

2つの内部ネットワークとインターネットを備えた ASA 8.3(x) ダイナミック PAT 設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[ASA CLI 設定](#)

[ASDM の設定](#)

[確認](#)

[一般の PAT ルールの確認](#)

[特定の PAT ルールの確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、ソフトウェア バージョン 8.3(1) が稼動する Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) のダイナミック PAT の設定例を紹介し、[ダイナミック PAT](#) は、リアル送信元アドレスと送信元ポートを、マッピングされたアドレスと一意のマッピングされたポートに変換することで、複数のリアル アドレスをマッピングされた単一の IP アドレスに変換します。送信元ポートがそれぞれの接続で異なるので、それぞれの接続には別々の変換セッションが必要です。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- 内部ネットワークが ASA の Inside に次の 2 つのネットワークを備えていることを確認します。192.168.0.0/24 : ASA に直接接続されているネットワーク。192.168.1.0/24 : ASA の Inside にあるものの、別のデバイス (ルータなど) の後ろにあるネットワーク。
- 内部ユーザが次のように PAT を取得することを確認します。192.168.1.0/24 サブネット上のホストは、ISP によって提供された予備の IP アドレス (10.1.5.5) への PAT を取得。ASA の Inside の背後にある他のホストは、ASA の Outside インターフェイス IP アドレス (10.1.5.1) への PAT を取得。

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。

- バージョン 8.3(1) の Cisco 適応型セキュリティ アプライアンス (ASA)
- ASDM バージョン 6.3(1)

注: ASA を ASDM で設定できるようにするには、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

本書の情報は、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、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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

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 CLI 設定](#)
- [ASDM の設定](#)

ASA CLI 設定

このドキュメントでは次に示す設定を使用しています。

ASA ダイナミック PAT 設定

```
ASA#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.

!--- 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 10.1.5.1), for internet bound traffic.
ASA(config)#object network OBJ_GENERIC_ALL
ASA(config-obj)#subnet 0.0.0.0 0.0.0.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface

!--- The above statements are the equivalent of the !---
nat/global combination (as shown below) in v7.0(x), !---
```

```

v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 interface

!--- Creates an object called OBJ_SPECIFIC_192-168-1-0.
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0
ASA(config-obj)#subnet 192.168.1.0 255.255.255.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5

!--- The above statements are the equivalent of the
nat/global !--- combination (as shown below) in v7.0(x),
v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA
code: nat (inside) 2 192.168.1.0 255.255.255.0
global (outside) 2 10.1.5.5

```

ASA 8.3(1) の実行コンフィギュレーション

```

ASA#show run
: Saved
:
ASA Version 8.3(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 10.1.5.1 255.255.255.0 !--- Configure the inside
interface. ! interface GigabitEthernet0/1 nameif inside
security-level 100 ip address 192.168.0.1 255.255.255.0
! 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:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0
  subnet 192.168.1.0 255.255.255.0
object network OBJ_GENERIC_ALL
  subnet 0.0.0.0 0.0.0.0

pager lines 24
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400

nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface
nat (inside,outside) source dynamic OBJ_SPECIFIC_192-
168-1-0 10.1.5.5

route inside 192.168.1.0 255.255.255.0 192.168.0.254 1

```

```
route outside 0.0.0.0 0.0.0.0 10.1.5.2
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:6ffffbd3dc9cb863fd71c71244a0ecc5f
: end
```

[ASDM の設定](#)

ASDM インターフェイスからこの設定を行うには、次の手順を実行する必要があります。

1. 3つのネットワークオブジェクトを追加します。この例では、次のネットワークオブジェクトを追加します。OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. 2つのNAT/PATルールを作成します。この例では、次のネットワークオブジェクト用のNATルールを作成します。OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

ネットワークオブジェクトの追加

次の手順を実行して、ネットワークオブジェクトを追加します。

1. ASDM にログインし、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択します。
2. [Add] > [Network Object] を選択して、ネットワークオブジェクトを追加します。[Add Network Object] ダイアログボックスが表示されます。
3. 次の情報を [Add Network Object] ダイアログボックスに入力します。ネットワークオブジェクトの名前（この例では OBJ_GENERIC_ALL を使用しています）ネットワークオブジェクトのタイプ（この例では Network を使用しています）ネットワークオブジェクトのIPアドレス（この例では 0.0.0.0 を使用しています）ネットワークオブジェクトのネットマスク（この例では 0.0.0.0 を使用しています）
4. [OK] をクリックします。ネットワークオブジェクトが作成され、次の画面に示すように [Network Objects/Groups] のリストに表示されます。
5. 2番目のネットワークオブジェクトを追加するには、前の手順を繰り返して [OK] をクリックします。この例では次の値を使用しています。[Name] : OBJ_SPECIFIC_192-168-1-0Type: ネットワークIP アドレス : 192.168.1.0[Netmask] : 255.255.255.02番目のネットワークオブジェクトが作成され、次の画面に示すように [Network Objects/Groups] のリストに表示されます。
6. 3番目のネットワークオブジェクトを追加するには、前の手順を繰り返して [OK] をクリックします。この例では次の値を使用しています。[Name] : 10.1.5.5Type: HostIP アドレス : 10.1.5.53番目のネットワークオブジェクトが作成され、[Network Objects/Groups] のリストに表示されます。この時点で、[Network Objects/Groups] リストには、NATルールで参照のために必要な3つの必須オブジェクトが含まれています。

NAT/PAT ルールの作成

次の手順を実行して、NAT/PATルールを作成します。

1. 最初のNAT/PATルールを作成します。ASDMで、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] をクリックします。[Add NAT Rule] ダイアログボックスが表示されます。[Match Criteria: Original Packet] エリアで、[Source Interface] ドロップダウンリストから [inside] を選択します。参照をクリックして下さい (...) 送信元アドレステキストフィールドの右へ見つけられるボタン。[Browse Original Source Address] ダイアログボックスが表示されます。[Browse Original Source Address] ダイアログボックスで最初に作成したネットワークオブジェクトを選択します（たとえば、[OBJ_GENERIC_ALL] を選択します）。[Original Source Address] をクリックして、[OK] をクリックします。OBJ_GENERIC_ALL ネットワークオブジェクトが、[Add NAT Rule] ダイアログボックスの [Match Criteria: Original Packet] エリアにある [Source Address] フィールドに表示されるようになります。[Action: Translated Packet] エリアで、[Source NAT Type] ドロップダウンリストから [Dynamic PAT (Hide)] を選択します。参照をクリックして下さい (...) 送信元アドレスフィールドの右へ見つけられるボタン。[Browse Translated Source Address] ダイアログボックスが表示されます。[Browse Translated Source Address] ダイアログボックスで、[outside] インターフェイスオブジェクトを選択します（このインターフェイスはオリ

ジナル設定の一部なので、すでに作成されています)。[Translated Source Address] をクリックして [OK] をクリックします。Outside インターフェイスが、[Add NAT Rule] ダイアログ ボックスの [Action: Translated Packet] エリアにある [Source Address] フィールドに表示されるようになります。注: [Destination Interface] フィールドも Outside インターフェイスに変更されます。1 番目に作成した PAT ルールが次のように表示されることを確認します。 [Match Criteria: Original Packet] エリアで、次の値を確認します。 Source Interface = inside Source Address = OBJ_GENERIC_ALL Destination Address = any Service = any [Action: Translated Packet] エリアで、次の値を確認します。 Source NAT Type = Dynamic PAT (Hide) Source Address = outside Destination Address = Original Service = Original [OK] をクリックします。1 番目の NAT ルールは、次の画像に示すように ASDM に表示されます。

- 2 番目の NAT/PAT ルールを作成します。ASDM で、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] をクリックします。[Match Criteria: Original Packet] エリアで、[Source Interface] ドロップダウン リストから [inside] を選択します。参照をクリックして下さい (...) 送信元アドレス フィールドの右へ見つけられるボタン。[Browse Original Source Address] ダイアログ ボックスが表示されます。[Browse Original Source Address] ダイアログ ボックスで 2 番目に作成したオブジェクトを選択します (この例では、[OBJ_SPECIFIC_192-168-1-0] を選択します)。[Original Source Address] をクリックして、[OK] をクリックします。OBJ_SPECIFIC_192-168-1-0 ネットワーク オブジェクトが、[Add NAT Rule] ダイアログ ボックスの [Match Criteria: Original Packet] エリアにある [Source Address] フィールドに表示されるようになります。[Action: Translated Packet] エリアで、[Source NAT Type] ドロップダウン リストから [Dynamic PAT (Hide)] を選択します。[Source Address] フィールドの右側にある [...] ボタンをクリックします。[Browse Translated Source Address] ダイアログ ボックスが表示されます。[Browse Translated Source Address] ダイアログ ボックスで [10.1.5.5] オブジェクトを選択します (このインターフェイスはオリジナル設定の一部なので、すでに作成されています)。[Translated Source Address] をクリックして [OK] をクリックします。10.1.5.5 ネットワーク オブジェクトが、[Add NAT Rule] ダイアログ ボックスの [Action: Translated Packet] エリアにある [Source Address] フィールドに表示されるようになります。[Match Criteria: Original Packet] エリアで、[Destination Interface] ドロップダウン リストから [outside] を選択します。注: このオプションで *outside* を選択しない場合、宛先インターフェイスは *Any* を参照します。2 番目に完了した NAT/PAT ルールが次のように表示されることを確認します。[Match Criteria: Original Packet] エリアで、次の値を確認します。 Source Interface = inside Source Address = OBJ_SPECIFIC_192-168-1-0 Destination Address = outside Service = any [Action: Translated Packet] エリアで、次の値を確認します。 Source NAT Type = Dynamic PAT (Hide) Source Address = 10.1.5.5 Destination Address = Original Service = Original [OK] をクリックします。完成した NAT 設定は、次の画像に示すように ASDM に表示されます。

3. [Apply] ボタンをクリックして、実行コンフィギュレーションへの変更を適用します。

これによって、Cisco 適応型セキュリティ アプライアンス (ASA) へのダイナミック PAT の設定が完了します。

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。

[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。

一般の PAT ルールの確認

- **show local-host** : ローカル ホストのネットワーク状態を表示します。

```
ASA#show local-host
```

```
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
  TCP flow count/limit = 2/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited
!--- The TCP connection outside address corresponds !--- to the actual destination of
125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051,
  idle 0:00:03, bytes 13758, flags UIO
  TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
  bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
  TCP flow count/limit = 2/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
  UDP flow count/limit = 0/unlimited

!--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA -
10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
  ri idle 0:00:17 timeout 0:00:30
  TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
  ri idle 0:00:17 timeout 0:00:30
```

```
Conn:
```

```
  TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03,
  bytes 13758, flags UIO
  TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
  bytes 11896, flags UIO
```

- **show conn** : 指定された接続タイプの接続状態を表示します。

```
ASA#show conn
```

```
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06,
  bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01,
  bytes 13526, flags UIO
```

- **show xlate** : 変換スロットについての情報を表示します。

```
ASA#show xlate
```

```
4 in use, 7 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
  T - twice
TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
  ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
  ri idle 0:00:23 timeout 0:00:30
```

特定の PAT ルールの確認

- **show local-host** : ローカル ホストのネットワーク状態を表示します。

```
ASA#show local-host
```

```
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <125.252.196.170>,
  TCP flow count/limit = 2/unlimited
  TCP embryonic count to host = 0
  TCP intercept watermark = unlimited
```

```
UDP flow count/limit = 0/unlimited
!--- The TCP connection outside address corresponds to !--- the actual destination of
125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067,
    idle 0:00:07, bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066,
    idle 0:00:03, bytes 11896, flags UIO
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <192.168.0.5>,
TCP flow count/limit = 2/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
```

```
!--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.
Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
    ri idle 0:00:17 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
    ri idle 0:00:17 timeout 0:00:30
```

```
Conn:
TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
    bytes 13758, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
    bytes 11896, flags UIO
```

- [show conn](#) : 指定された接続タイプの接続状態を表示します。

```
ASA#show conn
2 in use, 3 most used
TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
    bytes 13653, flags UIO
TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,
    bytes 13349, flags UIO
```

- [show xlate](#) : 変換スロットについての情報を表示します。

```
ASA#show xlate
3 in use, 9 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
    T - twice
TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
    ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags
    ri idle 0:00:23 timeout 0:00:30
```

[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](#)

- [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 \(RFC \)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)