Microsoft Azure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 ##VPN-PublicIP## 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 ##VPN-PublicIP##:Microsoft Azure手順書②「パブリックIPアドレスとゲートウェイの作成」手順11にてご確認ください
2	access-list 100 permit 50 host ##VPN-PublicIP## any	
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 3	デフォルト経路(PPPoE経由)
30	ip route 10.0.0.0 255.255.0.0 tunnel 1	
31	ip nat list 1 any	Internet向けNAT設定
32	!	
33	crypto ipsec policy IPSECPOL_001	IPsecポリシー設定
34	set security-association always-up	
35	set security-association rekey always	
36	set security-association lifetime seconds 3600	
37	set security-association transform-keysize aes 256 256 256	
38	set security-association transform esp-aes esp-sha256-hmac	
39	set mtu 1454	OuterのMTU長:PPPoEのMTUに合わせて1454を設定
40	exit	
41	!	
42	crypto ipsec selector SELECTOR_1	VPNセレクタ設定
43	src 1 ipv4 any	
44	dst 1 ipv4 any	
45	exit	
46	!	
47	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。
48	crypto isakmp log session	
49	crypto isakmp log negotiation-fail	
50	crypto isakmp negotiation retry timer 10 limit 3 timer-max 30 guard-time 0	
51	crypto isakmp negotiation always-up-params interval 1000 max-initiate 10 max-pending 10 delay 1	
52	!	
53	crypto isakmp policy ISAPOL_001	ISAKMPポリシー設定
54	authentication pre-share	
55	encryption aes	
56	encryption-keysize aes 256 256 256	
57	group 2	
58	lifetime 28800	
59	hash sha-256	
60	initiate-mode main	
61	exit	

	設定例	補足
62	!	
63	crypto isakmp profile ISAPROF_001	ISAKMPプロファイル設定 ##VPN-PublicIP## : Microsoft Azure手順書②「パブリックIPアドレスとゲートウェイの作成」手順11にてご確認ください ##Pre-Shared_Key## : Microsoft Azure手順書②「パブリックIPアドレスとゲートウェイの作成」手順18で設定したPSKをご使用ください
64	match identity address ##VPN-PublicIP##	
65	keepalive interval 10	
66	set isakmp-policy ISAPOL_001	
67	set ipsec-policy IPSECPOL_001	
68	set peer ##VPN-PublicIP##	
69	ike-version 1	
70	local-key ascii ##Pre-Shared_Key##	
71	exit	
72	!	
73	crypto map MAP1 ipsec-isakmp	VPNピアとのセレクタ情報のエントリを設定
74	match address SELECTOR_1	
75	set isakmp-profile ISAPROF_001	
76	exit	
77	!	
78	logging buffer level informational	logging level設定：informationalを設定してください
79	!	
80	aaa authentication login default local	
81	aaa authorization exec default local	
82	!	
83	username guest password guest-secret	
84	!	
85	hostname FITELnet	
86	!	
87	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
88	vlan-id 1	
89	bridge-group 1	
90	channel-group 1	
91	exit	
92	!	
93	interface GigaEthernet 2/1	GigaEthernet 2/1 にてPPPoEを有効にする
94	vlan-id 2	
95	bridge-group 2	
96	pppoe enable	
97	exit	
98	!	
99	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
100	ip address 192.168.1.1 255.255.255.0	
101	mss 1350	
102	exit	
103	!	
104	interface Tunnel 1	トンネルインタフェース設定（VPN）
105	tunnel mode ipsec map MAP1	
106	link-state sync-sa	
107	exit	
108	!	
109	interface Tunnel 3	トンネルインタフェース設定（PPPoE）
110	ip address ##furukawa-GW## 255.255.255.255	
111	ip access-group 100 in	
112	ip access-group 111 out	
113	ip access-group 112 in	
114	ip access-group 113 out	
115	ip access-group 114 out	
116	ip access-group 115 in	
117	ip access-group spi ftp-data enable	
118	ip nat inside source list 1 interface	
119	tunnel mode pppoe profile PPPOE_PROF0001	
120	pppoe interface gigaethernet 2/1	GigaEthernet 2/1にリンク付け
121	exit	
122	!	
123	pppoe profile PPPOE_PROF0001	PPPoEプロファイル設定
124	account user@xxxx.ne.jp secret	
125	exit	
126	!	
127	end	