Amazon Virtual Private Cloud (Amazon VPC) とVPN接続する:FITELnet設定例

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

	設定例	補足
1	access-list 100 permit udp host ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## eq 500 any 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 ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## : ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## : VPCの設定(aws_console_vpc.pdf)の手順10でダウンロードした ファイルにてご確認ください
2	access-list 100 permit udp host ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## eq 500 any eq 500	
3	access-list 100 permit 50 host ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## any	
4	access-list 100 permit 50 host ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## any	
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	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。
25	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。
26	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。
27	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。
28	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
29	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
30	!	
31	ip route 0.0.0.0 0.0.0.0 tunnel 3	デフォルト経路(PPPoE経由)
32	ip nat list 1 192.168.100.0 0.0.0.255	Internet向けNAT設定
33	!	
34	crypto ipsec policy IPSECPOL_001	IPsecポリシー設定(Tunnel#1)
35	set pfs group14	
36	set security-association always-up	
37	set security-association rekey always	
38	set security-association lifetime seconds 3600	
39	set security-association transform-keysize aes 256 256 256	
40	set security-association transform esp-aes esp-sha256-hmac	
41	set mtu 1454	OuterのMTU長:PPPoEのMTUに合わせて1454を設定
42	exit	
43	!	
44	crypto ipsec policy IPSECPOL_002	IPsecポリシー設定(Tunnel#2)
45	set pfs group14	
46	set security-association always-up	
47	set security-association rekey always	
48	set security-association lifetime seconds 3600	
49	set security-association transform-keysize aes 256 256 256	
50	set security-association transform esp-aes esp-sha256-hmac	
51	set mtu 1454	OuterのMTU長:PPPoEのMTUに合わせて1454を設定
52	exit	
53	!	
54	crypto ipsec selector SELECTOR_1	VPNセレクタ設定(Tunnel#1,#2)
55	src 1 ipv4 any	
56	dst 1 ipv4 any	
57	exit	
58	!	

	設定例	補足
59	crypto isakmp log sa	crypto isakmp log コマンドで、VPNの詳細なログ情報を残すようにしてください。
60	crypto isakmp log session	
61	crypto isakmp log negotiation-fail	
62	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time 0	
63	crypto isakmp negotiation always-up-params interval 1000 max-initiate 10 max-pending 10 delay 1	
64	!	
65	crypto isakmp policy ISAPOL_001	ISAKMPポリシー設定（Tunnel#1）
66	authentication pre-share	
67	encryption aes	
68	encryption-keysize aes 256 256 256	
69	group 14	
70	lifetime 28800	
71	hash sha-256	
72	initiate-mode main	
73	exit	
74	!	
75	crypto isakmp policy ISAPOL_002	ISAKMPポリシー設定（Tunnel#2）
76	authentication pre-share	
77	encryption aes	
78	encryption-keysize aes 256 256 256	
79	group 14	
80	lifetime 28800	
81	hash sha-256	
82	initiate-mode main	
83	exit	
84	!	
85	crypto isakmp profile ISAPROF_001	ISAKMPプロファイル設定（Tunnel#1） ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)## : ##Tunnel#1_Pre-Shared_Key##: VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードした ファイルにてご確認ください
86	match identity address ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)##	
87	keepalive interval 10	
88	set isakmp-policy ISAPOL_001	
89	set ipsec-policy IPSECPOL_001	
90	set peer ##Tunnel#1_Outside_IP(Virtual_Private_Gateway)##	
91	ike-version 1	
92	local-key ascii ##Tunnel#1_Pre-Shared_Key##	
93	exit	
94	!	
95	crypto isakmp profile ISAPROF_002	ISAKMPプロファイル設定（Tunnel#2） ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)## : ##Tunnel#2_Pre-Shared_Key##: VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードした ファイルにてご確認ください
96	match identity address ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)##	
97	keepalive interval 10	
98	set isakmp-policy ISAPOL_002	
99	set ipsec-policy IPSECPOL_002	
100	set peer ##Tunnel#2_Outside_IP(Virtual_Private_Gateway)##	
101	ike-version 1	
102	local-key ascii ##Tunnel#2_Pre-Shared_Key##	
103	exit	
104	!	
105	crypto map MAP1 ipsec-isakmp	VPNピアとのセレクタ情報のエントリの設定（Tunnel#1）
106	match address SELECTOR_1	
107	set isakmp-profile ISAPROF_001	
108	exit	
109	!	
110	crypto map MAP2 ipsec-isakmp	VPNピアとのセレクタ情報のエントリの設定（Tunnel#2）
111	match address SELECTOR_1	
112	set isakmp-profile ISAPROF_002	
113	exit	
114	!	
115	logging buffer level informational	logging level設定：informationalを設定してください
116	!	
117	aaa authentication login default local	
118	aaa authorization exec default local	
119	!	
120	username guest password guest-secret	
121	!	
122	hostname FITELnet	
123	!	
124	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
125	vlan-id 1	
126	bridge-group 1	
127	channel-group 1	
128	exit	
129	!	
130	interface GigaEthernet 2/1	GigaEthernet 2/1 にてPPPoEを有効にする
131	vlan-id 2	
132	bridge-group 2	
133	pppoe enable	
134	exit	
135	!	
136	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
137	ip address 192.168.100.1 255.255.255.0	
138	mss 1350	
139	exit	
140	!	
141	interface Tunnel 1	トンネルインタフェース設定（VPN：Tunnel#1）
142	ip address ##Tunnel#1_Inside IP(Customer_Gateway)##	
143	tunnel mode ipsec map MAP1	
144	link-state sync-sa	
145	exit	
146	!	

	設定例	補足
147	interface Tunnel 2	トンネルインタフェース設定（VPN：Tunnel#2）
148	ip address ##Tunnel#2_Inside_IP(Customer_Gateway)##	
149	tunnel mode ipsec map MAP2	
150	link-state sync-sa	
151	exit	
152	!	
153	interface Tunnel 3	トンネルインタフェース設定（PPPoE）
154	ip access-group 100 in	
155	ip access-group 111 out	
156	ip access-group 112 in	
157	ip access-group 113 out	
158	ip access-group 114 out	
159	ip access-group 115 in	
160	ip access-group spi ftp-data enable	
161	ip nat inside source list 1 interface	
162	tunnel mode pppoe profile PPPOE_PROF0001	
163	pppoe interface gigaethernet 2/1	GigaEthernet 2/1にリンク付け
164	exit	
165	!	
166	router bgp 65000	
167	bgp router-id 192.168.100.1	BGP設定 Amazon VPCの経路情報（10.0/16）を受信、かつ拠点LANの経路情報（192.168.100/24）を広告するためにBGPを使用します。 bgp log-neighbor-changes コマンドを設定してBGPのログ情報を残すようにしてください。 ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)##： ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)##： VPCの設定（aws_console_vpc.pdf）の手順10でダウンロードしたファイルにてご確認ください network コマンドで拠点LANの経路情報を設定します。
168	bgp log-neighbor-changes	
169	neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## remote-as 64512	
170	neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## timers 10 30	
171	neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## remote-as 64512	
172	neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## timers 10 30	
173	!	
174	address-family ipv4 unicast	
175	neighbor ##Tunnel#1_Inside_IP(Virtual_Private_Gateway)## activate	
176	neighbor ##Tunnel#2_Inside_IP(Virtual_Private_Gateway)## activate	
177	network 192.168.100.0 255.255.255.0	
178	exit	
179	!	
180	exit	
181	!	
182	pppoe profile PPPOE_PROF0001	PPPoEプロファイル設定
183	account user@xxxx.ne.jp secret	
184	exit	
185	!	
186	end	