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 2.9.2-11

Ver.2.9.2-11

以下のとおり機能追加、仕様変更、機能改善が行われました。

1. 本バージョンで仕様変更された機能

1) Telnet セッション数の制御

SET TELNET コマンドの MAXSESSIONS パラメーターにより、Telnet 同時接続セッション数の制御が可能になりました。

書式・パラメーター：SET TELNET [MAXSESSIONS={1-32}]

MAXSESSIONS: 同時接続可能な Telnetセッション数。ここで設定した値のセッション数になると、次に張ろうとするセッションが破棄される。また、設定する際に確立されているセッション数以下の値は設定できない。デフォルトは 32。

2. 本バージョンで変更された項目

1)ログメッセージタイプの名称変更

「コマンドリファレンス」/「運用・管理」/「ログ」DNS関連のログメッセージタイプの名称が、IPDNSから DNSに変更になりました。本仕様変更にともない、以前のバージョンの設定で以下のコマンドのMODULEパラメーターにIPDNSを指定している場合は、DNSへ変更してください。

○ 以前のバージョンでの設定（変更前）

ADD LOG OUTPUT [MODULE=IPDNS]

SET LOG OUTPUT FILTER [MODULE=IPDNS]

SHOW LOG [MODULE=IPDNS]

○ 本バージョンでの設定（変更後）

ADD LOG OUTPUT [MODULE=DNS]

SET LOG OUTPUT FILTER [MODULE=DNS]

SHOW LOG [MODULE=DNS]

2) SHOW IP DNSコマンド及びSHOW IP DNS CACHEコマンドの表示項目名の「IP Address」から「IPv4 Address」へ変更されました。

3) DHCPv4 サーバーの仕様変更

DHCPv4 サーバー機能において、DHCP クライアントに配布した IP アドレスが重複していた場合、DHCP クライアントが送信する DHCP DECLINE メッセージを受信しても同じIP アドレスを再配布することがありましたが、異なる IP アドレスを再配布するように仕様変更しました。

3. 本バージョンで修正された項目

1) WAN 側のフラッディングなどにより、ETH インターフェースに届けられる他の筐体宛のパケットを破棄しない場合がありましたが、これを修正しました。

2) 2.9.2-00 以降のファームウェアにおいて IP NAT 機能を使用する場合、TCP 通信が繰り返されることによって、少しずつメモリーリークが発生していましたが、これを修正しました。

3) PUBLIC 側からの TCP SYN パケットに対する代理応答機能(TCP セットアッププロキシー)を使用し、PRIVATE 側に位置する HTTP サーバーを PUBLIC 側に公開する場合、アクセスが集中すると PUBLIC から HTTP サーバーにアクセスできなくなることがありましたが、これを修正しました。

4) 2.9.2-00 以降のファームウェアにおいて P2P Filter(ADS 機能)を使用する場合、TCP の通信が行われることによって、少しずつメモリーリークが発生していましたが、これを修正しました。

5) FTP クライアントが FTP アクティブモードを使用したとき、送信した FTP 制御コマンドに対して FTP サーバー側からエラー応答された場合、ファイアウォールが誤ってデータコネクションを削除することがあり、その場合 FTP データが破棄されていましたが、これを修正しました。

6) PPP テンプレートを使用して動的に作成されるインターフェース(ダイナミック PPP インターフェース)に設定されたファイアウォールルールは、ルールの削除コマンドで削除できない場合がありましたが、これを修正しました。

7) DHCPv6 サーバー機能において、DHCP クライアントに配布した IP アドレスが重複していた場合、DHCP クライアントが送信する DHCP DECLINE メッセージを受信しても同じIP アドレスを再配布していましたが、これを修正しました。

8) L2TP トンネルの確立を行うとき、L2TP トンネルの接続処理のやり直しが繰り返し発生することにより、長時間完了できない場合がありましたが、これを修正しました。

9) IPv6 IPsec 接続時に高負荷が発生している場合、まれに本製品がリブートすることがありましたが、これを修正しました。

10) 受信した ESP パケットに対して復号化を行った際に、エラーを検出することによってIPsec 通信ができなくなる場合がありましたが、これを修正しました。

11) IPv6 IPsec 構成において、AR ルーターから送信される ESP パケットが対向ルーターで破棄される場合がありましたが、これを修正しました。

12) IPv6 IPsec トンネルを通過する IPv6 パケットにフラグメントヘッダーが付与されている場合、これを破棄していましたが、ルーティングするように修正しました。

13) L2TP/IPsec 使用時、対向機器が不在などの理由により接続ができない状況が続くことによって、まれにリブートが発生していましたが、これを修正しました。

14) Android 端末との間にリモートアクセス接続を行う場合、IPSec SA の更新が行われることによって、SA の保持数が誤ってカウントされていました。AR415S における SA の最大保持数 50 に達した場合、新しい IPSec SA を作成できない事象が発生していましたが、これを修正しました。

4. 本バージョンでの留意事項

（1）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。

（2）ポート認証

①ENABLE/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。

②DISABLE 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。

③RESET 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。

④802.1X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。

（3）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。

（4）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。

（5）DNS

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。

③IPsec/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はできません。

（6）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。

①2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

②DNS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。

（7）IPv6

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。

②6to4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。

③6to4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。）

④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。

（8）ファイアウォール

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。

③NAT 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。

④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。

（9）DHCPv6サーバー

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。

（10）L2TP

①ADD 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。

②L2TP インターフェースでOSPFオンデマンドを使用した場合、L2TPの自動接続を開始しません。

（11）IPsec

①Android 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。

②SET 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。

③SET 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。

④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。

⑤センター側ルーターの ISAKMPポリシーの設定に相手ルーター（拠点側）のリモートIDを追加し、正しい設定を行っても、ISAKMPポリシー適合時のポリシー名が誤って表示されます。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。

5. 取扱説明書・コマンドリファレンスの補足・誤記訂正

（1）CREATE ENCO KEY コマンド （「取扱説明書」92,96,103,107 ページ）

取扱説明書の記載に誤りがありましたので、下記のとおり訂正いたします。

[誤]「CREATE ECHO KEY」コマンド

[正]「CREATE ENCO KEY」コマンド

（2）WAN ポート仕様 （「取扱説明書」135 ページ）

取扱説明書に記載の製品仕様について、下記のとおり訂正いたします。

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）

（3）ICMP （「コマンドリファレンス」/「IP」）

本体宛 ICMPv4/v6 Echo Request パケットの ICMP チェックサムフィールド値が「0xffff」である場合、同フィールドの値が「0x0000」であると見なしてチェックサムを検証します。