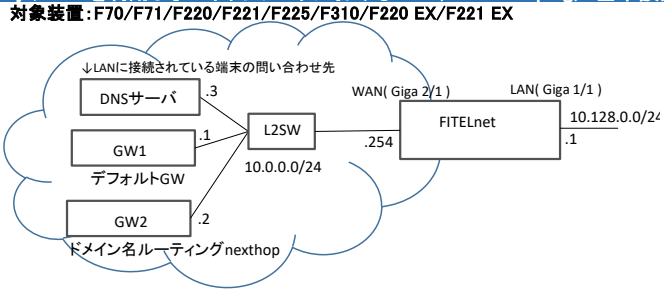
Proxyサーバを利用しないネットワークにおけるLBO(DNS snooping):基本設定

対象装置:F70/F71/F220/F221/F225/F310/F220 EX/F221 EX



	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
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	!	
28	ip route 0.0.0.0 0.0.0.0 10.0.0.1	Static経路(デフォルト経路)
29	!	
30	hardware-fault-detection action reboot	ハードウェア故障を検出した際の動作を指定(装置再起動)
31	!	
32	local-breakout enable	ローカルブレイクアウト(ドメイン名ルーティング)有効化
33	local-breakout PROF1 10.0.0.2	ドメイン名ルーティング対象パケットを中継するnexthopを指定 ※IPv4とIPv6で各1nexthopずつ設定可能
34	!	
35	lbo-profile PROF1	LBOプロファイル ※local-breakout設定で指定(指定出来るのは1プロファイルのみ)
36	dns-snooping enable	DNS ResponseのFQDNをチェックし、domain設定の内容と一致する場合にFQDNに対応するアドレスを宛先とする経路を登録します。
37	dns-snooping expire 300	dns-snoopingで登録した経路の有効期限を指定 ※DNS ResponseのTTL値が"0"の場合のみ有効になります。
38	domain *.example1.com	ドメイン名ルーティング対象となるFQDNを指定 ※"*"は任意の文字列に置き換えられます。 ※"*"のみを指定した場合、全てのFQDNが対象となります。
39	domain *.example2.com	ドメイン名ルーティング対象となるFQDNを指定 ※"*"は任意の文字列に置き換えられます。 ※"*"のみを指定した場合、全てのFQDNが対象となります。
40	exit	
41	!	
42	logging fixed-facility local7	外部サーバにSYSLOGを送信する際にFacilityを指定した値に変換
43	logging host 172.30.20.229 level informational	外部SYSLOGサーバとログレベルを指定
44	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。
45	!	
46	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)
47	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)
48	!	
49	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
50	!	
51	hostname FITELnet	hostname設定
52	!	
53	ntp server 172.30.20.229	NTPサーバ指定
54	!	
55	hostname FITELnet	hostname指定
56	!	

57	interface GigaEthernet 1/1	LAN側物理インタフェース設定
58	vlan-id 1	VLAN指定(ポートVLAN) ※必須
59	bridge-group 1	bridge-group指定 ※必須 ※同一bridge-groupのLANポートを複数設定する場合は、vlan-id, channel-groupも全てのインタフェースで合わせて設定して下さい
60	channel-group 1	LAN側論理インタフェース(Port-channel)と紐付け
61	exit	
62	!	
63	interface GigaEthernet 2/1	WAN側物理インタフェース設定
64	vlan-id 2	VLAN指定(ポートVLAN) ※必須
65	bridge-group 2	bridge-group指定 ※必須
66	channel-group 2	WAN側論理インタフェース(Port-channel)と紐付け
67	ip access-group 111 out	
68	ip access-group 112 in	
69	ip access-group 113 out	
70	ip access-group 114 out	
71	ip access-group 115 in	
72	ip access-group spi ftp-data enable	
73	exit	
74	!	
75	interface Port-channel 1	LAN側論理インタフェース設定
76	ip address 10.128.0.1 255.255.255.0	アドレス設定
77	exit	
78	!	
79	interface Port-channel 2	WAN側論理インタフェース設定
80	ip address 10.0.0.254 255.255.255.0	アドレス設定
81	dns-snooping enable	DNS ResponseのFQDNチェックを有効化します。 ※DNS Responseを受信するインタフェースに設定して下さい。
82	exit	
83	!	
84	line console	Consoleアクセス設定
85	exec-timeout 0	自動ログアウト時間(分) ※"0"指定時は自動ログアウトしません。 ※defaultは30分
86	authorization exec default local	Consoleログイン時の許可方式を指定 local: usernameコマンドで設定した特権レベルでログイン許可
87	exit	
88	!	
89	line telnet	Telnetアクセス設定
90	exec-timeout 0	自動ログアウト時間(分) ※"0"指定時は自動ログアウトしません。 ※defaultは30分
91	exit	
92	!	
93	end	