http://www.rtpro.yamaha.co.jp/RT/docs/relnote/Rev.15.02/relnote_15_02_29.html

Revision : 15.02.29

Release : Mar. 2023, ヤマハ株式会社

RTX830 Rev.15.02.29 リリースノート

---

〇ファームウェアのリビジョンアップを行う前に必ずお読みください

---

・Rev.15.02.03より前のファームウェアからリビジョンアップを行う際には以下の点にご注意ください

Rev.15.02.03では以下の変更をしています。

「RTX830 Rev.15.02.03 リリースノート」より、

http://www.rtpro.yamaha.co.jp/RT/docs/relnote/Rev.15.02/relnote_15_02_03.html

[1] 本機にアクセスするときのセキュリティーを強化した。

(8) 工場出荷状態の設定にtelnetd host lanコマンドを追加した。

Rev.15.02.03以降のファームウェアを使用して工場出荷状態からプロバイダーを設定すると、上記のコマンドが設定されているため遠隔からTELNETでログインができなくなります。
遠隔からTELNETでログインをする場合はtelnetd hostコマンドの設定を変更してくだ

さい。

・Rev.15.02.13より前のファームウェアからリビジョンアップを行う際には以下の点にご注意ください

「DPIを使用したアプリケーション制御機能」に対応したRev.15.02.13以降のファームウェアへリビジョンアップすると、Rev.15.02.10、またはそれ以前のファームウェアに対して工場出荷状態でのメモリー使用率が10%程度上昇します。

メモリーの空き容量が十分あることを確認のうえ、リビジョンアップを行うようにしてください。

---

〇RTX830 Rev.15.02.26 からの変更点
（メーカーリリース版 Rev.15.02.27～28 を含む）

---

■機能追加

[1] IKEv2で、Configuration Payloadに対応した。
この変更により、AndroidとiOSの端末でIKEv2を使ったリモートアクセスVPN接続が可能になる。

外部仕様書をよくご確認のうえ、ご利用ください。

http://www.rtpro.yamaha.co.jp/RT/docs/ipsec/ikev2_ras/index.html

[2] コマンドラインからOSPF、BGP、OSPFv3を設定したとき、以下の各コマンドの実行を促す注意喚起メッセージを表示するようにした。

- OSPF：ospf configure refreshコマンド
- BGP：bgp configure refreshコマンド
- OSPFv3：ipv6 ospf configure refreshコマンド

[3] コマンドラインから以下を設定したとき、再起動を促す注意喚起メッセージを表示するようにした。

- nat descriptor backward-compatibilityコマンド
- system packet-bufferコマンド

[4] IPv6の経路情報に変化があった時にログに記録するか否かを設定するコマンドを追加した。

〇IPv6の経路情報に変化があった時にログに記録するか否かの設定 ★

[書式]

ipv6 route change log LOG

no ipv6 route change log [LOG]

[設定値及び初期値]

・LOG

[設定値] :

on : IPv6経路の変化をログに記録する

off: IPv6経路の変化をログに記録しない

[初期値] : off

[説明]

IPv6の経路情報に変化があった時にそれをログに記録するか否かを設定する。

ログはINFOレベルで記録される。

[5] IPv6の経路情報に変化があった時にメールで通知するか否かをmail notifyコマンド

のオプションで設定できるようにした。

〇メール通知のトリガーの設定

[書式]

mail notify ID TEMPLATE_ID trigger backup IF_B [[RANGE_B] IF_B ...]

mail notify ID TEMPLATE_ID trigger route ROUTE [ROUTE ...]

mail notify ID TEMPLATE_ID trigger route6 ROUTE6 [ROUTE6 ...] ★

mail notify ID TEMPLATE_ID trigger filter ethernet IF_F DIR_F [IF_f DIR_F ...]

mail notify ID TEMPLATE_ID trigger status TYPE [TYPE ...]

mail notify ID TEMPLATE_ID trigger intrusion IF_I [RANGE_I] DIR_I [IF_I [RANGE_I] DIR_I ...]

mail notify ID TEMPLATE_ID trigger qac-tm QAC_TYPE

mail notify ID TEMPLATE_ID trigger lan-map

no mail notify ID [...]

[設定値及び初期値]

・ID

[設定値] : 設定番号(1..10)

[初期値] : -

・TEMPLATE_ID

[設定値] : テンプレートID(1..10)

[初期値] : -

・IF_B : メール通知を行うバックアップ対象のインターフェース

[設定値] :

---

設定値　説明

---

pp　PPバックアップ

lanN　LANバックアップ

tunnel　TUNNELバックアップ

---

[初期値] : -

・RANGE_B

[設定値] :

インターフェース番号および範囲指定

pp,tunnelのみ(*,xx-yy,zz etc)

[初期値] : -

・ROUTE

[設定値] :

ネットマスク付きの経路

default

[初期値] : -

・ROUTE6 ★

[設定値] :

プレフィックス長付きの経路

default

[初期値] : -

・IF_F

[設定値] : メール通知を行うイーサネットフィルターの設定されたLANイン

ターフェース

[初期値] : -

・DIR_F : フィルター設定の方向

[設定値] :

---

設定値 説明

---

in 受信方向

out 送信方向

---

[初期値] : -

・TYPE : メール通知で通知する情報

[設定値] :

---

設定値　説明

---

all　全ての内容

interface　インターフェースの情報

routing　ルーティングの情報

vpn　VPN の情報

nat　NAT の情報

firewall　ファイアウォールの情報

config-log　設定情報とログ

---

[初期値] : -

・IF_I : 不正アクセス検知設定のインターフェース

[設定値] :

---

設定値　説明

---

pp　PPインターフェース

lanN(N,M,N/M)　LANインターフェース

wan1　WANインターフェース

tunnel　TUNNELインターフェース

*　全てのインターフェース

---

[初期値] : -

・RANGE_I

[設定値] :

インターフェース番号および範囲指定

lan(*,x)

pp,tunnel(*,x,xx-yy,zz etc)

[初期値] : -

・DIR_I : 不正アクセス検知設定の方向

[設定値] :

---

設定値 説明

---

in 受信方向

out 送信方向

in/out 受信/送信方向

---

[初期値] : -

・QAC_TYPE : QAC/TM機能

[設定値] :

---

設定値 説明

---

server-error 管理サーバー情報更新失敗時

unqualified 不適格PC接続時

---

[初期値] : -

[説明]

メール通知の行うトリガー動作の設定を行う。バックアップ、経路変更、イーサネットフィルターのログ表示、mail notify status execコマンド実行時、および不正アクセス検知時をトリガーとして指定できる。

バックアップおよび経路については以下で設定されたものが対象となる。

---

PPバックアップ ¦ pp backup コマンド

LANバックアップ ¦ lan backup コマンド

TUNNELバックアップ ¦ tunnel backup コマンド

経路に対するバックアップ(IPv4) ¦ ip route コマンド

経路に対するバックアップ(IPv6) ¦ ipv6 route コマンド ★

---

イーサネットフィルターについてはログ表示されるものが対象となる。

イーサネットフィルター..... pass-log,reject-logパラメーターの定義

内部状態を通知する場合は、mail notify status execコマンドを実行する必要がある。

不正アクセス検知についてはip interface intrusion detectionコマンドの設定により検出されたものが通知対象となる。

QAC/TM機能については以下の条件が対象となる。

・管理サーバー情報の更新に失敗したとき

・クライアントPCの接続時の認定で不適格と判定したとき

LANマップによる異常検知についてはswitch control use interfaceコマンドが設定されたLANインターフェースが対象となる。

スナップショット機能による異常を含める場合は

lan-map snapshot use interfaceコマンドを設定する必要がある。

また、一つのテンプレートIDに所属するメール通知設定はまとめて処理される。

[6] IPヘッダーおよびIPv6ヘッダーのDSフィールドを書き換えるコマンドを追加した。

〇IPパケットのDSフィールドの書き換えの設定

[書式]

ip dscp supersede ID DSCP FILTER_NUM [FILTER_NUM_LIST]

no ip dscp supersede ID [DSCP]

[設定値及び初期値]

・ID

[設定値] : 識別番号 (1..65535)

[初期値] : -

・DSCP

[設定値] :

・書き換えるDSCP値 (0..63)

・以下のニーモニックが利用できる

・cs1/cs2/cs3/cs4/cs5/cs6/cs7/af11/af12/af13/af21/af22/af23/
af31/af32/af33/af41/af42/af43/ef

[初期値] : -

・FILTER_NUM

[設定値] : 静的フィルターの番号 (1..21474836)

[初期値] : -

・FILTER_NUM_LIST

[設定値] : 静的フィルターの番号 (1..21474836) の並び

[初期値] : -

[説明]

IP パケットを中継する場合に DS フィールドを指定した値に書き換える。
識別番号順にリストをチェックし、filter_num リストのフィルターを順次適用していく。そして、最初にマッチした IP フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。

reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

ip tos supersede コマンドの設定と本コマンドの設定で条件が同じ場合、本コマンドの設定が優先される。

[ノート]

RTX830 は Rev.15.02.27以降で使用可能。

〇IPv6パケットのDSフィールドの書き換えの設定

[書式]

ipv6 dscp supersede ID DSCP FILTER_NUM [FILTER_NUM_LIST]

no ipv6 dscp supersede ID [DSCP]

[設定値及び初期値]

・ID

[設定値] : 識別番号 (1..65535)

[初期値] : -

・DSCP

[設定値] :

・書き換えるDSCP値 (0..63)

・以下のニーモニックが利用できる

・cs1/cs2/cs3/cs4/cs5/cs6/cs7/af11/af12/af13/af21/af22/af23/af31/af32/af33/af41/af42/af43/ef

[初期値] : -

・FILTER_NUM

[設定値] : 静的フィルターの番号 (1..21474836)

[初期値] : -

・FILTER_NUM_LIST

[設定値] : 静的フィルターの番号 (1..21474836) の並び

[初期値] : -

[説明]

IPv6 パケットを中継する場合に DS フィールドを指定した値に書き換える。
識別番号順にリストをチェックし、filter_num リストのフィルターを順次適用していく。そして、最初にマッチした IPv6 フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。
reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

[ノート]
RTX830 は Rev.15.02.27以降で使用可能。

[7] ipsec ike durationコマンドで、古くなったSAの寿命を強制的に短縮する時間を設定できるようにした。

〇SAの寿命の設定

[書式]
ipsec ike duration SA GATEWAY_ID SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME] ★
no ipsec ike duration SA GATEWAY_ID [SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]] ★

[設定値及び初期値]
・SA
[設定値] :

| 設定値 | 説明 |
|---|---|
| ipsec-sa (もしくは child-sa) | IPsec SA (CHILD SA) |
| isakmp-sa (もしくは ike-sa) | ISAKMP SA (IKE SA) |

[初期値] : -
・GATEWAY_ID

[設定値] : セキュリティー・ゲートウェイの識別子

[初期値] : -

・SECOND

[設定値] : 秒数(300..691200)

[初期値] : 28800

・KBYTES

[設定値] : キロ単位のバイト数

---

設定値　　説明

---

100..2147483647 キロ単位のバイト数 (RTX830 Rev.15.02.27以降のファームウェア)

100..100000　キロ単位のバイト数 (その他のファームウェア)

off　　設定しない

---

[初期値] :

- 2000000 (RTX830 Rev.15.02.27以降のファームウェア)

- off (その他のファームウェア)

・REKEY : SAを更新するタイミング

[設定値] :

---

設定値　説明

---

70% - 90% パーセント

off　　更新しない(SAパラメーターでisakmp-sa (ike-sa) を指定したときのみ設定可能)

---

[初期値] : 75%

・DEL_TIME ★

[設定値] : 古くなったSAの寿命を強制的に短縮する時間(1..691200)

[初期値] : -

[説明]

各 SA の寿命を設定する。

KBYTES パラメーターを指定した場合には、 SECOND パラメーターで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。KBYTES パラメーターは SA パラメーターとして ipsec-sa (child-sa) を指定したときのみ有効である。SA の更新は KBYTES パラメーターに設定したバイト数の75%を処理したタイミングで行われる。また、IPsec SA が更新されたとき古くなった既存の IPsec SA の寿命が 30 秒以上である場合は、寿命が 30 秒に短縮される。

REKEY パラメーターは SA を更新するタイミングを決定する。例えば、 SECOND パラメーターで 20000 を指定し、 REKEY パラメーターで75%を指定した場合には、SA を生成してから 15000 秒経過したときに新しい SA を生成する。 REKEY パラメーターは SECOND パラメーターに対する比率を表すもので、 KBYTES パラメーターの値とは関係がない。

SA パラメーターで isakmp-sa(ike-sa) を指定したときに限り、REKEY パラメーターで 'off' を設定できる。このとき、 IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、 ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作するIKEのバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

・IKEv1

始動側として働く場合に、このコマンドで設定した寿命値が提案される。応

答側として働く場合は、このコマンドの設定に関係なく相手側から提案された寿命値に合わせる。

また、 ISAKMP SA に対する REKEY パラメーターを off に設定した場合、その効果を得るためには、次の2点に注意して設定する必要がある。

1. IPsec SAよりも ISAKMP SA の寿命を短く設定する。
2. ダングリングSAを許可する。すなわち、ipsec ike restrict-dangling-sa コマンドの設定を off にする。

RTX830 または、RTX1300、vRX が始動側になる場合は、最大で 2147483647 KB のバイト寿命値を相手側へ提案可能であるが、相手側機器が RTX830 および、RTX1300、vRX 以外の場合は 2 GB を超えるバイト寿命値を正しく認識できないため、RTX830 および、RTX1300、vRX 以外の機種と接続する場合は必ず 2 GB 以下に設定する必要がある。

・IKEv2

IKEv2 では SA 寿命値は折衝されず、各セキュリティー・ゲートウェイが独立して管理するものとなっている。従って、確立された SA には、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティー・ゲートウェイの方が SA 更新のタイミングが早ければ、 SA はその分早く更新されることになる。

forced-reduction オプションに時間を指定すると、SA を更新した際に古くなった既存の SA の寿命を強制的に設定値に変更し、消滅までの時間を早めることができる。ただし、IPsec SA で KBYTES パラメーターにバイト寿命値を指定している場合は、DEL_TIME パラメーターで 31 秒以上の値を設定していても、短縮される値は30 秒となる。また、IKEv1 では寿命が設定値よりも短い場合は変更しない。 ★

ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在するSAの寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

[ノート]

forced-reduction オプションは以下の機種およびリビジョンで使用可能。★

RTX830は Rev.15.02.27 以降。

[8] bgp export filterコマンドのpreferenceオプションが比較するBGP経路の種別を変更するコマンドを追加した。

○BGPで受信した経路に対するbgp export filterのpreferenceオプションを使用した経路選択プロセスの動作を設定 ★

[書式]

bgp export route selection rule RULE

no bgp export route selection rule [RULE]

[設定値及び初期値]

・RULE

[設定値] : ebgp-only, all

| 設定値 | 説明 |
|---|---|
| ebgp-only | eBGPで受信した同じ宛先の経路を比較対象とする。 |
| all | 全てのBGPで受信した同じ宛先の経路を比較対象とする。 |

[初期値] : ebgp-only

[説明]

BGP で同じ宛先の経路を複数の相手から受信した際、一方を選択するための優先度による比較対象を設定する。
本コマンドの設定により bgp export filter コマンドの preference オプションで比較する経路の種別が変更される。

RULE に ebgp-only を設定した場合、eBGP で受信した経路にのみ preference による比較が働く。このため、iBGP で受信した経路では、preference による比較は働かない。
RULE に all を設定した場合、全ての BGP で受信した経路に preference による比較が働く。このため、eBGP と iBGP で受信した経路間でも、preference による比較が働く。

従来 iBGP で受信した経路は eBGP で受信した経路よりも低い優先度の経路として扱われていたが、RULE に all を指定することで iBGP で受信した経路の優先度を eBGP で受信した経路よりも高くすることが可能になる。
また、bgp export filter コマンドの preference は Local Preference よりも高い優先度であるため、iBGP 経路同士の場合にもより柔軟にネットワークを設計することが可能になる。

本コマンドに対応していないリビジョンでは、RULE が ebgp-only のときの動作をする。

[ノート]

RTpro"BGP-4 仕様[http://www.rtpro.yamaha.co.jp/RT/docs/bgp/index.html]" に掲載している "コマンドで設定した優先度による比較" で比較する経路種別を制御することができる。
eBGP と iBGP 間で同じ宛先の経路を受信する環境下で特定の経路を優先するよう制御したい場合、本コマンドを設定することで実現できる。

RTX830 は、Rev.15.02.27 以降で使用可能。

[9] ipv6 routeコマンドで、ゲートウェイにRAにて決定されるデフォルトゲートウェイの指定を追加した。

〇IPv6の経路情報の追加

[書式]

ipv6 route NETWORK gateway GATEWAY [PARAMETER] [gateway GATEWAY [PARAMETER]]

no ipv6 route NETWORK [gateway...]

[設定値及び初期値]

・NETWORK

[設定値]

| 設定値 | 説明 |
|---|---|
| IPv6 アドレス/プレフィックス長 | 送り先のホスト |
| default | デフォルト経路 |

[初期値] : -

・GATEWAY : ゲートウェイ

[設定値] :

・IP アドレス % スコープ識別子

・pp PEER_NUM [dlci=DLCI] : PP インターフェースへの経路。
"dlci=dlci" が指定された場合は、フレームリレーの DLCI への経路

・PEER_NUM

・相手先情報番号

・anonymous

・pp anonymous name=NAME

---

設定値 説明

---

name　PAP/CHAP による名前

・dhcp INTERFACE

---

設定値　説明

---

INTERFACE DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インターフェース名、ブリッジインターフェース名(送り先がDefaultの時のみ有効)

・ra INTERFACE ★

---

設定値　説明

---

INTERFACE RA にて決定されるデフォルトゲートウェイを使う場合の、RAクライアントとして動作する LAN インターフェース名、ブリッジインターフェース名(送り先がDefaultの時のみ有効)

・tunnel TUNNEL_NUM : トンネルインターフェースへの経路

・LOOPBACK インターフェース名、NULL インターフェース名

[初期値] : -

・PARAMETER : 以下のパラメーターを空白で区切り複数設定可能

[設定値]

---

設定値 説明

---

metric メトリックの指定

METRIC ・METRIC

・メトリック値 (1..15)

・省略時は 1

hide 出力インターフェースが LAN インターフェース、または PP インターフェース、TUNNEL インターフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

[初期値] : -

[説明]

IPv6 の経路情報を追加する。LAN インターフェースが複数ある機種ではスコープ識別子でインターフェースを指定する必要がある。インターフェースに対応するスコープ識別子はshow ipv6 address コマンドで表示される。

LAN インターフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

なお LOOPBACK インターフェース、NULL インターフェースは常にアップ状態なので、hide オプションは指定はできるものの意味はない。

[ノート]

RTX1220、RTX1210、RTX830、RTX810 では、PP インターフェースの dlci= オプションは指定できない。

GATEWAY に ra を指定できるのは、RTX830 Rev.15.02.27 以降のファームウェアである。 ★

ブリッジインターフェースは RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[10] Web GUIのかんたん設定および詳細設定の[プロバイダー接続]-[IPv4 over IPv6 トンネルの設定]で、以下のサービスに対応した。

- transix

- v6 コネクト

- クロスパス (Xpass)

[11] YNOのLASで、機器統計情報の送信に対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/yno/agent/las/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[12] BIGLOBE IPv6オプションに対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/biglobe/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[13] SNMPで、MIB変数ifHighSpeed(1.3.6.1.2.1.31.1.1.1.15)に対応した。

■仕様変更

[1] DPIのファストパスに対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/dpi/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[2] IPv6の処理性能を改善した。

[3] 以下のとき、USB、SDインターフェースの給電停止時間を10秒に変更した。

- interface resetコマンドを実行したとき（変更前3秒）
- モバイル端末との接続に問題が発生したときのモバイル端末再アタッチ処理をしたとき（変更前1秒）

[4] モバイルインターネット接続機能で、モバイル端末をアタッチした際に、自局番号の取得に一定回数失敗した時、自局番号を取得せずにインターネットに接続できるようにした。

自局番号を取得しない場合、show status usbhostコマンドにて、ダミーの自局番号"----------"が表示される。

[5] モバイルインターネット接続機能で、FS040Uを使用しているときに網へ接続している状態でも電波受信レベルを取得できるようにした。

[6] UX302NCおよびUX302NC-Rで、使用するLTEバンドをチューニングした。

[7] USB通信端末が通信デバイスモードにならなかった場合、USB通信端末への給電をOFF、ONして再接続するようにした。

[8] RAプロキシーで、RAによるプレフィックスのpreferred lifetimeが残り60秒になったとき、RSを送出するようにした。

[9] show techinfoコマンドで表示される内容に、show dpi cacheコマンドの実行結果を追加した。

[10] ipsec ike durationコマンドのKBYTESパラメーターを以下のように変更した。
- 最大値を100000から2147483647に変更
- 初期値なしから2000000に変更

この修正により、初期値で2GBのバイト寿命を持つため、IPsec SAが古くなった時、forced-reductionオプションの設定がない場合でも、自動的に秒寿命が30秒に短縮される。

またバイト寿命の最大値が2,147,483,647KBの機種が始動側になる場合は、相手側機器がバイト寿命の最大値が2,147,483,647KBの機種ではないとき、バイト寿命を必ず2GB以下に設定する必要がある。

〇SAの寿命の設定

[書式]

ipsec ike duration SA GATEWAY_ID SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]

no ipsec ike duration SA GATEWAY_ID [SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]]

[設定値及び初期値]

・SA

[設定値] :

| 設定値 | 説明 |
|---|---|
| ipsec-sa (もしくは child-sa) | IPsec SA (CHILD SA) |
| isakmp-sa (もしくは ike-sa) | ISAKMP SA (IKE SA) |

[初期値] : -

・GATEWAY_ID

[設定値] : セキュリティー・ゲートウェイの識別子

[初期値] : -

・SECOND

[設定値] : 秒数(300..691200)

[初期値] : 28800

・KBYTES

[設定値] : キロ単位のバイト数

---

設定値　　説明

---

100..2147483647　キロ単位のバイト数 (RTX830 Rev.15.02.27以降のファームウェア) ★

100..100000　キロ単位のバイト数 (その他のファームウェア) ★

off　　設定しない ★

---

[初期値] :

- 2000000 (RTX830 Rev.15.02.27以降のファームウェア) ★
- off (その他のファームウェア) ★

・REKEY : SAを更新するタイミング

---

設定値　説明

---

70% - 90%　パーセント

off　　更新しない(SAパラメーターでisakmp-sa (ike-sa) を指定したときのみ設定可能)

---

[初期値] : 75%

・DEL_TIME

[設定値] : 古くなったSAの寿命を強制的に短縮する時間(1..691200)

[初期値] : -

[説明]

各 SA の寿命を設定する。

KBYTES パラメーターを指定した場合には、 SECOND パラメーターで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。

KBYTES パラメーターは SA パラメーターとして ipsec-sa (child-sa) を指定したときのみ有効である。SA の更新は KBYTES パラメーターに設定したバイト数の75%を処理したタイミングで行われる。また、IPsec SA が更新されたとき古くなった既存の IPsec SA の寿命が 30 秒以上である場合は、寿命が 30 秒に短縮される。★

REKEY パラメーターは SA を更新するタイミングを決定する。例えば、 SECOND パラメーターで 20000 を指定し、 REKEY パラメーターで75%を指定した場合には、SA を生成してから 15000 秒経過したときに新しい SA を生成する。 REKEY パラメーターは SECOND パラメーターに対する比率を表すもので、 KBYTES パラメーターの値とは関係がない。

SA パラメーターで isakmp-sa(ike-sa) を指定したときに限り、REKEY パラメーターで 'off' を設定できる。このとき、 IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、 ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作するIKEのバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

・IKEv1

始動側として働く場合に、このコマンドで設定した寿命値が提案される。
応答側として働く場合は、このコマンドの設定に関係なく相手側から提案された寿命値に合わせる。

また、 ISAKMP SA に対する REKEY パラメーターを off に設定した場合、その効果を得るためには、次の2点に注意して設定する必要がある。

1. IPsec SAよりも ISAKMP SA の寿命を短く設定する。

2. ダングリングSAを許可する。すなわち、 ipsec ike restrict-dangling-sa コマンドの設定を off にする。

RTX830 または、RTX1300、vRX が始動側になる場合は、最大で 2147483647 KB のバイト寿命値を相手側へ提案可能であるが、相手側機器が RTX 830および、RTX1300、vRX 以外の場合は 2 GB を超えるバイト寿命値を正しく認識できないため、RTX830 および、RTX1300、vRX 以外の機種と接続する場合は必ず 2 GB 以下に設定する必要がある。 ★

・IKEv2

IKEv2 では SA 寿命値は折衝されず、各セキュリティー・ゲートウェイが独立して管理するものとなっている。従って、確立された SA には、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティー・ゲートウェイの方が SA 更新のタイミングが早ければ、 SA はその分早く更新されることになる。

forced-reduction オプションに時間を指定すると、SA を更新した際に古くなった既存の SA の寿命を強制的に設定値に変更し、消滅までの時間を早めることができる。ただし、IPsec SA で KBYTES パラメーターにバイト寿命値を指定している場合は、DEL_TIME パラメーターで 31 秒以上の値を設定していても、短縮される値は 30 秒となる。また、IKEv1 では寿命が設定値よりも短い場合は変更しない。

ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、 ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在するSAの寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

[ノート]

forced-reduction オプションは以下の機種およびリビジョンで使用可能。

RTX830は Rev.15.02.27 以降。

[11] ipsec ike local idコマンド、およびipsec ike remote idコマンドを設定したとき、SAの削除およびIKEの初期化を行うようにした。

[12] ip flow timerコマンドで、FIN/RSTビットのセットされたTCPパケットの寿命の初期値を5秒に変更した。

〇フローテーブルの各エントリの寿命を設定する

[書式]

ip flow timer PROTOCOL TIME

no ip flow timer PROTOCOL [TIME]

[設定値及び初期値]

・PROTOCOL : 寿命を指定するプロトコル

[設定値] :

| 設定値 | 説明 |
|---|---|
| tcp | TCP パケット |
| udp | UDP パケット |
| icmp | ICMP パケット |
| slow | FIN/RST ビットのセットされた TCP パケット |

[初期値] :

tcp = 900

udp = 30

icmp = 30

slow = 5 (RTX830 Rev.15.02.27 以降)★

30 (上記以外)★

・TIME

[設定値] : 秒数 (1..21474836)

[初期値] : -

[説明]

フローテーブルの各エントリの寿命をプロトコル毎に設定する。

FIN/RSTの通過したエントリには 'slow' が適用される。

NATや動的フィルターを使用している場合には、それらのエントリの寿命が適用される。

[13] Web GUIのかんたん設定、および詳細設定の[プロバイダー接続]で、v6プラスとOCNバーチャルコネクトの表記を一部変更した。

[14] Web GUIの詳細設定の[プロバイダー接続]のヘルプで、「1.概要」の「IPv6 IPoE接続」に説明を追記した。

[15] Web GUIの以下の画面で、デザインやレイアウト等を修正し、視認性や操作性を改善した。

- LANマップ

[16] Web GUIのヘルプにWLX222に関する記述を追加した。

[17] DPI機能で、DPIシグネチャーの容量増大に対応するためにDPIシグネチャーの形式をVer. 1.1系に変更した。

これ以降、Ver. 1.0系のDPIシグネチャーは読み込めない。

Ver. 1.0系のDPIシグネチャーを読み込もうとした場合はDPI機能が有効にならない。

以下の設定を入れている場合はご注意ください。
- dpi signature download urlコマンドを使用して、DPIシグネチャーの読み込み先URLを変更
- external-memory dpi signature directoryコマンドを使用して、シグネチャーを保存する外部メモリーのディレクトリーを設定

http://www.rtpro.yamaha.co.jp/RT/docs/dpi/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[18] Luaスクリプト機能で、rt.httprequest関数のHTTPリクエスト設定テーブルのurlフィールドの最大文字数を半角255文字から半角2048文字に変更した。

[19] show dpi application detailコマンドで、シグネチャーのアプリケーションの説明がマルチバイト文字だった場合には、ヤマハの「Ysig Book」ページへ誘導するメッセージを表示するようにした。

DPIで識別可能なアプリケーション一覧 (Ysig Book)については、以下のURLをご覧ください。

http://www.rtpro.yamaha.co.jp/RT/signature/ysig_book/index.html

[20] tunnel templateコマンド実行時に、進捗状況を示すメッセージを出力するようにした。

[21] Web GUIのかんたん設定の[プロバイダー接続]および詳細設定の[プロバイダー接続]で接続種別にIPv6 IPoE接続を選択したとき、以下のIPv4 over IPv6トンネルを設定できるようにした。
- BIGLOBE

- IPv6 オプション
- IPv6 サービス ( IPIP )

[22] Web GUIの以下のプロバイダー接続の設定時に、設定されるLuaスクリプトのインデントを削除した。スクリプトの動作に変更はない。
- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]
- OCNバーチャルコネクト 固定IP1契約
- 「v6プラス」固定IPサービス

[23] Web GUIの以下のページで、「v6プラス」固定IPサービスを設定したとき、トンネルインターフェースのMTUの値を1280から1460へ変更した。
- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]

■バグ修正

[1] LANインターフェースやトンネルインターフェースなどの複数のインターフェースで同時にキープアライブがダウンしたとき、リブートすることがあるバグを修正した。

[2] pp selectコマンドで接続先を選択している状態、またはswitch selectコマンドでスイッチを選択している状態のときに、tunnel enable/disableコマンドの設定変更やloadコマンドで設定を読み込むと、トンネル接続の設定が正しく反映されなかったり、リブートすることがあるバグを修正した。

[3] Web GUIの[管理]-[保守]-[CONFIGファイルの管理]で、「CONFIGファイルのインポート」からPC上に保存されているCONFIGファイルをインポートするとリブートすることがあるバグを修正した。

[4] LANマップで、端末情報が大量に蓄積された状態で新規端末を検出すると、メモリーリークが発生することがあるバグを修正した。

Rev.15.02.19以降で発生する。

[5] Web GUIで、詳細設定の[メール通知]-[登録されているメールサーバーの一覧]からメールサーバーの設定をするとメモリーリークが発生するバグを修正した。

[6] YNOエージェント機能で、YNOエージェントが起動するタイミングでYNOのコマンドを変更すると、configは設定されるが、実行されないことがあるバグを修正した。

[7] YNOエージェント機能で、YNOマネージャーの[SYSLOG管理]-[リアルタイム表示]でSYSLOGが表示されなくなることがあるバグを修正した。
ルーターの内部時計を過去の時間に戻したときに発生する。

[8] YNOエージェント機能で、常時接続回線の状態が正しく通知されないバグを修正した。
LANバックアップのバックアップ回線に切り替わったときに発生する。

[9] モバイルインターネット接続機能で接続時に電波受信レベルが圏外で発呼が中断されたとき、show historyコマンドの通信履歴に"通信中"という履歴が表示されるバグを修正した。

[10] マルチポイントトンネルで、トンネルの切断後にクライアントが再接続処理を開始しないことがあるバグを修正した。

[11] DHCPv6のIRに対するReplyにReconfigure Acceptオプションが付与されていた場合、Replyを処理しないバグを修正した。

[12] OSPFとBGPで、自分側アドレスが設定されており相手側アドレスが設定されていないトンネルインターフェースをゲートウェイとする経路を広告できないバグを修正した。

[13] HTTPサーバー機能で、リクエストヘッダーやエンティティーヘッダーの、ヘッダー名の大文字小文字の違いが無視されないバグを修正した。

[14] OCNバーチャルコネクト 固定IP8/16契約で、以下の条件をすべて満たす場合に、MAP-Eトンネルに設定されたグローバルIPv6アドレスが更新されずIPv4通信ができなくなるバグを修正した。
- MAP-EトンネルにIPマスカレードの設定がない
- NGN網を介したリナンバリングが発生した

[15] IPv6機能で、DHCPv6のIRに対するReplyを連続で受信したとき、DNSサーバー情報が取得できないバグを修正した。

[16] bgp export filterコマンドで、preferenceパラメーターによる経路選択が正常に動作しないことがあるバグを修正した。

[17] VPN拡張ライセンスがインポートされていない状態で以下のコマンドを実行したとき、使用できないインターフェース番号の設定が入力されるバグを修正した。
- pp enabale allコマンド
- pp disable allコマンド
- tunnel enable allコマンド
- tunnel disable allコマンド

[18] LANマップで、端末情報が蓄積された状態で端末管理機能を無効にしたとき、再度端末管理機能を有効にしたときに検出できる端末の数が減少するバグを修正した。

Rev.15.02.19以降で発生する。

[19] Web GUIの管理の[保守]-[CONFIGファイルの管理]-[CONFIGファイルのインポート]で、末尾に改行コードがないテキストファイルをインポートしたとき、最終行の設定内容が反映されないバグを修正した。

[20] Web GUIのLANマップの以下のページの入力欄で、全角文字が使用できないバグを修正した。

- [機器一覧]-[端末一覧]
- [機器一覧]-[端末情報DB]

Rev.15.02.21以降で発生する。

[21] Web GUIの詳細設定の[プロバイダー接続]で、IPv4 over IPv6トンネルの設定を「使用する」から「使用しない」に変更したとき、IPv4 over IPv6トンネルの設定が削除されないバグを修正した。

[22] Web GUIの以下のページで、LAN分割時にIPv4 over IPv6トンネルの設定ができてしまうバグを修正した。

- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]

[23] Web GUIの以下のページで、「IPv6 IPoE接続」の「ひかり電話の契約」で「契約していない」を選択したとき、ngn typeコマンドが設定されないバグを修正した。

- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]

[24] Web GUIの以下の画面で、デザインやレイアウト等を修正し、視認性や操作性を改善した。

- 管理の[本体の設定]-[DOWNLOADボタンの設定]-[ソフトウェアライセンス利用規約]
- 管理の[保守]-[ファームウェアの更新]-[ネットワーク経由でファームウェアを更新]
- [ファームウェア更新の実行]

[25] Web GUIの管理の[保守]-[コマンドの実行]のヘルプページの実行できないコマンド一覧に、以下のコマンドを追記した。

- administrator passwordコマンド
- administrator password encryptedコマンド
- clear ex-licenseコマンド
- copyコマンド
- copy execコマンド
- deleteコマンド
- delete execコマンド
- execute batchコマンド
- import ex-license keyコマンド
- lessで始まるコマンド
- login passwordコマンド
- login password encryptedコマンド
- make directoryコマンド
- renameコマンド
- rtfs formatコマンド
- rtfs garbage-collectコマンド
- scpコマンド
- sshコマンド
- sshd host key generateコマンド
- '|' でgrepを連結したコマンド
- '|' でlessを連結したコマンド

[26] Web GUIの以下のヘルプページで、誤記を修正した。

- [かんたん設定]-[プロバイダー接続]

[27] コマンドヘルプの文字列中で、不当に改行されることがあるバグを修正した。

[28] コマンドヘルプの誤記を修正した。

[29] Web GUIの以下のページで、IPsecまたはL2TP/IPsecの設定をしているとき、ページを表示するとリブートすることがあるバグを修正した。

- ダッシュボードの[Live]-[VPN接続状態(拠点間)]ガジェット
- ダッシュボードの[Live]-[VPN接続状態(リモートアクセス)]ガジェット
- かんたん設定の[VPN]-[拠点間接続]
- かんたん設定の[VPN]-[リモートアクセス]

Rev.15.02.27 で発生する。

[30] Web GUIのダッシュボードの[Live]で、以下のガジェットを追加した状態でページを表示しているとメモリーリークが継続的に発生し、最終的にリブートすることがあるバグを修正した。

- VPN接続状態(拠点間)
- VPN接続状態(リモートアクセス)

Rev.15.02.27で発生する。

[31] system packet-bufferコマンドを設定して再起動すると、リブートを繰り返すことがあるバグを修正した。

Rev.15.02.13以降で発生する。

[32] 以下のコマンドにより外部メモリーに統計情報を保存する設定がされているとき、ごく稀にリブートすることがあるバグを修正した。
- external-memory statistics filename prefixコマンド
- statisticsコマンド

[33] IKEv2リモートアクセスVPN接続で、DNSサーバーアドレスにIPv6アドレスを設定すると、ルーターから誤ったDNSサーバーアドレスがクライアントに通知されるバグを修正した。

[34] フィルター型ルーティングまたはパケット転送フィルターを使用しているとき、ルーターからtelnetコマンドやrdateコマンドなどを実行すると、通信できないバグを修正した。

[35] DPIが一度もアクティベートしていないときに、DPIを用いたフィルター型ルーティングを使用すると、以下の機能が使用できないバグを修正した。
- DPI
- YNO
- ネットボランチDNS
- VPN拡張ライセンス

[36] SNMPで、SERIAL、TELNET、SSH、リモートセットアップでログインした場合に、以下のMIB変数が正しく更新されないバグを修正した。
- yrfLoginStatus
- yrfLoginUser
- yrfLoginSerial
- yrfLoginTelnet
- yrfLoginSSH

- yrfLoginRemote

Rev.15.02.21以降で発生する。

[37] SNMPで、SERIALポートからのログイン情報を表す以下のMIB変数がSFTPからのログアウトを契機に不当に変更されるバグを修正した。

- yrfLoginSerial
- yrfLoginStatus
- yrfLoginUser

[38] HTTPリビジョンアップ機能で、ファームウェアを更新したときに出力されるログの誤記を修正した。

[39] ipsec ike durationコマンドで、IKEv2のCHILD SAの寿命がIKE SAに対するforced-reductionオプションの設定値を参照してしまうバグを修正した。

[40] tunnel templateコマンドで、以下のコマンドが展開されないバグを修正した。

- ipsec ike backward-compatibilityコマンド
- ipsec ike mode-cfg methodコマンド
- ipsec ike negotiation receiveコマンド

[41] 以下のコマンドで、不正なオプションを設定することができるバグを修正した。

- dns sever コマンド
- dns sever dhcp コマンド
- dns sever pp コマンド
- dns sever pdp コマンド
- dns sever select コマンド

[42] ip INTERFACE intrusion detectionコマンドで、オプションに誤った文字列を指定

したとき、エラーが表示されないバグを修正した。

[43] Web GUIのLANマップの接続機器ビューと[一覧マップ]で、SWX2220-10NT/SWX2221P-10NTのポート10配下に端末もしくはL2MSエージェントが接続されているとき、ポート10のVLAN設定を表示するべき箇所にポート9のVLAN設定が表示されるバグを修正した。

[44] Web GUIの以下のプロバイダー接続で各設定項目に長い文字列を設定したとき、インターネットに接続できないことがあるバグを修正した。
- OCNバーチャルコネクト 固定IP1契約
- 「v6プラス」固定IPサービス

[45] Web GUIの詳細設定の[DNSサーバー]-[DNSサーバー機能の基本設定]ページで、「DNSサーバー機能を使用する(リカーシブサーバー)」を設定したとき、dns serviceコマンドの初期値が明示的に設定されるバグを修正した。

[46] Web GUIのかんたん設定の[プロバイダー接続]で、IPv6 PPPoE接続を設定したとき、ppp ipcp msext onコマンドが設定されないバグを修正した。

[47] Web GUIの管理の[保守]-[コマンドの実行]で、入力できないコマンドが入力できてしまうことがあるバグを修正した。

[48] Web GUIの管理の[保守]-[コマンドの実行]で、以下のコマンドが入力できないバグを修正した。
- administrator radius auth コマンド
- ssh encrypt algorithm コマンド
- ssh known hosts コマンド

[49] Web GUIのかんたん設定の[プロバイダー接続]で、モバイル接続(イーサネット方式)を設定するとき、プライマリーDNSサーバーのみアドレスを指定して設定すると、

不正なセカンダリーDNSサーバーのアドレスが設定されるバグを修正した。

[50] Web GUIの以下のページで、8桁のフィルター番号を設定したとき、1の位が表示されないバグを修正した。

- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv4 フィルターの一覧]-[インターフェースへの適用の設定]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv4 フィルターの一覧]-[インターフェースへの適用の設定]-[入力内容の確認]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv6 フィルターの一覧]-[インターフェースへの適用の設定]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv6 フィルターの一覧]-[インターフェースへの適用の設定]-[入力内容の確認]

[51] 以下のプロバイダー接続を設定しているとき、Web GUIのかんたん設定からVPN接続の設定をしても接続できないバグを修正した。

- BIGLOBE IPv6サービス(IPIP)
- OCNバーチャルコネクト 固定IP1/8/16契約
- transix IPv4接続(固定IP)
- v6 コネクト IPv4 over IPv6 接続 (IPIP)
- 「v6プラス」固定 IP サービス
- クロスパス (Xpass) 固定 IP1/8/16契約

[52] Web GUIの以下のページで、VLANインターフェースに[DHCP、または固定IPアドレスに接続]を指定して固定IPを設定したとき、WAN側IPアドレスが表示されないバグを修正した。

- かんたん設定の[プロバイダー接続]の「設定内容の確認」
- 詳細設定の[プロバイダー接続]-[設定内容]
- 詳細設定の[プロバイダー接続]-[設定内容]-[基本設定]-[入力内容の確認]

[53] Web GUIのダッシュボードで、以下のバグを修正した。

- [Live]-「VPN接続状態(リモートアクセス)」ガジェットにリモートアクセス以外のVPN接続状態が表示される
- [Live]-「トラフィック情報(TUNNEL)」ガジェットにIKEv2リモートアクセスVPNのトンネルが表示される
- [History]-「トラフィック情報(TUNNEL)」ガジェットにIKEv2リモートアクセスVPNのトンネルが表示される

[54] Web GUIの以下のページで、誤記を修正した。

- LANマップの[マップ]-[機器詳細と設定]
- ヘルプページ
  - LANマップの[詳細]-[マップ]

[55] コマンドヘルプの誤記を修正した。

---

■更新履歴

Dec. 2022, Rev.15.02.27 リリース

Jan. 2023, Rev.15.02.28 リリース

Mar. 2023, Rev.15.02.29 リリース

以上