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

内容

概要

このドキュメントでは、Embedded Event Manager(EEM)アプレットを使用して、デュアルISPシナリオ（ISP冗長性）でのネットワークアドレス変換(NAT)転送の動作を制御する方法について説明します。

適応型セキュリティアプライアンス(ASA)ファイアウォールを介して接続が処理される場合、パケットがどのインターフェイスに出力されるかを決定するときに、NATルールがルーティングテーブルよりも優先される可能性があることを理解することが重要です。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決定するためにNATルールが使用されます。これは「NAT転送」と呼ばれます。

NAT転送チェック（ルーティングテーブルを上書きできる内容）は、インターフェイスに着信する着信パケットの宛先アドレス変換を指定するNATルールがあるかどうかをチェックします。パケットの宛先IPアドレスの変換方法を明示的に指定するルールがない場合、出力インターフェイスを決定するためにグローバルルーティングテーブルが調べられます。パケットの宛先IPアドレスの変換方法を明示的に指定するルールがある場合、NATルールは変換の他のインターフェイスにパケットを「プル」または「転送」し、グローバルルーティングテーブルは実質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特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、ソフトウェアリリース9.2.1が稼働するASA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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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るコマンドの詳細については、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が設定されています。内部、外部（プライマリISP）、およびバックアップISP（セカンダリISP）。 これらの2つのNAT文は、特定のサブネット(203.0.113.0/24)に向かう場合にどちらのインターフェイスにもトラフィックを変換するように設定されています。

```
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
```

ルートトラッキングの設定

```
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するとどうなりますか

プライマリ（外部）リンクがダウンする前は、トラフィックはOutsideインターフェイスから期待どおりに流れます。テーブル内の最初のNATルールが使用され、トラフィックがOutsideインター

フェイス(192.0.2.100_nat)の適切なIPアドレスに変換されます。 これで、外部インターフェイスがダウンするか、ルートトラッキングが失敗します。トラフィックは引き続き最初のNAT文に従い、BackupISPインターフェイスではなくOutsideインターフェイスにNAT転送されます。これは、NAT即転送と呼ばれる動作です。203.0.113.0/24宛てのトラフィックは、実質的にブラックホール化されます。

この動作は、packet tracerコマンドで確認できます。NAT-NATフェーズのNAT Divert行に注意します。

```
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
```

これらのNATルールは、ルーティングテーブルを上書きするように設計されています。転送が発生しない可能性があるASAのバージョンもいくつかあり、このソリューションは実際に動作しますが、Cisco Bug ID CSCul98420に対する修正（および予想される転送の動作）により、パケットは必ず最初に設定出力インターフェイスに転送されます。インターフェイスがダウンしたり、トラッキング対象のルートが削除された場合、ここでパケットが廃棄されます。

回避策

設定にNATルールが存在するため、トラフィックは間違ったインターフェイスに転送されるため、問題を回避するために設定行を一時的に削除する必要があります。特定のNAT回線の「no」形

式を入力できますが、この手動による介入には時間がかかり、障害が発生する可能性があります。プロセスを高速化するには、何らかの方法でタスクを自動化する必要があります。これは、ASAリリース9.2.1で導入されたEEM機能を使用して実現できます。設定を次に示します。

```
event manager applet NAT
event syslog id 622001
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"
output none
event manager applet NAT2
event syslog id 622001 occurs 2
action 1 cli command "nat (any,Outside) 1 source dynamic any 192.0.2.100_nat destination
static obj_203.0.113.0 obj_203.0.113.0"
output none
```

このタスクは、syslog 622001が見つかった場合にEEMを使用してアクションを実行するときに機能します。このsyslogは、ラックに設置されたルートが削除されるか、ルーティングテーブルに再度追加されるときに生成されます。前に示したルートトラッキングの設定に従って、Outsideインターフェイスがダウンするか、またはトラックターゲットが到達不能になると、このsyslogが生成され、EEMアプレットが呼び出されます。ルートトラッキング設定の重要な側面は、イベントsyslog **id 622001 occurs 2の設定行**です。これにより、syslogが生成されるたびにNAT2*アプレット*が実行されます。NATアプレットは、syslogが表示されるたびに呼び出されます。この組み合わせにより、syslog ID 622001が最初に見つかった場合（追跡ルートが削除された場合）にNAT回線が削除され、次にsyslog 62201が見られた場合（追跡ルートがルーティングテーブルに再追加されたされました）に追加されます。 これは、ルートトラッキング機能と組み合わせてNAT回線を自動的に削除および再追加する効果があります。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

リンク障害をシミュレートします。これにより、追跡ルートがルーティングテーブルから削除され、検証が完了します。

プライマリISPリンクのダウン

最初に、プライマリ（外部）リンクをダウンさせます。

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

インターフェイスがダウン

外部インターフェイスがダウンし、トラッキングオブジェクトが到達可能性がダウンしていることを示していることに注意してください。

```
%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がトリガーされる

Syslog 622001はルートの削除の結果として生成され、EEMアプレット「NAT」が呼び出されます。show event managerコマンドの出力には、個々のアプレットのステータスと実行時間が反映されます。

```
%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の最初のNATルールが削除される

実行コンフィギュレーションをチェックすると、最初のNATルールが削除されたことが示されます。

```
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
```

Packet Tracerによる確認

```
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
```

トラブルシュート

現在、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。