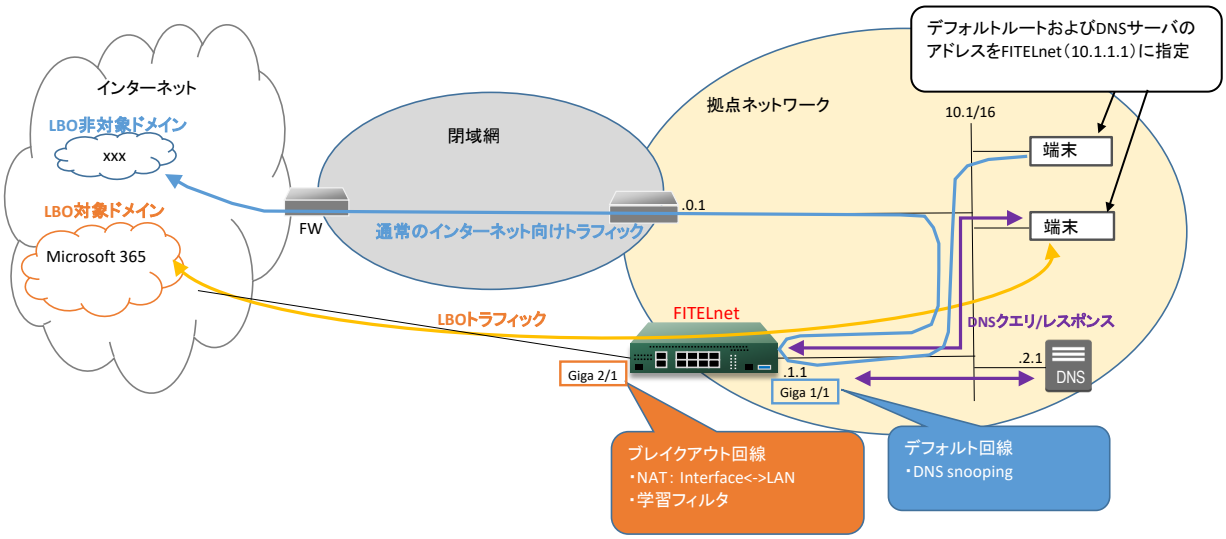
設定例

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/F225/F310/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ございません。
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IP/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	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。
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	!	

	設定例	補足
28	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）
29	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）
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 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）
34	!	
35	lbo-profile LBO	LBOプロファイル設定
36	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
37	dns-snooping enable	dns-snooping機能を有効とする設定
38	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）
39	exit	
40	!	
41	!	
42	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。
43	!	
44	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）
45	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）
46	!	
47	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
48	!	
49	hostname FITELnet	hostname設定
50	!	
51	!	
52	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
53	vlan-id 1	
54	bridge-group 1	
55	channel-group 1	
56	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）
57	exit	
58	!	
59	interface GigaEthernet 2/1	GigaEthernet 2/1 を PPPoE回線として使用
60	vlan-id 2	
61	bridge-group 2	
62	pppoe enable	
63	exit	
64	!	
65	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
66	ip address 10.1.1.1 255.255.0.0	
67	dns-snooping enable	Port-channel 1 で dns-snooping を行うための設定
68	link-state always-up	
69	exit	
70	!	
71	interface Tunnel 1	Tunnel 1（ブレイクアウト回線）にPPPoE接続設定
72	description FLETS	
73	ip access-group 111 out	
74	ip access-group 112 in	
75	ip access-group 113 out	
76	ip access-group 114 out	
77	ip access-group 115 in	
78	ip access-group spi ftp-data enable	
79	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）
80	tunnel mode pppoe profile PPPOE_PROF	
81	pppoe interface gigaethernet 2/1	
82	exit	
83	!	
84	pppoe profile PPPOE_PROF	PPPoEプロファイルの設定
85	account abc345@***.***.ne.jp zzzyyyxxx	
86	exit	
87	!	
88	Class-map CMap_101	クラスマップ設定（Microsoft TeamsのLBOにて必要）
89	match ip access-group 101	access-list 101を紐づけ
90	exit	
91	!	
92	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）
93	!	
94	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
95	count	
96	action nexthop tunnel 1	
97	exit	
98	!	
99	exit	
100	!	

	設定例	補足
101	dns-server ip enable	DNSサーバ機能およびProxyDNS機能を有効化
102	!	
103	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）
104	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）
105	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
106	!	
107	line console	
108	authorization exec default local	
109	exit	
110	!	
111	end	