NRA

FortiGate(OS 6.0)における クライアント証明書認証設定 手順

2023年01月18日

Ver. 1.02

改訂履歴

版	日付	内容	備考
Ver.		初版作成	
1.00			
Ver.	2022/7/25	誤植修正	
1.01	2022/1/25		
Ver.	2022/1/10	誤植修正	
1.02	2023/1/10		

<目 次>

1. 概要	3
2. 事前準備	4
3. クライアント証明書認証をするための設定手順	6
3.1. 証明書メニューの有効化	7
3.2. 証明書のインポート	8
3.3. PKI ユーザの作成	13
3.4. グループの作成	15
3.5. SSL-VPN の設定	16
3.6. ポリシーの設定	17
4. ユーザ側での準備(WindowsPC)	18
5. サーバ証明書の入れ替え手順	19
5.1. 新しいサーバ証明書のインポート	20
5.2. サーバ証明書の設定	21

本書は Fortinet 社が提供している FortiGate(OS 6.0)における SSL-VPN 機能について、クライアント証明 書認証設定手順を説明いたします。

あくまで一例としてご紹介させていただいておりますので、詳細な設定等は FortiGate の販売店もしくはメ ーカーへお問い合わせください。





2. 事前準備

■SSL サーバ証明書

初期状態では自己署名のサーバ証明書が入っていますが、信頼性の観点から証明書ベンダーから調達することを推奨します。インストールする際には、PEM 形式に変換する必要があります。

■ルート証明書

以下 URL よりダウンロードしてください

https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthority.crt

■中間証明書

ご利用中の中間認証局の証明書を以下の URL からダウンロードしてください。

・中間証明書(CA3)

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3.crt

・中間証明書(CA4)

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4.crt

■失効リスト配布 URL

失効リストをインポートする際に使用します。

・中間認証局(CA3)

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl

・中間認証局(CA4)

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl

【ご利用中の中間認証局の確認方法】

以下画像の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックしていただくと、適用されているサービス名が表示されます。サービス名の後に(CA4)という表記があれば CA4、なければ CA3 をご利用いただいております。



3. クライアント証明書認証をするための設定手順

本項から詳細な設定手順に関する説明になります。

流れは次の通りです。

FortiGate にて証明書を利用できるように設定します。

準備していただいた SSL サーバ証明書、ルート証明書、中間証明書、失効リストをインポートします。

3. PKI ユーザの作成......13

SSL-VPN を利用するユーザを登録します。

4. グループの作成......15

登録した SSL-VPN を利用するユーザのグループを作成します。

5. SSL-VPN の設定......16

SSL-VPN の機能に関する詳細設定をします。

SSL-VPN を利用時のアクセスに関するルールを作成します。

項目は以上です。次ページから各項目の説明の記載になります。

3.1. 証明書メニューの有効化

管理画面から「システム」-「フィーチャー選択」より証明書を有効化し適用をクリックします。



以下図のように「フィーチャー選択」の下に「証明書」の項目が表示されます。



3.2. 証明書のインポート

事前準備で用意した各証明書とCRL(失効リスト)をインポートします。

■サーバ証明書

「システム」-「証明書」を選択し、「インポート」から「ローカル証明書」を選択します。

FortiGate 60D fg60d-demo					
🚯 ダッシュボード		➡ 生成 📝 編集 🛗	削除	● インポート マ	 ● 詳細の表示 ▲ ダウンロード Q 検索
📥 FortiView	>	▼ 名前		ローカル証明書	▼ サブジェクト
🕂 ネットワーク	>	証明書 (3)		CA証明書	
💠 システム	~	Fortinet_Factory	C = US	リモート	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者		Fortinet_SSL	C = US	CRL	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者プロファイル		🔄 Fortinet_Wifi	C = U9	6, CN = auth-cert.for	tinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi
設定		ローカル CA 証明書 (2)			
		Kortinet_CA_SSL	C = US	5, CN = FGT60D4Q1	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
HA		Fortinet_CA_Untrusted	C = US	6, CN = Fortinet Untr	rusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
SNMP		エクスターナル CA 証明書	(3)		
差し替えメッセージ		Fortinet_CA	C = U9	6, CN = support, L = 5	Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
FortiGuard		Fortinet_Wifi_CA	C = US	6, OU = (c) 2012 Entr	rust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K
Cooperative Security Fabric		Fortinet_Wifi_CA2	C = US	5, OU = (c) 2009 Entr	rust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2
高度					
フィーチャー選択					
証明書	☆				
▶ ポリシー & オブジェクト	>				
🔒 セキュリティプロファイル	>				

「証明書をインポート」の画面が表示されます。「タイプ」のリストから「証明書」を選択し、証明書ファイル、キーファイル、パスワード(任意)を指定し OK をクリックします

証明書をインポート

タイプ	証明書			
証明書ファイル	ファイルを選択 fg60d-demapki.com.crt			
キーファイル	ファイルを選択 fg60d-dempki.com.key			
パスワード	••••			
証明書名	fg60d-demo.nrapki.com			
		ОК	キャンセル	

サーバ証明書がインポートされたことを確認します。

FortiGate 60D fg60d-de	emo		
🔗 ダッシュボード	➡ 生成 📝 編集 📋	削除 ● インボート ▼ ● 詳細の表示 ▲ ダウンロード Q検索	
FortiView	> 【 名前	▼ サブジェクト	
♣ ネットワーク	> 証明書 (4)		
🔅 システム	✓ I Fortinet_Factory	C=US,CN=FGT60D4Q15027154,L=Sunnyvale,O=Fortinet,ST=California,emailAddress=support@fortinet.com,OU=FortiGate	Т
管理者	Fortinet_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate = Support@fortBate =	Т
管理者プロファイル	Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi	Т
設定	🔄 fg60d-demo.nrapki.com	C = JP, CN = fg60d-demo.nrapki.com, O = Nippon RA Inc.	
PXAE	ローカル CA 証明書 (2)		
HA	Fortinet_CA_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	Т
SNMP	Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	Т
美し替えメッヤージ	/ - / · · ·		

■ルート証明書、中間証明書

「システム」-「証明書」を選択し、「インポート」から「CA 証明書」を選択します。

FortiGate 60D fg60d-demo								
ช ダッシュボード		╋生成	☑ 編集	前前除	- ♪インポート -	● 詳細の表示	🛓 ダウンロード	Q.検索
FortiView	>	1	名前		ローカル証明書		٢	サ ブジェクト
♣ ネットワーク	>	証明書 (3))	1	CA証明書			
🔅 システム	~	🔄 Fortinet	t_Factory	C = U	リモート	5027154, L = Sunn	yvale, O = Fortinet, S	T = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者		🔄 Fortinet	t_SSL	C = U	CRL	5027154, L = Sunn	yvale, O = Fortinet, S	T = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者プロファイル		🔄 Fortinet	t_Wifi	C = U	6, CN = auth-cert.for	tinet.com, L = Sunny	vale, O = Fortinet, S	T = California, OU = FortiWifi
設定		ローカル	CA証明書(2)				
		🔄 Fortinet	t_CA_SSL	C = U	6, CN = FGT60D4Q1	5027154, L = Sunn	yvale, O = Fortinet, S	T = California, emailAddress = support@fortinet.com, OU = Certificate Authority
HA		🔄 Fortinet	t_CA_Untru	sted C = US	6, CN = Fortinet Untr	rusted CA, L = Sunn	yvale, O = Fortinet, S	T = California, emailAddress = support@fortinet.com, OU = Certificate Authority
SNMP		エクスター	ーナル CA訂	E明書 (3)				
差し替えメッセージ		📑 Fortinet	t_CA	C = U	6, CN = support, L = S	Sunnyvale, O = Forti	net, ST = California, e	emailAddress = support@fortinet.com, OU = Certificate Authority
FortiGuard		Fortinet	t_Wifi_CA	C = U	6, OU = (c) 2012 Entr	ust, Inc for autho	rized use only, O = En	ntrust, Inc., CN = Entrust Certification Authority - L1K
Cooperative Security Fabric		Fortinet	t_Wifi_CA2	C = U	6, OU = (c) 2009 Entr	ust, Inc for autho	rized use only, O = En	ntrust, Inc., CN = Entrust Root Certification Authority - G2
高度								
フィーチャー選択								
証明書	☆							
▶ ポリシー&オブジェクト	>							
🔒 セキュリティプロファイル	>							

「ローカル PC」を選択し「ファイルを選択」からルート証明書を選択し OK クリックします。

CA証明書をインポート

SCEP			(SCEPサーバのURL) (CA識別名(オプション))
☑ □−カルPC	ファイルを選択 NipponRARAuthority.crt		
		ок	キャンセル

ルート証明書、中間証明書をインポートされたことを確認します。

ช ダッシュボード		➡ 生成 🗹 編集 💼	削除 ヨインボート ▼ ● 詳細の表示 よ ダウンロード Q 検索	
▲ FortiView	>	▼ 名前	▼ サブジェクト	
♣ ネットワーク	>	証明書 (4)		
🔅 システム	~	Fortinet_Factory	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	1
管理者		Fortinet_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	1
管理者プロファイル		Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWlfi	1
		🔄 fg60d-demo.nrapki.com	C = JP, CN = fg60d-demo.nrapki.com, O = Nippon RA Inc.	
設正		ローカル CA 証明書 (2)		
HA		Fortinet_CA_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	/ 1
SNMP		Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	1
差し替えメッセージ		エクスターナル CA 証明書	(5)	
FortiGuard		CA_Cert_1	C = JP, CN = Nippon RA Root Certification Authority, O = Nippon RA Inc.	T
Cooperative Security Fabric		CA_Cert_2	C = JP, CN = Nippon RA Certification Authority 3, O = Nippon RA Inc.	
高度		Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	
フィーチャー選択		Fortinet_Wifi_CA	C = US, OU = (c) 2012 Entrust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K	
=T AB ===	~	Fortinet_Wifi_CA2	C = US, OU = (c) 2009 Entrust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2	

ポリシー&オブジェクト >

同手順にて中間証明書もインポートします。

■CRL(失効リスト)

「システム」-「証明書」を選択し、「インポート」から「CRL」を選択します

FortiGate 60D fg60d-demo								
ช ダッシュボード		╋生成	☑ 編集	前前除	→ インポート	● 詳細の表示	🛓 ダウンロード	Q 検索
FortiView	>	T	名前		ローカル証明書			▼ サブジェクト
🕂 ネットワーク	>	証明書 (3)			CA証明書			
🔅 システム	~	🔄 Fortinet	t_Factory	C = l	9 リモート	5027154, L = Sunn	yvale, O = Fortinet, S	ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者		🔄 Fortinet	t_SSL	C = L		5027154, L = Sunn	yvale, O = Fortinet, S	ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者プロファイル		🔄 Fortinet	t_Wifi	C = l	S, CN = auth-cert.for	tinet.com, L = Sunny	vale, O = Fortinet, S	ST = California, OU = FortiWifi
		ローカル(CA証明書(2)				
5XAE		🔄 Fortinet	t_CA_SSL	C = l	S, CN = FGT60D4Q1	15027154, L = Sunny	vale, O = Fortinet, S	ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
HA		🔄 Fortinet	t_CA_Untru	sted C = L	S, CN = Fortinet Unt	rusted CA, L = Sunn	yvale, O = Fortinet, S	ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
SNMP		エクスター	ーナルCAI	E明書 (3)				
差し替えメッセージ	1	Fortinet	t_CA	C = l	S, CN = support, L = S	Sunnyvale, O = Forti	net, ST = California,	, emailAddress = support@fortinet.com, OU = Certificate Authority
FortiGuard		💼 Fortinet	t_Wifi_CA	C = L	S, OU = (c) 2012 Entr	rust, Inc for author	ized use only, O = Er	ntrust, Inc., CN = Entrust Certification Authority - L1K
Cooperative Security Fabric		Fortinet	t_Wifi_CA2	C = L	S, OU = (c) 2009 Ent	rust, Inc for author	rized use only, O = Er	ntrust, Inc., CN = Entrust Root Certification Authority - G2
高度								
フィーチャー選択								
証明書	☆							
▶ ポリシー&オブジェクト	>							
🔒 セキュリティプロファイル	>							

HTTP を選択し CRL 配布ポイントの URL を入力し、OK をクリックします。

CRLをインポート

🗸 НТТР	http://mpkicrl.managedpki.ne.jp/mpki/Nippo	onRACertification	(HTTPサーバのURL)
LDAP	[選択してください] 🗸		
SCEP	Fortinet_CA_SSL V		
			(SCEPサーバのURL)
□ □−カルPC	ファイルを選択選択されていません		
		ок	キャンセル

CRL がインポートされたことを確認します

FortiGate 60D fg60d-d	lem	o		
ช ダッシュボード		➡ 生成 📝 編集 💼	削除 2インポート ▼ ◎ 詳細の表示 2 ダウンロード Q 検索	
FortiView	>	▼ 名前	▼ サブジェクト	
🕂 ネットワーク	>	証明書 (4)		
🔅 システム	~	Fortinet_Factory	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	Т
管理者		Fortinet_SSL	C=US,CN=FGT60D4Q15027154,L=Sunnyvale,O=Fortinet,ST=California,emailAddress=support@fortinet.com,OU=FortiGate	Т
管理者プロファイル		Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi	Т
197fc		🔄 fg60d-demo.nrapki.com	C = JP, CN = fg60d-demo.nrapki.com, O = Nippon RA Inc.	
•XAL		ローカル CA 証明書 (2)		
HA		Fortinet_CA_SSL	C=US,CN=FGT60D4Q15027154,L=Sunnyvale,O=Fortinet,ST=California,emailAddress=support@fortinet.com,OU=CertificateAuthority	Т
SNMP		Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	Т
差し替えメッセージ		エクスターナル CA 証明書		
FortiGuard		CA_Cert_1	C = JP, CN = Nippon RA Root Certification Authority, O = Nippon RA Inc.	
Cooperative Security Fabric		CA_Cert_2	C = JP, CN = Nippon RA Certification Authority 3, O = Nippon RA Inc.	
高度		Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	
フィーチャー選択		Fortinet_Wifi_CA	C = US, OU = (c) 2012 Entrust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K	
証明書	☆	Fortinet_Wifi_CA2	C = US, OU = (c) 2009 Entrust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2	
■ ポリシー&オブジェクト	>.	証明書失効 (1)		
■ セキュリティプロファイル	>	CRL_1		

【補足】

CRL(失効リスト)がうまく取得できない場合は OCSP レスポンダをお試しください。

OCSP レスポンダ URL

http://mpkiocsp.managedpki.ne.jp/mpkiocsp

■OCSP レスポンダの設定方法

CLI コンソールを使って以下コマンドを<>の中を実際の値にして設定します。

config vpn certificate ocsp-server edit <任意の値>※画像では mpki_ocsp set url http://mpkiocsp.managedpki.ne.jp/mpkiocsp set cert <中間 CA の登録名> set unavail-action revoke end exit

設定が変更されているかを確認します。 ■確認コマンド① config vpn certificate ocsp-server edit 〈設定した任意の値> get

【設定完了画面①(例)】

FGT50E5619031121	(mpki_ocsp) # get
name	: mpki_ocsp
url	: http://mpkiocsp.managedpki.ne.jp/mpkiocsp
cert	: CA_Cert_1
secondary-url	:
secondary-cert	:
unavail-action	: revoke
source-ip	: 0.0.0.0

■確認コマンド②

config vpn certificate setting

get

【設定完了画面②(例)】

FGT50E5619031121 (set	ting) # get
ocsp-status :	enable
ssl-ocsp-status :	enable
ssl-ocsp-option :	server
ocsp-default-server :	mpki_ocsp
check-ca-cert :	enable
check-ca-chain :	disable
subject-match :	substring
cn-match :	substring
strict-crl-check :	disable
strict-ocsp-check :	disable
ssl-min-proto-version	: default
cmp-save-extra-certs:	disable
certname-rsa1024 :	Fortinet_SSL_RSA1024
certname-rsa2048 :	Fortinet_SSL_RSA2048
certname-dsa1024 :	Fortinet_SSL_DSA1024
certname-dsa2048 :	Fortinet_SSL_DSA2048
certname-ecdsa256 :	Fortinet_SSL_ECDSA256
certname-ecdsa384 :	Fortinet_SSL_ECDSA384

差異がある場合は以下コマンドを参考に変更してください。

config vpn certificate setting set ocsp-status enable

end

exit

3.3. PKI ユーザの作成

「ユーザ&デバイス」-「PKI」を選択し、新規作成を選択。

FortiGate 60D fg60d-	demo				
🚯 ダッシュボード	🕇 新規作成) 🗹	編集 💼 削除			
📥 FortiView	>	▼ 名前	▼ サブジェクト	T CA	
🕂 ネットワーク	> testvpn			CA_Cert_2	
💠 システム	> vpntest	test@test.j	p	CA_Cert_1	
💄 ポリシー & オブジェクト	>				
🔒 セキュリティプロファイル	>				
D VPN	>				
🚨 ユーザ&デバイス	~				
ユーザ定義					
ユーザグループ					
ゲストマネジメント					
デバイスインベントリ					
カスタムデバイス&グルー プ					
シングルサインオン					
LDAPサーバ					
RADIUSサーバ					
認証設定					
FortiToken					
РКІ	☆				
♥WiFi&スイッチコントロー ラー	>				

以下画像の赤枠内の項目を設定し OK をクリックします。

FortiGate 60D fg60	d-dem	0
	>	PKIユーザの作成
● セキュリティプロファイ ル □ VPN	>	名前 testvpn サブジェクト test@test.com
▲ ユーザ&デバイス	~	CA CA_Cert_2
ユーザ定義		○ 二要素認証
ユーザグループ		
ゲストマネジメント		
デバイスインベントリ		
■設定例		

名前:任意の値

サブジェクト:任意の値 ※【補足1】参照

CA: インポートした中間証明書

※二要素認証は必要に応じて設定してください。

【補足1】 サブジェクトについて

認証する証明書をサブジェクトにより制限します。証明書のサブジェクト O(会社名)で制限する場合は、 『O=xxxxxxx』の形式で入力して下さい。サブジェクト E(メールアドレス)で判断する場合には 『xxxx@xx.xx』のように、E=などは入力せずメールアドレスのみ入力してください。 空欄の場合、CA で設定した中間証明書の認証局で発行した証明書を認証します。

【補足 2】

「ユーザ&デバイス」に「PKI」をの項目がない場合は、CLIから以下コマンドにて一度登録してください。 登録後に一度管理画面がらログアウトし、再度ログインすると管理画面から「PKI」の項目が表示されます。

config user peer

edit <ユーザ名> ※任意の値

set ca CA_Cert_1 (CA_cert_1 は中間証明書。必要に応じて名前は変更)

<Email アドレス>(あとで UI で変更可能。今設定しなくても OK。)

end

exit

3.4. グループの作成

「ユーザ&デバイス」-「ユーザグループ」から「新規作成」をクリックします。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	FortiGate 60D fg60	d-der	no		i ?	[] admin▼
上 FortiView ・ グリーブ名 ・ グリーブタイブ ・ ジェック	🕫 ダッシュボード	í	◆新規作成 ● 「編集 ● クローン ●	削除 Q.検索		
・ネットワーク 121group(1メンバ) ゴフィアウカール 122 1 ・システム ドSSO_Guest(Users(0メンバ) Group(1メンバ) Group(1メンバ) 0 ・ポリシーをオブシット Guest-group(1メンバ) ゴフィアウカール Aguest 0 ・セキュリティブロファイ ・レ SSLVPN01(1メンバ) ゴフィアウカール Aguest 0 ・ロ SSLVPN01(1メンバ) ゴフィアウカール Aguest 0 ・ロ SSLVPN01(1メンバ) ゴフィアウカール Aguest 0 ・ロ napki-vpn-test-group(1メンバ) ゴフィアウカール Aguest 0 ・コ ・ロ ・ロ 0 0 0 ・コ ・ロ ・ロ ・ロ 0 0 0 ・コ ・ロ ・ロ ・ロ ・ロ 0	FortiView	>	▼ グループ名	▼ グループタイプ	フィント	▼ 参照
 	♣ ネットワーク	>	121group (1メンバ)	ロ ファイアウォール	å 122	1
トポリシー&オブジェクト・> Guest-group(1メンパ) ゴフィブウォール aguest o セキュリティブロファイ ル SSLVPN01(1メンパ) ゴフィブウォール Atest 2 ロVPN SSLVPN01(1メンパ) ゴフィブウオール Atest 0 ロVPN nrapki-vpn-test-grp(1メンパ) ゴフィブウオール Anaptive 0 Source (US x y (US x	✿ システム	>	FSSO_Guest_Users (0 メンバ)	■ Fortinetシングルサインオン(FSSO)		0
セキュリティブロファイ ル SSLVPN01(1メン/) ゴファイアウォール ▲ test 2 ロVPN SSL-VPN01(1メン/) © Fortinetシングルサインオン(FSSO) 0 0 ロVPN nrapki-vpn-test-grp(1メン/) ゴファイアウォール ▲ nrapki-vpn-test 0 So-ypn group(1メン/) ゴファイアウォール ▲ nrapki-vpn-test 0 0	💄 ポリシー & オブジェクト	>	Guest-group (1メンバ)	ロ ファイアウォール	👗 guest	0
リレ SSO_Guest_Users(0メンパ) Fortinetシングルサインオン(FSSO) ロ 0 ロ VPN nrapki-vpn-test-grp(1メンパ) ロファイアウォール ▲ nrapki-vpn-test 0 ▲ ユーザ&デパイス ss-vpn_group(1メンパ) ロファイアウォール ▲ LDAP PROXY 2	▲ セキュリティプロファイ		SSL-VPN01(1メンバ)	ロ ファイアウォール	🛔 test	2
ユ VPN 「「」」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」」 「」」」 <th」< th=""> 「」」」 <th」<< td=""><td>- JL</td><td>1</td><td>SSO_Guest_Users (0 メンバ)</td><td>■ Fortinetシングルサインオン(FSSO)</td><td></td><td>0</td></th」<<></th」<>	- JL	1	SSO_Guest_Users (0 メンバ)	■ Fortinetシングルサインオン(FSSO)		0
▲ ユーザ&デバイス Ss-vpn_group(1メンバ) 単ファイアウォール & LDAP PROXY 2	U VPN	2	nrapki-vpn-test-grp(1メンパ)	ロ ファイアウォール	🚨 nrapki-vpn-test	0
	▲ ユーザ&デバイス	9	ss-vpn_group(1メンバ)	ロ ファイアウォール	LDAP PROXY	2
ユーザ定義	ユーザ定義	_				

以下画像の赤枠内の項目を設定し OK をクリックします。

FortiGate 60D fg60d-dem	0	1	2	?	13	admin 🔻
Øツシュボード	ユーザグループ作成					·
▲ FortiView > ↓ ネットワーク >	名前 vpn-test タイプ ③ ファイアウォール 〇 Fortinetシングルサインオン(FSSO) 〇 グスト 〇 RADIUSシングルサインオン(RSSO) メンパ vontest					- 1
 システム 	י - אולאי - של					
ポリシー&オブジェクト >	📀 Create New 🛛 🖉 Edit. 🍵 Delete	_				_
● ^{セキュリティプロファイ} →	リモートサーバ グループ名 マッチするエントリーはありません。					- 1
□VPN >	(OK) キャンセル					- 1
🛓 ユーザ&デバイス 🛛 🗸 🗸						
ユーザ定義						
ユーザグループ 🏠						- 1
ゲストマネジメント						
■設定例						

名前:任意の値

ゲストマネジメント デバイスインベントリ カスタムデバイス&グル

タイプ:ファイアウォール

メンバ:作成した PKI ユーザを選択

3.5. SSL-VPN の設定

「VPN」-「SSL-VPN 設定	」から以下画像の赤枠の項目を設定し	「適用」をクリックします。
-------------------	-------------------	---------------

FortiGate 60D fg60d-o	demo	0			
Øッシュボード		SSL-VPN設定			
📥 FortiView	>				
♣ ネットワーク	>	接続設定 🚺			
🌣 システム	>	Listenするインターフェース	wan1 X		
💄 ポリシー & オブジェクト	>	Listenするポート	443		
● セキュリティプロファイル	>		● Webモードアクセスを listen するポート:	https://192.168.77.3	
ロ VPN IPsecトンネル	~	アクセスを制限	任意のホストからアクセス許可特定ホスト	ヘアクセス制限	
IPsecウィザード		アイドルログアウト	200		
IPsec トンネルテンプレート		inactive For	300 秒		
SSL-VPN ポータル		クライアント証明書を要求	1900a demonraphicom		
SSL-VPN 設定	☆	トン・フルテード クライマント きつ	÷ •		
▲ ユーザ&デバイス	>	ドノイルモートシライアント設		u dirinda	
♥WiFi&スイッチコントロー ラー	>	アドレス範囲	日期的にアトレス割り当て カスタムIP範囲和 Tunnel users will receive IPs in the range of 10	ご指正 .212.134.200 -	
<u>Ⅲ</u> ログ&レポート	>		10.212.134.210		
С Т	>	DNSサーバ WINSサーバを指定 エンドポイント登録を許可 〇	クライアントシステムのDNSと同じ 指定		
		認証/ボータルマッピング ()			_
		➡新規作成 🖸 編集 📋	〕 削除		
			ユーザ/グループ	ポータル	
		📽 vpn-test		full-access	
		すべてのその他のユーザ/グル	ーブ	tunnel-access	
Q					適用

■設定例

Listen するインターフェース: wan1

Listen するポート:任意(後述「ユーザ側での準備」で使用します)

サーバ証明書:インポートしたサーバ証明書を選択

クライアント証明書を要求:チェック

認証/ポータルマッピング:新規作成をクリックし、「ユーザ/グループ」は作成した PKI ユーザが入っている グループ、ポータルは任意で設定。

3.6. ポリシーの設定

「ポリシー&オブジェクト」-「IPv4 ポリシー」から新規作成をクリックします。



以下画像の赤枠内の項目を設定し OK をクリックします。

FortiGate 60D fg60d-	dem	D
🚯 ダッシュボード		ポリシーの作成
FortiView	>	
♣ ネットワーク	>	
🗘 システム	>	
💄 ポリシー & オブジェクト	~	出たファンティース (1997) 送信元 · · · · · · · · · · · · · · · · · · ·
IPv4ポリシー	☆	📽 vpn-test 🛛 🗶
アドレス		宛先アドレス III X
インターネットサービスデ		
ータベース		
サービス		
スケジュール		ファイアウォール/ネットワークオブション
パーチャルIP		NAT O
IPプール		
トラフィックシェーパー		ドノール線定 12154 フタブエーズのアドレス変換用 タイナミックドノール変換つ
トラフィックシェーピング		セキュリティブロファイル
■ ビキエッティブロブアイル	2	
ションPIN ミューザ&デバイス		アプリケーションコントロール ①
	1	CASI 🔘
♥WIFI @ 入1 ♥ + J 2 FU- 5-	>	SSLインスペクション ①
Ⅲ ログ&レポート	>	ロギングオプション
€ モニタ	>	許可トラフィックをログ 〇 セキュリティイベント すべてのセッション
		- うそこで、 (1)
Q		OKキャンセル

■設定例

入力インターフェース:SSL-VPN トンネルインターフェース 出力インターフェース:wan1(内側の設定は lan) 送信元:all、SSLVPN-UserGroup 宛先:all(スプリットトンネリング使う際は接続先アドレスを指定) スケジュール:always

サービス:ALL

※その他の項目は任意で設定してください。

以上で Fortigate(OS6.0)における SSL-VPN 機能の設定は完了です。

4. ユーザ側での準備(WindowsPC)

ユーザのご利用の端末にて Forticliant をダウンロード・インストールしてください。 Forticliant を起動し、「リモートアクセス」から「新規接続の追加」より、以下を参考に設定を追加してくだ さい。

■設定例
 VPN: SSL-VPN
 接続名:任意の値
 説明:任意の値
 リモートGW: fortiGateのグローバル IP アドレス
 ポートの編集:チェック入れ、4.SSL-VPN 設定で設定した「Listen するポート」を指定
 クライアント証明書: PKI ユーザ作成時に指定した証明書を選択
 認証:任意

新規VPN接続		
VPN	SSL-VPN IPsec VPN	
接続名	vpntest	
説明	test	
リモートGW	0.0.0.0	×
	◆リモートゲートウェイを追加	-
	✔ ポートの編集 443	
クライアント証明書	test test/Nippon RA Certification Authority 3	
認証	🔵 ユーザ名入力 🛛 ユーザ名を保存 🔹 💽 無効	
	── 無効なサーバ証明書の警告を非表示	
	キャンセル 保存	

5. サーバ証明書の入れ替え手順

本項ではインポートしたサーバ証明書の入れ替え手順の説明になります。 サーバ証明書の有効期限が切れる前に実施してください。

事前準備

・新しい SSL サーバ証明書(PEM 形式)

流れは次の通りです。

準備していただいた新しい SSL サーバ証明書をインポートします

インポートした新しいサーバ証明書と現在設定しているサーバ証明書を入れ替えます。

項目は以上です。次ページから各項目の説明の記載になります。

5.1. 新しいサーバ証明書のインポート

「システム」-「証明書」を選択し、「インポート」から「ローカル証明書」を選択します。

FortiGate 60D fg60d-dem	10		
🙆 ダッシュボード	➡ 生成 🕑 編集 🛗	削除 💽 インポート 🗸	● 詳細の表示 よ ダウンロード Q検索
FortiView >	▼ 名前	ローカル証明書	▼ サブジェクト
♣ネットワーク >	証明書 (3)	CA証明書	
🛊 ЭЛ Г Ь 🗸 🗸	Fortinet_Factory	C=US リモート	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者	Continet_SSL	C = US CRL	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
管理者プロファイル	🔄 Fortinet_Wifi	C = US, CN = auth-cert.for	tinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi
設定	ローカル CA 証明書 (2)		
BXAL	Fortinet_CA_SSL	C = US, CN = FGT60D4Q1	5027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
HA	Fortinet_CA_Untrusted	C = US, CN = Fortinet Unt	rusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
SNMP	エクスターナル CA 証明書	∄ (3)	
差し替えメッセージ	Fortinet_CA	C = US, CN = support, L = S	Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
FortiGuard	Fortinet_Wifi_CA	C = US, OU = (c) 2012 Entr	rust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K
Cooperative Security Fabric	Fortinet_Wifi_CA2	C = US, OU = (c) 2009 Entr	rust, Inc for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2
高度			
フィーチャー選択			
証明書			
💄 ポリシー & オブジェクト 💦 >			

▲ セキュリティプロファイル >

「証明書をインポート」の画面が表示されます。「タイプ」のリストから「証明書」を選択し、証明書ファイル、キーファイル、パスワード(任意)を指定し OK をクリックします

証明書をインポート

タイプ	証明書
証明書ファイル	ファイルを選択 fg60d-demapki.com.crt
キーファイル	ファイルを選択 fg60d-dempki.com.key
パスワード	••••
証明書名	fg60d-demo.nrapki.com
	ок <i>‡т>ти</i>

サーバ証明書がインポートされたことを確認します。

FortiGate 60D fg60d-d	demo)		
ช ダッシュボード	[+ 生成 ■ 編集 曲	削除 1 インボート ▼ ● 詳細の表示 2 ダウンロード Q 検索	
FortiView	>	▼ 名前	▼ サブジェクト	
◆ ネットワーク	>	証明書 (4)		
🔅 システム	~	Fortinet_Factory	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	т
管理者		Sortinet_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	т
管理者プロファイル		🗟 Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi	Т
設定	(🔄 fg60d-demo.nrapki.com	C = JP, CN = fg60d-demo.nrapki.com, O = Nippon RA Inc.	
PZ/E	_	ローカル CA 証明書 (2)		
HA		Fortinet_CA_SSL	C = US, CN = FGT60D4Q15027154, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	т
SNMP		Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	т
差し替えメッヤージ		/ / · / - ·		

5.2. サーバ証明書の設定

「VPN」-「SSL-VPN 設定」から「サーバ証明書」の項目をインポートした新しい証明書に変更し、「適用」 をクリックします。



以上の手順でサーバ証明書入れ替え完了です。古いサーバ証明書は必要に応じて削除してください。