPN アクセスのためのユーザの設定
- 生体認証

NetExtender について

SonicWall の SSL VPN NetExtender は、Windows および Linux ユーザ向けの透過的なソフトウェア アプリケーションであり、その機能を使うことでリモート ユーザは会社のネットワークにセキュアな方法で接続できます。NetExtender により、リモート ユーザは会社のネットワーク上の任意のアプリケーションを安全に実行できます。ファイルのアップロード/ダウンロード、ネットワーク ドライブのマウント、リソースへのアクセスといった作業がローカル ネットワークにいる感覚で行えます。

NetExtender により、リモート ユーザは保護された内部ネットワークへのフル アクセスが可能になります。その際の操作方法は、従来の IPSec VPN クライアントとほとんど同じです。Linux システムでも、NetExtender クライアントをインストールして使用することができます。Windows ユーザは、ポータルからクライアントをダウンロードする必要があり、モバイル機器を使用している ユーザは、アプリケーション ストアから Mobile Connect をダウンロードする必要があります。

NetExtender スタンドアロン クライアントは、ユーザによるポータルからの NetExtender の初回起動時にインストールできます。そのため、Windows システムでは「スタート」メニューからの直接アクセスが可能です。また Linux システムでも、パス名によって、あるいはショートカット バーから直接アクセスできます。

インストール後、NetExtender が自動的に起動し、SSL VPN を利用した安全なポイントツーポイント アクセスによって内部ネットワーク上の許可されたホストおよびサブネットにアクセスするための仮想アダプタに接続します。

トピック:

- NetExtender 範囲に対するアドレス オブジェクトの作成
- アクセスの設定
- プロキシの設定
- スタンドアロン クライアントのインストール

NetExtender 範囲に対するアドレス オブジェクトの作成

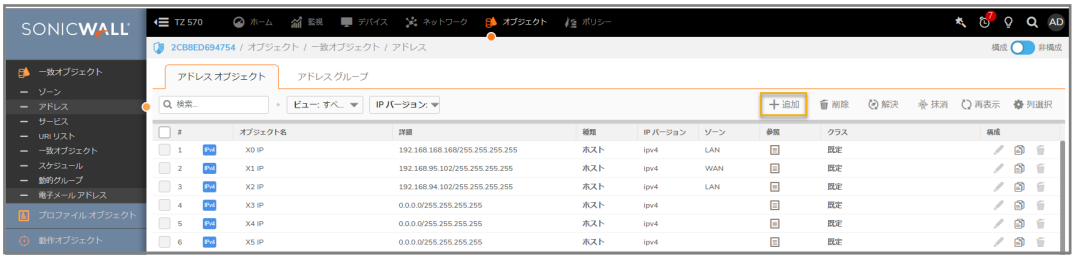
NetExtender 設定の一部として、NetExtender IP アドレス範囲に対するアドレス オブジェクトを作成する必要があります。その後、このアドレス オブジェクトはデバイス プロファイルの設定時に使用します。

使用する IPv4 アドレス範囲と IPv6 アドレス範囲の両方のアドレス オブジェクトを、「**SSL VPN > クライアント設定**」で作成できます。アドレス オブジェクトで設定されるアドレス範囲は、NetExtender セッション中にリモート ユーザに割り当てられるアドレスを含む IP アドレス プールを定義します。この範囲は、サポートする NetExtender 同時ユーザの最大数に対応できる大きさにする必要があります。さらにアドレスを追加して対応数を増やすことはできますが、これは必須ではありません。

ⓘ **補足:** 装置と同じセグメント上に他のホストが存在する場合は、アドレス範囲が、他の割り当て済みアドレスと重複したり衝突したりしないようにしてください。

NetExtender IP アドレス範囲に対するアドレス オブジェクトを作成するには、以下の手順に従います。

1. 「**オブジェクト > アドレス オブジェクト**」に移動します。
2. 「追加」を選択します。



3. 「名前」フィールドにわかりやすい名前を入力します。
4. 「ゾーンの割り当て」で、「**SSLVPN**」を選択します。
5. 「種別」で、「**範囲**」を選択します。
6. 「開始アドレス」フィールドに、使用するアドレス範囲内の最小 IP アドレスを入力します。

   メモ: IP アドレス範囲は、SSL VPN サービスで使用されるインターフェースと同じサブネット上になければなりません。IP アドレス範囲が他の割り当て済み範囲と衝突しないようにしてください。
7. 「終了アドレス」フィールドに、使用するアドレス範囲内の最大 IP アドレスを入力します。

8. 「**追加**」を選択します。
9. 「**閉じる**」を選択します。

アクセスの設 定

NetExtender クライアント ルートは、SSL VPN ユーザによる各種ネットワーク リソースへのアクセスを許可または拒否するために使用されます。アドレス オブジェクトを使用することで、ネットワーク リソースへのアクセスを動的かつ容易に設定できます。強制トンネル方式では、リモート ユーザとやり取りされるすべてのトラフィックが (リモート ユーザのローカル ネットワークへのトラフィックを含め) SSL VPN NetExtender トンネルを経由します。これは、次のルートをリモート クライアントのルート テーブルに追加することで実行されます。

リモート クライアントのルート テーブルに追加されるルート

IP アドレス	サブネット マスク
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender は、接続中のすべてのネットワーク接続のローカル ネットワーク ルートも追加します。これらのルートには既存のルートよりも高いメトリックが設定されているため、ローカル ネットワークへのトラフィックは強制的に SSL VPN トンネル経由に切り替えられます。例えば、リモート ユーザが 10.0.*.* ネットワークの IP アドレス 10.0.67.64 を使用している場合、ルート 10.0.0.0/255.255.0.0 が追加され、トラフィックが SSL VPN トンネルを経由するようになります。

ⓘ **補足:** 強制トンネル方式を設定するにはまた、0.0.0.0 のアドレス オブジェクトを設定して、SSL VPN NetExtender ユーザとグループがこのアドレス オブジェクトへのアクセスを持つように割り当てる必要があります。

管理者も、NetExtender の接続が確立および切断されたときにバッチ ファイル スクリプトを実行できます。これらのスクリプトを使って、ネットワーク ドライブやプリンタのマッピングおよび切断、アプリケーションの起動、ファイルやウェブ サイトの表示などを行うことができます。NetExtender の接続スクリプトでは任意の有効なバッチ ファイル コマンドを使用できます。

プロキシの設定

SonicWall SSL VPN は、プロキシ設定を使用した NetExtender セッションをサポートしています。現在サポートされているのは、HTTPS プロキシのみです。プロキシ設定は、NetExtender クライアントでの手動設定も可能です。NetExtender は、Web Proxy Auto Discovery (WPAD) プロトコルに対応したプロキシ サーバ用のプロキシ設定を自動的に検出できます。

NetExtender には、次の 3 つのプロキシ設定オプションが用意されています。

- 「設定を自動検出する」 — この設定を使用するには、プロキシ サーバが Web Proxy Auto Discovery Protocol プロトコルをサポートしていて、プロキシ設定スクリプトをクライアントに自動送信できる必要があります。
- 自動設定スクリプトを使用する — プロキシ設定スクリプトの場所がわかっている場合は、このオプションを選択してスクリプトの URL を指定することができます。
- プロキシ サーバを使用する — このオプションを選択すると、プロキシ サーバの IP アドレスとポートを指定できます。また、「プロキシのバイパス」フィールドに IP アドレスまたはドメインを入力すれば、それらのアドレスに直接接続してプロキシ サーバをバイパスすることができます。必要に応じて、プロキシ サーバ用のユーザ名とパスワードも入力できます。プロキシ サーバがユーザ名とパスワードを要求しているのにそれらを指定していない場合は、最初の接続時に NetExtender のポップアップ ウィンドウが表示され、その入力を求められます。

プロキシ設定を使用して接続する場合、NetExtender は、ファイアウォールのサーバに直接接続せず、プロキシ サーバへの HTTPS 接続を確立します。その後、プロキシ サーバによってトラフィックが SSL VPN サーバに転送されます。すべてのトラフィックは、NetExtender とネゴシエートされた証明書を使って SSL によって暗号化されます。これについては、プロキシ サーバ側は関知していません。プロキシを使用してもしなくても、接続のプロセスに違いはありません。

スタンドアロン クライアントのインストール

ユーザによる NetExtender の初回起動時にインストーラをダウンロードして、ユーザのシステムで実行することもできます。インストーラでは、ユーザのログイン情報に基づいてプロファイルが作成されます。その後、インストーラのウィンドウが閉じ、NetExtender が自動的に起動します。旧バージョンの NetExtender が既にインストールされていた場合、インストーラは古い NetExtender を最初にアンインストールするかユーザにアンインストールするよう要求し、その後、新バージョンをインストールできます。

NetExtender スタンドアロン クライアントのインストール後、Windows の場合は「スタート > プログラム」メニューまたはシステム トレーを使用して NetExtender を起動し、Windows の起動時に NetExtender が起動されるように設定できます。Mac の場合は、システムのアプリケーション フォルダから NetExtender を起動できます。また、アイコンをドックにドラッグしてすばやくアクセスすることもできます。Linux システムでは、インストーラによってデスクトップ ショートカットが /usr/share/NetExtender に作成されます。このショートカットは、Gnome や KDE といった環境のショートカット バーにドラッグできます。

補足: SonicWall 装置に NetExtender をインストールする詳細な手順については、ナレッジ ベースの記事「*SonicOS 5.9 以降で SSL-VPN 機能 (NetExtender アクセス) を設定する方法 (SW10657)*」を参照してください。

ビデオ: 「*How to configure SSL VPN*」(SSL VPN の設定方法) というビデオでも NetExtender の設定手順を説明しています。

SSL VPN アクセスのためのユーザの設定

ユーザは、SSL VPN サービスにアクセスできるためには、SSLVPN サービス グループに割り当てられている必要があります。「SSLVPN サービス」グループに属していないユーザが仮想オフィスからログインを試みても、アクセスは拒否されます。

トピック:

- ローカル ユーザの場合
- RADIUS および LDAP ユーザの場合
- 強制トンネル方式アクセスの場合

ローカル ユーザの場合

以下はクイック リファレンスで、SSLVPN サービスの有効化に必要なユーザ設定が記載されています。

ローカル ユーザ向けの SSL VPN アクセスを設定するには、以下の手順に従います。

1. 「**管理 | システム セットアップ | ユーザ > ローカル ユーザ & グループ**」に移動します。

2. 設定したいユーザに対する編集アイコンを選択するか、「ユーザの追加」を選択して新しいユーザを作成します。
3. 「**グループ**」を選択します。
4. 「**ユーザ グループ**」列の「**SSLVPN サービス**」を選択し、右矢印を選択してこれを「**所属するグループ**」列に移動します。
5. 「**VPN アクセス**」を選択し、適切なネットワーク リソース VPN ユーザ（GVC、NetExtender、または仮想オフィス ブックマーク）を「**アクセス リスト**」に移動します。

   ⓘ **補足:** 「VPN アクセス」設定は、GVC、NetExtender、または SSL VPN 仮想オフィス ブックマークを使ってネットワーク リソースにアクセスするリモート クライアントの能力に影響します。GVC、NetExtender、または仮想オフィスのユーザにネットワーク リソースへのアクセスを許可するには、ネットワーク アドレス オブジェクトかグループを「VPN アクセス」の「アクセス リスト」に追加する必要があります。
6. 「OK」を選択します。

RADIUS、LDAP、TACACS+ ユーザの場合

RADIUS、LDAP、TACACS+ ユーザの設定手順は同様です。これらのユーザを「SSL VPN サービス」ユーザ グループに追加する必要があります。

RADIUS、LDAP、TACACS+ ユーザ向けの SSL VPN アクセスを設定するには、以下の手順に従います。

1. 「**オブジェクト | ユーザ オブジェクト > 設定**」表示を選択して、「**認証**」タブを選択します。

2. 「ユーザ認証方式」フィールドで:「**RADIUS**」または「**RADIUS + ローカル ユーザ**」を選択します。「**LDAP**」または「**LDAP + ローカル ユーザ**」を選択します。
3. 以下を選択します。**RADIUS の構成または LDAP の構成**
4. 以下を選択します。「**RADIUS ユーザ > ユーザ & グループ**」
5. 適切なフィールドの「**SSLVPN サービス**」を選択します。すべての RADIUS ユーザが所属する既定のユーザグループまたは既定の LDAP ユーザ グループ

6. 「OK」を選択します。

強制トンネル方式アクセスの場合

ローカル ユーザおよびグループの詳しい追加方法と設定方法が、『*SonicOS/X ユーザ*』に記載されています。以下はクイック リファレンスで、「**強制トンネル**」方式に対してユーザとグループを設定するために必要なユーザ設定が記載されています。

SSL VPN NetExtender ユーザとグループを強制トンネル方式のために設定するには、以下の手順を実行します。

1. 「**オブジェクト | ユーザ オブジェクト | ユーザ > ローカル ユーザ & グループ**」に移動します。

2. 追加アイコンをクリックし、SSLVPN を選択したグループとして定義します。
3. 「VPN アクセス」を選択します。

4. 「WAN リモート アクセス ネットワーク」アドレス オブジェクトを選択し、右矢印をクリックして「アクセス リスト」まで移動させます。

5. 5 SSL VPN NetExtender を使うすべてのローカル ユーザおよびグループに対して、このプロセスを繰り返します。

生体認証

ⓘ **重要:** 生体認証を使用するには、モバイル デバイスに Mobile Connect 4.0 以上をインストールしてファイアウォールに接続しておく必要があります。

SonicOS/X は、SonicWall Mobile Connect と連携して生体認証をサポートしています。Mobile Connect は、ユーザがモバイル デバイスからプライベート ネットワークに安全にアクセスできるようにするアプリケーションです。Mobile Connect 4.0 では、ユーザ名とパスワードの代わりにフィンガー タッチによる認証を使用できます。

この認証方法を許可する設定項目は「**ネットワーク | SSL VPN > クライアント設定**」ページにあります。これらのオプションが表示されるのは、Mobile Connect を使用してファイアウォールに接続している場合のみとなります。

「**SSL VPN > クライアント設定**」ページで生体認証を設定した後、ユーザのスマートフォンまたはその他のデバイスで、TouchID (iOS) または指紋認証 (Android) を有効にする必要があります。

4

SSL VPN サーバの動作の設定

「**SSL VPN > サーバ設定**」ページでは、SSL VPN サーバとして機能するファイアウォールを設定します。

サーバ設定ページ

トピック:

- ゾーンの SSL VPN 状況
- SSL VPN サーバ設定
- RADIUS ユーザ設定
- SSL VPN クライアント ダウンロード URL

ゾーン上の SSL VPN 状況

このセクションには、ゾーン毎の SSL VPN アクセス状況が表示されます。

- 緑色は、SSL VPN が有効であることを示します。
- 赤色は、SSL VPN が無効であることを示します。

SSL VPN アクセスを有効または無効にするには、ゾーン名を選択します。

SSL VPN サーバ設定

SSL VPN サーバを設定するには、以下の手順に従います。

1. 「**SSL VPN ポート**」フィールドに SSL VPN ポート番号を入力します。既定値は 4433 です。
2. 「**証明書の選択**」ドロップダウン メニューから、SSL VPN ユーザを認証するために使う証明書を選択します。既定の方法は、「**自己署名証明書を使用**」です。
3. 「**ユーザ ドメイン**」フィールドにユーザのドメインを入力します。これは、NetExtender クライアントのドメイン フィールドと一致する必要があります。既定は「**LocalDomain**」です。
    - 認証パーティションを使用していない場合、このフィールドの値は、NetExtender クライアントのドメイン フィールドと一致している必要があります。

- 認証パーティションを使用している場合は、NetExtender で、そのパーティションを使用して設定されたドメイン名のいずれかをユーザが入力できるため、RADIUS または LDAP 経由で外部から名前/パスワードの認証を行う場合にこのパーティションを選択します。この場合、ここで設定される名前はユーザがローカル認証のために入力する既定の名前（またはローカル アカウントを持っていないユーザが既定のパーティションで認証のために入力する既定の名前）となります。
- いずれの場合も、このユーザのドメイン名は、外部認証を取得して使用すると RADIUS/LDAP サーバには送信されず、外部認証がない単純なユーザ名が送信されます。

4. SSL VPN を介したウェブ管理を有効にするには、「**SSL VPN でウェブ管理を有効にする**」ドロップダウン メニューから「有効」を選択します。既定は「無効」です。
5. SSL VPN を介した SSH 管理を有効にするには、「**SSL VPN で SSH 管理を有効にする**」ドロップダウン メニューから「有効」を選択します。既定は「無効」です。
6. 「**無動作タイムアウト（分）**」フィールドにユーザをログアウトさせるまでの無動作時間を分単位で入力します。既定値は 10 分です。

RADIUS ユーザの設定

このセクションは、「**オブジェクト | ユーザ オブジェクト > 設定**」ページでの SSL VPN ユーザ認証のために、RADIUS か LDAP のどちらかが設定されている場合のみ利用可能です。RADIUS の MSCHAP モードが有効になっている場合、ユーザはログイン時に期限切れのパスワードを変更できます。

MSCHAP または MSCHAPv2 モードを設定するには、以下の手順に従います。

1. 「**RADIUS を以下のモードで使用する**」を選択します。
2. 次の 2 つのモードのどちらかを選択します。
   - **MSCHAP**
   - **MSCHAPV2**

   ⓘ **補足:** LDAP では、Active Directory（アクティブ ディレクトリ）を TLS と共に使用して管理アカウントでそれにバインドしている場合か Novell eDirectory（ノベル イーディレクトリ）を使用している場合にのみ、パスワードを変更できます。

   このオプションが設定されており、「ユーザ > 設定」ページの「ログインの認証方法」として LDAP が選択されているが、LDAP がパスワードの更新を許可する設定になっていない場合、LDAP を使用してユーザ認証が行われた後で、MSCHAP モードの RADIUS を使用して SSL VPN ユーザのパスワードの更新が実行

されます。

3. ページ下部にある「**適用**」を選択します。

SSL VPN クライアント ダウンロード URL

このページのこのセクションでは、クライアント システムによる SSL VPN クライアントのダウンロード元を設定します。装置からファイルをダウンロードしてウェブ サーバに配置することで、このクライアント パッケージをホストする独自のサーバを提供できます。それ以外の場合、クライアントはファイアウォールから SSL VPN ファイルをダウンロードできます。

SSL VPN クライアント ファイルのダウンロード用に独自のウェブ サーバを設定するには、以下の手順に従います。

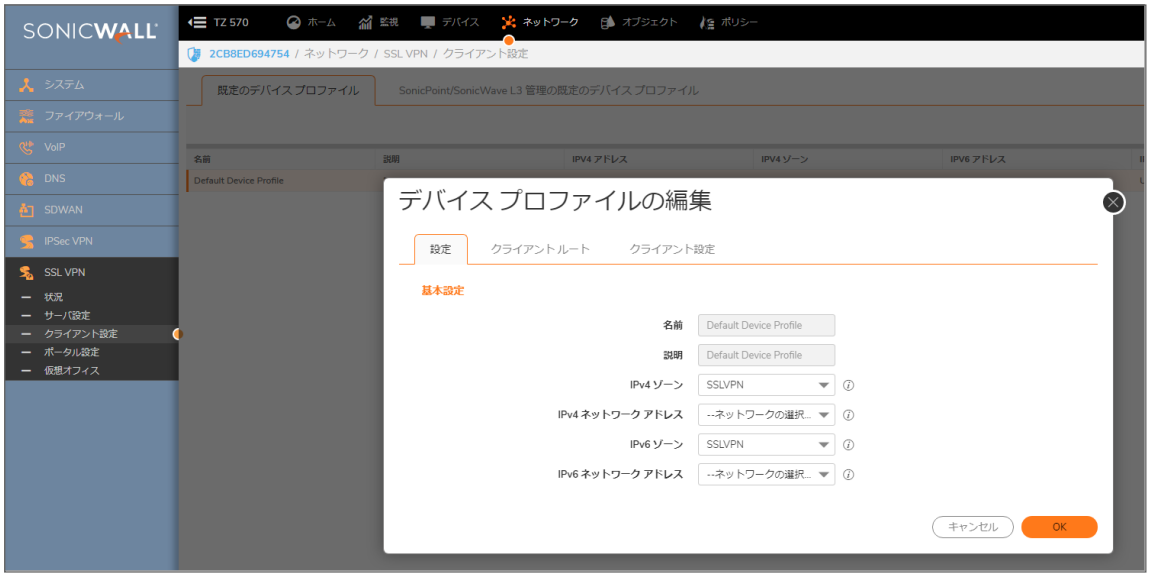
1. 「**ここを選択すると、すべての SSL VPN クライアント ファイルが含まれた SSL VPN zip ファイルをダウンロードします**」のリンクを選択して、すべてのクライアント SSL VPN ファイルを装置からダウンロードします。ファイルを開いて解凍し、HTTP サーバ上のフォルダに置きます。
2. **顧客の HTTP サーバをダウンロード URL として使用する: (http://)**」を選択して、表示されたフィールドに SSL VPN クライアント ダウンロード URL を入力します。
3. 「**適用**」を選択します。

5

SSL VPN クライアントの設定

「**SSL VPN > クライアント設定**」ページで、既定のデバイス プロファイルを編集できます。既定のデバイス プロファイルは、ゾーン上の SSL VPN アクセスの有効化を可能にして、クライアント ルートの設定、クライアント DNS と NetExtender の設定を行います。

「**SSL VPN > クライアント設定**」ページには、SSL VPN アクセスが有効化されている設定済みの IPv4 および IPv6 ネットワーク アドレスとゾーンも表示されます。



既定のデバイス プロファイルを編集して、ゾーンと NetExtender アドレス オブジェクトを選択し、クライアント ルートを設定し、クライアント DNS と NetExtender を設定します。

SSL VPN アクセスがゾーン上で有効になっていなければ、ユーザは仮想オフィス ウェブ ポータルにアクセスできません。SSL VPN アクセスは、「**ネットワーク | SSL VPN | サーバ設定**」ページで設定できます。

トピック:

- 設定オプションの構成
- クライアント ルートの設定
- クライアント設定の指定

設定オプションの設定

既定のデバイス プロファイルを設定するには、以下の手順に従います。

1. 「**ネットワーク | SSL VPN > クライアント設定**」ページに移動します。
2. 「既定のデバイス プロファイル」の編集アイコンをクリックします。「基本」タブを選択します。

既定のデバイス プロファイルの「**名前**」と「**説明**」は変更できません。

3. このプロファイルのゾーン バインド設定を行うには、「**ゾーン IP V4**」ドロップダウン メニューから「**SSL VPN**」またはユーザ定義のゾーンを選択します。
4. 「**ネットワーク アドレス IP V4**」ドロップダウン メニューで、このプロファイル用に作成済みの IPv4 NetExtender アドレス オブジェクトを選択します。詳細については、「NetExtender 範囲に対するアドレス オブジェクトの作成」を参照してください。この設定により、このプロファイルの IP プールとゾーン バインド設定が選択されます。NetExtender クライアントは、このプロファイルと一致する場合、このアドレス オブジェクトから IP アドレスを取得します。
5. このプロファイルのゾーン バインド設定を行うには、「**ゾーン IP V6**」ドロップダウン メニューから SSLVPN またはユーザ定義のゾーンを選択します。
6. 「**ネットワーク アドレス IP V6**」ドロップダウン メニューで、作成済みの IPv6 NetExtender アドレス オブジェクトを選択します。
7. 「**OK**」を選択して、設定を保存し、ウィンドウを閉じます。または、「クライアント ルートの設定」に進みます。

クライアント ルートの設定

「クライアント ルート」では、SSL VPN ユーザに許可するネットワーク アクセスを制御できます。NetExtender クライアント ルートは、すべての NetExtender クライアントに渡され、SSL VPN 接続経由でリモート ユーザがアクセスできるプライベート ネットワークおよびリソースの決定に使用されます。

クライアント ルートの設定を行うには、以下の手順に従います。

1. 「**ネットワーク | SSL VPN > クライアント設定**」ページに移動します。
2. 「既定のデバイス プロファイル」の編集アイコンをクリックします。

3. 「**クライアント ルート**」を選択します。

4. NetExtender ユーザに対するすべてのトラフィック（リモート ユーザのローカル ネットワーク宛てのトラフィックも含む）を強制的に SSL VPN NetExtender トンネルに通すには、「強制トンネル方式」ドロップダウン メニューから「有効」を選択します。
5. 「**ネットワーク**」で、SSL VPN アクセスを許可するアドレス オブジェクトを選択します。
6. 右矢印を選択して、選択したアドレス オブジェクトを「クライアント ルート」リストに移します。
7. クライアント ルートに使用するすべてのアドレス オブジェクトを移し終えるまで繰り返します。

   クライアント ルートを作成すると、アクセス ルールも自動的に作成されます。SSL VPN ゾーンに対するアクセス ルールを手動で設定することもできます。アクセス ルールの設定方法の詳細については、「*SonicOS および SonicOSX 7 のアクセス ルール*」を参照してください。
8. 「**OK**」を選択して、設定を保存し、ウィンドウを閉じます。または、「クライアント設定の指定」に進みます。

クライアント設定の指定

「クライアント設定」画面には、オプションを含む次の 2 つのセクションがあります。

- SSLVPN クライアント DNS 設定
- NetExtender クライアント設定

SSLVPN クライアント DNS 設定を行うには、以下の手順に従います。

1. 「**ネットワーク | SSL VPN > クライアント設定**」ページに移動します。
2. 「既定のデバイス プロファイル」の編集アイコンをクリックします。
3. 「**クライアント設定**」を選択します。画面に、「SSLVPN クライアント」セクションと「DNS 設定」セクションが表

示されます。


デバイス プロファイルの編集
設定
クライアント ルート
クライアント設定
クライアント設定
SSLVPN クライアント DNS 設定
DNS サーバ 1
0.0.0.0
既定の DNS 設定
DNS サーバ 2
0.0.0.0
DNS 検索リスト (検索順)
WINS サーバ 1
0.0.0.0
WINS サーバ 2
0.0.0.0
NETEXTENDER クライアント設定
クライアントの自動更新を有効にする
切断後にクライアントを終了する
iOS デバイスのタッチ ID を許可する
Android デバイスの指紋認証を許可する
SSLVPN を越えた NetBIOS を有効にする
クライアント終了後にアンインストールする
キャンセル
OK

6

SSL VPN ウェブポータルの設定

「**SSL VPN > ポータル設定**」ページでは、SSL VPN 仮想オフィス ウェブ ポータルの外観と機能を設定できます。仮想オフィス ポータルは、NetExtender を起動するために（またはブックマークを選択して内部リソースにアクセスするために）ユーザがログインするウェブ サイトです。カスタマイズによって、どんな既存の企業ウェブ サイトやデザインスタイルにも合わせることができます。

トピック:

- ポータル設定
- ポータル ロゴ設定

ポータル設定

ログインしようとするユーザから見える内容がポータル設定によってカスタマイズされます。会社の要件に応じてオプションを設定してください。「**ネットワーク | SSL VPN > ポータル設定**」に移動します。

オプション定義

- ポータル サイト タイトル: このフィールドには、ポータル ページのトップ タイトルとして表示するテキストを入力します。既定は、「SonicWall – 仮想オフィス」です。
- ポータル バナー タイトル: このフィールドには、ページ最上部のロゴの隣に表示するテキストを入力します。既定は、「仮想オフィス」です。
- ホームページ メッセージ: NetExtender アイコンの上に表示するメッセージの HTML コードを入力します。独自のテキストを入力するか、「サンプル テンプレート」を選択して既定のテンプレートに基づいてフィールドの内容を設定し、それをそのまま使うか編集します。ホーム ページ メッセージの体裁を確認するために「プレビュー」を選択します。
- ログイン メッセージ: 仮想オフィスへログインしようとするユーザに表示するメッセージの HTML コードを入力します。独自のテキストを入力するか、「サンプル テンプレート」を選択して既定のテンプレートに基づいてフィールドの内容を設定し、それをそのまま使うか編集します。ログイン メッセージの体裁を確認するために「プレビュー」を選択します。

次の設定は、仮想オフィス ポータルの機能をカスタマイズするものです。

- キャッシュ制御のための HTTP メタ タグを有効にする（推奨）– ウェブ ブラウザに「仮想オフィス」ページをキャッシュしないように指示する HTTP タグを挿入します。
- ログイン後に NetExtender を起動する – ユーザのログイン後に自動的に NetExtender を起動します。このオプションは、既定では選択されていません。
- 証明書のインポート ボタンを表示する – 「仮想オフィス」ページに「証明書のインポート」ボタンを表示します。これにより、ファイアウォールの自己署名証明書をウェブ ブラウザにインポートする処理が開始されます。このオプションは、既定では選択されていません。

ⓘ **補足:** このオプションは、「SSL VPN > サーバ設定」ページの「証明書の選択」ドロップダウン メニューで、「自己署名証明書を使用」が選択されている場合に、Windows を搭載する PC 上の Internet Explorer ブラウザにのみ適用されます。

ポータル ロゴ 設定

このセクションでは、仮想オフィス ポータルの最上部に表示されるロゴを構成するための設定について説明します。

- **既定のポータル ロゴ** – 既定のポータル ロゴ（SonicWall ロゴ）を表示します。
- **既定の SonicWall ロゴを使用する** – 装置で提供されている SonicWall ロゴを使用します。このオプションは、既定では選択されていません。
- **個別ロゴ（ロゴの URL を入力）** – 表示するロゴの URL を入力します。

ⓘ **ヒント:** ロゴは、155 X 36 サイズの GIF 形式でなければならず、透明または薄い背景色が推奨されます。

7

SSL VPN セッションの表示

「ネットワーク」表示の「**SSL VPN > 状況**」ページは、「状況」ページの使用中の NetExtender セッションと、「ブックマーク」ページのブックマークの概要を表示します。

状況ページ

「状況」ページは、ユーザ名、仮想 IP アドレス、WAN IP アドレス、ログイン継続時間、無動作時間、ログイン時刻を表示します。個々のユーザ セッションに対するトラフィック統計を表示することもできます。

「SSL VPN セッション状況情報」テーブルは、個々のユーザ セッション、または利用可能なアクションについて、状況情報を示します。

SSL VPN セッション 状況情報

状況	説明
ユーザ名	ユーザ名を表示します。
クライアント仮想 IP	NetExtender クライアント IP アドレス プールからユーザに割り当てられた IP アドレスを表示します。
クライアント WAN IP	NetExtender が接続されている WAN インターフェースの IP アドレスを表示します。
ログイン経過時間	ユーザのログインが継続している時間を表示します。
無動作時間	ユーザが無動作になっていた時間を表示します。
ログイン時間	ユーザが最初にログインした日付と時刻を表示します。
トラフィック	統計アイコンをクリックするとユーザ セッションのトラフィック統計を表示します。
コメント	アイコンをクリックするとユーザ セッションに関するコメントが表示されます。

ブックマーク ページ

「ブックマーク」ページは、サーバ名、ブックマークの種類、ログイン情報、サービス時間、最後に使用中だった時間を表示します。

8

仮想オフィスの設定

「**SSL VPN > 仮想オフィス**」ページでは、SonicOS/X 管理インターフェースの内部に仮想オフィス ウェブ ポータルが表示されます。

トピック:

- 仮想オフィス ポータルへのアクセス
- NetExtender の使用
- SSL VPN ブックマークの設定

仮想オフィス ポータルへのアクセス

仮想オフィス ポータルには、2 つの方法でアクセスできます。システム管理者は、装置インターフェースを通じてアクセス可能で、サイト全体に適用される変更を行う権限を持ちます。ユーザはそれとは異なる手順でアクセスし、ユーザ自身の特定のプロファイルに影響する変更しか行うことができません。

システム管理者が SSL VPN 仮想オフィス ポータルにアクセスするには、以下の手順に従います。

1. 「**ネットワーク**」表示を選択します。
2. 「**SSL VPN > 仮想オフィス**」の下を見ます。

ユーザが SSL VPN 仮想オフィス ウェブ ポータルを表示するには、以下の手順に従います。

1. ファイアウォールの IP アドレスに移動します。
2. 「**ログイン**」ページの下部にあるリンク「**SSLVPN へのログインは、ここを選択します**」を選択します。

NetExtender の使用

SonicWall NetExtender は、リモート ユーザがリモート ネットワークにセキュアな方法で接続できるようにする透過的なソフトウェア アプリケーションです。NetExtender により、リモート ユーザはリモート ネットワーク上の任意のアプリケーションを安全に実行できます。ファイルのアップロード/ダウンロード、ネットワーク ドライブのマウント、リソースへのアクセスといった作業がローカル ネットワークにいる感覚で行えます。NetExtender の接続では、ポイント ツー ポイント プロトコル (PPP) 接続を使用します。仮想オフィス ポータルには、NetExtender クライアントをダウンロードするためのリンクが表示されます。

ユーザは、次の 3 通りの方法で NetExtender にアクセスできます。

- SonicWall セキュリティ装置によって提供される仮想オフィス ポータルにログインし、NetExtender ダウンロード リンクを選択し、NetExtender をインストールして起動する。
- スタンドアロンの NetExtender クライアントを起動する。仮想オフィス ポータルから NetExtender をダウンロードして初めてインストールした後、他のクライアント アプリケーションと同様に、ユーザの PC から NetExtender に直接アクセスできます。

NetExtender は、起動時にポップアップ ウィンドウを表示します。SonicWall サーバには、NetExtender を最初に起動してクライアントをダウンロードするときに使用されるサーバが事前に設定されています。このドメインには、対応するドメインも設定されています。ユーザはユーザ名とパスワードを入力し、「接続」を選択します。

接続が確立されると、NetExtender ウィンドウに 3 つの画面が表示されます。「状況」、「ルート」、および「DNS」です。「状況」画面には、サーバ、クライアント IP アドレス、送受信されたキロバイト数、およびスループット (バイト/秒) が表示されます。「ルート」画面には、送信先サブネット IP アドレスおよび対応するネットマスクが表示されます。「DNS」画面には、DNS サーバ、DNS サフィックス、および WINS サーバが表示されます。ルートと DNS 設定は、SonicOS/X 装置の SonicWall 管理者によって制御されます。

ユーザは、接続が確立されたら NetExtender ウィンドウを閉じることができます。接続は開いたままになりますが、ウィンドウは最小化され、システム トレーから再度開くことができます (Windows の場合)。

NetExtender の詳細については、「*NetExtender について*」を参照してください。

SSL VPN ブックマークの設 定

仮想オフィス ホームページに表示する、ユーザ ブックマークを定義できます。ユーザは管理者の作成したブックマークを変更または削除することはできません。

ⓘ **補足:** ブックマークの作成の際、サービスによっては、非標準ポートで動作するものや、接続時にパスを要求するものがあることに注意が必要です。ブックマークの設定の際、**サービス**種別と**ホスト名または IP アドレス**の正しい形式とを合わせる必要があります。これらのオプションを設定する場合、次のテーブルを参照してください。

ⓘ **補足:** SonicOS/X 7 には、ActiveX と Java のサービス種別は存在しません。アップグレードの最中に、古いバージョンのプリファレンスが HTML5 に変換されます。

サービス種別に対するブックマーク名または IP アドレスの形式

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
RDP — ActiveX RDP — Java IP アドレス	IP:ポート (非標準) FQDN ホスト名	10.20.30.4 10.20.30.4:6818 JBJONES-PC.sv.us.sonicwall.com JBJONES-PC
VNC IP アドレス	IP: ポート (セッションへ割り当て済み) FQDN ホスト名 ⓘ **補足:** ポートの代わりにセッション番号または表示番号を使用しないでください。10.20.30.4	10.20.30.4:5901 (セッション 1 へ割り当て済み) JBJONES-PC.sv.us.sonicwall.com JBJONES-PC ⓘ **補足:** 10.20.30.4:1 を使用しないでください。

サービス種別	形式	「ホスト名または IP アドレス」フィールドの入力例
		ヒント: Linux サーバへのブックマークについては、この表の下にヒントがあります。
Telnet	IP アドレス IP:ポート（非標準） FQDN ホスト名	10.20.30.4:6818 JBJONES-PC.sv.us.sonicwall.com JBJONES-PC 10.20.30.4
SSHv1 SSHv2	IP アドレス IP:ポート（非標準） FQDN ホスト名	10.20.30.4 10.20.30.4:6818 JBJONES-PC.sv.us.sonicwall.com JBJONES-PC

重要: Linux サーバへの仮想ネットワークコンピューティング（VNC）ブックマークを作成するときは、「ホスト名または IP アドレス」フィールドで、Linux サーバの IP アドレスとともにポート番号とサーバ番号を ipaddress:port:server の形式で指定する必要があります。例えば、Linux サーバの IP アドレスが 192.168.2.2、ポート番号が 5901、サーバ番号が 1 の場合は、「ホスト名または IP アドレス」フィールドに 192.168.2.2:5901:1 を指定します。

ポータル ブックマークを追加するには、以下の手順に従います。

1. 「**ネットワーク | SSL VPN > 仮想オフィス**」ページに移動します。
2. 「**追加**」を選択します。

3. わかりやすいブックマーク名を「ブックマーク名」フィールドに入力します。
4. LAN 上のホスト コンピュータの完全修飾ドメイン名 (FQDN) または IPv4 アドレスを「名前または IP アドレス」フィールドに入力します。所定のサービス種別で想定される名前または IP アドレスの例については、「サービス種別に対するブックマーク名または IP アドレスの形式」の表を参照してください。
5. 適切なサービスの種類を「サービス」ドロップダウン リストで選択します。
   - RDP (HTML5-RDP)
   - SSHv2 (HTML5-SSHv2)
   - TELNET (HTML5-TELNET)
   - VNC (HTML5-VNC)

   選択によって表示が変わります。

6. 選択したサービスに適した情報を残りのフィールドへ入力します。オプションおよび定義については、以下のテーブルを参照してください。

サービスが RDP (HTML5-RDP) に設定されている場合、以下の設定を行います。	
画面サイズ	ドロップダウン メニューで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。
	ドロップダウン メニューで、このブックマークの実行時に使用される既定のターミナル サービス画面サイズを選択します。
画面の色	ドロップダウン メニューで、このブックマークの実行時に使用されるターミナル サービス画面の既定の色深度を選択します。
アプリケーションおよびパス (オプション)	必要であれば、リモート コンピュータ上のアプリケーションが存在するローカル パスを入力します。
次のフォルダから開始	必要であれば、アプリケーション コマンドを実行するローカル フォルダを入力します。
ウィンドウ詳細オプションの表示	矢印をクリックして拡張し、ウィンドウ詳細オプションの全体を表示します。有効化が必要なチェックボックスをオンにします。 • クリップボードをリダイレクトする • 自動再接続 • ウィンドウ ドラッグ • 音声をリダイレクトする • デスクトップ背景 • メニューとウインドウ アニメーション
自動的にログインする	自動的にログインする チェックボックスをオンにします。選択する場合、以下のどちらの認証情報を使用するか選択します。 • SSL-VPN アカウント認証情報を使用する • ユーザ定義資格情報を使用する 個別認証情報を使用することを選択した場合、ユーザ名、パスワード、ドメインに、個別認証情報を入力します。 ⓘ **補足:** ユーザ名とドメインには、動的変数を使用できます。詳細については、下記の「動的変数」の表を参照してください。
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが SSHv2 (HTML5-SSHv2) に設定されている場合、以下を設定してください。	
自動的にホスト キーを受け入れる	有効にする場合、チェックボックスをオンにします。
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが TELNET (HTML5-TELNET) に設定されている場合、以下を設定してください。	
Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。
サービスが VNC (HTML5-VNC) に設定されている場合、以下を設定してください。	
表示のみ	ブックマークを表示のみモードにする場合はチェックボックスをオンにします。
デスクトップ共有	デスクトップ共有機能を有効にします。

Mobile Connect クライアントにブックマークを表示する	Mobile Connect ユーザにブックマークを表示する場合はチェックボックスをオンにします。

7「**OK**」を選択して設定を保存します。

動的変数

用途	変数	使用例
ログイン名	%USERNAME%	US￥%USERNAME%
ドメイン名	%USERDOMAIN%	%USERDOMAIN￥%USERNAME%

IPv6 用のデバイス プロファイルの設定

SonicOS/X は IPv6 アドレスによるユーザ向けの NetExtender 接続をサポートしています。「**SSL VPN > クライアント設定**」ページで、まず従来の IPv6 IP アドレス プールを設定し、次に IPv6 IP プールを設定します。クライアントには、IPv4 と IPv6 の 2 つの内部アドレスが割り当てられます。

ⓘ | **補足:** IPv6 Wins サーバはサポートされていません。

「**SSL VPN > クライアント ルート**」ページで、事前定義されたすべての IPv6 アドレス オブジェクトを含む、すべてのアドレス オブジェクトのドロップダウン リストからクライアント ルートを選択できます。

ⓘ | **補足:** IPv6 FQDN がサポートされています。

9

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。
- https://mysonicwall.com にアクセスする。
- 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 および SonicOSX SSL VPN 管理ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005450-00 Rev B

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