L2TP/IPsecを利用するための設定例

対象装置：FITELnet F70/F71/F220/F221/F225/F310/F220 EX/F221 EX

Phase1 SA：RSA認証、PPPセッション：Local認証

※ログインID/Passwordは"test"/"test"です。

	設定例	補足
1	access-list 100 permit udp any host <FITELnet_global_IPaddress> eq 500	フィルタ用(許可　isakampパケット)
2	access-list 100 permit udp any host <FITELnet_global_IPaddress> eq 4500	フィルタ用(許可　sakampパケット NAT-T)
3	access-list 100 permit 50 any any	フィルタ用(許可　ESPパケット)
4	access-list 111 deny udp any eq 135 any	UDPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
5	access-list 111 deny udp any any eq 135	UDPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
6	access-list 111 deny tcp any eq 135 any	TCPポート135（MS DCOM / RPC）からの全てのトラフィックを拒否します。
7	access-list 111 deny tcp any any eq 135	TCPポート135（MS DCOM / RPC）への全てのトラフィックを拒否します。
8	access-list 111 deny udp any range 137 139 any	UDPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
9	access-list 111 deny udp any any range 137 139	UDPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
10	access-list 111 deny tcp any range 137 139 any	TCPポート137-139（NetBIOS関連）からの全てのトラフィックを拒否します。
11	access-list 111 deny tcp any any range 137 139	TCPポート137-139（NetBIOS関連）への全てのトラフィックを拒否します。
12	access-list 111 deny udp any eq 445 any	UDPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
13	access-list 111 deny udp any any eq 445	UDPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
14	access-list 111 deny tcp any eq 445 any	TCPポート445（Microsoft-DS / SMB）からの全てのトラフィックを拒否します。
15	access-list 111 deny tcp any any eq 445	TCPポート445（Microsoft-DS / SMB）への全てのトラフィックを拒否します。
16	access-list 112 deny ip 192.168.100.0 0.0.0.255 any	IPアドレス範囲192.168.100.0/24からの全てのトラフィックを拒否します。
17	access-list 112 permit icmp any 192.168.100.0 0.0.0.255	192.168.100.0/24へのICMPトラフィックを許可します。
18	access-list 113 spi tcp any any eq ftp	TCPポート21（FTP）への全てのトラフィックを許可します。応答パケットも許可されます。
19	access-list 113 spi tcp any any eq ftp-data	TCPポート20（FTPデータ）への全てのトラフィックを許可します。応答パケットも許可されます。
20	access-list 113 spi tcp any any eq www	TCPポート80（HTTP）への全てのトラフィックを許可します。応答パケットも許可されます。
21	access-list 113 spi udp any any eq domain	UDPポート53（DNS）への全てのトラフィックを許可します。応答パケットも許可されます。
22	access-list 113 spi tcp any any eq smtp	TCPポート25（SMTP）への全てのトラフィックを許可します。応答パケットも許可されます。
23	access-list 113 spi tcp any any eq pop3	TCPポート110（POP3）への全てのトラフィックを許可します。応答パケットも許可されます。
24	access-list 113 spi tcp any any eq 587	TCPポート587（SMTPサブミッション）への全てのトラフィックを許可します。応答パケットも許可されます。
25	access-list 113 spi tcp any any	全てのTCPトラフィックを許可します。応答パケットも許可されます。
26	access-list 113 spi udp any any	全てのUDPトラフィックを許可します。応答パケットも許可されます。
27	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
28	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
29	!	
30	ip route 0.0.0.0 0.0.0.0 tunnel 1	経路設定
31	ip local pool POOL1 192.168.1.101 192.168.1.200	IPsec やL2TP/PPP により通知するアドレス範囲の設定
32	ip nat list 1 192.168.1.0 0.0.0.255	NAT/NAT+ 変換で変換後アドレスとして利用可能範囲の設定
33	!	
34	traffic-manager network	
35	to-host protocol ipv4 l2tp policer 11	自局宛トラフィックが入力されるポリサーの設定
36	exit	
37	!	
38	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
39	!	
40	logging buffer level informational	装置内部バッファへ出力するログレベルを指定 ※"show logging buffer"で確認可能
41	!	
42	aaa authentication ppp LOCAL_AUTH local-group LOCAL_GROUP	PPP セッションの認証方式を設定
43	!	
44	aaa authentication login default local	ログイン認証方式を指定 local: usernameコマンドで設定した内容(id, password)で認証 login: "password login"コマンドで設定した内容(id: operator) ※default設定
45	aaa authorization exec default local	TELNETログイン時の許可方式を指定 local: usernameコマンドで設定した特権レベルでログイン許可
46	!	
47	aaa local group LOCAL_GROUP	CLIENT- データベース設定モード
48	username user1 password secret1	接続を許可するユーザ名とパスワードの設定
49	username user2 password secret2	
50	exit	
51	!	
52	username guest password guest-secret	
53	!	
54	hostname FITELnet	hostname設定
55	!	

©2021 Furukawa Electric Co., Ltd

	設定例	補足
56	crypto ipsec policy IPSECPOL_1	IPsecポリシー設定(Phase2 SAのパラメータを指定)
57	mode transport	
58	set security-association lifetime seconds 86400	Phase2 SAのLifetime(秒)を指定 ※defaultのRekeyの開始タイミングはResponder動作時はLifetime満了の30秒前、Initiator動作時は90秒前に開始 set security-association softlimit initiate seconds 90 set security-association softlimit respond seconds 30
59	set security-association transform-keysize aes 128 256 256	暗号化アルゴリズム(AES)の鍵サイズを指定 ※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値
60	set security-association transform esp-aes esp-3des esp-md5-hmac esp-sha-hmac	暗号化アルゴリズム(AES)とハッシュアルゴリズム(SHA1)を指定
61	set ip df-bit 0	ポストフラグメント指定 ※プリフラグメント指定の場合は削除 ※暗号化後のESPパケットのDFビットを"0"に設定します。 (defaultでは暗号化対象パケットのDFビットをコピーします)
62	set ip fragment post	ポストフラグメント指定 ※プリフラグメント指定の場合は削除
63	set udp-encapsulation nat-t keepalive interval 30 always-send	ESP パケットのUDP カプセル化を行うポリシー個別の方式の設定
64	exit	
65	!	
66	crypto isakmp keepalive always-send	DPD設定(Traffic監視) ※interval内にESP、又はDPD-R-U-THEREパケットを受信していない場合にRequestを送信します。 (interval毎に毎回送信する場合はalways-sendを指定)
67	crypto isakmp log sa detail	SYSLOGにSA確立／解放のログを出力 ※Phase1, 2 SA確立時にSession確立、どちらも削除された際にSession切断となります
68	crypto isakmp log session detail	SYSLOGにSession確立・切断のログを出力 ※Phase1, 2 SA確立時にSession確立、どちらも削除された際にSession切断となります
69	crypto isakmp log negotiation-fail detail	SYSLOGにIKEネゴシエーション失敗のログを出力
70	!	
71	crypto isakmp policy ISAPOL_1	ISAKMPポリシー設定(Phase1 SAのパラメータを指定)
72	authentication rsa-sig	RSA-signatures認証を指定
73	encryption aes	暗号化アルゴリズムを指定
74	encryption-keysize aes 256 256 256	暗号化アルゴリズム(AES)の鍵サイズを指定 ※受け入れ可能な鍵サイズの最小値、最大値、Initiator提案時の最優先値
75	group 1 2 5 14 15	DHグループを指定
76	lifetime 86400	Phase1 SAのLifetime(秒)を指定 ※Lifetime満了時にISAKMP SAを削除し、Rekey、及びDPD契機で再接続します
77	hash sha	ハッシュアルゴリズムを指定
78	initiate-mode main	IKE接続方式としてMainモードを指定
79	exit	
80	!	
81	crypto isakmp profile ISAPROF_001	ISAKMPプロファイル設定
82	self-identity fqdn CENTER.example.com	本装置の識別方法を設定(fqdn="CENTER.example.com") ※証明書登録のために必要な設定です。
83	set isakmp-policy ISAPOL_1	ISAKMPポリシーを指定
84	set ipsec-policy IPSECPOL_1	IPsecポリシーを指定
85	ike-version 1	IKEバージョンを指定
86	ca trustpoint rootCA	登録したCA証明書名を指定(rootCA)
87	exit	
88	!	
89	crypto map MAP_001 ipsec-isakmp dynamic	CRYPTO MAP設定
90	set isakmp-profile ISAPROF_001	セレクタを指定
91	exit	ISAKMPプロファイルと紐付け
92	!	
93	interface GigaEthernet 1/1	物理インタフェース
94	vlan-id 1	VLAN指定(ポートVLAN) ※必須
95	bridge-group 1	bridge-group指定 ※必須
96	channel-group 1	論理インタフェース(Port-channel)と紐付け
97	exit	
98	!	
99	interface GigaEthernet 2/1	物理インタフェース
100	vlan-id 2	VLAN指定(ポートVLAN) ※必須
101	bridge-group 2	bridge-group指定 ※必須
102	pppoe enable	pppoe enable
103	exit	
104	!	
105	interface Port-channel 1	論理インタフェース設定
106	ip address 192.168.1.1 255.255.255.0	アドレス設定
107	ip proxy-arp	proxy-arp 動作を行う設定
108	exit	
109	!	

©2021 Furukawa Electric Co., Ltd

	設定例	補足
110	interface Tunnel 1	Tunnelインタフェース設定(PPPoE Tunnel)
111	ip address <FITELnet_global_IPaddress> 255.255.255.255	アドレス設定
112	ip access-group 100 in	フィルタリング設定
113	ip access-group 111 out	IPv4アクセスリスト紐づけ
114	ip access-group 112 in	IPv4アクセスリスト紐づけ
115	ip access-group 113 out	IPv4アクセスリスト紐づけ
116	ip access-group 114 out	IPv4アクセスリスト紐づけ
117	ip access-group 115 in	IPv4アクセスリスト紐づけ
118	ip access-group spi ftp-data enable	学習フィルタ追加
119	ip nat inside source list 1 interface	nat設定
120	tunnel mode pppoe profile PPPOE_PROF	PPPoEプロファイルと紐付け
121	pppoe interface gigaethernet 2/1	PPPoEインタフェース指定
122	exit	
123	!	
124	ppp-template PPP_001	PPP テンプレート設定モード
125	pool POOL1	PPP で通知するIP アドレス範囲の、アドレスプール名を設定
126	ppp authentication chap LOCAL_AUTH	PPP の認証タイプと認証方式名を設定
127	exit	
128	!	
129	l2tpv2 tunnel-profile LNS_001	L2TPv2 トンネル設定モード
130	ppp accept template PPP_001	該当L2TPv2 トンネル上で収容するPPP セッションを関連付け
131	local name LNS1	LNS装置のホスト名を指定
132	tunnel protection ipsec map MAP_001	VPN セレクタ名指定
133	exit	
134	!	
135	l2tpv2 log ccn	L2TPv2 メッセージを出力（Control connection の確立/ 解放）
136	l2tpv2 log session	L2TPv2 メッセージを出力（セッション確立/ 解放）
137	l2tpv2 log negotiation-fail	L2TPv2 メッセージを出力（ネゴシエーション失敗）
138	!	
139	pppoe profile PPPOE_PROF	PPPoEプロファイル
140	account <pppoe_user> <pppoe_password>	アカウント設定
141	exit	
142	!	
143	dns-server ip enable	DNS サーバ機能およびProxyDNS機能の有効化
144	!	
145	proxydns domain 1 any * any ipcp tunnel 1	ProxyDNSの正引き動作条件の設定
146	!	クラスにマッチしたパケット数をカウントする設定
147	end	クラスにマッチしたパケットを経路表に従って送信する設定

©2021 Furukawa Electric Co., Ltd