IOS VPN（ルータ）： 既存の L2L VPN への新しい L2L のトンネルまたはリモート アクセスの追加

目次

概要

このドキュメントでは、新しい L2L VPN トンネルまたはリモート アクセス VPN を IOS ルータにすでに存在する L2L VPN 設定に追加するために必要な手順について説明します。

前提条件

要件

この設定を実行する前に、現在動作している L2L IPSec VPN トンネルが正しく設定されていることを確認してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 12.4 および 12.2 が稼働する 2 つの IOS ルータ

- ソフトウェア バージョン 8.0 が稼働する Cisco 適応型セキュリティ アプライアンス（ASA）

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

この出力は、本社（ハブ）ルータとブランチ オフィス 1（BO1）ASAで現在実行中の設定です。この設定では、本社と BO1 ASA 間に設定されている IPSec L2L トンネルがあります。

現在の本社（ハブ）ルータの設定

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
!
!
!
!
interface Ethernet0/0
```

```
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

BO1 ASA の設定

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
```

```
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
```

```
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

背景説明

現在、本社オフィスと BO1 オフィス間には既存の L2L トンネルが設定されています。 最近会社の新しいブランチ オフィス (BO2) が設立されました。 この新しいオフィスでは、本社オフィスにあるローカル リソースへの接続が必要です。 さらに、従業員が自宅から安全に内部ネットワークにあるリソースにリモートでアクセスできるようにする必要もあります。 この例では、新しい VPN トンネルと本社オフィスにあるリモート アクセス VPN サーバを設定します。

設定への新しい L2L トンネルの追加

次に、この設定のネットワーク図を示します。

手順説明

このセクションでは、ハブの本社ルータで実行する必要のある手順を説明します。

次の手順を実行します。

1. 対象トラフィックを定義するために、クリプト マップで使用されるこの新しいアクセス リストを作成します。
   ```
   HQ_HUB(config)#ip access-list extended VPN_BO2
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   ```

   警告： 通信を行うには、この特定のネットワークとは反対の Access Control List (ACL; アクセス コントロール リスト) エントリを、もう一方のトンネルに設定する必要があります。
2. 次のネットワーク間で NAT を免除するには、no nat ステートメントにこれらのエントリを追加します。
   ```
   HQ_HUB(config)#ip access-list extended NAT_Exempt
   HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
   ```

   これらの ACL を既存のルート マップ nonat に追加します。
   ```
   HQ_HUB(config)#route-map nonat permit 10
   HQ_HUB(config-route-map)#match ip address NAT_Exempt
   HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
   ```

警告： 通信を行うには、この特定のネットワークとは反対の ACL エントリを、もう一方のトンネルに設定する必要があります。

3. 次に示されるように、フェーズ 1 設定のピア アドレスを指定します。

```
HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
```

注: 事前共有鍵はトンネルの両側で完全に一致する必要があります。

4. 新しい VPN トンネルのクリプト マップ設定を作成します。 すべてのフェーズ 2 設定は同じであるため、最初の VPN 設定と同じトランスフォーム セットを使用します。

```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
 HQ_HUB(config-crypto-map)#set peer 192.168.12.2
 HQ_HUB(config-crypto-map)#set transform-set newset
 HQ_HUB(config-crypto-map)#match address VPN_BO2
```

5. これで新しいトンネルの設定が完了したため、トンネルを介して対象トラフィックを送信して、トンネルを起動する必要があります。 これを行うには、extended ping コマンドを発行して、リモート トンネルの内部ネットワークにあるホストに ping を送信します。この例では、トンネルのもう一方にある、10.20.20.16 のアドレスが指定されているワークステーションに ping が送信されます。 これにより、本社と BO2 間のトンネルが起動します。 以上で 2 つのトンネルが HQ オフィスに接続されました。 トンネルの背後にあるシステムにアクセスできない場合、『Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions 』で、management-access を使用する別のソリューションを参照してください。

設定例

HUB_HQ - 新しい L2L VPN トンネル設定の追加

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
```

```
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

```
HQ_HUB#
```

BO2 L2L VPN トンネルの設定

```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
```

```
!
ip nat inside source route-map nonat interface Ethernet1
overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

設定へのリモート アクセス VPN の追加

次に、この設定のネットワーク図を示します。

この例では、**split-tunneling** と呼ばれる機能が使用されています。 この機能により、パケットをリモート アクセス IPSec クライアントから暗号化された形式で条件に応じて IPSec トンネル経由で送信したり、ネットワーク インターフェイスにクリア テキスト形式で送信したりできます。スプリット トンネリングをイネーブルにすると、IPSec トンネルのもう一方の宛先に送信されていないパケットを暗号化して、トンネルを介して送信し、復号化して、最終的な宛先にルーティングする必要がありません。 この概念は、スプリット トンネリング ポリシーを、指定したネットワークに適用します。 デフォルトでは、すべてのトラフィックをトンネルします。 スプリット トンネリング ポリシーを設定するには、インターネット用のトラフィックを示すことができる ACL を指定します。

手順説明

このセクションでは、リモート アクセス機能を追加して、リモート ユーザがすべてのサイトにアクセスできるようにするために必要な手順を説明します。

次の手順を実行します。

1. VPN トンネルを介して接続するクライアントが使用する IP アドレス プールを作成します。また、設定の完了後に VPN にアクセスするための基本ユーザを作成します。
   ```
   HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50


   HQ_HUB(config)#username vpnuser password 0 vpnuser123
   ```
2. 特定のトラフィックを NAT から免除します。

```
HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit
```

これらの ACL を既存のルート マップ nonat に追加します。

```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

この例では、VPN トンネル間の NAT 通信が免除されていることに注目してください。

3. 既存の L2L トンネルとリモート アクセス VPN ユーザ間の通信を許可します。

```
HQ_HUB(config)#ip access-list extended VPN_BO1
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

これにより、リモート アクセス ユーザは指定したトンネルの背後にあるネットワークと通信できるようになります。**警告：** 通信を行うには、この特定のネットワークとは反対の ACL エントリを、もう一方のトンネルに設定する必要があります。

4. **スプリット トンネリングの設定**VPN 接続のスプリット トンネリングを有効にするには、ルータで ACL が設定されていることを確認してください。 この例では、access-list split_tunnel コマンドがスプリット トンネリング用のグループに関連付けられ、トンネルは 10.10.10.0 /24、10.20.20.0/24、および 172.16.1.0/24 ネットワークに対して形成されます。ACL スプリット トンネルで定義されていないデバイス (インターネット上のデバイスなど) へのトラフィック フローは暗号化されません。

```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

5. wins、dns. interesting traffic acl および ip pool などのローカル認証、認証およびクライアント設定情報を、 VPN クライアント向けに設定します。

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```

6. VPN トンネルの作成に必要なダイナミック マップとクリプト マップの情報を設定します。

```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
```

```
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

設定例

設定例 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
```

```
hmac
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255




!
route-map nonat permit 10
```

```
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **ping**：このコマンドを使用すると、次に示すように L2L VPN トンネルを開始できます。

トラブルシューティング

設定のトラブルシューティングに使用できる情報については、次のドキュメントを参照してください。

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- IP Security のトラブルシューティング：debug コマンドの説明と使用

ヒント： セキュリティ アソシエーションをクリアしても、IPSec VPN の問題を解決できない場合は、さまざまな問題を解決するために、関連するクリプト マップを削除して再適用します。

警告： インターフェイスからクリプト マップを削除すると、そのクリプト マップに対応付けられているすべての IPSec トンネルがダウンします。 これらの手順は十分に注意して実行し、実行する前にお客様の組織の変更管理ポリシーを十分に考慮してください。

例

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

関連情報

- IP セキュリティ（IPSec）暗号化の概要
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- IPSec ルータでのダイナミック LAN-to-LAN ピアと VPN Client の設定
- テクニカル サポートとドキュメント – Cisco Systems