http://www.rtpro.yamaha.co.jp/RT/docs/relnote/Rev.14.01/relnote_14_01_40.html

Revision : 14.01.40

Release : Apr. 2021, ヤマハ株式会社

RTX1210 Rev.14.01.40 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.14.01.26以降のファームウェアへ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.14.01.26では以下の変更をしています。

「RTX1210 Rev.14.01.26 リリースノート」より、

http://www.rtpro.yamaha.co.jp/RT/docs/relnote/Rev.14.01/relnote_14_01_26.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.14.01.26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.14.01.38 からの変更点

---

■脆弱性対応

[1] OpenSSLの以下の脆弱性対応を行った。

- CVE-2020-1971(JPCERT/CC JVNVU#91053554)

[2] Web GUIの以下の脆弱性対応を行った。

- CVE-2021-20843 (JPCERT/CC JVNVU#91161784)
- CVE-2021-20844 (JPCERT/CC JVNVU#91161784)

■機能追加

[1] L2MSで以下の機種に対応した。

- SWX3220-16MT
- SWX3220-16TMs
- SWX2322P-16MT
- SWX2320-16MT
- SWX2110P-8G
- SWX2110-16G
- SWX2110-8G
- SWX2110-5G
- WLX413
- UTX200

- UTX100

[2] YNOエージェント機能で、LAS (ログ分析サービス) 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。

[3] モバイルインターネット機能で、以下のデータ通信端末に対応した。

- SoftBank A002ZT

http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[4] IPv6のフラグメントパケットを再構成するために保持しておく時間を設定できるようにした。

〇IPv6のフラグメントパケットを再構成するために保持しておく時間を設定

[書式]

ipv6 reassembly hold-time TIME

no ipv6 reassembly hold-time [TIME]

[設定値及び初期値]

TIME

[設定値]

秒数（1 ... 60）

[初期値]

60秒

[説明]

IPv6のフラグメントパケットを再構成するために保持しておく時間。
設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。
コマンド実行時にすでに保持していたパケットについては変更しない。

[5] トンネルQoSで、トンネルインターフェースのデフォルトクラスを設定できるようにした。

〇デフォルトクラスの設定
[書式]
queue tunnel default class CLASS
no queue tunnel default class [CLASS]
[設定値及び初期値]
- CLASS
[設定値] : クラス (1..16; RTX5000、RTX3500 の場合は 1..100)
[初期値] : 2
[説明]
インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[6] IPv6で、近隣キャッシュの最大エントリー数を変更できるようにした。また、近隣キャッシュの最大エントリー数の初期値を256から1024へ変更した。

〇近隣キャッシュの最大エントリー数の設定
[書式]
ipv6 INTERFACE neighbor cache max entry NUM
no ipv6 INTERFACE neighbor cache max entry [NUM]
[設定値及び初期値]
INTERFACE

[設定値]

LANインターフェース名

[初期値]

なし

NUM

[設定値]

最大エントリー数（256…20480）

[初期値]

1024

[説明]

インターフェースごとに近隣キャッシュの最大エントリー数を設定する。

近隣キャッシュのエントリー数が、設定した最大エントリー数に達した場合は、

古い近隣キャッシュを削除する。

本コマンド実行時、現在の近隣キャッシュのエントリー数が最大エントリー数を

超える場合は、古い近隣キャッシュを削除する。

[7] IPv6 RAプロキシ機能で、RDNSSオプションに対応した。

〇ルーター広告の送信の制御

[書式]

ipv6 INTERFACE rtadv send PREFIX_ID [PREFIX_ID...] [OPTION＝VALUE...]

ipv6 pp rtadv send PREFIX_ID [PREFIX_ID...] [OPTION＝VALUE...]

no ipv6 INTERFACE rtadv send [...]

no ipv6 pp rtadv send [...]

[設定値及び初期値]

・INTERFACE

[設定値] : LANインタフェース名

[初期値] : -

・PREFIX_ID

[設定値] : プレフィックス番号

[初期値] : -

・OPTION＝VALUE : NAME=VALUEの列

[設定値] :

---

NAME　　VALUE　　説明

---

m_flag　　on、off　　managed address configurationフラグ。ルーター広告による自動設定とは別に、DHCP6に代表されるルーター広告以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。

o_flag　　on、off　　other stateful configurationフラグ。ルーター広告以外の手段によりIPv6アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。

max-rtr-adv-interval 秒数　　ルーター広告を送信する最大間隔 (4-1,800秒)

min-rtr-adv-interval 秒数　　ルーター広告を送信する最小間隔 (3-1,350秒)

adv-default-lifetime 秒数　　ルーター広告によって設定される端末のデフォルト経路の有効時間 (0-9,000秒)

adv-reachable-time　ミリ秒数　　ルーター広告を受信した端末

が、ノード間で確認した到達
性の有効時間 (0-3,600,000
ミリ秒)

adv-retrans-time　ミリ秒数　　ルーター広告を再送する間隔
(0-4,294,967,295ミリ秒)

adv-cur-hop-limit　ホップ数　　ルーター広告の限界ホップ数
(0-255)

mtu　　auto、off、バイト数 ルーター広告にMTUオプショ
ンを含めるか否かと、含める
場合の値の設定。
autoの場合はインタフェース
のMTUを採用する。

rdnss　　rdnss、off、dhcpv6 ルーター広告にRDNSSオプショ
ンを含めるか否かと、含める
場合の値の設定。
rdnssの場合はRAのRDNSSオプ
ションで割り当てられたサー
バー群を通知する。 ★

---

[初期値] :

- m_flag = off
- o_flag = off
- max-rtr-adv-interval = 600
- min-rtr-adv-interval = 200
- adv-default-lifetime = 1800
- adv-reachable-time = 0
- adv-retrans-time = 0
- adv-cur-hop-limit = 64
- mtu = auto

・rdnss = rdnss ★

[説明]

インタフェースごとにルーター広告の送信を制御する。送信されるプレフィックスとして、ipv6 prefixコマンドで設定されたものが用いられる。

また、オプションとしてm_flagおよびo_flagを利用して、管理するホストがルーター広告以外の自動設定情報をどのように解釈するかを設定することができる。

オプションでは、送信するルーター広告の送信間隔や、ルーター広告に含まれる情報の設定を行うこともできる。

[8] Web GUIのダッシュボードの[Live]に、UTXセキュリティーガジェットを追加した。

UTXセキュリティーガジェットでは、UTX100/UTX200から取得したセキュリティーレポートの概要を確認できる。

http://www.rtpro.yamaha.co.jp/RT/docs/dashboard_ver2/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

■仕様変更

[1] Web GUIで、Internet Explorer11のサポートを終了した。

詳細および最新の推奨ブラウザーについては、以下のURLをご覧ください。

http://www.rtpro.yamaha.co.jp/RT/FAQ/gui/browser.html

[2] IPIPトンネルで、L2TP/IPsecおよびL2TPv3に対応した。

ただし、IPv6 IPoE + IPv4 over IPv6 接続のサービスでは、契約形態により制限があるため、以下の技術資料をご確認のうえ、ご利用ください。

http://www.rtpro.yamaha.co.jp/RT/docs/#ipoe_46

[3] show ipv6 neighbor cacheコマンドで、インターフェースを指定して表示できるようにした。また、エントリー数のみを表示できるようにした。

〇近隣キャッシュの表示

[書式]

show ipv6 neighbor cache [INTERFACE] ★

show ipv6 neighbor cache [INTERFACE] summary ★

[設定値及び初期値]

INTERFACE ★

[設定値]

LANインターフェース名

[初期値]

なし

[説明]

近隣キャッシュの状態を表示する。インターフェース名を指定した場合、そのインターフェース経由で得られた近隣キャッシュの状態のみ表示する。

summaryを指定した場合、近隣キャッシュのエントリー数のみ表示する。

[4] clear ipv6 neighbor cacheコマンドで、インターフェースを指定して消去できるようにした。

〇近隣キャッシュの消去

[書式]

clear ipv6 neighbor cache [INTERFACE] ★

[設定値及び初期値]

INTERFACE ★

[設定値]

LANインターフェース名

[初期値]

なし

[説明]

近隣キャッシュを消去する。インタフェース名を指定した場合、そのインタフェース経由で得られた近隣キャッシュのみ消去する。

[5] OCNバーチャルコネクトサービスで、通信を安定化させるために以下を変更した。

- ルーター起動時、MAPルールの処理を開始してから取得を行うまでの待機時間を3秒から8秒へ変更した
- 固定IP契約で、起動時にルーターが保持しているMAPルールのプレフィックスと受信したプレフィックスが一致しない場合に、MAP-Eルールの取得するタイミングを1～10分後から15～20分後へ変更した
- 動作中にプレフィックスが変更された場合に、MAP-Eルールの取得するタイミングを3秒後から15分後へ変更した

[6] 以下のコマンドで、始点IPアドレスおよび終点IPアドレスにmap-eを指定できるようにした。

- ip filterコマンド
- ip filter dynamicコマンド
- ipv6 filterコマンド
- ipv6 filter dynamicコマンド

〇IPパケットのフィルタの設定

[書式]

ip filter FILTER_NUM PASS_REJECT SRC_ADDR[/MASK] [DEST_ADDR[/MASK] [PROTOCOL [SRC_PORT_LIST [DEST_PORT_LIST]]]]

no ip filter FILTER_NUM [PASS_REJECT]

[設定値及び初期値]

FILTER_NUM

[設定値] : 静的フィルタ番号 (1..21474836)

[初期値] : -

PASS_REJECT

[設定値] :

---

設定値　　説明

---

pass　　一致すれば通す ( ログに記録しない )

pass-log　　一致すれば通す ( ログに記録する )

pass-nolog　　一致すれば通す ( ログに記録しない )

reject　　一致すれば破棄する ( ログに記録する )

reject-log　　一致すれば破棄する ( ログに記録する )

reject-nolog　一致すれば破棄する ( ログに記録しない )

restrict　　回線が接続されていれば通し、切断されていれば破棄する ( 破棄する場合のみログに記録する )

restrict-log　回線が接続されていれば通し、切断されていれば破棄する ( ログに記録する )

restrict-nolog 回線が接続されていれば通し、切断されていれば破棄する ( ログに記録しない )

---

[初期値] : -

SRC_ADDR : IPパケットの始点IPアドレス

[設定値] :

・IPアドレス

・A.B.C.D (A～D: 0～255もしくは*)

・上記表記でA～Dを*とすると、該当する8ビット分については

すべての値に対応する

・間に - を挟んだ2つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

・, を区切りとして複数設定することができる。

・FQDN

・任意の文字列 (半角255文字以内。/ ： は使用できない。, は区切り文字として使われるため、使用できない)

・* から始まるFQDNは * より後ろの文字列を後方一致条件として判断する。例えば *.example.co.jpは www.example.co.jp、mail.example.co.jpなどと一致する

・, を区切りとして複数設定することができる。

・map-e ★

・MAP-Eのマップルールにより生成されたグローバルIPv4アドレスを表すキーワード ★

・* (すべてのIPアドレスに対応)

[初期値] : -

DEST_ADDR : IPパケットの終点IPアドレス

[設定値] :

・src_addrと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

MASK : IPアドレスのビットマスク (SRC_ADDRおよびDEST_ADDRがネットワークアドレスの場合のみ指定可)

[設定値] :

・A.B.C.D (A～D: 0～255)

・0x に続く十六進数

・マスクビット数

・省略時は 0xffffffff と同じ

[初期値] : -

PROTOCOL : フィルタリングするパケットの種類

[設定値] :

・プロトコルを表す十進数 (0..255)

・プロトコルを表すニーモニック

icmp 1 ICMPパケット

tcp 6 TCPパケット

udp 17 UDPパケット

ipv6 41 IPv6パケット

gre 47 GREパケット

esp 50 ESPパケット

ah 51 AHパケット

icmp6 58 ICMP6パケット

・上項目のカンマで区切った並び (5個以内 )

・特殊指定

---

設定値　　説明

---

icmp-error　　TYPEが3、4、5、11、12、31、32のいずれか
であるICMPパケット

icmp-info　　TYPEが0、8～10、13～18、30、33～36のいず
れかである ICMPパケット

tcpsyn　　SYNフラグの立っているtcpパケット

tcpfin　　FINフラグの立っているtcpパケット

tcprst　　RSTフラグの立っているtcpパケット

established　　ACKフラグの立っているtcpパケット内から外
への接続は許可するが、外から内への接続は
拒否する機能

tcpflag=VALUE/MASK　TCPフラグの値とMASKの値の論理積 (AND) が、

tcpflag!=VALUE/MASK VALUEに一致、または不一致であるTCPパケッ
トVALUEとMASKは0xに続く十六進数で0x0000
～0xffff
* すべてのプロトコル
---

・省略時は * と同じ。

[初期値] : -

SRC_PORT_LIST : PROTOCOLに、TCP(tcp/tcpsyn/tcpfin/tcprst/established/
tcpflag)、UDP(udp)のいずれかが含まれる場合は、TCP/UDPの
ソースポート番号。PROTOCOLがICMP(icmp)単独の場合には、
ICMPタイプ。

[設定値] :

・ポート番号、タイプを表す十進数

・ポート番号を表すニーモニック (一部)

ftp 20,21

ftpdata 20

telnet 23

smtp 25

domain 53

gopher 70

finger 79

www 80

pop3 110

sunrpc 111

ident 113

ntp 123

nntp 119

snmp 161

syslog 514

printer 515

talk 517

route 520

uucp 540

submission 587

・間に - を挟んだ2つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

・上項目のカンマで区切った並び (10個以内)

・* (すべてのポート、タイプ)

・省略時は * と同じ。

[初期値] : -

DEST_PORT_LIST

[設定値] : PROTOCOLに、TCP(tcp/tcpsyn/tcpfin/tcprst/established/tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDPのデスティネーションポート番号。PROTOCOLがICMP(icmp) 単独の場合には、ICMPコード

[初期値] : -

[説明]

IPパケットのフィルタを設定する。本コマンドで設定されたフィルタは ip filter directed-broadcast、ip filter dynamic、ip filter set、ip forward filter、ip fragment remove df-bit、ip INTERFACE rip filter、ip INTERFACE secure filter、およびip routeコマンドで用いられる。

[ノート]

restrict-log及びrestrict-nologを使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに有効である。

例えば、時計を合わせるためのNTPパケットがこれに該当する。ICMPパケットに対して、ICMPタイプとICMPコードをフィルタでチェックしたい場合には、PROTOCOLには'icmp'だけを単独で指定する。

PROTOCOLが'icmp'単独である場合にのみ、SRC_PORT_LISTはICMPタイプ、DEST_PORT_LISTはICMPコードと見なされる。
PROTOCOLに'icmp'と他のプロトコルを列挙した場合にはSRC_PORT_LISTとDEST_PORT_LISTの指定はTCP/UDPのポート番号と見なされ、ICMPパケットとの比較は行われない。
また、PROTOCOLに'icmp-error'や'icmpinfo'を指定した場合には、SRC_PORT_LIST とDEST_PORT_LISTの指定は無視される。
PROTOCOLに'*'を指定するか、TCP/UDPを含む複数のプロトコルを列挙している場合には、SRC_PORT_LISTとDEST_PORT_LISTの指定はTCP/UDPのポート番号と見なされ、パケットがTCPまたはUDPである場合のみポート番号がフィルタが比較される。
パケットがその他のプロトコル (ICMPを含む) の場合には、SRC_PORT_LISTとDEST_PORT_LISTの指定は存在しないものとしてフィルタと比較される。
Rev.10.00系以降のすべてのファームウェアでPROTOCOLに'tcpsyn'を指定可能。
RTX1200 Rev.10.01.47以降のファームウェア、および、Rev.11.01系以降のすべてのファームウェアでSRC_PORT_LISTまたはDEST_PORT_LISTにsubmissionを指定可能。
RTX1500 / RTX1100 / RT107e Rev.8.03.68以降、RTX3000 Rev.9.00.31以降のファームウェア、および、Rev.10.00系以降のすべてのファームウェアでICMPのタイプとコードを指定可能。
SRC_ADDRおよびDEST_ADDRはIPアドレスとFQDNとmap-eを混合することも可能 ★
SRC_ADDRおよびDEST_ADDRにFQDNを指定することによって、固定IPアドレスではないサーバーや1つのFQDNに対して複数の固定IPアドレスを持つサーバーを対象にしたフィルタリングを行うことができる。
FQDNを使用する場合、ルーター自身がDNSリカーシブサーバーとして動作し、ルータ配下の端末は、DNSサーバーとして本機を指定する必要がある。
SRC_ADDRおよびDEST_ADDRへのFQDNの指定はRTX5000 Rev.14.00.26以降、RTX3500 Rev.14.00.26以降、
RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX810 Rev.11.01.28 以降で指定可能。

指定したFQDNに一致する通信が発生した場合、設定したFQDNに該当するIPアドレスの情報が保持される。

保持される期間は、ip filter fqdn timerコマンドで指定できる。

SRC_ADDRおよびDEST_ADDRへのmap-eの指定はRTX1210 Rev.14.01.40以降で指定可能。 ★

〇動的フィルタの定義

[書式]

ip filter dynamic DYN_FILTER_NUM SRCADDR[/MASK] DSTADDR[/MASK] PROTOCOL [OPTION ...]

ip filter dynamic DYN_FILTER_NUM SRCADDR[/MASK] DSTADDR[/MASK] filter FILTER_LIST [in FILTER_LIST] [out FILTER_LIST] [OPTION...]

no ip filter dynamic DYN_FILTER_NUM

[設定値及び初期値]

DYN_FILTER_NUM

[設定値] : 動的フィルタ番号 (1..21474836)

[初期値] : -

SRCADDR

[設定値] : 始点IPアドレス

・ip filterコマンドのsrc_addrと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

DSTADDR

[設定値] : 終点IPアドレス

・SRCADDRと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

MASK : IPアドレスのビットマスク (src_addrおよびdest_addrがネットワークアドレスの場合のみ指定可)

[初期値] : -

PROTOCOL : プロトコルのニーモニック

[設定値] :

・tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting

Rev.10.01以降では以下が使用できます

・echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/
whois/dns/domain/

・tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/
ms-rpc/

・netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/
imap3/ldap/

・https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/

・ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/

・ping/ping6/tcp/udp

Rev.10.01以降では以下が設定できますが、動的フィルターとして動作しません

・dhcpc/dhcps/dhcpv6c/dhcpv6s

Rev.10.01.47以降、および、Rev.11.01以降では以下が使用できます

・submission

[初期値] : -

FILTER_LIST

[設定値] : ip filterコマンドで登録されたフィルタ番号のリスト

[初期値] : -

OPTION

[設定値] :

・syslog=SWITCH

onコネクションの通信履歴をSYSLOGに残す

offコネクションの通信履歴をSYSLOGに残さない

・timeout=time

timeデータが流れなくなったときにコネクション情報を解放するま
での秒数

[初期値] : syslog=on

[説明]

動的フィルタを定義する。第1書式では、あらかじめルーターに登録されている
アプリケーション名を指定する。
第2書式では、ユーザーがアクセス制御のルールを記述する。キーワードのfilter、
in、outの後には、ip filterコマンドで定義されたフィルタ番号を設定する。
filterキーワードの後に記述されたフィルタに該当するコネクション (トリガ)
を検出したら、それ以降inキーワードとoutキーワードの後に記述されたフィル
タに該当するコネクションを通過させる。
inキーワードはトリガの方向に対して逆方向のアクセスを制御し、outキーワー
ドは動的フィルタと同じ方向のアクセスを制御する。
なお、ip filterコマンドのIPアドレスは無視される。pass/rejectの引数も同様
に無視される。
プロトコルとしてtcpやudpを指定した場合には、アプリケーションに固有な処理
は実施されない。
特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定
する。

〇IPv6フィルタの定義

[書式]

ipv6 filter FILTER_NUM PASS_REJECT SRC_ADDR[/PREFIX_LEN] [DEST_ADDR[/PREFIX_LEN] [PROTOCOL [SRC_PORT_LIST [DEST_PORT_LIST]]]]

no ipv6 filter FILTER_NUM [PASS_REJECT]

[設定値及び初期値]

FILTER_NUM

[設定値] : 静的フィルタ番号 (1..21474836)

[初期値] : -

PASS_REJECT

[設定値] : フィルタのタイプ (ip filterコマンドに準ずる)

[初期値] : -

SRC_ADDR

[設定値] : IPパケットの始点IPアドレス

・IPv6アドレス

・静的または動的IPv6アドレス

・, を区切りとして複数設定することができる。

・map-e ★

・MAP-Eのマップルールにより生成されたグローバルIPv6アドレス

を表すキーワード ★

[初期値] : -

PREFIX_LEN

[設定値] : プレフィックス長

[初期値] : -

DEST_ADDR

[設定値] : IPパケットの終点IPアドレス

・SRC_ADDRと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

PROTOCOL : フィルタリングするパケットの種類 (ip filterコマンドに準ずる )

[設定値] :

---

設定値　説明

---

icmp-nd　近隣探索に関係するパケットの指定を示すキーワード。

(TYPEが133、134、135、136のいずれかであるICMPv6パケット)

icmp4　ICMPv4パケットの指定を示すキーワード

icmp　　ICMPv6パケットの指定を示すキーワード

icmp6

---

[初期値] : -

SRC_PORT_LIST

[設定値] : TCP/UDPのソースポート番号、あるいはICMPv6タイプ

(ip filterコマンドに準ずる)

[初期値] : -

DEST_PORT_LIST

[設定値] : TCP/UDPのデスティネーションポート番号、あるいはICMPv6コー

ド

[初期値] : -

[説明]

IPv6のフィルタを定義する。

〇IPv6 動的フィルタの定義

[書式]

ipv6 filter dynamic DYN_FILTER_NUM SRCADDR[/PREFIX_LEN] DSTADDR[/PREFIX_LEN] PROTOCOL [OPTION ...]

ipv6 filter dynamic DYN_FILTER_NUM SRCADDR[/PREFIX_LEN] DSTADDR[/PREFIX_LEN] filter FILTER_LIST [in FILTER_LIST] [out FILTER_LIST] [OPTION ...]

no ipv6 filter dynamic DYN_FILTER_NUM [SRCADDR ...]

[設定値及び初期値]

・DYN_FILTER_NUM

[設定値] : 動的フィルタ番号 (1..21474836)

[初期値] : -

・SRCADDR

[設定値] : 始点IPv6アドレス

・ipv6 filterコマンドのsrc_addrと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

・PREFIX_LEN

[設定値] : プレフィックス長

[初期値] : -

・DSTADDR

[設定値] : 終点IPv6アドレス

・SRCADDRと同じ形式

・省略した場合は一個の * と同じ

[初期値] : -

・PROTOCOL : プロトコルのニーモニック

[設定値] :

・tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet

Rev.10.01以降では以下が設定できます

・echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time

/whois/dns/domain/dhcps/

・dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp

/ntp/ms-rpc/

・netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp

/imap3/ldap/

・https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/

・dhcpv6c/dhcpv6s/ms-sql/radius/l2tp/pptp/nfs/msblast

/ipsec-nat-t/sip/

・ping/ping6/tcp/udp

[初期値] : -

・FILTER_LIST

[設定値] : ipv6 filterコマンドで登録されたフィルタ番号のリスト

[初期値] : -

・OPTION

[設定値] :

・syslog=SWITCH

onコネクションの通信履歴をsyslogに残す

offコネクションの通信履歴をsyslogに残さない

・timeout=TIME

timeデータが流れなくなったときにコネクション情報を解放するまでの秒数

[初期値] :

・syslog=on

・timeout=60

[説明]

IPv6の動的フィルタを定義する。第1書式では、あらかじめルーターに登録されているアプリケーション名を指定する。

第2書式では、ユーザーがアクセス制御のルールを記述する。キーワードのfilter、in、outの後には、ipv6 filterコマンドで定義されたフィルタ番号を設定する。

filterキーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降inキーワードとoutキーワードの後に記述されたフィルタに該当するコネクションを通過させる。

inキーワードはトリガの方向に対して逆方向のアクセスを制御し、outキーワードは動的フィルタと同じ方向のアクセスを制御する。

なお、ipv6 filterコマンドのIPアドレスは無視される。pass/rejectの引数も同様に無視される。

ここに記載されていないアプリケーションについては、filterキーワードを使って定義することで扱える可能性がある。

特にsnmpのように動的にポート番号が変化しないプロトコルの扱いは容易である。

tcpかudpを設定することで扱える可能性がある。特に、telnetのように動的にポート番号が変化しないプロトコルはtcpを指定することで扱うことができる。

src_addrおよびdest_addrはIPv6アドレスとmap-eを混合することも可能 ★

src_addrおよびdest_addrへのmap-eの指定はRTX1210 Rev.14.01.40以降で指定可能。 ★

[7] Web GUIのかんたん設定の[VPN]-[クラウド接続]からAmazon VPCの設定をしたとき、接続安定化のために以下のコマンドを設定するようにした。

- ipsec ike remote id N 0.0.0.0/0
- ipsec ike local id N 0.0.0.0/0
- ipsec ike remote id M 0.0.0.0/0
- ipsec ike local id M 0.0.0.0/0

[8] Web GUIの以下で、OCNバーチャルコネクトサービス 固定IP1契約の設定時に設定されるLuaスクリプトを変更した。

- 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]

[9] Web GUIの詳細設定の[LAN]-[IPアドレス]で、IPアドレスを手動で設定するとき、その他の設定のIPアドレスを自動で変更する範囲の初期値を以下のように変更した。
これに伴い、設定項目の表示順序を変更した。

- 変更前：DHCPで払い出すIPアドレスの範囲のみ変更する
- 変更後：設定に含まれるIPアドレスをすべて変更する

[10] Web GUIのLANマップで、以下の箇所に表示されるRTX1210のアイコンを変更した。

- マップのツリービュー
- タグVLANのツリービュー
- マルチプルVLANのツリービュー
- 一覧マップ

■バグ修正

[1] IKEv2でPKI証明書を利用した認証を行うとき、ペイロードの不一致により接続できない場合にリブートすることがあるバグを修正した。

[2] IKEv2を使用してIPsecトンネルを確立している場合、SAの更新処理が行われるときにリブートやハングアップすることがあるバグを修正した。

[3] 以下のコマンドを実行したとき、リブートすることがあるバグを修正した。
- syslog execute command
- no syslog execute command

[4] bgp importコマンドで、不正なオプションを入力した時にリブートすることがあるバグを修正した。

[5] トンネルテンプレート機能を使用して生成した大量のIPsecトンネルで、IKEキープアライブパケットの到達性がない状態が続くとリブートすることがあるバグを修正した。

Rev.14.01.14以降で発生する。

[6] IPsecトンネルの接続数が多いとき、ipsec refresh saを実行するとリブートすることがあるバグを修正した。

[7] 全ノードマルチキャストアドレス(ff02::1)、および全ルーターマルチキャストアドレス(ff02::2)宛のパケットを送信するとき、リブートすることがあるバグを修正した。

Rev.14.01.20以降で発生する。

[8] IPv6機能で、複数のインターフェースにipv6 rtadv sendコマンドを設定し、RAでプレフィックスの更新通知を受信するとリブートする可能性があるバグを修正した。

Rev.14.01.36以降で発生する。

[9] Web GUIのLANマップで、Webブラウザーの複数のタブやウィンドウでそれぞれ異なるインターフェースのLANマップ画面を同時に開いているとき、インターフェース間でスレーブを移動したのちにツリービューから当該スレーブを選択すると、リブートしたり状態が正常に表示されなかったりすることがあるバグを修正した。

Rev.14.01.16以降で発生する。

[10] 大量のユーザーがWeb GUIへ同時にログインしたとき、リブートすることがあるバグを修正した。

[11] LANマップで端末監視が有効のとき、消失端末情報が内部的に蓄積し続けリブートする可能性があるバグを修正した。
ただし、この現象は確認されていない。

[12] 不正な多重タグパケットを受信したとき、ハングアップすることがあるバグを修正した。

[13] DHCPサーバー機能で、DHCP DISCOVERを一度に大量に受信したとき、ハングアップすることがあるバグを修正した。

Rev.14.01.26以降で発生する。

[14] httpd service offコマンドが設定されているとき、disconnect userコマンドを実

行すると、ハングアップすることがあるバグを修正した。

[15] IKEv2のIPsecトンネルにおいて、ipsec ike keepalive useコマンドでICMP Echo以外のキープアライブ方式を設定している場合、IKE SAの更新処理が行われる度にメモリーリークが発生するバグを修正した。

[16] IPv6プレフィックスのRAの有効寿命が尽きたとき、メモリーリークが発生するバグを修正した。

[17] 複数のルーティングプロトコルから同一の経路を受信しているとき、bgp exportコマンドでルーティングテーブルに取り込まない設定になっている BGP 由来の経路がshow ip route detailコマンドの結果に表示されることがあるバグを修正した。

[18] ospf export from ospfコマンドが設定されているとき、BGPで受信した経路がbgp exportコマンドの設定どおりにルーティングテーブルに取り込まれないことがあるバグを修正した。

[19] 複数のルーティングプロトコルから同一の経路を受信しているとき、OSPFの優先度が最も高く設定されていると、他のルーティングプロトコル由来の経路をbgp importコマンドの設定どおりにBGPに取り込むことができないことがあるバグを修正した。

[20] YNOエージェント機能で、以下のいずれかの状態でルーターが起動すると、"[YNO_AGENT] internal error"がDEBUGレベルのSYSLOGに出力されるバグを修正した。

- yno useコマンドがon、かつyno access codeコマンドが設定されている
- yno useコマンドがon、かつyno zero-config idコマンドが設定されている

[21] YNOエージェント機能で、以下のバグを修正した。

- 発生したアラームが正常にYNOマネージャーに通知されないことがある
- 発生したアラームが重複してYNOマネージャーに通知されることがある

[22] YNOエージェント機能で、YNOマネージャーでアクセスコードを変更したときYNOマネージャーに接続済みのルーターに変更したアクセスコードが適用されないことがあるバグを修正した。

[23] YNOエージェント機能で、LANインターフェースの状態を正しく取得できないバグを修正した。
このバグにより、YNOマネージャーの[機器一覧]-[機器詳細]-[LAN]の状態にdisabledと表示される。

Rev.14.01.36以降で発生する。

[24] YNOのGUI Forwarder経由で、Web GUIの詳細設定の[プロバイダー接続]から既存の設定で「IPv4 over IPv6 トンネルの設定」を「使用する」に変更すると、正常にページ遷移が行われないバグを修正した。

[25] マルチポイントトンネルインターフェースのアドレスがゲートウェイに指定されている静的経路が、対象のトンネルの切断時に消失し、トンネルが再確立しても復元せずに当該経路の通信ができなくなるバグを修正した。

Rev.14.01.35以降で発生する。

[26] IKEv2のレスポンダーとして動作しているとき、イニシエーターからIDr無しのIKE_AUTHを受信した場合に認証エラーとなり、IKEv2の接続ができないことがあるバグを修正した。

[27] IKEv2のレスポンダーとして動作しているとき、イニシエーターからのIKE_SA_INIT

を2回以上受信すると、IKE_AUTH以降の処理で不正な値のresponderSPIを送信して接続できないことがあるバグを修正した。

[28] L2TP/IPsecおよびL2TPv3/IPsecにおいて、tunnel disableコマンドが設定されているときに接続できてしまうバグを修正した。

[29] IPマスカレード機能では、PPTPで使用されるGREパケットはIPヘッダー部の書き換えと共にGREヘッダー部を書き換えるが、PPTPの通信パケットとは認識されないGREパケットのGREヘッダー部を不当に書き換えることがあるバグを修正した。

[30] L2MSでスタック1台構成、かつ、スタックIDが1以外のスレーブが接続されているとき、認識できないスレーブとして検出されるバグを修正した。

[31] 動的フィルター機能で、ファストパスが有効かつNATまたはIPマスカレードが適用される通信において、動的フィルターセッションの戻り方向の通信が発生しているにもかかわらず、当該セッションがタイムアウトで削除されることがあるバグを修正した。

[32] RAプロキシー配下のLANインタフェースで、RA受信により生成したIPv6アドレスが、暫定IPv6アドレスのままになることがあるバグを修正した。

Rev.14.01.35以降で発生する。

[33] メール通知機能で、SMTP認証を有効にしたとき一部のメールサーバーに対してメールを送信できないバグを修正した。

[34] IPv6でマルチプレフィックスになったとき、優先度の低いプレフィックスのRAを送信し続けてしまうバグを修正した。

Rev.14.01.36以降で発生する。

[35] DHCPサーバー機能で、DHCP REQUESTメッセージのOptionにEndが入っていないとき、不正な値をOptionの値として取得してしまうことがあるバグを修正した。

[36] 送信元MACアドレスが、マルチキャストアドレスであるパケットをLAN1インターフェースで受信できないバグを修正した。

[37] LAN分割時に、ファストパスでIPv6マルチキャストパケットを送信できないバグを修正した。

[38] トンネルQoSで、ファストパス経由のパケットはトンネルインターフェースのクラス分け設定に従うのに対し、ノーマルパス経由のパケットはトンネルの送出インターフェースとなっている物理インターフェースのクラス分け設定に従ってしまい、ファストパスとノーマルパスでクラス分け結果が異なるバグを修正した。

[39] OCNバーチャルコネクトサービスで、接続中の回線を動的IP契約から固定IP契約へ切り替えたとき、IPマスカレードで利用するポートの範囲が更新されないバグを修正した。

[40] dhcp scope optionコマンドで、オプション番号252の設定値をバイナリで入力したとき、show configコマンド実行時に余分な文字列が表示されることがあるバグを修正した。

[41] show status mobile signal-strengthコマンドで、不正なキーワードを入力してもエラーが表示されないバグを修正した。

[42] showコマンドの表示中にログインタイマーが満了しても、showコマンドの実行結果

の表示が止まらず、ログアウトされないバグを修正した。

[43] 動的フィルターの適用されたインターフェースで受信したIPv4フラグメントパケットにおいて、再構成のために保持しておく時間がip reassembly hold-timeコマンドの設定値に従っていないバグを修正した。

[44] nat descriptor masqurade incomingコマンドで、actionパラメーターがthroughまたはforwardに設定されているとき、TCP、UDP、ICMP、GRE以外のパケットを外から内向きに転送すると、不要なNATエントリーが登録されることがあるバグを修正した。

[45] no ipsec tunnelコマンドで、policy_idオプションに整数以外が指定できるバグを修正した。
これにより、ipsec tunnelコマンドが意図せず削除されトンネルがダウンすることがなくなる。

[46] IPマスカレード機能で、UPnPのポートマッピングのリクエストまたはFTPのPASV/PORTコマンドに応じたNATエントリーの作成および削除が行われると、以後TCP以外のセッションまたはFTPセッションで正常に通信ができなくなることがあるバグを修正した。
ただし、nat descriptor backward-compatibilityコマンドが1に設定されているときは本バグは発現しない。

Rev.14.01.35以降で発生する。

[47] show arpコマンドのカウント数が不正な値になることがあるバグを修正した。

[48] httpd serviceコマンドをonとoffに繰り返して設定した場合、Web GUIへログインできなくなることがあるバグを修正した。

[49] Web GUIにログインしているとき、httpd serviceコマンドをonからoffに設定すると、ログインタイマー満了後にユーザーがログアウトされないバグを修正した。

[50] Web GUIの以下のページでプロバイダーの設定を追加したとき、dns hostコマンドがdns host lan1に上書きされ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]

[51] Web GUIのかんたん設定の[VPN]-[リモートアクセス]で、L2TP/IPsecの認証鍵にスペースや「"」「#」「¥」などの特殊文字が含まれている状態でリモートアクセスのユーザーを追加したとき、正しく設定されないバグを修正した。

[52] Web GUIのかんたん設定の[VPN]-[リモートアクセス]で、ユーザーの登録ページからユーザーを削除しようとしても、設定の一部が残ってしまうバグを修正した。

Rev.14.01.36以降で発生する。

[53] Web GUIのLANマップの設定[マスターモード時の動作設定]-[端末の管理]-[下記無線AP配下の端末の更新間隔]で、対象の機種一覧にWLX212が記載されていないバグを修正した。

[54] Web GUIのLANマップで、タグVLANの設定を追加または変更したとき、dns hostコマンドにタグVLANのインターフェースが重複して設定されることがあるバグを修正した。

[55] Web GUIの管理の[アクセス管理]-[各種サーバーの設定]-[SSH/SFTP を使用したアクセス]で、利用できないアルゴリズムが表示されるバグを修正した。

[56] Web GUIの以下のページで、IPv6 IPoE(DHCP)接続の「v6プラス」固定IPサービスを設定したとき、不正な内容が設定されてIPv4で通信できなくなるバグを修正した。

- 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]

[57] Web GUIのかんたん設定の[YNOエージェント]で、半角カタカナが含まれている文字列を設定しようとすると、すでに設定されているyno useコマンドとyno access codeコマンドが削除されるバグを修正した。

[58] Web GUIのダッシュボードの[Live]の各ガジェットで、URLを直接Webブラウザーに指定したときに正常に表示されないバグを修正した。

Rev.14.01.34以降で発生する。

[59] Web GUIのダッシュボードの[Live]の以下のガジェットで、警告が表示されると[解除]ボタンの左側に「+」が表示されるバグを修正した。
- リソース情報ガジェットのCPU使用率
- リソース情報ガジェットのメモリ使用率

Rev.14.01.34以降で発生する。

---

■更新履歴

Apr. 2021, Rev.14.01.40 リリース
May. 2021, 誤記修正
Jul. 2021, バグ修正[5]文面修正
Nov. 2021, 脆弱性対応[2] 追加

以上