サザンクロスルータシステム「AR260S V2」
ファームウェアリリースノート
Version 3.3.0

Ver.3.3.0

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

アプリケーション検出機能

ADS(Application Detection System: アプリケーション検出システム) 機能として、下記の検出が可能になりました。なお、検出はWAN 側インターフェース (Ethernet またはPPPoE)にて受信した場合に行われ、検出後の動作として「破棄」もしくは「通過」を設定できます。

●Winny(Version2)

2. 本バージョンで仕様変更された機能

(1)かんたんVPN

これまでの「かんたんVPN」設定が「1 対1 接続」に変更され、新たに「多拠点接続」が追加されました。 閉域網サービスを利用したセンターと各拠点を、ハブ＆スポーク型で接続するVPN を構築します。 接続形態ごとに以下のメニューが選択可能です。

①センタールーターとして設定

②拠点ルーターとして設定

●拠点となるルーターは、他拠点およびインターネット宛のパケットをセンタールーター経由で送るように設定されます。

●フレッツ・VPN ワイド等のCUG サービスで使用する場合、事前に管理者によるIP アドレスの割当等を行ってください。

(2)Web GUI

①Web GUI 使用時のブラウザーとして、Microsoft Internet Explorer 8(Windows 版)に対応しました。

②かんたん接続に、フレッツ 光ネクストの「サービス情報サイト」設定画面を追加しました。

③かんたん接続で設定されるNTT東日本のフレッツ・スクウェアの経路情報を更新しました。

(平成21年3月13 日現在の内容)

④DHCP に、任意の動的DHCP クライアントを固定クライアントに登録できる設定を追加しました。

⑤アクセス制御で設定されるアクセスリストのプロトコル設定画面で、プロトコル番号を指定できるようにしました。

（3）ファイアウォール、NAT 機能の拡張

①ファイアウォール/NATのFTP ALG 機能が、FTP Extensions (EPRT、EPSV コマンド) に対応しました。

②ファイアウォール/NAT のキャッシュ数が最大値を超えた場合、古いキャッシュを削除して新しいキャッシュを作成するようにしました。

（4）ファイアウォール、セルフアクセス機能の拡張

セルフアクセス制御の有効/ 無効をインターフェース単位でも設定できるようにしました。 これにより、システム全体でのセルフアクセス [有効/ 無効] および、インターフェース単位でのセルフアクセス [有効/ 無効] の組み合わせによる動作が、以下のようになります。

システム	インターフェース	動作結果
有効	有効	有効
	無効	無効
無効	有効	無効
	無効	無効

システム:「システム管理」内のセルフアクセス

インターフェース:「セルフアクセス」内のインターフェース単位のセルフアクセス

3. 本バージョンで修正された項目

（1）JVNVU#410676「ISC DHCP dhclient におけるバッファオーバーフローの脆弱性」の対策を実施しました。

（2）ファイアウォールが有効な際に、通信負荷が高い状態でアクセスリストのキャッシュや、NAT キャッシュの削除を行う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。

（3）ファイアウォールが有効な際に、"Sequence number error" がログに記録され、通信が中断されることがありましたが、これを修正しました。

（4）ENAT を設定した構成において、NAT 変換後のIP アドレス（WAN 側インターフェースのIP アドレス）を送信元IP アドレスに持つパケットをLAN 側インターフェースで受信した場合、WAN 側に転送していましたが、これを破棄するようにしました。

（5）高負荷状態でIPsec のRekey が発生すると、まれにIPsec 通信が一時的に不安定になることがありましたが、これを修正しました。

（6）IPsec を使用した際、通信負荷が高い状態が続くと、通信に使用していたIPsec/ISAKMP SA が削除された場合、通信できなくなることがありましたが、これを修正しました。

（7）IPsec を使用した際、通信負荷が高い状態が続くと確立済みのIPsec SA のSPI を持つESP パケットが未学習のSPI パケットとなり通信できなくなることがありましたが、これを修正しました。

（8）IPsec のRekey の際に更新されたSPI のESP パケットを受信すると、未学習のSPI と認識されてしまいパケットが破棄される場合がありましたが、これを修正しました。

（9）IPsec の内部NAT を使用している際に、"BLOCKED (match NAT address)" とログに記録され、しばらくの間拠点間の通信が行えなくな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）PPPoE インターフェース複数使用時のIPsec 経路変更

PPPoE インターフェースを複数設定し、仮想トンネルインターフェースを使用するIPsec 環境において、IPsec 対向機器に対する経路（ルーティングテーブル）を変更する場合は、一度「切断」ボタンを押してPPPoE インターフェースを切断してから行ってください。

（2）MSS クランプ値の手動設定時のMSS 値

WAN 側インターフェースの設定においてMSS クランプ値を手動設定にした場合、MTU 値が1454Byte 以外の時にMSS 値が正しく設定されないことがあります。 そのため、自動設定を使用するか、正しいMSS 値になるようにMSS クランプ値を調整してください。

（3）デフォルトルートの出力インターフェース

トンネルインターフェースを利用した IPsec 構成において、デフォルトルートの出力インターフェースをトンネルインターフェースにしている場合、WAN 設定の内容を変更すると、デフォルトルートの出力インターフェースが、PPPoE インターフェースに変更されてしまいます。