NAT を使用する Router-to-Router Dynamic-to-Static IPSec の設定

内容

はじめに

この設定例では、リモート ルータが IP Control Protocol（IPCP）と呼ばれる PPP の一部を介して IP アドレスを受信します。リモート ルータは、ハブ ルータに接続するために IP アドレスを使用します。この設定により、ハブ ルータがダイナミック IPSec 接続を受け入れることができます。リモート ルータでは、ネットワーク アドレス変換（NAT）を使用して、背後にあるプライベート アドレスの付けられたデバイスが、ハブ ルータの背後にあるプライベート アドレスの付けられたネットワークに「参加」できるようにしています。リモート ルータは、エンドポイントを認識し、ハブ ルータへの接続を開始できます。ただし、ハブ ルータはエンドポイントを認識しないため、リモート ルータへの接続を開始できません。

この例では、dr_whoovie がリモート ルータで、sam-i-am がハブ ルータです。アクセス リストで暗号化するトラフィックが指定されているため、dr_whoovie は暗号化するトラフィックと sam-i-am エンドポイントの場所を認識します。リモート ルータが接続を開始する必要があります。両側で、NAT オーバーロードが実行されています。

前提条件

要件

このマニュアルは、IPSec プロトコルに関する基本的知識を前提とします。IPSec の詳細については、『IP Security（IPSec）暗号化の概要』を参照してください。

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いています。

- Cisco IOS® ソフトウェア リリース 12.2(24a)
- Cisco 2500 シリーズ ルータ

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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

表記法の詳細については、『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。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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 セットアップを使用します。

コンフィギュレーション

このドキュメントでは、次のコンフィギュレーションを使用します。

- sam-i-am
- dr_whoovie

<#root>

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log up time
no service password-encryption
!
hostname sam-i-am
```

```
!
ip subnet-zero
!
!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the
crypto isakmp policy
 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--

hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

!--- Configures a pre-shared authentication key, !--- used in global configuration mode.
!
!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This

crypto dynamic-map rtpmap 10

!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation re

set transform-set rtpset

!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.

match address 115

!--- Assign an extended access list to a crypto map entry !--- that is used by IPSec to determine whic

crypto map rtptrans 10 ipsec-isakmp dynamic rtpmap

!--- Specifies that this crypto map entry is to reference !--- a preexisting dynamic crypto map.
!
interface Ethernet0
```

```
 ip address 10.2.2.3 255.255.255.0
 no ip directed-broadcast

ip nat inside

 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA
 no mop enabled
!
interface Serial0
 ip address 99.99.99.1 255.255.255.0
 no ip directed-broadcast

ip nat outside

 !--- This indicates that the interface is connected !--- to the outside network.

crypto map rtptrans

!--- Use the
crypto map
 interface configuration command !--- to apply a previously defined crypto map set to an interface.
!
ip nat inside source route-map nonat interface Serial0 overload

!--- Except the private network from the NAT process.
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!
access-list 115 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 deny ip 10.2.2.0 0.0.0.255 any

!--- Include the private-network-to-private-network traffic !--- in the encryption process.

access-list 120 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 120 permit ip 10.2.2.0 0.0.0.255 any

!--- Except the private network from the NAT process.

route-map nonat permit 10
 match ip address 120
!
line con 0
```

```
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

dr_whoovie

<#root>

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
ip subnet-zero
!
!--- These are the IKE policies.

crypto isakmp policy 1

!--- Defines an Internet Key Exchange (IKE) policy. !--- Use the
crypto isakmp policy
 command !--- in global configuration mode. !--- IKE policies define a set of parameters to be used !--


hash md5
authentication pre-share

!--- Specifies pre-shared keys as the authentication method.

crypto isakmp key cisco123 address 99.99.99.1


!--- Configures a pre-shared authentication key, !--- used in global configuration mode.
!
!--- These are the IPSec policies.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !--- This
```

```
!
crypto map rtp 1 ipsec-isakmp


!--- Creates a crypto map and indicates that IKE will be used !--- to establish the IPSec SAs for prote

set peer 99.99.99.1

!--- Use the
set peer
 command to specify an IPSec peer in a crypto map entry.

set transform-set rtpset


!--- Configure IPSec to use the transform set "rtpset" !--- that was defined previously.


match address 115

!--- Include the private-network-to-private-network traffic !--- in the encryption process.

!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
 no ip directed-broadcast

ip nat inside

 !--- This indicates that the interface is connected to the !--- inside network, which is subject to NA

 no mop enabled
!
interface Serial0
 ip address negotiated

 !--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiatio

 no ip directed-broadcast

ip nat outside

 !--- This indicates that the interface is connected !--- to the outside network.

 encapsulation ppp
 no ip mroute-cache
 no ip route-cache
```

```
crypto map rtp


 !--- Use the

crypto map

 interface configuration command !--- to apply a previously defined crypto map set to an interface.


ip nat inside source route-map nonat interface Serial0 overload


!--- Except the private network from the NAT process.

ip classless
ip route 0.0.0.0 0.0.0.0 Serial0
no ip http server
!

access-list 115 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 115 deny ip 10.1.1.0 0.0.0.255 any


!--- Include the private-network-to-private-network traffic !--- in the encryption process.


access-list 120 deny   ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 any


!--- Except the private network from the NAT process.

dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit

route-map nonat permit 10
 match ip address 120

!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

特定の show コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、show コマンド出力の分析を表示できます。

- ping：基本的なネットワーク接続の診断に使用されます。

この例は、dr_whoovie 上の 10.1.1.1 イーサネット インターフェイスから sam-i-am 上の 10.2.2.3 イーサネット インターフェイスへの ping を示しています。

<#root>

```
dr_whoovie#
```

ping

```
Protocol [ip]:
Target IP address: 10.2.2.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
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 5, 100-byte ICMP Echos to 10.2.2.3,
  timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5),
  round-trip min/avg/max = 36/38/40 ms
```

- show crypto ipsec sa：フェーズ 2 セキュリティ アソシエーション（SA）を表示します。
- show crypto isakmp sa：フェーズ 1 SA を表示します。

出力例

この出力は、ハブ ルータ上で発行された show crypto ipsec sa コマンドからのものです。

<#root>

```
sam-i-am#
```

show crypto ipsec sa

```
interface: Serial0
    Crypto map tag: rtptrans, local addr. 99.99.99.1
```

local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

```
   current_peer: 100.100.100.1
     PERMIT, flags={}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
```

```
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0


local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1

     path mtu 1500, ip mtu 1500, ip mtu interface Serial0
     current outbound spi: 52456533


inbound esp sas:

      spi: 0x6462305C(1684156508)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:


outbound esp sas:

      spi: 0x52456533(1380279603)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
        sa timing: remaining key lifetime (k/sec): (4607999/3510)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:
```

このコマンドは、ピア デバイス間で構築された IPSec SA を表示します。暗号化されたトンネルが dr_whoovie 上の 100.100.100.1 インターフェイスと sam-i-am 上の 99.99.99.1 インターフェイスを接続しています。このトンネルは、ネットワークの 10.2.2.3 と 10.1.1.1 の間でやり取りされるトラフィックを伝送します。インバウンドとアウトバウンドで 2 つの Encapsulating Security Payload（ESP）SA が作成されます。トンネルは、sam-i-am がピア IP アドレス（100.100.100.1）を認識していない場合でも確立されます。認証ヘッダー（AH）SA は、AH が設定されていないため、使用されません。

次の出力例は、dr_whoovie 上のシリアル インターフェイス 0 が IPCP 経由で 100.100.100.1 の IP アドレスを受信することを示しています。

- IP アドレスのネゴシエート前：

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570


Internet address will be negotiated using IPCP

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

- IP アドレスのネゴシエート後：

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
  Hardware is HD64570


Internet address is 100.100.100.1/32

  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
```

この例は、ラボで peer default ip address command コマンドを使用して dr_whoovie 上のシリアル 0 インターフェイスのリモート エンドで IP アドレスを割り当てるためにセットアップされたものです。IP プールはリモート エンドで ip local pool command を使用して定義されます。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

トラブルシューティングのためのコマンド

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します。

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。

- debug crypto ipsec：フェーズ 2 の IPSec ネゴシエーションを表示します。

- debug crypto isakmp：フェーズ 1 の Internet Security Association and Key Management Protocol（ISAKMP）ネゴシエーションを表示します。
- debug crypto engine：暗号化されたトラフィックを表示します。
- debug ip nat detailed：（オプション）ルータで変換されたすべてのパケットに関する情報を表示することによって、NAT 機能の動作を確認します。

  注意：このコマンドを実行すると、大量の出力が生成されます。このコマンドは、IP ネットワーク上のトラフィックが低い場合にのみ使用してください。
- clear crypto isakmp：フェーズ 1 に関連する SA をクリアします。
- clear crypto sa：フェーズ 2 に関連する SA をクリアします。
- clear ip nat translation：変換テーブルからダイナミック NAT 変換をクリアします。

関連情報

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。