

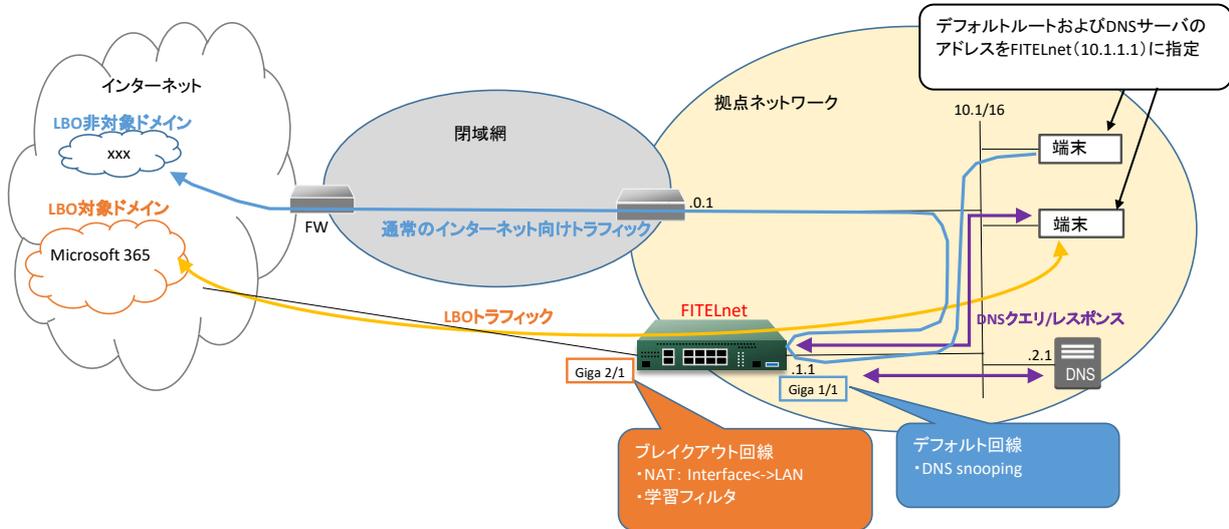
設定例

ローカルブレイクアウト(LBO): ProxyDNSを利用してMicrosoft 365をブレイクアウトする

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

概要

- 以下のような場合に、FITELnetのProxyDNS機能を利用してLBOを行うことができます。
- FITELnetが端末⇄DNSサーバ間のパケットを覗き見できない場合(LANのDNSサーバを利用する場合等)
 - FITELnetがMicrosoft 365のエンドポイント情報をブレイクアウト回線経由で取得する場合
⇒ProxyDNS-LBO連携により、FITELnet自身が名前解決したアドレスをLBO対象経路として登録することで、どちらも実現可能



【注意】

- 本設定例にてSaaS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ありません。
- SaaS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。

※ログインID/パスワードは"test"/"test"です。

	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 10.1.0.1	デフォルト経路(閉域網経由)
4	ip name-server 127.0.0.1	DNSサーバ設定 (ProxyDNS利用時は、FITELnet自身をサーバとする)
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 LBO 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 (tunnel 1)
9	!	
10	lbo-profile LBO	LBOプロファイル設定
11	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
12	dns-snooping enable	dns-snooping機能を有効とする設定
13	domain endpoints.office.com	LBO回線経由でMicrosoft 365エンドポイント情報を取得するための設定 (デフォルト回線経由で取得する場合は不要)
14	exit	
15	!	
16	logging buffer level informational	
17	!	
18	aaa authentication login default local	
19	aaa authorization exec default local	
20	!	
21	username test privilege 15 password 2 \$1\$5jqHeXmk\$V1/EnzL3r124dQdtfSto0/	装置のログインID/Password(test/test)
22	!	
23	hostname FITELnet	
24	!	
25	sntp server ntp.nict.jp	
26	!	
27	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
28	vlan-id 1	
29	bridge-group 1	
30	channel-group 1	
31	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)

	設定例	補足
32	exit	
33	!	
34	interface GigaEthernet 2/1	GigaEthernet 2/1 を PPPoE回線として使用
35	vlan-id 2	
36	bridge-group 2	
37	pppoe enable	
38	exit	
39	!	
40	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
41	ip address 10.1.1.1 255.255.0.0	
42	dns-snooping enable	Port-channel 1 で dns-snooping を行うための設定
43	link-state always-up	
44	exit	
45	!	
46	interface Tunnel 1	Tunnel 1(ブレイクアウト回線) にPPPoE接続設定
47	description FLETS	
48	ip access-group default spi	学習フィルタ(SPI)を設定
49	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)
50	tunnel mode pppoe profile PPPOE_PROF	
51	pppoe interface gigaethernet 2/1	
52	exit	
53	!	
54	pppoe profile PPPOE_PROF	PPPoEプロファイルの設定
55	account abc345@***.***.ne.jp zzzzyyxxx	
56	exit	
57	!	
58	Class-map CMap_101	クラスマップ設定(Microsoft TeamsのLBOにて必要)
59	match ip access-group 101	access-list 101を紐づけ
60	exit	
61	!	
62	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)
63	!	
64	class CMap_101	
65	count	
66	action nexthop tunnel 1	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
67	exit	
68	!	
69	exit	
70	!	
71	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化
72	!	
73	proxydns domain 1 any * any static 10.1.2.1	ProxyDNSの正引き動作条件を指定(DNSサーバ10.1.2.1をリレー先に指定)
74	proxydns address 1 any static 10.1.2.1	ProxyDNSの逆引き動作条件を指定(DNSサーバ10.1.2.1をリレー先に指定)
75	proxydns lbo enable	ProxyDNSとして受信したDNSレスポンスパケットに対するdns-snooping機能を有効化
76	!	
77	line console	
78	authorization exec default local	
79	exit	
80	!	
81	end	

