サザンクロスルータシステム「AR415S」
ファームウェアリリースノート
Ver.2.9.2-14

Ver.2.9.2-11 から Ver.2.9.2-14 の変更点

以下のとおり機能追加・機能改善が行われました。

1. 本バージョンで追加された機能

■ IPv6 over IPv4/6to4 トンネルインターフェースにおけるMSS クランプ機能

IPv6 over IPv4 および6to4 トンネルインターフェースにおいて、IPv6 上のTCP Syn パケットを監視し、TCP ヘッダー内のMSS オプションの値が1220 を超える場合、同オプションの値を1220 に書き換えるMSS クランプ機能をサポートしました。本機能はつねに有効であり、無効にはできません。また、MSS の値は1220 固定です。

なお、本機能では、IPv6 パケットがIPv4 パケットにカプセル化される時点で、IPv6 パケット内TCP Syn パケットのMSS オプション値を書き換えます。IPv6 パケットのカプセル化を解除するときは、書き換えを行いません。

2. 本バージョンで仕様変更された項目

■ インターフェース統計カウンターの表示変更

本バージョンより、下記のコマンドで64 ビットのMIB カウンターifHCInOctets とifHCOutOctets が表示されるようになっていますが、これらのカウンターは未サポートです。

- SHOW INTERFACE (COUNTERS オプション指定時)
- SHOW ETH COUNTERS

また、MIB オブジェクトifHCInOctets とifHCOutOctets も同様に未サポートとなります。

3. 本バージョンで修正された項目

(1) ログメール送信機能を使用した場合に、一部のログを送信できない場合がありましたが、これを修正しました。

(2) 起動時にトリガースクリプトが実行される際、スクリプトファイルのファイル名（ベース名）が9文字以上だと該当スクリプトを正常に実行できない場合がありましたが、これを修正しました。

(3) スイッチポートのDESCRIPTION を削除した際に、SHOW INTERFACE COUNTERSで表示されるスイッチポートのインターフェース名がデフォルトの表示に戻りませんでしたが、これを修正しました。

(4) Ethernet ポートでリンクダウンをともなうポート無効に設定後、該当ポートの速度設定を変更すると、SHOW ETH STATE コマンドで表示されるActual speed/duplexの表示がConfigured speed/duplex と同じ表示になっていましたが、これを修正しました。

(5) ADD BRIDGE FILTER コマンドのPORT パラメーターに無効な文字列を指定するとリブートすることがありましたが、これを修正しました。

(6) OSPF が設定されたIP インターフェースを通じてパケットを送信中に、同IP インターフェースを削除すると機器が再起動していましたが、これを修正しました。

(7) IPsec/ISAKMP 使用時、対向機器のアドレスをFQDN で指定する場合は、DNS キャッシュ機能との併用ができませんでしたが、本バージョンより併用が可能になりました。

(8) 6 番目に設定されたIP インターフェースでDNS サーバーからのDNS レスポンスパケットを受信した場合、DNS による解決に失敗していましたが、これを修正しました。
なお本事象は、本製品のDNS リレー機能を使用する場合と、本製品自身が直接DNS解決をする場合に発生するものであり、本製品配下のDNS クライアントが直接DNSサーバーに問い合わせる場合には発生しませんでした。

(9) DVMRP を使用したマルチキャストルーティング環境において、同一VLAN に複数のホストが存在するとき、ホストが接続されているポートの1 つがリンクダウンすると、他のポートに接続されたホストへのマルチキャストトラフィックも一時的に停止することがありましたが、これを修正しました

(10) ファイアウォール有効時、フラグメントされたマルチキャストパケットを受信してもルーティングしませんでしたが、これを修正しました。

(11) 2 つのファイアウォールポリシーにおいて、複数のVLAN と1 つのWAN インターフェースとの間でENAT を使用している場合、片方のポリシーに設定されている外部から内部への通信を許可するルールが動作しないことがありましたが、これを修正しました。

(12) DHCPv6 サーバー機能使用時に、DHCPv6 クライアントが接続されているポートの所属VLAN を変更すると、該当クライアントが変更後のVLAN でIPv6 アドレスを取得しようとしても、正しいIPv6 アドレスを割り当てられませんでしたが、これを修正しました。

(13) DHCPv6 サーバー機能使用時に、DHCPv6 クライアントが異なるVLAN 所属のポートに移動した場合、該当クライアントが移動後のVLAN でIPv6 アドレスを取得しようとしても、正しいIPv6 アドレスを割り当てられませんでしたが、これを修正しました。

(14) L2TP インターフェースでOSPF オンデマンドを使用した場合、L2TP の自動接続ができませんでしたが、これを修正しました。

(15) ルーター間のL2TP 接続環境において、L2TP トンネル経由の通信中にL2TP トンネルが切断されると、まれに再接続と切断を繰り返すことがありましたが、これを修正しました。

(16) SHOW ISAKMP SA で表示されるPolicy name 欄に誤ったポリシー名が表示されることがありましたが、これを修正しました。

4. 本バージョンでの留意事項

(1) コンパクションと VLAN インターフェーストリガー
コンパクション中に VLAN のインターフェーストリガーが起動した場合、まれにフラッシュメモリーからファイルが読み込めなくなる場合があります。ファームウェアのバージョンアップ時など大きなファイルを削除する場合は、コンパクションが発生する可能性がありますので、あらかじめ VLAN の

インターフェーストリガーを無効にしてください。

(2) 認証サーバー

RADIUS サーバーを複数登録している場合、最初に登録したRADIUS サーバーに対してのみ、SET RADIUS コマンドの RETRANSMITCOUNT パラメーターが正しく動作しません。最初の RADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも 1 回少なくなります。本現象は 802.1X 認証を使用した場合のみ発生します。

(3) ログ

スクリプトの実行結果を Syslog サーバーに転送すると、20 行分しか送信されません。

(4) インターフェース

- SHOW SWITCH PORT COUNTER コマンドで表示されるスイッチポートの統計カウンターTransmit Discards はつねに「0」であるべきですが、カウントアップされる場合があります。
- 「RESET INTERFACE COUNTER」の実行後に「RESET SWITCH PORT COUNTER」を実行すると、「SHOW INTERFACE COUNTER」で表示されるスイッチポートのカウンターが異常な値を示すことがあります。その場合は、もう一度「RESET INTERFACECOUNTER」を実行して、該当カウンターをリセットしてください。なお、カウンター値が異常になるのは「SHOW INTERFACE COUNTER」の表示だけであり、MIB で取得する値には影響しません。
- 「RESET ETH COUNTER」や「RESET INTERFACE COUNTER」の実行後、「SHOWETH COUNTER」や「SHOW INTERFACE COUNTER」で表示されるカウンターが異常な値を示す場合があります。

(5) ポート認証

- ENABLE/SET PORTAUTH PORT コマンドの SERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで TIMEOUT×(RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。
- DISABLE PORTAUTH コマンドで、PORTAUTH パラメーターに 8021X を指定すると、EAP Success パケットを送信してしまいます。
- RESET ETH コマンドによって Ethernet インターフェースを初期化しても、認証状態は初期化されません。
- 802.1X 認証済みのクライアントがログオフした場合、ログオフしたクライアントの MAC アドレスがフォワーディングデータベース (FDB) に保持されたままになります。

(6) ブリッジング

ポート 1 がタグ付きパケットのブリッジングの対象となる VLAN に所属し、その VLAN に IP アドレスが設定されている場合、ポート 1 から VLAN の IP アドレス宛ての通信をしようとすると、 ルーターが ARP に応答せず、通信ができません。これはポート 1 でのみ発生し、他のポートでは発生しません。

(7) OSPF

- MD5 認証を行う OSPF インターフェースにおいて、大量の LSU (Link State Update) パケットを受信した場合、「MD5 authentication Fails」のログが出力されます。
- 本バージョンでは OSPF の仮想リンクを使用できません。仮想リンクを使用する場合は、バージョン 2.9.1-21 以前のファームウェアをご使用ください。

(8) DNS

○ ダイナミック DNS のアップデートで、以下の 2 つのケースにおいて、アップデートは再送されません。

・ 本製品からの TCP SYN パケットに対して、ダイナミック DNS サーバーからの SYN ACK パケットが返って来ない場合
・ 本製品からの TCP SYN パケットに対して、ICMP Host Unreachable メッセージが返される場合

○ ダイナミック DNS のアップデート（HTTP GET）に対する応答として、ダイナミック DNS（HTTP）サーバーから特定のエラーコード（404 Not Found）を受信すると、SHOW DDNS コマンドの Suggested actions の項目に HTML タグの一部が表示されることがあります。

(9) DNS リレー

○ DNS リレー機能有効時、下記条件のとき、クライアントからの名前解決要求に対してクライアントが指定したアドレスとは異なるアドレスで応答します。

・ 2 つ以上の VLAN が設定されており、それぞれが異なる IP ネットワークに所属している
・ DNS クライアントが、DNS サーバーのアドレスとして自身が所属していない VLAN の IP アドレスを指定している

これを回避するには、自身が所属している VLAN の IP アドレスを DNS サーバーとして設定してください。

○ DNS リレーと DNS キャッシュの併用時､あるドメインの IPv6 アドレス(AAAA レコード)が DNS キャッシュに登録されている状態で、DNS クライアントから該当ドメインの IPv4 アドレス（A レコード)に対する問い合わせを受けた場合､キャッシュ済みの IPv6 アドレスを返答してしまいます。またこれとは逆に､あるドメインの IPv4 アドレス（A レコード）がキャッシュされている状態で、該当ドメインの IPv6 アドレス（AAAA レコード）を要求された場合、キャッシュ済みの IPv4 アドレスを返答してしまいます。この事象を回避するには DNS キャッシュ機能を無効化してください。

(10) IPv6

○ RIPng 経路を利用して IPv6 マルチキャスト通信を行っている場合、経路が無効（メトリック値が 16）になっても、しばらくその経路を利用して通信を行います。

○ 6to4 トンネルは、本製品 1 台につき 1 個だけをサポートします。

○ 6to4 トンネルコマンドを保存し、再起動するとエラーメッセージが出力されます。(動作に問題はありません。)

○ ガーベージコレクションタイマーが動作中の RIPng 経路は、新しいメトリック値を持つ経路情報を受信しても、タイマーが満了するまで経路情報を更新しません。

(11) ファイアウォール

○ ファイアウォールにてリモート IP を指定せずにダブル NAT ルールを設定すると、ルーターがすべての Gratuitous ARP に対して応答してしまうため、Host にてアドレス重複を検出し、通信できないことがあります。

○ ファイアウォールにて動的に IP アドレスが割り当てられるインターフェースを Public インターフェースとして設定した際、ルール NAT の GBLIP パラメーターに"0.0.0.0"を設定すると、NAT 後のソースアドレスが Public インターフェースの IP ではなく、"0.0.0.0" に変換されるためパケットを送信しません。

○ ファイアウォールにて 3 つ以上のファイアウォールポリシーが設定され、かつそれぞれのポリシ

ーにルールが設定されていても、設定されたポリシーのうち 2 つのポリシーのルールしか正しく動作しません。ポリシーにルールを設定する場合はポリシーを 2 つまでにしてください。

○ NAT ループバックの設定で FTP を行うと、3 ウェイハンドシェークが終了しているにもかかわらず、FTP パケットが破棄されます。

○ ファイアウォールでダイナミックインターフェーステンプレートを使用する構成において、ADD FIREWALL POLICY RULE コマンドで既存ルールの番号を指定した場合、重複しないようにルール番号の再設定が行われますが、異なるルールに対して、同じルール番号が設定される場合があります。重複する番号を持つルールは、どちらも動作しており、表示上の問題となります。

○ 本製品自身が送信するパケットにスタティック NAT(1 対 1 のアドレス変換)を適用する場合は、インターフェース NAT のスタティック NAT（NAT=STANDARD）ではなく、ルール NAT のスタンダード NAT（NATTYPE=STANDARD）を使用してください。インターフェース NAT のスタティック NAT では意図したとおりに NAT が行われないことがあります。

(12) DHCPv6 サーバー

○ DHCPv6 サーバーで認証機能を使用した場合、ADD DHCP6 KEY コマンドの STRICT パラメーターが動作しません。

○ ADD DHCP6 POLICY コマンドで DHCPv6 サーバーの設定を変更しても、サーバーから Reconfigure メッセージが送信されません。ADD DHCP6 POLICY コマンドの実行後、さらに SET DHCP6 POLICY コマンドを実行してください。これにより、Reconfigure メッセージが送信されます。

(13) L2TP

ADD L2TP USER コマンドで ACTION パラメーターに dnslookup を指定し、PREFIX パラメーターは未設定とした場合、設定を保存し、再起動するとコンフィグエラーになります。これを回避するには、再起動トリガーで ADD L2TP USER コマンドを再入力してください。

(14) IPsec

○ Android OS 標準の VPN クライアントではない独自 VPN クライアントを実装して IPsec DPD に対応したスマートフォン N-06C とリモートアクセス VPN を行うと、N-06C の送信する R-U-THERE メッセージを受信しても本製品は R-U-THEREACK メッセージを返しません。
これを回避するには、PPP LCP エコーの間隔を短くするなどして、通信中は端末側からの IPsec DPD を動作させないようにしてください。

○ SET ISAKMP POLICY コマンドで IPsec DPD と ISAKMP ハートビートを同時に指定すると、DPD の動作モードが正しく反映されません。IPsec DPD と ISAKMP ハートビートを設定する場合には、同時に指定しないようにしてください。

○ SET IPSEC POLICY コマンドを実行した場合、該当する IPsec ポリシー上に確立している IPSec SA が削除されますが、削除された IPSec SA に IP ルートテンプレートが設定されている場合、テンプレートを通じて追加された経路が削除されません。
DELETE IP ROUTE コマンドで該当する IP ルート情報を削除することにより、この不整合から復旧させることができます。

○ 拠点側の IP アドレスが不定であり、ISAKMP フェーズ 1 の IKE 交換モードが Aggressive モードである環境において、センター側の設定に ISAKMP ポリシーが以下の順で登録されていると、拠点側からの ISAKMP ポリシーによる相手ルーターの検索時、本来適合させたい ISAKMP ポリシー(2) に適合せず、リモート ID 未設定のポリシー(1) にマッチしてしまいます。
(1) ISAKMP の相手ルーターの ID（リモート ID）が未設定の ISAKMP ポリシー
(2) 本来適合させたい ISAKMP ポリシー

この現象は IPsec DPD、ISAKMP ハートビートのどちらを使用している場合でも発生します。たとえば、以下の設定を利用した場合、IKE ネゴシエーションが行われると、センター側では ISAKMP ポリシーi_a が誤って選択されます。

〈 センター側: アドレス固定〉

```
CREATE ISAKMP POLICY="i_a" PEER=ANY MODE=AGGRESSIVE KEY=1
MSGRETRYLIMIT=3 DELETEDELAY=10
CREATE ISAKMP POLICY="i_b" PEER=ANY MODE=AGGRESSIVE KEY=1
SENDNOTIFY=TRUE DELETEDELAY=10 HEARTBEATMODE=BOTH
REMOTEID="id_b"
```

〈 拠点側: アドレス不定〉

```
CREATE ISAKMP POLICY="i_b" PEER=10.0.0.1 MODE=AGGRESSIVE KEY=1
SENDNOTIFY=TRUE HEARTBEATMODE=BOTH LOCALID="id_b"
```

これを回避するには、コマンドリファレンス（「IPsec」/「概要・基本設定」）に示されているように、相手ルーターの ID を正しく設定してください。