# ISP 冗長性が使用される場合に Twice NAT の NAT 転送動作を制御するために EEM を使用する設定例

## 目次



## 概要

この資料に二重 ISP シナリオ ( ISP 冗長性 ) でネットワーク アドレス変換 ( NAT ) の動作を制御するために組み込みイベント マネージャ ( EEM ) アプレットを使用する方法を転換します記述されています。

インターフェイス パケット出力判断がなされるとき接続が ( ASA ) ファイアウォールによって適応型セキュリティ アプライアンス ( ASA ) ソフトウェア処理されるとき、NAT ルールはルーティング テーブルに優先できることを理解しておくことは重要です。 着信パケットが NAT 文の変換された IP アドレスと一致する場合適切な出力 インターフェイスを判別するために、NAT ルールは使用されます。 これは「NAT として転換します」知られています。

( ルーティング テーブルを無効にすることができるものがである NAT はインターフェイスに着く着信パケットのための宛先アドレス 変換を規定 する NAT ルールがあるかどうか見るためにチェック ) チェックを転換します。 出力 インターフェイスを判別するためにあればそのパケットの宛先 IP アドレス、グローバル ルーティング テーブルを変換する方法を明示的に 規定 するルールは参照しません。 あればパケットの宛先 IP アドレス、NAT ルールを「変換する方法を明示的に 規定 するルールは引っ張るか」、または変換の他のインターフェイスにパケットを「転換し」、グローバル ルーティング テーブルは効果的にバイパスされます。

# 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

この文書に記載されている情報はソフトウェア リリース 9.2.1 を実行する ASA に基づいています。

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。

# 設定

> **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。

3 つのインターフェイスは設定されました; 、の外部で（プライマリ ISP）内部、および BackupISP（セカンダリ ISP）。 これら二つの NAT 文は特定のサブネット（203.0.113.0/24）に行くときどちらかのインターフェイス トラフィックを変換するために設定されました。

```
nat (any,Outside) source dynamic any 192.0.2.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
```

## 設定ルート トラッキング

```
sla monitor 40
type echo protocol ipIcmpEcho 192.0.2.254 interface Outside
num-packets 2
timeout 2000
threshold 500
frequency 10
sla monitor schedule 40 life forever start-time now

route Outside 203.0.113.0 255.255.255.0 192.0.2.254 1 track 40
route BackupISP 203.0.113.0 255.255.255.0 198.51.100.254 100
```

### プライマリ リンクがダウン状態になると何が起こりますか。

予想通りダウン状態になるプライマリ（外部で）リンク前トラフィックフロー Outside インターフェイス。 表の最初の NAT ルールは使用され、トラフィックは Outside インターフェイス

（192.0.2.100_nat）のための適切な IP アドレスに変換されます。 この場合 Outside インターフェイスはダウン状態になります、またはルート トラッキングは失敗します。 トラフィックはまだ最初の NAT 文に続き、Outside インターフェイスに転換する NAT **ない** BackupISP インターフェイスです。 これは NAT として知られている動作転換しますです。 203.0.113.0/24 に向かうトラフィックは効果的にブラックホール化されします。

この動作は**パケット トレーサー** コマンドで観察することができます。 **NAT に転換します UN-NAT** フェーズの行を注意して下さい。

```
ASA(config-if)#packet-tracer input inside tcp 10.180.10.10 1024 203.0.113.50 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff2af839a0, priority=1, domain=permit, deny=false
hits=1337149272, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (any,Outside) source dynamic any 192.0.2.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
Additional Information:
NAT divert to egress interface Outside
Untranslate 203.0.113.50/80 to 203.0.113.50/80

<Output truncated>

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: Outside
output-status: administratively down
output-line-status: down
Action: allow
```

これらの NAT ルールはルーティング テーブルを無効にする設計されています。 転換がこのソリューションが起こらないかもしれない Cisco バグ ID CSCul98420 のための修正とこれらのルール（および前に進む予期された動作最初の設定された出力 インターフェイスに）確定的にパケットを実際にはたらくかもしれませんがか転換します ASA バージョンがあり。 パケットはインターフェイスがダウン状態になるか、またはトラッキングされたルートが取除かれれば場合ここに廃棄されます。

## 回避策

設定の NAT ルールの存在が誤ったインターフェイスに転換するためにトラフィックを強制するので問題を回避するために設定行は一時的に削除される必要があります。 この手動操作の介入が時

間をかけるかもしれないし、停止が直面できるどんなに仕様 NAT 行の「いいえ」形式を入力することができないし。 プロセスを高速化するために、タスクは何らかの方法で自動化される必要があります。 これを ASA リリース 9.2.1 で導入される EEM 機能と達成することができます。 設定はここに示されています:

```
ASA(config-if)#packet-tracer input inside tcp 10.180.10.10 1024 203.0.113.50 80 detailed

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff2af839a0, priority=1, domain=permit, deny=false
hits=1337149272, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (any,Outside) source dynamic any 192.0.2.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
Additional Information:
NAT divert to egress interface Outside
Untranslate 203.0.113.50/80 to 203.0.113.50/80

<Output truncated>

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: Outside
output-status: administratively down
output-line-status: down
Action: allow
```

syslog 622001 が見られる場合処置をとるのに EEM が活用 されて いる場合のこのタスク作業。 この syslog は悩まされたルートがルーティング テーブルに再び取除かれるか、または追加されるとき生成されます。 Outside インターフェイスがダウン状態になるかまたはトラック ターゲットがもはや到達可能にならなければ、ルートを与えられて呼び出されるこの syslog を EEM アプレット先に示されている設定をトラッキングすることは生成され。 設定をトラッキングするルートの重要な側面は**イベント syslog ID 622001** 設定行**発生します 2** です。 これにより NAT2 アプレットは*その他*すべての時間 syslog が生成される起こります。 NAT アプレットは syslog が見られる度に呼び出されます。 この組み合せは取除かれる NAT 行という結果にとき syslog ID 622001 である見られる第 1 終ります（取除かれるトラッキングされたルート）およびそれから NAT 行は syslog 62201 見られます 2 回目に再追加されます（トラッキングされたルートはルーティング テーブルに再追加されました）。 これはルート トラッキング機能と共の NAT 行の自動削除および再付加の効果をもたらします。

# 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。

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。

確認を完了するためにトラッキングされたルートをルーティング テーブルから取除きますリンク障害を模倣して下さい。

## プライマリ ISP リンクをダウンさせて下さい

最初にプライマリ（外部で）リンクをダウンさせて下さい。

```
ciscoasa(config-if)# int gi0/0
ciscoasa(config-if)# shut
```

## インターフェイスはダウン状態になります

到達可能性がダウンしていることを Outside インターフェイスがダウン状態になるトラッキングオブジェクトが示すことに注意すれば。

```
%ASA-4-411004: Interface Outside, changed state to administratively down
%ASA-4-411004: Interface GigabitEthernet0/0, changed state to administratively down

ciscoasa(config-if)# show track
Track 40
Response Time Reporter 40 reachability
Reachability is Down
5 changes, last change 00:00:44
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

## EEM は引き起こされます

Syslog 622001 はルート削除の結果として生成され、EEM アプレット「NAT」は呼び出されます。 **提示イベント manager コマンド**の出力は個々のアプレットのステータスおよび実行行時を反映します。

```
%ASA-6-622001: Removing tracked route 203.0.113.0 255.255.255.0 192.0.2.254,
distance 1, table default, on interface Outside
%ASA-5-111008: User 'eem' executed the 'no nat (any,Outside) source dynamic
any 192.0.2.100_nat destination static obj_203.0.113.0 obj_203.0.113.0' command.
%ASA-5-111010: User 'eem', running 'CLI' from IP 0.0.0.0, executed 'no nat
(any,Outside) source dynamic any 192.0.2.100_nat destination static obj_203.0.113.0
obj_203.0.113.0'
%ASA-6-305010: Teardown static translation from Outside:203.0.113.0 to
any:203.0.113.0 duration 0:01:20

ciscoasa(config-if)# show event manager
Last Error: Command failed @ 2014/05/13 05:17:07
Consolidated syslog range: 622001-622001
event manager applet NAT, hits 3, last 2014/05/13 05:18:27
last file none
event syslog id 622001, hits 3, last 622001 @ 2014/05/13 05:18:27
action 1 cli command "no nat (any,Outside) source dynamic any 192.0.2.100_nat
```

```
destination static obj_203.0.113.0 obj_203.0.113.0", hits 3, last 2014/05/13 05:18:27
event manager applet NAT2, hits 1, last 2014/05/13 05:17:07
last file none
event syslog id 622001, hits 3, last 622001 @ 2014/05/13 03:11:47
action 1 cli command "nat (any,Outside) source dynamic any 192.0.2.100_nat
destination static obj_203.0.113.0 obj_203.0.113.0", hits 1, last 2014/05/13 05:17:07
```

## EEM 最初に NAT ルールによって取除かれます

実行コンフィギュレーションのチェックは最初の NAT ルールが取除かれたことを示します。

```
ciscoasa(config-if)# show run nat
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination static
obj_203.0.113.0 obj_203.0.113.0
```

## パケット トレーサーと確認して下さい

```
ciscoasa(config-if)# packet-tracer input inside icmp 10.180.10.10 8 0 203.0.113.100


Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff2b1862a0, priority=1, domain=permit, deny=false
hits=1, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
Additional Information:
NAT divert to egress interface BackupISP
Untranslate 203.0.113.50/80 to 203.0.113.50/80

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0
Additional Information:
Dynamic translate 10.180.10.10/0 to 198.51.100.100/47312
Forward Flow based lookup yields rule:
in id=0x7fff2b226090, priority=6, domain=nat, deny=false
hits=0, user_data=0x7fff2b21f590, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
dst ip/id=203.0.113.0, mask=255.255.255.0, port=0, tag=0, dscp=0x0
input_ifc=any, output_ifc=BackupISP
```

```
-------------Output Omitted -----------------

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

# 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。