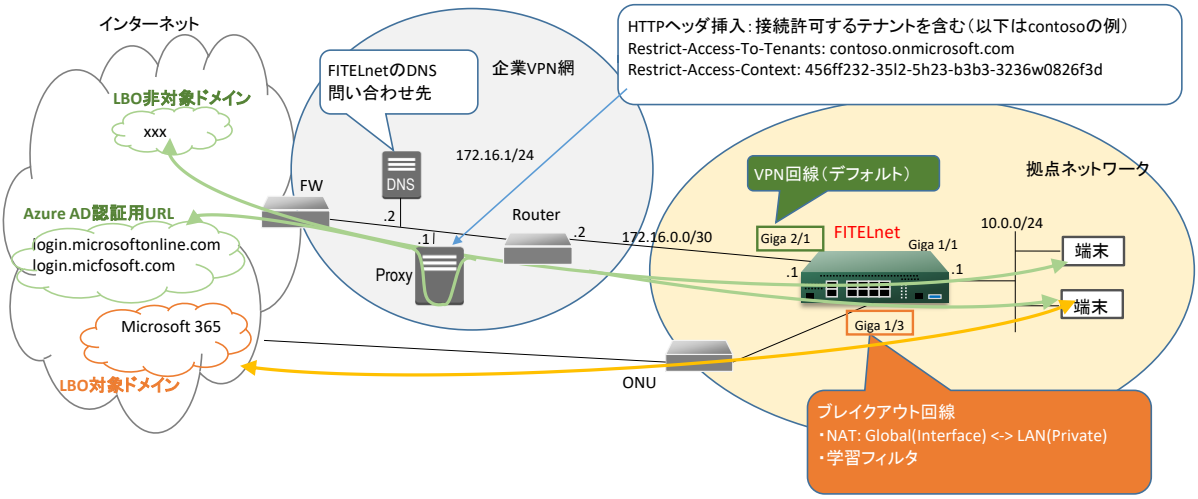
設定例

ローカルブレイクアウト（LBO）：Proxy環境下で、Microsoft 365のテナント制限とhttp-snoopingの併用

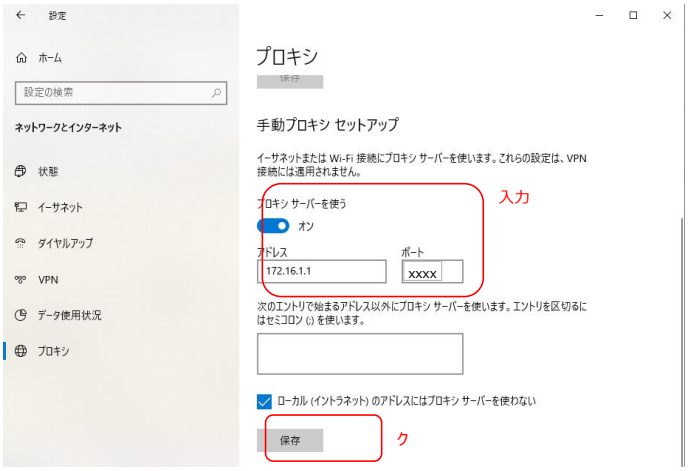
（対象機種：F70/F71/F220/F221/F220 EX/F221 EX）

概要

FITELnetでは、Proxy環境下にて、Microsoft 365のテナント制限とhttp-snoopingを併用した動作が可能です。
Microsoft 365のテナント制限については、以下のURLをご参照ください。
https://learn.microsoft.com/ja-jp/azure/active-directory/manage-apps/tenant-restrictions
FITELnetは、LBOのbypass指定を利用することで、Microsoft 365の認証用のパケットのみProxy宛に転送してテナント制限を行いながら、
Microsoft 365のLBO（http-snooping）を行うことが可能です。



・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。
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	!	
3	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）
4	ip name-server 172.16.1.2	DNS問い合わせ先
5	ip nat list 1 any	
6	!	
7	local-breakout enable	ローカルブレイクアウトを行う設定
8	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）

	設定例	補足
9	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）
10	!	
11	lbo-profile LBO_Microsoft365	LBOプロファイル設定（Microsoft 365/Microsoft Teams）
12	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
13	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。
14	domain login.microsoft.com bypass	login.microsoft.com をLBO対象外ドメインに指定
15	domain login.microsoftonline.com bypass	login.microsoftonline.com をLBO対象外ドメインに指定
16	domain login.windows.net bypass	login.windows.net をLBO対象外ドメインに指定
17	exit	
18	!	
19	logging buffer level informational	logging bufferに出力するログレベルを設定（informational） ※問題発生時の解析のため、informational設定を推奨します
20	!	
21	aaa authentication login default local	
22	aaa authorization exec default local	
23	!	
24	username test privilege 15 password 2 $1$5jqHeXmk$V1/EnzL3rI24dQdtfSTo0/	装置のログインID/Password（test/test）
25	!	
26	hostname FITELnet	
27	!	
28	sntp server ntp.nict.jp	
29	!	
30	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
31	vlan-id 1	
32	bridge-group 1	
33	channel-group 1	
34	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）
35	exit	
36	!	
37	interface GigaEthernet 1/3	GigaEthernet 1/3 をPPPoE回線として使用
38	vlan-id 3	
39	bridge-group 3	
40	pppoe enable	
41	exit	
42	!	
43	interface GigaEthernet 2/1	GigaEthernet 2/1 に Port-channel 2 をリンク付け
44	vlan-id 2	
45	bridge-group 2	
46	channel-group 2	
47	exit	
48	!	
49	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
50	ip address 10.0.0.1 255.255.255.0	
51	http-snooping enable	http-snoopingを行うための設定
52	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。
53	exit	
54	!	
55	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
56	ip address 172.16.0.1 255.255.255.252	
57	exit	
58	!	
59	interface Tunnel 1	Tunnel 1（ブレイクアウト回線）にPPPoE接続設定
60	description FLETS	
61	ip access-group default spi	学習フィルタ（SPI）を設定
62	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）
63	tunnel mode pppoe profile PPPOE_PROF	
64	pppoe interface gigaethernet 1/3	
65	exit	
66	!	
67	pppoe profile PPPOE_PROF	PPPoEプロファイルの設定
68	account abc345@***.***.ne.jp zzzyyyxxx	
69	exit	
70	!	
71	Class-map CMap_101	クラスマップ設定（Microsoft TeamsのLBOにて必要）
72	match ip access-group 101	access-list 101を紐づけ
73	exit	
74	!	
75	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）
76	!	
77	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
78	count	
79	action nexthop tunnel 1	
80	exit	
81	!	
82	exit	
83	!	
84	end	