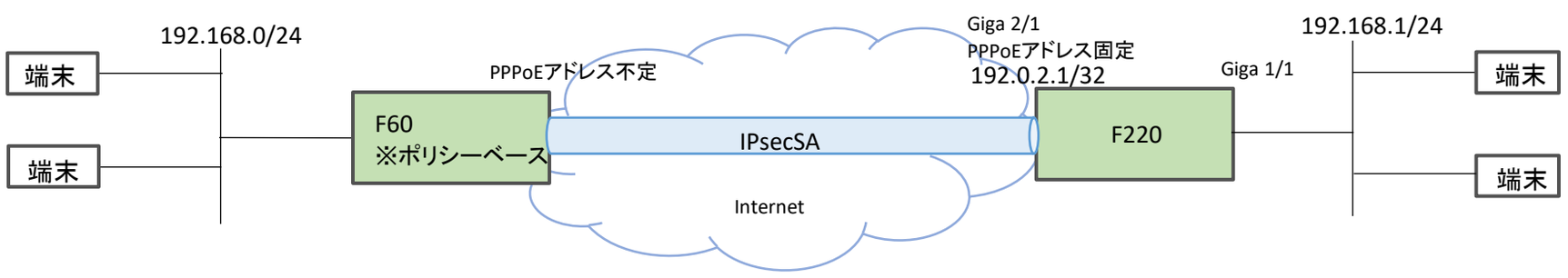
設定例

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

概要

F60をポリシーベース方式として、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)のsrc/dstアドレス設定が双方で一致していれば、SA接続および通信可能です。
・F220のIPsecセレクタ設定ではプロトコルやポート番号は指定出来ないので、F60側のIPsecセレクタ設定もアドレスのみとしてください。
・本設定例はF60-F220間で1SAを接続する場合です。F60をポリシーベース方式としてF60-F220間で複数SAを接続する場合は、F220にてポリシールーティングを併用することにより可能です。



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	!	
3	access-list 99 permit 192.168.0.0 0.0.0.255	
4	!	
5	vpn enable	
6	vpnlog enable	
7	!	
8	ipsec access-list 1 ipsec ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255	
9	ipsec access-list 64 bypass ip any any	
10	ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac	
11	!	
12	interface lan 1	
13	ip address 192.168.0.254 255.255.255.0	
14	exit	
15	interface pppoe 1	
16	crypto map CENTER	
17	ip nat inside source list 99 interface	
18	pppoe server FLETS-ADSL	
19	pppoe account abc345@***.***.ne.jp zzzyyyxxx	
20	pppoe type host	
21	exit	
22	!	
23	crypto isakmp policy 1	
24	authentication prekey	
25	encryption aes 256	
26	group 14	
27	hash sha	
28	idtype-pre userfqdn	
29	key ascii SECRET-VPN	
30	lifetime 86400	
31	my-identity id-kyoten	
32	negotiation-mode aggressive	
33	peer-identity address 192.0.2.1	
34	exit	
35	crypto map CENTER 1	
36	match address 1	
37	set peer address 192.0.2.1	
38	set pfs group14	
39	set security-association lifetime seconds 28800	
40	set security-association always-up	
41	set transform-set P2-POLICY	
42	exit	
43	!	
44	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
2	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。
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
26	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
27	!	
28	ip route 0.0.0.0 0.0.0.0 tunnel 1	
29	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
30	ip nat list 1 192.168.1.0 0.0.0.255	
31	!	
32	logging level informational	isakmpログを記録するためにログレベルを設定
33	!	
34	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
35	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
36	!	
37	username guest password guest-secret	
38	!	
39	crypto ipsec policy P2-POLICY	IPsecポリシー設定(共有設定)
40	set pfs group14	
41	set security-association lifetime seconds 28800	
42	set security-association transform-keysize aes 256 256 256	
43	set security-association transform esp-aes esp-sha-hmac	
44	set mtu 1454	
45	set ip df-bit 0	
46	set ip fragment post	
47	exit	
48	!	
49	crypto ipsec selector SELECTOR0001	セレクタ設定(対向拠点毎に設定)
50	src 1 ipv4 192.168.1.0 255.255.255.0	送信元セレクタをF220のLANネットワークを対象に設定
51	dst 1 ipv4 192.168.0.0 255.255.255.0	宛先セレクタをF60のLANネットワークを対象に設定
52	exit	
53	!	
54	crypto isakmp keepalive	
55	crypto isakmp log sa	
56	crypto isakmp log session	
57	crypto isakmp log negotiation-fail	
58	!	
59	crypto isakmp policy P1-POLICY	ISAKMPポリシー設定(共有設定)
60	authentication pre-share	
61	encryption aes	
62	encryption-keysize aes 256 256 256	
63	group 14	
64	lifetime 86400	
65	hash sha	
66	initiate-mode aggressive	
67	exit	
68	!	
69	crypto isakmp profile PROF0001	ISAKMPプロファイル設定(対向拠点毎に設定)
70	match identity user id-kyoten	
71	local-address 192.0.2.1	
72	set isakmp-policy P1-POLICY	
73	set ipsec-policy P2-POLICY	
74	ike-version 1	
75	local-key SECRET-VPN	
76	exit	
77	!	

78	crypto map KYOTEN0001 ipsec-isakmp	CRYPTO MAP設定（ 対向拠点毎に設定）
79	match address SELECTOR0001	
80	set isakmp-profile PROF0001	
81	exit	
82	!	
83	interface GigaEthernet 1/1	
84	vlan-id 1	
85	bridge-group 1	
86	channel-group 1	
87	exit	
88	!	
89	interface GigaEthernet 2/1	
90	vlan-id 2	
91	bridge-group 2	
92	pppoe enable	
93	exit	
94	!	
95	interface Port-channel 1	
96	ip address 192.168.1.254 255.255.255.0	
97	mss 1300	
98	exit	
99	!	
100	interface Tunnel 1	
101	description FLETS	
102	ip address 192.0.2.1 255.255.255.255	
103	ip access-group 100 in	
104	ip access-group 111 out	IPv4アクセスリスト紐づけ
105	ip access-group 112 in	IPv4アクセスリスト紐づけ
106	ip access-group 113 out	IPv4アクセスリスト紐づけ
107	ip access-group 114 out	IPv4アクセスリスト紐づけ
108	ip access-group 115 in	IPv4アクセスリスト紐づけ
109	ip access-group spi ftp-data enable	学習フィルタ追加
110	ip nat inside source list 1 interface	
111	tunnel mode pppoe profile PPPOE_PROF0001	
112	pppoe interface gigaethernet 2/1	
113	exit	
114	!	
115	interface Tunnel 2	Tunnel（ IPsec）インタフェース設定（ 対向拠点毎に設定）
116	tunnel mode ipsec map KYOTEN0001	
117	exit	
118	!	
119	pppoe profile PPPOE_PROF	
120	account abc012@***.***.ne.jp xxxyyyzzz	
121	exit	
122	!	
123	end	