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
Version 2.9.2-00

Ver.2.9.2-00

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

（1）アプリケーション検出・遮断機能（Application Detection System：ADS）

ファイル共有ソフトによるP2P 通信は、特定のホストが大量のTCP セッションを使用するため、帯域を占有してしまうことになります。また、ファイル共有ソフトの使用により、意図せず有害なファイルや企業の極秘情報等を拡散させてしまう恐れがあります。ADS(Application Detection System) 機能は、このようなP2P 通信を検知し、必要に応じてブロックすることができる機能です。

（2）IPsec パススルー機能

IPsec パススルー機能とは、NAT 機器配下にあるIPsec 端末が、NAT 機器の先にあるIPsec端末とIPsec 通信ができるようにするための機能です。通常、エンハンストNAT では、送信元アドレスに加えて、送信元ポート番号の変換も行いますが、IPsec 通信で使用されるESP パケットにはポート番号の概念がないため、NAT 機器配下に複数のIPsec 端末が接続されている場合、最初に接続してきたIPsec 端末だけしか接続できません。しかし、エンハンストNAT を使用する際に、PROTOCOL パラメーターで ESP を指定することによって、NAT 機器配下の複数のIPsec 端末がNAT 機器の先にある IPsec 端末とIPsec通信ができます。

（3）IPsec DPD機能

IPsec DPD は、IPsec の対向側の接続断を検知する機能です。本機能では、IPsec SA 上にトラフィックがある限り、対向側が動作していることを証明し、DPD メッセージを送る必要はないと認識するトラフィックベースの検知方法を使用しており、一定時間トラフィックが止まると、対向側の状況が不明と認識し、DPD メッセージを送信します。また、DPD メッセージを受信した対向側は、送信側にDPD ACK メッセージを返信することにより、自身が動作していることを証明します。

2. 本バージョンで修正された項目

（1）MAC ベース認証ポートに指定しているインターフェースをブリッジポートに指定すると、不正なユーザー名の認証リクエストが送出されていましたが、これを修正しました。

（2）ETH ポートにて、リンクアップ/ リンクダウンが発生することにより、まれにパケットの受信ができなくなることがありましたが、これを修正しました。

（3）DHCP クライアント機能使用時、DHCP サーバーから新しいDNS サーバーアドレスを通知されてもDNS サーバーリストを更新せず、以前に通知されたDNS サーバーアドレスを使い続けていましたが、これを修正しました。

（4）RIP 使用時、スタティック経路が削除されても該当経路をメトリック16 で通知しませんでしたが、これを修正しました。

（5）RIP 使用時、インターフェースがリンクアップしてもトリガーアップデートを送信しませんでしたが、これを修正しました。

（6）RIP 機能において、複数に分割されたRIP response パケットを正常に受信することができず、最初の1 パケットのみしか受信することができませんでしたが、これを修正しました。

（7）OSPF ルーターとして動作する場合、LSA を作成、通知を行った後、同じLSA を再度通知することによって、一時的なLSA の不一致が発生することがありましたが、これを修正しました。

（8）ファイアウォールポリシーにMAC アドレスリストを登録するとき、先頭文字がa ～ fのMAC アドレスが登録されませんでしたが、これを修正しました。

（9）ダブルNAT を使用した状態でWAN インターフェースをリンクダウンさせ、ダブルNAT ルールに合致する通信を行うと、本製品がリブートする場合がありましたが、これを修正しました。

（10）ファイアウォール有効時にRSTP のContinuation パケットの遅延が発生し、動画配信が止まることがありましたが、これを修正しました。

（11）DHCP レンジの範囲外にあるIP インターフェースでDHCP Discover メッセージを受信したとき、dhcpRangeExhaustedTrap トラップ（プライベートMIB）を送信していましたが、これを修正しました。

3. 本バージョンでの留意事項

（1）認証サーバーについて

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。

（2）ポート認証について

①DISABLE 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。

②RESET 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。

③802.1x 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。

④ENABLE/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。

（3）ブリッジングについて

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。

（4）ダイナミックDNSについて

①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

②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。

（5）DNSリレーについて

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場合

・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場合

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。

（6）IPv6について

①RIPng 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。

②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。

（7）ファイアウォールについて

①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。

②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。

（8）DHCPv6 サーバーについて

①DHCPv6 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。

②ADD 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。

（9）L2TPについて

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。

（10）IPSecについて

ISAKMP フェーズ1 で使用するIKE 交換モードをAGGRESSIVE モードに設定し、ピアのアドレスをFQDN で設定すると、そのFQDN からISAKMP パケットを受信しても応答しません。

4. 取扱説明書（613-000666 Rev.B）・コマンドリファレンス（613-000667 Rev.D）の誤記訂正

WAN ポート仕様について

取扱説明書（135 ページ）に記載の製品仕様は、以下のように訂正します。

A.7 製品仕様/ ハードウェア/ インターフェース/WAN ポート

[誤] 10BASE-T/100BASE-TX × 1（オートネゴシエーション、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定、常にMDI/MDI-X 自動切替）

[正] 10BASE-T/100BASE-TX × 1（オートネゴシエーション時MDI/MDI-X 自動切替、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定時はMDI 固定）