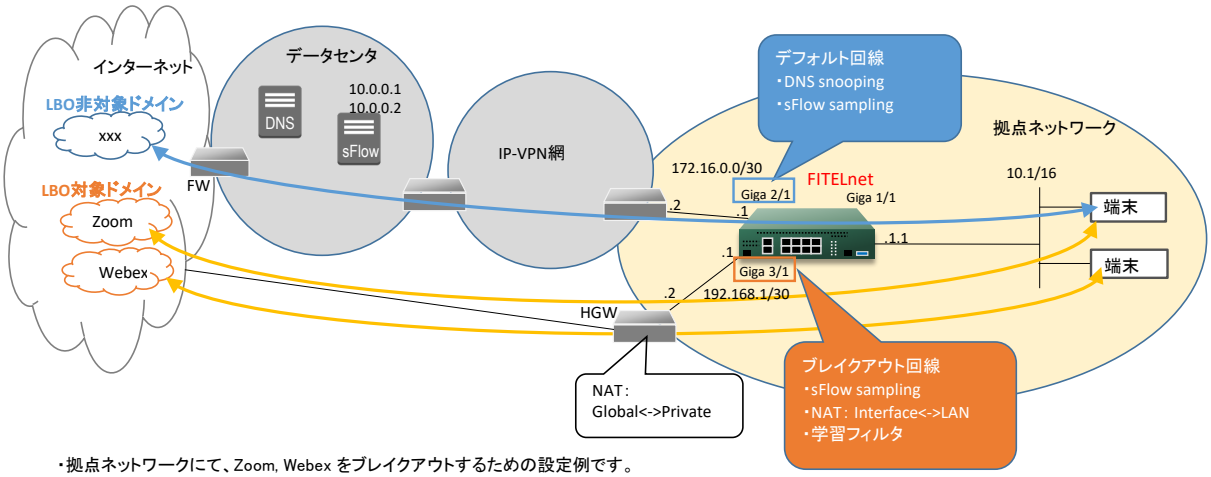
設定例

ローカルブレイクアウト（LBO）：Zoom, Webexをdns-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

LBO機能により、Zoom, Webex をブレイクアウトするためのサンプルコンフィグです。
社内の複数拠点をIP-VPN網で接続している構成にて、インターネット向けのトラフィックがデータセンタに集中して帯域圧迫するのを回避するため、
拠点ネットワークのFITELnetでLBO機能を利用します。
LBO機能の導入により、前記SaaSの通信品質の改善が見込まれます。



・拠点ネットワークにて、Zoom, Webex をブレイクアウトするための設定例です。

・LBO対象ドメイン（Zoom, Webex）の通信は、ブレイクアウト回線（Giga 3/1）からFW2を経由してインターネットに出力します。
・LBO非対象ドメインの通信は、デフォルト回線（Giga 2/1）からIP-VPN網、データセンタを経由してインターネットに出力します。

・sFlow機能を用いて、デフォルト回線とブレイクアウト回線に流れるフローのサンプリングを行います。
　sFlowデータは、デフォルト回線から出力されてsFlowコレクタ（10.0.0.1, 10.0.0.2）に送信されます。
　※sFlowによるフロー監視の使用例として設定しています。LBO機能はsFlowが無くても動作可能です。

【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
　※ログインIP/パスワードは"test"/"test"です。

	設定例	補足
1	!	
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 0.0.0.0 172.16.0.2	デフォルト経路（イントラネット経由）
29	ip nat list 1 10.1.0.0 0.0.255.255	
30	!	
31	local-breakout enable	ローカルブレイクアウトを行う設定
32	local-breakout LBO 192.168.1.2	ローカルブレイクアウト対象パケットの中継先を設定（FW2経由）
33	!	
34	lbo-profile LBO	LBOプロファイル設定
35	dns-snooping enable	dns-snooping機能を有効とする設定
36	dns-snooping expire 10800	経路有効期限を3時間に設定 （Zoomのブレイクアウト経路が直ぐに削除されるケースを回避）
37	domain *cloudfront.net	ローカルブレイクアウト対象ドメインを設定（Zoom）
38	domain *zoom.us	ローカルブレイクアウト対象ドメインを設定（Zoom）
39	domain *.wbx2.com	ローカルブレイクアウト対象ドメインを設定（Webex）
40	domain *.ciscospark.com	ローカルブレイクアウト対象ドメインを設定（Webex）
41	domain *.webexcontent.com	ローカルブレイクアウト対象ドメインを設定（Webex）
42	domain *.webex.com	ローカルブレイクアウト対象ドメインを設定（Webex）
43	domain *.identrust.com	ローカルブレイクアウト対象ドメインを設定（Webex）
44	domain *.quovadisglobal.com	ローカルブレイクアウト対象ドメインを設定（Webex）
45	domain *.digicert.com	ローカルブレイクアウト対象ドメインを設定（Webex）
46	domain *.godaddy.com	ローカルブレイクアウト対象ドメインを設定（Webex）
47	domain *.lencr.org	ローカルブレイクアウト対象ドメインを設定（Webex）
48	domain *.intel.com	ローカルブレイクアウト対象ドメインを設定（Webex）
49	domain *.accompany.com	ローカルブレイクアウト対象ドメインを設定（Webex）
50	domain *.eum-appdynamics.com	ローカルブレイクアウト対象ドメインを設定（Webex）
51	domain *.appdynamics.com	ローカルブレイクアウト対象ドメインを設定（Webex）
52	domain *.vbrickrev.com	ローカルブレイクアウト対象ドメインを設定（Webex）
53	domain *.slido.com	ローカルブレイクアウト対象ドメインを設定（Webex）
54	domain *.sli.do	ローカルブレイクアウト対象ドメインを設定（Webex）
55	domain *.data.logentries.com	ローカルブレイクアウト対象ドメインを設定（Webex）
56	domain *.cisco.com	ローカルブレイクアウト対象ドメインを設定（Webex）
57	domain *.walkme.com	ローカルブレイクアウト対象ドメインを設定（Webex）
58	domain bmmp.ciscospark.com	ローカルブレイクアウト対象ドメインを設定（Webex）
59	exit	
60	!	
61	snmp-server community public ro	
62	snmp-server enable traps snmp	
63	snmp-server host 10.0.0.3 public	
64	!	
65	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。
66	!	
67	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）
68	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）
69	!	
70	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
71	!	
72	hostname FITELnet	hostname設定
73	!	
74	sntp server 10.0.0.4 source port-channel 1	
75	sntp poll-interval 86400	
76	sntp retry limit 10 interval 64	
77	!	
78	interface GigaEthernet 1/1	GigaEthernet 1/1 に Port-channel 1 をリンク付け
79	vlan-id 1	
80	bridge-group 1	
81	channel-group 1	
82	exit	
83	!	
84	interface GigaEthernet 2/1	GigaEthernet 2/1 に Port-channel 2 をリンク付け
85	vlan-id 2	
86	bridge-group 2	
87	channel-group 2	
88	speed-duplex 100 full	speed/duplexを設定　※VPNサービスの指定等に合わせて設定ください
89	mdi mdi	MDIを設定 ※speed-duplex auto 以外では、デフォルトはMDI-X固定となります。 MDIでご使用の場合は "mdi" を設定してください
90	exit	

	設定例	補足
91	!	
92	interface GigaEthernet 3/1	GigaEthernet 3/1 に Port-channel 3 をリンク付け
93	vlan-id 3	
94	bridge-group 3	
95	channel-group 3	
96	ip access-group 111 out	
97	ip access-group 112 in	
98	ip access-group 113 out	
99	ip access-group 114 out	
100	ip access-group 115 in	
101	ip access-group spi ftp-data enable	
102	exit	
103	!	
104	interface Port-channel 1	Port-channel 1 にLANのアドレスを設定
105	ip dhcp service relay 10.0.0.5	
106	ip address 10.1.1.1 255.255.0.0	
107	link-state always-up	
108	exit	
109	!	
110	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
111	ip address 172.16.0.1 255.255.255.252	
112	dns-snooping enable	Port-channel 2 で dns-snooping を行うための設定
113	exit	
114	!	
115	interface Port-channel 3	Port-channel 3（ブレイクアウト回線）にFW2と接続するためのアドレスを設定
116	ip address 192.168.1.1 255.255.255.252	
117	ip nat inside source list 1 interface	NAT+設定（送信元アドレスをLAN側アドレスからPort-channel 3のアドレスに変換）
118	exit	
119	!	
120	line console	
121	authorization exec default local	
122	exit	
123	!	
124	sflow-agent address 172.16.0.1	sFlow Agentアドレスとして本装置のデフォルト回線のアドレスを設定
125	!	
126	sflow profile 1	sFlowプロファイルの設定
127	collector address 10.0.0.1	sFlowデータ送信先のコレクタのアドレスを設定
128	collector address 10.0.0.2	sFlowデータ送信先のコレクタのアドレスを設定
129	collector address local	sFlow統計情報を本装置に保持するための設定
130	source-interface port-channel 2	sFlowデータの送信元アドレスを設定
131	exit	
132	!	
133	sflow interface gigaethernet 2/1 sflow-profile 1 sampling-rate 100	sFlowサンプリング対象インタフェース（Giga 2/1）、プロファイル番号、サンプリングレートの設定
134	sflow interface gigaethernet 3/1 sflow-profile 1 sampling-rate 100	sFlowサンプリング対象インタフェース（Giga 3/1）、プロファイル番号、サンプリングレートの設定
135	!	
136	end	