IPSec Over Cableのサンプルコンフィギュレーションおよびデバッグ

目次

概要

インターネット プロトコル セキュリティ（IPsec）は、IP ネットワーク上でセキュアなプライベート通信を確保するオープン スタンダードのフレームワークです。 Internet Engineering Task Force（IETF）によって開発された標準に基づき、IPSec はパブリック IP ネットワークを通過するデータ通信の機密性、整合性、および信頼性を保証します。 IPSec は、ネットワーク全体のセキュリティ ポリシーを展開するために、標準ベースの柔軟なソリューションに必要なコンポーネントを提供します。

この資料は 2 つの Ciscoケーブルモデム間の IPsec の設定例を提供したものです。 この設定は 2 つの Cisco UBR9XX シリーズ ケーブル modem ルータ間のケーブルネットワークを渡る暗号化トンネルを作成します。 2 つのネットワーク間のすべてのトラフィックは暗号化されます。 しかし他のネットワークに向かうトラフィックは非暗号化を渡すことができます。 small office， home office （SOHO） ユーザ向けに、これはケーブルネットワークを渡るバーチャル プライベート ネットワーク（VPN）の作成を可能にします。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

モデムは 2 つのケーブルモデムの IPsec を設定するこれらの必要条件に合致する必要があります:

- ルーティングモードの Cisco uBR904、uBR905、または uBR924
- IPsec 56 機能セット
- Cisco IOS® ソフトウェア リリース 12.0(5)T または それ 以降

さらに、Data-over-Cable Service Interface Specifications（DOCSIS）- Cisco UBR7246、Cisco UBR7223、または Cisco uBR7246VXR のような対応ヘッドエンド ケーブルルータ、である Cable Modem Termination System（CMTS）がなければなりません。

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

背景理論

この資料の例は uBR904 ケーブルモデム、uBR924 ケーブルモデムおよび uBR7246VXR CMTS を使用します。 ケーブルモデムは Cisco IOS ソフトウェア リリース 12.1(6)を実行し、CMTS は Cisco IOS ソフトウェア リリース 12.1(4)ec を実行します。

注: この例はコンソールポートを通したケーブルモデムのマニュアル設定で行われます。 自動化された プロセスが DOCSISコンフィギュレーションファイルを通して（実行された ios.cfg スクリプトは IPSec構成）そしてアクセス リストで 100 および 101 使用することができません作成されます。 これは簡易ネットワーク管理プロトコル（SNMP） docsDevNmAccess 表の Ciscoインプリメンテーションが Cisco IOS アクセス リストを使用するという理由によります。 それはインターフェイス毎に 1 つのアクセス リストを作成します。 uBR904 で、924 および 905 は、最初の 2 つのアクセス リスト 一般に使用されます（100 および 101）。 ユニバーサル シリアル バス（USB）を、CVA120 のような、3 つのアクセス リスト サポートするケーブルモデムで使用されます（100、101、および 102）。

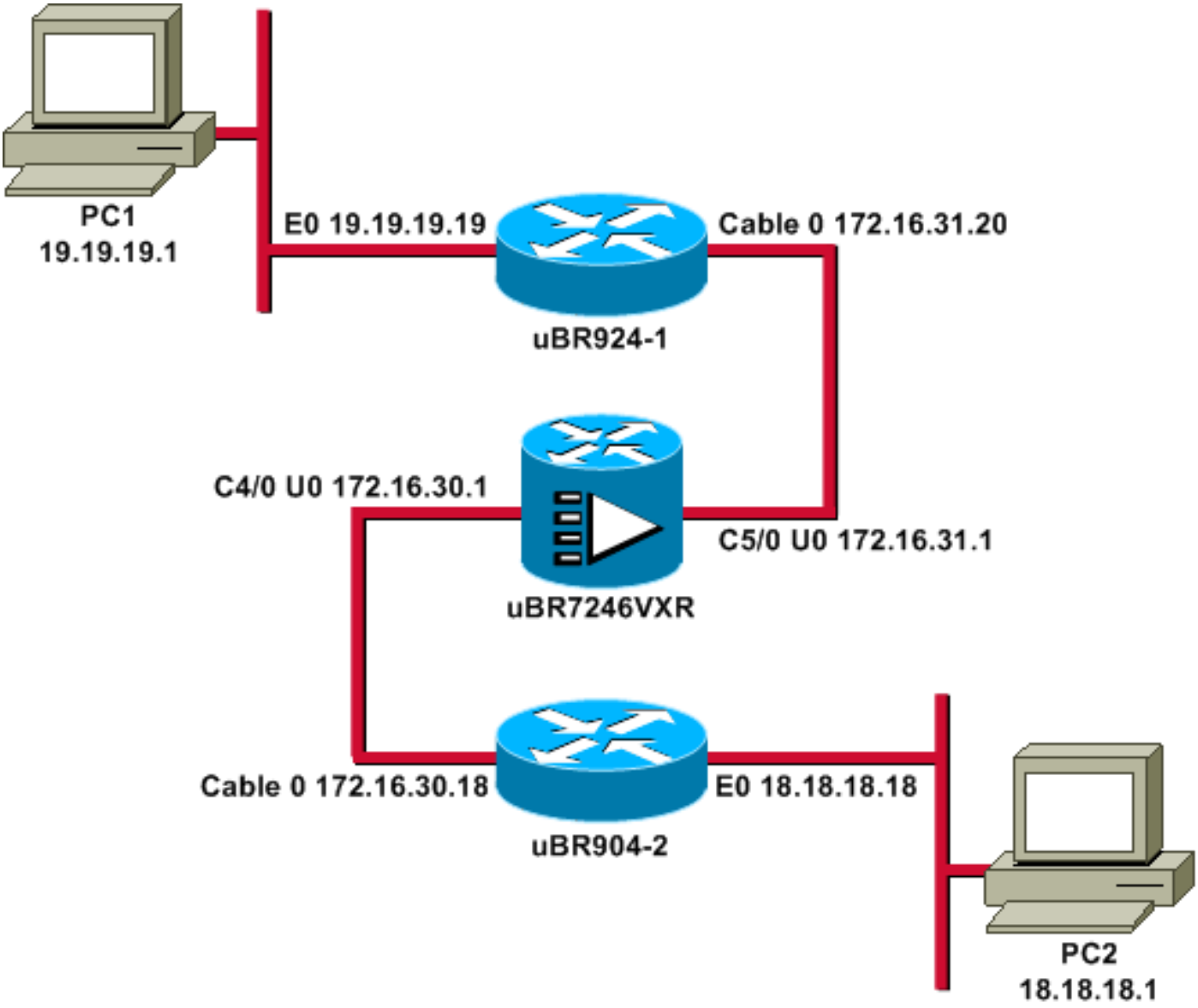
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: この資料のコマンドについてのその他の情報を見つけるのに Command Lookup Tool（登録ユーザのみ）を使用して下さい。

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。



注: このダイアグラムの IP アドレスすべてに 24 ビット マスクがあります。

設定

このドキュメントでは、次の設定を使用します。

- uBR924-1
- uBR904-2
- uBR7246VXR

uBR924-1

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr924-1
!
enable password ww
!
!
!
!
```

```
clock timezone - -8
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!
crypto isakmp policy 10 !--- Creates an Internet Key
Exchange (IKE) policy with the specified priority !---
number of 10. The range for the priority is 1 to 10000,
where 1 is the !--- highest priority. This command also
enters Internet Security Association !--- and Key
Management Protocol (ISAKMP) policy configuration
command mode. hash md5 !--- Specifies the MD5 (HMAC
variant) hash algorithm for packet authentication.
authentication pre-share !--- Specifies that the
authentication keys are pre-shared, as opposed to !---
dynamically negotiated using Rivest, Shamir, and Adelman
(RSA) public !--- key signatures. group 2 !--- Diffie-
Hellman group for key negotiation. lifetime 3600 !---
Defines how long, in seconds, each security association
should exist before !--- it expires. Its range is 60 to
86400, and in this case, it is 1 hour. crypto isakmp key
mykey address 18.18.18.18 !--- Specifies the pre-shared
key that should be used with the peer at the !---
specific IP address. The key can be any arbitrary
alphanumeric key up to !--- 128 characters. The key is
case-sensitive and must be entered identically !--- on
both routers. In this case, the key is mykey and the
peer is the !--- Ethernet address of uBR904-2 . ! crypto
IPSec transform-set TUNNELSET ah-md5-hmac esp-des !---
Establishes the transform set to use for IPsec
encryption. As many as !--- three transformations can be
specified for a set. Authentication Header !--- and ESP
are in use. Another common transform set used in
industry is !--- esp-des esp-md5-hmac. ! crypto map
MYMAP local-address Ethernet0 !--- Creates the MYMAP
crypto map and applies it to the Ethernet0 interface.
crypto map MYMAP 10 ipsec-isakmp !--- Creates a crypto
map numbered 10 and enters crypto map configuration
mode. set peer 18.18.18.18 !--- Identifies the IP
address for the destination peer router. In this case,
!--- the Ethernet interface of the remote cable modem
(ubr904-2) is used. set transform-set TUNNELSET !---
Sets the crypto map to use the transform set previously
created. match address 101 !--- Sets the crypto map to
use the access list that specifies the type of !---
traffic to be encrypted. !--- Do not use access lists
100, 101, and 102 if the IPsec config is !--- downloaded
through the ios.cfg in the DOCSIS configuration file. !
! ! ! voice-port 0 input gain -2 output attenuation 0 !
voice-port 1 input gain -2 output attenuation 0 ! ! !
interface Ethernet0 ip address 19.19.19.19 255.255.255.0
ip rip send version 2 ip rip receive version 2 no ip
route-cache no ip mroute-cache ! interface cable-modem0
ip rip send version 2 ip rip receive version 2 no ip
route-cache no ip mroute-cache cable-modem downstream
saved channel 525000000 39 1 cable-modem mac-timer t2
40000 no cable-modem compliant bridge crypto map MYMAP
!--- Applies the previously created crypto map to the
cable interface. ! router rip version 2 network 19.0.0.0
network 172.16.0.0 ! ip default-gateway 172.16.31.1 ip
classless ip http server ! access-list 101 permit ip
```

```
19.19.19.0 0.0.0.255 18.18.18.0 0.0.0.255 !--- Access
list that identifies the traffic to be encrypted. In
this case, !--- it is setting traffic from the local
Ethernet network to the remote !--- Ethernet network.
snmp-server manager ! line con 0 transport input none
line vty 0 4 password ww login ! end
```

他のケーブルモデムの設定は非常に類似した、そう以前のコンフィギュレーションのコメントのほとんど省略されますです。

uBR904-2

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ubr904-2
!
enable password ww
!
!
!
!
!
clock timezone - -8
ip subnet-zero
no ip finger
!
!
!
crypto isakmp policy 10 hash md5 authentication pre-
share group 2 lifetime 3600 crypto isakmp key mykey
address 19.19.19.19 ! ! crypto IPSec transform-set
TUNNELSET ah-md5-hmac ESP-Des ! crypto map MYMAP local-
address Ethernet0 crypto map MYMAP 10 ipsec-isakmp set
peer 19.19.19.19 !--- Identifies the IP address for the
destination peer router. In this case, !--- the Ethernet
interface of the remote cable modem (uBR924-1) is used.
set transform-set TUNNELSET match address 101 ! ! ! !
interface Ethernet0 ip address 18.18.18.18 255.255.255.0
ip rip send version 2 ip rip receive version 2 !
interface cable-modem0 ip rip send version 2 ip rip
receive version 2 no keepalive cable-modem downstream
saved channel 555000000 42 1 cable-modem Mac-timer t2
40000 no cable-modem compliant bridge crypto map MYMAP !
router rip version 2 network 18.0.0.0 network 172.16.0.0
! ip default-gateway 172.16.30.1 ip classless no ip http
server ! access-list 101 permit ip 18.18.18.0 0.0.0.255
19.19.19.0 0.0.0.255 snmp-server manager ! line con 0
transport input none line vty 0 4 password ww login !
end
```

ルーティングがはたらくように、CMTS uBR7246VXR はまたルーティング情報プロトコル（RIP）バージョン 2 を実行します。 これは CMTS で使用される Rip コンフィギュレーションです:

uBR7246VXR

```
router rip
 version 2
```

```
network 172.16.0.0
no auto-summary
```

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。

IPsec がはたらくことを確認するため:

- これらの事柄を確認して下さい:Cisco IOSソフトウェアは IPsec をサポートします。実行コンフィギュレーションは正しいです。インターフェイスは稼働しています。作業のルーティング。トラフィックを暗号化するために定義されるアクセス リストは正しいです。
- トラフィックを生成し、増加している量を見るために暗号化および復号化を、検知 して下さい。
- 暗号のためのデバッグをつけて下さい。

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。

両方のケーブルモデムの **show version コマンドを**発行して下さい。

```
ubr924-1#show version Cisco Internetwork Operating System Software IOS (tm) 920 Software
(UBR920-K1O3SV4Y556I-M), Version 12.1(6), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
Cisco Systems, Inc. Compiled Wed 27-Dec-00 16:36 by kellythw Image text-base: 0x800100A0, data-
base: 0x806C1C20 ROM: System Bootstrap, Version 12.0(6r)T3, RELEASE SOFTWARE (fc1) ubr924-1
uptime is 1 hour, 47 minutes System returned to ROM by reload at 10:39:05 - Fri Feb 9 2001
System restarted at 10:40:05 - Fri Feb 9 2001 System image file is "flash:ubr920-k1o3sv4y556i-
mz.121-6" cisco uBR920 CM (MPC850) processor (revision 3.e) with 15872K/1024K bytes of memory.
Processor board ID FAA0422Q04F Bridging software. 1 Ethernet/IEEE 802.3 interface(s) 1 Cable
Modem network interface(s) 3968K bytes of processor board System flash (Read/Write) 1536K bytes
of processor board Boot flash (Read/Write) Configuration register is 0x2102
```

uBR924-1 は VALUE SMALL OFFICE/VOICE/FW IPSEC 56 機能セットと Cisco IOS ソフトウェア リリース 12.1(6)を実行します。

```
ubr904-2#show version Cisco Internetwork Operating System Software IOS (TM) 900 Software
(UBR900-K1OY556I-M), Version 12.1(6), RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by cisco
Systems, Inc. Compiled Wed 27-DEC-00 11:06 by kellythw Image text-base: 0x08004000, database:
0x085714DC ROM: System Bootstrap, Version 11.2(19980518:195057), RELEASED SOFTWARE ROM: 900
Software (UBR900-RBOOT-M), Version 11.3(11)NA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) ubr904-2
uptime is 1 hour, 48 minutes System returned to ROM by reload at 10:38:44 - Fri Feb 9 2001
System restarted at 10:40:37 - Fri Feb 9 2001 System image file is "flash:ubr900-k1oy556i-
mz.121-6" cisco uBR900 CM (68360) processor (revision D) with 8192K bytes of memory. Processor
board ID FAA0235Q0ZS Bridging software. 1 Ethernet/IEEE 802.3 interface(s) 1 Cable Modem network
interface(s) 4096K bytes of processor board System flash (Read/Write) 2048K bytes of processor
board Boot flash (Read/Write) Configuration register is 0x2102
```

uBR904-2 は小さい OFFICE/FW IPSec 56 機能セットと Cisco IOS ソフトウェア リリース 12.1(6)を実行します。

```
ubr924-1#show ip interface brief Interface IP-Address OK? Method Status Protocol Ethernet0
19.19.19.19 YES NVRAM up up cable-modem0 172.16.31.20 YES unset up up ubr904-2#show ip interface
brief Interface IP-Address OK? Method Status Protocol Ethernet0 18.18.18.18 YES NVRAM up up
cable-modem0 172.16.30.18 YES unset up up
```

最後のコマンドから、イーサネットインターフェイスが稼働していることがわかります。 イーサネットインターフェイスの IP アドレスは手動で入力されました。 ケーブルインターフェイスはまたアップであり、DHCP によって IP アドレスを学びました。 これらの外電略号が動的に割り当てられるので、IPSec構成で同位として使用することができません。

```
ubr924-1#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - ISIS level-1, L2 - ISIS level-2, ia - ISIS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
172.16.31.1 to network 0.0.0.0 19.0.0.0/24 is subnetted, 1 subnets C 19.19.19.0 is directly
connected, Ethernet0 R 18.0.0.0/8 [120/2] via 172.16.31.1, 00:00:23, cable-modem0 172.16.0.0/16
is variably subnetted, 4 subnets, 3 masks R 172.16.135.0/25 [120/1] via 172.16.31.1, 00:00:23,
cable-modem0 R 172.16.29.0/27 [120/1] via 172.16.31.1, 00:00:23, cable-modem0 R 172.16.30.0/24
[120/1] via 172.16.31.1, 00:00:23, cable-modem0 C 172.16.31.0/24 is directly connected, cable-
modem0 R 192.168.99.0/24 [120/3] via 172.16.31.1, 00:00:24, cable-modem0 10.0.0.0/24 is
subnetted, 2 subnets R 10.10.10.0 [120/2] via 172.16.31.1, 00:00:24, cable-modem0 S* 0.0.0.0/0
[1/0] via 172.16.31.1
```

このから uBR904-2 のイーサネットインターフェイスである uBR924-1 がルート 18.18.18.0 について学んでいること出力するために見ることができます。

```
ubr904-2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
ISIS, L1 - ISIS level-1, L2 - ISIS level-2, IA - ISIS inter area * - candidate default, U - per-
user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
172.16.30.1 to network 0.0.0.0 R 19.0.0.0/8 [120/2] via 172.16.30.1, 00:00:17, cable-modem0
18.0.0.0/24 is subnetted, 1 subnets C 18.18.18.0 is directly connected, Ethernet0 172.16.0.0/16
is variably subnetted, 4 subnets, 3 masks R 172.16.135.0/25 [120/1] via 172.16.30.1, 00:00:17,
cable-modem0 R 172.16.29.224/27 [120/1] via 172.16.30.1, 00:00:17, cable-modem0 C 172.16.30.0/24
is directly connected, cable-modem0 R 172.16.31.0/24 [120/1] via 172.16.30.1, 00:00:17, cable-
modem0 R 192.168.99.0/24 [120/3] via 172.16.30.1, 00:00:18, cable-modem0 10.0.0.0/24 is
subnetted, 1 subnets R 10.10.10.0 [120/2] via 172.16.30.1, 00:00:18, cable-modem0 S* 0.0.0.0/0
[1/0] via 172.16.30.1
```

uBR904-2 のルーティング テーブルから、uBR924-1 のイーサネットのためのネットワークがルーティング テーブルにあることがわかります。

注: 2 つのケーブルモデムの間でルーティング プロトコルを作動できないケースがあるかもしれません。 このような場合、ケーブルモデムのイーサネットインターフェイスのための直接トラフィックに CMTS におけるスタティック・ ルートを追加して下さい。

チェックするべき次の事柄はアクセス リストの認証です; 両方のルータの **show access-lists コマンドを**発行して下さい。

```
ubr924-1#show access-lists Extended IP access list 101 permit ip 19.19.19.0 0.0.0.255 18.18.18.0
0.0.0.255 (2045 matches) ubr904-2#show access-lists Extended IP access list 101 permit ip
18.18.18.0 0.0.0.255 19.19.19.0 0.0.0.255 (2059 matches)
```

アクセス リストは IPSecセッションを時 uBR924-1 （ 19.19.19.0 ） uBR904-2 の後ろのの後ろの LAN LAN への送信 IP トラフィック 設定 しました (18.18.18.0) 、またその逆にも。 それが問題を引き起こすので、アクセス リストで「どれでも」使用しないで下さい。 IPSec ネットワークセキュリティの詳細については設定を参照して下さい。

IPSecトラフィックがありません。 **show crypto engine connection active** コマンドを発行して下さい。

```
ubr924-1#show crypto engine connection active ID Interface IP-Address State Algorithm Encrypt
Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 ubr904-2#show crypto engine connection active ID Interface
IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0
```

トラフィックがアクセス リストと一致しなかったので IPSec接続がありません。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

次 の ステップは関連 トラフィックを生成するためにいくつかの暗号デバッグをつけることです

。

この例では、これらのデバッグはつきます:

- debug crypto engine
- debug crypto ipsec
- debug crypto key-exchange
- debug crypto isakmp

最初にデバッグの出力を見るために関連 トラフィックを生成して下さい。 uBR904-2 のイーサネットポートから uBR924-1 （ 19.19.19.1 ） IP アドレスの PC に拡張ピングを実行して下さい。

```
ubr904-2#ping ip Target IP address: 19.19.19.1 !--- IP address of PC1 behind the Ethernet of
uBR924-1. Repeat count [5]: 100 !--- Sends 100 pings. Datagram size [100]: Timeout in seconds
[2]: Extended commands [n]: y Source address or interface: 18.18.18.18 !--- IP address of the
Ethernet behind uBR904-2. Type of service [0]: Set DF bit in IP header? [no]: Validate reply
data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range
of sizes [n]: Type escape sequence to abort. Sending 100, 100-byte ICMP Echos to 19.19.19.1,
timeout is 2 seconds:
```

uBR924-2 はこのデバッグ 出力を示します:

```
ubr904-2#
01:50:37: IPSec(sa_request): , (key eng. msg.) src= 18.18.18.18, dest= 19.19.19.19, src_proxy=
18.18.18.0/255.255.255.0/0/0 (type=4), dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4),
protocol= AH, transform= ah-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0x19911A16(428939798),
conn_id= 0, keysize= 0, flags= 0x4004 01:50:37: IPSec(sa_request): , (key Eng. msg.) src=
18.18.18.18, dest= 19.19.19.19, src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), dest_proxy=
19.19.19.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= ESP-Des , lifedur= 3600s and
4608000kb, spi= 0x7091981(118036865), conn_id= 0, keysize= 0, flags= 0x4004 01:50:37: ISAKMP:
received ke message (1/2) 01:50:37: ISAKMP (0:1): sitting IDLE. Starting QM immediately
(QM_IDLE) 01:50:37: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1108017901 01:50:37:
CryptoEngine0: generate hmac context for conn id 1 01:50:37: ISAKMP (1): sending packet to
19.19.19.19 (I) QM_IDLE 01:50:37: ISAKMP (1): received packet from 19.19.19.19 (I) QM_IDLE
01:50:37: CryptoEngine0: generate hmac context for conn id 1 01:50:37: ISAKMP (0:1): processing
SA payload. message ID = 1108017901 01:50:37: ISAKMP (0:1): Checking IPSec proposal 1 01:50:37:
ISAKMP: transform 1, AH_MD5 01:50:37: ISAKMP: attributes in transform:
01:50:3.!!!!!!!!!!!!!!!!!!!!!!7: ISAKMP: encaps is 1 01:50:37: ISAKMP: SA life type in seconds
01:50:37: ISAKMP: SA life duration (basic) of 3600 01:50:37: ISAKMP: SA life type in kilobytes
01:50:37: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 01:50:37: ISAKMP: authenticator is
HMAC-MD5 01:50:37: validate proposal 0 01:50:37: ISAKMP (0:1): atts are acceptable. 01:50:37:
ISAKMP (0:1): Checking IPSec proposal 1 01:50:37: ISAKMP: transform 1, ESP_DES 01:50:37: ISAKMP:
attributes in transform: 01:50:37: ISAKMP: encaps is 1 01:50:37: ISAKMP: SA life type in seconds
01:50:37: ISAKMP: SA life duration (basic) of 3600 01:50:37: ISAKMP: SA life type in kilobytes
01:50:37: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 01:50:37: validate proposal 0
01:50:37: ISAKMP (0:1): atts are acceptable. 01:50:37: IPSec(validate_proposal_request):
proposal part #1, (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18, dest_proxy=
19.19.1!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!! Success
rate is 99 percent (99/100), round-trip min/avg/max = 30/40/70 ms ubr904-2#
```

最初の PING が失敗したことに注意して下さい。 これは接続を確立する必要があるという理由によります。

uBR924-1 はこのデバッグ 出力を示します:

```
ubr924-1#
01:50:24: ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE 01:50:24: CryptoEngine0:
generate hmac context for conn id 1 01:50:24: ISAKMP (0:1): processing SA payload. Message ID =
1108017901 01:50:24: ISAKMP (0:1): Checking IPSec proposal 1 01:50:24: ISAKMP: transform 1,
AH_MD5 01:50:24: ISAKMP: attributes in transform: 01:50:24: ISAKMP: encaps is 1 01:50:24:
ISAKMP: SA life type in seconds 01:50:24: ISAKMP: SA life duration (basic) of 3600 01:50:24:
ISAKMP: SA life type in kilobytes 01:50:24: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
```

01:50:24: ISAKMP: **authenticator is HMAC-MD5** 01:50:24: validate proposal 0 01:50:24: ISAKMP (0:1): atts are acceptable. 01:50:24: ISAKMP (0:1): Checking IPSec proposal 1 01:50:24: ISAKMP: **transform 1, ESP_DES** 01:50:24: ISAKMP: attributes in transform: 01:50:24: ISAKMP: encaps is 1 01:50:24: ISAKMP: SA life type in seconds 01:50:24: ISAKMP: SA life duration (basic) of 3600 01:50:24: ISAKMP: SA life type in kilobytes 01:50:24: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 01:50:24: **validate proposal 0** 01:50:24: ISAKMP (0:1): atts are acceptable. 01:50:24: IPSec**(validate_proposal_request)**: proposal part #1, (key Eng. msg.) **dest= 19.19.19.19, src= 18.18.18.18,** dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= AH, transform= ah-md5-hmac** , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 01:50:24: IPSec(validate_proposal_request): proposal part #2, (key Eng. msg.) **dest= 19.19.19.19, src= 18.18.18.18**, dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= ESP, transform= ESP-Des** , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 01:50:24: validate proposal request 0 01:50:24: ISAKMP (0:1): processing NONCE payload. Message ID = 1108017901 01:50:24: ISAKMP (0:1): processing ID payload. Message ID = 1108017901 01:50:24: ISAKMP (1): ID_IPV4_ADDR_SUBNET src 18.18.18.0/255.255.255.0 prot 0 Port 0 01:50:24: ISAKMP (0:1): processing ID payload. Message ID = 1108017901 01:50:24: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 19.19.19.0/255.255.255.0 prot 0 Port 0 01:50:24: **ISAKMP (0:1): asking for 2 spis from IPSec** 01:50:24: IPSec(key_engine): got a queue event... 01:50:24: IPSec(spi_response): getting spi 393021796 for SA from 18.18.18.18 to 19.19.19.19 for prot 2 01:50:24: IPSec(spi_response): getting spi 45686884 for SA from 18.18.18.18 to 19.19.19.19 for prot 3 01:50:24: **ISAKMP: received ke message (2/2)** 01:50:24: CryptoEngine0: generate hmac context for conn id 1 01:50:24: ISAKMP (1): sending packet to 18.18.18.18 (R) QM_IDLE 01:50:24: ISAKMP (1): received packet from 18.18.18.18 (R) QM_IDLE 01:50:24: **CryptoEngine0: generate hmac context for conn id 1** 01:50:24: IPSec allocate flow 0 01:50:24: IPSec allocate flow 0 01:50:24: **ISAKMP (0:1): Creating IPSec SAs** 01:50:24: **inbound SA from 18.18.18.18 to 19.19.19.19 (proxy 18.18.18.0 to 19.19.19.0)** 01:50:24: has spi 393021796 and conn_id 2000 and flags 4 01:50:24: lifetime of 3600 seconds 01:50:24: lifetime of 4608000 kilobytes 01:50:24: **outbound SA from 19.19.19.19 to 18.18.18.18 (proxy 19.19.19.0 to 18.18.18.0)** 01:50:24: has spi 428939798 and conn_id 2001 and flags 4 01:50:24: lifetime of 3600 seconds 01:50:24: lifetime of 4608000 kilobytes 01:50:24: **ISAKMP (0:1): Creating IPSec SAs** 01:50:24: **inbound SA from 18.18.18.18 to 19.19.19.19 (proxy 18.18.18.0 to 19.19.19.0)** 01:50:24: has spi 45686884 and conn_id 2002 and flags 4 01:50:24: lifetime of 3600 seconds 01:50:24: lifetime of 4608000 kilobytes 01:50:24: **outbound SA from 19.19.19.19 to 18.18.18.18 (proxy 19.19.19.0 to 18.18.18.0)** 01:50:24: has spi 118036865 and conn_id 2003 and flags 4 01:50:25: lifetime of 3600 seconds 01:50:25: lifetime of 4608000 kilobytes 01:50:25: ISAKMP (0:1): deleting node 1108017901 error FALSE reason "quick mode done (await()" 01:50:25: **IPSec(key_engine): got a queue event...** 01:50:25: **IPSec(initialize_sas):** , (key Eng. msg.) **dest= 19.19.19.19, src= 18.18.18.18**, dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= AH, transform= ah-md5-hmac** , lifedur= 3600s and 4608000kb, spi= 0x176D0964(393021796), **conn_id= 2000**, keysize= 0, flags= 0x4 01:50:25: **IPSec(initialize_sas):** , (key Eng. msg.) **src= 19.19.19.19, dest= 18.18.18.18**, src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= AH, transform= ah-md5-hmac** , lifedur= 3600s and 4608000kb, spi= 0x19911A16(428939798), **conn_id= 2001**, keysize= 0, flags= 0x4 01:50:25: **IPSec(initialize_sas):** , (key Eng. msg.) dest= 19.19.19.19, src= 18.18.18.18, dest_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), src_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= ESP, transform= ESP-Des** , lifedur= 3600s and 4608000kb, spi= 0x2B92064(45686884), **conn_id= 2002**, keysize= 0, flags= 0x4 01:50:25: **IPSec(initialize_sas):** , (key Eng. msg.) **src= 19.19.19.19, dest= 18.18.18.18**, src_proxy= 19.19.19.0/255.255.255.0/0/0 (type=4), dest_proxy= 18.18.18.0/255.255.255.0/0/0 (type=4), **protocol= ESP, transform= ESP-Des** , lifedur= 3600s and 4608000kb, spi= 0x7091981(118036865), **conn_id= 2003**, keysize= 0, flags= 0x4 01:50:25: IPSec(create_sa): sa created, (sa) sa_dest= 19.19.19.19, sa_prot= 51, sa_spi= 0x176D0964(393021796), sa_trans= ah-md5-hmac , sa_conn_id= 2000 01:50:25: IPSec(create_sa): sa created, (sa) sa_dest= 18.18.18.18, sa_prot= 51, sa_spi= 0x19911A16(428939798), sa_trans= ah-md5-hmac , sa_conn_id= 2001 01:50:25: IPSec(create_sa): sa created, (sa) sa_dest= 19.19.19.19, sa_prot= 50, sa_spi= 0x2B92064(45686884), sa_trans= ESP-Des , sa_conn_id= 2002 01:50:25: IPSec(create_sa): sa created, (sa) sa_dest= 18.18.18.18, sa_prot= 50, sa_spi= 0x7091981(118036865), sa_trans= ESP-Des , sa_conn_id= 2003 ubr924-1#

IPSecトンネルが作成されれば、接続および暗号化パケット および 復号化パケットを表示できます。

ubr924-1#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 cable-modem0 172.16.31.20 set **HMAC_MD5 0 99** 2001

cable-modem0 172.16.31.20 set HMAC_MD5 **99 0** 2002 cable-modem0 172.16.31.20 set **DES_56_CBC 0 99** 2003 cable-modem0 172.16.31.20 set DES_56_CBC **99 0**

最初の 200x 行は受信される 99 のパケットを示します。 それは PC1 にそれらを送信 するためにパケットを復号化しなければなりません。 第 2 行は 99 の送信されたパケットを示します。 それは uBR904-2 にそれらを送信 する前にパケットを暗号化しなければなりません。 第 3 および第 4 行は AH-MD5-HMAC の代りに ESP-DES トランスフォームの同じプロセスを、実行します。

注: トランスフォームがケーブルモデムで設定されるなら ESP-DES ESP-MD5-HMAC、見れば 2 つの自律システム（AS）を、設定 したら前の**表示コマンド**で示されている 4 に対してだけ。

ubr904-2#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 **cable-modem0 172.16.30.18** set **HMAC_MD5 0 99** 2001 cable-modem0 172.16.30.18 set HMAC_MD5 **99 0** 2002 **cable-modem0 172.16.30.18** set **DES_56_CBC 0 99** 2003 cable-modem0 172.16.30.18 set DES_56_CBC **99 0**

カウンターが暗号化パケット および 復号化パケットのために増分するかどうか見るために uBR924-1 からの PC2 に拡張ピングを実行して下さい。

ubr924-1#**ping ip Target IP address: 18.18.18.1** Repeat count [5]: **50** Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y **Source address or interface: 19.19.19.19** Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 50, 100-byte ICMP Echos to 18.18.18.1, timeout is 2 seconds: **!!** Success rate is **100 percent** (50/50), round-trip min/avg/max = 28/30/33 ms ubr924-1#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 cable-modem0 172.16.31.20 set HMAC_MD5 **0 149** 2001 cable-modem0 172.16.31.20 set HMAC_MD5 **149 0** 2002 cable-modem0 172.16.31.20 set DES_56_CBC **0 149** 2003 cable-modem0 172.16.31.20 set DES_56_CBC **149 0** ubr904-2#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 cable-modem0 172.16.30.18 set HMAC_MD5 **0 149** 2001 cable-modem0 172.16.30.18 set HMAC_MD5 **149 0** 2002 cable-modem0 172.16.30.18 set DES_56_CBC **0 149** 2003 cable-modem0 172.16.30.18 set DES_56_CBC **149 0**

別の拡張ピングはカウンターが再度増分することがわかるために実行することができます。 今回は、uBR904-2 から uBR924-1 のイーサネットインターフェイスに 500 パケット PING を送信 します（19.19.19.19）。

ubr904-2#**ping ip Target IP address: 19.19.19.19** Repeat count [5]: **500** Datagram size [100]: 1000 Timeout in seconds [2]: Extended commands [n]: y **Source address or interface: 18.18.18.18** Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 500, 1000-byte ICMP Echos to 19.19.19.19, timeout is 2 seconds:
!!
!!! 01:59:06: IPSec(encapsulate): encaps area too small, moving to new buffer: idbtype 0, encaps_size 26, header size 60, avail 84!!!!!!!!! !!
!!
!!
!!
!! !!!!!!!!!! **Success rate is 100 percent** (500/500), round-trip min/avg/max = 98/135/352 ms ubr904-2#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 cable-modem0 172.16.30.18 set HMAC_MD5 **0 649** 2001 cable-modem0 172.16.30.18 set HMAC_MD5 **649 0** 2002 cable-modem0 172.16.30.18 set DES_56_CBC **0 649** 2003 cable-modem0 172.16.30.18 set DES_56_CBC **649 0** ubr924-1#**show crypto engine connection active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 set HMAC_MD5+DES_56_CB 0 0 2000 cable-modem0 172.16.31.20 set HMAC_MD5 **0 649** 2001 cable-modem0 172.16.31.20 set HMAC_MD5 **649 0** 2002 cable-modem0 172.16.31.20 set DES_56_CBC **0 649** 2003 cable-modem0 172.16.31.20 set DES_56_CBC **649 0**

接続をクリアする **clear crypto isakmp** および **clear crypto sa コマンドを**発行できます。 また IPSecトンネルを渡るトラフィックが有効期限の間になければ、IPsec は接続を自動的にリセットします。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- IPSec ネットワーク セキュリティ コマンド
- IPセキュリティ（IPSec）暗号化入門-デバッグ情報
- IPsec 設定例
- IPsec ネットワーク セキュリティの設定
- Cisco UBR900 シリーズ ケーブル アクセス ルータの設定
- Cisco ケーブル/ブロードバンドに関するダウンロード（登録ユーザ専用）
- ブロードバンド ケーブルに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems