設定例

ローカルブレイクアウト（LBO）：Windows Update / Microsoft Update
対象装置：FITELnet F70/F71/F220/F221

概要

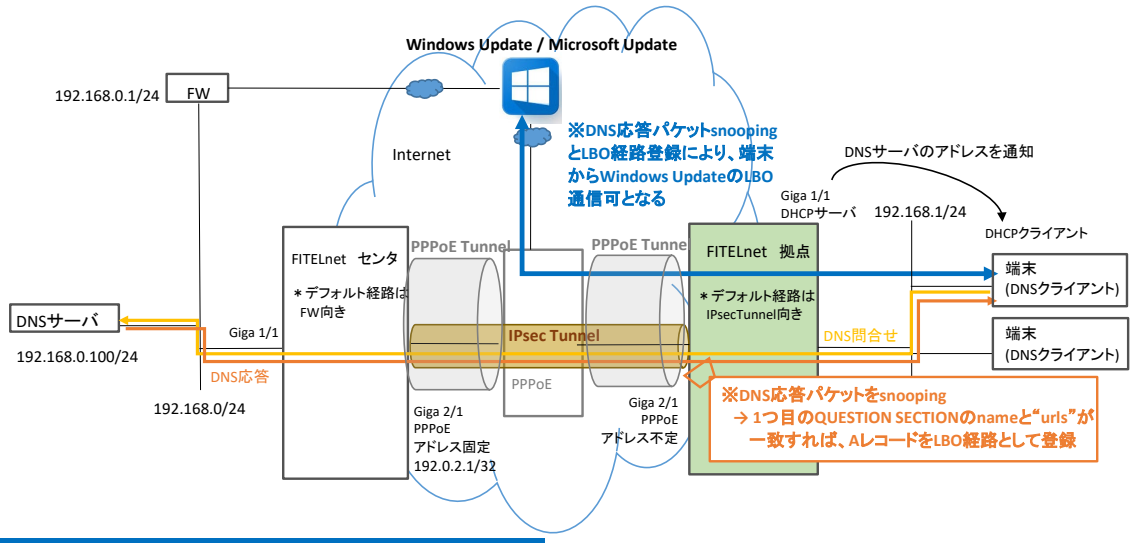
Windows Update / Microsoft Update のDNS応答パケットをsnoopingしLBO経路として登録して、LBO通信を行うための設定例です。
下記※の動作により、端末からWindows Update / Microsoft Update 通信へのLBO通信が可能となります。

※端末が通信開始しようとしてDNSサーバへアドレスを問い合わせた際に、拠点はDNSサーバが端末宛に送信したDNS応答パケットをsnoopingします。
DNS応答パケットに書かれた1つ目のQUESTION SECTIONのnameが、lbo-profile内のdomain設定と一致すれば、拠点はnameに対応するAレコード（IPv6の場合はAAAAレコード）をLBO経路として登録します。

DNS応答パケットにより登録されたLBO経路は、dns-snooping expire設定時間（デフォルト86,400秒）保持、
DNS応答パケットのANSWER SECTIONに記載のTTL時間がdns-snooping expire以上であれば、TTL時間満了まで保持します。
（上記タイマ動作は、F70/F71：V01.02以降、F220/F221：V01.04以降の動作となります）
ただし、lbo-profile内のdomain設定削除等でLBO対象ドメインで無くなった場合には削除します。

下記説明資料の6ページを合わせてご確認ください。
ローカルブレイクアウト説明資料

下記設定例の、Microsoft365のエンドポイント情報を使ったLBOを併用する際には、拠点側FITELnetがDNSサーバに問い合わせを行うための
「ip name-server」設定と、「o365 enable」設定を追加してください。
ローカルブレイクアウト：Microsoft365（旧Office365）エンドポイント情報を使う



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-256
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-256
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

センタ側FITELnetの設定

	設定例	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 ip any any	学習フィルタリングの設定
4	access-list 121 spi ip any any	学習フィルタリングの設定
5	!	
6	ip route 0.0.0.0 0.0.0.0 192.168.0.1	Default経路(FW経由)
7	ip route 192.168.1.0 255.255.255.0 tunnel 2	拠点LAN宛てStatic経路(IPsec Tunnel経由)
8	ip route 192.168.1.0 255.255.255.0 null 0 250	IPsec Tunnelダウン時に拠点LAN宛てパケットを破棄する設定
9	!	
10	hostname CENTER	
11	!	
12	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
13	set pfs group14	
14	set security-association lifetime seconds 28800	
15	set security-association transform-keysize aes 256 256 256	
16	set security-association transform esp-aes esp-sha256-hmac	
17	set mtu 1454	
18	set ip df-bit 0	
19	set ip fragment post	
20	exit	

	設定例	補足
21	!	
22	crypto ipsec selector SELECTOR	VPNセレクタの設定
23	src 1 ipv4 any	
24	dst 1 ipv4 any	
25	exit	
26	!	
27	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
28	logging level informational	VPN通信動作中の詳細なログを残す設定
29	crypto isakmp log sa	
30	crypto isakmp log session	
31	crypto isakmp log negotiation-fail	
32	crypto isakmp tunnel-route ip interface tunnel 1	VPNピアへの経路情報をTunnel 1向けに登録する設定(トンネルルート機能)
33	!	
34	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
35	authentication pre-share	
36	encryption aes	
37	encryption-keysize aes 256 256 256	
38	group 14	
39	lifetime 86400	
40	hash sha-256	
41	initiate-mode aggressive	
42	exit	
43	!	
44	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
45	match identity user id-kyoten	
46	local-address 192.0.2.1	
47	set isakmp-policy P1-POLICY	
48	set ipsec-policy P2-POLICY	
49	ike-version 1	
50	local-key SECRET-VPN	
51	exit	
52	!	
53	crypto map KYOTEN ipsec-isakmp	拠点のVPNピアとのセレクタ情報のエントリー
54	match address SELECTOR	
55	set isakmp-profile PROF0001	
56	exit	
57	!	
58	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
59	vlan-id 1	
60	bridge-group 1	
61	channel-group 1	
62	exit	
63	!	
64	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
65	vlan-id 2	
66	bridge-group 2	
67	pppoe enable	
68	exit	
69	!	
70	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
71	ip address 192.168.0.254 255.255.255.0	
72	mss 1300	
73	exit	
74	!	
75	interface Tunnel 1	Tunnel インタフェース(PPPoE)の設定
76	description FLETS	
77	ip address 192.0.2.1 255.255.255.255	
78	ip access-group 100 in	
79	ip access-group 111 in	
80	ip access-group 121 out	
81	tunnel mode pppoe profile PPPOE_PROF	
82	pppoe interface gigaethernet 2/1	
83	exit	
84	!	Tunnel インタフェース(IPsec)の設定
85	interface Tunnel 2	
86	tunnel mode ipsec map KYOTEN	
87	link-state sync-sa	
88	exit	
89	!	
90	pppoe profile PPPOE_PROF	PPPoEの設定
91	account abc012@***.***.ne.jp xxxyyyzzz	
92	exit	
93	!	
94	end	

拠点側FITELnetの設定

	設定例	補足
1	access-list 100 permit udp 192.0.2.1 0.0.0.0 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
2	access-list 100 permit 50 192.0.2.1 0.0.0.0 any	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 ip any any	学習フィルタリングの設定
4	access-list 121 spi ip any any	学習フィルタリングの設定
5	!	
6	ip route 192.0.2.1 255.255.255.255 tunnel 1	センタPPPoEIFへの経路(PPPoE経由)
7	ip route 0.0.0.0 0.0.0.0 tunnel 2	Default経路(IPsec Tunnel経由)
8	ip nat list 1 192.168.1.0 0.0.0.255	NATの設定
9	!	
10	ip dhcp server-profile lan1	DHCP サーバ機能を利用する設定
11	address 192.168.1.1 192.168.1.200	配布IPアドレスの範囲
12	lease-time 28800	DHCPリース期間(秒)
13	dns 192.168.0.100	プライマリDNSサーバIPアドレス
14	gateway 192.168.1.254	デフォルトルータのIPアドレス
15	exit	
16	!	

	設定例	補足
17	crypto ipsec policy P2-POLICY	IPSECポリシーの設定
18	set pfs group14	
19	set security-association always-up	
20	set security-association lifetime seconds 28800	
21	set security-association transform-keysize aes 256 256 256	
22	set security-association transform esp-aes esp-sha256-hmac	
23	set mtu 1454	
24	set ip df-bit 0	
25	set ip fragment post	
26	exit	
27	!	
28	crypto ipsec selector SELECTOR	VPNセレクタの設定
29	src 1 ipv4 any	
30	dst 1 ipv4 any	
31	exit	
32	!	
33	crypto isakmp keepalive	KeepAlive機能として使用するDPDの設定
34	logging level informational	VPN通信動作中の詳細なログを残す設定
35	crypto isakmp log sa	
36	crypto isakmp log session	
37	crypto isakmp log negotiation-fail	
38	!	
39	hostname KYOTEN	
40	!	
41	crypto isakmp policy P1-POLICY	ISAKMP ポリシーの設定
42	authentication pre-share	
43	encryption aes	
44	encryption-keysize aes 256 256 256	
45	group 14	
46	lifetime 86400	
47	hash sha-256	
48	initiate-mode aggressive	
49	exit	
50	!	
51	crypto isakmp profile PROF0001	ISAKMPプロファイルの設定
52	self-identity user-fqdn id-kyoten	
53	set isakmp-policy P1-POLICY	
54	set ipsec-policy P2-POLICY	
55	set peer 192.0.2.1	
56	ike-version 1	
57	local-key SECRET-VPN	
58	exit	
59	!	
60	crypto map CENTER ipsec-isakmp	センタのVPNピアとのセレクタ情報のエントリー
61	match address SELECTOR	
62	set isakmp-profile PROF0001	
63	exit	
64	!	
65	interface GigaEthernet 1/1	GigaEthernet インタフェースに、port-channel をリンク付け
66	vlan-id 1	
67	bridge-group 1	
68	channel-group 1	
69	exit	
70	!	
71	interface GigaEthernet 2/1	PPPoE 通信で使用する物理インタフェースの設定
72	vlan-id 2	
73	bridge-group 2	
74	pppoe enable	
75	exit	
76	!	
77	interface Port-channel 1	Port-channel にLAN側IPアドレスを設定
78	ip address 192.168.1.254 255.255.255.0	
79	ip dhcp service server	DHCPサーバ機能を有効化
80	ip dhcp server-profile lan1	DHCPサーバ機能で使用するプロファイルの指定
81	mss 1300	
82	exit	
83	!	
84	interface Tunnel 1	Tunnel インタフェース（PPPoE）の設定
85	description FLETS	
86	ip access-group 100 in	
87	ip access-group 111 in	
88	ip access-group 121 out	
89	ip nat inside source list 1 interface	
90	tunnel mode pppoe profile PPPOE_PROF	
91	pppoe interface gigaethernet 2/1	
92	exit	
93	!	
94	interface Tunnel 2	Tunnel インタフェース（IPsec）の設定
95	tunnel mode ipsec map CENTER	
96	dns-snooping enable	dns-snooping機能を有効とする設定
97	exit	
98	!	
99	pppoe profile PPPOE_PROF	PPPoEの設定
100	account abc345@***.***.ne.jp zzzyyyxxx	
101	exit	
102	!	
103	local-breakout enable	ローカルブレイクアウトを行う設定
104	local-breakout LBO1 tunnel 1	ローカルブレイクアウト対象パケットの中継先を設定
105	!	

	設定例	補足
106	lbo-profile LBO1	LBOプロファイル設定
107	dns-snooping enable	dns-snooping機能を有効とする設定
108	dns-snooping expire 86400	dns-snooping により登録した経路の有効期限を設定
109	domain *.dl.delivery.mp.microsoft.com	ローカルブレイクアウト対象ドメインを設定
110	domain *.do.dsp.mp.microsoft.com	
111	domain *.download.microsoft.com	
112	domain *.download.windowsupdate.com	
113	domain *.emdl.ws.microsoft.com	
114	domain *.mp.microsoft.com	
115	domain *.update.microsoft.com	
116	domain *.windowsupdate.com	
117	domain download.microsoft.com	
118	domain download.windowsupdate.com	
119	domain login.live.com	
120	domain mp.microsoft.com	
121	domain ntservicepack.microsoft.com	
122	domain update.microsoft.com	
123	domain windowsupdate.com	
124	exit	
125	!	
126	end	