PIX/ASA 7.x/FWSM 3.x： スタティック ポリシー NAT を使用した、複数のグローバル IP アドレスから単一のローカル IP アドレスへの変換

目次

概要

このドキュメントでは、PIX/Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) 7.x ソフトウェア上でポリシーベースのスタティック Network Address Translation (NAT; ネットワーク アドレス変換) を使用して、1 つのローカル IP アドレスを複数のグローバル IP アドレスにマッピングする設定例を示します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- PIX/ASA 7.x CLI に関する実務知識およびアクセス リストとスタティック NAT を設定した経験が必要です。

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。

- この具体例では ASA 5520 を使用します。 ただし、ポリシー NAT コンフィギュレーションは、7.x が稼働するすべての PIX または ASA アプライアンスで動作します。

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。

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。

設定

この設定例では、ASA の背後（192.168.100.50）に内部 Web サーバを持ちます。 このサーバから、内部 IP アドレス 192.168.100.50 および外部アドレス 172.16.171.125 を使用して外部ネットワーク インターフェイスにアクセス可能であることが要件です。 プライベート IP アドレス 192.168.100.50 には、ネットワーク 172.16.171.0/24 からのみアクセス可能であるというセキュリティ ポリシー要件もあります。 さらに、内部 Web サーバへの着信に許可されるプロトコルは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）およびポート 80 トラフィックのみです。 単一のローカル IP アドレスに 2 つのグローバル IP アドレスがマッピングされているため、ポリシー NAT を使用する必要があります。 そうしないと、PIX/ASA は、2 つの 1 対 1 スタティックを重複アドレス エラーとして拒否します。

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

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。

設定

このドキュメントでは次の設定を使用します。

```
ciscoasa(config)#show run : Saved : ASA Version 7.2(2) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface GigabitEthernet0/0 nameif
outside security-level 0 ip address 172.16.171.124
255.255.255.0 ! interface GigabitEthernet0/1 nameif
inside security-level 100 ip address 192.168.100.1
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 nameif
management security-level 100 ip address 192.168.1.1
255.255.255.0 management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- policy_nat_web1 and
policy_nat_web2 are two access-lists that match the
source !--- address we want to translate on. Two access-
lists are required, though they !--- can be exactly the
same. access-list policy_nat_web1 extended permit ip
host 192.168.100.50 any access-list policy_nat_web2
extended permit ip host 192.168.100.50 any !--- The
inbound_outside access-list defines the security policy,
as previously described. !--- This access-list is
applied inbound to the outside interface. access-list
inbound_outside extended permit tcp 172.16.171.0
```

```
255.255.255.0 host 192.168.100.50 eq www access-list
inbound_outside extended permit icmp 172.16.171.0
255.255.255.0 host 192.168.100.50 echo-reply access-list
inbound_outside extended permit icmp 172.16.171.0
255.255.255.0 host 192.168.100.50 echo access-list
inbound_outside extended permit tcp any host
172.16.171.125 eq www access-list inbound_outside
extended permit icmp any host 172.16.171.125 echo-reply
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo pager lines 24 logging asdm
informational mtu management 1500 mtu inside 1500 mtu
outside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400 !-
-- This first static allows users to reach the
translated global IP address of the !--- web server.
Since this static appears first in the configuration,
for connections !--- initiated outbound from the
internal web server, the ASA translates the source !---
address to 172.16.171.125. static (inside,outside)
172.16.171.125 access-list policy_nat_web1 !--- The
second static allows networks to access the web server
by its private !--- IP address of 192.168.100.50. static
(inside,outside) 192.168.100.50 access-list
policy_nat_web2 !--- Apply the inbound_outside access-
list to the outside interface. access-group
inbound_outside in interface outside route outside
0.0.0.0 0.0.0.0 172.16.171.1 1 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 uauth 0:05:00 absolute http
server enable http 192.168.1.0 255.255.255.0 management
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
context
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

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。

1. アップストリーム IOS® ルータ 172.16.171.1 上で、**ping** コマンドを使用して Web サーバの両方のグローバル IP アドレスに到達できることを確認します。`router#ping 172.16.171.125`
   `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.171.125, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms router#ping 192.168.100.50 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to`

```
192.168.100.50, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/1/4 ms
```

2. ASA 上で、変換（xlate）テーブルを表示してテーブル内に変換が組み込まれていることを確認します。`ciscoasa(config)#`**`show xlate global 192.168.100.50`** `2 in use, 28 most used` **`Global 192.168.100.50 Local 192.168.100.50`** `ciscoasa(config)#`**`show xlate global 172.16.171.125`** `2 in use, 28 most used` **`Global 172.16.171.125 Local 192.168.100.50`**

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。

ping または接続が失敗した場合は、Syslog を使用して変換設定に問題がないかを確認します。（ラボ環境などの）使用率の低いネットワークでは、通常は、ロギング バッファ サイズで十分問題をトラブルシューティングできます。 ロギング バッファ サイズでは十分でない場合は、Syslog を外部 Syslog サーバに送信する必要があります。 これらの Syslog エントリで設定が正しいことを確認するために、レベル 6 でのバッファへのロギングをイネーブルにします。

```
ciscoasa(config)#logging buffered 6 ciscoasa(config)#logging on !--- From 172.16.171.120,
initiate a TCP connection to port 80 to both the external !--- (172.16.171.125) and internal
addresses (192.168.100.50). ciscoasa(config)#show log Syslog logging: enabled Facility: 20
Timestamp logging: disabled Standby logging: disabled Deny Conn when Queue Full: disabled
Console logging: disabled Monitor logging: disabled Buffer logging: level debugging, 4223
messages logged Trap logging: disabled History logging: disabled Device ID: disabled Mail
logging: disabled ASDM logging: level informational, 4032 messages logged %ASA-5-111008: User
'enable_15' executed the 'clear logging buffer' command. %ASA-7-609001: Built local-host
outside:172.16.171.120 %ASA-7-609001: Built local-host inside:192.168.100.50 %ASA-6-302013:
Built inbound TCP connection 67 for outside:172.16.171.120/33687 (172.16.171.120/33687) to
inside:192.168.100.50/80 (172.16.171.125/80) %ASA-6-302013: Built inbound TCP connection 72 for
outside:172.16.171.120/33689 (172.16.171.120/33689) to inside:192.168.100.50/80
(192.168.100.50/80)
```

ログ内に変換エラーを見つけた場合は、NAT 設定を再度チェックします。 Syslog で確認しない場合は、ASA の **capture** 関数を使用してインターフェイス上のトラフィックのキャプチャを試行します。 キャプチャをセットアップするには、最初に特定タイプのトラフィックまたは TCP フローに一致するアクセス リストを指定する必要があります。 次に、キャプチャ パケットを開始するために、このキャプチャを 1 つ以上のインターフェイスに適用する必要があります。

```
!--- Create a capture access-list to match on port 80 traffic to !--- the external IP address of
172.16.171.125. !--- Note: These commands are over two lines due to spatial reasons.
ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.120 host 172.16.171.125 eq 80
ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.125 eq 80 host 172.16.171.120
ciscoasa(config)# !--- Apply the capture to the outside interface. ciscoasa(config)#capture
capout access-list acl_capout interface outside !--- After you initiate the traffic, you see
output similar to this when you view !--- the capture. Note that packet 1 is the SYN packet from
the client, while packet !--- 2 is the SYN-ACK reply packet from the internal server. If you
apply a capture !--- on the inside interface, in packet 2 you should see the server reply with
!--- 192.168.100.50 as its source address. ciscoasa(config)#show capture capout 4 packets
captured 1: 13:17:59.157859 172.16.171.120.21505 > 172.16.171.125.80: S 2696120951:2696120951(0)
win 4128 <mss 1460> 2: 13:17:59.159446 172.16.171.125.80 > 172.16.171.120.21505: S
1512093091:1512093091(0) ack 2696120952 win 4128 <mss 536> 3: 13:17:59.159629
172.16.171.120.21505 > 172.16.171.125.80: . ack 1512093092 win 4128 4: 13:17:59.159873
172.16.171.120.21505 > 172.16.171.125.80: . ack 1512093092 win 4128
```

関連情報

- ASA 7.2 コマンド リファレンス
- Cisco PIX Firewall ソフトウェア

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems