

モバイル VPN 簡単設定ガイド

Jas	
	XTM 5 Series

ウォッチガード・テクノロジー・ジャパン株式会社 2014 年 8 月 Rev-04

目次

はじめに4
モバイル VPN PPTP の設定方法5
Firebox 側の PPTP 有効化と設定5
モバイル PPTP ユーザーの作成8
PPTP クライアントの設定10
モバイル VPN IPsec の設定方法11
Firebox 側の IPSec VPN 有効化と設定11
モバイル IPsec ユーザーの作成
IPsec クライアントの設定22
インストール方法23
エンドユーザプロファイルのインポート方法27
モバイル VPN(IPsec)クライアントの接続方法29
モバイル VPN(IPsec)クライアントの切断方法30
モバイル VPN SSL の設定方法
Firebox 側の設定31
Firebox 側の設定31 モバイル SSL VPN のユーザー作成
Firebox 側の設定
Firebox 側の設定
Firebox 側の設定
Firebox 側の設定 31 モバイル SSL VPN のユーザー作成 38 Windows/MacOS の SSL クライアントの設定 40 クライアントの条件 40 クライアントソフトウェアのダウンロード 41 クライアントソフトウェアのインストール 41
Firebox 側の設定 31 モバイル SSL VPN のユーザー作成 38 Windows/MacOS の SSL クライアントの設定 40 クライアントの条件 40 クライアントソフトウェアのダウンロード 41 クライアントソフトウェアのインストール 41 SSL VPN の接続方法 42
Firebox 側の設定 .31 モバイル SSL VPN のユーザー作成 .38 Windows/MacOS の SSL クライアントの設定 .40 クライアントの条件 .40 クライアントソフトウェアのダウンロード .41 クライアントソフトウェアのインストール .41 SSL VPN の接続方法 .42 Android OS の SSL クライアントの設定 .43
Firebox 側の設定

おわりに		60
------	--	----

改訂履歴:

第1版	2010年3月17日	初版発行
第2版	2011 年 2 月 17 日	

- 第3版 2012年7月10日
- 第4版 2014年8月19日

はじめに

XTM は、モバイル VPN の接続に以下の3つのプロトコルをサポートしています。

- PPTP(Point-to-Point Tunneling Protocol)
- IPsec(Security Architecture for Internet Protocol)
- SSL(Secure Socket Layer)

このガイドでは、プロトコル毎の設定方法を説明します。

モバイル VPN PPTP の設定方法

Firebox 側の PPTP 有効化と設定

① ポリシーマネージャーから VPN > Mobile VPN > PPTP を選択します。



 次にモバイル VPN(PPTP)を利用するために、「Mobile VPN with PPTP をアクティブにする」にチェックを いれます。この項目にチェックをいれると、WatchGuard PPTP ポリシーと、PPTP ユーザーが自動的に 追加されます。

また、PPTP 接続では、Radius サーバーによる認証を利用することができます。

Radius サーバーを利用する場合、「Radius 認証を使用して Mobile VPN with PPTP ユーザーを認証する」 にチェックを入れてください。

シー 接続 12	"WatchGuard PPTP" が作成され、インターネットから外部インターフェイスへの PPTP が可能になります。 Mobile VPN with PPTP をアクティブにする Radius 認証を使用して Mobile VPN with PPTP ユーザーを認証する 座島化の設定
	■号にの設定 ● 128 ビット暗号化が必要 ● 128 ビットから 40 ビットへの暗号化の低下を許可する ● 暗号化は必要ではない
	その他の設定 最大転送単位 (MTU): 1400 → バイト 最大受信単位 (MRU): 1400 → バイト セッション タイムアウト: 12 → 時間 マ アイドル タイムアウト: 15 → 分 マ
	アドレスブール: <u>追加</u> 削除
棈	ŧ成できる Mobile VPN with PPTP ユーザーは 50 人までです。

次にその他の設定を行います。

設定できる項目は以下となります。

- ・ 最大転送単位(MTU):1回の転送で送信できるデータの最大値を変更
- ・ 最大受信単位(MRU):1回の転送で受信できるデータの最大値を変更
- ・ セッションタイムアウト: デフォルトでは 12 時間に設定
- アイドルタイムアウト:デフォルトでは15分に設定
- IP アドレスプール:XTM では、同時セッション数が 50 に制限されており IP アドレスにより、接続ユーザーを制限することができます。

IP Address Pool 横の Add ボタンをクリックすると、Add Address ダイアログが表示されます。プールする IP アドレスは、ホスト IP もしくは、ホスト範囲で指定することができます。

アドレスの追加	x
種類の選択:	ホスト範囲 ▼
值:	192.168. 51.101
終了:	192.168.51.150
	<u>Q</u> K キャンセル

③ 設定完了後、「OK」ボタンをクリックします。

ポリシーマネージャーに「WatchGuard PPTP」ポリシーが追加されていることを確認してください。

1	🔣 C:¥Users¥user¥Documents¥My WatchGuard¥configs¥XTM21.xml- Fireware XTM Policy Manager										
	ファイル 編集 表示 セットアップ ネットワーク V <u>P</u> N セキュリティサービス ヘルプ										
	🚊 🖳 🗁 🗟 🔯 🕂 🗶 🖳 😫 🥼 🏨 🎎 🖳 🖉 🔗 🖬 🖓 🖓										
ľ	ファイ	アウォール	Mobile VPN with IPSec								
	順序	アクション	ポリシー名	ポリシーの	送信元	送信先	ポート	PBR	App Cont		
	1	\checkmark	🖾 FTP	FTP	Any-Trusted	Any-External	tcp:21		なし		
	2	\checkmark	WatchGuard Authentication	WG-Auth	Any-Trusted Any-Opti	Firebox	tcp:4100		なし		
	3	<	WatchGuard Web UI	WG-Fireware	Any-Trusted Any-Opti	Firebox	tcp:8080		なし		
	4	<u>_</u>	🔊 Ping	Ping	Any-Trusted Any-Opti	Anv	ICMP (type:		なし		
	5	\checkmark	WatchGuard PPTP	PPTP	Any	Firebox	tcp:1723 GRE		なし		
	6	\checkmark	WatchGuard	WG-Firebox	Any-Trusted Any-Opti	Firebox	tcp:4105 tcp		なし		
	7	\checkmark	Cutgoing	TCP-UDP	Any-Trusted Any-Opti	Any-External Any-Opt	. tcp:0 (Any)		なし		
								Fireware	XTM v11.6.0		

以上で、XTM 側のモバイル VPN(PPTP)の設定は終了となります。

次にモバイル PPTP で接続するためのユーザーを作成します。

ポリシーマネージャーのセットアップ> 認証> 認証サーバーをクリックします。

C:¥Users¥user¥Documents¥My WatchGuard¥configs¥XTM21.xml- Fireware XTM Policy Manager										
ファイル 編集 表示 <mark>セットアップ メ</mark> ットワーク VPN セキュリティサービス ヘルプ										
🚊 🛓 🗁 🖷		システム		💰 🖳 🚂 🔊 🖬 🔍 🕯	?					
ファイアウォール	м	機能キー	F							
順序 アクション	T	エイリアス		の 送信元	ì	送信先	ポート	PBR	App Cont	
1 🗸		ログ記録		Any-Trusted	Any-Exte	rnal	tcp:21		なし	
2		EDEL			1		tcp:4100		なし	
3 🗸		oc all	_				tcp:8080		なし	
4 🗸 🛄	(アクション		認証されたユーザー/グル・	= 7		ICMP (type:		なし	
5 🗸		Default Threat Protection	•	Webサーバー証明書			tcp:1723 GRE		なし	
6 🗸	•	Default filleat Frotection	· •				tcp:4105 tcp		なし	
7 🗸	÷ .	NTP		認証設定		rnal Any-Opt	.tcp:0 (Any)		なし	
		SNMP								
		管理対象のデバイス設定	м							
		グローバル設定								
								Fireware	XTM v11.6.0	

認証サーバーのダイアログで「追加」をクリックします。

「「認証サーバー
Firebox RADIUS SecuriD LDAP Active Directory
▼ Firebox 内部テータペースを有効にする _ユーザー
追加
ニーザー グループ
PPTP-Users
<u>追加</u> 追加 鋼条 削除

ユーザー情報に任意の名前を入力します。

パスフレーズは8文字以上の英数字を入力します。

Firebox 認証グループには、PPTP を有効にしたときに自動的に作成された PPTP-Users を選択し、<< をクリックし、新しいユーザーを PPTP-Users グループに含めます。

🔣 Firebox ユーザーの	のセット	アップ 🔽
_ユーザー情報 	_	
	名前:	pptp-user-01
	説明:	
,	フレーズ:	•••••
	確認:	•••••
セッションタイ/	ムアウト:	8 🚔 [時間 👻
アイドル タイノ	ムアウト:	30 🌩 😽 👻
Firebox 認証グルーフ	7	
メンバー:		使用可能:
		PPTP-Users
		~
	<u>о</u> к	キャンセル ヘルブ

以下の状態になります。

<<	
<<	
+ *	ンセル ヘルプ
) + *

ユーザー追加と認証サーバーのダイアログの OK をクリックして閉じたら、ポリシーマネージャーで設定を保存します。

次にクライアント機の設定を行います。ここでは例として Windows7 の設定方法を記載します。その他の Windows バージョンにつきましては、ヘルプの「PPTP 用クライアント コンピュータを準備する」を参照ください。

PPTP クライアントの設定

- ① Windows のスタートメニュー>コントロールパネル>ネットワークと共有センターを選択します
- ネットワーク設定の「新しい接続またはネットワークのセットアップ」をクリックします。
- ③ 新しい接続ウィザードの開始画面が表示されたら、「次へ」をクリックします
- ④「職場に接続します」を選択し、「次へ」をクリックします
- ⑤ 「既存の接続を利用しますか?」には、「いいえ、新しい接続を作成します」を選択し「次へ」をク リックします
- ⑥ 「インターネット接続(VPN)を使用します」をクリックします
- ⑦ インターネットアドレスには、XTM の External のアドレス、もしくは名前解決できるのであれば ホスト名を入力します。接続先の名前は任意(例:モバイル PPTP VPN 接続)です。入力したら 「次へ」をクリックします
- ⑧ ユーザー名、パスワードを入力し、「このパスワードを記憶する」にチェックを入れ、最後に「接続」をクリックします。
- ⑨ 以上の設定内容で接続が始まります。「接続されています」と表示されれば設定完了です。

以上で、モバイル VPN(PPTP)の設定は終了です。

モバイル VPN IPSEC の設定方法

Firebox 側の IPSec VPN 有効化と設定

① ポリシーマネージャーから VPN > Mobile VPN > IPsec を選択します。

R	🧝 C:¥Users¥user¥Documents¥My WatchGuard¥configs¥XTM21.xml- Fireware XTM Policy Manager									
7	ァイル 編集 表示	・ セットアップ ネットワーク	VPN	セキュリティサービス ヘルプ						
1.	🖹 🔁 📕	🕅 + 🗙 🗄 🖉 🕷	Â	Branch Office ゲートウェイ	?					
7	ァイアウォール	Mobile VPN with IPSec	a di la calenda	Branch Office Tunnel						
)8	原 アクション	ポリシー名	ă	BOVPN ポリシーの作成		送信先	ボート	PBR	App Cont	
1	~	ETP 🔄	1	フェーズ2のブロポーザル	Any	/-External	tcp:21		なし	
2	\checkmark	WatchGuard Authentication	1	Mobile VPN		IPSec	tcp:4100		なし	
3	\checkmark	🗢 WatchGuard Web UI					tcp:8080		なし	
4	V 🖳	Ping		VPN 設定		PPTP	ICMP (type:		なし	
5		WatchGuard PPTP	PPTP	Any		SSL	tcp:1723 GRE		なし	
6		WatchGuard	WG-F	irebox Any-Trusted Any-Opti		NOX	tcp:4105 tcp		なし	
7	1	Outgoing	TCP-L	JDP Any-Trusted Any-Opti	. Any	-External Any-	-Opt tcp:0 (Any)		なし 📗	
	-									
								Fireware	XTM v11.6.0	

② 次に新しいモバイル VPN(IPsec)接続を作成します。追加ボタンをクリックします。

ig Mobile VPN with IPSec の構成	×
Mobile VPN with IPSec を新規作成するには、[追加] をクリックしま	追加
	編集
	削除
	i¥钿
ー モバイル ユーザーの構成ファイルのセットを再作成するには、上記り: トでモバイル ユーザー グループを選択し、[作成] をクリックします。	ス 生成
Shrew Soft VPN クライアントは、WatchGuard Mobile VPN with IPSec	σ
すべての構成の設定をサポートしているわけではありません。 Shrew Soft VDN クライアントがサポートしていない設定のリフトについてけ	
[ヘルプ]をクリックしてください。	
この Firebox には、 Mobile VPN with IPSec ユーザーの機能キーが 1 人分	うあります。
<u></u> K キャンセル	ヘルフ

「Add mobile VPN with IPsec Wizard」が起動するので「次へ」をクリックします。

R Add Mobile VPN with IPSec	: Wizard
	ようこそ。
	Add Mobile VPN with IPSec Wizard 🔨
	このウィザードを使用して、モバイル ユーザー用の仮想プライベート ネットワークを作 成することができます。
	詳細情報 <u>WatchGuard Mobile VPN with IPSec</u> 。
	統行するには、[次へ] をクリックします。
	<戻る 次へ > キャンセル ヘルブ

- ③ 次に IPsec 接続に使用する認証サーバーを設定します。認証サーバーは、以下の 5 つから選択することができます。
- Firebox-DB
- RADIUS
- SecureID
- LDAP

ここでは、例として認証サーバーに Firebox-DB を選択します。

Group Name は、認証はサーバーとして Firebox-DB を選択した場合、新たに作成したいグループ名を入力 してください。ウィザード終了時に自動的にユーザグループが作成されます。

その他の認証サーバーを選択した場合は、実際に認証サーバー上に存在するグループ名を入力してください。

入力後、「次へ」ボタンをクリックし次に進んでください。

R Add Mobile VPN with IPSec Wizard	×
ユーザー認証サーバーを選択します。	WatchGuard
Firebox でモバイル ユーザーの認証に使用するサーバーおよびグループを選択します。	
認証サーバー: Firebox-DB ▼	
グループ名: IPSec-Users	
	す。グループ名では大文字と小文
< 戻る 次へ >	キャンセル ヘルプ

④ 次に認証方法を設定します。

VPN 接続でパスワード認証を行う場合は、「このパスフレーズを使用する」にチェックを入れてください。 8 文字以上の英数字を使い、パスフレーズを入力します。

K Add Mobile VPN with IPSec Wizard	×
トンネル認証方法を選択します。	WatchGuard
Firebox で安全な VPN トンネルを確立するために使用する認証メソッドを選択します。	
◎ このパスフレーズを使用する:	
トンネルのパスフレーズ: ●●●●●●●●]
パスフレーズの再入力: ●●●●●●●●]
○ WatchGuard Management Server が発行する RSA 証明書を使用します。	
サーバーの管理用パスフレーズを入力します。	
詳細情報 <u>認証メソッド</u> 。	
<戻る 次へ >	キャンセル ヘルブ

WatchGuard Management Server による RSA 認証を利用する場合は、「WatchGuard Management Server が発行する RSA 証明書を使用します」にチェックを入れます。

IP Address 及び Administration Passphrase には、Management Server の情報を入力します。

⑤ 次にインターネットトラフィックのフローを指定します。

R Add Mobile VPN with IPSec Wizard	×
インターネット トラフィックのフローを指定します。	WatchGuard
モバイル コンピュータとインターネットとの間のすべてのトラフィックがトンネルを経由するように	しますか?
いいえ、インターネット トラフィックをモバイル ユーザーの ISP に直接送信するようにします。	(柔軟性は高く、)
◎ はい、すべてのインターネット トラフィックがトンネルを経由するようにします。(柔軟性は低	く、安全性は高い)
詳細情報 インターネット トラフィックがトンネルを経由するようにダイレクトします。	
<戻る 次へ > キャン	セル ヘルプ

インターネットトラフィックは直接 ISP へ接続する場合

→「いいえ、インターネットトラフィックをモバイルユーザーの ISP に直接送信するようにします。」を選択し、 ⑥-1 に進む

インターネットトラフィックを VPN トンネル経由で接続する場合

→「はい、すべてのインターネットトラフィックがトンネルを経由するようにします。」を選択し、⑥-2に進む

6-1

VPN トンネルを経由させる IP アドレスを設定する画面が表示されます。

IP アドレスは、ホスト IP またはネットワーク IP 単位で登録することができます。「追加」をクリックし、登録 後、「次へ」をクリックします。

🔣 Add Mobile VPN with I	PSec Wizard	×
トンネル経由でアクセス	「できるリソースを特定します。	
VPN トンネルを経由してモ	バイル ユーザーがアクセスできるコンピュータおよびネットワークを	E注加します。
種類	IP アドレス	<u>追加</u>
Network IP	192.168.111.0/24	削除
	<戻る 次へ >	キャンセル ヘルプ

⑥-2VPN トンネルを経由するネットワークが表示されます。デフォルトでは Any-External と 0.0.0.0/0 が表示されるので、「次へ」をクリックしてください。

🎇 Add Mobile VPN with IP	Sec Wizard	×
トンネル経由でアクセス	できるリソースを特定します。	
VPN トンネルを経由してモ/	バイル ユーザーがアクセスできるコンピュータおよびネットワークを	を追加します。
種類	■ アドレス	〕追加
Alias	Any-External	
Network IP	0.0.0/0	
	< <u>戻る</u> × × ×	キャンセル ヘルブ

⑦ 次に VPN トンネルで使用する IP アドレスを設定します。

ここで登録した IP アドレスは、モバイル VPN ユーザーに割り当てられます。

「追加」をクリックし、ホスト IP またはホストレンジを登録し、「次へ」をクリックし、任意のローカル IP アドレス (例:192.168.0.10-192.168.0.15)を設定してください。

🔣 Add Mobile VP	N with IPSec Wizard			×
仮想IPアドレス	プールを作成します。			WatchGuard
Firebox でモバイル	ケコンピュータに割り当てる IP アドレン	スを追加します。		
				<u>`注意力口</u>] 自119余
 この Firebo 詳細情報 <u>仮想 P 3</u> 	x には、最大1人分の Mobile VPN with <u>Pドレス</u> 。	IPSec ユーザー ライセンスがあり	žŢ.	
		<戻る 次へ :	· +·	ャンセル ヘルプ
	1	×		
	4			
種類の選択:	ホスト範囲	-		
值:	192.168.115.101			
終了:	<u>192.168.115.105</u> ок	キャンセル		

⑧ 以下の画面が表示されたら、モバイル VPN(IPsec)の設定は終了となります。

K Add Mobile VPN with IPSec	s Wizard
Add Mobile VPN with IPSed	 Wizard Add Mobile VPN with IP Sec Wizard が正常に完了しました。 おめでとうこざいます!モバイル ユーザー用の仮想プライベート ネットワークが新規作成されました。 VPN 構成ファイルは次のフォルダにあります。 C:\Users\Public\Shared WatchGuard\muvpn\ \IPSec-Users\wgx .wgx ファイルは、トンネルのパスフレーズで暗号化されています。 .vpn および .ini ファイルは暗号化されません。安全な方法を使用して、これらのファイルを配信してください。 ウィザードが完了したら、チェックボックスを選択してユーザーをグループ "IPSec-Users" に追加してください。 ア iPSec-Users にユーザーを追加する
	<戻る 完了 キャンセル ヘルブ

注意:ウィザードが成功すると、VPN 設定ファイルの保存場所が表示されるので、ご確認ください。このファイ ルには、shared key、ユーザー情報、IP アドレス、VPN の設定情報が含まれており、クライアント機の設定 に使用します。

また、このファイルはパスフレーズにより暗号化されており、このファイル自体を編集することはできません。

また、「IPSec-Users にユーザーを追加する」(グループ名は作成時の任意のもの)にチェックを入れると、自動的にモバイル VPN ユーザグループにユーザーが追加されます。

必ずチェックを入れてから「完了」ボタンをクリックしてください。

ウィザードの完了後、次のようなアラートが表示されたら、追加で設定が必要になります。



以下の手順で追加設定を完了させてください。

① 接続プロファイルを選択し、編集ボタンをクリックします

I Mobile VPN with IPSec の構成	×
	<u>追加</u> 編集 削除
モバイル ユーザーの構成ファイルのセットを再作成するには、上記リ. トでモバイル ユーザー グループを選択し、[作成] をクリックします。	詳細 ス 生成
Shrew Soft VPN クライアントは、WatchGuard Mobile VPN with IPSec すべての構成の設定をサポートしているわけではありません。 Shrew Soft VPN クライアントがサポートしていない設定のリストについては、 [ヘルブ] をクリックしてください。 この Firebox には、Mobile VPN with IPSec ユーザーの機能キーが 1人ろ	ರು ⇔ಹಾರ್ಶಕ್ಷ
残りの数は0です。 <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <u></u> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i> <i></i>	<u>ヘルプ</u>

② Firebox IP アドレスの欄に VPN 接続用の External IP アドレスもしくはホスト名を指定します。

K Mobile VPN with IPSec の編集
グループ名: IPSec-Users
全般 IPsecトンネル リソース 詳細
-認証サーバー
Firebox-DB 🔻
「パスフレーズ
このグループの Mobile VPN with IPSec エンドユーザー プロファイルの暗号化に使用します。
確認: ▶●●●●●●●●●●●
Firebox IP アドレス
Mobile VPN with IPSec クライアントはこれらの外部 IP アドレスまたはドメインの 1 つに接続します。
プライマリ:
バックアップ:
Firebox を認証サーバーとして使用する場合は、Firebox ユーザー アカウントごと にタイムアウトを設定します。
セッション: 480 🛬 分
アイドル: 30 🔦 分
<u></u>

入力するとOK ボタンがアクティブになりますので、OK をクリックして設定を反映させます。

External の IP アドレスが固定でなく、DDNS のホスト名を指定した場合には以下のアラートが表示されますが、「はい」をクリックしてください。



モバイル IPsec ユーザーの作成

次に IPsec 接続を行うユーザーを作成します。

① ポリシーマネージャーからセットアップ> 認証> 認証サーバーを選択します。

Firebox タブからユーザー欄下の追加ボタンをクリックします。

「「「「認証サーバー
Firebox RADIUS SecurID LDAP Active Directory ✓ Firebox 内部データペースを有効にする
pptp-user-01
<u>追加…</u> 編集… 削除 ユーザー グループ
IPSec-Users PPTP-Users
<u>追加…</u> [] [] [] [] [] [] [] [] [] [] [] [] []
<u>OK</u> キャンセル ヘルブ

- ② IPsec ユーザーを作成します。
 - 名前:ユーザー名
 - 説明:ユーザーの説明(備考)
 - パスフレーズ:ユーザーのパスフレーズ
 - 確認:パスフレーズの確認
 - セッションタイムアウト:セッション開始後の時間の閾値(デフォルトは8時間)
 - アイドルタイムアウト:アイドル状態の時間の閾値(デフォルトは 30 分)

「Firebox 認証グループ」には、先程のウィザードで作成したユーザグループを選択し、Member 欄に追加後、OK ボタンをクリックします。

IFirebox ユーザーのセット	アップ 💌
「ユーザー情報	
名前:	ipsec-user-01
説明:	
パスフレーズ:	•••••
確認:	•••••
セッション タイムアウト:	8 🔷 時間 🔻
アイドル タイムアウト:	30 🌩 😽 🔻
 Firebox 認証グループ─────	
メンバー:	使用可能:
	IPSec-Users
	<
	>>
<u>о</u> к	キャンセル ヘルプ
[

以上で、IPsec ユーザーの作成は終了です。

IPsec クライアントの設定

IPsec クライアントを設定するには、クライアントソフトウェア Shrew VPN Client のインストールが必要です。

クライアントソフトウェアは、WatchGuard Customer Support サイトからダウンロード可能です。

https://www.watchguard.com/support/index.asp

ご利用の Firebox バージョンにあわせた IPsec クライアントソフトウェアをダウンロードしてください。

Mobile VPN with IPSec Software

<u>Shrew VPN Client 2.1.7 for Windows</u> by Shrew Soft, Inc. (<u>www.shrew.net</u>) For Windows 2K, XP, Vista, and 7 32/64 bits

vpn-client-*.*.*-release.zip(*印はバージョン)を展開すると、インストーラーの vpn-client-*.*.*release.exe が抽出できます。

クライアントの必要条件:

- モバイル VPN IPsec クライアントソフトウェアをインストールするには、以下のバージョンの Windows が必要です。
 - ➢ Windows 2000
 - ➢ Windows XP (32-bit and 64-bit)
 - ➢ Windows Vista (32-bit and 64-bit)
 - Windows 7 (32-bit and 64-bit)
 - また、クライアント PC にインストールされている Firewall(Windows Firewall)を無効にする必要が あります。
- モバイル VPN IPsec クライアントソフトウェアをインストールする前に、すべてのサービスパックが利用 できるか確認することをお勧めいたします。
 - モバイル VPN IPsec クライアントソフトウェアをインストールすると、VPN 接続に使用する WINS サーバーと DNS サーバーの情報がクライアント PC にインポートされます。

クライアントソフトウェアのインストール:

クライアントソフトウェアのインストールは、2つのパートに分かれています。

- クライアントソフトウェアのインストール
- エンドユーザープロフィールのインポート

また、インストールを始める前に、以下のインストールコンポーネントがあることを確認してください。

- Mobile VPN クライアントソフトウェア(vpn-client-*.*.*-release.exe)
- ・ エンドユーザ プロファイル(ファイルの拡張子が.vpn のファイル)

→ウィザードが成功すると表示される VPN 設定ファイルです。デフォルトでは、

C:¥Users¥Public¥Shared WatchGuard¥muvpn 配下にあります。

- ・ パスフレーズ (Add mobile VPN with IPsec Wizard の④で設定したパスフレーズ)
- ・ 認証に証明書を利用する場合、cacert.pem ファイルと.p12 ファイル
- ・ ユーザー名とパスワード

インストール方法

- ① ステップ1でダウンロードしたソフトウェアをダブルクリックすると、WatchGuard モバイル VPN インストールウィザードが始まります。
- Welcome の画面では「Next」をクリックしてください



③ License Agreement(ライセンスの同意)では「I Agree」をクリックします



④ Choose Component(コンポーネントの選択)ではそのままの状態で「Next」をクリック

O Shrew Soft VPN Client Se	tup					
Choose Components Choose which features of Shre install.	Choose Components Choose which features of Shrew Soft VPN Client you want to install.					
Check the components you wa install. Click Next to continue.	nt to install and uncheck the com	ponents you don't want to				
Select components to install:	 Remove Components Program Files Network Drivers Network Services Start Menu Shortcuts 	Description Position your mouse over a component to see its description,				
Space required: 8.2MB						
Nullsoft Install System v2,45 —	< <u>B</u> ack	Next > Cancel				

⑤ Choose Install Location(インストール先)はそのままで「Next」をクリックします

🕖 Shrew Soft VPN Client Setup	
Choose Install Location Choose the folder in which to install Shrew Soft VPN Client.	SHREW SOFT. VPNCLIENT
Setup will install Shrew Soft VPN Client in the following folder. To in click Browse and select another folder. Click Next to continue.	stall in a different folder,
Destination Folder	Browse
Space required: 8.2MB Space available: 32.7GB	
Nullsoft Install System v2,45	Next > Cancel

⑥ 次の画面が表示されたら、「Next」をクリックしてインストールを開始します

📀 Shrew Soft VPN Client Setup	
Checking for installed software A previous install of the Shrew Soft VPN Client was detected.	SHREW SOFT. VPNCLIENT
Before this install process can continue, the currently installed vers To remove the currently installed version, dick Next. To keep the c click Cancel.	ion needs to be removed. urrently installed version,
Nullsoft Install System v2.45 ————————————————————————————————————	Next > Cancel

🕖 Shrew Soft VPN Client Setup	X
Installing Please wait while Shrew Soft VPN Client is being installed.	NT
Stopping the DNS Proxy Service	
Delete file: C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥ShrewSoft V Delete file: C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥ShrewSoft V Delete file: C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥ShrewSoft V Delete file: C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥ShrewSoft V Remove folder: C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥ShrewSoft V Stopping the DNS Proxy Service	
Nullsoft Install System v2.45 < Back Next > Cancel	

⑦ 以下の画面が表示されたら、インストールウィザードは完了です。

Finish をクリックしてください。

🕖 Shrew Soft VPN Client Se	etup
	Completing the Shrew Soft VPN Client Setup Wizard Shrew Soft VPN Client has been installed on your computer. Click Finish to close this wizard.
	< <u>B</u> ack Einish Cancel

エンドユーザプロファイルのインポート方法

 Windows のスタートメニューからプログラム > ShrewSoft VPN Client > Access Manager をクリックし ます

 ShrewSoft VPN Client Access Manager Documentation Trace Utility Uninstall 	既定のプログラム ヘルプとサポート ファイル名を指定して実行	
↓前に戻る		
プログラムとファイルの検索	▶ シャットダウン	

② File> Import をクリックします

(B) Shrew Soft VPN Access Manager			
File Edit View Help	_		
Connect			
Import	y Delete		
Export			
Preferences			
Exit			
	_		

③ IPsec ウィザードで作成されたエンドユーザプロファイル(.vpn ファイル)を選択します

(B) Import VPN File		×
	wgxの検索	٩
整理 ▼ 新しいフォルダー	:=== ▼	
■ ダウンロード Añ ^	更新日時	種類
■ デスクトップ ③ 最近表示した場所	7/11/2012 16:05	VPN ファイ,
■ デスクトップ ⇒ ライブラリ ≪ ホームグループ B user ■ コンピューター ▲ ローカル ディ: ④ DVD/CD-RW ● ネットワーク ▼ く 111		•
ファイル名(<u>N</u>): IPSec-Users.vpn 🔹	Shrew Soft VPN File ((*.vpn) 👻
	開<(<u>0</u>) ▼ キ	ヤンセル

④ .vpn ファイルを選択すると Access Manager に接続設定のエントリーが表示されます



以上でプロファイルのインポートは完了です。

モバイル VPN(IPsec)クライアントの接続方法

- Windows のスタートメニューからプログラム > ShrewSoft VPN Client > Access Manager をクリックし ます
- ② 接続するプロファイルを選択し、Connect ボタンをクリックします



③ 接続のダイアログが表示されますので、Username と Password を入力し、Connect ボタンをクリックし ます



以下のように tunnel enabled と表示されれば接続成功です。



モバイル VPN(IPsec)クライアントの切断方法

Mobile VPN Monitor ダイアログボックスから Disconnect をクリックします。

🐼 Shrew Sof	t VPN Connect	
Connect Netv	vork	
client configu local id config pre-shared ke bringing up tu network devic tunnel enable	red jured sy configured innel ce configured d	
Credentials		
Username	ipsec-user-01	
Password		
	Disconnect	Cancel

モバイル VPN SSL の設定方法

モバイル VPN (SSL) クライアントは、ソフトウェアアプリケーションのインストールが必要です。モバイル VPN クライアントは SSL (Secure Sockets Layer)を使用します。

Firebox 側の設定

 ポリシーマネージャーから VPN > Mobile VPN > SSL を選択すると Mobile VPN with SSL Configuration ダイアログが表示されます。

🔣 C:¥Users¥user¥Documents¥My WatchGuard¥configs¥XTM21.xml- Fireware XTM Policy Manager									
ファイ	ル 編集 表示	ミ セットアップ ネットワーク	V <u>P</u> N	マキュリティサービ:	ス ヘルプ				
温 ファイ	基 🗁 暑 アウォール	🕅 🕂 🗙 🖞 💆 🎼 Mobile VPN with IPSec	11 11	Branch Office ゲート Branch Office <u>T</u> unne	ウェイ ? L				
順序	アクション	ポリシー名	*	BOVPN ポリシーの作	بمt ;	送信先	ボート	PBR	App Co
1 2 3 4 5 6 7		 FTP WatchGuard Authentication WatchGuard Web UI Ping WatchGuard PPTP WatchGuard Outgoing 	PPTP WG-F TCP-L	フェーズ2のプロボ Mobile VPN VPN設定 irebox-Mgmt JDP	Any Any-Trusteu An Any-Trusted Ar	Any-External PSec PPTP SSL n Any-External An	tcp:21 tcp:4100 tcp:8080 ICMP (type: 8 tcp:1723 GRE tcp:4105 tcp: tcp:0 (Any) u		なななななななししししし
								Fireware	XTM v11.6.0

Activate Mobile VPN with SSL にチェックを入れ、モバイル VPN(SSL)を有効にします。この欄にチェックをいれると SSL VPN Users Group と WatchGuard SSL VPN ポリシーが自動的に作成されます。

In Mobile VPN with SSL の構成
When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.
Firebox IP アドレス 接続先の SSL VPN ユーザーの Firebox IP アドレスまたはドメイン名を入力あるいは選択してください。 プライマリ: マ バックアップ: マ ネットワークおよびIP アドレスプール
VPNトンネルを経由してトラフィックを送信するためにFireboxで使用する方法を選択します。指定したネットワークにユーザーをブリッジで接続する には、【VPNトラフィックのブリッジ】を選択します。指定したネットワークおよびリソースにFireboxでVPNトラフィックをルーティングするに は、【VPNトラフィックのルーティング】を選択します。
 「「すべてのクライアントをトンネル経由にする ・信頼するインターフェイス、任意インターフェイス、および VLAN インターフェイスを経由して接続したネットワークへのアクセスを許可する ・許可するリソースの指定
 道加 削除 仮想Pアドレス ブール
Fireboxにローカルに接続されるコンピュータによって使用されないサブネットを入力してください。 11 名の Mobile VPN with SSL ユーザーが Firebox を使用することができます。 192.168.113.0/24
<u></u>

③ 次に SSL VPN ユーザーが接続に使用する IP アドレスかドメイン情報を設定します。

Firebox が複数の WAN 接続を持っている場合、Backup のドロップダウンリストから、違うグローバルな IP アドレスを選択してください。

SSL クライアントを持つモバイル VPN は、Primary に設定した IP アドレスとの通信が確立できない際に Backup の IP アドレスを使用します。

R Mobile VPN with SSL の構成
When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.
✓ Mobile VPN with SSLをアクティブにする
全般 認証 詳細
「Firebox IP アドレス
接続先の SSL VPN ユーザーの Firebox IP アドレスまたはドメイン名を入力あるいは選択してください。
プライマリ: 74.125.235.151 ▼ パックアップ: 74.125.235.152
「ネットワークおよびIPアドレス ブールー
VPNトンネルを経由してトラフィックを送信するためにFireboxで使用する方法を選択します。 指定したネットワークにユーザーをブリッジで接続する には、【VPNトラフィックのブリッジ】を選択します。 指定したネットワークおよびリソースにFireboxでVPNトラフィックをルーティングするに は、【VPNトラフィックのルーティング】を選択します。
VPNトラフィックのルーティング ▼
□ すべてのクライアントをトンネル経由にする
◎ 信頼するインターフェイス、任意インターフェイス、および VLAN インターフェイスを経由して接続したネットワークへのアクセスを許可する
◎ 許可するリソースの指定
/ 3追加 単明余
┌仮想Pアドレス ブール
Fireboxにローカルに接続されるコンピュータによって使用されないサブネットを入力してください。 11 名の Mobile VPN with SSL ユーザーが Firebox を使用することができます。
192.168.115. 0 /24

④ 次にモバイル VPN SSL クライアントが使用するネットワークと IP アドレスプールを設定します。

IN Mobile VPN with SSL の構成
When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.
☑ Mobile VPN with SSL をアクティブにする
全般 認証 詳細
Firebox IP アドレス
接続先の SSL VPN ユーザーの Firebox IP アドレスまたはドメイン名を入力あるいは選択してください。
プライマリ: 74.125.235.151 ▼ パックアップ: 74.125.235.152 ▼
_ 「ネットワークおよびIPアドレス ブールー
VPNトンネルを経由してトラフィックを送信するためにFireboxで使用する方法を選択します。 指定したネットワークにユーザーをブリッジで接続する には、【VPNトラフィックのブリッジ】を選択します。 指定したネットワークおよびリソースにFireboxでVPNトラフィックをルーティングするに は、【VPNトラフィックのルーティング】を選択します。
VPNトラフィックのルーティング ▼
🔲 すべてのクライアントをトンネル経由にする
◎ 結額するインターフェイス、任意インターフェイス、および VLAN インターフェイスを経由して接続したネットワークへのアクセスを許可する
◎ 許可するリソースの指定
/
仮想IPアドレス ブール
Fireboxにローカルに接続されるコンピュータによって使用されないサフネットを人力してください。 11 名の Mobile VPN with SSL ユーザーか Firebox を使用することができます。
<u> <u> </u> <u></u></u>

- ⑤ Firebox がトラフィックを送信するために使用するメソッドを選択します。
- ・ VPN トラフィックのルーティング
- ・ VPN トラフィックのブリッジ

•

⑥ 次に「すべてのクライアントをトンネル経由にする」を設定します。

この欄にチェックを入れた場合、すべてのプライベートネットワーク・トラフィックとインターネットトラフィックが 全て VPN トンネルを経由します。 ⑦ 次に「仮想 IP アドレスプール」を設定します。

モバイル VPN(SSL)クライアントが使用する IP アドレスを入力します。このアドレスプールの中の仮想 IP アドレスが SSL VPN で接続したクライアントデバイスに割当てられます。

Mobile VPN with SSL の堪成
When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.
☑ Mobile VPN with SSL をアクティブにする
全般 認証 詳細
「Firebox IP アドレス
接続先の SSL VPN ユーザーの Firebox IP アドレスまたはドメイン名を入力あるいは選択してください。
プライマリ: <mark>74.125.235.151 ▼</mark> バックアップ: <mark>74.125.235.152 ▼</mark>
VPNトンネルを経由してトラフィックを送信するためにFireboxで使用する方法を選択します。 指定したネットワークにユーザーをブリッジで接続する には、 [VPNトラフィックのブリッジ] を選択します。 指定したネットワークおよびリソースにFireboxでVPNトラフィックをルーティングするに は、 [VPNトラフィックのルーティング] を選択します。
VPNトラフィックのルーティング
── すべてのクライアントをトンネル経由にする
◎ 伝播オスインターファイフ 任美インターファイフ お上だい(ハハインターファイフス終曲」で接続したう…トロークへのマクセフな設可する
Cardy Soft - Xwinz
/ 道加 削除
⊳仮想Pアドレス ブール
Fireboxにローカルに接続されるコンピュータによって使用されないサブネットを入力してください。 11 名の Mobile VPN with SSL ユーザーが
Fireboxを使用することができます。
192.168.115. 0 /24
<u> </u> <u> </u> <u> </u> <u> </u>

IP アドレスを入力後、「OK」をクリックしてください。

⑧ 次に詳細タブをクリックします。

en you activate Mobile VPN	with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from 1
rnet to the external interface	e.
Mobile VPN with SSL をアク	フティブにする
般認証証	
2 af :	
经专任:	AES (256-bit)
データ チャンネル:	
#成チャンネル:	TCP : 443 🙀
- プァライブ:	間隔: 10 🚽 秒
	タイムアウト: 60 🚔 秒
ミネゴシエート チーク チャ	
ドメイン名: DNSサーバー: 8.8.1	8.8 8.4.4
WINS # = // = ·	
Wind 9 77	
	に た. 上 道 に 戻 9

詳細タブでは以下の項目を設定します。

・ 認証:認証で使用するアルゴリズムを選択します。選択肢は以下です。

MD5, SHA, SHA-1, SHA-256, SHA-512

・ 暗号化:暗号化で使用するアルゴリズムを選択します。選択肢は以下です。

Blowfish, DES, 3DES, AES (128 bit, 192 bit, 256 bit)

暗号化の強度とパフォーマンスの高さから、MD5とBlowfishの組み合わせをお勧めします。

データ チャンネル:SSL 接続に使用するプロトコル(TCP or UDP)とポート番号を設定します。デフォルトは、TCP の 443 番ポートです。

- キープ アライブ:SSL 接続のキープアライブを設定します。
- ・ 再ネゴシエートデータチャネル:SSLの再接続を要求する時間間隔です。デフォルトは 61 分です。
- ・ DNS and WINS Servers:内部ネットワークの DNS/WINS サーバーを登録します。

リモート環境から内部ネットワーク資源の名前解決を行う場合に必要です。

⑨ 以上で、Firebox モバイル VPN(SSL)の設定は終了です。

ポリシーマネージャーに「Allow SSLVPN-Users」ポリシーが追加されていることを確認してください。

また、ポリシーマネージャーよりセットアップ> 認証> 認証サーバーを選択し、ユーザグループに「SSL VPN-Users group」が追加されていることを確認してください

注意:「Allow SSLVPN-Users」ポリシーでは、Trusted Network へのアクセスを許可していません。Trusted Network のアクセスを許可するには、ヘルプの「信頼済みネットワークへアクセスするように Mobile VPN with SSL ユーザーを許可する」を参照ください。

モバイル SSL VPN のユーザー作成

次にモバイル PPTP で接続するためのユーザーを作成します。

ポリシーマネージャーのセットアップ> 認証> 認証サーバーをクリックします。



認証サーバーのダイアログで「追加」をクリックします。

属 認証サーバー	×
Firebox RADIUS Secu	IID LDAP Active Directory
	ペースを有効にする
ipsec-user-01	
pptp-user-01	
	追加
「 ^{ユーザー グループ} ──	
IPSec-Users	
PPTP-Users	
33LVPN-08618	
	追加 」編集」削除

ユーザー情報に任意の名前を入力します。

パスフレーズは8文字以上の英数字を入力します。

Firebox 認証グループには、PPTP を有効にしたときに自動的に作成された PPTP-Users を選択し、<< をク リックし、新しいユーザーを PPTP-Users グループに含めます。

🔣 Firebox ユーザーのセットアップ			
名論	前: ssl-user-01		
說明	明:		
パスフレーン	⊼: ●●●●●●●●		
確	₽: ●●●●●●●●		
セッションタイムアウト	ト: 8- 時間 ▼		
アイドル タイムアウト	ト: 30 * 分 ▼		
Firebox 認証グループーー			
メンバー:	使用可能:		
	IPSec-Users		
	PPTP-Users		
	SSLVPN-OSers		
<u>QK</u> キャンセル ヘルプ			

以下の状態になります。

Firebox 認証グループ――			
メンバー:	_	使用可能:	
SSLVPN-Users		IPSec-Users	
	<<	PPTP-Users	
	>>		

ユーザー追加と認証サーバーのダイアログで OK をクリックして閉じたら、ポリシーマネージャーで設定を保存します。

Windows/MacOS の SSL クライアントの設定

クライアントの条件

モバイル VPN(SSL)クライアントソフトウェアをインストールできる OS は以下となります。

- ・ Microsoft Windows Vista (32-bit および 64-bit)
- ・ Microsoft Windows 7 および 8 (32-bit および 64-bit)
- ・ Microsoft Windows Server 2003 (32 ビット)
- Mac OS X 10.5 (Leopard)以降
- クライアント PC が Windows Vista または 7 および 8 の場合、モバイル VPN SSL クライアントソフト ウェアのインストールは管理者権限で行う必要があります。
- クライアント PC が MacOS X の場合、SSL クライアントのインストールおよび利用に管理者権限は必要 ありません。
- ・ クライアント PC に Firewall ソフトウェアがインストールされている場合、次のポートを許可してください。 TCP 4100 ポート

クライアントソフトウェアのダウンロード

① 次のサイトにアクセスします

https:// XTM の IP アドレス:4100/sslvpn.html

② あらかじめ作成しておいた SSLVPN ユーザーのユーザー名とパスワードを入力します

WatchGuard	Username: Password:
	Login Reset

ログインするとダウンロードサイトが表示されます。

- ③ クライアント PC の OS に応じたインストーラーをダウンロードしてください
- ④ ダウンロードしたインストーラーをデスクトップ等の任意の場所に保存します

クライアントソフトウェアのインストール

Windows の場合

- ① WG-MVPN-SSL.exe.をダブルクリックすると、The Mobile VPN with SSL client Setup ウィザードが起動 します
- ② デフォルトの設定が表示されるため「Accept」ボタンをクリックしてください
- ③ 「Finish」ボタンをクリックし、ウィザードを閉じてください

Mac OS の場合

- WG-MVPN-SSL.dmg をダブルクリックすると、デスクトップに WatchGuard Mobile VPN Volume が作成 されます
- ② WatchGuard Mobile VPN Volume をダブルクリックすると WatchGuard Mobile VPN with SSL Installer V15.mpkg が起動します
- ③ デフォルトの設定が表示されるため「Accept」ボタンをクリックしてください
- ④ 「Finish」ボタンをクリックし、ウィザードを閉じてください

クライアントソフトウェアのインストール後、自動的に XTM に接続します。XTM に接続する度に、クライアント ソフトウェアのアップデータがないか確認します。

SSL VPN の接続方法

(Windows の場合)

- ① クライアントソフトウェアを起動します
 - スタートメニュー>プログラム>WatchGuard Mobile VPN with SSL client>Mobile VPN with SSL clientを選択
- ② サーバー、ユーザー名、パスワードを入力します



- ※サーバーは、通常 External インターフェースに設定されている IP アドレスです
- ③ 「接続」ボタンをクリックします

(Mac OS の場合)

- Finder ウィンドウを開き、Applications > WatchGuard から WatchGuard Mobile VPN with SSL アプ リケーションをダブルクリックします
- ② メニューバーに WatchGuard Mobile VPN with SSL アイコンが表示されます
- ③ 表示されたアイコンをクリックし、「Connect」を選択します
- ④ 接続したい XTM の IP アドレスとユーザー名、パスワードを入力します

※XTM の IP アドレスは、通常 External インターフェースに設定されている IP アドレスです

⑤ 「Connect」ボタンをクリックします

Android OS の SSL クライアントの設定

プロファイルのダウンロード

モバイルデバイスの SSL クライアントアプリケーションから読み込むプロファイルは

<u>https://XTM の IP:4443/sslvpn.html</u> にアクセセスし、作成済みのアカウントでログインします。

WatchGuard	Username: username Password: •••••••• Login Reset

Mobile VPN with SSL client profile の download ボタンをクリックします。

Items available to downloa	d
Download	Mobile VPN with SSL client software for Windows Use this client to make a secure VPN connection to the company network from a Windows computer.
Download	Mobile VPN with SSL client software for Mac Use this client to make a secure VPN connection to the company network from a Mac computer.
Download	Mobile VPN with SSL client profile Import this profile to enable a secure VPN connection from any SSL VPN client that supports .ovpn configuration files.

保存します。

				1
Do you want to open or save client.ovpn (3.67 KB) from xtm.watchguardjapan.com?	<u>O</u> pen	Save •	<u>C</u> ancel ×	€ 100% -

client.ovpn というファイルが保存されます。



このファイルを SD カードに保存し、Android デバイスに転送します。

もしくはメールの添付ファイルで送信し、Android デバイスで受信したものを保存しておきます。



クライアントソフトウェアのインストール

Google Play ストアで OpenVPN を検索します。検索結果の OpenVPN Connect をタップします。



OpenVPN Connect インストールします。



画像/メディア/ファイル へのアクセスに同意します。



インストールが完了したら、アプリを開いてみます。



起動すればインストールは完了です。





Import Profile from SD card をタップします。



保存しておいたプロファイルを選択し、Select ボタンをタップします。

	🖋 🤝 📋 13:12		
OpenVPN Connect			
Please select .ovpn profile to import Select: /sdcard/Download/client.ovp	n		
► /			
■/			
■ client.ovpn			
Select	Cancel		

プロファイル インポートの画面になります。

接続先の XTM のホスト名または IP アドレスになっているか確認してください。

Profile Imported To create a shortcut to this profile or access the profile context menu (for delete, etc.), press and hold on the profile name below. To switch to a diffe tap the profile name briefly.	rename, erent profile,
OpenVPN Profile:	
xtm.watchguardjapan.com	
Username:	
Password:	
	Save
Profile successfully imported : xtm.watchguardjapan.c	om
Connect	

Username と Password を入力して Connect ボタンをタップします。



VPN 接続が作成される際にアラートが表示されますので、チェックして OK をタップします。



Username と Password を入力し、Connect ボタンをクリックします。



接続が成功すると、OpenVPN: Connected と表示されます。Tap for more detail リンクをタップ すると、VPNの接続状況の詳細が確認できます。



VPN 接続でデバイスが付与された IP アドレスなどが確認できます。



Ping コマンドを実行するアプリで、応答を確認できます。



RDP アプリで Windows マシンにアクセスできます。



iOS の SSL クライアントの設定

クライアントソフトウェアのインストール

App Store で OpenVPN を検索し、OpenVPN Connect をインストールします。

●●●●○ SoftBank 중 14:23
Q openvpn 11件の結果 😒
OpenVPN Connect OpenVPN Technolog
.∎L Verizon 🗢 11:15 💷
About OpenVPN Help
New profiles are available
1 new OpenVPN profile is available for import.
Private Tunnel/London Autologin profile
Autologin profile
Disconnected >
OFF
More from OpenVPN Technologies
Constructed private tunnel.com Your Secure
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$

アプリを開きます。



正常に起動すればインストールは完了です。

••••	SoftBank 穼	14:23		•		
Abc	out	OpenVPN	×	lelp		
WE	WELCOME TO OPENVPN					
OpenVPN requires a profile (.ovpn file) to connect to a server. Please use one of the following apps to import a profile:						
P	Import your profile.	Private Tunnel	Go			
If you are importing a profile from an OpenVPN Access Server, log into the server using Safari and click on "user- locked" or "autologin" profile.						
	Enter Acce	ss Server host	name			
,	Using iTune device, go t "apps" tab, and related file sharing v	s Sync, select o OpenVPN ur and drop your cert/key files ir window.	your ider the .ovpn nto the	>		
	If you receiv attachment open it in Op is less secu	re the profile as in the Mail app penVPN (Note: re).	s a .ovpn o, you can : this methc	od		

プロファイルの入手方法は、前章の「プロファイルのダウンロード」を参照してください。

VPN 接続プロファイルをメールの添付ファイルで送信し、iPhone/iPad で受け取ります。 添付されたプロファイルをタップします。



添付ファイルをどのアプリで開くか候補が出るので、「OpenVPN で開く」をタップします。



OpenVPN が新しいプロファイルが読み込み可能であることを表示します。接続先が正しいことを確認し、問題なければ ● をタップしてインポートします。



ユーザー名とパスワードを入力します。問題なければ Save も有効にします。Disconnected の下のスライド を右に移動し、接続します。



接続を許可するかたずねられたら、Yes をタップします。



Connected と表示されたら、正常に接続できています。下方の+ をタップすると、VPN の接続状況の詳細が 確認できます。

VPN 接続でクライアントデバイスが取得した IP アドレスなどが確認できます。

CONNECTION DETAILS					
Duration	0:17:34				
Packet received	4 seconds ago				
Bytes In	705.69 KB				
Bytes Out	148.83 KB				
VPN IPv4	192.168.113.2				
VPN IPv6					
User	username				
Client IP					
Server	xtm.watchguardjapan.com				
Server IP	202.171.138.193				
Port	4443				
Protocol	TCPv4				

Ping コマンドを実行するアプリで、応答を確認できます。

●●●●○ SoftBank 중 VPN 14:44	
Ping to 172.16.1.121 ping host = [172.16.1.121], Speed = [99ms] ping host = [172.16.1.121], Speed = [100ms] ping host = [172.16.1.121], Speed = [99ms] ping host = [172.16.1.121], Speed = [100ms] ping host = [172.16.1.121], Speed = [100ms]	

RDP アプリで Windows マシンにアクセスできます。



おわりに

VPN かんたん接続ガイドをご活用いただき、ありがとうございます。

このガイドを通して、WatchGuard 製品によっていかにモバイル VPN の接続環境の構築が容易か、実感していただけたと思います。

WatchGuard XTM が御社のセキュリティにお役に立てれば幸いです。