clearswift

SECURE Gateways バージョン 4 の主な機能の概要

Clearswift SECURE Gateways

1.0 版

2016 年 9 月

著作権

修正番号 1.0　2016 年 9 月

Clearswift Ltd.発行

目次

はじめに

本文書では、Clearswift SECURE Gateway 製品バージョン 4（2016 年 11 月にリリースのバージョン 4.5 まで）の主な機能に関して説明します。いずれもバージョン 3.x では利用できなかった機能です。

プラットフォーム

Red Hat Enterprise Linux（RHEL）

RHEL を利用する場合、下記に示す多くの利点があります。

- エンタープライズグレードの セキュリティ。
- 親しみのある Redhat OS 環境が利用できます。
- フォーチュン 500 社（政府、軍事、金融業界）で幅広く使用されています。
- 新しいハードウェアのサポート拡大
- 64 ビット オペレーティングシステム（4GB 超の RAM を使用できます。）
- クラウド環境のサポート改善（AWS、Azure などの公開クラウドプロバイダー）
- サードパーティのアプリケーションおよびドライバーのサポートにより、ツールをプラットフォームへロードしてシステムの運用および管理をサポートできます。
- IPv6 対応（予定）
- 製品を「アプライアンス」または「ソフトウェア」として導入できます。

プラットフォーム コンソール

ネットワーキング構成、外部接続（NTP、SNMP、SCOM サーバーなど）、コマンドラインアクセス、製品アップデートの管理が、システムコンソールを介して行われるようになり、システム管理者のみが重要なシステムパラメーターを変更できます。

強力なコンソール パスワード

セキュリティ強化のため、システムでは、コンソールアクセスのために強力なパスワードの使用を求められます。

SNMP および SCOM の監視

SNMP や SCOM などの標準システム管理ツールを使用したプラットフォームの監視が標準となりました。

ウイルス対策

アンチスパムエンジンの強化

スパムの検出を向上させ、誤検出を減らすために、下記のような複数の改良が施されました。

1. 新しい TRUSTmanager 送信者 IP システム（導入が簡単で、より正確）
2. 新しい署名エンジン（下記に基づくメッセージの検索と分類）
    a. バルクメールの検出
    b. メッセージのレピュテーション チェック
    c. 内容チェック
    d. スパムトリックの検出
3. DKIM サポート

Kaspersky Security Network

Kaspersky が新しいウイルスを検出すると、クラウド参照を介して新しい署名を利用することができるようになり、これは次の署名に追加されます。この方法により、新しいマルウェアの変異体のスパム検出が大幅に向上します。というのは、新しいマルウェアは、Kaspersky によりマルウェアとして認識されるため数分で検出されるからです。

クラウドベースの参照により、ウイルス署名の時間が数時間からわずか 3 分に減らすことができます。

Sophos Live Protection

Sophos が新しいウイルスを検出すると、クラウド参照を介して新しい署名を利用することができるようになり、これは次の署名に追加されます。この方法により、新しいマルウェアの変異体のスパム検出が大幅に向上します。というのは、新しいマルウェアは、Sophos によりマルウェアとして認識されるため数分で検出されるからです。

クラウドベースの参照により、ウイルス署名の時間が数時間からわずか 3 分に減らすことができます。

AV　ヒューリスティックスキャン、行動スキャン

いずれの AV ツールも定期的に更新される署名ファイルを使用しますが、新たに判明したマルウェアであるか否かを判断するためにリアルタイムの参照も行います。また、ヒューリスティック分析をファイルに対して実行し、過去に観察された他のマルウェアに類似していないかファイルのコード／構造を検査します。したがって、100%保証できるわけではありませんが、マルウェアの新しい亜種を検出できます。

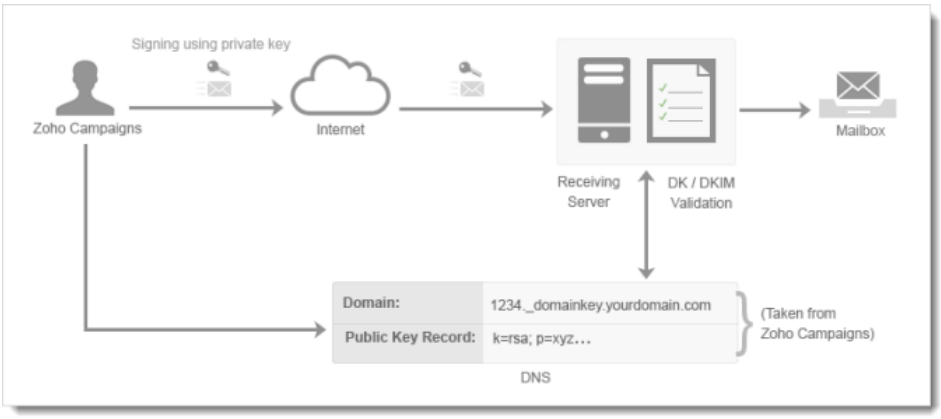
行動スキャンでは、プログラムの行動を理解するために、コードエミュレーション機能を介してコードを実行します。コードが予期しない動作を実行している場合、AV エンジンは、このファイルを問題ありとしてフラグを付けることもできます。

スプーフィングメールの保留および新しいスプーフィング検出アルゴリズム

スプーフィングメールは、組織にとって大きな問題であり、それを監視および検出する方法を提供することが鍵です。バージョン 4.x では、スプーフィングメールを隔離することができ、また検出を簡素化するための新しいアルゴリズムが追加されています。

DKIM（DomainKeys Identified Mail）

DKIM は、正規の電子メールであるか否かを特定する方法の 1 つであり、送信されてくる不正メッセージの量を減らすために役に立ちます。



また、こちら送信したメッセージがビジネスパートナーにより正式のメールとして信頼されるためにも役に立ちます。

CIDR ベースのホワイトリストのサポート

CIDR（Classless Inter-Domain Routing）アドレスは、簡単な短い方法で隣接する IP アドレスをリストアップし、それをホワイトリストで簡単に使用できるようにする方法の 1 つです。

たとえば、192.168.1.0～192.168.1.255 の範囲のアドレスは、CIDR の表記法を使用して 192.168.1.0/24 と表記できるため、より簡単に使用できます。

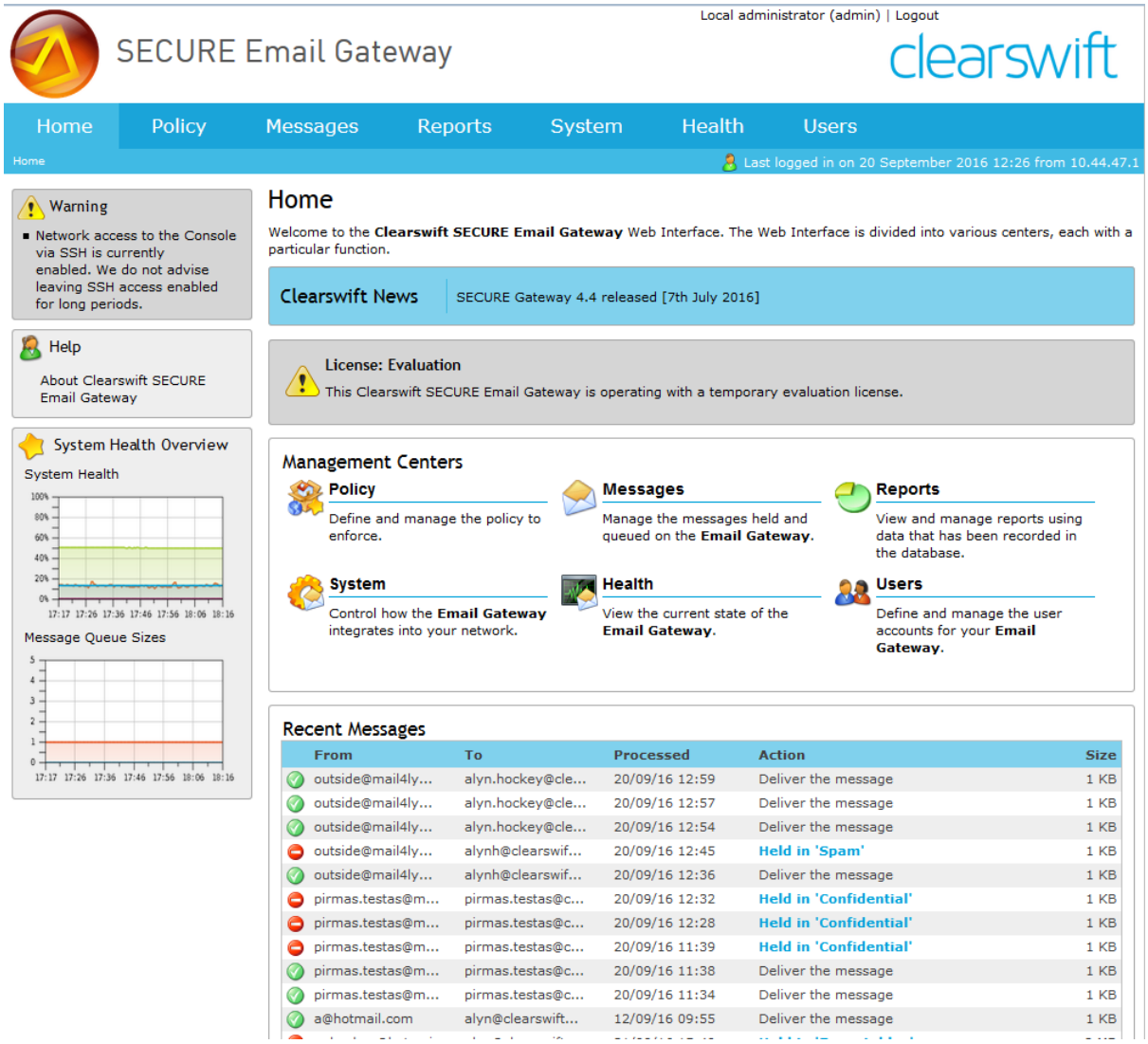
ニュースレター スパム オプション

ニュースレター（メールマガジン）は、一部の人にとっては不要（スパム）でも他の人は欲しがるような種類のメッセージとして一般に捉えられています。企業がどのようにスパム検出を設定したいかにもよりますが、このアプローチを気に入れば、下記の指示を使用して不要なメールマガジンの誤分類を管理できます。

1. スパムの疑いがあれば、それを「保留エリア」にセットします。
2. PMM を使用してスパムを管理し、受信したいメールマガジンをホワイトリストに登録します。

clearswift

ユーザーインターフェースの刷新



バージョン 4.5（2016 年 11 月リリース）のユーザーインターフェースは、現代化かつ最適化されており、フラッシュオブジェクトはすべて削除されています。

こうした変更によりユーザーインターフェースの応答性が向上しています。

メッセージ処理の向上

アダプティブリダクション（秘匿化）－Open Office

データリダクション（秘匿化）、構造サニタイゼーション、ドキュメントサニタイゼーションのサポートが追加され、Open Office ファイルフォーマットの検索や修正が可能になりました。

	VBA Macro	Javascript	Vbscript	ActiveX	OO Basic	Python	Beanshell
DocX	y	n/a	n/a	y	n/a	n/a	n/a
PptX	y	n/a	n/a	y	n/a	n/a	n/a
XlsX	y	n/a	n/a	y	n/a	n/a	n/a
HTML	n/a	y	y	y	n/a	n/a	n/a
RTF encoded HTML	n/a	y	y	y	n/a	n/a	n/a
PDF	n/a	y	n/a	y	n/a	n/a	n/a
RTF	n/a	n/a	n/a	y	n/a	n/a	n/a
Calc	n/a	Y	n/a	n/a	Y	Y	Y
Draw	n/a	Y	n/a	n/a	Y	Y	Y
Impress	n/a	Y	n/a	n/a	Y	Y	Y
Writer	n/a	Y	n/a	n/a	Y	Y	Y

データリダクション（秘匿化）－Excel

Excel シートでテキスト項目をスキャンして編集できるようになりました。

DLP トークンの拡張範囲

電子メールアドレスや IP アドレスなどメッセージにおける PCI、PII、その他の役に立つアイテムを検出でき量に、DLP トークンの範囲に 90 を超える新しいトークンが追加されました。

メッセージを複数のエリアに隔離

メッセージを複数のメッセージエリアに保留できます。各コピーは、互いに独立しており、別々の管理者がアクセスすることができ、それぞれにメッセージエリアの自動有効期限が適用されます。

「Relay-to」書き換えオプション

メッセージが「Relay-to」を使用してメールサーバーへ送信された場合、受信者のドメイン名を修正できます。これはアーカイブの目的で役に立つことがあります。

外部コマンド

顧客、パートナー、システムインテグレータがコードを書いて（または一連の Linux コマンドを使用するだけで）標準の SECURE Email Gateway ではできないメッセージのスキャンを実行できるように、メッセージ処理能力を拡張できます。

たとえば、メッセージに添付する画像を参照するアプリを作成し、二次元バーコードを検出した時には別の処理を実行できます。（すなわち、電子メールアーカイブへの配信と送信、または別の受信者への送信）

メッセージ再処理オプション

検疫済みメッセージは、元のメッセージまたは修正したメッセージにより再処理して、メッセージがどのように再評価されるかを検証することができます。これは特に新しいポリシーを設定する場合に役に立ちます。

デフォルトでは、メッセージは同じポリシールートを使用して処理されますが、別のルートを使用するために上書きすることができます。

アドレスルートと同じポリシールートとのペアリング

メッセージルートは、送信者、受信者、ルールのリストに基づいています。設定が完了すると、定義されたすべての送信者は、定義されたすべての受信者へメールを送信することができ、定義されたルールに沿って評価されます。

この方法では、ポリシーによって、すべての送信者がすべての受信者へ送信できるリスクを冒したくない場合に複数のルートを作成する必要があります。そこで、新しいアドレスルートを設定することになります。これには欠点があります。というのは、ポリシーが大型化し、新しいルールを複数のルートに追加しなければならず、一貫性が失われる可能性が生じるからです。

ただし、分離されていても同じルールセットを共有する複数のルートアドレスを持つポリシールートを作成できます。

アウトバウンドルート	
ルートグループ 1	
営業、マーケティング	*顧客*
ルートグループ 2	
技術	*サプライヤー*
ルール	
マルウェア検出、機密ファイルのチェック、免責事項の追加	

バージョン 3.x では、システムにより、*営業*、*マーケティング*、*エンジニアリング*が「送信者」リストに統合され、*顧客*および*サプライヤー*「受信者」アドレスと照合されます。

これは望ましくない影響をもたらすことがあります。というのは、*エンジニア*が*顧客*へ直接メッセージを送信することができ、それは許可されない場合があるからです。

バージョン 4.5 では、これらリストはルーティンググループと分離して使用されるため、望ましいレベルのセキュリティを実現し、複雑なポリシーの作成に必要なルートの数を減らすことができます。

サーバーの主な改善点

最新版の Gateways は以下をサポートしています。

- バイナリー認証
- AD サーバーからの認証の収集サポート
- LDAP/S および HTTP/S のキー検索法

暗号化された電子メールの使用プロセスがより簡単になります。

ネットワーキングの向上

保護プロトコル

SECURE Email Gateway (SEG)は、FTP および FTPS プロトコルをサポートし、システム構成のバックアップおよびリストアが可能です。

バックアップ／リストアおよびエクスポートのトランザクションログを下記の方法で外部ソースへ転送できます。

- S/FTP FTP over SSH（TCP 22）
- FTPS（暗黙モード） FTP over SSL（TCP 990）
- FTPS（明示モード） FTP over SSL（TCP 21）

また、SEG は、LDAP/S を介したディレクトリサーバー参照もサポートしています。

必須 TLS のサポート

必須 TLS 接続は、定義されたとおり双方向で確立され、ドメイン名および IP アドレスに基づいて定義できます。TLS 無しで送受信しようとするとブロックされます。

便宜的 TLS のサポート拡張

TLS のハンドシェーク中に問題が発生し、接続が確立できないことがあります。便宜的 TLS のサポートを主張しているにも関わらず、繰り返し失敗しているサイトに関して例外リストを示すことができます。