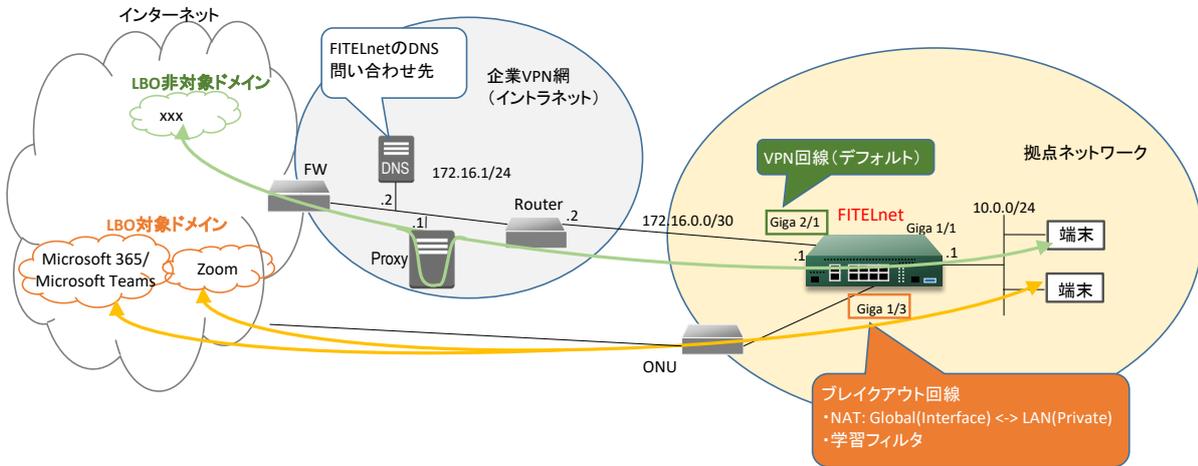


設定例

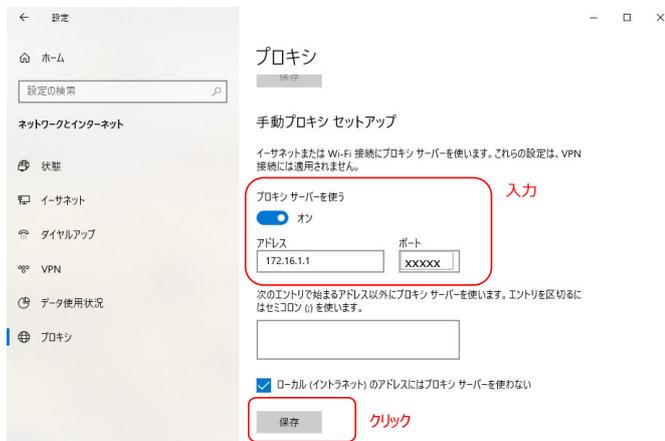
ローカルブレイクアウト(LBO): Proxy環境下で、Microsoft 365/Microsoft Teams, Zoomを http-snoopingによりブレイクアウトする (対象機種: F70/F71/F220/F221/F220 EX/F221 EX)

概要

社内ネットワーク(Proxy環境下)にて、Microsoft 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ありません。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 | ! | |
| 3 | ! | |
| 4 | 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) |
| 5 | ip name-server 172.16.1.2 | DNS問い合わせ先 |
| 6 | ip nat list 1 any | |
| 7 | ! | |
| 8 | local-breakout enable | ローカルブレイクアウトを行う設定 |
| 9 | 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) |
| 10 | 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) |
| 11 | 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) |

| | 設定例 | 補足 |
|----|--|--|
| 12 | ! | |
| 13 | lbo-profile LBO_Zoom | LBOプロファイル設定 (Zoom) |
| 14 | 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。 |
| 15 | domain *zoom.us | ローカルブレイクアウト対象domainを設定 (Zoom) |
| 16 | exit | |
| 17 | ! | |
| 18 | lbo-profile LBO_Microsoft365 | LBOプロファイル設定 (Microsoft 365/Microsoft Teams) |
| 19 | 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 |
| 20 | 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。 |
| 21 | exit | |
| 22 | ! | |
| 23 | 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 |
| 24 | ! | |
| 25 | aaa authentication login default local | |
| 26 | aaa authorization exec default local | |
| 27 | ! | |
| 28 | username test privilege 15 password 2 \$1\$5jqHeXmk\$V1/EnzL3rH24dQdtfSTo0/ | 装置のログインID/Password(test/test) |
| 29 | ! | |
| 30 | hostname FITELnet | |
| 31 | ! | |
| 32 | interface GigaEthernet 1/1 | GigaEthernet 1/1 に Port-channel 1 をリンク付け |
| 33 | vlan-id 1 | |
| 34 | bridge-group 1 | |
| 35 | channel-group 1 | |
| 36 | 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) |
| 37 | exit | |
| 38 | ! | |
| 39 | interface GigaEthernet 1/3 | GigaEthernet 1/3 をPPPoE回線として使用 |
| 40 | vlan-id 3 | |
| 41 | bridge-group 3 | |
| 42 | pppoe enable | |
| 43 | exit | |
| 44 | ! | |
| 45 | interface GigaEthernet 2/1 | GigaEthernet 2/1 に Port-channel 2 をリンク付け |
| 46 | vlan-id 2 | |
| 47 | bridge-group 2 | |
| 48 | channel-group 2 | |
| 49 | exit | |
| 50 | ! | |
| 51 | interface Port-channel 1 | Port-channel 1 にLANのアドレスを設定 |
| 52 | ip address 10.0.0.1 255.255.255.0 | |
| 53 | http-snooping enable | http-snoopingを行うための設定 |
| 54 | 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。 |
| 55 | exit | |
| 56 | ! | |
| 57 | 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 |
| 58 | ip address 172.16.0.1 255.255.255.252 | |
| 59 | exit | |
| 60 | ! | |
| 61 | interface Tunnel 1 | Tunnel 1(ブレイクアウト回線) にPPPoE接続設定 |
| 62 | description FLETS | |
| 63 | ip access-group default spi | 学習フィルタ(SPI)を設定 |
| 64 | 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) |
| 65 | tunnel mode pppoe profile PPPOE_PROF | |
| 66 | pppoe interface gigaethernet 1/3 | |
| 67 | exit | |
| 68 | ! | |
| 69 | pppoe profile PPPOE_PROF | PPPoEプロファイルの設定 |
| 70 | account abc345@***.***.ne.jp zzzzyyxxx | |
| 71 | exit | |
| 72 | ! | |
| 73 | Class-map CMap_101 | クラスマップ設定 (Microsoft TeamsのLBOにて必要) |
| 74 | match ip access-group 101 | access-list 101を紐づけ |
| 75 | exit | |
| 76 | ! | |
| 77 | 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) |
| 78 | ! | |
| 79 | class CMap_101 | |
| 80 | count | 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 |
| 81 | action nexthop tunnel 1 | |
| 82 | exit | |
| 83 | ! | |
| 84 | exit | |
| 85 | ! | |
| 86 | end | |