パケットトレーサで学ぶNW構築
（基礎編）

④　VPN（IPSEC）で通信の内容を暗号化してみよう！！

お　品　書　き

１　構成の確認

２　VPN（IPSEC）通信の基礎

３　ルータ間でVPN（IPSEC）を構成してみよう！

４　参考
（1）VPN（IPSEC）不具合時の確認POINT！
（2）SPANを利用した通信の補足

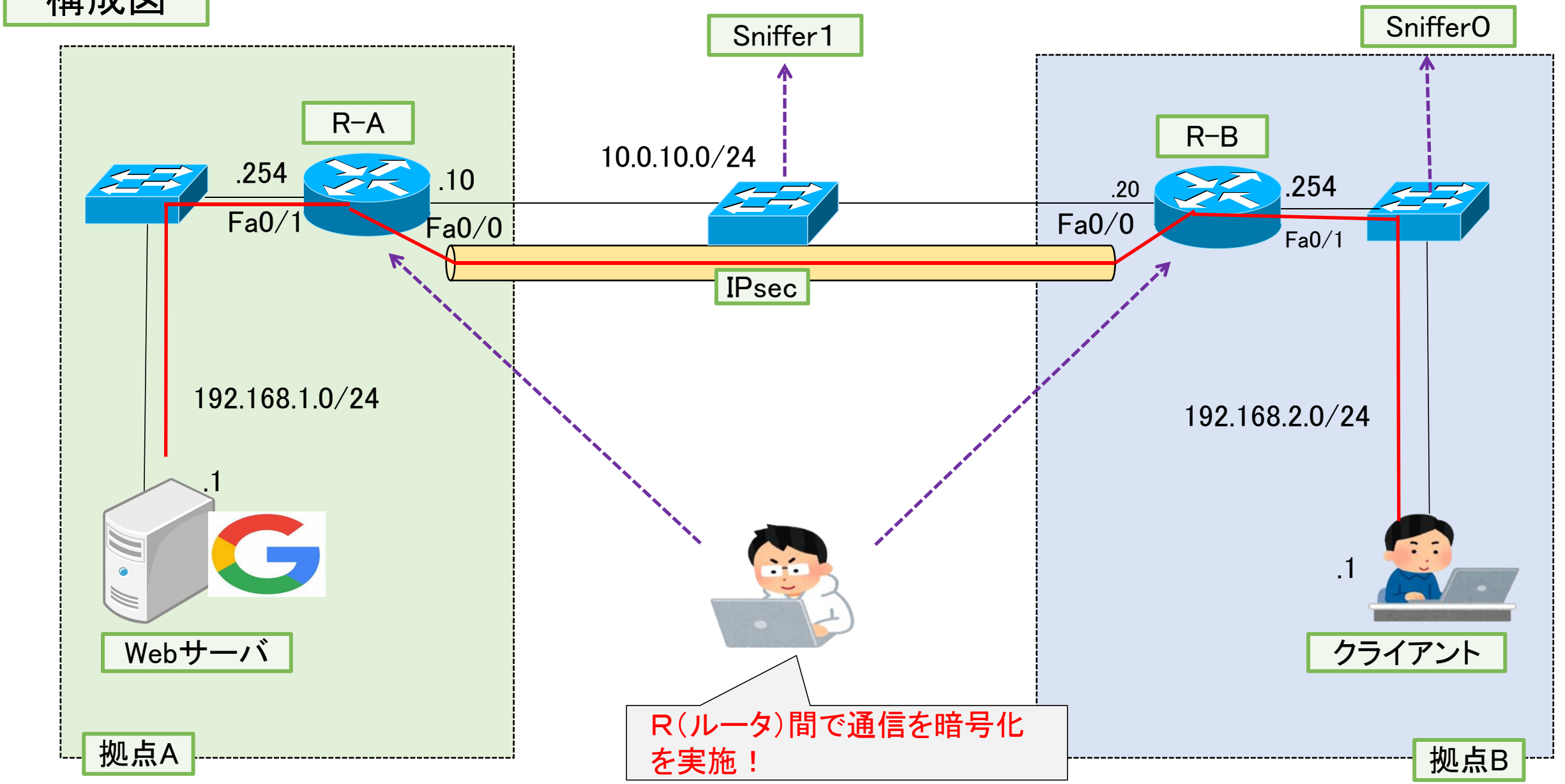
参考サイト：ネットワークエンジニアとして（IPSECをはじめから）
https://www.infraexpert.com/study/study10.html

使用する実習ファイルはNO.4.pktになります！

1 構成の確認

1　構成の確認

構成図

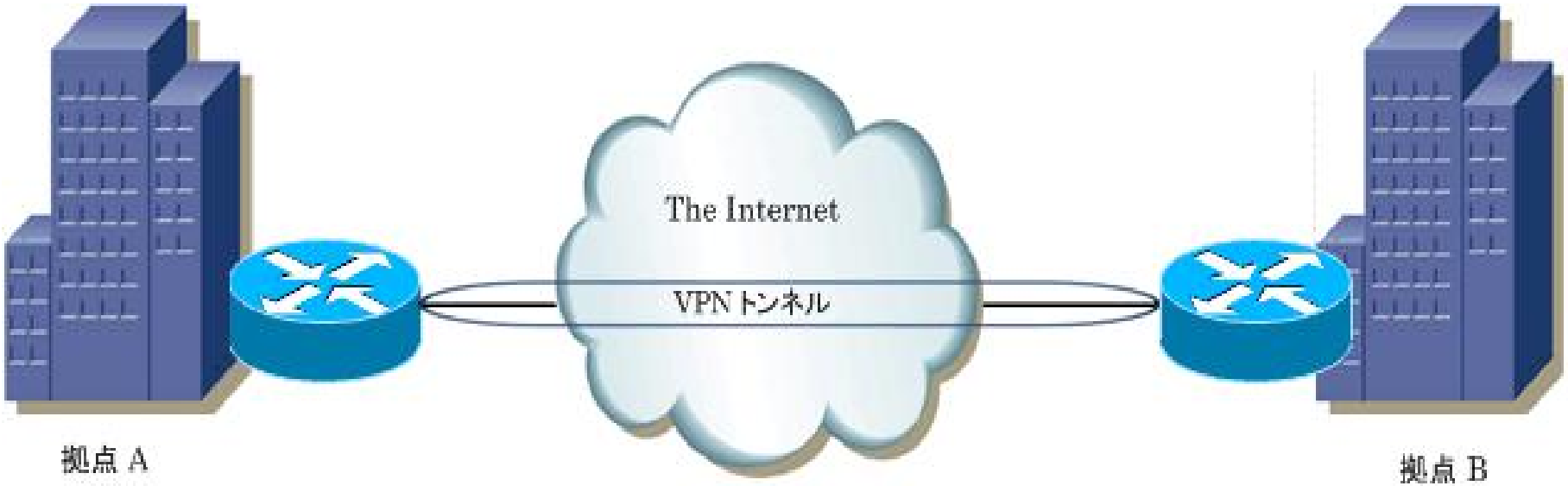

Sniffer1
SnifferO
R-A
R-B
10.0.10.0/24
.254
.10
Fa0/1
Fa0/0
.20
.254
Fa0/0
Fa0/1
IPsec
192.168.1.0/24
192.168.2.0/24
.1
.1
Webサーバ
クライアント
R（ルータ）間で通信を暗号化を実施！
拠点A
拠点B

２　VPN(IPSEC)通信の基礎

2　VPN（IPSEC）通信の基礎

【VPNとは？？】

VPN（Virtual Private Network）とは、仮想的なプライベートネットワーク接続のことです。VPNによりインターネットなどの公衆網を利用する場合でも、IPsec等の高度なセキュリティを実装させられるので、安全に企業の拠点間通信を実現できます。また、安価なFTTHの広帯域な回線をWANとして利用できます。



出典：ネットワークエンジニアとして（VPNとは？？）
https://www.infraexpert.com/study/ipsec.html

２　VPN（IPSEC）通信の基礎

【VPNの種類】

VPNはインターネットVPNとIP-VPNの大きく2つに分類できます。

インターネットVPN
：インターネットなどの公衆網を利用したVPN

IP-VPN
：通信事業者が提供するクローズドなIPネットワークを利用したVPN
（MPLS技術を採用されることが多い）

インターネットVPNには2種類があります。

IPsec-VPN：セキュリティプロトコルにIPsecを使用したVPN

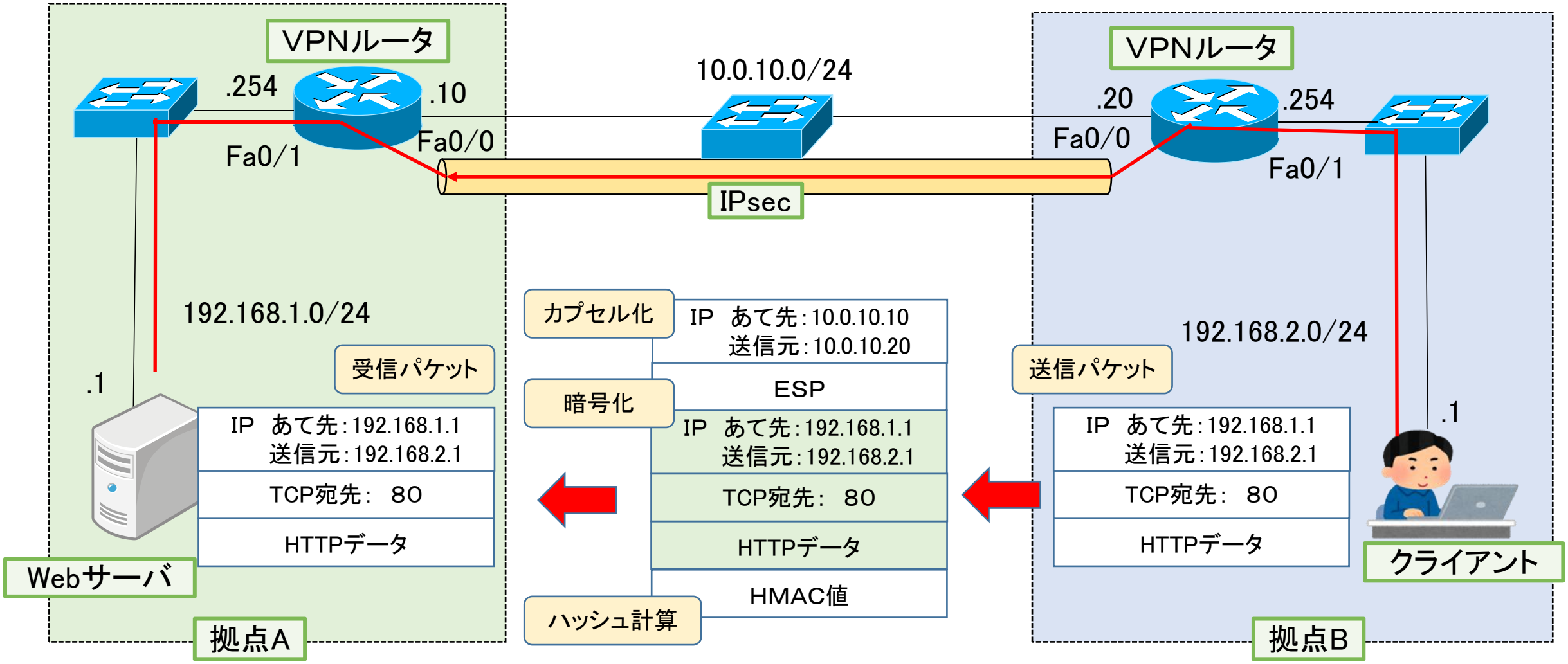
SSL-VPN：セキュリティプロトコルにSSLを使用したVPN

今回はIPSECを利用したVPNについて説明します！

2　VPN（IPSEC）通信の基礎

【IPSEC動作の流れ】

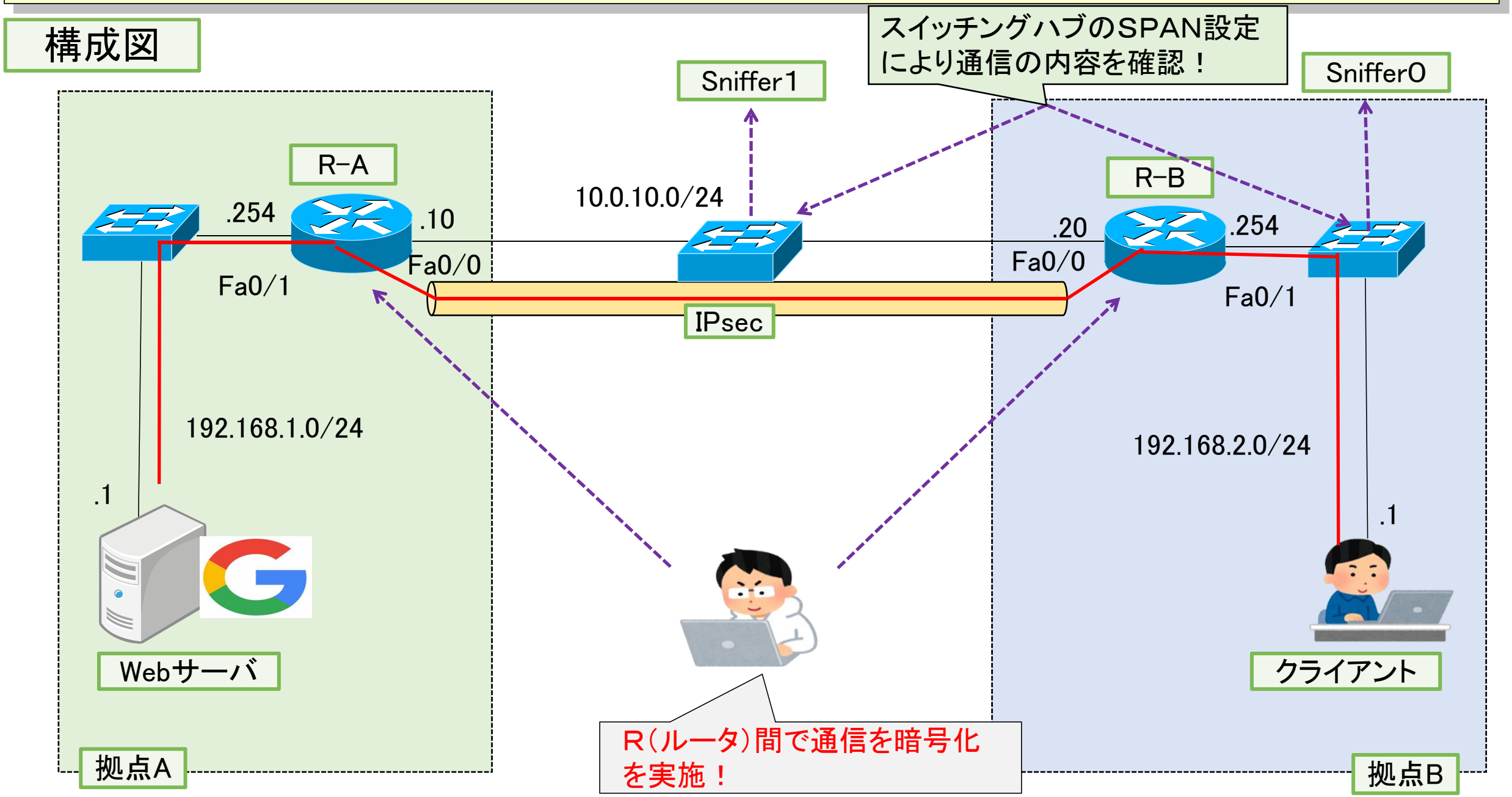
ルータ（VPNルータ）同士で暗号化したパケットをやりとりします。
ルータはパケットのカプセル化、暗号化、改ざんの検証を実施します！



３　ルータ間でVPN（IPSEC）を構成してみよう！

3　ルータ間でVPN（IPSEC）を構成してみましょう！

構成図



３　ルータ間でVPN（IPSEC）を構成してみましょう！

【設定及び確認内容】

① 各ルータにNW及びルーティング（StaticRoute）の設定をします

② IPSEC設定に必要な以下の条件を設定します。
　ア　フェーズ1 ISAKMP設定
　イ　フェーズ2 生成されたISAKMP SAでIPsec SAを生成

③ 設定後、ルータ区間が暗号化されているかを確認します。
　○　show crypto isakmp sa でIKEフェーズ１の状態を確認しましょう
　○　show crypto ipsec sa でIKEフェーズ２の状態を確認しましょう

④ クライアント～サーバ間の通信時のパケットをSnifferで確認してみましょう！

３　ルータ間でVPN（IPSEC）を構成してみましょう！

【設定内容】

R-A　の場合

② IPSEC設定に必要な以下の条件を設定します。　　ア　フェーズ1 ISAKMP設定

```
crypto isakmp policy 10
        /  ISAKMP SAを生成するためのポリシー設定(数値が低いほど優先度高)
encryption aes 256
        /  暗号化アルゴリズムの設定
hash sha
        /ハッシュアルゴリズムの設定
authentication pre-share      /  認証方式の設定
group 2                       /  グループの設定
lifetime 86400                /  ISAKMP SAのライフタイムの設定
crypto isakmp key TEST1 address 10.0.0.20
        /  (pre-share)ハッシュアルゴリズムにおいて事前共有鍵を指定した場合、
           対向先との事前共有鍵を設定
```

３　ルータ間でVPN（IPSEC）を構成してみましょう！

【設定内容】

R-A　の場合

② IPSEC設定に必要な以下の条件を設定します。

イ　フェーズ2 生成されたISAKMP SAでIPsec SAを生成

/　セキュリティプロトコル＋暗号化(esp-aes)＋認証(esp-sha-hmac)で設定する

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
```

/　IPsecの対象となる送信先と宛先のアクセスリストを設定する

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

３　ルータ間でVPN（IPSEC）を構成してみましょう！

【設定内容】

R-A　の場合

② IPSEC設定に必要な以下の条件を設定します。

イ　フェーズ2 生成されたISAKMP SAでIPsec SAを生成

/　CyptoMap設定

```
crypto map CMAP 10 ipsec-isakmp       /暗号マップ（crypto map）の設定
set peer 10.0.10.20                   /対抗先(RouterB)のアドレスの設定
match address 101                     /暗号マップに関連付けるアクセスリスト(101)の設定
set transform-set TSET                /暗号マップに関連付けるIPsecトランスフォームの設定
```

/　VPNルータの対向インターフェース（fa0/0）でCyptoMapを有効化

```
int fa0/0
crypto map CMAP
```

3　ルータ間でVPN（IPSEC）を構成してみましょう！

【IPSEC設定まとめ】

R-A　の場合

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp key TEST1 address 10.0.10.20
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.10.20
 set transform-set TSET
 match address 101
!
interface FastEthernet0/0
 crypto map CMAP
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

事前共有鍵：
対向のルータと同じにします！

IPSEC時の暗号化及び
crypto mapに割り当て

crypto mapを
インタフェースに割り当て

暗号化対象NWを
crypto mapに割り当て

３　ルータ間でVPN（IPSEC）を構成してみましょう！

③　設定後、ルータ区間が暗号化されているかを確認します。

○　show crypto isakmp sa でIKEフェーズ１の状態を確認しましょう

・端末が通信する前にコマンドを打ってみましょう！

PINGで通信していない場合は　表示されません

・端末間で通信した後にコマンドを打ってみましょう！

それでも表示されない場合。。

Routing設定及びアクセスリストを確認しましょう！

○　show crypto ipsec sa でIKEフェーズ２の状態を確認しましょう

パケットが暗号化/復号化された数を知ることができます

○　今回は使用できませんが。。（パケットトレーサではコマンドなし。。）

show crypto engine connection active で暗号/復号された

パケット数を確認できます

端末間で通信しながら
ルータのコマンドを打って
確認してみましょう！！

３　ルータ間でVPN（IPSEC）を構成してみましょう！

③　設定後、ルータ区間が暗号化されているかを確認します。

○　show crypto isakmp sa でIKEフェーズ1の状態を確認しましょう

【PING送信前】

```
R-A#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

何も表示されません。。

```
R-A#show access-lists
Extended IP access list 101
    10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

ACLのカウンタ
も上がりません。。

３　ルータ間でVPN（IPSEC）を構成してみましょう！

③　設定後、ルータ区間が暗号化されているかを確認します。

○　show crypto isakmp sa でIKEフェーズ1の状態を確認しましょう

【PING送信後】

```
R-A#show access-lists
Extended IP access list 101
    10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 (1 match(es))

R-A#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.10.20      10.0.10.10      QM_IDLE           1058    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

ルータ配下の端末から送信
された場合はカウンタが上がります

”QM__IDLE” となれば
フェース1は確立されています

細部は　４　VPN（IPSEC）不具合時の確認POINT！！を確認してください～

3　ルータ間でVPN（IPSEC）を構成してみましょう！

③　設定後、ルータ区間が暗号化されているかを確認します。

○　show crypto ipsec sa でIKEフェーズ2の状態を確認しましょう

【PING送信後】

```
R-A#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: CMAP, local addr 10.0.10.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 10.0.10.20 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
   #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.10.10, remote crypto endpt.:10.0.10.20
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x07E39734(132355892)
```

encrypto：暗号化された数
decrypto：復号化された数
が表示されていればOK！

3　ルータ間でVPN（IPSEC）を構成してみましょう！

③　設定後、ルータ区間が暗号化されているかを確認します。

○　show crypto ipsec sa でIKEフェーズ2の状態を確認しましょう

【PING送信後】

○　フェーズ2での接続状況の詳細を確認することができます！

```
local crypto endpt.: 10.0.10.10, remote crypto endpt.:10.0.10.20
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x07E39734(132355892)

inbound esp sas:
 spi: 0x7D2B36C4(2099984068)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2008, flow_id: FPGA:1, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4525504/1417)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x07E39734(132355892)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2009, flow_id: FPGA:1, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4525504/1417)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE
```

ESPの入力側

ESPの出力側

３　ルータ間でVPN（IPSEC）を構成してみましょう！

○　PING送信時の注意点

ルータ間のVPN（IPSEC）が確立される前はPINGが成功しません～

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

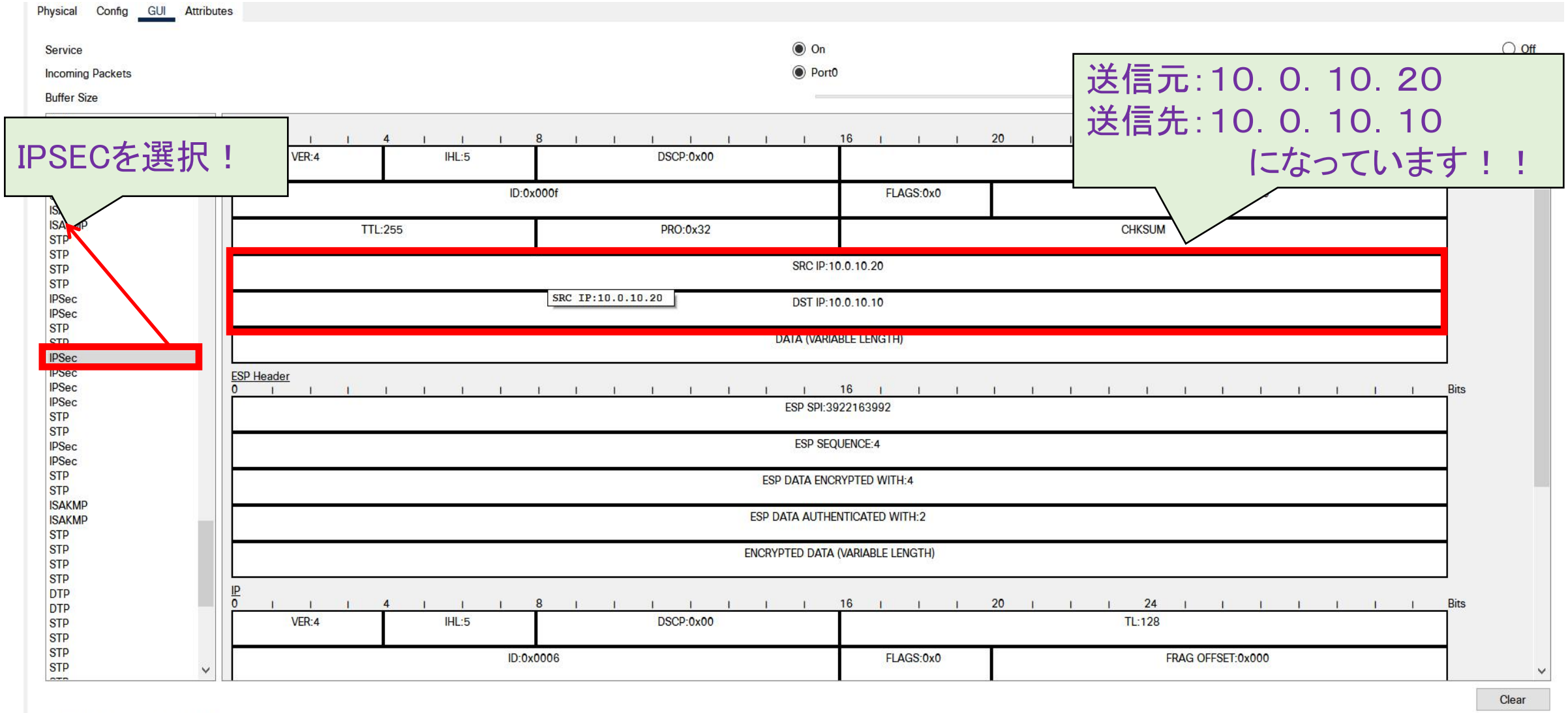
IPSec未確立の場合は
PINGに失敗します・・

ルータ間のVPN（IPSEC）が確立された場合ははPINGが全て成功します！

3　ルータ間でVPN（IPSEC）を構成してみましょう！

④　クライアント～サーバ間の通信時のパケットをSnifferで確認してみましょう！

Snifferでの確認結果（クライアント　→　サーバ　にPING実施）



３　ルータ間でVPN（IPSEC）を構成してみましょう！

研究：拠点AのSWにSniffer2を設置して、通信の中身を確認してみましょう！

手順

SWにログインしてSPAN設定を実施します。
Sniffer2を設置します。
Sniffer2のFilter設定を実施します。
拠点Bから拠点Aに対して通信を実施し、流れている通信を確認してみましょう！

注意：今回、接続するSW（Catalist2950）はAUTO-MDI/MDI-X非対応のため、Snifferを接続する際はクロスケーブルを使用してください！！

４　　参　　考

（1） IPSEC不具合時の確認POINT！！

4　参考

（1） IPSEC不具合時の確認POINT！！

・以下3つのパターンについて紹介します

◇ Pattern 1

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                 src                 state          conn-id status
```

◇ Pattern 2 （失敗）

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                 src                 state          conn-id status
11.11.111.111       22.22.222.222       MM_NO_STATE          0 ACTIVE
```

◇ Pattern 3 （成功）

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                 src                 state          conn-id status
11.11.111.111       22.22.222.222       QM_IDLE           1001 ACTIVE
```

（出典）

ネットワークエンジニアのメモ　IPsec-VPN：MM_NO_STATEとQM_IDLEの原因と解決策

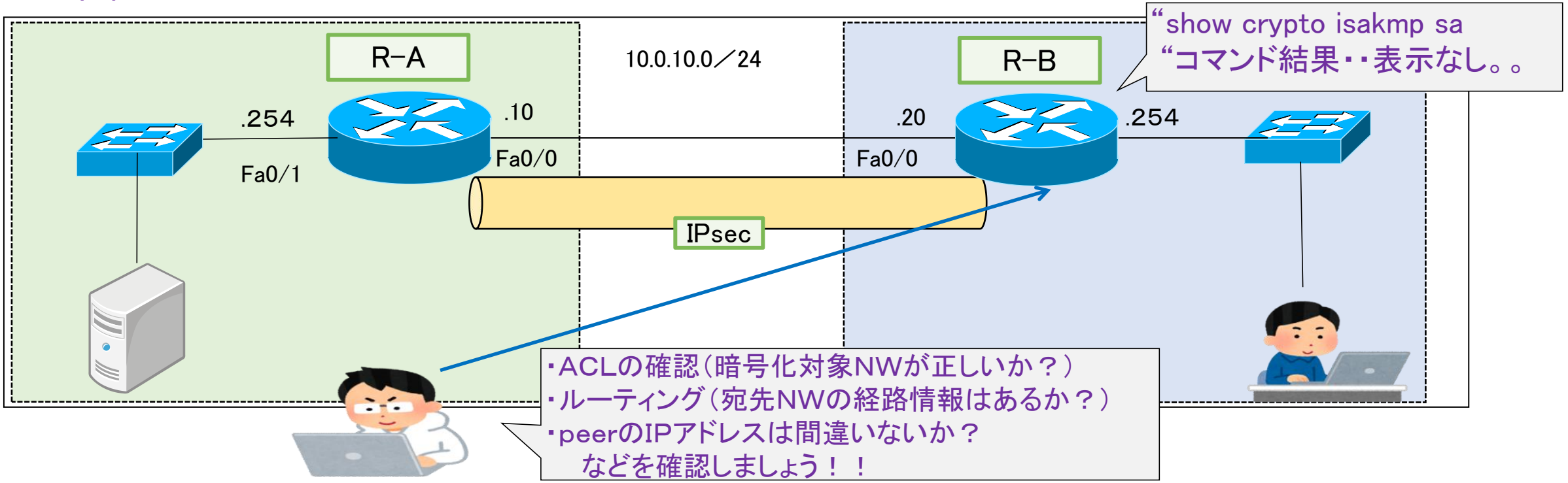
https://www.infraeye.com/2018/04/04/network035/

4　参考

（1） IPSEC不具合時の確認POINT！！

（パターン1）

ステータスに何も表示されないケース。このステータスはIPsec通信が行われていない状態を意味します。つまり、end-to-endで通信が行われていない状態であるためPCから対向拠点のPCに対してPINGなどで通信を行ってみましょう。それでも、何も表示されていない場合にはIPsec対象のACL設定ミス、ルーティング設定ミスである可能性が高いです。【あとisakmp peerのアドレス（IPSEC終端ルータ）が間違っているなど。。】



４　参　考

（１） IPSEC不具合時の確認POINT！！

（パターン2）
ステータスにMM_NO_STATEと表示されるケース。このステータスはIKEフェーズ1の失敗を意味します。IPsec-VPN接続を行う両方のルータでIKEフェーズ1の設定に間違いがないかどうかを確認しましょう。例えば、Pre-shared Key（crypto isakmp key）の設定が両端のルータで同じ値なのかを確認してみましょう。また、ACLの設定が原因である可能性もあるので障害切り分けのために、ACLを外したり、一時的に緩いACLに変更して問題を切りわけましょう。
この問題はルータの再起動によって解決する事例も報告されており、MM_NO_STATE（失敗）ステータスから、QM_IDLE（成功）ステータスに遷移してくれる場合もあります。

（パターン3）
ステータスにQM_IDLEと表示されるケース。このステータスは、IKEフェーズ1の成功を意味します。従って、現状のIKEフェーズ1の設定は正しいことを意味するので、IPsec-VPN接続の通信が正常に行えない場合は、IKEフェーズ1ではなくて、IKEフェーズ2の設定に問題があることを意味します

４　　参　　考

（２） SPANポートを使用した通信の補足

４　参　考

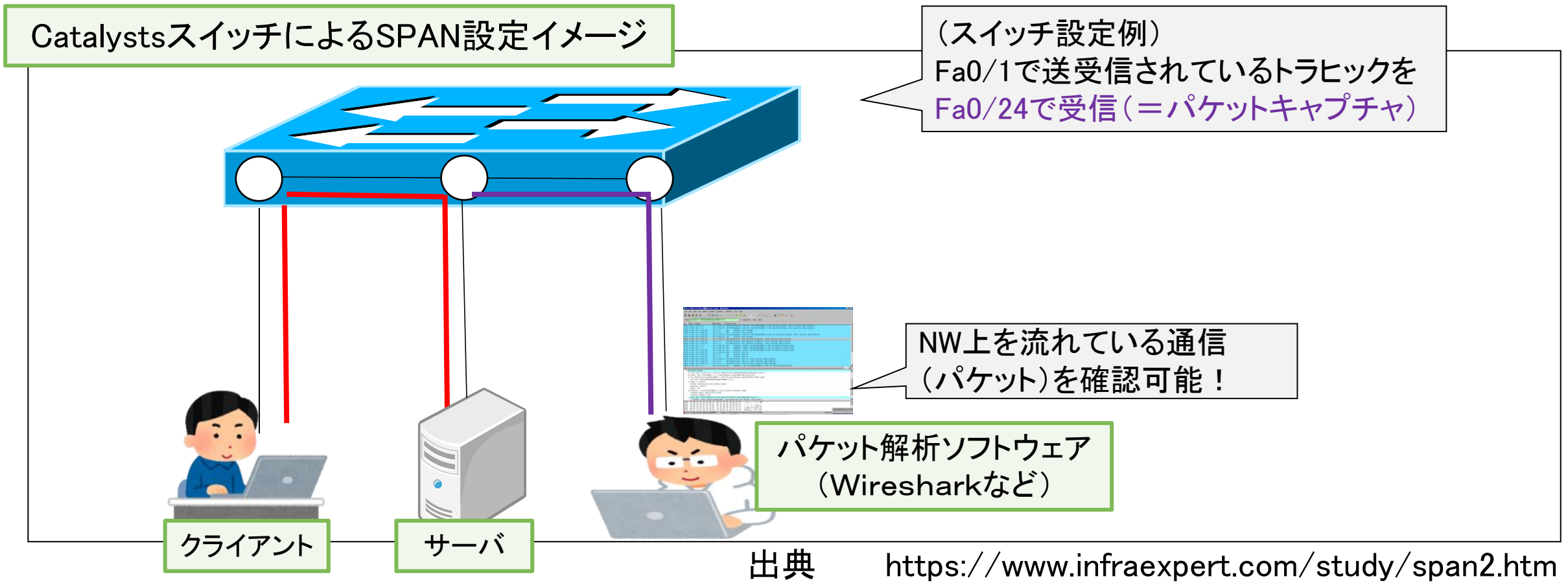
(2)　SPANポートを使用した通信の確認

SPAN（Switched Port Analyzer）とは？？

パケットキャプチャを行う際にスイッチに実装するミラーリング機能のことです。

Catalystスイッチではポート上またはVLAN上を流れるトラフィックを、SPANを利用することによりトラフィック（パケット）のコピーを送信できます。

CatalystsスイッチによるSPAN設定イメージ



出典　https://www.infraexpert.com/study/span2.htm

4 参 考

(2) SPANポートを使用した通信の確認

設定例

【設定コマンド】

```
SW-1#show tun
SW-1#show running-config | in
SW-1#show running-config | include monitor
monitor session 1 source interface Fa0/2
monitor session 1 destination interface Fa0/24
SW-1#
```

【設定後の確認コマンド】

```
SW-1#show monitor session all
Session 1
---------
Type                   : Local Session
Description            : -
Source Ports           :
    Both               : Fa0/2
Destination Ports      : Fa0/24
    Encapsulation      : Native
          Ingress      : Disabled


SW-1#
```