ASA 8.4(x) で単一の内部ネットワークをインターネットに接続する設定例

内容

概要

このドキュメントでは、単一の内部ネットワークで使用するためにバージョン 8.4(1) 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。

バージョン 8.2 以前の Cisco 適応型セキュリティ アプライアンス（ASA）の同一の設定については、「PIX/ASA：単一の内部ネットワークをインターネットと接続する設定例」を参照して、同じ設定を確認してください。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、バージョン 8.4(1) の ASA に基づくものです。

このマニュアルの情報は、特定のラボ環境に置かれた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、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

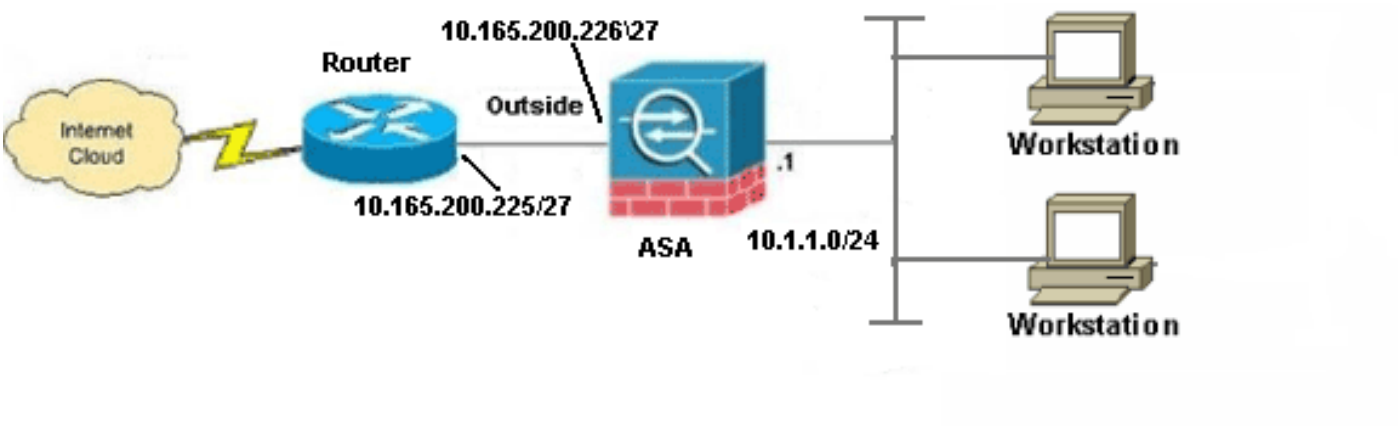
設定

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。



> **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。これらはラボ環境で使用された RFC 1918 のアドレスです。

ASA 8.4 の設定

このドキュメントでは、次の構成を使用します。

- ルータの設定
- ASA 8.4 以降の設定

ルータの設定

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

ASA 8.4 以降の設定

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
```

```
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
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 rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

注：ASA バージョン 8.4 でのネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）の設定に関する詳細については、「NAT に関する情報」を参照してください。

ASA バージョン 8.4 上のアクセス リスト設定の詳細は、『アクセス リストに関する情報』を参照してください。

確認

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ています。接続が成功すると、次の出力がASA CLIに表示されます。

Connection

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
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 | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

ASA ファイアウォールは正常動作中に syslog を生成します。Syslog の詳細レベルはログ設定に基づきます。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 つの 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な TCP の変換（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（Xlate）

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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、xlate（変換）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の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 10.165.200.226 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。さまざまなNAT設定の詳細については、『NATに関する情報』を参照してください。

トラブルシュート

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。

パケット トレーサ

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 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が内部に到達する。
- 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 **10.1.1.154** 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。
- トラフィックの宛先はポート 80 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 トレーサ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 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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については、**tcp host 10.1.1.154 host 198.51.100.100に一致する内部インターフェイス (入力または出力) で見られるトラフィックを照合することを指定しまし**た。つまり、**host 10.1.1.154からhostにに送信されるTCPトラフィックををキャプチャ** 198.51.100.100また。match キーワードを使用することで、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 アドレスとは照合できません。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。

関連情報

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems