FURUKAWA ELECTRIC

FURUKAWA ELECTRIC GROUP

FITELnet F220/F221
トレーニング資料
(F200との比較有り)
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2版

目次

IPsecの設定①

F220	F200
crypto isakmp profile PROF0001	crypto isakmp policy 1
match identity address 10.11.0.11 set peer 10.11.0.11	peer-identity address 10.11.0.11
self-identity user-fqdn kyoten0001	my-identity kyoten0001
set ipsec-policy P2-POLICY P2-POLICYを指定(次ページ)	
set isakmp-policy P1-POLICY P1-POLICYを指定	
ike-version 1 デフォルトはv2	
local-key SECRET-VPN	key ascii SECRET-VPN
exit	
crypto isakmp policy P1-POLICY	
authentication pre-share	authentication prekey
encryption aes	encryption aes 256
encryption-keysize aes 256 256 256	
group 2	group 2
lifetime 86400	lifetime 86400
hash sha-256	hash sha-256
initiate-mode aggressive	negotiation-mode aggressive
exit	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

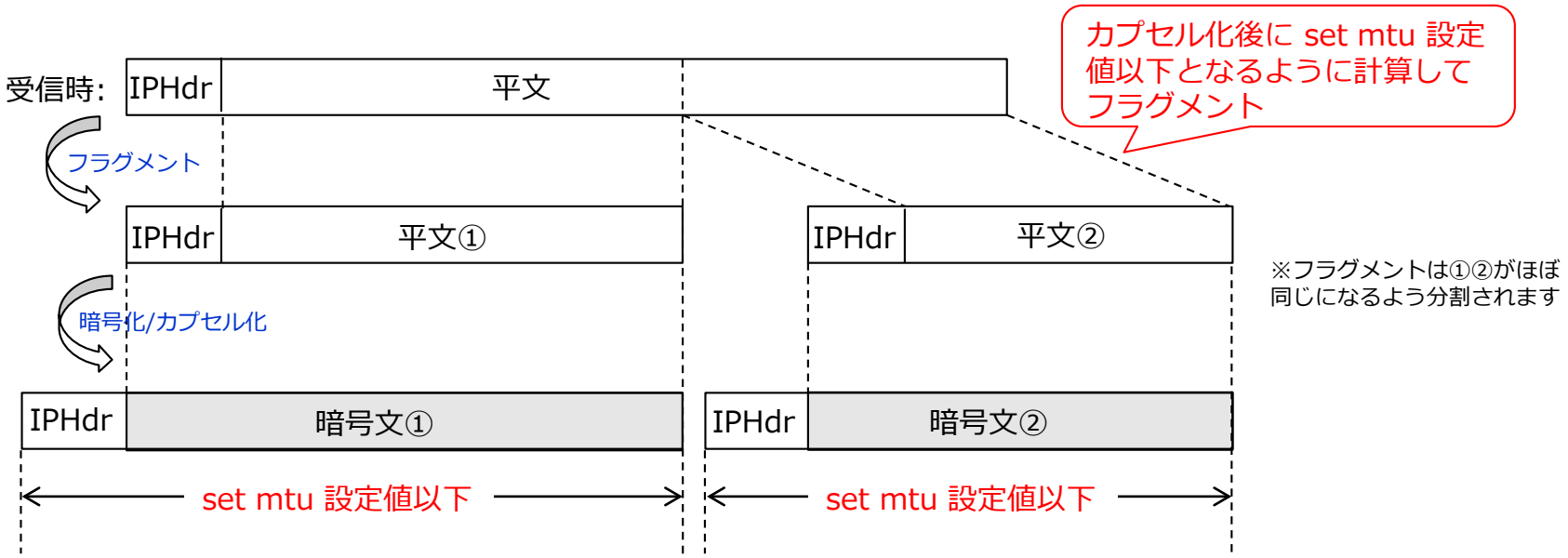
F220	F200
crypto ipsec selector SELECTOR	ipsec access-list 1 ipsec ip any any
src 1 ipv4 any	
dst 1 ipv4 any	
exit	
F220では暗号アルゴリズムはpolicy内で指定する	ipsec transform-set TRANS esp-aes-256 esp-sha256-hmac
crypto map KYOTEN0001 ipsec-isakmp	crypto map KYOTEN0001 1
match address SELECTOR	match address 1
set isakmp-profile PROF0001 profile(P1)を指定する	
exit	
crypto ipsec policy P2-POLICY P2-POLICYはprofile内で指定される	
set pfs group2	set pfs group2
set security-association lifetime seconds 28800	set security-association lifetime seconds 28800
set security-association transform esp-aes esp-sha256-hmac encryption-keysize aes 256 256 256	set transform-set TRANS
set mtu 1454 カプセル化後のMTU値を指定する(pre-fragmentでは、通常、物理IFのMTUと同じ値にします)	F200ではIFに指定する
set ip df-bit 0	F200ではouterのdfは常に0
set ip fragment post	F200ではipsecifとESPが送信されるIFのMTUにより決定される
exit	exit
interface Tunnel 1	interface ipsecif 2
tunnel mode ipsec map KYOTEN0001 map(P2)を指定する	crypto map KYOTEN0001
exit	exit

- 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

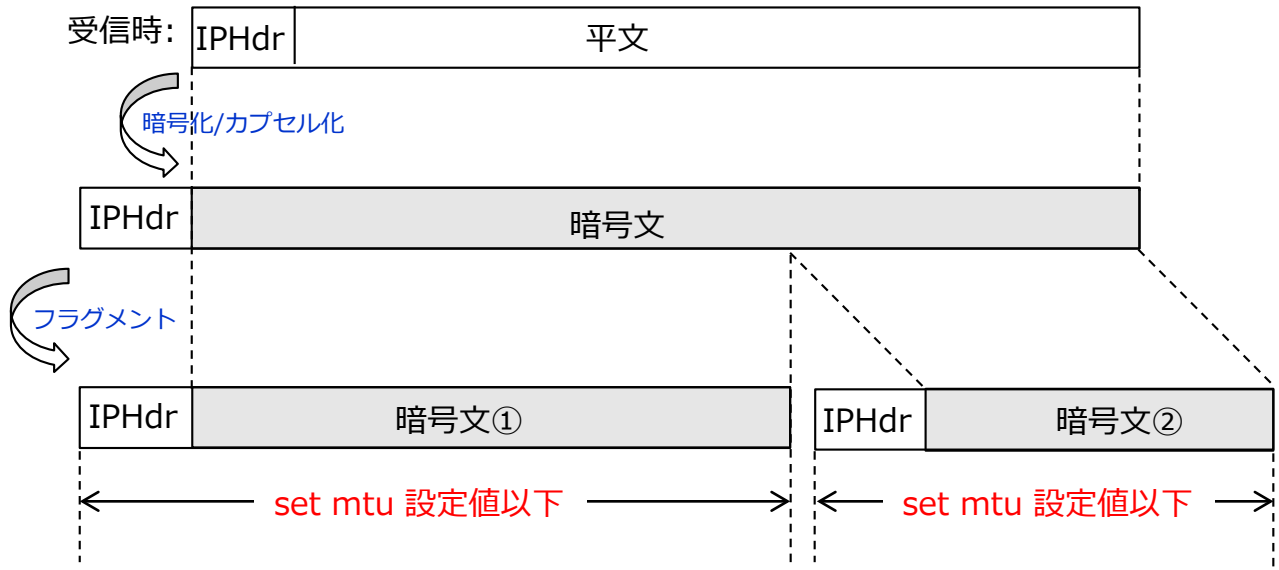
F220	F200
(vpn enableはF220には無い。無くてもIPsecが動作する)	vpn enable
(ipsec access-listのbypassが無くてもF220は平文を通す。 平文を通したくない場合、access-listでdenyを設定する)	ipsec access-list 128 bypass ip any any
crypto log isakmp negotiation-fail (IKEネゴ失敗ログを出力) crypto log isakmp sa (SA確立/解放ログを出力) crypto log isakmp session (セッション確立/解放ログを出力)	vpnlog enable
	crypto ipsec-log
(block-type-discardログは出力されない)	nolog-block-type-discard
(spi-no-matchログは出力されない)	nolog-spi-no-match
	exit

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)



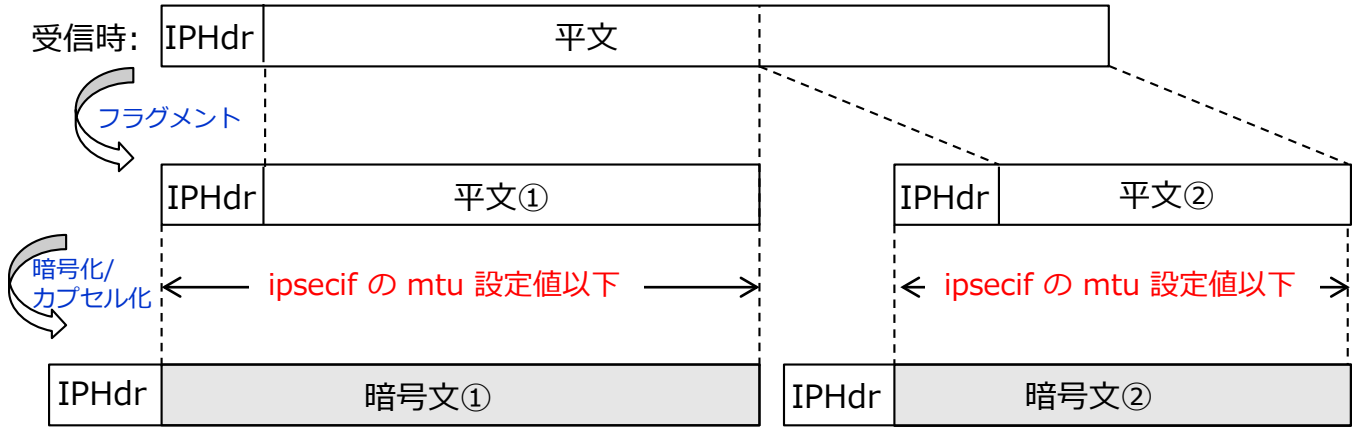
- カプセル化後にフラグメントする方式をpost-fragmentと言います
- フラグメントされる場合でもESPを受信したIPsecGWがリアセンブルしてから復号するため、最終的にユーザが受信する平文パケットはフラグメントされる前と同じというメリットがあります
- 受信した平文パケットのIP HeaderのDFが0でも1でもフラグメント可能です
- F220では、下記２つを設定(両方必要)することでpost-fragmentとなります

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

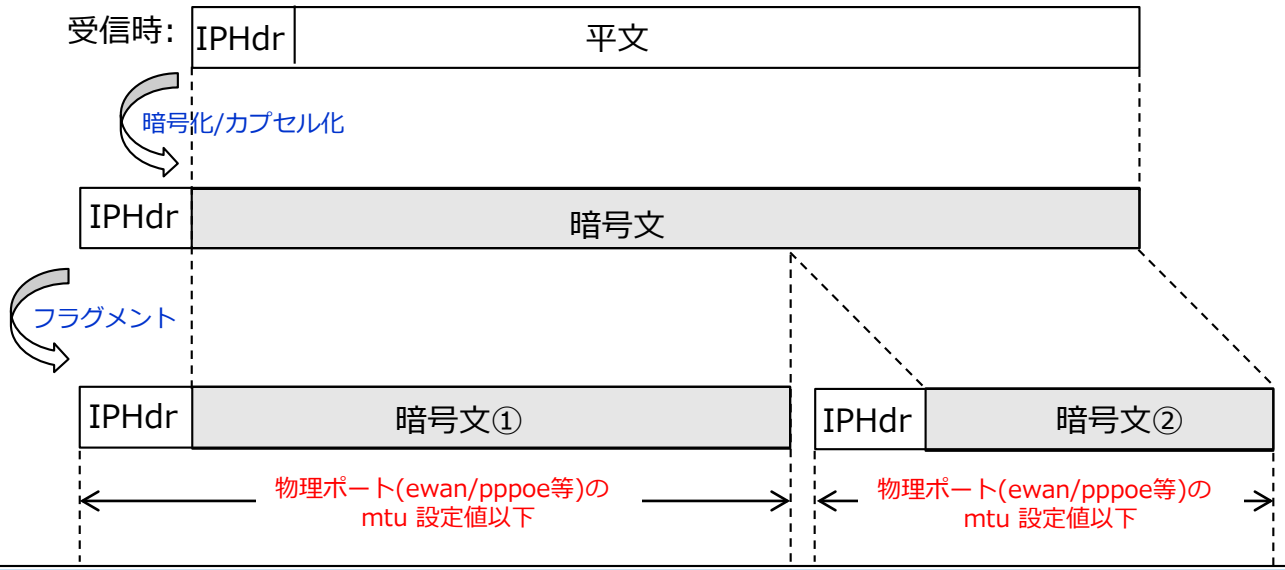
- set ip df-bitは、カプセル化後のDF値を決める設定です。設定値としては下記があります。
  0: DFを0にする
  1: DFを1にする
  copy: 受信した平文のDF値をカプセル化後にコピーする
  カプセル化後のESPパケットはフラグメントされているので、DF=0となる必要があります
- カプセル化後のMTU値をset mtuで指定します

F200のIPsecのフラグメント方式

pre-fragment(ipsecifのMTUを小さくする)



post-fragment(ipsecifのMTUを大きくし、物理ポートのMTUを小さくする)



ポリシーベースIPsec設定からの変換

- F220ではポリシーベースIPsecをサポートしておりません。
  F200でポリシーベースIPsecをご利用いただいたお客様にて、F220へのリプレースをご検討いただく場合は、ポリシーベースに合わせたルートベースIPsecの設定が必要となります。
  以下、詳細をご説明いたします。

	F220（ルートベースIPsec）	F200（ポリシーベースIPsec）
IPsec対象を設定するIF	IPsecトンネルインタフェース	WAN側インタフェース
暗号化/非暗号化対象の指定	ip routeの中継先で指定	IPsecセレクタで指定（ipsec/bypass）
IPsecセレクタのチェック ※補足ページを参照	なし（デフォルト動作） ※設定により変更可（制限あり）	あり ※設定による変更不可

- 本資料ではIPsec対向側がポリシーベースIPsecを利用している場合のF220で従来のポリシーベースIPsec設定からルートベースIPsec設定へ移行する為の設定のポイントについて解説します。

  ①　　：暗号化通信（IPsec）用の経路設定および非暗号化通信用（インターネット等）用の経路設定とIPsecトンネルインタフェース設定について
  ②　　：センタ側とのIPsecトンネル経由でインターネット接続を行う場合の経路設定について
  ③～④：同一VPNピア複数IPsec SA構成時の設定について
  ⑤～⑦：同一VPNピア複数IPsec SA構成時の設定とポリシールーティング機能との併用について

- 以下のコマンドについての解説は省略しておりますので、profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください
  - crypto ipsec policy
  - crypto isakmp policy
  - crypto isakmp profile

- 解説の中ではPPPoEを利用するインタフェースを interface Tunnel 1000 としています

ポリシーベースIPsec設定からの変換（補足）

- IPsecセレクタのチェックについて
  F200ではIPsec SA確立時のSAのセレクタ情報とESPパケット復号化後の送信元/宛先のチェックを行い、セレクタ情報に一致しないパケットを廃棄する動作となっております（設定による変更は不可）。

  F220では設定でセレクタチェックの有効化/無効化が変更可能であり、デフォルト動作としてはセレクタチェックは無効として動作し、以下のいずれかの設定で有効化することが可能です。

  - crypto ipsec selector-check（装置全体でセレクタチェックを有効化する）
  - set selector-check enable（IPsecポリシー毎にセレクタチェックを有効化する）

  ただし、F220でセレクタチェック機能を有効化できるのは4つまでの制限があり、5つ以上のIPsecセレクタを利用する場合はセレクタチェック機能を無効にしてください。
  ※代替設定として、IPsecを利用するTunnel IF設定内で復号化後の送信元/宛先に対してaccess-listによるフィルタリングを行うことは可能です。

例）

```
access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 120 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 199 deny ip any any
!
interface Tunnel 1
 ip access-group 110 out
 ip access-group 120 in
 ip access-group 199 out
 ip access-group 199 in
 tunnel mode ipsec map CENTER0001
exit
```

ポリシーベースIPsec設定からの変換①
～IPsec対象を設定するIF設定と経路設定の移行について～

F220（ルートベースIPsec）	F200（ポリシーベースIPsec）
ip route 0.0.0.0 0.0.0.0 tunnel 1000　非暗号化対象通信用 ip route設定	ip route 0.0.0.0 0.0.0.0 pppoe 1　暗号化対象通信も非暗号化対象通信(平文)もデフォルト経路を利用する
ip route 192.168.1.0 255.255.255.0 tunnel 1　暗号化対象通信用 ip route設定	
crypto ipsec selector SELECTOR	ipsec access-list 1 ipsec ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
src 1 ipv4 192.168.2.0 255.255.255.0	ポリシーベースIPsecでは暗号化対象か非暗号化対象かを ipsec access-list で指定する
dst 1 ipv4 192.168.1.0 255.255.255.0	ipsec：暗号化対象
exit	bypass :非暗号化対象(平文)
bypass用のcrypto ipsec selector設定は不要 (ipsec access-listのbypassが無くてもF220は平文を通す。 平文を通したくない場合、access-listでdenyを設定する)	ipsec access-list 128 bypass ip any any
interface Tunnel 1	interface pppoe 1
tunnel mode ipsec map KYOTEN0001	crypto map KYOTEN0001
exit　WAN側IFとは別にIPsecトンネルIF設定が必要 IPsecトンネルIFにcrypto map設定を行いIPsec対象を指定	exit　WAN側IFにcrypto map設定を行いIPsec対象を指定
crypto map KYOTEN0001 ipsec-isakmp	crypto map KYOTEN0001 1
match address SELECTOR	match address 1
set isakmp-profile PROF0001	set peer address 192.0.2.1
exit	

- ポリシーベースIPsecと異なりルートベースIPsecでは、暗号化対象通信をip route設定で指定します
- WAN側インタフェースとは別にIPsecを利用する為のIPsecトンネルインタフェース設定が必要です
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください

ポリシーベースIPsec設定からの変換②
～センタIPsecトンネル経由でインターネット接続を行う場合～

F220（ルートベースIPsec）	F200（ポリシーベースIPsec）
ip route 192.0.2.1 255.255.255.255 tunnel 1000 IPsec対向のVPNピア宛の経路 IKEネゴシエーション用 ip route設定	ip route 0.0.0.0 0.0.0.0 pppoe 1 暗号化対象通信も非暗号化対象通信(平文)もデフォルト経路を利用する(IPsec対向のVPNピア宛の経路も含まれる)
ip route 0.0.0.0 0.0.0.0 tunnel 1 全て(any)の宛先への経路 暗号化対象通信用 ip route設定	
crypto ipsec selector SELECTOR	ipsec access-list 1 ipsec ip 192.168.2.0 0.0.0.255 any
src 1 ipv4 192.168.2.0 255.255.255.0	センタ側とのIPsec経由でインターネット接続を行う場合は全ての通信を暗号化対象とする為、宛先をanyで指定
dst 1 ipv4 any	
exit	
interface Tunnel 1	interface pppoe 1
tunnel mode ipsec map KYOTEN0001	crypto map KYOTEN0001
exit WAN側IFとは別にIPsecトンネルIF設定が必要 IPsecトンネルIFにcrypto map設定を行いIPsec対象を指定	exit WAN側IFにcrypto map設定を行いIPsec対象を指定
crypto map KYOTEN0001 ipsec-isakmp	crypto map KYOTEN0001 1
match address SELECTOR	match address 1
set isakmp-profile PROF0001	set peer address 192.0.2.1
exit	

- ルートベースIPsecで拠点側がセンタとのIPsecトンネル経由でインターネット接続を行う場合、デフォルトルートだけではIKEネゴシエーションが行えない為、センタ側のVPNピア宛の平文経路設定が必要です
- Responderとなるセンタ側の設定で、拠点側のIP不定の場合は以下のトンネルルート設定が必要です。「crypto isakmp tunnel-route」もしくは「tunnel-route」
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください

ポリシーベースIPsec設定からの変換③
～同一VPNピア複数IPsec SAを利用する場合(1/2)～

IPsec対向側のLANに複数のセグメントがあるケースでは、従来のポリシーベースIPsecでは同一VPNピアに対して複数のIPsec SAを確立させて、各セグメント毎にipsec access-listで送信元/宛先を指定する必要がありました。
F220で従来のポリシーベースIPsecのように同一VPNピアに対して複数のIPsec SAを確立させる場合は、match address設定の設定方法が変わるため、以下で設定のポイントについて解説します。
※IKEv1のみ利用可能です

F220（ルートベースIPsec）		F200（ポリシーベースIPsec）
ip route 0.0.0.0 0.0.0.0 tunnel 1000	非暗号化対象通信用 ip route設定	ip route 0.0.0.0 0.0.0.0 pppoe 1 複数の宛先への暗号化対象通信も非暗号化対象通信(平文)もデフォルト経路を利用する
ip route 192.168.1.0 255.255.255.0 tunnel 1	暗号化対象通信1用 ip route設定	
ip route 192.168.10.0 255.255.255.0 tunnel 2	暗号化対象通信2用 ip route設定	
crypto ipsec selector SELECTOR_001		ipsec access-list 1 ipsec ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
src 1 ipv4 192.168.2.0 255.255.255.0		暗号化対象通信1の送信元/宛先を ipsec access-list で指定
dst 1 ipv4 192.168.1.0 255.255.255.0		
exit		
crypto ipsec selector SELECTOR_002		ipsec access-list 2 ipsec ip 192.168.2.0 0.0.0.255 192.168.10.0 0.0.0.255
src 1 ipv4 192.168.2.0 255.255.255.0		暗号化対象通信2の送信元/宛先を ipsec access-list で指定
dst 1 ipv4 192.168.10.0 255.255.255.0		
exit		

- IPsec対向側に複数のLANセグメントが存在する場合、ルートベースIPsecでは宛先毎に経路設定が必要です
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください
- 同一VPNピア複数のIPsec SA利用時のcrypto ipsec selector設定とmap(P2)設定との関連付け方法は次のページで解説します

ポリシーベースIPsec設定からの変換④
～同一VPNピア複数IPsec SAを利用する場合(2/2)～

F220	F200
interface Tunnel 1	interface pppoe 1
tunnel mode ipsec map KYOTEN0001 match address SELECTOR_001	crypto map KYOTEN0001
exit	exit
interface Tunnel 2	
tunnel mode ipsec map KYOTEN0001 match address SELECTOR_002	
exit	
crypto map KYOTEN0001 ipsec-isakmp	crypto map KYOTEN0001 1
~~match address SELECTOR~~	match address 1
set isakmp-profile PROF0001	set peer address 192.0.2.1
exit	
同一VPNピアに対して複数のIPsec SAを確立させる場合は crypto map 設定内では match addresss 設定は不要 ※match address 設定は各Tunnelインタフェース設定で指定する ※IKEv1のみ利用可能	crypto map KYOTEN0001 2
	match address 2
	set peer address 192.0.2.1

- ポリシーベースIPsecでは、複数のIPsec SAを確立させる場合もWAN側となる1つのインタフェースでIPsec通信が利用可能でしたが、ルートベースIPsecでは、IPsec SA毎にIPsecトンネルインタフェース設定が必要です
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください
- 同一VPNピアに対して複数のIPsec SAを確立させる場合、crypto map(P2)設定は複数設定する必要はなく、各IPsec Tunnelインタフェース設定内でmap名称を共通にして関連付けて、match address設定毎に利用するIPsecセレクタを指定します
- 次ページの注意点もご参照ください

同一VPNピア複数IPsec SA構成時の注意点

◆同一VPNピア複数IPsec SA構成時の注意点
- IKEv1のみ利用可能
- crypto ipsec selector以外のIPsecパラメータは同一設定を利用すること
- IPsecのResponderとして利用する場合に、IPsecセレクタの送信元/宛先が包含関係にないこと

OKな例

```
crypto ipsec selector SELECTOR_001
 src 1 ipv4 192.168.2.0 255.255.255.0
 dst 1 ipv4 192.168.1.0 255.255.255.0
exit

crypto ipsec selector SELECTOR_002
 src 1 ipv4 192.168.2.0 255.255.255.0
 dst 1 ipv4 192.168.10.0 255.255.255.0
exit
```

NGな例

```
crypto ipsec selector SELECTOR_001
 src 1 ipv4 192.168.2.0 255.255.255.0
 dst 1 ipv4 192.168.1.0 255.255.255.0
exit

crypto ipsec selector SELECTOR_002
 src 1 ipv4 192.168.2.0 255.255.255.0
 dst 1 ipv4 192.168.0.0 255.255.0.0      ※SELECTOR_001のdstと包含関係にある
exit
```

ポリシーベースIPsec設定からの変換⑤
～同一VPNピア複数IPsec SA+ポリシールーティング機能の併用(1/3)～

ルートベースIPsecでは暗号化対象の宛先毎に経路設定が必要ですが、同一VPNピアに対して複数のIPsec SAを確立させる構成で自身のLAN側に複数のセグメントがあるケースでは暗号化対象通信の宛先経路の重複が発生してしまう場合があります。
F220で従来のポリシーベースIPsecのように、暗号化対象通信の送信元/宛先によって使用するIPsecトンネルを振り分けるには別途ポリシールーティング機能との併用が必要となる為、以下でポリシールーティング設定のポイントについて解説します。

F220（ルートベースIPsec）	F200（ポリシーベースIPsec）
ip route 0.0.0.0 0.0.0.0 tunnel 1000　非暗号化対象通信用ip route設定	ip route 0.0.0.0 0.0.0.0 pppoe 1 送信元/宛先に関係なく暗号化対象通信も非暗号化対象通信(平文)もデフォルト経路を利用する
各暗号化対象通信用のip route設定を行うと宛先経路の重複が発生してしまう為、ip route設定は行わない。 ip route設定の代わりにポリシールーティング機能を利用して、access-list設定でポリシールーティング対象を指定する（後述）	
crypto ipsec selector SELECTOR_001	ipsec access-list 1 ipsec ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255　暗号化対象通信1の送信元/宛先は ipsec access-list で指定
src 1 ipv4 192.168.2.0 255.255.255.0	
dst 1 ipv4 192.168.1.0 255.255.255.0	
exit	
crypto ipsec selector SELECTOR_002	ipsec access-list 2 ipsec ip 192.168.20.0 0.0.0.255 192.168.1.0 0.0.0.255　暗号化対象通信2の送信元/宛先は ipsec access-list で指定
src 1 ipv4 192.168.20.0 255.255.255.0	
dst 1 ipv4 192.168.1.0 255.255.255.0	
exit	

- 同一VPNピア複数のIPsec SA利用時、LAN側に複数のLANセグメントが存在する環境で、暗号化対象通信の宛先が同じ場合は経路設定は行わない
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください
- ポリシールーティング設定については次のページで解説します

ポリシーベースIPsec設定からの変換⑥
～同一VPNピア複数IPsec SA+ポリシールーティング機能の併用(2/3)～

F220	F200
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255	ipsec access-list 1 ipsec ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.1.0 0.0.0.255	ipsec access-list 2 ipsec ip 192.168.20.0 0.0.0.255 192.168.1.0 0.0.0.255
class-map PBR_Tunnel_01	
match ip access-group 101	
exit	
class-map PBR_Tunnel_02	
match ip access-group 102	
exit	
policy-route-map PBR	
!	
class PBR_Tunnel_01	
count	
action nexthop tunnel 1	
exit	
!	
class PBR_Tunnel_02	
count	
action nexthop tunnel 2	
exit	
!	
exit	

ip route設定の代わりにaccess-list設定でポリシールーティング対象とする送信元/宛先を指定してポリシールーティング設定のclass-mapでmatch ip access-group設定と紐づける
暗号対象通信1用：access-list 101 中継先 Tunnel 1
暗号対象通信2用：access-list 102 中継先 Tunnel 2

ポリシールーティング設定
LAN側物理IF（GigaEthernet 1/x）のpolicy-route input設定と紐づける名称を指定

class-map設定とclass設定を紐づける

count設定によりポリシールーティングにmatchした統計情報が確認可能
show policy-route statistics interface gigaethernet 1/1

ポリシールーティングの中継先として
tunnel 1を指定

class-map設定とclass設定を紐づける

ポリシールーティングの中継先として
tunnel 2を指定

ポリシーベースIPsec設定からの変換⑦
～同一VPNピア複数IPsec SA+ポリシールーティング機能の併用(3/3)～

F220	F200
interface Tunnel 1	interface pppoe 1
tunnel mode ipsec map KYOTEN0001 match address SELECTOR_001	crypto map KYOTEN0001
exit	exit
interface Tunnel 2	
tunnel mode ipsec map KYOTEN0001 match address SELECTOR_002	
exit	
crypto map KYOTEN0001 ipsec-isakmp	crypto map KYOTEN0001 1
set isakmp-profile PROF0001	match address 1
exit	set peer address 192.0.2.1
interface GigaEthernet 1/1	crypto map KYOTEN0001 2
vlan-id 1	match address 2
bridge-group 1	set peer address 192.0.2.1
channel-group 1	
policy-route input PBR	
exit	

interface GigaEthernet 1/1～1/8 で共通設定

ポリシールーティング機能を利用する LAN側物理IF（GigaEthernet 1/x） で policy-route-map設定と紐づける名称を指定

- 上記例では、LAN側物理IF(GE1/1)で受信する各access-listで指定した条件に一致した通信がポリシールーティングの対象となります。
  - 送信元：192.168.2.0/24、宛先：192.168.1.0/24 に該当する通信はIPsec Tunnel 1へ中継
  - 送信元：192.168.20.0/24、宛先：192.168.1.0/24 に該当する通信はIPsec Tunnel 2へ中継
- policy-route input設定を設定できるのは1つのインタフェースにつき1つだけです
- profile(P1)とpolicy(P1/P2) 設定については、本資料の「IPsecの設定①～③」を参照してください

PPPoEの設定(NAT/学習Filtering/ProxyDNS)

F220	F200
ip route 0.0.0.0 0.0.0.0 tunnel 1	ip route 0.0.0.0 0.0.0.0 pppoe 1
ip nat list 1 192.168.0.0 0.0.0.255	access-list 1 permit 192.168.0.0 0.0.0.255
access-list 111 deny ip any any	access-list 111 deny ip any any
access-list 121 spi ip any any	access-list 121 dynamic permit any any
pppoe profile PPPOE_PROF	
account user@xxxx.ne.jp secret	
exit	
interface tunnel 1	interface pppoe 1
tunnel mode pppoe profile PPPOE_PROF	pppoe account user@xxxx.ne.jp secret
	pppoe type host
pppoe interface gigaethernet 2/1	pppoe interface ewan 1
ip nat inside source list 1 interface	ip nat inside source list 1 interface
ip access-group 111 in	ip access-group 111 in
ip access-group 121 out	ip access-group 121 out
exit	exit
interface GigaEthernet 2/1	
vlan-id 2	
bridge-group 2	
pppoe enable	
exit	
dns-server ip enable	proxydns mode v4
proxydns domain 1 any * any ipcp tunnel 1	

pppoeはtunnelに変更

学習フィルタリングはdynamic→spi

PPPoEのアカウント情報はprofileで指定

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

ip nat list番号を指定

物理インタフェースの指定は必須

IPv4のDNSサーバ機能の有効化

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)

F220	F200
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	interface lan 1
ip address 192.168.0.1 255.255.255.0	ip address 192.168.0.1 255.255.255.0
ip dhcp service server DHCPサーバ有効化(IF毎に設定)	
ip dhcp server-profile lan1	
exit	exit
	service dhcp-server DHCPサーバ有効化(装置全体)
ip dhcp server-profile lan1	ip dhcp pool lan 1 IF名を指定
address 192.168.0.101 192.168.0.254 払出しアドレスの範囲を指定	allocate-address 192.168.0.101 154 払出しアドレスの先頭と数を指定
dns 192.168.0.1	dns-server 192.168.0.1
gateway 192.168.0.1	default-router 192.168.0.1
lease-time 28800 払出しアドレス有効時間を秒単位で指定	lease-time 0 8 払出しアドレス有効時間を<日><時><秒>で指定
exit	exit

profileを指定

※dns, gatewayに0.0.0.0指定はできません

snmp(MIB/Trap)およびsntpクライアント

F220	F200
snmp-server community public ro	snmp-server community public ro
snmp-server contact admin	snmp-server contact admin
snmp-server name FITELnet-F220-1	snmp-server name FITELnet-F200-1
snmp-server location Tokyo	snmp-server location Tokyo
snmp-server enable traps	snmp-server enable traps
snmp-server host 192.168.0.150 public v2c	snmp-server host 192.168.0.150 public v2c
!	!
sntp server 192.168.0.100	sntp server 192.168.0.100
sntp poll-interval 86400 sntpの問い合わせ間隔を秒単位で指定 (F220は必ず装置起動時に問い合わせをするため、F200のboot有と同じ動作です)	sntp schedule boot interval 24 sntpの問い合わせ間隔を時間単位で指定

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。F200でも出力可能）
  - logging buffer（F220内部バッファに出力。F200ではelog,vpnlog等種別毎にあったが、F220では一つ）
  - logging console（コンソールに出力。F200では出力不可）
  - logging telnet（telnetに出力。F200では出力不可）

- syslogで送信されるファシリティについて
  - F200：syslog facilityで指定した値で送信されます(デフォルトは1)
  - F220：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F200同様に指定した値で送信することができます

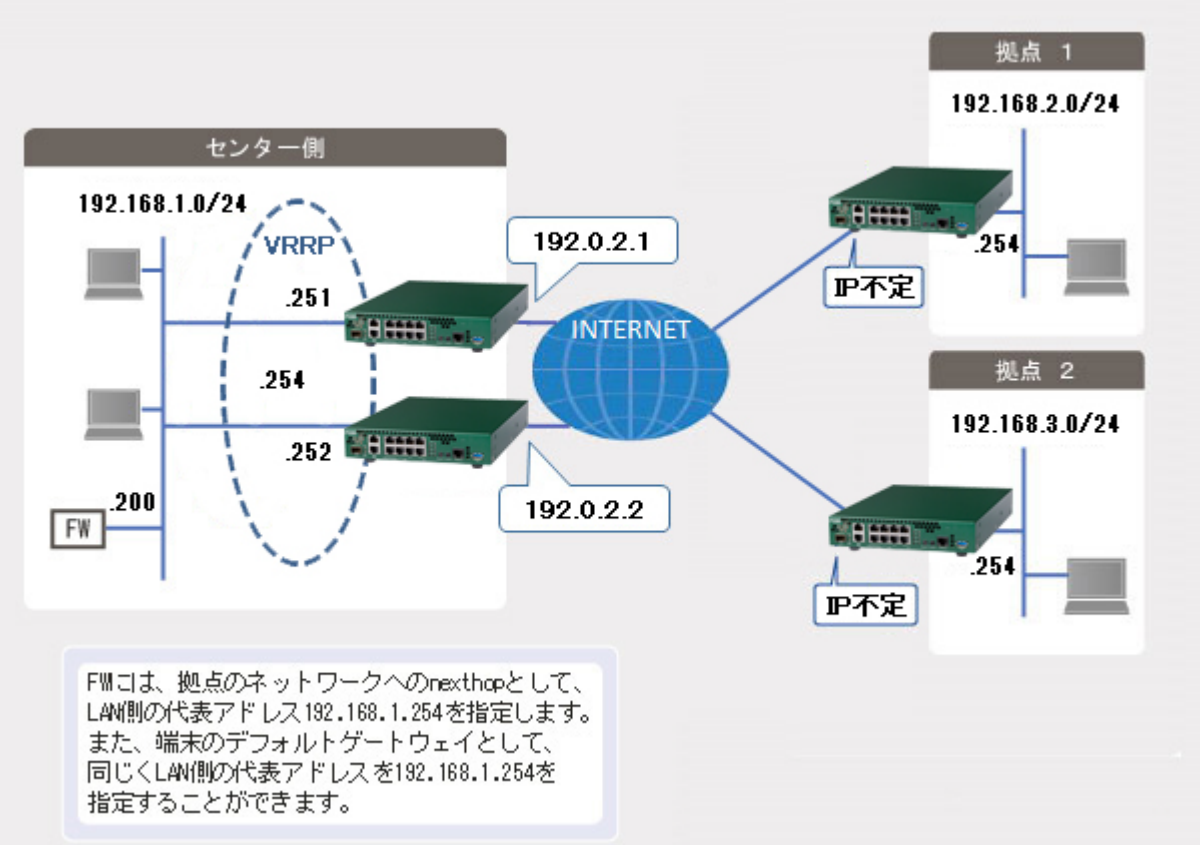
- syslogで送信されるレベルについて
  - F200：logging-level <ログ種別>で種別(elog,vpnlog等)毎にレベルを変更できます
  - F220：ログ毎にレベルが異なります(メッセージ集に記載)

  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	F200
logging host 192.168.0.3	syslog server 192.168.0.3 syslog level 6 informational(6)以上のログをsyslogサーバへ出力 (F200内部バッファへはレベルに関係なくに出力)
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	F200はclass/action/mapに分かれていましたが、F220はevent一action内にevent/action両方設定します
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	

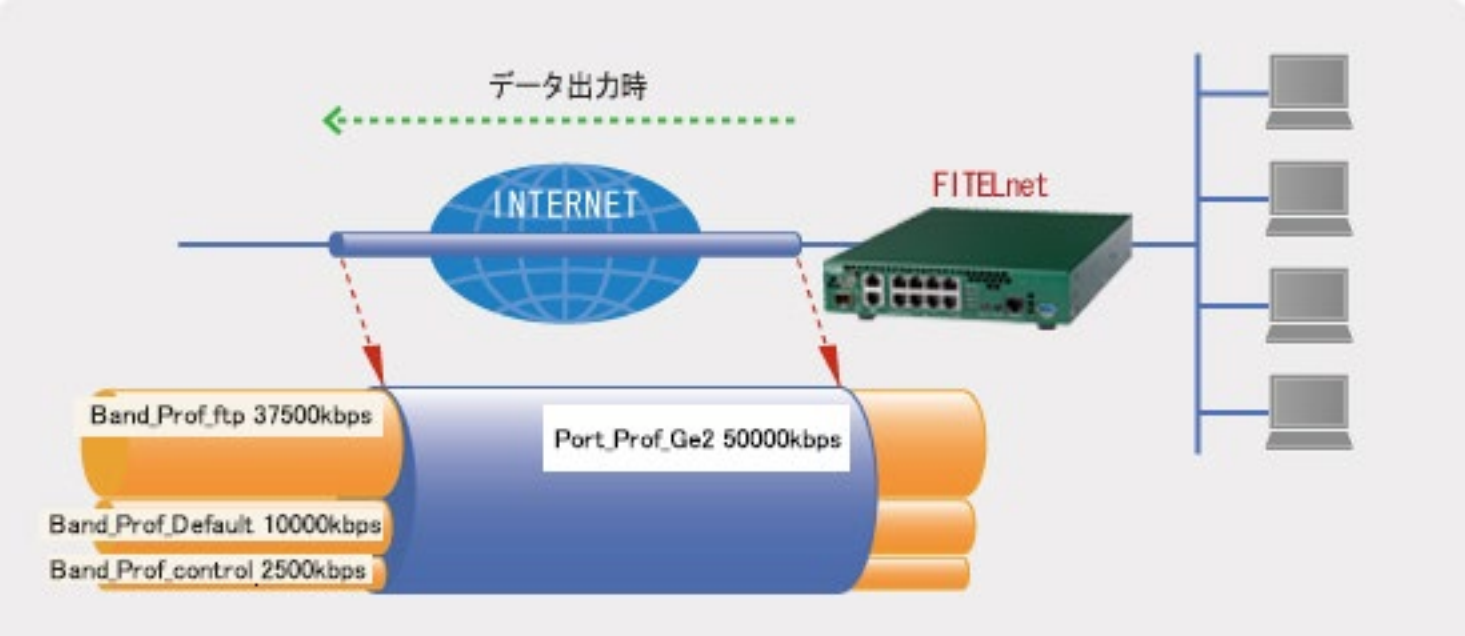
1系のVRRP状態がinitializeとなることで、
2系のVRRP状態がmasterとなる

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	

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