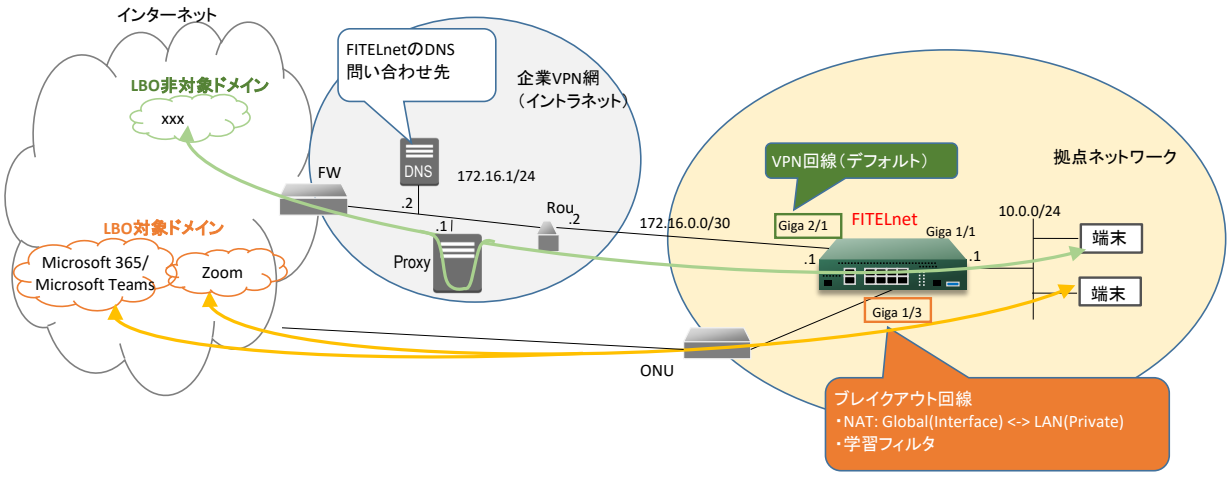
設定例

ローカルブレイクアウト（LBO）：Proxy環境下で、Microsoft 365/Microsoft Teams, Zoomを http-snoopingによりブレイクアウトする

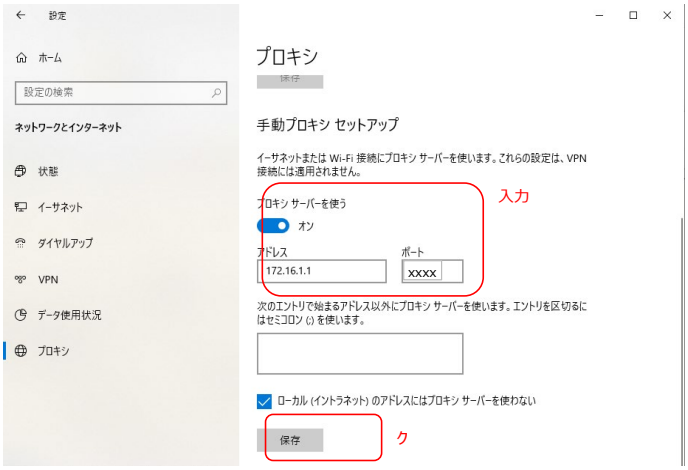
（対象機種：F70/F71/F220/F221/F225/F310/F220 EX/F221 EX）

概要

社内ネットワーク（Proxy環境下）にて、Microsoff 365/Microsoft TeamsとZoomをInternet回線にブレイクアウトするための設定例です。



・LBO非対象ドメインの通信は、デフォルト回線（Giga 2/1）からイントラネットを経由してインターネットに出力します。
・LBO対象ドメイン（Microsoft 365/Microsoft Teams, Zoom）の通信は、ブレイクアウト回線（Giga 1/3）からONUを経由してインターネットに出力します。
・拠点ネットワークの端末にて、Proxyサーバを有効にしてください（例：Windows 10の場合は、下記プロキシ設定を行ってください）。



【注意】
・本設定例にてアプリケーションの基本的な動作確認を行っておりますが、全ての動作を保証するものではございません。
アプリケーションの用途に合わせて、十分に検証を行ってから、ご利用ください。

コマンド設定例

FITELnetの設定

黄色セル：LBO機能、もしくは上記構成にてLBO機能を利用するために必要な設定です。
赤色セル：Microsoft 365/Microsoft TeamsをLBOするために必要な設定です。
青色セル：ZoomをLBOするために必要な設定です。
白色セル：LBO機能と直接関係しない設定ですが、上記構成図に対応して入れております。お使いの環境に合わせて設定ください。

	設定例	補足
1	access-list 101 permit udp any any range 3478 3481	宛先ポート番号3478-3481のUDPパケットをヒットさせるための設定 （Microsoft TeamsのLBOにて必要）
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。

	設定例	補足
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 0.0.0.0 172.16.0.2	デフォルト経路（イントラネット経由）
29	ip name-server 172.16.1.2	DNS問い合わせ先
30	ip nat list 1 any	
31	!	
32	local-breakout enable	ローカルブレイクアウトを行う設定
33	local-breakout proxy-server ip any port <ポート番号>	ローカルブレイクアウト対象のプロキシ宛通信のポート番号を設定 （設定されたポート番号を監視してLBO対象かどうかのチェックを行います）
34	local-breakout LBO_Zoom tunnel 1	ローカルブレイクアウト対象パケット（Zoom）の中継先を設定（PPPoE Tunnel）
35	local-breakout LBO_Microsoft365 tunnel 1	ローカルブレイクアウト対象パケット（Microsoft 365/Microsoft Teams）の中継先を設定（PPPoE Tunnel）
36	!	
37	lbo-profile LBO_Zoom	LBOプロファイル設定（Zoom）
38	http-snooping enable with-route	http-snooping機能を有効とする設定。with-routeオプションにより、TCP接続時に宛先アドレスを経路情報として登録して、TCP以外のLBOが可能となります。
39	domain *zoom.us	ローカルブレイクアウト対象domainを設定（Zoom）
40	exit	
41	!	
42	lbo-profile LBO_Microsoft365	LBOプロファイル設定（Microsoft 365/Microsoft Teams）
43	o365 enable	ローカルブレイクアウト対象としてMicrosoft 365/Microsoft Teamsを有効とする設定
44	http-snooping enable with-route	http-snooping機能を有効とする設定。with-routeオプションにより、TCP接続時に宛先アドレスを経路情報として登録して、TCP以外のLBOが可能となります。
45	exit	
46	!	
47	logging buffer level informational	装置内部バッファへ出力するログレベル（informational）を指定：指定したレベル名称以上（レベル番号以下）のログ情報を出力します。
48	!	
49	aaa authentication login default local	本装置にログインする□場合の認証方式を指定（username コマンドで登録したID/パスワードとする）
50	aaa authorization exec default local	本装置でコマンド実行を許可するかどうかの□許可方式を指定（username コマンドで登録した特権レベルとする）
51	!	
52	username guest password guest-secret	ログインユーザ□□名（guest）とパスワード □□guest-secret）の登録
53	!	
54	hostname FITELnet	hostname設定
55	!	
56	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
57	vlan-id 1	
58	bridge-group 1	
59	channel-group 1	
60	policy-route input PRMap_Teams	Giga 1/1から入力したパケットに　ポリシールーティング（PRMap_Teams）を適用 （Microsoft TeamsのLBOにて必要）
61	exit	
62	!	
63	interface GigaEthernet 1/3	GigaEthernet 1/3 をPPPoE回線として使用
64	vlan-id 3	
65	bridge-group 3	
66	pppoe enable	
67	exit	
68	!	
69	interface GigaEthernet 2/1	GigaEthernet 2/1 に Port-channel 2 をリンク付け
70	vlan-id 2	
71	bridge-group 2	
72	channel-group 2	
73	exit	
74	!	

	設定例	補足
75	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
76	ip address 10.0.0.1 255.255.255.0	
77	http-snooping enable	http-snoopingを行うための設定
78	mss 1300	MSSを設定：LAN回線のMSSをLBO回線よりも小さい値に設定してください ※LANインタフェースのMSSの方が大きいと、TCPセッション変換テーブル作成時に整合性チェックでエラーして変換テーブルが作成されないことがあります。
79	exit	
80	!	
81	interface Port-channel 2	Port-channel 2（デフォルト回線）にデフォルトGWと接続するためのアドレスを設定
82	ip address 172.16.0.1 255.255.255.252	
83	exit	
84	!	
85	interface Tunnel 1	Tunnel 1（ブレイクアウト回線）にPPPoE接続設定
86	description FLETS	
87	ip access-group 111 out	
88	ip access-group 112 in	
89	ip access-group 113 out	
90	ip access-group 114 out	
91	ip access-group 115 in	
92	ip access-group spi ftp-data enable	
93	ip nat inside source list 1 interface	NAT+設定（送信元アドレスをTunnel 1のアドレスに変換）
94	tunnel mode pppoe profile PPPOE_PROF	
95	pppoe interface gigaethernet 1/3	
96	exit	
97	!	
98	pppoe profile PPPOE_PROF	PPPoEプロファイルの設定
99	account abc345@***.***.ne.jp zzzyyyxxx	
100	exit	
101	!	
102	Class-map CMap_101	クラスマップ設定（Microsoft TeamsのLBOにて必要）
103	match ip access-group 101	access-list 101を紐づけ
104	exit	
105	!	
106	Policy-route-map PRMap_Teams	ポリシールートマップ設定（Microsoft TeamsのLBOにて必要）
107	!	
108	class CMap_101	class-map CMap_101（access-list 101）に合致するパケットをTunnelインタフェース1に転送
109	count	
110	action nexthop tunnel 1	
111	exit	
112	!	
113	exit	
114	!	
115	end	