

WatchGuard System Manager and Fireware™

WSM v10.2.8 / Fireware v10.2.8X リリースノート

概要

ウォッチガードは、この度 WatchGuard System Manager (WSM) v10.2.8管理ソフトウェアと、Fireware / Fireware Pro v10.2.8アプライアンス・ソフトウェアをリリース致しました。

今回のリリースでは、ハイ・アベイラビリティ、Mobile VPN with SSL、シングル・サインオンなどウォッチガード・ユーザの皆様より報告された問題をいくつも取り上げ、バグフィックスを用意しました。また、新しいMobile VPN with IPSec client (v10.2)もこのリリースには含まれています。

修正問題の詳細については「解決した問題」の欄を参照してください。

インストール前の注意点

このリリースをインストールする前に、次のアイテムがあることを確認してください：

- (重要) Fireware、Fireware Pro v8.3またはそれ以降にリリースされたバージョンがFireboxにインストールされていること。旧バージョンのFirewareをFireboxにインストールしている場合は、Fireware v10.2.8をインストールする前にFireware v8.3、またはそれ以降にリリースされたバージョンをまずインストールしてください。手順詳細については「既知の問題」の欄をご覧ください。
- (重要) 現在使用しているFirewareまたはWFSの設定ファイルのコピーがあること。設定ファイルのバックアップを取る方法については、WatchGuard System Managerユーザガイドの「Configuration Files」を参照してください。
- (重要) Firewareイメージのフル・バックアップ、またはFirebox X WFSのイメージがあること。イメージのバックアップを取る方法については、WatchGuard System Managerユーザガイドの「Configuration Files」を参照してください。
- 下記の「WSM v10.2.8 システム条件」でリストに挙げられている必要なハードウェアとソフトウェア・コンポーネント、状況に適したFireboxなどがあること。
- Fireboxに使うフィーチャー・キーがあること。新規ユーザは、Fireboxを登録後にフィーチャー・キーをWatchGuard LiveSecurityのウェブサイトで購入してください。Firebox X CoreやPeak e-Seriesをすでに登録しているが、v9.0のリリース以来フィーチャー・キーをアップデートしていないという場合は、新しいフィーチャー・キーをダウンロードしFireboxにそれを保存することで、フィーチャー・キーに制限をかけるファイアウォール・スループットの変更事項を活用することができます。
- ドキュメントはウェブサイトより入手可能です。www.watchguard.com/help/documentation

WatchGuard System Manager v10.2.8 必要最低条件

	WatchGuard System Managerクライアント・ソフトウェアのみをインストールしている場合	WatchGuard System ManagerとWatchGuard Serverソフトウェアをインストールする場合
オペレーティング・システム	Windows Vista (32-bit)、XP SP2 (32-bit)、Windows Server 2003 (32-bit)	Windows Vista (32-bit)、Windows XP SP2 (32-bit)、Windows Server 2003 (32-bit)
ブラウザ	IE 6、IE 7、Firefox v2	該当なし
CPU	インテルPentium 4	インテルPentium 4
プロセッサ速度	1 GHz	2 GHz
メモリ	512 MB	1 GB
ディスクの空き容量	80 MB	1GB

ソフトウェアをダウンロードするには

WSMやFireware v10.2.8をダウンロードするには:

- 1.LiveSecurityのウェブサイトにあるSoftware Downloadsページ
<http://www.watchguard.com/archive/softwarecenter.asp>にアクセスしてください。
- 2.LiveSecurityのウェブサイトでログインしてください。次に、使用している製品シリーズを選択しWSMとFireware v10.2.8ソフトウェア・ダウンロードの欄を探してください。

インストールとアップグレード

WatchGuard System Managerソフトウェアをインストールする前に、下記の「既知の問題」の欄を読んでください。

注意

WSM v10.2.8インストーラはWSMのフル・インストールとは異なります。WSM v10.2.8にアップグレードするには、WSM v10.2、またはそれ以降にリリースされたバージョンがインストールされていなければなりません。WSM v10.2のインストール手順については、WSM v10.2リリースノートをご覧ください。

FireboxでWSMとFireware v10.2.xを実行していてWSMとFireware v10.2.8をアップグレードする場合

1. **Policy Manager File > Backup**で現状のFireboxイメージのバックアップを取ります。
2. WSMをアンインストールする前にアプリケーションを全て閉じ、WatchGuardのツールバーを使って全サーバを停止させます。
3. Management Serverを使用している場合は、アップグレードを行う前にManagement Server設定のバックアップを取って下さい(Management Serverのアイコンを右クリックして**Backup/Restore**を選択)。
4. WSM10_2_8.exeをスタートさせ、画面に表示されるインストール手順に従って下さい。注意: WSM10_2_8.exeを実行する前にWSM v10.2またはそれ以降のバージョンがインストールされていなければなりません。
5. fireware10_2_8.exeをスタートさせ、画面に表示されるインストール手順に従って下さい。
6. FireboxをFireware v10.2.8にアップグレードするには、WSM v10.2.8を使ってFireboxに接続します。Firebox X PeakやFirebox X Coreの設定ファイルを開くにはPolicy Managerを使ってください。
7. Policy Managerから**File > Upgrade**を選択したら、
C:\Program Files\CommonFiles\WatchGuard\resources\Fireware\10.2に行きます。
8. FW1020B215550.wgu ファイルを選択したらOKをクリックし、Fireboxが再起動するのを待ちます。アップグレードが完了すると、メッセージが表示されます。
9. イメージ・アップグレードが終了したら、**File > Save > To Firebox**で設定をFireboxに保存します。

Firebox X CoreやPeak e-Seriesデバイスで初めてFirewareやFireware Proソフトウェアをインストールする場合

ソフトウェア・インストールと初期設定については、Quick Start Guideの手順を参考にしてください。

Firebox X CoreのWFSからFirewareアプライアンス・ソフトウェアにアップグレードするには

このリリースをインストールするには、www.watchguard.com/help/documentationから入手できるMigration Guideの手順を参考にしてください。FireboxをManagement Serverとして使っている場合は、まずWSM/Fireware v8.3にアップグレードしなければなりません。WSM/Fireware v8.3に問題なく移行したら、上記の手順を参考にWSM/Fireware v10.2.8へのアップグレードを完了させてください。

- Gateway AntiVirus for E-mailやSpamScreenのサブスクリプションはWFSを実行しているFirebox Xでのみ利用可能であるため、Firebox XをWFSからFirewareにアップグレードすると、そうしたサービス機能は停止します。

- まだ有効期限が切れていないGAV for E-MailやSpamScreenを使用している場合は、新しいGateway AntiVirus/IPSやspamBlockerサービス・サブスクリプションを割引価格で購入することができます。詳細については弊社のリセラーまでお問合せください。
- LiveSecurityおよびWebBlockerのサブスクリプションにおいては、アップグレード後も変更はありません。

Mobile VPN with IPSec v10.2クライアント・ソフトウェアを入手しインストールするには

LiveSecurityのウェブサイトで購入できるMobile VPN with IPSec v10.2リリースノートの手順を参考にしてください。

Windowsでv10.2.8 Mobile VPN with SSLをインストールするには

v10.2.8 Mobile VPN with SSLクライアントはFireware 10.2.8アプライアンス・ソフトウェアに統合されています。Mobile VPN with SSLユーザには、Fireboxからv10.2.8クライアントをダウンロードする方法と、リモート・ユーザがポート4100でFireboxにアクセスすることができない場合に、WatchGuardのウェブサイトからv10.2.8をダウンロードする方法があります。旧バージョンのクライアント・ソフトウェアを実行しているSSLクライアント・コンピュータがv10.2.8を使用しているFireboxに接続すると、SSLクライアントをバージョン1.14にアップグレードするように促されます。**Yes** をクリックしてMobile VPNクライアントをv10.2.8にアップグレードしてください。ユーザがアップグレードをしない場合でもMobile VPN with SSLは機能しますが、Mobile VPN with SSLクライアントのv10.2.8を対象としたフィックスを受取ることはできません。

シングル・サインオン (SSO)ソフトウェアをインストールするには

旧バージョンのSSOインプリメンテーションからアップグレードする場合は、まず既存のSSOエージェントをアンインストールしなければなりません。v10.2.8リリースでは、新しいSSOクライアント・ソフトウェア・パッケージをインストールし、シングル・サインオン・インプリメンテーションの効率性と正確性を向上させることができます。この新しいSSOインプリメンテーションの詳細については、Fireboxのヘルプシステムを参照することをおすすめします。

v10.2.8 シングル・サインオン・エージェント・ソフトウェアをインストールするには:

1. <http://www.watchguard.com/support> に行き、LiveSecurityユーザ名とパスワードを入力してログインします。Software Downloadsページへ行き、WatchGuard Single Sign-On Agent v10.2.8をダウンロードしてください。次に、WG-Authentication-Gateway.exe ファイルをハードディスクに保存します。
2. Microsoft Windows 2003やWindows XP、Windows Vistaを使用している静的IPアドレスのドメイン・コンピュータでファイルをインストールし、セットアップ・ウィザードを完了させます。この場合、ドメイン・コントローラにSSOエージェント・ソフトウェアをインストールすることをおすすめします。設定手順の詳細については、WSM/Firewareヘルプシステムを参照してください。

v10.2.8 シングル・サインオン・クライアント・ソフトウェアをインストールするには:

1. <http://www.watchguard.com/support> に行き、LiveSecurityユーザ名とパスワードを入力してログインします。Software Downloadsページへ行き、WatchGuard Single Sign-On Client v10.2.8をダウンロードしてください。WatchGuard-Authentication-Client.msiファイルをハードディスクに保存します。
2. SSOクライアント・インストーラーはMSIファイルであるため、ユーザがドメインにログオンすると自動的にユーザのコンピュータにインストールされるようにすることも可能です。Active Directoryグループ・ポリシーを使い、ユーザがドメインにログオンすると自動的にソフトウェアをインストールするように設定することも可能です。Active Directoryグループ・ポリシー・オブジェクトのソフトウェア・インストールの詳細については、<http://www.microsoft.com>を参照してください。Microsoft Windows 2003、Windows XP、Windows Vistaを実行しているコンピュータでのみ、クライアント・ソフトウェアをインストールすることができます。

解決した問題

一般

- このリリースでは上4つのポートを使用中のFireboxデバイスに見られる複数の安定性問題を解決しています。
[27896] [29899] [30057] [30093]
- 数日に渡り、Fireboxのロード量が多かった後でも、WSMやFirebox System Managerがこれまで以上に安定した状態でFireboxに接続することができるようになりました。[35309]
- いくつかのポリシーがある状態で設定を保存する場合の所有時間が60%も削減されました。[27791]
- IPSがCPUを100%使用している場合でもFireboxが機能します。[31361]
- 保存領域を大幅に取らないようにするため、サポートファイルが正確に交換されるようになりました。[33551]

ネットワークとVPN

- このリリースでは、PPPoEとの不安定性問題を修正しています。[29212]
- Fireboxが隣のネットワークからOSPFルーティング・テーブル情報を受信しなかった問題を解決しました。[27202]
- 2人のユーザが同じ名前とIPアドレスでログインした場合に、IKEDプロセスが無反応だった問題を解決しました。
[33067] [33361]
- 複数のモバイルVPNユーザがログインしている状態で設定を保存しても、MIAプロセスがクラッシュしないようになりました。[33617]
- ユーザはDynDNSを使わずに、動的アドレスの外部インターフェイスとMobile VPN (SSL、PPTP、IPSec)を使用できるようになりました。[32707] [32715] [32716]

- Fireboxで設定するユーザ名にスペースを使用できるようになりました。[33687]
- サーバ・ロード・บาลancingが、10分ではなく30秒内に停止したサーバを検知できるようになりました。

WatchGuard System Manager (WSM)

- Firebox X Peak e-Seriesデバイスのロードが少ない場合でも、Traffic Monitorのトラフィック・ロードを測定する機能が100%と誤って表示していた問題を解決しました。[27950]
- Firebox System Manager Traffic Monitor機能の“highlight search results”が大文字と小文字を区別しないようになりました。[33318]
- Log Serverのアラーム/通知メールで送信者のアドレスが表示されるようになりました。[31489]
- Report ServerがPOP3レポートを生成できるようになりました。[332974]
- 複数のLog Serverを使った場合でも、デバイスの接続性が正しく記されるようになりました。[31524]
- spamBlockerが100%大量スパムメールと誤って報告しないようになりました。[28562]

シングル・サインオン

- Authentication ListのSSOログイン情報がすぐに更新されるようになりました。[31856]
- SSOエージェントがWindowsイベント・メッセージ:EventType clr20r3でクラッシュしないようになりました [32775]
- SSOクライアントが正しいドメイン名を戻すようになりました。
- SSOクライアントとエージェントは、ADドメイン名情報とNetBIOSドメイン名情報のどちらをも正確に処理できるようになりました。
- SSOクライアントとエージェントは、予期していなかった接続不良が10秒以内に発生した場合でも、正確に反応できるようになりました。

ハイ・アベイラビリティ

- 外部ファイバー・インターフェイスでのHA監視が正しく機能するようになりました。[32967]
- HAを有効にしても、ほぼ2分ごとにブランチオフィスVPNがre-keyを行わないようになりました。[33402]
- 重要なプロセスがフェイルした場合、HAフェイルオーバーがすぐに実行されるようになりました。[33823]

Mobile VPN with SSL

- パスワードを入力しなかったり、長いパスワードを入力しても、SSLVPNデーモンがフェイルしないようになりました。
[31894] [35183]
- Mobile VPN with SSL Mac OS Xクライアントが、バ운드IPアドレスとゲートウェイに接続したIPアドレスを正しく表示できるようになりました。[34561]
- Mobile VPN with SSL Mac OS Xクライアントが切断されたり終了した場合、検索ドメインとDNS情報を除去するようになりました。[34564]
- Mobile VPN with SSL Mac OS XクライアントがどちらのWINSアドレスも表示するようになりました。[34560] [23635]
- Mobile VPN with SSL Mac OS Xクライアントがデフォルトのログ・レベルを低く設定するようになりました。
[34563]
- Windows Vistaを実行しているコンピュータでMobile VPN with SSLクライアント・ソフトウェアをインストールした場合、利用可能なネットワーク経路が正しく追加されるようになりました。[34558]

既知の問題と制限

WatchGuard System ManagerやFireware v10.2.8の既知の問題は次の通りです。問題の中には、回避策があるものもあります。

Fireware v8.2またはそれ以前のバージョンからFireware v10.2.8にアップグレードする場合

- Fireware v8.0、v8.1、v8.2.xから直接Fireware v10.2.8にアップグレードすることはできません。Fireware v10.2.8をインストールする前に、まずFireware v8.3にアップグレードしてください。
- IE6を使っている場合、ウェブベースのクイック・セットアップ・ウィザードでFireboxへのソフトウェアのロードや初期設定が不完全である場合がありますが、これはInternet Explorer6が古いキャッシュ・ファイルやスクリプトを処理する方法に起因しています。

回避策

ウェブ・ブラウザのキャッシュを削除し、再度試してください。キャッシュを削除するには、Internet Explorerのツールバーからツール> インターネット・オプション > ファイル削除を選択してください。

Quick Setup Wizard

- 管理ステーションにインストールしているQuick Setup Wizardは、セットアップ時に設定ファイルにあるLog ServerのIPアドレスを管理ステーションにある一時的な動的IPアドレスに設定します。(10.0.1.100/24)[13908]

回避策

WSMベースのQuick Setup Wizardは、Log Serverがすでにインストールされている静的IPアドレスがあるコンピュータでのみ使用してください。

認証

- https://xy_wz:4100のようにURLパスで下線“_”を使用すると、認証アプレットはロードしません。[27196]

回避策

FireboxにDNSエントリを使用している場合は、URLで下線を使用しないでください。

SNMP

- Fireware v10.xは、Fireware v9.0やそれ以前のバージョンで使われているHA-MIBをサポートしません。[23998]

WatchGuardサーバ問題

- WatchGuard Log ServerやReport Serverをすでにインストールしていて、Management Serverを初めてインストールするためにWSMインストーラを再び実行している場合、再起動するまでManagement Serverにタスクバー・アイコンが表示されません。[27459]

- 英語以外のWindows 2000にサーバ・ソフトウェアをインストールすることはおすすめしません。

- Report ServerとLog Serverの管理ユーザ・インターフェイス、メール設定では**Server Settings tab > Send a warning if the database reaches the warning threshold**を有効にしなければなりません。少なくとも**Send warning message to**のテキストボックスを埋めるに充分の長さが必要です。Log ServerやReport Serverから送信されるメール通知はこのアドレスに送られます。Log ServerやReport Serverが送信する全てのメールのメール・セNDERは、Expiration SettingsタブにあるNotification Setupで設定できます。このサーバからメール通知を送信する前に、**Turn on notification**のボックスをチェックして有効にし、**Send email from**のテキストボックスを完了してください。

- Management Server、Report Server、Log Server、Quarantine Serverは同じ管理パスワードを使います。Management Serverにバックアップ設定を保存する場合は、全サーバの管理パスワードが変わります。[22381]

- Master Encryption Keyを変更した場合は、WatchGuardサーバを全て停止し再起動させなければなりません。[27416]

- 停止したサーバは、サーバ・ソフトウェアがインストールされているコンピュータが再起動した後に再び開始します。[2752]

回避方法

コンピュータのスタート時に自動的にサービスを開始させたくない場合は、Windows Servicesアプレット (スタート> プログラム > 管理ツール > サービス) を使って、状況に適したサービスを手動開始に変更するためにStartup Typeを設定してください。

検疫サーバ

- Quarantine Serverは、ログイン・ディレクトリがないディレクトリに設定されていた場合スタートしません。
[23540]

ロギング / ログ・サーバ

- **Maximum Database size** 設定は、しきい値の通知にのみ使われます。この設定は Log Serverデータベースによって使用されるディスクの空き容量を制限しません。[27338]
- v10.xロギング/レポート・システムにおいては、ログファイルをWFS 7.xフォーマットからXMLに変換するためのツールが必要ないため、WSM v10.xには含まれていません。新システムはログファイルの作成を行ったり、WFSアプライアンス・ソフトウェアがインストールされているFireboxにレポートしたりすることができます。
- Windows 2000を実行しているコンピュータでLog Serverをインストールしている場合、Windows Installer 3.1やService Pack 4をインストールしないとLog Serverがスタートしません。[24169]

レポート / レポート・サーバ

- レポートを統合させるために10台以上のFireboxをグループでまとめた場合、Most Popular Domainレポートの合計バイト数が不正確である場合があります。[23838]
- Report ServerがLog Serverにログ・メッセージを送信するように設定しており、どちらのサーバも同じコンピュータにある場合、Boxes Under ManagementレポートはManagement Serverレポートのリストではなく、Report Serverレポートのリストに表示されます。[23834]
- Report Managerのロード・レポートをキャンセルした場合、停止するまでに長時間かかる場合があります。[22887]
- Denied Packets Summaryレポートは、処理された記録数のレポートと概要で拒否された数の差を表示します。パケットが拒否された最後のデバイスは、そのレポートに表示されません。[23805]
- WSM Device ManagerはUTC フォーマット(YYYY-MM-DDTHH:MM:SSZ)で挿入された時間を含むログ・メッセージを送信しますが、これはReport Serverのローカル時間として誤って表示されます。UTC情報は除去されますが、タイムスタンプがローカル時間に変換されません。[23822]
- Report Managerからレポートをメールで送信する前にメール・クライアントを設定していないと、メールは送信されず、Report Managerがメール・クライアントにログインできなかったことを示すJavaポップアップが画面に表示されます。
[23774]
- v10.xリリースではレポート機能において様々な改善点を施していますが、新しいLog Serverは、これまでのHistorical Reportsに対応しないので、旧バージョンのWSMで利用可能なレガシーのHistorical Reportsツールを好み、それを使用したい場合は既存のLog Serverを使用し続けなければなりません。WFSを実行しているアプライアンス・ユーザーや、その他ユーザで既存のレポート・ツールに慣れている場合は、WSM v10.xにアップグレードする前にドキュメントをよく読んでください。

Firebox X EdgeデバイスのWSM Centralized Management

- Dead Peer Detection for Mobile User with IPSecを集中管理で設定することはできません。[29568]
- ワイヤレス・クライアントとしたEdgeの外部インターフェイスを設定するために、WSMを使うことはできません。
[23081]
- Mobile VPN with IPSecをグループで設定するオプションはWSMにはありません。[23097]
- マルチWANが有効になっているEdgeの受信ポリシーでは、WAN1またはWAN2のみの設定を許可しません。
[23199]
- WSMでグローバル・コンフィギュレーション設定が有効になっている場合、WSMは1-to-1 NAT設定をサポートしません。[23251]
- Mobile VPN with SSL仮想IPアドレス範囲を設定する場合は、IPアドレス範囲がDHCPやPPTPで使用されているものと重ならないようにしてください。[22460]
- x10からx55へアップグレード後、WSMはステータス・タブでEdgeの製品タイプを変更しません。[15809]
- Firebox X Edgeデバイスが集中管理設定に追加され、再起動が必要な変更が行われた場合でも、変更事項を適用するために再起動が必要であることを知らせる通知はありません。[11985]
- v8.6.xやv10.xを実行しているFirebox X Edge e-Seriesのワイヤレス・コンフィギュレーション設定でWPA2を選択することはできません。[21557]
- 集中管理の環境下で「Apply to VPN」オプションはありません。IPSec BOVPNTラフィック用のVPN-Anyポリシーが作成されています。[23195]
- Gateway AV/IPSページにVirus Outbreak Detectionオプションが表示されますが、このオプションはspamBlockerでのみ適用することができます。[23180]

Management Server

- Management ServerのFile > Import from File機能を使うことができません。Management Serverの設定を回復させるには、Management Serverのタスクバー・アイコンを右クリックしBackup/Restoreオプションを使います。[27511]
- 管理しているFireboxの証明書が取り消しになっても、Management Serverのリースが無効になるまで表示されません。[14041]
- Management Serverは、マルチWANを使用し静的および動的の外部インターフェイスの両方を備え、管理されているデバイスを正しく認識しません。WSM v10.x Management Server は、EdgeやFirebox X Core、Peakなどを静的または動的のどちらかで認識しますが両方で認識することはありません。Fireboxに静的と動的の外部インターフェイスがある

場合、BOVPNTunnelは最初の外部インターフェイスにのみ設立されます。[21416]

- フェーズ1用にAES暗号を使ったカスタムVPNポリシー・テンプレートは、Fireware v9.0やそれ以前のバージョンを実行しているFireboxでは使うことができません。Management Server は、v10.xとフェーズ1用にAESを使ったv9.1までのバージョンではドラッグ・アンド・ドロップでトンネルを設立することができましたが、v9.1以前のバージョンが入っているFireboxではその設定が拒否されます。[21627]

- ドロップイン・モードで設定されているFireboxの内側にManagement Serverがあり、また別のドロップイン・モードで設定されているFireboxに対してBOVPNが作成されていてBOVPNTunnelが確立されていない場合、リモートFireboxはManagement Serverと通信することができません。[21475]

- 標準設定で管理されているVPNTunnelは、NATトラバーサルを有効にしません。[23756]

- 標準設定によるVPNTunnel機能を使う場合、リモート・ネットワークからのトラフィックはすべてManagement Serverが作成したデフォルトのANYポリシーにマッチします。リモート・ブランチオフィスVPNTraフィックが集中ロケーションで設定されたほかのファイアウォール・ポリシーにマッチすることを妨げます。この集中ロケーション特定のポリシーにトラフィックがマッチするように強制したい場合は、VPNテンプレートを使用しなければなりません。Management ServerのVPNテンプレートは、集中ロケーションのファイアウォール・ポリシーにマッチすべきトラフィック以外のブランチオフィスVPNTunnelを介したトラフィックすべてにマッチするポートを含まなければなりません。[21965]

Firebox System Manager (FSM)

- Firebox System Managerが何時間もFireboxに接続していた場合、Fireboxで多少のメモリ・リークが見られることがあります。[15518]

- Fireware v10.x を使用しているFirebox X CoreやPeakと、v10.xを実行しているFirebox X Edge間で管理されているブランチオフィスVPNTunnelのステータスがFirebox System Managerで正しく表示されないことがあります。[23413]

WatchGuard System Manager (WSM)

- WSM 10.2.x をインストールした後も **Start Menu > All Programs** には、これまでと同様にWatchGuard System Manager 10.2と表示されます。

- v9.xからv10.2.xにアップグレードすると、**Setup > Logging > Advanced Diagnostics > Set all sub-categories to same level of detail** ボックスのチェックが外されます。[27514]

- Firebox がマルチWAN用に設定されていた場合、WSMはPPPoE-based WANインターフェイスのステータスを表示しません。[19564]

- NetMeetingパケット・フィルタが機能しません。NetMeetingトラフィックがFireboxを通過できるようにするには、H.323プロキシ・ポリシーを使用してください。[24281]

- Fireboxがドロップイン・モードに設定されていた場合、Status Reportは実際のドロップイン・ネットワークのサブネットにかかわらず、外部インターフェイスのサブネットマスクが255.255.255.0であると誤って表示します。[21458]

ネットワーキング

- インターフェイスのエイリアスを使用する静的NATルールがある場合、インターフェイスIPアドレスを変更すると静的NATルールが機能しません。[23502]

回避方法

ポリシーから静的NATルールを除去し、インターフェイス・エイリアス使用のIPアドレスを使うルールと取り代えてください。

- DHCPリース更新が起きると、通常では見られないログ・メッセージが表示されます。リース更新は問題なく完了、ログ・メッセージは無視して構いません。ログ・メッセージは次の通りです：Deny x.x.x.x x.x.x.x icmp-Dest_Unreach code(3) 1-Trusted Firebox icmp error with data src_ip=x.x.x.x dst_ip=x.x.x.x pr=dhcp/bootp-client/udp src_port=67 dst_port=68 src_intf='1-Trusted' dst_intf='0' cannot match any flow, drop this packet 176 128 (internal policy) rc="104" [27364]
- セカンダリ・ネットワークでDHCPを使用する場合、DHCPクライアントに与えられたDHCPサーバのIPアドレスは、プライマリ・インターフェイスIPであり、セカンダリ・インターフェイスIPアドレスではありません。[10365]
- インテルのCSA bus-based MAC (i82547) を使用するFirebox X Peak製品シリーズの5000、6000、8000とMarvell PCI bus-based MAC (88E8001)の間に互換性の問題があります。場合によって、ネットワーク・インターフェイスは1000MBの代わりに100MBで交渉することがあります。[13659]
- インターフェイスのリンク速度を1000MBに強制することで、インターフェイス・リンク速度の交渉にフェイルした結果、フルまたはハーフ・デュプレックス(半二重)になることがあります。リンク速度の自動交渉オプションを常に使用することをおすすめします。[21319]
- ICMPプロトコルの届かなかったメッセージはFireboxを通過しません。Setup > Global Settings > ICMP Error Handlingで Protocol Unreachable Messagesを許可するオプションは使えません。[21236]

プロキシとサービス

- FTPプロキシ・ポリシーを使うとアクティブ・モードのFTPコマンドがフェイルする場合があります。問題が発生した場合のFTPプロキシのログ・メッセージの例は次の通りです。proxy[1854] 1:1193825662: ftp response '425 Can't open data connection.¥x0d¥x0a' [22229]
- **Turn on logging for reports** オプションの標準設定のプロキシ・ポリシーには一貫がありません。POP3プロキシ・トラフィックはデフォルトでログされていますが、その他のプロキシ・ポリシーはデフォルトでログ・メッセージを送信することはありません。このオプションでは Traffic Monitorでプロキシ・トランザクションの詳細を表示するかどうか管理します。[23259]
- HTTPプロキシ経由ではQuickTime Video-On-Demandが機能しません。[19112]
- 同じTCP-UDPプロキシ・ポリシーでIntrusion Preventionが有効にされていないと、TCP-UDPプロキシでブロックするアプリケーションの通知が機能しません。[27305]

- TCP-UDPプロキシを有効にすると、送信用のSIP接続がTCP-UDPプロキシに正しく送信されません。[23546]

回避方法

SIP接続を直接処理できるようにするため、SIPプロキシを設定してください。

- TCP-UDPプロキシを有効にすると、送信用のFTP接続がTCP-UDPプロキシに正しく送信されません。[23533]

回避方法

FTP接続を直接処理できるようにするため、FTPプロキシを設定してください。

- POP3プロキシ設定で**Hide Server Replies**ボックスのチェックが外されていても、サーバ・セッションのExitバナーは匿名になります。[23714]

- Uuencoded および BinHexの添付ファイルを遮断するためにSMTPプロキシを設定する場合、添付ファイルのヘッダーの一部は拒否されたメッセージと共にメールの本文に残ります。[22989]

回避方法

Uuencoded や BinHex添付ファイルを阻止する機能を無効にしてください。

- SMTPプロキシやspamBlockerでアドバンス・ロギング・レベルを高く設定し過ぎた場合、Fireboxはプロキシ・トラフィックが高レベルになっているため不安定になる場合があります。[21459]

- 設定に複数のフィーチャー・キーがあり、そのうちの1つの有効期限が無効になると、v10.xにアップグレードした後でセキュリティ・サブスクリプションやシグネチャ・アップデートがフェイルします。[24050]

回避方法

Policy Managerで設定を開き**Setup > Feature Keys**に行きます。有効期限が切れているフィーチャー・キーを削除するため、**Remove** を1度だけクリックしてください。設定をFireboxに保存します。

- Firebox X Core製品シリーズのX500、X700、X1000、X2500などでプロキシ・ポリシーを複数使用している場合は、Fireboxのメモリを512MBにアップグレードすることをおすすめします。512MBメモリ・アップグレード・キット購入をご検討されている場合は、ウォッチガードのリセラーまでお問合せください。

- VoIPデプロイメントは複雑であることが多く、様々なスタンダードや専用のプロトコルを使用します。ベーシック・ボイスやビデオ・トランスファー用の現プロキシでは、H.323とSIPプロトコルを使用するスタンダードベースのトラフィックのみをサポートしています。VoIPの業界用語では、そうした新しいプロキシをより正確に表すため、アプリケーション・レイヤー・ゲートウェイ(ALG)と呼ばれています。データ・ファイル転送(チャット、whiteboarding、ファックス送信など)、トラフィック・コントロール(QoS)、各プロトコルでその制限が記されているものなど、ALG機能やサービス、設定の中にはサポートされていない機能もあります。こうした理由から、プロダクション・デプロイメントに入る前に自己環境下で互換性と相互運用性をテストすることを強くおすすめします。

- H.323プロキシはボイス・アンド・ビデオトラフィックでNATトラバーサルをサポートします。H.323ゲートキーパー(PBXホスティング/トランキング)とT.120マルチメディアは今回のリリースでサポートされていません。このため、ビデオ会議のようなポイント・ツー・ポイントでのプロキシ使用には制限があります。互換性や相互運用性を保証することはできませんが、ポイント・ツー・ポイントのオーディオやビデオ接続に関しては一般的なソフトウェア・クライアントやビデオ会議用のハードウェアで実証されています。

- トランスペアレントSIPプロキシは、ボイストラフィックやビデオトラフィックでNATトラバーサルをサポートします。通常のスタンドアロン、SIPレジストラ・プロキシのPBXレジストレーション機能は提供していませんが、SIPトラフィックに対したランスペアレントなアプリケーション・レイヤー・ゲートウェイを提供しています。このトランスペアレントSIPプロキシは、PBXトラフィックのパススルーをサポートしますが、こうした接続をルートするには自分のレジストラ・プロキシ・サーバが必要となります。今回のリリースでは、Firebox(トランキングではなくホステッド状態)の外部セグメントにあるPBXでのみ、トランスペアレントSIPプロキシがテストされています。互換性や相互運用性を保証することはできませんが、ポイント・ツー・ポイントのオーディオやビデオ接続に関しては一般的なソフトウェア・クライアントで実証されています。また、ホステッド・オーディオ接続も様々な電話ハンドセットで実証済みです。

spamBlocker

- Virus Outbreak Detection (VOD)を使ったspamBlockerを有効にしている、Gateway AVでメールをスキャンしている場合にSMTPプロキシがスパム兼ウィルスのメールを検出すると、SMTPプロキシはVODのメッセージ対応設定に従います。特に、VODアクションが**Strip**で設定されていて添付ファイルがメッセージから除去され、それを回復することができない場合に見られます。VODアクションが**Lock**で設定されている場合、添付ファイルは検疫されたメッセージ内でロックされた状態になります。[23709, 23711]

- Virus Outbreak Detection (VOD) がメール検出をしたことにspamBlockerが気付くと、メールの添付ファイルは全て取り除かれるか検疫されます。メールがHTML形式で送信されていた場合は、メール本文もその対象になります。[23485, 全プラットフォーム]

- 感染したメールから複数の添付ファイルが(埋め込まれたメール本文など)VODで検出され、Firebox が**Strip** アクションを実行するように設定されていた場合、添付ファイルで拒否されたメッセージと共に添付ファイルのメール・ヘッダーの一部が受信した添付ファイル内に残ります。ただし、ウィルスの中身は常に取り除かれるようになっているため、ヘッダー情報が問題となることはほぼありません。[23550, 全プラットフォーム]

- Firebox X Core製品シリーズのX500、X700、X1000、X2500で spamBlocker Proactive Patterns機能を使うことはできません。Policy Managerでは、ユーザがe-Series Core Firebox以外でプロアクティブ・パターン機能を設定することができても実際にはそれが機能することはありません。[21496]

Gateway AV/IPS

- Firebox System Manager Security Servicesタブは、毎時間1度、AVエンジン、AVシグネチャ、IPSシグネチャの入手可能なバージョン情報のみを更新します。このため、手動アップデート後、インストールしているバージョンよりも古いバージョンが入手可能なバージョンとして表示されることがあります。Security Services情報を更新するには、Fireboxと繋がっているFSMを切断してから再度接続してください。[21639]

- 感染したメール・メッセージをGateway AVがロックするように設定している場合に、メールの添付ファイルが100Kバイト以上で、最初の100Kバイト以降にウィルスが検知されるとログ・メッセージではそのファイルがロックされたと表示

されますが、実際には添付ファイルはロックされずに切断されます。[21489]

WebBlocker

- WSM 9.x またはそれ以前のバージョンからWSM v10.xにアップグレードした場合、WebBlocker Server用にWebBlockerの新しいフル・データベースをダウンロードしなければなりません。WebBlocker Serverデータベースは、40カテゴリから54カテゴリにアップグレードされました。以前のWSMバージョンのWebBlockerデータベースや設定ファイルを維持することにした場合でも、このアクションを実行する必要があります。アップグレード後、WebBlockerのプロファイル設定を確認し、新しいカテゴリを活用できることをチェックしてください。

- WebBlocker設定によりHTTPS接続が正しく阻止されると、クライアントに拒否メッセージが送り戻されません。阻止されたHTTPS接続はログ・ファイルに正確に記録されます。[22515、全プラットフォーム]

- v9.1 のWebBlockerで**Deny All Categories** のボックスがチェックされている状態で、WSM/Fireware v10.xにアップグレードするとボックスのチェックが外されます。[23679]

回避方法

v9.xまたはそれ以前のバージョンからWSM/Fireware v10.xにアップグレードした後は、**Deny All Categories**ボックスを再びチェックし、変更事項をFireboxに保存してください。

ユーザ・インターフェイス

- WSM v10.2.x ソフトウェアには、ユーザ・インターフェイスに影響のない様々なバグ・フィックスが含まれています。v10.2.x リリースで施されたユーザ・インターフェイスへの変更はローカライズされていません。ローカライズ版のv10.1からv10.2.x リリースにアップグレードする場合は、新しいUI は英語のままとなることに注意してください。ローカライズされたヘルプ・コンテンツのアップデートはありません。

ブランチオフィスVPN

- 複数のIKE フェーズ1とフェーズ2のプロポーザルがPolicy Managerで設定されている場合、FirewareはVPNトンネルが始まると最初のIKEプロポーザルのみを送信します。FirewareがVPNトンネルをスタートさせない場合、Firewareはそのマッチが見つかるまでプロポーザルのリストを循環させます。こうした問題から、プロポーザルを複数使用している場合は、VPNトンネルの両端でフェーズ1とフェーズ2のプロポーザルの順がマッチするようにしておくことが大切です。[24834]

- 証明書が撤回されたり更新された場合、有効な証明書を備えているマネージド・ブランチオフィスVPNトンネルは、ドロップイン・モードでFirewareを始動させた場合に表示されません。[11409]

回避方法

WSMを使ってマネージド・ブランチオフィスVPNトンネルを削除してから再びトンネルを確立してください。

- v8.3リリースより、BOVPN共有キーでASCII以外の文字を使用できないようになっているため、共有キーの欄でASCII以外の文字を入力することはできません。

Mobile VPN with IPsec

- Add Mobile VPN with IPSec Setup Wizardの終わりに、グループにユーザを追加するためのボックスが見えないことがあります。[27554]

回避方法

ボックスを見れるようにするには、Setup Wizardのウィンドウ・サイズを拡張してください。

- 稀に、リモートのMobile VPNクライアントからの大きなFTP転送がドロップされることがあります。これは特に、フェーズ2のre-keyで転送が切断された場合に見られます。クライアントは2回目のフェーズ2 Security Association (SA)を使って再度接続し、1回目のSAからのパケットがドロップされる前に2回目のSAからパケットが来るようになります。[12340]

回避方法

フェーズ2のProposal Forced Key Expirationスレッショールドのバイト数を0に設定し、タイムアウト設定を増やしてください。

Mobile VPN with PPTP

- Mobile User with PPTPを設定すると、設定ページの下半分が利用できない場合があります。[27621]

回避方法

設定ページ全体を表示するにはウィンドウ・サイズを拡張してください。

- ネットワーク設定で1つ以上のDNSサーバやWINSサーバを定義する場合、PPTPクライアントには最初に設定したDNSサーバまたはWINSサーバのみを挙げたリストが提示されます。[12575]
- FireboxにPPTPクライアントが接続する場合、connection-specific DNSサフィックスは指定されません。[17394]

Mobile VPN with SSL

- Mobile VPN with SSLクライアントの初期接続後に行われるMobile VPN with SSL設定への変更は、Windows Vista SP1クライアントとの接続問題の原因になります。クライアントは正常に接続しているように見えますが、フラッシュに失敗したARPテーブルのログ・メッセージを送信します。[29621]

回避方法

この問題を回避する方法は2つあります。

1. Vista PCのUser Account Control (UAC) を無効にしてください。
2. Program Files >WatchGuard >WatchGuard Mobile VPN with SSLに行き、wgsslvpcnを右クリックしてください。Run as Administratorを選択します。

- Mobile VPN with SSLクライアントは、12またはそれ以上のネットワークにルートするように設定されている場合に接続に失敗することがあります。クライアントは、クライアント設定サイズによりサポートできるルート数に制限があります。ルート制限数は正確なものではありませんが、設定のデータによりその制限は12から25までとなります。[24226]

- クライアント・コンピュータに1つ以上のアクティブ・ネットワーク・インターフェイスがあった場合、Mobile VPN with

SSLクライアントは接続を維持できない場合があります。[27112]

- Mobile VPN with SSL Active Directory 認証で、(ä,ö,ü,ß) のようなASCII 文字をユーザ名に使用することはできません。[23647]
- Windows 2000 Professionalを入れているコンピュータでMobile VPN with SSLクライアントをインストールすることはできません。[22550] [23667]
- Mobile VPN with SSLが有効になっている場合、SSLVPN Anyサービスを除去することはできません。[24656]

回避方法

Mobile VPN with SSLユーザにカスタム・ポリシーを追加し、SSLVPN Anyポリシーを無効にしてカスタム・ポリシーを追加することができます。

ユーザガイド

WSM/Fireware v10.2.8リリースのユーザガイド変更事項は、ヘルプシステム(英語) www.watchguard.com/help/documentation で説明しています。今回のリリースでは、WSM ユーザガイドのアップデート版はありません。

テクニカル・サポート

技術に関する御質問はウォッチガードのテクニカル・サポートへお電話またはウェブサイト

<http://www.watchguard.com/support> よりお問合せください。テクニカル・サポートにお問合せの際は、登録している製品のシリアル番号とLiveSecurityキー、またはパートナーIDを予めご用意ください。

	電話番号
米国エンドユーザ	877.232.3531
海外のエンドユーザ	+1 206.613.0456
ウォッチガードの代理店	206.521.8375

10.2.x リリースで解決した問題

この欄では参考までに、10.2.xバージョンまでのリリースノートで解決した問題をリストにしています。各リリースのインストール手順や技術情報、既知の問題については必要なバージョンのリリースノートをダウンロードしてください。

WSM/Fireware v10.2.1で解決した問題

認証

- Vasco 2-factor認証とMobile VPN with IPSecを使用している場合でも、Fireboxが正確にユーザとグループを関連できるようになりました。Policy ManagerのAuthentication > Group configurationで正しいグループ名になっていれば、FireboxはRADIUSサーバが戻すグループ名をマッチさせることができるようになりました。ユーザが認証した後、グループをベースにしたポリシーは、そのユーザに対して正常に機能するようになりました。[26819]

注意

Filter-IDの属性値は、Mobile VPN with IPSecのユーザ・グループの名称とマッチしなければならず、そうでない場合はMobile VPN with IPSec認証がフェイルします。Firewareポリシーへのアクセスをフィルターするため、ファイアウォール認証(ブラウザを使いFireboxへポート4100接続)に、二要素認証(two-factor authentication)を使用している場合Filter-IDの属性値は、認証を実施するためのポリシーで使用しているグループ名とマッチしなければなりません。

- SSL VPNユーザ・グループではなく、Fireboxの別のグループにいるユーザがMobile VPN for SSLクライアントから問題なく認証できるようにしていた問題を解決しました。ユーザはMobile VPN for SSLクライアントでFireboxに認証するには、SSL VPNユーザ・グループに入っていなければならないようになりました。[25790]

WatchGuard System Manager (WSM)

- 9.xから10.2.1にアップグレードすると、Dead Peer Detectionが既存のBOVPNトンネルでデフォルトで有効にされないようになりました。[27899]

Firebox System Manager (FSM)

- HostWatchにあるビュー・フィルターのボックスにチェックが付いていない場合は、HostWatchがゼロ接続を表示しないようになりました。[27568]

Mobile VPN with SSL

- Mobile VPN with SSLとFirebox認証を使う場合、パスワードの最初の文字として#を使うことができるようになりました。[25499]

プロキシ

- SSLエンドポイントがドメインのないSSL接続に応答しても、HTTPSプロキシがクラッシュしないようになりました。[27983]
- SMTPプロキシとPOP3プロキシが、base64-encodedメッセージからのエクストラ・パディング文字列の入った添付ファイルを遮断しないようになりました。[27445]

アップグレードに関する問題

- 1-to-1 NATとVLANを使ってFirebox v10.1からアップグレードする場合でも、Fireboxがクラッシュしないようになりました。[27758]

レポート / レポート・サーバ

- Report Server Administration Logging タブでWindows Event Logオプションを無効にすると、Event Logへのログインが正確に無効になるようになりました。[27795]
- レポートで定義済みのレポート・カテゴリが何度も表示されないようになりました。新たにインストールしたv10.2.1のReport Serverでのみ、このフィックスは適用されています。現在この問題の影響を受けているユーザは、Report Serverのデータベースに起因するこの問題を修正するスクリプトについてウォッチガードのサポート部まで連絡するか、Report Serverをアンインストールしてから再度インストールし、Report Server インストールに関連するデータを全て除去する方法をとることができます。[27815]
- Report Server は次のログ・メッセージでHTTP URL Detailレポートの生成に失敗しないようになりました。Error (8203), Exception get_http_url_detail_records().[27811]

Logging/ Log Server

- 2台のデバイス間のSSL接続が90秒以上に渡り待ち状態になっている場合、FireboxとLog Server間の接続をログイン・プロセスが再スタートさせるようになりました。待ち状態にあるため、動けない状態になっていた接続を正確に検知できずFireboxがLog Server にログ・メッセージの送信を停止していた問題を解決することができました。[27788]
- v10.xからv10.2.1にアップグレードした後、レポート定義ファイルのディレクトリ・ロケーションが過去のバージョンに向けられていたため、Report Managerがスタートに失敗していましたが、その問題を解決しました。[27624]
- 同時ログイン接続の数が多かった場合にLog Serverをクラッシュさせていたバグを解決しました。[27343]
- v10.x からv10.2.x にアップグレードした後、Log Serverがフェイルする原因となっていた問題を解決しました。[27775]

WSM/Fireware v10.2.2で解決した問題

認証

- 認証機能コードに見られたメモリ・リークの問題を解決しました。[28417]

WatchGuard System Manager (WSM)

- 設定を保存後、サーバ・ロード・バランシング用のスティッキー接続設定が標準設定の8時間にリセットされなくなりました。[27833]
- Mobile VPN with PPTPのMTUやMRU設定の標準値が1400になりました。PPTPベースのVPNトンネルを介したアプリケーションの中には、これにより相互運用性を改善できるものもあります。[27316]

レポート / レポート・サーバ

- データを見やすくするため、拒否されたパケットのレポート概要やSMTPプロキシのレポート概要がトップ50件のみを表示するようになりました。[28328]

Logging/ Log Server

- Additional Info Columnをベースにした検索クエリが情報を戻さなくしていた原因のLogViewer Search Manager問題を解決しました。[28067]

VPN

- 新しいBOVPNTunnelを設定しやすくするため、Fireware v10.2.2や Edge v10.2.2でのブランチオフィスVPNの標準設定が同じになりました。[27979] [28389]

ネットワーキング

- Firebox X CoreやPeak e-Seriesデバイスでのイーサネット・ポート4から7のトラフィックにおいて、デバイスが検出した無効なIPパケットのログ・メッセージ: invalid IP packet detected by device, firewall dropでフェイルしないようになりました。これは、HA ハートビートでポート4から7が使用されていた場合のハイ・アベイラビリティの不安定性により生じていた問題です。[23817] [25947]

WSM/Fireware v10.2.3で解決した問題

WatchGuard System Manager (WSM)

- Firebox の管理者がWSMをインストールするために使用したアカウントとは別のアカウントで管理ステーションにログインした場合、Windows Vista EnterpriseがPolicy Managerをスタートできないようにしていましたが、その問題が解決されました。[27450]
- Edgeの集中管理機能を使用していて、**Require User Authentication**ボックスのチェックが外された場合でもLDAPやRADIUS認証用の設定ページが無効にならないようになりました。[29339]

レポート / レポート・サーバ

- v10.x のReport Serverが作成したレポートにフィルターを使うことができるようになりました。新しいレポートは作成されませんが、レポートで表示されるデータをフィルターにかけることができます。[28729]

Logging/ Log Server

- Additional Info Columnをベースにした検索クエリが情報を戻さなくしていたLogViewer Search Manager問題を解決しました。[28067]

注意

この問題は v10.2.2リリースで修正されたと誤って報告されていました。

検疫サーバ

- HTML形式やリッチテキスト形式で検疫サーバに送信されたメールが、検疫サーバから解放された後にプレーンテキスト形式で表示されないようになりました。[28058]

SMTPプロキシ

- spamBlockerの例外にマッチしたメールを検疫するようにspamBlockerを設定している場合、SMTPプロキシが200サクセス・メッセージを送信するようになりました。スパム、大量メール、不審メール、VODとして分類されたメールを検

疫するようにspamBlockerが設定されている場合も、200サクセス・メッセージは送信されます。送信メールクライアントに200サクセス・メッセージを送り返すことで、検疫サーバでのメール重複を防げることが可能です。[29332] [29333]

Mobile VPN with IPSec

- 認証サーバがセッションやアイドル・タイムアウトの属性を送信しない場合、Mobile VPN with IPSecのPolicy Managerでセッション・タイムアウトやアイドル・タイムアウトの設定が義務付けられるようになりました。[19657]
- 複数のMobile VPN with IPSecクライアントがNATを行っている同じリモート・デバイスの内側からFireboxに認証しても、Ikedがクラッシュしないようになりました。[27748] [28601]

Mobile VPN with SSL

- Mobile VPN with SSLクライアントがWindow Vista SP1をサポートするようになりました。[27901]
- Mobile VPN with SSLクライアントとゲートウェイが中間者攻撃から保護するようになりました。IPアドレスがFireboxの外部インターフェイスに指定された場合、Mobile VPN with SSLゲートウェイは自己署名によるx.509証明書を生成します。v10.2.3クライアントの初回接続時にゲートウェイはこの証明書を提示しますが、証明書が自己署名であるためMobile VPN with SSLの全ユーザが最初にFireboxに接続すると、不審な証明書に関する警告メッセージが表示されます。ユーザには、その証明書を信頼しローカルに保存するオプションが与えられます。その証明書を信頼できるものとして許可すると、証明書が変更され中間者攻撃の可能性が出た場合にMobile VPN with SSLクライアントはユーザに対し警告することができます。[27304]

シングル・サインオン

- ドメイン名に見られるASCIIではない文字が、Malformed “list” reponse from SSO Agentというログ・メッセージで認証を失敗させる原因にならないようになりました。v10.2.3 SSO Agentはこの問題を解決します。[27198]

ネットワークング

- Firebox(例:/29ネットワーク)の内側で使用するために、ISPはひとまとまりになっているパブリック・アドレスを提供しますが、サブネットのネットワーク・アドレスをFireboxの外部インターフェイスに指定することでFirewareがPPPoE設定をサポートするようになりました。[27823]

WSM/Fireware v10.2.4 で解決した問題

一般

- SNMPシステム・アップタイムが248日で停止しないようになりました。システム・アップタイムは497日まで延長され、その後は再び0からカウントされます。[29753]
- WSMインストール手順時の言語選択オプションで、英語ではなく日本語で日本語選択が表示されるようになりました。[30265]

WatchGuard System Manager (WSM)

- wgauth_adminツールがManagement Serverから除去されました。このツールは、Management Serverにログインしていたユーザがサーバ管理のパスワードやログ暗号キーを入手し変更できるようにしていました。[30429]

レポート / レポート・サーバ

- WFSを実行しているFireboxでWebBlockerレポートを使えるようになりました。[28596]

Logging/ Log Server

- Log Serverに送信されるログ・メッセージの量を減らすため、FireboxはSMTPやPOP3プロキシ・ポリシーにより、デフォルトで拒否されるESMTPのログ・メッセージを送信しないようになりました。[29700]
- これまでのログ暗号キーを使わずに、ログ暗号キーを変更できるようになりました。[28730]
- ログ・メッセージのタイムがNTPサーバと同期化している場合、Fireboxはログ・メッセージを送信します。[13038]

HTTPSプロキシ

- HTTPSプロキシのアイドル・タイムアウトがセッション・タイムアウトとして処理されないようになりました。[28706]

認証

- ポート4100での認証がSSLv2をサポートしないようになり、Payment Card Industry (PCI) のスタンダードに準拠するようになりました。[29863]

シングル・サインオン

- シングル・サインオン・ソリューションはv10.2.4リリースで改善されました。シングル・サインオン・クライアントは、ネットワークの各コンピュータにインストールすることができるようになり、認証している人物のを正確性を向上させることができます。詳細情報については上記のクライアント・インストール手順を参照してください。
- 100人以上の認証済みユーザがネットワークにいる場合、Firebox経由でのアクセスがre-query時に中断されていましたが、認証ユーザのリストが2分ごとにリセットされないようになりました。ユーザのリストが再度クエリされるにはそれぞれリセットが必要です。[27965]

WSM/Fireware v10.2.6 で解決した問題

一般

- SNMP システム・アップタイムがゼロのままにならないようになりました。[31399]
- SNMPトラップが有効になっている場合、SNMPがクラッシュしないようになりました。[31110]
- バンド幅メーターがデータ表示を停止しないようになりました。[31392]
- ハイ・アベイラビリティ・ペアに設定を保存する際に、Mobile VPN with IPSec接続が切断されないようになりました。[27928]
- セカンダリ外部IPアドレスが設定された場合に、Fireboxを再起動した後もPPPoEが問題なく交渉するようになり

ました。[30812]

WatchGuard System Manager (WSM)

- ポリシーに適用されたスケジュールが無効になると、アクティブ・セッションが終了するようになりました。[29223]
- フォワード・スラッシュ(/) 記号が、組織名やよくあるCA証明書名で使われないようにするため、Management Server Setup Wizardと管理用UI を変更しました。旧バージョンではUIがフォワード・スラッシュの使用を許可していましたが、Management Server がスタートに失敗していました。[27898]

レポート / レポート・サーバ

- クライアントによるURLの詳細レポートが、IPアドレスの代わりにユーザ名を表示するようになりました。[29535]
- レポートのタイトルに表示される日付が、レポートにあるデータの日付範囲に対応するようになりました。これまではレポートが生成された日付が表示されていました。[28295]
- 例外スタック・トレースでレポート作成がフェイルしたり、レポート実行の速度を低下させていたReport Serverに見られたメモリ・リーク問題を修正しました。[29087] [28565]

HTTPプロキシ

- セキュリティ機能がどちらにおいても有効になっている場合、HTTPプロキシがIPSとGateway AVのためのボディ・スキャンを実行しないようになりました。Gateway AVとIPSがどちらも有効になっている場合、Gateway AVにのみボディ・コンテンツ・スキャンが実行され、IPSはGateway AV のボディ・コンテンツ・スキャンの結果を使用します。また、これによりスキャン重複がなくなるため、スループットが改善されます。[28002]

シングル・サインオン

- SSOの例外が正常に機能するようになりました。[27964]

Mobile VPN with SSL

- Mobile VPN with SSLのFirebox認証ページで、0-9, a-z, A-Z, . _ - @といった文字もサポートするようになりました。サポートされていない文字や記号を使用すると、それが無効であることを知らせるメッセージが表示されます。これは挿入攻撃を阻止するために役立ちます。[30538]
- Mobile VPN with SSLクライアントがポート4100でFireboxにアクセスすることができない場合、クライアントが接続するまで長時間待つことがなくなりました。[30570]
- Mobile VPN with SSLクライアントをスタートさせると、そのコンピュータのDNSクライアント・サービスが停止し、Mobile VPN with SSLクライアント設定で提供されているDNSサーバのIPアドレスをコンピュータが使うようにアップデートするため、再起動させます。[28120]

WSM/Fireware v10.2.7で解決した問題

一般

- Firebox X CoreやPeak e-Seriesを介したブランチオフィスVPNやMobile VPN with IPSecトラフィックに関係するカーネル・クラッシュ問題をこのリリースで解決しました。[29491]
- 設定を保存する場合にトラフィック・パスをFireboxが停止しないようになりました。[27821]
- BOVPNTunnel・ルートの設定ページで1-to-1 NAT用のホスト範囲エントリーをPolicy Managerが阻止しないようになりました。[30010]
- サーバが応答せず、サーバにトラフィックが送信されなくなった場合、Firewareのサーバ・ロード・バランシング機能がそれを正確に検知するようになりました。[27276]

WatchGuard System Manager (WSM)

- VPN ファイアウォール: マネージドBOVPNTunnel用のポリシー・テンプレートを作成する場合、QoSとスケジュールを適用できるようになりました。[10270]
- WSMに接続しようとした場合でも、HTTP response code: 500 for URL https://x.x.x.x:4117/cmm/cmd というエラー・メッセージが表示されないようになりました。[29336]

ハイ・アベイラビリティ

- 設定保存中に、Fireboxに対しアクティブになっているMobile VPN with PPTPトンネル接続があった場合、Firebox System Managerは「in-transition」としてHAピア・ステータスを表示しないようになりました。[27557]
- HA コンフィギュレーションで設定された2台のFireboxに設定を保存した後も、WSMとFirebox System Manager接続がフェイルしないようになりました。[31990]

Mobile VPN with SSL

- Windows SSL VPNクライアントをWindows XPでインストールする場合にRuntime Errorメッセージが表示され、インストールに失敗することがなくなりました。[31932]
- コンピュータの節電モードが解除された後にWindows SSL VPNクライアントが正しく機能するようになりました。[31523]