ASA リリース 9.(X) 3 つの内部ネットワークとインターネットの接続の設定例

目次

概要

このドキュメントでは、3 つの内部ネットワークで使用するためにバージョン 9.1(5) の Cisco 適応型セキュリティ アプライアンス (ASA) を設定する方法について説明します。 話を簡単にするため、ルータでスタティック ルートを使用します。

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

このドキュメントの情報は、Cisco 適応型セキュリティ アプライアンス (ASA) バージョン 9.1(5) に基づくものです。

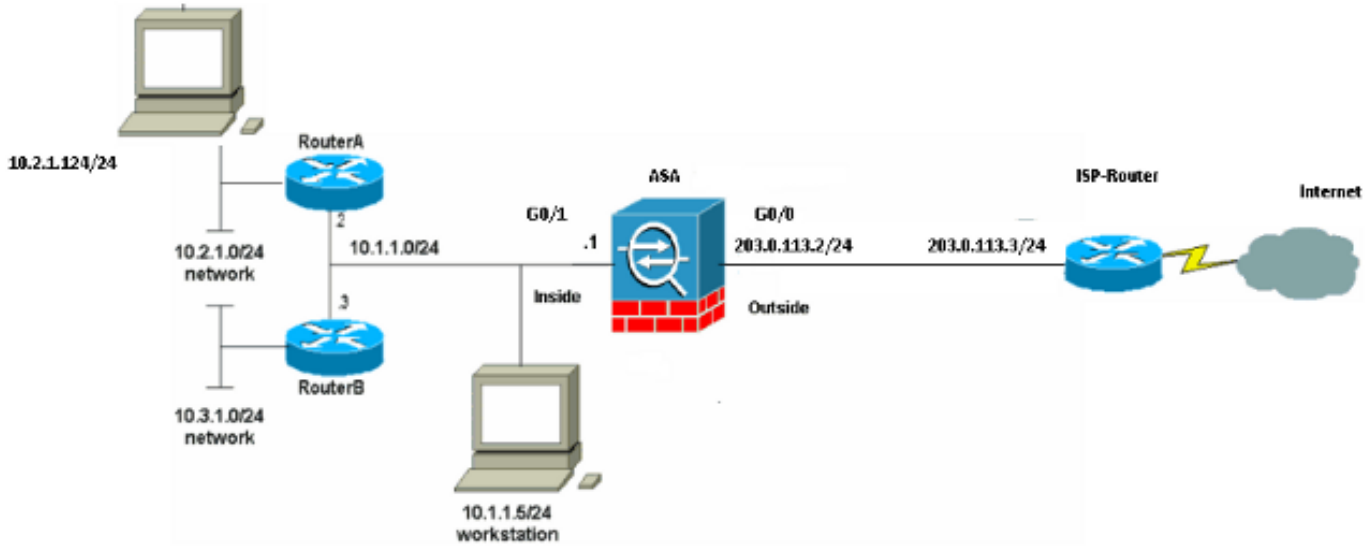
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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:** このセクション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



> **注:** この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 で使用されているアドレスであり、ラボ環境で使用されたものです。

ASA 9.1 の設定

このドキュメントでは、次の設定を使用します。 ご使用のシスコ デバイスの **write terminal** コマンドの出力データがある場合は、アウトプット インタープリタ（登録ユーザ専用）を使用して、今後予想される障害や修正を表示できます。

設定

- ルータ A の設定
- ルータ B の設定
- ASA リビジョン 9.1 以降の設定

ルータ A の設定

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

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
```

```
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

ルータ B の設定

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

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
```

```
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA リビジョン 9.1 以降の設定

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
```

```
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

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。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

Web ブラウザで HTTP を介して Web サイトにアクセスしてみます。 この例では 198.51.100.100 でホストされているサイトを使用します。 接続が成功すると、次の出力が ASA CLI に表示されます。

接続

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
flags UIO
```

ASA はステートフル ファイアウォールであり、Web サーバからのリターン トラフィックはファイアウォール接続テーブルの***接続***の 1 つと一致するため、ファイアウォールの通過を許可されます。 事前に存在する接続の 1 つと一致するトラフィックは、インターフェイス ACL によってブロックされないでファイアウォールの通過を許可されます。

上の出力では、内部インターフェイス上のクライアントが外部インターフェイスからの 198.51.100.100 ホストへの接続を確立しました。 この接続では TCP プロトコルが使用されており、6 秒間アイドル状態です。 接続のフラグは、この接続の現在の状態を示します。 接続のフラグの詳細については、「ASA の TCP 接続フラグ」を参照してください。

Syslog

```
ASA(config)# show log | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

ASA ファイアウォールは正常動作中に syslog を生成します。 syslog の冗長さはログ設定に基づいて変化します。 この出力はレベル 6、つまり「情報」レベルでの 2 種類の syslog を示します。

この例では、2 種類の syslog が生成されています。 1 番目は、ファイアウォールが変換を作成したこと、具体的にはダイナミック TCP 変換（PAT）を行ったことを示すログ メッセージです。 これは、トラフィックが内部インターフェイスから外部インターフェイスに渡るときの、送信元 IP アドレスとポート、および変換後の IP アドレスとポートを示します。

2 番目の syslog は、ファイアウォールがクライアントとサーバ間のこの特定のトラフィック用に接続テーブルで接続を作成したことを示します。 この接続試行をブロックするようにファイアウォールが設定された場合や、その他の要因（リソース制約または設定ミスの可能性）によってこの接続の作成が妨げられる場合は、ファイアウォールは接続が確立されたことを示すログを生成しません。 通常は、代わりに、接続が拒否される理由や、接続の作成を妨げた要因に関する兆候を記録します。

NAT 変換

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

この設定の一部として、内部ホストの IP アドレスをインターネットでルーティングできるアドレスに変換するために PAT が設定されます。 これらの変換が作成されていることを確認するには、NAT 変換（xlate）テーブルをチェックします。 コマンド **show xlate** は **local** キーワードおよび内部ホストの IP アドレスと組み合わせると、そのホストの変換テーブルにあるすべてのエントリを表示します。 上記の出力は、内部インターフェイスと外部インターフェイス間でこのホストに対して現在作成された変換があることを示しています。 内部ホストの IP とポートは設定を通じて 203.0.113.2 アドレスに変換されます。 示されているフラグ **ri** は、変換が**ダイナミック**であり、**ポートマップ**であることを示しています。 異なる NAT 設定の詳細は、『NAT に関する情報』を参照してください。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ASA は接続をトラブルシュートするための複数のツールを提供しています。 設定を確認して前述の出力をチェックした後でも問題が解決されない場合、これらのツールとテクニックは接続障害の原因を判別するために役立つ場合があります。

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 1234 198.51.100.100 80


--Omitted--

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

ASA のパケット トレーサ機能を使用すると、シミュレートされたパケットを指定して、ファイアウォールでトラフィックを処理するときに通るさまざまなステップ、チェック、機能をすべて確認できます。 このツールを使用すると、ファイアウォールをパススルーすることが許可されるはずのトラフィックの例を識別するために役立ち、その 5 タプルを使用してトラフィックをシミュレートできます。 前記の例では、以下の条件を満たす接続試行をシミュレートするために、パケット トレーサを使用します。

- シミュレートされたパケットは**内部**に到達します。
- 使用されているプロトコルが **TCP** である。
- シミュレートされたクライアントの IP アドレスが **10.2.1.124** である。
- クライアントは送信元がポート **1234** であるトラフィックを送信している。
- トラフィックは、IP アドレス **198.51.100.100** のサーバ宛てに送信されます。
- トラフィックはポート **80** 宛てです。

コマンドにインターフェイス **outside** に関する言及がないことに注意してください。 これはパケット トレーサの設計による動作です。 このツールは、このタイプの接続試行をファイアウォールでどのように処理するのかを示し、ルーティングの方法や、どのインターフェイスから送信するのかが含まれます。 パケット トレーサの詳細については、パケット トレースを使用したパケットのトレースを参照してください。

キャプチャ

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured
```

```
  1: 11:31:23.432655       10.2.1.124.18711 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA ファイアウォールでは、インターフェイスに着信または発信するトラフィックをキャプチャできます。 このキャプチャ機能は、トラフィックがファイアウォールに着信したかやファイアウォールから送信したかを確実に保証できるため便利です。 前の例は、内部インターフェイスの **capin** と外部インターフェイスの **capout** という 2 個のキャプチャの設定を示しています。 capture コマンドは、**match** キーワードを使用します。キャプチャするトラフィックを具体的に指定できます。

キャプチャ **capin** に対しては、**tcp host 10.2.1.124 host 198.51.100.100** と一致する内部インターフェイス (入力または出力) 上のトラフィックを照合することを示しています。 つまり、**host 10.2.1.124** から **host 198.51.100.100** に送信されたかこの**逆**の TCP トラフィックをすべてキャプチャする必要があります。 **match** キーワードを使用すると、ファイアウォールでトラフィックを双方向でキャプチャできるようになります。 外部インターフェイスに定義された capture コマンドは、ファイアウォールがそのクライアントの IP アドレスに PAT を実行するため、内部クライアントの IP アドレスを参照しません。 したがって、そのクライアントの IP アドレスと**照合**できません。 代わりに、この例では、可能性のあるすべての IP アドレスがその基準と一致することを示すために **any** を使用します。

キャプチャを設定したら、次に接続の確立を再試行してから、**show capture *<capture_name>*** コマンドによるキャプチャの表示に進みます。 この例では、キャプチャにある TCP の 3 ウェイ ハンドシェイクによって明らかなようにクライアントがサーバに接続できたことを確認できます。