IPsec VPN トラブルシューティング ラボ v1.1

Cisco ASA および IOS デバイス上の LAN-to-LAN IPsec VPN 接続のトラブルシューティング

最終更新日:2017 年 12 月 04 日

このラボについて

この事前設定済みラボのガイドには、次の内容が含まれています。

要件

次の表に、このラボの要件を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect

このソリューションについて

このラボでは、ASA と IOS デバイス上で、LAN-to-LAN IPsec VPN 接続が稼働している場合に使用できるトラブルシューティング技術について説明します。この技術は、シスコ テクニカル サポートが解決したサービス リクエストから直接得られたものです。これらの手法の多くは、IPsec VPN 接続について詳細なトラブルシューティングを行う前に実施することができます。そのため、このラボ セッションには、Cisco TAC に連絡する前に IPSec VPN 接続をトラブルシューティングするために実施すべき、一般的な手順についてのチェックリストが用意されています。

前提条件

IPsec をベースとした VPN テクノロジーについての知識

IOS デバイスおよび ASA デバイスのトラブルシューティングに関する基礎的な経験

免責事項

このトレーニング ドキュメントは、LAN-to-LAN IPSec VPN トンネルのトラブルシューティングするためのアプローチを理解することを目的としています。このラボの設計および設定例は参考として利用するためのものであり、実際の設計ではありません。そのため推奨されている機能の一部が使用されていなかったり、最適な状態で有効化されていなかったりします。設計に関する質問については、シスコの担当者、またはシスコ パートナーまでお問い合わせください。

Cisco Live の関連セッション

Cisco Live では、以下のような VPN テクノロジーに関する有意義なセッションも行われます。

TECSEC-3725：Advanced Remote Access and Site-to-Site VPN design with IOS（IOS を使用した高度なリモート アクセスおよびサイト間 VPN の設計）

LTRSEC-3004：Advanced IOS IPSec VPN with FlexVPN hands-on Lab（FlexVPN を使用した高度な IOS IPSec VPN についてのハンズオンラボ）

BRKSEC-3054：IOS FlexVPN Remote Access, IoT and Site-to-Site advanced Crypto VPN Designs（IOS FlexVPN のリモート アクセス、IoT およびサイト間の高度な暗号化 VPN の設計）

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ(Topology)] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. 論理トポロジ

セッション ユーザ

以下の表には、指定されたデバイス上でのセッションで使用可能な、事前設定済みユーザについての詳細が記載されています。

各デバイスにアクセスするには、ホストから PuTTY クライアントを使用します。

表 2. ユーザの詳細

デバイス名	ユーザ名およびパスワード	イネーブル パスワード
ASAv	admin/C1sco12345	C1sco12345
router-10	admin/C1sco12345	
router-20	admin/C1sco12345	
Host	administrator/C1sco12345	

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る]

注:セッションがアクティブになるまで最長で 10 分かかることがあります。

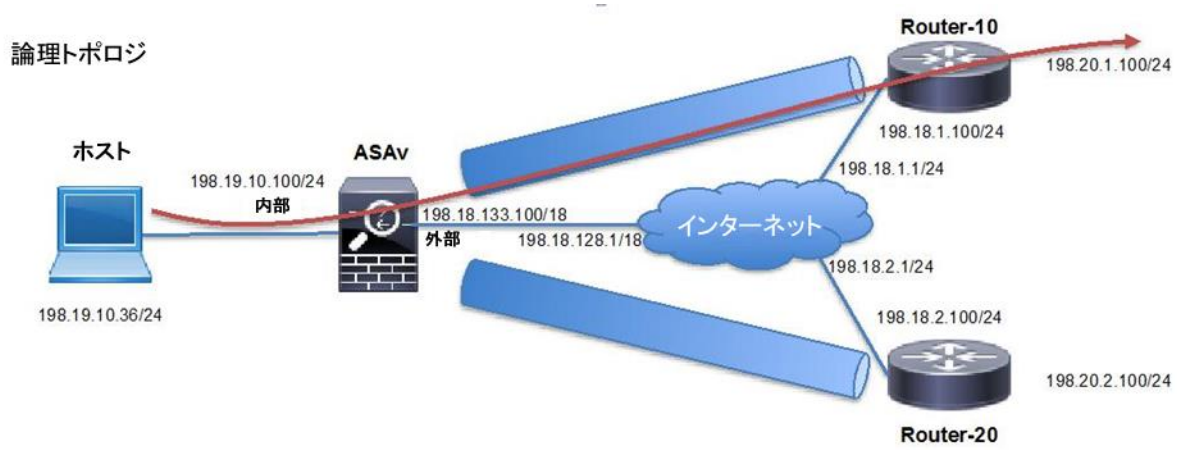
2. 最適なパフォーマンスを得るために、**Cisco AnyConnect VPN** [手順を見る] およびラップトップの**ローカル RDP クライアント** [手順を見る] を使用してワークステーションに接続します。

   ワークステーション 1:**198.18.133.36**、ユーザ名:**administrator**、パスワード:**C1sco12345**

注:Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] 。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。

シナリオ 1.　ASA の内側にあるホストから Router-10 の内側にあるサブネットへのトラフィックが発生しない

図 2.　ネットワーク構成図



問題の詳細

ネットワーク管理者が、IKEv1 IPSec LAN-to-LAN VPN トンネルを使用して、本社の ASA ファイアウォールに 2 つの新しいサイトを接続しました。この接続で、問題がいくつか発生しています。最初の問題は、ASA（198.19.10.100/24）の背後のサブネットと、Router-10 のロケーション（198.20.1.0/24）の内側にあるサブネットとの間が接続できていないことです。

注：次の手順は、詳細なトラブルシューティング フローを示すものです。答えを確認する前に問題を自分でトラブルシューティングしてみる場合は、設定を変更する際に十分注意してください。実際の環境をできるだけ忠実に再現するために、デバイスへの接続はコンソールを経由していないためです。

手順

1. ホストから Router-10 のループバック（設定をシンプル化するために、router-10 および router-20 の両方でループバック インターフェイスによって LAN サブネットをシミュレーションしています）への連続 ping を開始します。

暗号マップ ベースの IPSec LAN-to-LAN トンネルが、インタレスティング トラフィックによって開始されます。トラフィックが発生しない場合、VPN トンネルがダウンしていると推測されます。トラブルシューティングを開始する前に、以下のようにして、インタレスティング トラフィックが連続で送信されていることを確認します。

```
C:\Users\Administrator>ping 198.20.1.100 -t

Pinging 198.20.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
```

注:トラフィックが送信元と宛先の間で連続して送信されるようにすることで、トラフィックの開始元であるホストに戻らずに、接続を簡単にトラブルシューティングすることができます。これにより、特にパケット サイズのようなパラメータなどを含む、トラフィックの送信元と宛先を制御することも可能です。

2. ASA の内部インターフェイスで、trace detail オプションを指定してパケット キャプチャを設定します。

注:ASA およびその他のデバイスにログインするには、PuTTY クライアントを使用します(各デバイス用に保存されたセッションがあります)。クレデンシャルは、このガイドの始めにある表に記載されています。デフォルトでは、すべてのデバイスで admin/C1sco12345 です。

ASA の内部インターフェイスでパケット キャプチャを設定することで、ファイアウォールの内部インターフェイスにトラフィックが到達しているかどうかを確認できるようになります(トラフィックが確認できない場合、次のステップは LAN 接続のトラブルシューティングになります)。

```
ASAv# capture IN interface inside trace detail match icmp host 198.19.10.36 host 198.20.1.100
ASAv# show capture
capture IN type raw-data trace detail interface inside [Capturing - 90 bytes]
  match icmp host 198.19.10.36 host 198.20.1.100
```

注:trace detail オプションにより、キャプチャされたパケットが ASA のパケット トレーサ機能と同様の方法でトレースされます。これにより、ルーティング、NAT、ドロップの可能性など、実際のパケットの処理を把握できるようになります。

3. 収集されたパケット キャプチャを表示し、確認します。

```
ASAv# show capture IN

4 packets captured

   1: 10:36:34.608473198.19.10.36 > 198.20.1.100: icmp: echo request
   2: 10:36:39.608672198.19.10.36 > 198.20.1.100: icmp: echo request
   3: 10:36:44.608916198.19.10.36 > 198.20.1.100: icmp: echo request
   4: 10:36:49.608183 198.19.10.36 > 198.20.1.100: icmp: echo request 4
packets shown
```

注:ICMP の echo request パケットは、ASA の内部インターフェイスで受信されています。ただし、応答が返されていません。

特定のパケットが ASA によってどのように処理されているかを検証し、トラフィックが正常に暗号化されて、リモートの VPN ピアに送信されているかどうかを確認します。そのためには、キャプチャで有効化された trace detail オプションを使用します(出力の一部は省略されています)。

```
ASAv# show capture IN packet-number 1 trace detail

5 packets captured

   1: 10:36:34.608473 0050.56a9.4d95 0050.56a9.448f 0x0800 Length: 74
      198.19.10.36 > 198.20.1.100: icmp: echo request (ttl 128, id 8829)
[…]

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 198.18.128.1 using egress ifc outside
```

```
Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static LAN_NETWORK LAN_NETWORK destination static 110_NETWORK 110_NETWORK
no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 198.20.1.100/0 to 198.20.1.100/0

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static LAN_NETWORK LAN_NETWORK destination static 110_NETWORK 110_NETWORK no-
proxy-arp route-lookup
Additional Information:
Static translate 198.19.10.36/1 to 198.19.10.36/1
 Forward Flow based lookup yields rule:
 in  id=0x7f13bda43ee0, priority=6, domain=nat, deny=false
        hits=49, user_data=0x7f13bda317c0, cs_id=0x0, flags=0x0, protocol=0 src
        ip/id=198.19.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=198.20.1.0, mask=255.255.255.0, port=0, tag=any,
        dscp=0x0 input_ifc=inside, output_ifc=outside

[…]

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f13be1905d0, priority=70, domain=encrypt, deny=false
        hits=49, user_data=0x3894, cs_id=0x7f13bdf890e0, reverse, flags=0x0,
        protocol=0 src ip/id=198.19.10.0, mask=255.255.255.0, port=0, tag=any
        dst ip/id=198.20.1.0, mask=255.255.255.0, port=0, tag=any,
        dscp=0x0 input_ifc=any, output_ifc=outside

[…]

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

1 packet shown
ASAv#
```

注: 上記の出力から、このトラフィックは UN-NAT および NAT の両方の対象になっていることがわかります。UN-NAT および NAT には、この VPN トラフィックに NAT を適用しないようにする役割があります。これは多くの環境において、トラフィックを外部のインターフェイス IP に PAT 処理しないようにするために必要です。

出力の後半部分では、トラフィックが暗号化されています(これは、このトラフィックの暗号化を行う VPN トンネル(特に IPSec Phase2)が有効になっていることも示しています)。最終的な結果は allow(許可)であり、正しい出力インターフェイス(外部)が使用されています。

4. ASAv の show crypto ipsec sa の出力で encaps/decaps のカウンタを確認します。

show crypto ipsec sa の出力で encaps/decaps のカウンタを確認することで、トラフィックが正しく暗号化され、VPN ピアに送信されているかどうかも確認できます。

```
ASAv# show crypto ipsec sa peer 198.18.1.100 | i ident|caps:
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
      #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
ASAv#
ASAv#
ASAv# show crypto ipsec sa peer 198.18.1.100 | i ident|caps:
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
      #pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 13
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
ASAv#
```

注: 上記の出力を複数回収集することで、カウンタが増加していることを確認できます。カウンタが増加していることを確認するには、出力を収集する間隔を 5 秒以上にすることが必要です。Windows では、5 秒がデフォルトの ICMP タイムアウトであるためです。

注目すべきなのは、encaps/encrypt/digest のカウンタが増加している(これは出力トラフィックを表します)一方で、リターン トラフィック(decaps/decrypt/verify)がないことです。これは、リモート ピアでの状況を確認する必要があることを示しています。

5. router-10 での show crypto ipsec sa 出力の encaps/decaps カウンタを確認します。

```
router-10#show crypto ipsec sa peer 198.18.133.100 | i ident|caps
   local ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   local  ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 22
router-10#
router-10#
router-10#
router-10#show crypto ipsec sa peer 198.18.133.100 | i ident|caps
   local ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

```
   local  ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 23, #pkts decrypt: 23, #pkts verify: 23
router-10#
```

注: 上記の出力から、トラフィックが受信されていることがわかります。ただし、リターン トラフィックがありません。

6. router-10 で、ASAv の内側にあるサブネットへのルーティングをチェックします。

ICMP トラフィックの開始元であるホストへのルーティングをチェックし、GigabitEthernet2 インターフェイス経由でルーティングしていることを確認します。

```
router-10#show ip route 198.19.10.36
Routing entry for 198.19.10.0/24
  Known via "ospf 1", distance 110, metric 21, type intra area
  Last update from 198.18.1.1 on GigabitEthernet2, 00:39:36 ago
  Routing Descriptor Blocks:
  * 198.18.1.1, from 198.19.10.100, 00:39:36 ago, via
      GigabitEthernet2 Route metric is 21, traffic share count is 1
```

暗号マップは GigabitEthernet2 に適用されており、ルーティングの観点では問題がないように思われます。

```
router-10#sh run int gi2
Building configuration...

Current configuration : 123 bytes
!
interface GigabitEthernet2
 ip address 198.18.1.100 255.255.255.0
 ip nat outside
 negotiation auto
 crypto map VPN
end
```

7. トラフィックを暗号化しないようにしている可能性がある他の機能がないか、確認します。

指定されたトラフィックに対して IPSec SA が稼働している場合、フローに対して有効化されている特定の機能が原因で、そのトラフィックが暗号化されない、またはドロップされている可能性があります。最も一般的な機能としては、NAT、PBR、ZBF があります。

アクティブな NAT 変換をチェックして、ICMP フローが変換されていることを確認します。

```
router-10#sh ip nat translations icmp
Pro  Inside global         Inside local          Outside local         Outside global
icmp 198.18.1.100:1        198.20.1.100:1        198.19.10.36:1        198.19.10.36:1
Total number of translations: 1
```

注: NAT は暗号化の前に実行されるため、インタレスティング トラフィックが NAT 変換処理の対象となった場合、暗号化が失敗する可能性があります。

ダイナミック NAT が設定されており、変換するトラフィックが route-map で定義されています。

```
router-10#show running-config | section nat
 ip nat inside
 ip nat outside
ip nat inside source route-map nonat interface GigabitEthernet2 overload
route-map nonat permit 10
 match ip address 111
router-10#sh access-lists 111
Extended IP access list 111
    10 deny ip 198.20.1.0 0.0.0.255 198.20.2.0 0.0.0.255
    20 permit ip 198.20.1.0 0.0.0.255 any
router-10
```

注: 上記の設定ではトラフィックが NAT 処理されるため、暗号化に失敗します。NAT 処理は暗号化前に発生します。つまり、暗号マップが評価されたときに、このトラフィックがインタレスティング トラフィックに一致しないということです。

この問題を修正するために、access-list 111 に VPN トラフィックの拒否ルールを追加します。

```
router-10#conf t
router-10(config)#ip access-list extended 111
router-10(config-ext-nacl)#5 deny ip 198.20.1.0 0.0.0.255 198.19.10.0 0.0.0.255
router-10(config-ext-nacl)#end
```

このトラフィックはまだ機能しない可能性があります。既存のアクティブな接続が存在するためです。以下のように NAT 変換をクリアして、トラフィックが流れるようにします（これはラボ環境であるため、すべてのエントリがクリアされますが、実際のシナリオでは条件を設定します）。

```
router-10#clear ip nat translation *
```

8. router-10 で encaps カウンタが増えていることを確認します。

NAT 非適用を追加すると encaps が増加しますが、連続 ping はまだ成功しません。

注: ping が引き続き失敗していても、5 秒のタイムアウトとカウンタの変更は続いていることに注意してください。

```
router-10#show crypto ipsec sa peer 198.18.133.100 | i ident|caps
   local ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   local ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
    #pkts decaps: 46, #pkts decrypt: 46, #pkts verify: 46 router-
10#show crypto ipsec sa peer 198.18.133.100 | i ident|caps
   local ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   local       ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
    #pkts encaps: 12, #pkts encrypt: 12, #pkts digest: 12
    #pkts decaps: 47, #pkts decrypt: 47, #pkts verify: 47
router-10#
```

クライアント マシンで ping は引き続きタイム アウトになります。

```
Request timed out.
Request timed out.
Request timed out.
```

9. トラフィックが ASA で復号されており、内部セグメントに転送されていることを確認します。

トラフィックは ASA で受信されています。

```
ASAv# show crypto ipsec sa peer 198.18.1.100 | i ident|caps:
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
      #pkts encaps: 55, #pkts encrypt: 55, #pkts digest: 55
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
ASAv#
```

内部インターフェイスでのキャプチャをクリアして、確認します。

```
ASAv# clear cap IN

[10 秒後]

ASAv# sh cap IN

2 packets captured

   1: 11:17:59.588409198.19.10.36 > 198.20.1.100: icmp: echo request
   2: 11:18:04.589508 198.19.10.36 > 198.20.1.100: icmp: echo request 2
packets shown
ASAv#
```

ICMP エコーの応答が内部インターフェイスで確認できないことがわかります。

10. 暗号化された受信トラフィックに対して、trace detail オプションを指定してパケット キャプチャを設定し、フローの状態を確認します。

```
ASAv# capture OUT interface outside trace detail match ip host 198.18.133.100 host 198.18.1.100
```

注: 暗号化されたトラフィックのキャプチャでは内部トラフィック（暗号化されている）をフィルタ処理できないため、実際の環境では、もっと多数のトラフィックが存在します。この場合、ping のパケット サイズを変更すると効果的です。たとえば 1,000 バイトに設定します。Windows での ICMP タイムアウトが 5 秒であることがわかっているので、5 秒ごとにサイズが「1,000 バイト + IPsec オーバーヘッド」のパケットが送信されると想定されます。

正確な IPsec オーバーヘッドを計算するには、*https://cway.cisco.com/tools/ipsec-overhead-calc/* のツールを使用します。

ping を変更して、パケット長を 1,000 バイトに設定します。

```
C:\Users\Administrator>ping 198.20.1.100 -t -l 1000

Pinging 198.20.1.100 with 1000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

キャプチャ内の暗号化された ICMP パケット サイズは 1076 バイトです。

```
ASAv# show capture OUT

44 packets captured

   1: 11:19:09.588211198.18.133.100 > 198.18.1.100:          ip-proto-50, length 100
   2: 11:19:09.589202198.18.1.100 > 198.18.133.100:          ip-proto-50, length 100
   […]
  13: 11:19:39.588836198.18.133.100 > 198.18.1.100:          ip-proto-50, length 100
  14: 11:19:39.590011198.18.1.100 > 198.18.133.100:          ip-proto-50, length 100
  15: 11:19:47.153541198.18.133.100 > 198.18.1.100:          ip-proto-50, length 1076
  16: 11:19:47.154670198.18.1.100 > 198.18.133.100:          ip-proto-50, length 1076
  17: 11:19:52.088511198.18.133.100 > 198.18.1.100:          ip-proto-50, length 1076
[…]
```

暗号化された ICMP 着信応答に関する詳細なトレース情報を表示します（出力の一部は省略されています）。

注:トレースしなければならないパケット数は毎回異なる可能性があるため、長さ 1076 バイトの着信パケットを見つけます。

```
ASAv# show capture OUT packet-number 16 trace detail

90 packets captured

  16: 11:19:47.154670 0050.5600.0001 0050.56a9.a495 0x0800 Length: 1110
      198.18.1.100 > 198.18.133.100:  ip-proto-50, length 1076 (ttl 254, id 136)
[…]

Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
in   id=0x7f13bda2d2f0, priority=1, domain=permit, deny=false
     hits=30781, user_data=0x0, cs_id=0x0, l3_type=0x8 src
     mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000
        input_ifc=outside, output_ifc=any

Phase: 6
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 198.19.10.36 using egress ifc inside

Phase: 7
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static LAN_NETWORK LAN_NETWORK destination static 110_NETWORK 110_NETWORK
no-proxy-arp route-lookup
```

```
Additional Information:
NAT divert to egress interface inside
Untranslate 198.19.10.36/1 to 198.19.10.36/1

Phase: 8
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f13bda54ac0, priority=11, domain=permit, deny=true
        hits=563, user_data=0x6, cs_id=0x0, use_real_addr, flags=0x0,
        protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=outside, output_ifc=any

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule


1 packet shown
```

このトラフィックは ACL によってドロップされています。ASA ファイアウォールでは、デフォルトで VPN トラフィックが許可されるので、これは予期されていない動作です。この動作を変更するオプションがあります。

次の手順として、デフォルト動作の変更点を確認します。

```
ASAv# sh running-config sysopt
no sysopt connection permit-vpn
```

デフォルト設定は「sysopt connection permit-vpn」ですが、変更されています。ソリューションとしては、設定変更をロール バックするか、インバウンド方向の外部 ACL でトラフィックを許可します。

```
ASAv# conf t
ASAv(config)# sysopt connection permit-vpn
ASAv(config)#
```

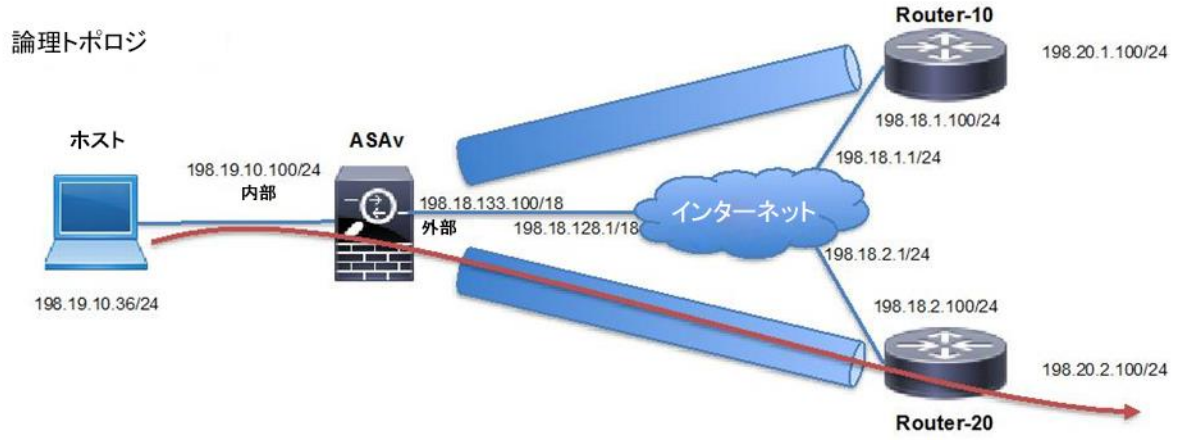
変更後、トラフィックは正常に通過するようになります。

```
Request timed out.
Request timed out.
Request timed out.
Reply from 198.20.1.100: bytes=1000 time=2ms TTL=255
Reply from 198.20.1.100: bytes=1000 time=2ms TTL=255
Reply from 198.20.1.100: bytes=1000 time=2ms TTL=255
Reply from 198.20.1.100: bytes=1000 time=2ms TTL=255
```

sysopt connection permit-vpn の詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s17.html#pgfId-1567918 [英語] を参照してください。

シナリオ 2.　ASAv と Router-20 の間のトンネルを開始できない

図 3.　ネットワーク構成図



問題の詳細

ローカルのホストと Router-10 間のネットワークを修正しましたが、ローカルのホストと Router-20 のサイト間の到達可能性に関してまだいくつか問題が残っています。トラフィックが ASA またはルータ エンドのどちらで開始されている場合でも、トンネルが確立されません。

注：次の手順は、詳細なトラブルシューティング フローを示すものです。答えを確認する前に問題を自分でトラブルシューティングしてみる場合は、設定を変更する際に十分注意してください。実際の環境をできるだけ忠実に再現するために、デバイスへの接続はコンソールを経由していないためです。

手順

1.　packet-tracer の detail コマンドを使用して ASA からトンネルを開始します。

ASA ファイアウォールに達するインタレスティング トラフィックがない場合は、packet-tracer を使用して VPN トンネルをトリガーすることができます。トンネルを開始するために、packet-tracer を 2 回実行します。

注：packet-tracer の最初の結果は常にドロップになります。これは、最初のパケットが消費されて、トンネルを開始するために使用されるからです。トンネルが正しく確立されたか（ALLOW）されなかったか（DROP）を確認できるのは、2 回目にコマンドを実行した場合です。

```
ASAv# packet-tracer input inside icmp 198.19.10.36 8 0 198.20.2.100 detail

[…]

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static LAN_NETWORK LAN_NETWORK destination static 220_NETWORK 220_NETWORK
```

```
no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 198.20.2.100/0 to 198.20.2.100/0

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static LAN_NETWORK LAN_NETWORK destination static 220_NETWORK 220_NETWORK
no-proxy-arp route-lookup
Additional Information:
Static translate 198.19.10.36/0 to 198.10.36/0
 Forward Flow based lookup yields rule:
 in  id=0x7fdfa9a4e000, priority=6, domain=nat, deny=false
    hits=0, user_data=0x7fdfa93e3810, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=198.19.10.0, mask=255.255.255.0, port=0, tag=any
    dst ip/id=198.20.2.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=outside

[…]

Phase: 8
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7fdfaa018420, priority=70, domain=encrypt, deny=false
        hits=1, user_data=0x0, cs_id=0x7fdfa919e520, reverse, flags=0x0, protocol=0
    src ip/id=198.19.10.0,    mask=255.255.255.0, port=0, tag=any
    dst ip/id=198.20.2.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=outside


Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule
```

同じ出力を 2 回実行しても、結果は引き続き DROP になります。

```
[…]

Phase: 7
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
 Forward Flow based lookup yields rule:
```

```
 out id=0x7fdfaa018420, priority=70, domain=encrypt, deny=false
     hits=2, user_data=0x0, cs_id=0x7fdfa919e520, reverse, flags=0x0, protocol=0
     src ip/id=198.19.10.0, mask=255.255.255.0, port=0, tag=any
     dst ip/id=198.20.2.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
     input_ifc=any, output_ifc=outside

Result:
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

結果は DROP になりましたが、IKEv1 Phase1 のステータスを確認することは常に重要です。問題についてのヒントを確認できるためです。

2. ASA と Router-20 の間の IKEv1 Phase 1 のステータスを確認します。

注: 以下の出力は短時間しか表示されません。適切な出力を表示するためには、前の手順を繰り返して、再度トンネルをトリガーしなければならない可能性があります。

ASA で Phase1 を確認します。

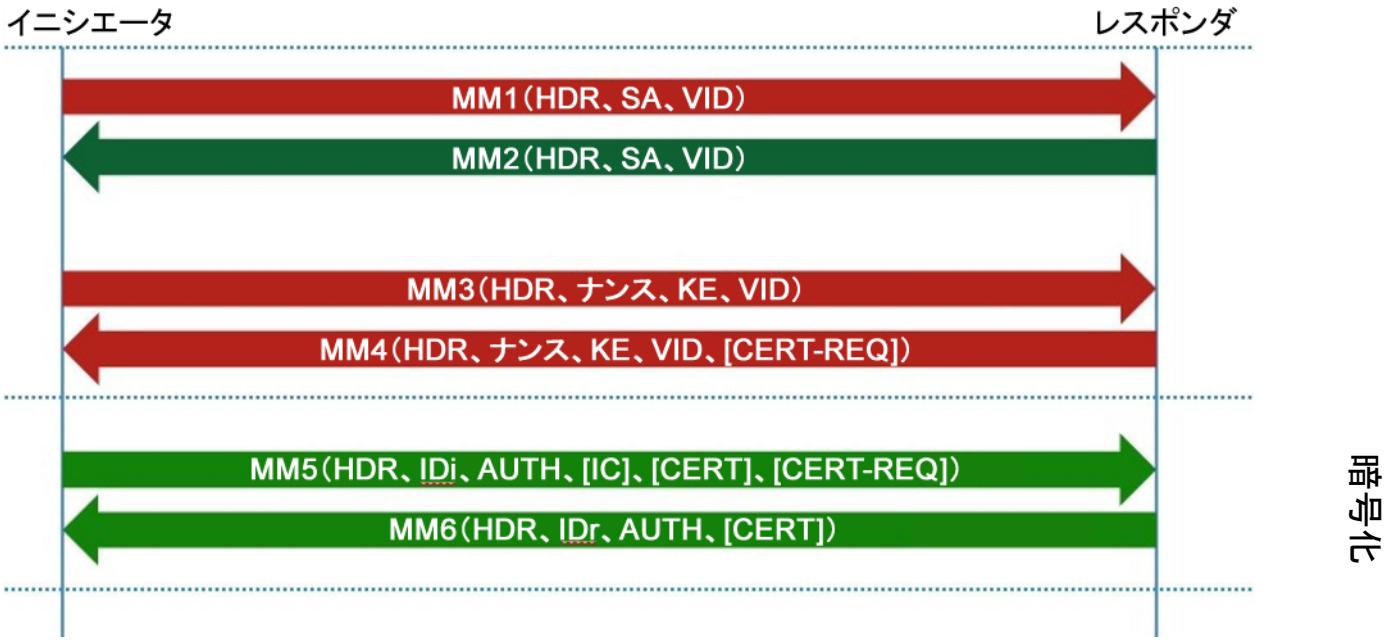
```
ASAv# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 198.18.2.100
    Type     : L2L             Role    : initiator
    Rekey    : no              State   : MM_WAIT_MSG6
```

IOS ルータで Phase1 を確認します。

```
router-20#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
198.18.2.100    198.18.133.100  MM_KEY_EXCH       1004 ACTIVE
```

MM5 が送信されたあと、ASA は router-20 からの MM6 メッセージを待機しています。router-20 は MM_KEY_EXCH 状態にあります。つまり ASA から受信した MM5 に問題があるということです。IKEv1 の Phase 1 のパケット フローを詳しく確認して、トンネルに関して考えられる問題について検証します。

図 4. パッケージ交換



IKEv1 のパケット交換で、MM5 は暗号化される最初のメッセージです。暗号化は、事前共有キーに基づいて生成することもできる共有秘密キーを使用して実行されます。これまでの情報に基づくと、事前共有キーが両端で異なっている可能性があります。

3. トンネルの両端で、事前共有キーを確認します。

```
router-20#sh running-config | section crypto isakmp
key crypto isakmp key c1sco address 198.18.133.100

ASAv# more system:running-config | beginning tunnel-group
198.18.2.100 tunnel-group 198.18.2.100 type ipsec-l2l tunnel-group
198.18.2.100 ipsec-attributes
 ikev1 pre-shared-key cisco
```

両端の事前共有キーが一致していません。以下のようにして、この状態を修正します。

```
router-20#conf t
Enter configuration commands, one per line.End with CNTL/Z.
router-20(config)#no crypto isakmp key c1sco address 198.18.133.100
router-20(config)#crypto isakmp key cisco address 198.18.133.100
```

4. packet-tracer の detail コマンドを使用して ASA からトンネルを開始します。

トンネルを開始するために、packet-tracer を 2 回実行します。

```
ASAv# packet-tracer input inside icmp 198.19.10.36 8 0 198.20.2.100 detail

[…]

Phase: 7
Type: VPN
Subtype: encrypt
Result: DROP
Config:
```

```
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f199603c820, priority=70, domain=encrypt, deny=false
    hits=3, user_data=0x0, cs_id=0x7f19960214e0, reverse, flags=0x0, protocol=0 src ip/id=198.19.10.36,
    mask=255.255.255.255, port=0, tag=any
    dst ip/id=198.20.2.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=outside
```

結果は引き続き DROP ですが、Phase 1 および Phase 2 のステータスを確認することが重要です。

注: 以下の出力は短時間しか表示されません。適切な出力を表示するためには、前の手順を繰り返して、再度トンネルをトリガーしなければならない可能性があります。

```
ASAv# show crypto isakmp sa

 IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1

1    IKE Peer: 198.18.2.100
     Type    : L2L            Role    : initiator
     Rekey   : no             State   : MM ACTIVE
```

```
ASAv# show crypto ipsec sa peer 198.18.2.100

There are no ipsec sas for peer 198.18.2.100
```

```
router-20#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
198.18.2.100    198.18.133.100  QM_IDLE           1006 ACTIVE
```

Phase 1 は機能していますが、2 は機能していません。

5. 問題の根本原因を見つけるために、両方のデバイスでデバッグを開始します。

両方の VPN ピアで debug を有効にし、トンネルの確立に関する詳細を確認します。

```
ASAv# debug crypto ikev1 127
ASAv# debug crypto ipsec 127
```

```
router-20#debug crypto isakmp
Crypto ISAKMP debugging is on
router-20#debug crypto ipsec
Crypto IPSEC debugging is on
router-20#terminal monitor
```

次の手順として、前の手順の packet-tracer を再度実行し、「undebug all」を実行して debug を無効にします。

ASA の debug 結果を以下に示します（出力の一部は省略されています）。

```
[…]

Jan 16 00:11:39 [IKEv1]Group = 198.18.2.100, IP = 198.18.2.100, PHASE 1 COMPLETED
Jan 16 00:11:39 [IKEv1]IP = 198.18.2.100, Keep-alive type for this connection: DPD
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, Starting P1 rekey timer:
82080 seconds.
Jan 16 00:11:39 [IKEv1]Group = 198.18.2.100, IP = 198.18.2.100, Add to IKEv1 Tunnel Table succeeded for
SA with logical ID 12288
Jan 16 00:11:39 [IKEv1]Group = 198.18.2.100, IP = 198.18.2.100, Add to IKEv1 MIB Table succeeded for SA
with logical ID 12288
IPSEC: New embryonic SA created @ 0x00007fdfa9313310,
    SCB: 0xAA13CF50,
    Direction: inbound
    SPI      : 0x7A371738
    Session ID: 0x00003000
    VPIF num   : 0x00000003
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, IKE got SPI from key engine: SPI =
0x7a371738
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, oakley constucting quick mode
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, constructing blank hash payload
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, constructing IPSec SA payload
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, constructing IPSec nonce payload
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, constructing proxy ID Jan 16
00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, Transmitting Proxy Id:
  Local subnet:  198.19.10.0  mask 255.255.255.0 Protocol 0 Port 0
  Remote subnet: 198.20.2.0   Mask 255.255.255.0 Protocol 0 Port 0
Jan 16 00:11:39 [IKEv1 DECODE]Group = 198.18.2.100, IP = 198.18.2.100, IKE Initiator sending
Initial Contact
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, constructing qm hash payload
Jan 16 00:11:39 [IKEv1 DECODE]Group = 198.18.2.100, IP = 198.18.2.100, IKE Initiator sending 1st QM pkt:
msg id = 3db9df89
Jan 16 00:11:39 [IKEv1]IP = 198.18.2.100, IKE_DECODE SENDING Message (msgid=3db9df89) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 16 00:11:39 [IKEv1]IKE Receiver: Packet received on 198.18.133.100:500 from 198.18.2.100:500
Jan 16 00:11:39 [IKEv1]IP = 198.18.2.100, IKE_DECODE RECEIVED Message (msgid=95331c7c) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
Jan 16 00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, processing hash payload Jan 16
00:11:39 [IKEv1 DEBUG]Group = 198.18.2.100, IP = 198.18.2.100, processing notify payload
Jan 16 00:11:39 [IKEv1]Group = 198.18.2.100, IP = 198.18.2.100, Received non-routine Notify message: No
proposal chosen (14)
```

Router-20 のデバッグ結果を以下に示します（出力の一部は省略されています）。

```
[…]

*Jan 16 00:16:10.308: ISAKMP:(1008):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Jan 16 00:16:10.308: ISAKMP:(1008):Old State = IKE_P1_COMPLETE    New State = IKE_P1_COMPLETE

*Jan 16 00:16:10.310: ISAKMP (1008): received packet from 198.18.133.100 dport 500 sport 500 Global (R)
QM_IDLE
*Jan 16 00:16:10.310: ISAKMP: set new node 1916387846 to QM_IDLE
*Jan 16 00:16:10.310: ISAKMP:(1008): processing HASH payload. message ID = 1916387846
*Jan 16 00:16:10.310: ISAKMP:(1008): processing SA payload. message ID = 1916387846
*Jan 16 00:16:10.310: ISAKMP:(1008): Checking IPSec proposal 1
*Jan 16 00:16:10.310: ISAKMP: transform 1, ESP_AES
```

```
*Jan 16 00:16:10.310: ISAKMP:   attributes in transform:
*Jan 16 00:16:10.310: ISAKMP:      SA life type in seconds
*Jan 16 00:16:10.310: ISAKMP:      SA life duration (basic) of 28800
*Jan 16 00:16:10.310: ISAKMP:      SA life type in kilobytes
*Jan 16 00:16:10.310: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Jan 16 00:16:10.310: ISAKMP:      encaps is 1 (Tunnel)
*Jan 16 00:16:10.310: ISAKMP:      authenticator is HMAC-SHA
*Jan 16 00:16:10.310: ISAKMP:      key length is 128
*Jan 16 00:16:10.310: ISAKMP:(1008):atts are acceptable.
*Jan 16 00:16:10.310: IPSEC(validate_proposal_request): proposal part #1
*Jan 16 00:16:10.310: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.)INBOUND local= 198.18.2.100:0, remote= 198.18.133.100:0,
    local_proxy= 198.20.2.0/255.255.255.0/256/0,
    remote_proxy= 198.19.10.0/255.255.255.0/256/0,
    protocol= ESP, transform= NONE   (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jan 16 00:16:10.310: Crypto mapdb : proxy_match
   src addr         : 198.20.2.0
   dst addr         : 198.19.10.0
   protocol         : 0
   src port         : 0
   dst port         : 0
*Jan 16 00:16:10.310: IPSEC(ipsec_process_proposal): invalid transform proposal flags -- 0x1
*Jan 16 00:16:10.310: ISAKMP:(1008): IPSec policy invalidated proposal with error 1024
*Jan 16 00:16:10.312: ISAKMP:(1008): phase 2 SA policy not acceptable! (local 198.18.2.100 remote
198.18.133.100)
*Jan 16 00:16:10.312: ISAKMP: set new node 2184325447 to QM_IDLE
*Jan 16 00:16:10.312: ISAKMP:(1008):Sending NOTIFY PROPOSAL_NOT_CHOSEN protocol 3
    spi 140098131981752, message ID = 2184325447

[…]
```

一部のパラメータが両側で一致していないため、phase 2 を確立することができません（***IPSEC(ipsec_process_proposal): invalid transform proposal flags***）。

6. 両方のデバイスで phase 2 の設定を比較します。

Router-20：

```
router-20#
router-20#show running-config | section crypto
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco address 198.18.133.100
crypto ipsec transform-set TS esp-aes esp-sha-hmac
 mode tunnel
crypto map VPN 10 ipsec-isakmp
 set peer 198.18.133.100
 set transform-set TS
 set pfs group20
 match address 110
 crypto map VPN
```

ASA:

```
ASAv# show run crypto
crypto ipsec ikev1 transform-set AES128SHA1 esp-aes esp-sha-hmac
[…]
crypto map OUTSIDE_MAP 220 match address VPN220
crypto map OUTSIDE_MAP 220 set peer 198.18.2.100
crypto map OUTSIDE_MAP 220 set ikev1 transform-set AES128SHA1
[…]
```

phase 2 に対して、追加のパラメータ pfs group20 が設定されています。

注: PFS（Perfect Forward Secrecy）は同じキーが再度生成されないようにする機能であるため、キーの再生成が実行されるたびに、新しい Diffie-Hellman キー交換が強制的に実行されます。phase 2 のその他の属性である PFS は、トンネルの両側で一致しなければなりません。

日常業務では、設定の誤りを防ぐために、TAC エンジニアが開発した IPSec Lan-to-Lan チェッカーを使用します。このツールは ASA または IOS ルータのいずれかからの「show tech」または「show running-config」を受け入れるように設計されています。このツールは設定を検査し、暗号マップ ベースの Lan-to-Lan IPsec トンネルが設定されているかどうかを検出します。トンネルが設定されている場合、このツールは設定の複数ポイント チェックを行い、設定エラーがあれば、ネゴシエーション対象のトンネルの設定と合わせて強調表示します。

このツールは、https://cway.cisco.com/tools/L2L-Checker/ で利用できます。

7. 相違点を修正して、トンネルを確立できることを確認します。

ルータで pfs を無効にします（セキュリティの観点からは、実際には ASA で PFS を有効にしておくことが推奨されます）。

```
router-20#conf t
Enter configuration commands, one per line.End with CNTL/Z.
router-20(config)#crypto map VPN 10 ipsec-isakmp router-
20(config-crypto-map)#no set pfs group20 router-20(config-
crypto-map)#end
```

PC から ping を実行します。

```
C:\Users\Administrator>ping 198.20.2.100 -t

Pinging 198.20.2.100 with 32 bytes of data:
Request timed out.
Reply from 198.20.2.100: bytes=1000 time=2ms TTL=255
Reply from 198.20.2.100: bytes=1000 time=2ms TTL=255
Reply from 198.20.2.100: bytes=1000 time=2ms TTL=255
```

ASA で Phase1 および Phase2 を検証し、トンネルが確立されてトラフィックが送信されることを確認します。

```
ASAv# sh crypto isakmp sa

IKEv1 SAs:

   Active SA: 2
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

 1  IKE Peer: 198.18.1.100
    Type    : L2L             Role    : initiator
```

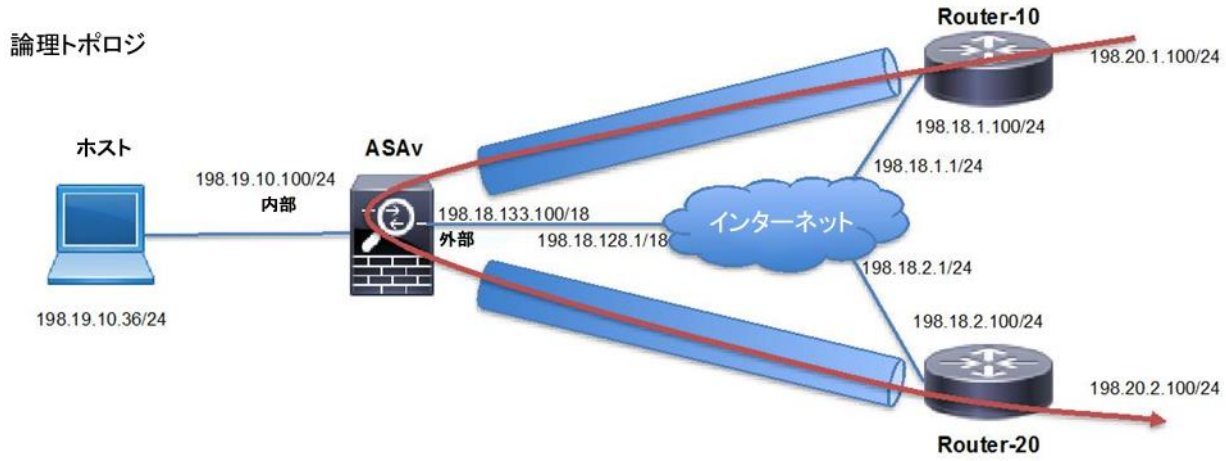
```
    Rekey   : no              State   : MM_ACTIVE
 2  IKE Peer: 198.18.2.100
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ASAv# show crypto ipsec sa peer 198.18.2.100
peer address: 198.18.2.100
Crypto map tag: OUTSIDE_MAP, seq num: 220, local addr: 198.18.133.100

      access-list VPN220 extended permit ip 198.19.10.0 255.255.255.0 198.20.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (198.19.10.0/255.255.255.0/0/0) remote ident
      (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
      current_peer: 198.18.2.100

      #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
      #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
[…]
```

Router-20 で Phase1 および Phase2 を確認します。

```
router-20#sh crypto session
Crypto session current status

Interface: GigabitEthernet2
Session status: UP-ACTIVE
Peer: 198.18.133.100 port 500
  IKEv1 SA: local 198.18.2.100/500 remote 198.18.133.100/500 Active
  IPSEC FLOW: permit ip 198.20.2.0/255.255.255.0 198.20.1.0/255.255.255.0
        Active SAs: 0, origin: crypto map
  IPSEC FLOW: permit ip 198.20.2.0/255.255.255.0 198.19.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

シナリオ 3. Router-10 の内側にあるサブネットと Router-20 の内側にあるサブネット間でトラフィック フローが発生しない

図 5. ネットワーク構成図



問題の詳細

両方の VPN トンネルを修正したので、管理者は必要な接続がすべて機能していると考えました。しかし、Router-10 の内側のロケーションにいるユーザから、Router-20 の内側にいるユーザに電話をかけることができないという報告がありました。両方のロケーション間の接続が機能していないようです。この間のトラフィックは、ハブ ロケーションとして機能している ASA を通過します。

注: 次の手順は、詳細なトラブルシューティング フローを示すものです。答えを確認する前に問題を自分でトラブルシューティングしてみる場合は、設定を変更する際に十分注意してください。実際の環境をできるだけ忠実に再現するために、デバイスへの接続はコンソールを経由していないためです。

手順

1. Router-10 のループバックから Router-20 のループバックへの ping を開始します。

両方のサイト間で連続してトラフィックを生成します。

```
router-10#ping 198.20.2.100 sour lo1 repeat 10000
Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 198.20.2.100, timeout is 2 seconds:
Packet sent with a source address of 198.20.1.100
....
```

2. Router-10 と ASA の間のインタレスティング トラフィックに対して IPSec SA が確立されていることを確認します。

```
ASAv# sh crypto ipsec sa peer 198.18.1.100
peer address: 198.18.1.100
    Crypto map tag: OUTSIDE_MAP, seq num: 110, local addr: 198.18.133.100
[…]
      access-list VPN110 extended permit ip 198.20.2.0 255.255.255.0 198.20.1.0 255.255.255.0
      local ident (addr/mask/prot/port): (198.20.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (198.20.1.0/255.255.255.0/0/0)
      current_peer: 198.18.1.100
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 49, #pkts decrypt: 49, #pkts verify: 49
[…]
```

IPSec トンネルが確立されており、decaps カウンタが増加している（#pkts decaps: 49）ので、パケットは受信されていますが、送信パケットのカウンタは増えていません（#pkts encaps: 0）。つまり、Router-10 に対してはトンネル経由でトラフィックが送信されていないということです。

ASA が Router-10 から着信するトラフィックをどのように処理しているかを確認します。

3. Router-10 から ASA に到着する ESP パケットに対して、trace detail オプションを指定してパケット キャプチャを設定します。

ASA が受信した暗号化パケットをどのように処理しているかを把握するために、trace detail オプションを指定してパケット キャプチャを設定します。また、古いキャプチャの削除も行います。

```
ASAv# no cap IN
ASAv# no cap OUT
ASAv# cap UTURN trace detail interface outside match ip host 198.18.1.100 host 198.18.133.100
```

show capture UTURN 出力で着信パケットの 1 つを指定し、トレースの詳細情報を確認します。

```
ASAv# show capture UTURN packet-number 1 trace detail

3 packets captured

   1: 11:23:07.537402 0050.5600.0001 0050.56ab.cf66 0x0800 Length: 182
      198.18.1.100 > 198.18.133.100:  ip-proto-50, length 148 (ttl 254, id 183)
[…]

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x7f79b11b4d20, priority=70, domain=ipsec-tunnel-flow, deny=false
    hits=183, user_data=0x48fc, cs_id=0x7f79b1f8a8a0, reverse, flags=0x0, protocol=0
    src ip/id=198.20.1.0, mask=255.255.255.0, port=0, tag=any
    dst ip/id=198.20.2.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
    input_ifc=outside, output_ifc=any

[…]

Phase: 12
Type: VPN
Subtype: encrypt
Result: DROP
Config:
```

```
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f79b11d26d0, priority=70, domain=encrypt, deny=false
    hits=183, user_data=0x0, cs_id=0x7f79b1f87a20, reverse, flags=0x0, protocol=0
    src ip/id=198.20.1.100, mask=255.255.255.255, port=0, tag=any
    dst ip/id=198.20.2.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=outside

Result:
[…]
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

注: パケット キャプチャのトレース機能は、暗号化されたトラフィックに対しても使用できます。

結果は DROP です。Phase 12 では IPsec トンネルで使用されるプロキシ ID に関する情報が示されています。詳細に確認すると、これらが誤っていることがわかります。Router-10 のピアに設定された SA にサブネット全体が含まれ、ホスト アドレスのみになっていません。

4. 誤って適用されているアクセスリストを確認します。

どのアクセスリストにそのようなホスト同士のエントリがあるのかを確認します。

```
ASAv# show access-list | i host 198.20.1.100 host 198.20.2.100 access-list VPN40 line 1 extended permit
ip host 198.20.1.100 host 198.20.2.100 (hitcnt=1727) 0xed66411d
```

5. 暗号マップの設定を確認します。

アクセスリスト VPN40 を使用している暗号マップがあるかどうかを確認します。

```
ASAv# show run crypto map | i VPN40

ASAv# show run crypto map | i OUTSIDE_MAP 40
crypto map OUTSIDE_MAP 40 match address VPN40
crypto map OUTSIDE_MAP 40 set peer 198.18.1.40
crypto map OUTSIDE_MAP 40 set ikev1 transform-set
AES128SHA1 […]
```

アクセスリスト VPN40 がシーケンス 40 で暗号マップに適用されています。これは Router-10 のピアに使用されている 110 より小さいシーケンスです。ASA は、一致する暗号アクセスリストを設定の順序に従って確認するので、最初に一致したものが適用されます。Router-10 からのトラフィックは、Router-20 との間に確立された IPSec トンネルに転送されるのではなく、VPN ピア 198.18.1.40 に送信されています。

6. ピア 198.18.1.40 に対して使用されている暗号マップの設定を削除します。

トラフィックをブラックホール処理していた暗号マップ エントリを削除します。

```
ASAv(config)# clear configure crypto map OUTSIDE_MAP 40

ASAv(config)# show running-config crypto map
crypto map OUTSIDE_MAP 50 match address VPN50
crypto map OUTSIDE_MAP 50 set peer 198.18.1.50
crypto map OUTSIDE_MAP 50 set ikev1 transform-set AES128SHA1
[…]
```

注: 実稼働ネットワークでは、所定のエントリが使用されていないことを確認してください。使用されている場合は設定が誤っている可能性があります。

7. キャプチャをクリアして、パケット トレーサを再度使用します。

```
ASAv# clear capture UTURN
ASAv# show capture UTURN trace detail

3 packets captured

   1: 12:07:54.021529 0050.5600.0001 0050.56ab.cf66 0x0800 Length: 182
      198.18.1.100 > 198.18.133.100:  ip-proto-50, length 148 (ttl 254, id 10312)
[…]
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x7f79b2221660, priority=70, domain=encrypt, deny=false
    hits=9, user_data=0xfeec, cs_id=0x7f79b2010ff0, reverse, flags=0x0, protocol=0
    src ip/id=198.20.1.0, mask=255.255.255.0, port=0, tag=any
    dst ip/id=198.20.2.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=outside
Result:

[…]
Action: drop
Drop-reason: (unable-to-create-flow) Flow denied due to resource limitation
```

Phase 12 が ALLOW を示しているにも関わらず、最終的な結果は引き続きパケットがドロップされることを示しています。ASA は Router-10 からのトラフィックを受信したインターフェイスと同じインターフェイスを使用して Router-20 にトラフィックを送信する必要があるため、同じセキュリティ許可機能が設定されているかどうかを確認します。

注:ASA は、デフォルトでは、トラフィックの受信に使用したインターフェイスを使用してトラフィックを送信することを許可していません。詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s1.html#pgfId-1444448 [英語] を参照してください。

same-security-traffic permit intra-interface 機能が設定されているかどうかを確認します。

```
ASAv# show run same-security
ASAv#
```

8. same-security 機能を設定して、結果を確認します。

same-security-traffic permit intra-interface が無効化されているので、これを設定に追加します。

```
ASAv# conf t
ASAv(config)# same-security-traffic permit intra-interface
```

9. 接続を確認します。

両方のロケーション間の ping が成功します。

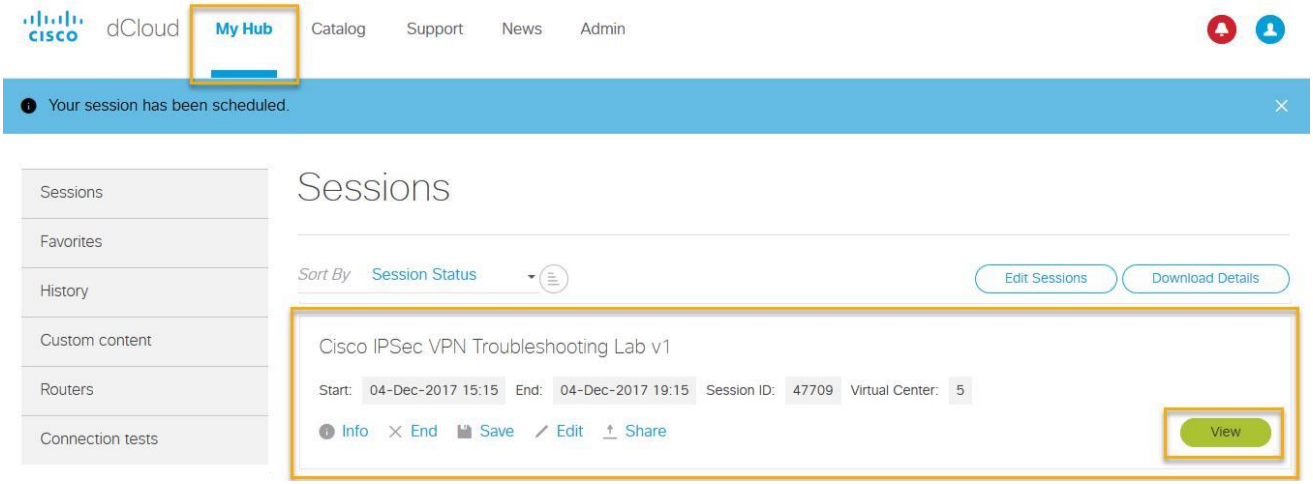
```
router-10#ping 198.20.2.100 sour lo1 repeat 10000
Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 198.20.2.100, timeout is 2 seconds:
Packet sent with a source address of
198.20.1.100 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
```

付録 A.　dCloud のサーバのリセット

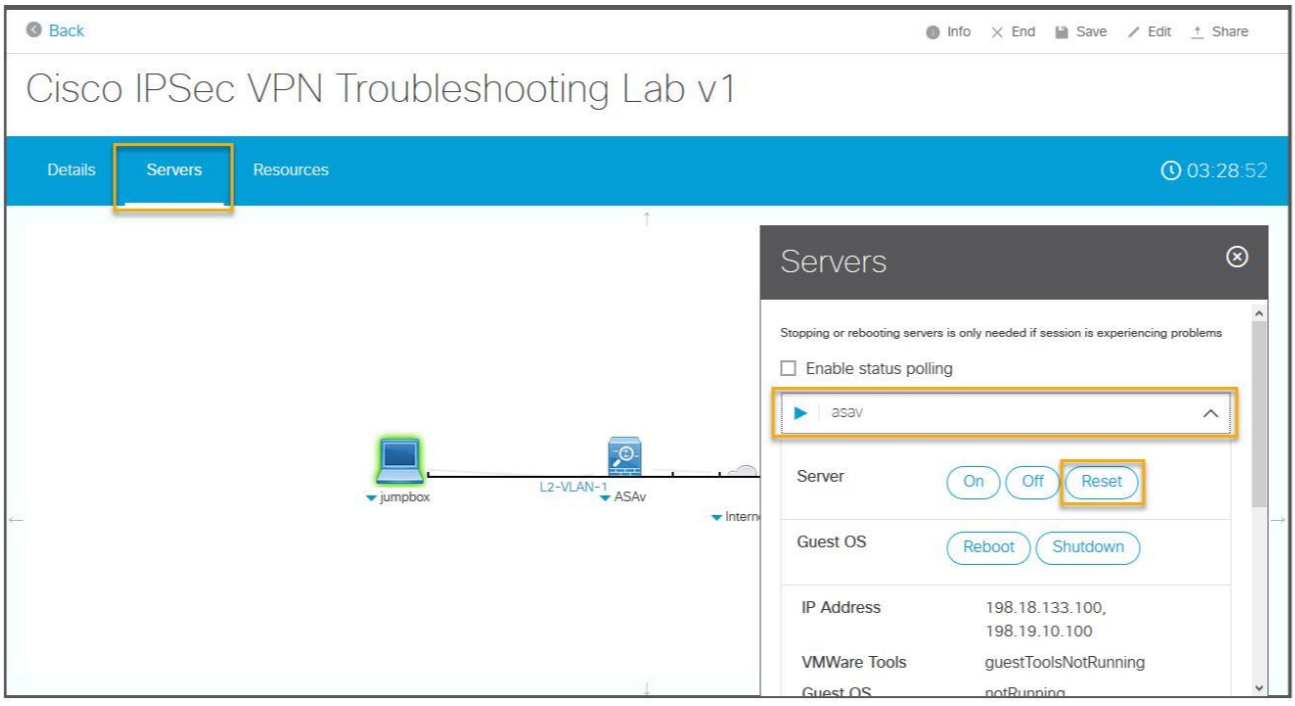
このデモンストレーションで使用される VM は非永続状態です。環境全体の実行が完了したら、次の手順を使用して環境を初期状態に戻してください。新しいセッションをスケジュールする必要はありません。

手順

1. dCloud UI で [マイ ハブ（My Hub）] を選択し、セションを確認します。[表示（View）] をクリックします。



2. [サーバ（Servers）] をクリックして使用可能なサーバのリストを表示します。
3. サーバの横にある矢印をクリックして情報を展開します。[リセット（Reset）] をクリックします。
4. 必要に応じて、すべての [サーバ（Servers）] について上記の手順を繰り返します。環境の複雑さに応じてサーバのリセットが完了するまでに 5 ～ 30 分かかります。



お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp