NAT のサポート

機能の概要と変更履歴

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、CUPS UP におけるファイアウォール NAT ポートの解放動作の変更を明確化。	21.27.x
最初の導入。	21.24 より前

機能説明

CUPS はネットワークアドレス変換（NAT）をサポートしているため、ネットワークアドレスの設定が可能です。NAT IP アドレスと NAT ポートを使用して、UE の送信元 IP または送信元ポートアドレスをカプセル化したデータパケットを自動的に転送するようにシステムを設定できます。

サポートされる NAT の組み合わせは次のとおりです。

- NAT44 オンデマンド多対 1

- NAT44 オンデマンド 1 対 1
- NAT64 オンデマンド多対 1
- NAT 64 オンデマンド 1 対 1
- NAT44 非オンデマンド多対 1
- NAT44 非オンデマンド 1 対 1
- NAT64 非オンデマンド多対 1
- NAT64 非オンデマンド 1 対 1

NAT の補足情報については、StarOS の『*NAT Administration Guide*』[英語] を参照してください。

注：StarOS『 *NAT Administration Guide*』 に記載されているすべての機能が CUPS アーキテクチャに当てはまるわけではありません。

NAT ポート解放の動作

ICMP NAT ポートの使用率は、以下の理由により、レガシーよりも CUPS ソリューションで高くなります。

- レガシーでは、ICMP応答を受信すると、次のメッセージに使用できるようにNATポートが解放されます。CUPS では、100 番目の ICMP メッセージを受信した後にのみ NAT ポートが解放されます。
- レガシーでは、要求に対する ICMP 応答が受信されない場合、20 個の NAT ポートが連続的に割り当てられ、最初のポートから解放されます。CUPS では、100 番目の ICMP パケットの後にのみ削除が行われます。

制限事項

NAT のサポートには次の制限事項があります。

- 多対 1 およびオンデマンドモードの NAT44 のみがサポートされます。
- すべてのNATプールは、接続先コンテキストの個別のユーザープレーンで設定されます。
- fw-and-nat ポリシーでの CLI アクション拒否を使用した課金アクション、および active-charging-service での flow-any-error 課金アクションはサポートされていません。
- 「dynamic-only」および「static-and-dynamic」で設定されたアクセスルール：外部サーバーからのルールはサポートされません。
- 同じレルムからの複数の IP サポートは、この機能ではサポートされていません。
- NAT プールでのネクストホップ転送はサポートされていません。
- NAT プールのポート範囲はサポートされていません。

- プライベート IP チェック CLI のスキップはサポートされていません。
- RADIUS および Gy で返される Fw-and-nat ポリシーベースの NAT ポリシーの適用はサポートされていません。
- ベアラー固有のフィルタは、access-ruledefs ではサポートされていません。
- アクセスルールは、fw-and-nat ポリシーでの open-port ポート範囲設定のトリガーをサポートしていません。
- SR/ICSR 後の NAT ポートリカバリ（fw-and-nat アクション）はサポートされていません。
- NAT 再構成タイムアウト CLI は、active-charging サービスではサポートされていません。代わりに、UP の汎用コンテキストレベル CLI を使用する必要があります。
- NAT フラグメンテーションの再構成の失敗は、基本的な CUPS の再構成に関する未解決のバグによりサポートされていません。
- NAT flow-mapping タイマーはサポートされていません
- N:M 冗長性の場合、各 UP ホストのインターフェイス設定の一部として RCM から設定される NAT IP プール、およびプール名は、すべてのアクティブなユーザープレーンで一意である必要があります。そのため、fw-and-nat ポリシーで参照される同じ NAT レルムをすべてのユーザープレーンに適用できるように、すべてのプールに NAT グループを使用することが必須になります。
- N:M 冗長性の場合、RCM を介してすべての UP でまとめて設定される NAT IP プールの総数は、IP プールの最大制限数（2,000）に従う必要があります。すべてのアクティブ UP の累積合計が最大値を超えると、スタンバイユーザープレーンの設定は失敗します。

CUPS での NAT の設定

NAT の関連設定は CP で行われ、UP にプッシュされます。プール関連の設定のみがユーザープレーンに存在します。

NAT 関連の CLI コマンドの詳細については、StarOS NAT アドミニストレーション ガイド [英語] の「NAT Configuration」の章を参照してください。

注：StarOS NAT アドミニストレーション ガイド [英語] の「NAT Configuration」の章に記載されているすべての CLI コマンドと設定を CUPS アーキテクチャに適用できるわけではありません。

設定例

コントロール プレーン

次に、CUPS で NAT を有効にするためにコントロールプレーンで必要な設定例を示します。この設定は、PFD メカニズムを介したユーザープレーンの登録時にユーザープレーンにプッシュされます。

```
configure
active-charging service ACS
     access-ruledef all
       ip any-match = TRUE
     #exit
     access-ruledef udp
       udp any-match = TRUE
     #exit
     access-ruledef tcp
       tcp any-match = TRUE
     #exit
     access-ruledef icmp
       icmp any-match = TRUE
     #exit
     fw-and-nat policy NatPolicy1
        access-rule priority 1 access-ruledef tcp permit nat-realm NAT44_GRP1
        access-rule priority 2 access-ruledef icmp permit nat-realm NAT44_GRP1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only default-nat-realm NAT44_PUBLIC5
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     fw-and-nat policy NatPolicy2
        access-rule priority 1 access-ruledef all permit nat-realm NAT44_PUBLIC1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     rulebase cisco
     fw-and-nat default-policy NatPolicy1
     flow end-condition normal-end-signaling session-end timeout edr NBR
     #exit
#exit
end
```

ユーザープレーン

ISP コンテキストのユーザープレーンでは、次のプール関連の設定が必要です。

```
configure
   context ISP1-UP
      ip pool NAT44_PUBLIC1 209.165.200.225 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC2 209.165.200.226 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC3 209.165.200.227 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 8 max-chunks-per-user 1 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC4 209.165.200.228 255.255.255.224 napt-users-per-ip-address 4
 on-demand port-chunk-size 32256 max-chunks-per-user 4 group-name NAT44_GRP2
```

```
      ip pool NAT44_PUBLIC5 209.165.200.229 255.255.255.224 napt-users-per-ip-address
8064 on-demand port-chunk-size 8 max-chunks-per-user 2
      end
```

さまざまな NAT プールタイプの NAT プール関連の設定例

```
1-1 on-demand:
----------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_1_1 209.165.200.230 255.255.255.224 nat-one-to-one on-demand
nat-binding-timer 60
end

N-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_N_1 209.165.200.231 255.255.255.224 napt-users-per-ip-address 2
max-chunks-per-user 2 port-chunk-size 8
end

1-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_NOD_1_1 209.165.200.232 255.255.255.224 nat-one-to-one
end
```

Note コントロールプレーンの設定は、ユーザープレーンで設定された必須 NAT プール/グループのいずれかにマッピングされた 1 つ以上のアクセスルール定義とともに追加する必要があります。詳細については、『*Ultra Packet Core CUPS Control Plane Administration Guide*』[英語] を参照してください。

モニタリングおよびトラブルシューティング

NAT 統計の収集

次の表に、NAT 統計の収集に使用できるコマンドを示します。

最初の列には収集する統計、2 つ目の列には使用するコマンドを挙げています。

統計/情報	show コマンド
アクティブまたは休止中のセッションがある、現在のすべてのサブスクライバに関する情報。サブスクライバに関連付けられている IP アドレスを確認します。NAT レルムで使用されているすべての IP アドレスも表示されます。	**show subscribers user-plane-only full all**

統計/情報	show コマンド
NAT サブシステムの統計情報。	**show user-plane-service statistics all**
NAT 関連のすべての統計。	**show user-plane-service statistics nat all**
NAT レルム関連のすべての統計。	**show user-plane-service statistics nat nat-realm all**
NAT IP プールグループ内のすべての NAT IP プールの統計。	**show user-plane-service statistics nat nat-realm** *pool_name*
生成された NAT バインドレコードに関する情報。	**show user-plane-service edr-format statistics all**
UP の APN で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service pdn-instance name** *name*
UP での fw-an-nat ポリシーの設定を確認します。	**show user-plane-service fw-and-nat policy all**
ポートチャンクの割り当ておよび解放のために生成された NAT バインドレコードに関する情報。	**show user-plane-service rulebase name** *name*
アクセス ruledef に関する情報。	**show user-plane-service ruledef all**
UP の rulebase で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service rulebase name** *name*

clear コマンド

この機能をサポートする、次の clear CLI コマンドを使用できます。

- **clear user-plane-service statistics nat nat-realm all**
- **clear user-plane-service statistics nat all**

NAT パラメータしきい値の SNMP トラップ

NAT パラメータしきい値に対する次の SNMP トラップがサポートされます。

SNMP トラップ	説明
ThreshNATPortChunks	NAT ポートのチャンク使用率が、しきい値により設定された限度に達すると生成されます。
ThreshClearNATPortChunks	NAT ポートのチャンク使用率が、クリアしきい値により設定された限度に達すると生成されます。
ThreshNATPktDrop	NAT パケットドロップが、しきい値により設定された限度に達すると生成されます。

SNMP トラップ	説明
ThreshClearNATPktDrop	NAT パケットドロップが、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolUsed	IP プールで使用されている IP の数が、しきい値により設定された限度に達すると生成されます。
ThreshClearIPPoolUsed	IP プールで使用されている IP の数が、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolFree	IP プールが解放され、しきい値が定める限度に達すると生成されます。
ThreshClearIPPoolFree	IP プールが使用され、クリアしきい値が定める限度に達すると生成されます。
ThreshIPPoolAvail	IP プールが次のフローで使用可能になり、設定されたしきい値に達すると生成されます。
ThreshClearIPPoolAvail	IP プールが使用され、設定されたしきい値に達すると生成されます。

注：これらのトラップを有効にするには、それぞれの CLI をユーザープレーンで設定する必要があります。

バルク統計情報

コンテキストスキーマ

Table 1: コンテキストスキーマ

変数名	データ タイプ	カウンタタイプ	説明
nat-total-flows	Int64	Counter	NAT44 および NAT64 フローの総数
nat44-total-flows	Int64	Counter	NAT44 フローの総数
nat64-total-flows	Int64	Counter	NAT64 フローの総数
bypass-nat-total-flows	Int64	Counter	NAT44 および NAT64 バイパス NAT フローの総数
bypass-nat-ipv4-total-flows	Int64	Counter	NAT44 バイパス NAT フローの総数
bypass-nat-ipv6-total-flows	Int64	Counter	NAT64 バイパス NAT フローの総数
nat-current-flows	Int64	ゲージ	NAT44 および NAT64 フローの現在の数

変数名	データ タイプ	カウンタタイプ	説明
nat44-current-flows	Int64	ゲージ	NAT44 フローの現在の数
nat64-current-flows	Int64	ゲージ	NAT64 フローの現在の数
bypass-nat-current-flows	Int64	ゲージ	NAT44 および NAT64 バイパス NAT フローの現在の数
bypass-nat-ipv4-current-flows	Int64	ゲージ	NAT44 バイパス NAT フローの現在の数
bypass-nat-ipv6-current-flows	Int64	ゲージ	NAT64 バイパス NAT フローの現在の数
sfw-total-rxpackets	Int64	Counter	サービスによって受信されたパケットの総数
sfw-total-rxbytes	Int64	Counter	サービスによって受信されたバイトの総数
sfw-total-txpackets	Int64	Counter	サービスによって転送されたパケットの総数
sfw-total-txbytes	Int64	Counter	サービスによって転送されたバイトの総数
sfw-total-injectedpkts	Int64	Counter	サービスによって挿入されたパケットの総数
sfw-total-injectedbytes	Int64	Counter	サービスによって挿入されたバイトの総数
sfw-dnlnk-droppkts	Int64	Counter	サービスによってドロップされたダウンリンクパケットの総数
sfw-dnlnk-dropbytes	Int64	Counter	サービスによってドロップされたダウンリンクバイトの総数
sfw-uplnk-droppkts	Int64	Counter	サービスによってドロップされたアップリンクパケットの総数
sfw-uplnk-dropbytes	Int64	Counter	サービスによってドロップされたアップリンクバイトの総数

Note スキーマは CUPS のユーザープレーンでサポートされています。

ECS スキーマ

***Table 2: ECS* スキーマ**

変数名	データタイプ	カウンタタイプ	説明
nat-current-ipv4-pdn-subscribers	Int32	ゲージ	現在の NAT IPv4 PDN サブスクライバ数
nat-current-ipv6-pdn-subscribers	Int32	ゲージ	現在の NAT IPv6 PDN サブスクライバ数
nat-current-ipv4v6-pdn-subscribers	Int32	ゲージ	現在の NAT IPv4v6 PDN サブスクライバ数
nat-total-ipv4-pdn-subscribers	Int64	Counter	NAT IPv4 PDN サブスクライバの総数
nat-total-ipv6-pdn-subscribers	Int64	Counter	NAT IPv6 PDN サブスクライバの総数
nat-total-ipv4v6-pdn-subscribers	Int64	Counter	NAT IPv4v6 PDN サブスクライバの総数
nat-current-ipv4-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv4 PDN サブスクライバ数
nat-current-ipv6-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv6 PDN サブスクライバ数
nat-current-ipv4v6-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv4v6 PDN サブスクライバ数
nat-total-ipv4-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv4 PDN サブスクライバの総数
nat-total-ipv6-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv6 PDN サブスクライバの総数
nat-total-ipv4v6-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv4v6 PDN サブスクライバの総数
nat-total-unsolicited-dwnlnk-pkts	Int64	Counter	受信した不正ダウンリンクパケットの合計数

変数名	データタイプ	カウンタタイプ	説明
nat-total-icmp-hu-sent-for-dwnlnk-pkts	Int64	Counter	ダウンリンクパケットで送信された ICMP ホスト到達不能の合計数

Note スキーマは CUPS のユーザープレーンでサポートされています。

NAT レルムスキーマ

NAT レルムはユーザープレーンで設定され、統計情報はコンテキストごと、レルムごとに保存されます。これらの統計変数（累積とスナップショットの両方）は、NAT レルムスキーマで使用できます。

***Table 3: NAT* レルムスキーマ**

変数名	データ型	カウンタタイプ	説明
Vpnname	文字列	Info	コンテキスト名
Realmname	文字列	Info	レルム名。
nat-rlm-bind-updates	Int64	Counter	送信された暫定 AAA NBU の合計。
nat-rlm-bytes-txferred	Int64	Counter	レルムによって転送された NAT44 および NAT64 バイトの合計数（アップリンク+ダウンリンク）。
nat-rlm-bytes-nat44-tx	Int64	Counter	レルムによって転送された NAT44 バイトの合計数。
nat-rlm-bytes-nat64-tx	Int64	Counter	レルムによって転送された NAT64 バイトの合計数。
nat-rlm-ip-flows	Int64	Counter	レルムで使用された NAT44 および NAT64 フローの総数。
nat-rlm-nat44-flows	Int64	Counter	レルムによって処理された NAT44 フローの総数。
nat-rlm-nat64-flows	Int64	Counter	レルムによって処理された NAT64 フローの総数。
nat-rlm-ip-denied	Int32	Counter	NAT IP アドレスが拒否された NAT44 および NAT64 フローの総数。

変数名	データ型	カウンタタイプ	説明
nat-rlm-ip-denied-nat44	Int64	Counter	IP が拒否された NAT44 フローの総数。
nat-rlm-ip-denied-nat64	Int64	Counter	IP が拒否された NAT64 フローの総数。
nat-rlm-port-denied	Int32	Counter	ポートが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-port-denied-nat44	Int64	Counter	ポートが拒否された NAT44 フローの総数。
nat-rlm-port-denied-nat64	Int64	Counter	ポートが拒否された NAT64 フローの総数。
nat-rlm-memory-denied	Int64	Counter	メモリが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-memory-denied-nat44	Int64	Counter	メモリが拒否された NAT44 フローの総数。
nat-rlm-memory-denied-nat64	Int64	Counter	メモリが拒否された NAT64 フローの総数。
nat-rlm-ttl-ips	Int32	ゲージ	NAT レルムあたりのコンテキストごとの NAT パブリック IP アドレスの総数。スタティック値です。
nat-rlm-ips-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに、現在使用されている NAT IP アドレスの総数。
nat-rlm-current-users	Int32	ゲージ	NAT レルムを現在使用しているサブスクライバの総数。
nat-rlm-ttl-port-chunks	Int32	ゲージ	NAT レルムあたりのコンテキストごとのポートチャンクの総数。スタティック値です。
nat-rlm-chunks-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに現在使用されているポートチャンクの総数。
nat-rlm-port-chunk-size	Int32	ゲージ	NAT レルムのポートチャンクのサイズ。

変数名	データ型	カウンタタイプ	説明
nat-rlm-port-chunk-average-usage-tcp	Int32	ゲージ	割り当てられた TCP ポートの平均 TCP ポート使用率。つまり、割り当てられた TCP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-udp	Int32	ゲージ	割り当てられた UDP ポートの平均 UDP ポート使用率。つまり、割り当てられた UDP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-others	Int32	ゲージ	割り当てられた他のポートでの他の（ICMP または GRE）ポートの平均使用率（つまり、割り当てられた「他の」ポートのうち、使用された数）。パーセンテージ値ではありません。
nat-rlm-max-port-chunk-subs	Int64	Counter	最大数のポートチャンクを使用したサブスクライバの総数。
nat-rlm-max-port-chunk-used	Int32	Counter	使用された最大ポートチャンク数。
nat-rlm-max-cur-port-chunk-subs	Int64	ゲージ	ポートチャンクの最大数を使用している現在のサブスクライバ数。
nat-rlm-max-cur-port-chunk-used	Int32	ゲージ	アクティブなサブスクライバによって使用された最大ポートチャンク数。

EDR

通常の EDR では、次の NAT 固有の属性がサポートされています。

- sn-nat-subscribers-per-ip-address：NAT IP アドレスごとのサブスクライバ
- sn-subscriber-nat-flow-ip：NAT 対応サブスクライバの NAT IP アドレス
- sn-subscriber-nat-flow-port：NAT 対応サブスクライバの NAT ポート番号

EDR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,sn-server-port,
sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,sn-nat-realm-name,
sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,sn-nat-port-chunk-alloc-time-gmt,
sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
```

```
02/18/2020 12:11:11:630,02/18/2020
12:11:11:632,1,209.165.200.225,209.165.201.1,0,0,,,,209.165.200.230,1024,,2,,,,,,0,0
02/18/2020 12:11:08:672,02/18/2020
12:11:09:671,6,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.230,1034,,2,,,,,,0,0
02/18/2020 12:11:14:499,02/18/2020
12:11:14:499,17,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.240,1025,,8064,,,,,,0,0
```

NAT バインドレコード

NAT IP アドレスまたは NAT ポートチャンクがサブスクライバとの間で割り当てまたは割り当て解除されるたびに、NAT バインドレコード（NBR）を生成できます。NBR の生成は、ファイアウォールと NAT ポリシーの設定で設定できます。

NBR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,
sn-server-port,sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,
sn-nat-realm-name,sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,
sn-nat-port-chunk-alloc-time-gmt,sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
,,,209.165.200.225,,,,209.165.201.1,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,1,02/18/2020
06:41:08,,,
,,,209.165.200.225,,,,209.165.201.2,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,1,02/18/2020
 06:41:14,,,
,,,209.165.200.225,,,,209.165.201.3,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,0,02/18/2020
06:41:08,02/18/2020 06:42:12,,
,,,209.165.200.225,,,,209.165.201.14,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,0,02/18/2020
 06:41:14,02/18/2020 06:44:24,,
```

パケットドロップ EDR

パケットドロップ EDR の例

```
#sn-nat-no-port-packet-dropped,sn-start-time,sn-end-time,sn-subscriber-imsi
2,03/13/2020 08:28:24,03/13/2020 08:28:54,123456789012345
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。