FURUKAWA ELECTRIC

FURUKAWA ELECTRIC GROUP

FITELnet F220/F221 トレーニング資料 （F200との比較無し） 資料4：設定コマンドの解説

2022年10月

古河電気工業株式会社
古河ネットワークソリューション株式会社

第3版

目次

タイトル	ページ
IPsecについて	
IPsecの設定	3
フラグメント	6
PPPoEの設定(NAT/学習Filtering/ProxyDNS)	8
LANの設定(DHCPサーバ)	9
snmp(MIB/Trap)およびsntpクライアント	10
ログ出力設定(syslog/内部バッファ)	11
冗長構成	12
QoS	16
ローカルブレイクアウト	19

IPsecの設定①

設定	説明
crypto isakmp profile PROF0001	ISAKMP(Phase1)プロファイル設定
match identity address 10.11.0.11	ピアの識別子(identity)
set peer 10.11.0.11	ピアのアドレス(ドメイン名でも可能)
self-identity user-fqdn kyoten0001	自装置の識別子
set ipsec-policy P2-POLICY P2-POLICYを指定(次ページ)	IPsec(Phase2)ポリシーを指定
set isakmp-policy P1-POLICY	ISAKMP(Phase1)ポリシーを指定
ike-version 1	IKEバージョン (デフォルトはIKEv2となります)
local-key SECRET-VPN	事前共有鍵
exit	
crypto isakmp policy P1-POLICY	ISAKMP(Phase1)ポリシー設定
authentication pre-share	認証方法(pre-share:事前共有鍵/rsa-sig:RSA証明書)
encryption aes	暗号化方式(aes/3des/des)
encryption-keysize aes 256 256 256	暗号化方式の鍵長
group 2	DHグループ
lifetime 86400	Phase1のライフタイム
hash sha-256	ハッシュ方式
initiate-mode aggressive	ネゴシエーションモードの指定(main/aggressive)
exit	

- IPsecの設定はprofile(P1)/map(P2)とpolicyに分かれています
  - ✓ profile/mapはIDや鍵等を設定します
  - ✓ policyは暗号アルゴリズム等を設定します
- profileとpolicyの紐付けは set isamkp-policy で行います
- 1つのpolicyを複数のprofileに紐付けることが可能です
  (policyとprofileを1:Nに紐付け可能)

IPsecの設定②

設定	説明
crypto ipsec selector SELECTOR	セレクタ設定
src 1 ipv4 any	セレクタの送信元アドレス
dst 1 ipv4 any	セレクタの宛先アドレス
exit	
crypto map KYOTEN0001 ipsec-isakmp	map(Phase2)設定
match address SELECTOR	セレクタを指定
set isakmp-profile PROF0001	ISAKMP(Phase1)プロファイルを指定
exit	
crypto ipsec policy P2-POLICY	IPsec(Phase2)ポリシー設定
set pfs group2	PFS
set security-association lifetime seconds 28800	Phase2のライフタイム
set security-association transform esp-aes esp-sha256-hmac	Phase2の暗号・ハッシュアルゴリズム
encryption-keysize aes 256 256 256	Phase2の暗号アルゴリズムの鍵長
set mtu 1454	ESPカプセル化後のMTU値(P.6～7を参照)
set ip df-bit 0	ESPカプセル化後のDFビット
set ip fragment post	ESPカプセル化する際のフラグメント方式(P.6～7を参照)
exit	
interface Tunnel 1	トンネルインタフェース設定
tunnel mode ipsec map KYOTEN0001	IPsec用トンネルであることと、map(Phase2)を指定
exit	

profileを指定(前ページ)

- profileとpolicyの紐付けは set ipsec-policy (crypto isakmp profileモード)で行います
- 1つのpolicyを複数のmapに紐付けることが可能です(policyとmapを1:Nに紐付け可能)
- ルートベースをサポートしており、ポリシーベースは未サポートです
  (宛先アドレスでSAを決定します。ポート番号でSAを決定することはできません)

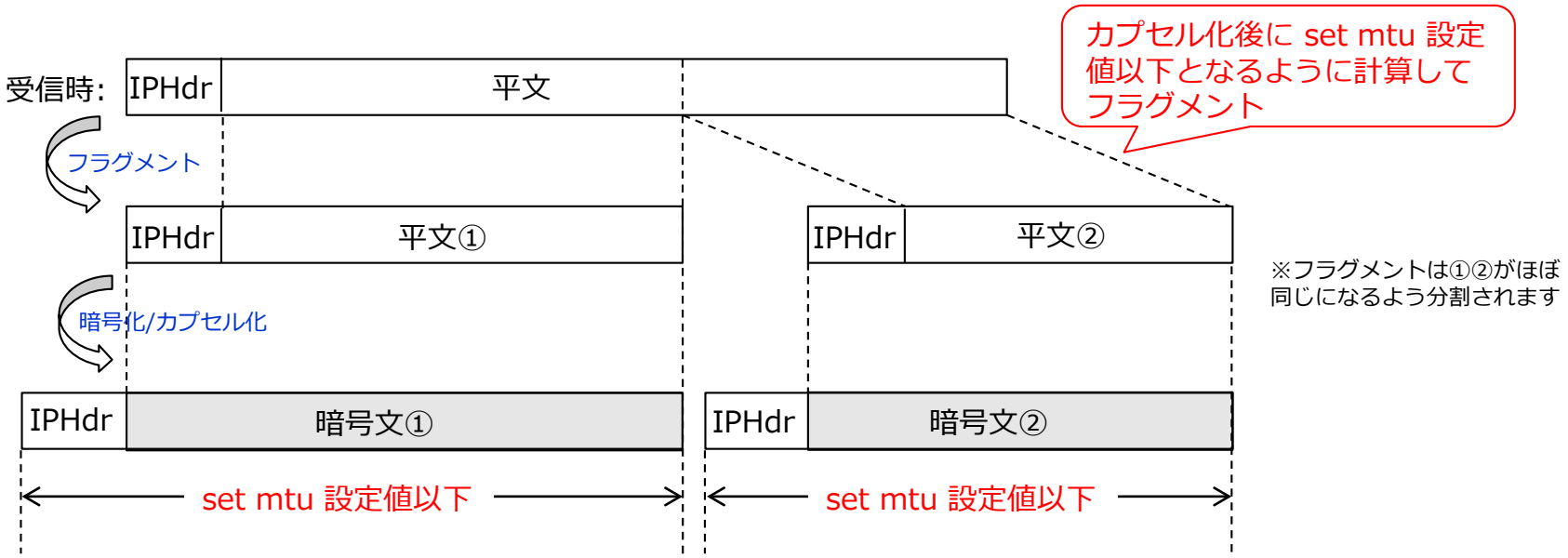
IPsecの設定③

その他、IPsec 設定時の注意事項

- デフォルトでIPsecは動作する動作となります。有効化させるための設定はありません
- 平文を通したくない場合、明示的に access-list で deny を設定して破棄する必要があります
- 下記の設定で IPsec 関連のログを有効化します

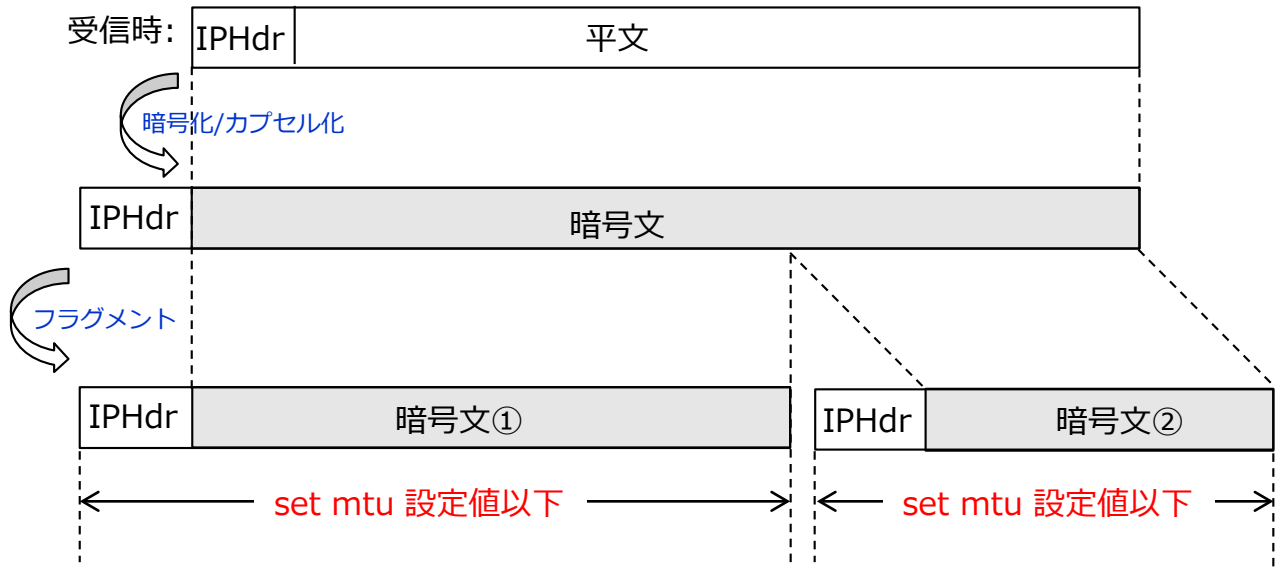
設定	説明
crypto log isakmp negotiation-fail	IKEネゴ失敗ログを出力
crypto log isakmp sa	SA確立/解放ログを出力
crypto log isakmp session	セッション確立/解放ログを出力
logging level informational	デフォルトではerrors(3)以上(数字の小さい)のログを出力しますが、上記ログ出力の主なものはレベルがinformational(6)となっています。そのため、informational以下(6以上)にする必要があります

IPsecのフラグメント方式(pre-fragment)



- カプセル化前にフラグメントする方式をpre-fragmentと言います
- ESP受信側でリアセンブルする必要が無く、個々のフラグメントパケットを復号できるため、受信側の負荷を小さくできるメリットがあります
- 受信した平文パケットのIP HeaderのDF(Don't Fragment)が0である必要があります。DFが1でカプセル化後にset mtu超となる場合、ICMP の Fragumentation needed and DF setを送信元に返信します(Path MTU Discoveryの動作)
- F220では、`set ip fragment post`（`crypto ipsec policy`モード）が設定されていない場合にpre-fragmentとなります
- カプセル化後のMTU値を`set mtu`（`crypto ipsec policy`モード）で指定します

IPsecのフラグメント方式(post-fragment)



- カプセル化後にフラグメントする方式をpost-fragmentと言います
- フラグメントされる場合でもESPを受信したIPsecGWがリアセンブルしてから復号するため、最終的にユーザが受信する平文パケットはフラグメントされる前と同じというメリットがあります
- 受信した平文パケットのIP HeaderのDFが0でも1でもフラグメント可能です
- F220では、下記２つを設定(両方必要)することでpost-fragmentとなります

```
set ip fragment post
set ip df-bit 0
```

- set ip df-bitは、カプセル化後のDF値を決める設定です。設定値としては下記があります。
  0: DFを0にする
  1: DFを1にする
  copy: 受信した平文のDF値をカプセル化後にコピーする
  カプセル化後のESPパケットはフラグメントされているので、DF=0となる必要があります
- カプセル化後のMTU値をset mtuで指定します

PPPoEの設定(NAT/学習Filtering/ProxyDNS)

設定	説明
ip route 0.0.0.0 0.0.0.0 tunnel 1	デフォルトルートをtunnel1(modeはPPPoE)にする
ip nat list 1 192.168.0.0 0.0.0.255	NATする送信元アドレス範囲
access-list 111 deny ip any any	(学習フィルタリング以外の)全パケット破棄するためのACL
access-list 121 spi ip any any	学習フィルタリングのACL
pppoe profile PPPOE_PROF	PPPoEプロファイル設定
account user@xxxx.ne.jp secret	PPPoEのアカウント名およびパスワード
exit	
interface tunnel 1	トンネル設定
tunnel mode pppoe profile PPPOE_PROF	PPPoE用トンネルであることと、PPPoEプロファイルを指定
!ip address …	端末型接続: 設定不要 (固定IPの場合、 ip addressで設定) LAN型接続: ip unnumberedを設定
pppoe interface gigaethernet 2/1	PPPoEの物理IF
ip nat inside source list 1 interface	NAT/NAPT変換ルール(ip nat list 1の送信元アドレスをIFアドレスに変換)
ip access-group 111 in	受信ACL
ip access-group 121 out	送信ACL(学習フィルタリング)
exit	
interface GigaEthernet 2/1	物理IFの指定(必須となります)
vlan-id 2	
bridge-group 2	
pppoe enable	このIFでPPPoEを使用可能とする
exit	
dns-server ip enable	IPv4のDNSサーバ機能の有効化
proxydns domain 1 any * any ipcp tunnel 1 優先度 IF名	tunnel 1にipcpで通知されたDNSサーバIPアドレスをリレー先に使用 (複数のリレー先がある場合、優先度を指定可能。この例では優先度は1)

LANの設定(DHCPサーバ)

設定	説明
interface GigaEthernet 1/1	
vlan-id 1	
bridge-group 1	
channel-group 1	
exit	
interface GigaEthernet 1/2	
vlan-id 1	
bridge-group 1	
channel-group 1	
exit	
… GigaEthernet 1/1～1/8まで同様の設定	
interface Port-channel 1	
ip address 192.168.0.1 255.255.255.0	
ip dhcp service server	DHCPサーバ有効化
ip dhcp server-profile lan1	DHCPサーバプロファイルを指定
exit	
ip dhcp server-profile lan1	DHCPサーバプロファイル設定
address 192.168.0.101 192.168.0.254	払出しアドレスの範囲を指定
dns 192.168.0.1	DHCPで通知するDNSサーバ
gateway 192.168.0.1	DHCPで通知するデフォルトゲートウェイ
lease-time 28800	払出しアドレス有効時間を秒単位で指定
exit	

snmp(MIB/Trap)およびsntpクライアント

設定	説明
snmp-server community public ro	SNMPコミュニティ名を指定
snmp-server contact admin	sysContactを指定
snmp-server name FITELnet-F220-1	sysNameを指定
snmp-server location Tokyo	sysLocationを指定
snmp-server enable traps	トラップ送信を有効化
snmp-server host 192.168.0.150 public v2c	トラップの送信先SNMPマネージャのアドレスとバージョンを指定
!	
sntp server 192.168.0.100	SNTPで問い合わせるサーバのアドレスを指定
sntp poll-interval 86400	SNTPの問い合わせ間隔を秒単位で指定

ログ出力設定(syslog/内部バッファ)

- F220ではログの出力先には下記があり、個別に制御することが可能です
  logging host（syslogサーバに出力）
  logging buffer（F220内部バッファに出力）
  logging console（コンソールに出力）
  logging telnet（telnetに出力）

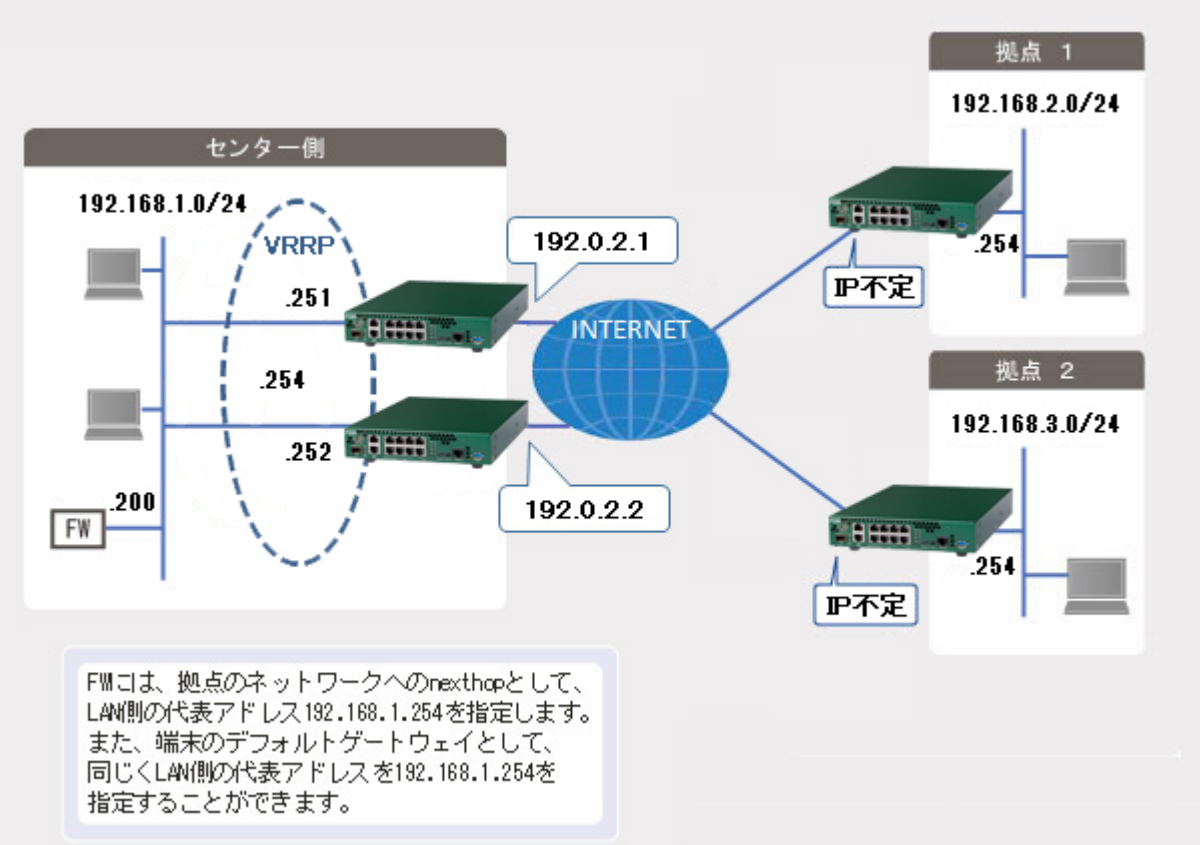
- syslogで送信されるファシリティについて
  ログ毎にファシリティが異なります(マニュアルのメッセージ集に記載)
  logging fixed-facilityで指定した値で送信することができます

- syslogで送信されるレベルについて
  ログ毎にレベルが異なります(メッセージ集に記載)
  出力先毎に logging（host|buffer|console|telnet） level で出力されるレベルを設定可能で、この設定が無い場合は logging buffer で設定された値で動作します。デフォルト値は errors(3) です。

F220
logging host 192.168.0.3
logging level informational informational(6)以上(レベル番号は小さい)のログを出力する

IPsec使用時はinformationalを推奨します。
SA確立・切断ログがinformationalのためです。

冗長構成(構成図)



冗長構成(センター側 1系)

設定	解説
event-action 1	イベント-アクション設定
event interface tunnel 1 down	eventを指定(tunnel 1 がdownしたら)
action 1.0 interface gigaethernet 1/1 down	actionを指定(gigaethernet 1/1 をdownさせる)
exit	
event-action 2	
event interface tunnel 1 up	eventを指定(tunnel 1 がupしたら)
action 2.0 interface gigaethernet 1/1 up	actionを指定(gigaethernet 1/1 をupさせる)
exit	
interface Tunnel 1	PPPoEインタフェース
tunnel mode pppoe profile PPPOE_PROF	
pppoe interface gigaethernet 2/1	
…	
exit	
interface GigaEthernet 1/1	
channel-group 1	
…	
exit	
ip vrrp enable	VRRP機能を有効化
interface Port-channel 1	
ip address 192.168.1.251 255.255.255.0	
vrrp 1 address 192.168.1.254	VRRP仮想アドレスを指定
vrrp 1 priority 200	VRRP優先度を指定
vrrp 1 preempt	preempt設定
exit	

PPPoEがDownしたら
GE1/1をdownさせ、
VRRP状態がinitializeとなる

PPPoEがupしたら
GE1/1をupさせ、
VRRP状態がmasterとなって
切り戻る

冗長構成(センター側 2系)

設定	解説
interface Tunnel 1	PPPoEインタフェース
tunnel mode pppoe profile PPPOE_PROF	(profileは略)
pppoe interface gigaethernet 2/1	
…	
exit	
interface GigaEthernet 1/1	
channel-group 1	
…	
exit	
ip vrrp enable	VRRP機能を有効化
interface Port-channel 1	
ip address 192.168.1.252 255.255.255.0	
vrrp 1 address 192.168.1.254	VRRP仮想アドレスを指定
vrrp 1 priority 100	VRRP優先度を指定
vrrp 1 preempt	preempt設定
exit	

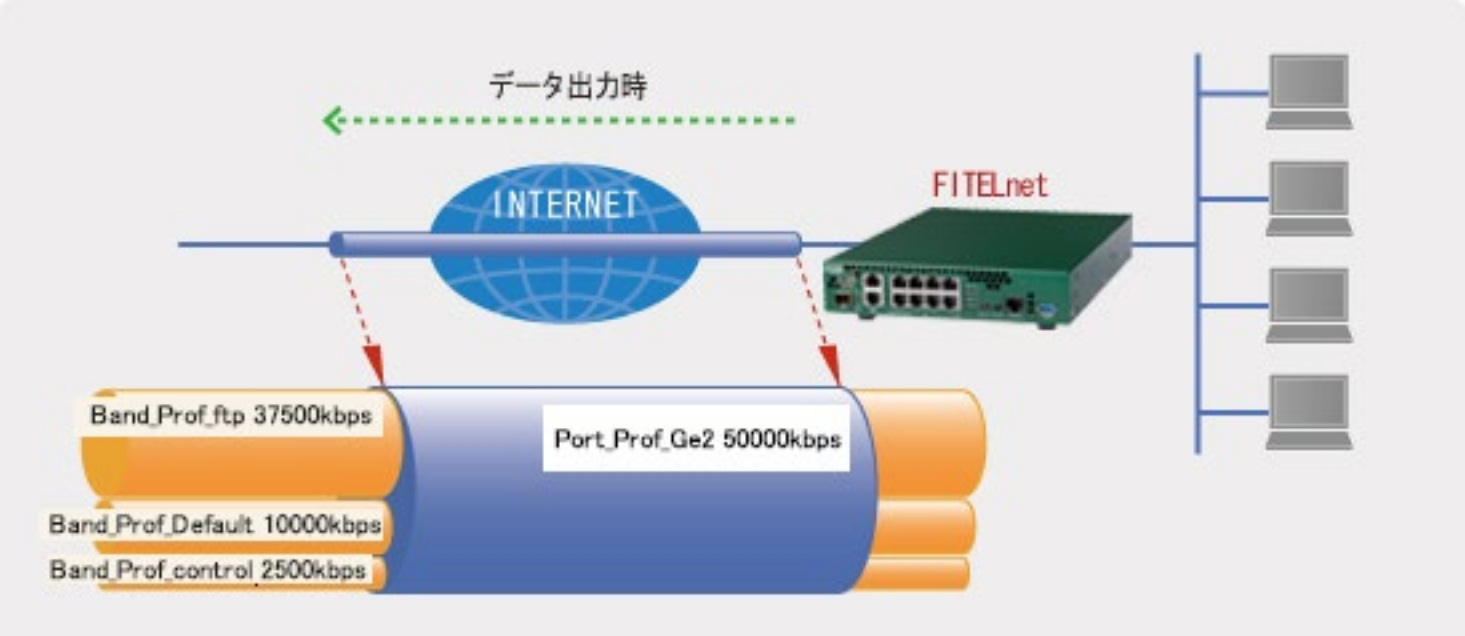
1系のVRRP状態がinitializeとなることで、
2系のVRRP状態がmasterとなる

1系のVRRP状態がmasterに戻ると、
2系のVRRP状態がbackupとなって
切り戻る

冗長構成(拠点)

設定	解説
ip route 192.168.1.0 255.255.255.0 null 0 150	tunnel 2,3のdown時、センタ宛の通信が平文で出ないように null ルートを設定
ip route 192.168.1.0 255.255.255.0 tunnel 2 survey name t2_ICMP	survey機能と連動したセンタ宛のメイン経路を設定
ip route 192.168.1.0 255.255.255.0 tunnel 3 100	センタ宛のバックアップ経路を設定
survey 192.168.1.251 name t2_ICMP survey-map ICMP-Kanshi source port-channel 1 nexthop tunnel 2 interworking	interface Tunnel 2経由でセンタ側のLAN側IPアドレスをICMP監視して、"interworking"を指定することでICMP監視の結果によってtunnel インタフェースのup/downを同期
survey-map ICMP-Kanshi	
retry 2 interval 10000	ICMPの応答が無い場合、再送を10,000ミリ秒間隔で2回実施
frequency every 10000	10,000ミリ秒間隔で監視を実施
stability 2 interval 10000	surveyがDOWN状態の際、10,000ミリ秒間隔で2回ICMP監視が成功したらUP状態となる
exit	
interface Tunnel 2	メイン側(1系)のIPsecトンネル
tunnel mode ipsec map CENTER	
exit	
interface Tunnel 3	
tunnel mode ipsec map CENTER_BK	バックアップ側(2系)のIPsecトンネル
link-state sync-sa	IFのup/downを、SA確立状態と連動させる
exit	

QoS(CBQによる帯域制御)①



- 50,000kbps を帯域制御に使用 → Port_Prof_Ge2
- FTP用に 37,500kbps を割り当て → Band_Prof_ftp
- ICMP用に 2,500kbps を割り当て → Band_Prof_control
- 上記以外に 10,000kbps を割り当て → Band_Prof_Default

QoS(CBQによる帯域制御)②

設定	解説
traffic-manager network	
port profile Port_Prof_Ge2	ポートスケジューラ プロファイルにてシェーピング帯域を設定
shape pir 50000 pbs 3072	シェーピングレート 50,000 kbps、バーストサイズ 3,072 bytes
exit	
port scheduler gigaethernet 2/1 Port_Prof_Ge2	GE2/1に対し ポートスケジューラ Port_Prof_Ge2 を指定
bandwidth profile Band_Prof_control	bandwidthスケジューラ プロファイルを設定(control-class用)
shape cir 2500 cbs 1024	保証レート 2,500 kbps、バーストサイズ 1,024 bytes
exit	
bandwidth profile Band_Prof_ftp	bandwidthスケジューラ プロファイルを設定 (ftp-class用)
shape cir 37500 cbs 1024 borrow	保証レート 37,500 kbps、バーストサイズ 1,024 bytes borrowにより、保証レートを超えたトラフィックを低優先で送信
priority 3	スケジューラの優先度を 3 に指定(デフォルトは0)
exit	
bandwidth profile Band_Prof_Default	bandwidthスケジューラ プロファイルを設定(class-default用)
shape cir 10000 cbs 1024 borrow	保証レート 10,000 kbps、バーストサイズ 1,024 bytes borrowにより、保証レートを超えたトラフィックを低優先で送信
exit	
exit	

次ページで参照される

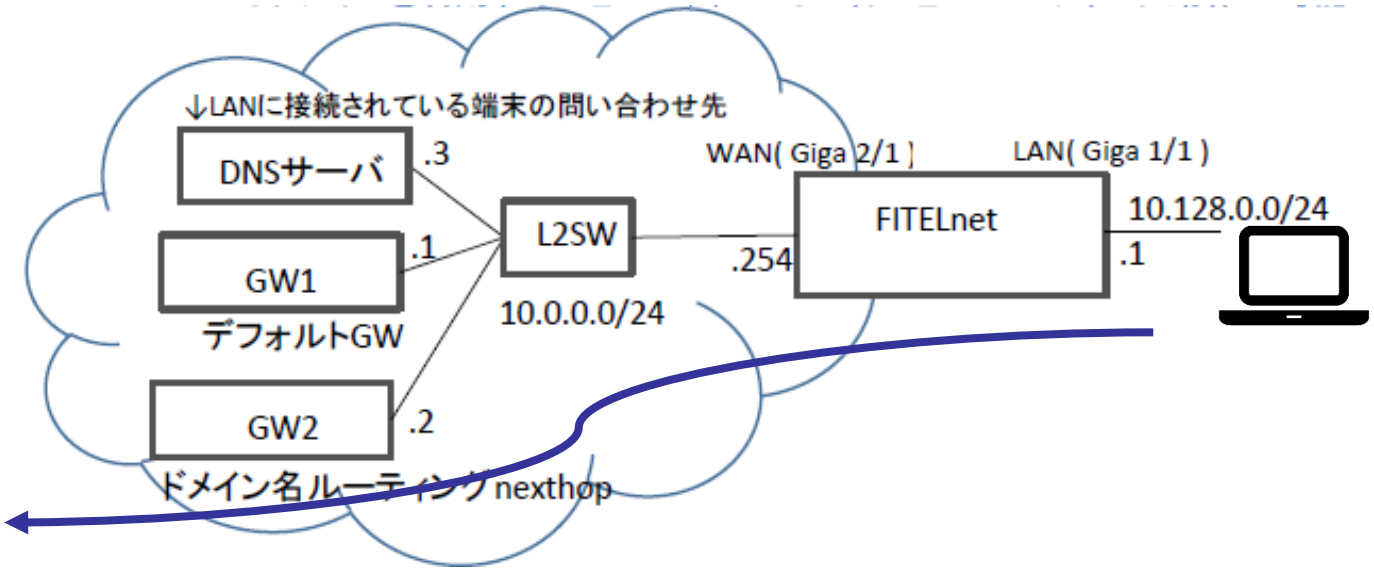
次ページで参照される

次ページで参照される

QoS(CBQによる帯域制御)③

設定	解説
access-list 100 permit tcp any any eq ftp	
access-list 100 permit tcp any any eq ftp-data	
access-list 120 permit 1 any any	
class-map ftp-class	クラスマップでパケットを分類 (ftp-class)
match ip access-group 100	QoS対象にftp(TCP 21),ftp-data(TCP 20)を指定
exit	
class-map control-class	クラスマップでパケットを分類 (control-class)
match ip access-group 120	QoS対象にICMP(protocol 1)を指定
exit	
policy-map ftp-policy	ポリシーマップで各クラスにbandwidthスケジューラを割り当て
class ftp-class	
bandwidth profile Band_Prof_ftp	ftp-class に Band_Prof_ftp スケジューラを割り当て
exit	
class control-class	
bandwidth profile Band_Prof_control	control-class に Band_Prof_control スケジューラを割り当て
exit	
class class-default	どのクラスにも属さないフローに対するポリシーを設定
bandwidth profile Band_Prof_Default	class-default に Band_Prof_Default スケジューラを割り当て
exit	
exit	
interface GigaEthernet 2/1	
…	
service-policy output ftp-policy	
exit	

ローカルブレイクアウト①



ドメイン名ルーティングを行うことで、特定のサービス（ドメイン）毎にトラフィックを振り分ける（ローカルブレイクアウト）ことが可能です

ローカルブレイクアウト②

設定	解説
ip route 0.0.0.0 0.0.0.0 10.0.0.1	Static経路（デフォルト経路）
!	
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
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
!	
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)
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
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 ※"*"のみを指定した場合、全てのFQDNが対象
exit	
!	
interface port-channel 1	
ip address 10.10.0.254 255.255.255.0	
dns-snooping enable	DNS ResponseのFQDNチェックを有効化 ※DNS Responseを受信するインタフェースに設定
exit	

設定例

下記URLにF220/F221の設定例がございます。

https://www.furukawa.co.jp/fitelnet/product/setting/index.html

https://www.furukawa.co.jp/fitelnet/product/f220/setting/index.html