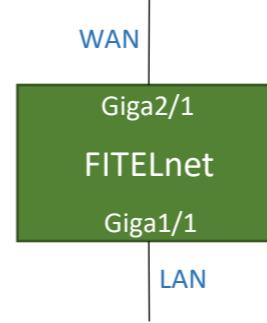


ピッグロープ社「IPv6オプション」を利用するための設定例

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

ケース2：HGWなし/ひかり電話なし



※ログインID/Passwordは“test”/“test”です。

	設定例	補足
1	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。
2	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。
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。
20	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。
21	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。
22	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。
23	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。
24	access-list 114 permit ip any any	全てのIPトラフィックを許可します。
25	access-list 115 deny ip any any	全てのIPトラフィックを拒否します。
26	access-list 4000 permit icmp6 any any neighbor-advertisement	IPv6アクセリスト (NA許可)
27	access-list 4000 permit icmp6 any any neighbor-solicitation	IPv6アクセリスト (NS許可)
28	access-list 4000 permit icmp6 any any router-advertisement	IPv6アクセリスト (RA許可)
29	access-list 4000 permit udp any any eq 546	IPv6アクセリスト (DHCPv6許可)
30	access-list 4009 deny ipv6 any any	IPv6アクセリスト (全拒否)
31	access-list 4010 spi ipv6 any any	IPv6アクセリスト (SPI)
32	access-list 4100 permit tcp any any eq 53	IPv6アクセリスト (IPv6 TCP DNS/ポリシールーティング用)
33	access-list 4100 permit udp any any eq 53	IPv6アクセリスト (IPv6 UDP DNS/ポリシールーティング用)
34	access-list 4101 permit tcp any ::1/128	IPv6アクセリスト (IPv6 TCP loopback/ポリシールーティング用)
35	access-list 4101 permit udp any ::1/128	IPv6アクセリスト (IPv6 UDP loopback/ポリシールーティング用)
36	!	
37	ip route 0.0.0.0 0.0.0.0 tunnel 1	IPv4デフォルトルート設定 (デフォルトルートをMAPトンネルに設定)
38	ip name-server ::1	DNSサーバ設定 (自装置をサーバに設定)
39	!	
40	ip dhcp server-profile DHCPv4_server	LAN側DHCPv4サーバ設定
41	address 192.168.100.2 192.168.100.254	配布アドレス設定
42	lease-time 259200	DHCPリース期間設定
43	dns 192.168.100.1	配布DNSサーバアドレス設定
44	gateway 192.168.100.1	配布Gatewayアドレス設定
45	exit	
46	!	
47	ip nat list 1 192.168.100.0 0.0.0.255	NAT変換対象アドレス設定 (LAN側 192.168.100.0/24)
48	ip nat wellknown 1 1 65535 off	NAT+変換にて全ポート番号を変換対象とする設定
49	ip nat port-sharing enable	NATポートシェアリング設定 (宛先アドレス/ポートの異なる複数のトラフィックに対して同一のNATエントリを適用して、NATのリソースを節約します。)
50	!	
51	ipv6 dhcp client-profile DHCPv6_client	WAN側DHCPv6クライアント設定
52	option-request dns-server	DNSサーバ要求設定
53	option-request dns-server-domain	DNSサーバドメイン要求設定
54	option-request sntp-server	SNTPサーバ要求設定
55	retries infinity	DHCPメッセージの応答があるまで再送する設定
56	exit	
57	!	
58	ipv6 dhcp server-profile DHCPv6_server	LAN側DHCPv6サーバ設定
59	dns port-channel 2	WAN側で受信したDNSサーバを配布する設定
60	domain port-channel 2	WAN側で受信したドメイン名を配布する設定
61	exit	
62	!	

	設定例	補足
63	ipinip tunnel-profile MAPCE	MAPトンネルプロファイル
64	profile-mode map-encap option-b	トンネルのプロファイルモードを指定
65	map rule-get	MAPルール取得設定
66	ipinip fragment pre	プリフラグメント指定
67	exit	
68	!	
69	logging buffer level informational	装置内部バッファへ出力するログレベルを設定 ※show logging bufferで確認出来ます。
70	!	
71	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ID/パスワードで認証 ※お客様の環境に合わせて設定ください。
72	aaa authorization exec default local	SSH/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 ※お客様の環境に合わせて設定ください。
73	!	
74	sntp server dhcp port-channel 2	NTPサーバもしくはSNTPサーバを指定 ※お客様の環境に合わせて設定してください。本設定例ではDHCPで取得した SNTPサーバを指定しています。 NTPサーバ指定の場合は ntp server コマンドを設定ください。
75	!	
76	username st privilege 15 password 2 \$1\$yg27Q4xa\$FzRzJaCNDLIPbh86A/Q9z/	装置のログインID/Password(test /test)
77	!	
78	hostname FITELnet	hostname設定
79	!	
80	interface GigaEthernet 1/1	物理インターフェース (LAN側)
81	vlan-id 1	vlan-id設定 (ポートVLAN)
82	bridge-group 1	ブリッジグループ設定
83	channel-group 1	LAN側論理インタフェース (Port-channel) と紐付け
84	policy-route input DNS-POLICY	LAN側ポリシールーティング設定
85	exit	
86	!	
87	interface GigaEthernet 2/1	物理インターフェース (WAN側)
88	vlan-id 2	vlan-id設定 (ポートVLAN)
89	bridge-group 2	ブリッジグループ設定
90	channel-group 2	WAN側論理インタフェース (Port-channel) と紐付け
91	ipv6 access-group 4000 in	IPv6アクセリスト紐付け (NS/NA/RA/DHCPv6)
92	ipv6 access-group 4009 in	IPv6アクセリスト紐付け (deny)
93	ipv6 access-group 4010 out	IPv6アクセリスト紐付け (SPI)
94	ipv6 access-group spi ftp-data enable	ダイナミックフィルタリング (FTP)
95	exit	
96	!	
97	interface Port-channel 1	論理インターフェース (LAN側)
98	ip dhcp service server	DHCPv4サーバ設定
99	ip dhcp server-profile DHCPv4_server	DHCPv4サーバプロファイル紐付け
100	ip address 192.168.100.1 255.255.255.0	IPv4アドレス設定
101	ipv6 enable	IPv6リンクローカルアドレス設定
102	ipv6 address autoconfig	IPv6アドレス設定 (RAからアドレス生成)
103	ipv6 address autoconfig-map-encap MAPCE	IPv6アドレス設定 (RAからMAP-E用アドレス生成)
104	ipv6 nd other-config-flag	RA 0フラグセット
105	ipv6 nd send-ra	RA送信設定
106	ipv6 trust-ra-prefix-lifetime	RAで通知されたprefix valid lifetimeをそのままアドレスのlifetimeに反映する設定 * RA送信側でプレフィックスの削除(lifetime=0)が行われた場合に、端末側に即時反映させるための設定です。デフォルトでは、サービス否認攻撃回避のため、2時間よりも短い値はlifetimeに反映しません。端末側のプレフィックス残留により通信ができないくなるケースを回避するために、本設定を推奨します。 ※本設定はLAN側/WAN側の両方の論理インタフェースにて必要です。
107	ipv6 dhcp service server	DHCPv6サーバ設定
108	ipv6 dhcp server-profile DHCPv6_server	DHCPv6サーバプロファイル紐付け
109	link-state always-up	本論理インタフェースを常にリンクアップさせる設定 * 装置起動時にリンクダウンしているとMAPルール取得に失敗するため、本設定を推奨します。
110	mss 1420	MSS設定 (1420byte : MAPトンネルから送信するIPv4overIPv6パケットのinner最大長に合わせた値です。)
111	exit	
112	!	
113	interface Port-channel 2	論理インターフェース (WAN側)
114	ipv6 enable	IPv6リンクローカルアドレス設定
115	ipv6 nd receive-ra prefix-delegation port-channel 1	RA-proxy設定
116	ipv6 router-lifetime-receive-enable	RA default経路登録設定
117	ipv6 trust-ra-prefix-lifetime	RAで通知されたprefix valid lifetimeをそのままアドレスのlifetimeに反映する設定 * 論理インタフェース (LAN側) の補足欄に記載の通り、本設定を推奨します。 ※本設定はLAN側/WAN側の両方の論理インタフェースにて必要です。
118	ipv6 dhcp service client	DHCPv6クライアント設定
119	ipv6 dhcp client-profile DHCPv6_client	DHCPv6クライアントプロファイル紐付け
120	exit	

	設定例	補足
121	!	
122	interface Tunnel 1	MAPトンネルインターフェース
123	ip access-group 111 out	IPv4アクセリスト紐づけ
124	ip access-group 112 in	IPv4アクセリスト紐づけ
125	ip access-group 113 out	IPv4アクセリスト紐づけ
126	ip access-group 114 out	IPv4アクセリスト紐づけ
127	ip access-group 115 in	IPv4アクセリスト紐づけ
128	ip access-group spi ftp-data enable	学習フィルタ追加
129	ip access-group spi ftp-data enable	ダイナミックフィルタリング(FTP)
130	ip nat inside source list 1 map-encap overload	MAP用NAT+設定
131	tunnel mode ipinip tunnel-profile MAPCE	MAP用プロファイルと紐付け
132	exit	
133	!	
134	line console	Consoleアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。
135	exec-timeout 0	自動ログアウト時間(分) * "0"指定時は自動ログアウトしません。
136	authorization exec default local	Console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
137	exit	
138	!	
139	line telnet	SSH/TELNETアクセス設定 ※本設定モードは、お客様の環境に合わせて設定ください。
140	exec-timeout 0	自動ログアウト時間(分) * "0"指定時は自動ログアウトしません。
141	exit	
142	!	
143	class-map DNS6	ポリシールーティング用class-map
144	match ipv6 access-group 4100	IPv6アクセリスト紐付け(宛先ポート番号53:DNSサーバ宛)
145	exit	
146	!	
147	class-map DNS6_L0	ポリシールーティング用class-map
148	match ipv6 access-group 4101	IPv6アクセリスト紐付け(宛先アドレス[::1/128]:自装置のloopback宛)
149	exit	
150	!	
151	policy-route-map DNS-POLICY	ポリシールーティング用のポリシー設定
152	!	
153	class DNS6	ポリシールーティング用のクラス設定(IPv6 DNSアクセス)
154	search-sequence 10	クラスの検索優先度を10に設定(DNS6_L0より検索優先度が低い)
155	count	クラスにマッチしたパケット数をカウントする設定
156	action nexthop 2001:db8::1	クラスにマッチしたパケットのnexthopを設定(2001:db8::1): ★IPv6 Documentation Prefixの範囲(2001:db8::/32)のアドレスを指定してください。 ※HGWでproxyDNSが動作している場合など、DNSサーバアドレスがRAで受信したプレフィックスに包含されるような場合に、本装置が送信するDNSサーバ宛パケットがLAN方向に送信されて、名前解決が行われなくなることを防ぐための設定です。このため、IPv6デフォルトルートに包含されるアドレスを指定する必要があります。
157	exit	
158	!	
159	class DNS6_L0	ポリシールーティング用のクラス設定(IPv6 loopbackアクセス)
160	search-sequence 1	クラスの検索優先度を1に設定(DNS6より検索優先度が高い)
161	count	クラスにマッチしたパケット数をカウントする設定
162	action transmit	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
163	exit	
164	!	
165	exit	
166	!	
167	local policy-route DNS-POLICY	自発パケットのポリシールーティング設定
168	!	
169	dns-server ip enable	DNSv4サーバ設定
170	dns-server ipv6 enable	DNSv6サーバ設定
171	!	
172	proxydns domain 1 any * any dhcp ipv6 port-channel 2	proxyDNS 順引き設定(IPv6 DNS / any)
173	proxydns address 1 any dhcp ipv6 port-channel 2	proxyDNS 逆引き設定(IPv6 DNS / any)
174	!	
175	end	