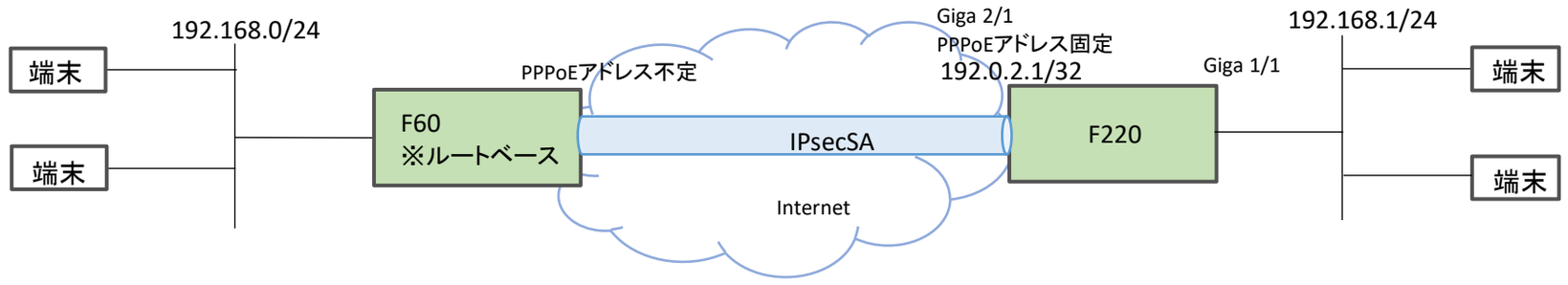
設定例

F60とIPsecでトンネリングする：F60ルートベース-F220ルートベース

概要

F60をルートベース方式として（IPsecインタフェースを利用）、F220とIPsecトンネリング接続するための設定例です。
・暗号化対象(IPsecセレクタ)を全src/dstアドレスとして、双方で対向拠点のLANネットワークへのTunnel（IPsec）経路を登録すれば、SA接続および通信可能です。



パラメータ設定例

ISAKMPポリシー

IKEバージョン	1
モード	Aggressiveモード
認証方式	事前共有鍵方式
暗号化方式	AES 256ビット
ハッシュ方式	SHA-1
Diffie-Hellman	Group 14
ライフタイム	86400秒

IPSECポリシー

PFS	Group 14
暗号化方式	AES 256ビット
ハッシュ方式	SHA-1
ライフタイム	28800秒
フラグメント	ポストフラグメント

コマンド設定例

F60の設定

	設定例(F60)	補足
1	ip route 0.0.0.0 0.0.0.0 pppoe 1	
2	ip route 192.168.1.0 255.255.255.0 connected ipsecif 1	F220のLANネットワークへのTunnel（IPsec）経路を登録
3	ip route 192.168.1.0 255.255.255.0 connected null 0 150	IPsecインターフェースがダウンしたときに、F220のLANネットワーク宛の通信が平文で出力されないための設定 #set security-association always-up設定により、SAの有無に連動してIPsecインタフェースがアップ、ダウンする
4	!	
5	access-list 99 permit 192.168.0.0 0.0.0.255	
6	!	
7	vpn enable	
8	vpnlog enable	
9	!	
10	ipsec access-list 1 ipsec ip any any	
11	ipsec access-list 64 bypass ip any any	
12	ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac	
13	!	
14	interface ipsecif 1	
15	crypto map CENTER	
16	exit	
17	interface lan 1	
18	ip address 192.168.0.254 255.255.255.0	
19	exit	
20	interface pppoe 1	
21	ip nat inside source list 99 interface	
22	pppoe server FLETS-ADSL	
23	pppoe account abc345@***.***.ne.jp zzzyyyxxx	
24	pppoe type host	
25	exit	
26	!	
27	crypto isakmp policy 1	
28	authentication prekey	
29	encryption aes 256	
30	group 14	
31	hash sha	
32	idtype-pre userfqdn	
33	key ascii SECRET-VPN	
34	lifetime 86400	
35	my-identity id-kyoten	
36	negotiation-mode aggressive	
37	peer-identity address 192.0.2.1	
38	exit	
39	crypto map CENTER 1	
40	match address 1	
41	set peer address 192.0.2.1	
42	set pfs group14	
43	set security-association lifetime seconds 28800	
44	set security-association always-up	
45	set transform-set P2-POLICY	
46	exit	
47	!	
48	end	

F220の設定

	設定例（F220）	補足
1	access-list 100 permit udp any eq 500 192.0.2.1 0.0.0.0 eq 500	VPNで使用するパケットを受信許可するフィルタリングの設定
2	access-list 100 permit 50 any 192.0.2.1 0.0.0.0	VPNで使用するパケットを受信許可するフィルタリングの設定
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
27	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
28	!	
29	ip route 0.0.0.0 0.0.0.0 tunnel 1	
30	ip route 192.168.0.0 255.255.255.0 tunnel 2	F60のLANネットワークへのTunnel（IPsec）経路を登録
31	ip nat list 1 192.168.1.0 0.0.0.255	
32	!	
33	logging level informational	isakmpログを記録するためにログレベルを設定
34	!	
35	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
36	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
37	!	
38	username guest password guest-secret	
39	!	
40	crypto ipsec policy P2-POLICY	IPsecポリシー設定（共有設定）
41	set pfs group14	
42	set security-association lifetime seconds 28800	
43	set security-association transform-keysize aes 256 256 256	
44	set security-association transform esp-aes esp-sha-hmac	
45	set mtu 1454	
46	set ip df-bit 0	
47	set ip fragment post	
48	exit	
49	!	
50	crypto ipsec selector SELECTOR	セレクタ設定（共有設定）
51	src 1 ipv4 any	送信元セレクタを全IPv4アドレスを対象に設定
52	dst 1 ipv4 any	宛先セレクタを全IPv4アドレスを対象に設定
53	exit	
54	!	
55	crypto isakmp keepalive	
56	crypto isakmp log sa	
57	crypto isakmp log session	
58	crypto isakmp log negotiation-fail	
59	!	
60	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定（共有設定）
61	authentication pre-share	
62	encryption aes	
63	encryption-keysize aes 256 256 256	
64	group 14	
65	lifetime 86400	
66	hash sha	
67	initiate-mode aggressive	
68	exit	
69	!	
70	crypto isakmp profile PROF0001	ISAKMPプロファイル設定（対向拠点毎に設定）
71	match identity user id-kyoten	
72	local-address 192.0.2.1	
73	set isakmp-policy P1-POLICY	
74	set ipsec-policy P2-POLICY	
75	ike-version 1	
76	local-key SECRET-VPN	
77	exit	
78	!	

79	crypto map KYOTEN0001 ipsec-isakmp	CRYPTO MAP設定（対向拠点毎に設定）
80	match address SELECTOR	
81	set isakmp-profile PROF0001	
82	exit	
83	!	
84	interface GigaEthernet 1/1	
85	vlan-id 1	
86	bridge-group 1	
87	channel-group 1	
88	exit	
89	!	
90	interface GigaEthernet 2/1	
91	vlan-id 2	
92	bridge-group 2	
93	pppoe enable	
94	exit	
95	!	
96	interface Port-channel 1	
97	ip address 192.168.1.254 255.255.255.0	
98	mss 1300	
99	exit	
100	!	
101	interface Tunnel 1	
102	description FLETS	
103	ip address 192.0.2.1 255.255.255.255	
104	ip access-group 100 in	
105	ip access-group 111 out	IPv4アクセスリスト紐づけ
106	ip access-group 112 in	IPv4アクセスリスト紐づけ
107	ip access-group 113 out	IPv4アクセスリスト紐づけ
108	ip access-group 114 out	IPv4アクセスリスト紐づけ
109	ip access-group 115 in	IPv4アクセスリスト紐づけ
110	ip access-group spi ftp-data enable	学習フィルタ追加
111	ip nat inside source list 1 interface	
112	tunnel mode pppoe profile PPPOE_PROF	
113	pppoe interface gigaethernet 2/1	
114	exit	
115	!	
116	interface Tunnel 2	Tunnel（IPsec）インタフェース設定（対向拠点毎に設定）
117	tunnel mode ipsec map KYOTEN0001	
118	exit	
119	!	
120	pppoe profile PPPOE_PROF	
121	account abc012@***.***.ne.jp xxxyyyzzz	
122	exit	
123	!	
124	end	