■新機能
●IPsec VPN
・IPsec VPN:IPSecVPNのGCMおよびスイートB暗号のサポートが導入されました。IPsec用のAES-GCMにより、IPsec VPNのパフォーマンスが大幅に向上します。
・リモートアクセスIPsec: IPsecリモートアクセス接続の最大アイドル タイムアウトを6時間に増やしました。
・ルートベースのVPN: ソースNATルールを使用したルートベースのVPN接続の場合、MASQは内部IPヘッダーでxfrm IPアドレスを、外部ヘッダーでWAN IPアドレスを伝送するようになりました。
・IKEv2プロファイル: サイト間IPsec接続用の既定のIKEv2プロファイル (本社(IKEv2)および支社(IKEv2)) を追加して、本社と支社間の改善されたトンネルを提供します。これにより、キーの再生成間隔、デッドピア検出(DPD)の選択、キー ネゴシエーションの再試行など、既存のデフォルトの本社および支社のプロファイルに必要な手動の微調整が不要になります。これは、キー再生成の衝突とDPD関連の問題を排除するのに役立ちます。
・トンネルフラッピング: IPsecトンネルが確立またはダウンしたときに非TCP(例:VoIP、RDP、Skype、Zoom、UDP) 接続がフラッピングしないようにデフォルトを変更しました。新しいデフォルト設定は次のとおりです。
 - vpn conn-remove-tunnel-up: 無効
 - vpn conn-remove-on-failover: 有効
 この変更は新しい構成にのみ適用され、ファームウェアのアップグレードまたは移行後の既存の構成には影響しません。

●認証
・時間ベースのOTP(TOTP)を使用した MFA:
 - 組み込みの「admin」アカウントの MFA サポートと、MFAを使用していないすべての管理者アカウントのアラート通知を追加しました。
 - Web管理コンソールにサインインするためのトークン初期化プロセスと、ユーザー ポータルにサインインする既存のユーザーのためのトークン初期化プロセスを追加しました。
 - Web管理コンソールでMFA設定を見つけて構成しやすくすることで、MFAエクスペリエンスを合理化しました。
 - トークンリカバリ用の既存のOTPシークレットとQRコードを表示する機能を削除しました。失われたトークンは、サインインプロセスを通じて削除し、再初期化する必要があります。
・ユーザー: Active Directoryユーザーの複数のグループメンバーシップの表示が強化されました。Web管理コンソールに、ユーザーが属するすべてのグループが表示されるようになりました。

●証明書
・CSRおよびアップロードされた証明書の秘密鍵をダウンロードする機能を削除しました。そのため、デバイスで生成されたCSRと秘密鍵を外部システムに使用することはできません。オペレーティングシステムに組み込まれているツールなど、他の方法を使用する必要があります。
・さまざまな種類の認証局に関する有用な情報を示しました。
・ローカルに追加された証明書と秘密鍵を含む証明書を簡単に見つけられるようになりました。
・証明書の公開鍵を簡単にコピーまたはダウンロードして確認および確認できるようにしました。

●総合トラブルシューティングレポート(CTR)
・CTRでのログファイルのローテーションを含む、完全なトラブルシューティングログをキャプチャする機能が導入されました。
・バックエンドからCTRを生成する機能が導入されました。
・CTR生成中のタイムアウトとコンソールのフリーズが解消されました。

●ユーザビリティ
・HTTPSリクエストのIPv6Web分類: IPv6アドレスに直接接続するHTTPSリクエストには、「無効な URL」ではなく「IPアドレス」Webカテゴリが含まれるようになりました。これは、TLSポリシーの選択とロギングの両方に影響を与え、IPv6接続を、同等のIPv4接続の処理方法と一致させます。
・Sophos Central: Sophos Centralの資格情報不要の登録が導入されました。
・TLS除外: 新しいドメインをTLS除外リストに追加しました:gotowebinar、ava.expertcity.com、cdn-apple、mzstatic、zoom.us、device.login.microsoftonline.com。
・DDNS: Cloudflare DDNSプロバイダーのサポートが追加されました。
・IPSスイッチ: [侵入防止] > [IPS ポリシー] にグローバル スイッチを追加して、IPS保護をオンまたはオフにします。現在IPSを使用している場合、スイッチは自動的にオンに設定されます。
・インストール ウィザード: 以前のすべてのポートの単一ブリッジ構成ではなく、2ポートブリッジのデフォルトオプションが提供されました。

・DHCPオプション
 - Web管理コンソールでDHCP IPv4オプションとブートサーバーを構成できます。これは、CLIで設定する既存の機能に追加されます。

- デバイスをDHCPサーバーとして設定する場合、DHCPおよび起動オプションを追加して、設定パラメータをDHCPクライアントに提供することもできます。カスタムおよび定義済みのDHCPオプションを追加できます。

・マルチキャスト転送:
- 静的マルチキャスト ルートフォワーディングでの存続可能時間(TTL)値を制御するためのサポートが導入されました。これにより、転送時にTTL値が期限切れになったためにマルチキャストトラフィックがドロップされるのを防ぐことができます。次のCLIコマンドを使用できます: set routing multicast-decrement-ttl
- より多くのOSPFネイバーをサポートするために、デフォルトのマルチキャストグループの制限を250に増やしました。次のCLIコマンドを使用して、マルチキャストグループの制限を変更できます。
・セルラーWAN: セルラーWANのQMIドライバーサポートが追加されました。
・ログ: トラブルシューティングを改善するために、ログファイルの処理とCSCのログ記録が改善されました。
・ゼロデイ保護: クラウドベースの機械学習ファイル分析用の追加のデータセンターの場所が、オーストラリアのシドニーのアジア太平洋地域で利用できるようになりました。
・いくつかの重要なセキュリティ、パフォーマンス、および信頼性の強化が導入されました。

●SD-WAN
・VPNオーケストレーションSD-WANネットワークは、Sophos Centralからすでに利用可能です。複雑なSD-WANオーバーレイネットワークを一元的にオーケストレーションし、プロセスを簡素化できます。 SD-WAN接続グループを参照してください。
・ファイアウォールでXstream SD-WANを提供するようになりました。
- Xstream SD-WANプロファイルは、VDSL、DSL、ケーブル、LTE/セルラー、MPLSなど、複数のWANリンクのルーティング戦略をサポートします。3つ以上のゲートウェイを構成し、最初に使用可能なリンクまたはパフォーマンス基準に基づいてルーティング戦略を指定できます。
- パフォーマンスベースのSLAは、ジッター、遅延、またはパケット損失に基づいて最適なWANリンクを自動的に選択します。SLAは、最高のパフォーマンスまたはカスタムSLA値に基づくことができます。複数のプローブターゲットを使用して、ヘルスチェックを実行できます。
- リンクパフォーマンスがしきい値を下回り、セッションをよりパフォーマンスの高いWANリンクに移行する場合、影響のない再ルーティングにより、アプリケーションセッションが維持されます。
- [診断] > [SD-WAN パフォーマンス] のSD-WAN監視グラフは、すべてのWANリンクの遅延、ジッター、およびパケット損失に関するリアルタイムの洞察を提供します。時間を選択できます。 SD-WANプロファイルのステータスをクリックして、診断に移動することもできます。
- ログには、SD-WANルーティング情報が含まれています。新しいSD-WANログ モジュールを使用すると、SD-WANのルーティングと正常性に固有のログエントリに集中できます。ログエントリには、SD-WANルールIDと、ルート要求と応答方向の名前が含まれます。
- トラブルシューティングを容易にするために、ルールIDとインデックス列をSD-WANプロファイル リストに追加しました。

●Xstream FastPathアクセラレーション
・IPsecアクセラレーション:IPsecトラフィックのXstream FastPathアクセラレーションは、プロセッサのハードウェア暗号化機能を利用して、Xstreamフロープロセッサを介してIPsec VPNトラフィックフローをFastPathに自動的に配置します。これにより、ESPカプセル化と暗号化、カプセル化解除と復号化など、IPsecトンネルに必要なCPU集約型の処理がXstreamフロープロセッサに移され、CPUリソースが解放され、パフォーマンスが向上します。
・IPsecトラフィックのXstream FastPathアクセラレーションは、サイト間（ポリシーベースおよびルートベースのIPsecを含む）とリモートアクセスVPNトラフィックの両方で機能しますが、脆弱な暗号または認証アルゴリズム（DES、3DES、BlowFish、MD5）は機能しません。

●Web
・接続ごとの認証: 明示的プロキシモードでは、Web認証が同じ送信元アドレスからの複数の異なるユーザーを処理できるようになりました。これは、ターミナルサービス、Windowsリモートデスクトップ、または直接アクセスシステムの認証に役立ちます。
・テナント制限: O365のテナント制限機能は、送信HTTPS要求にヘッダーを追加することでユーザーがサインインできるドメインを制限するために使用され、Webポリシーで利用できます。これにより、Microsoft Azure ADは制限を適用できます。これは通常、個人アカウントがデバイスで保護されたネットワークからO365にアクセスするのを制限するために使用されます。
・WebポリシーでX-Forwarded-Forヘッダーにより、送信元IPアドレスをアップストリームでロードバランサーまたはプロキシに渡すことができます。

●VPN
・ユーザー体験
VPNメニューとユーザーインターフェイスは、より直感的になるように再編成されました。
- リモートアクセスとサイト間VPNは、個別の左側のメニュー項目です。
- IPsec、SSL、およびL2TPは、対応する設定に簡単にアクセスできるように、ページ上にIPsecプロファイル、クライアント ダウンロード、およびログへのリンクがあるトップメニュー項目です。

- IPsecポリシーの名前がIPsecプロファイルに変更されました。これは、[システム] > [プロファイル] の下にあります。
- リモートアクセスSSL VPNの新しいアシスタントにより、合理化され、簡単な構成が可能になります。
- クライアントレスポリシー、ブックマーク、およびブックマークグループは、クライアントレスSSL VPNポリシーに統合されました。
- サイト間VPNでAmazon VPCを使用すると、VPC構成ファイルまたはAWSセキュリティ資格情報をインポートするオプションを使用して、Amazon Web Services VPCトンネルを簡単にセットアップできます。
・機能強化
リモートアクセスIPSecVPNのカスタムポリシーサポートは、デフォルトのリモートアクセスIPSecポリシーでの潜在的なPCIコンプライアンスの問題に対処します。
- 4時間ごとにMFAプロンプトが表示されないように、カスタムキー再生成時間を構成する機能が追加されました。
- アイドルタイムアウトを10分から6時間に延長するオプションを追加しました。
・ルートベースVPN(RBVPN)
- スタティックマルチキャストルートのサポートが追加されました。
- XFRMインターフェイスの自動構成と選択したホストのルート管理を使用して、ルートベースのVPNのトラフィックセレクターを指定できます。設定されたローカルアドレスとリモートアドレスのペアに一致するトラフィックだけがトンネルに入ります。
・IPsecのGCM およびSuite-B暗号スイートのサポート
-IPSec用のAES-GCMにより、IPsec VPNのパフォーマンスが大幅に向上します。
・SSL VPN
- OpenVPNとOpenSSLをアップグレードしました。
- SSL VPNトンネルでのデフォルトのTLS 1.3サポート。
- AES-NIパス対応。
- GCM暗号化のサポート。
- マルチインスタンスサポートの追加により、SSL VPNキャパシティの大幅なパフォーマンス強化。
- 従来のSSL VPNクライアントは、2022年1月31日にサポートが終了しました。ユーザーポータルでダウンロードすることはできなくなりました。ユーザーは代わりに Sophos Connect クライアントをダウンロードできます。
- ファイアウォール上および外部RADIUSサーバーからのリモートアクセスSSL VPNユーザー用の静的IPアドレスリースが導入されました。 デバイスは、リモートアクセスSSL VPNユーザーを静的IPアドレスにマップするようになり、ユーザーの監視と可視性、およびユーザーを追跡する機能が強化されました。
・VPNロギング
ログビューアでVPNを選択できるため、リモートアクセスやサイト間のIPSecおよびSSL VPNトンネルのVPN接続を簡単に監視およびトラブルシューティングできます。さらに、IPsecロギングメッセージが強化され、詳細がより明確になりました。
- AWS VPC
この新機能により、オンプレミスファイアウォールをAWSネットワークインフラストラクチャに簡単に接続できます。AWSからVPC設定XMLファイルをインポートして、関連するルーティングおよびIPSecポリシーを含め、デバイスでのトンネル設定を自動化できるようになりました。サイト間 > AWS VPCでAWS VPC接続をインポート、監視、および管理できます。

■機能強化
・スパム対策エンジン: スパム対策スキャンのために、電子メール保護は、スパム対策エンジンの代わりにSophos Anti-Spam Interface (SASI)を使用するようになりました。
・カーネルダンプ: ファイアウォールは、カーネルクラッシュが発生したときにカーネルダンプ レポートを生成し、改善された根本原因の分析とトラブルシューティングを可能にします。
・マルウェアエンジン: マルウェアスキャンエンジンと関連コンポーネントを完全な64ビット操作にアップグレードして、最適なパフォーマンスと将来のサポートを確保します。
- Avira: 2番目のマルウェアスキャンエンジンのベンダーであるAviraは、2022年12月31日以降、現在の32ビット形式で検出アップデートを提供しません。
- デュアルスキャンモードまたはAviraをプライマリエンジンとして使用しているお客様は、できるだけ早く19.0 MR1にアップグレードすることをお勧めします。
- アップグレードできない場合は、電子メールおよびWebマルウェアスキャン用のSophosエンジンのみに切り替えることをお勧めします。
- Sophosエンジン: Sophosエンジンのみを使用しているお客様は影響を受けません。
・電子メール: 検疫リリースページで、スパム電子メールを誤検出として報告する機能が追加されました。
・DHCP: Web管理コンソールにDHCP IPv4オプションとブートサーバー構成を追加しました。
・グローバルIPSスイッチ: [侵入防止] > [IPS ポリシー] にグローバルスイッチを追加して、IPSをオンまたはオフにします。19.0に移行すると、以前の構成に基づいてスイッチが自動的に設定されます。たとえば、IPSを使用している場合は、オンに設定されています。
・多要素認証: デフォルトの管理者アカウントのWeb管理コンソールにサインインするためにワンタイムパスワードを使用するMFAを要求するオプションが追加されました。これにより、セキュリティ、ワークフロー、および使いやすさが向上します。

・認証: 何千人ものユーザーによる高負荷の状況を緩和する、認証パフォーマンスの向上。
・Synchronized Security: 正当なトラフィックを妨害するスプーフィングされたMACアドレスの使用を防ぐためのラテラルムーブメント プロテクションの更新。
・ゼロデイ保護: クラウドベースの機械学習ファイル分析用の追加のデータセンターの場所が、オーストラリアのシドニーにあるアジア太平洋地域で利用できます。これにより、日本、ドイツ、英国、および米国の既存のデータセンターの場所が追加されます。
・ログの抑制: モジュール内で繰り返されるファイアウォールログは、繰り返し回数とともに1つのイベントとして表示されます。これにより、トラブルシューティングが改善され、ロギングのスケーラビリティとストレージ効率が最適化されます。
・ユーザー体験
 - デバイスと管理 ID: デバイスのホスト名がブラウザタブに表示され、アクティブなユーザーIDがWeb管理コンソールの右上隅に表示されるようになりました。これにより、複数のファイアウォールと管理者アカウントの管理が容易になります。
 - 検索機能:
  - グローバル検索: オートコンプリート機能を備えた新しいインテリジェント検索ボックスがメインメニューの上に表示され、ファイアウォール内の任意のページまたは機能を見つけることができます。
  - オブジェクト検索: ネットワークオブジェクトまたはサービスを検索して、ルールとポリシーに含めることができます。これには、ラベルまたは値で検索できるフリーテキスト検索オプションが含まれており、ユーザーエクスペリエンスが向上します。
 - フローモニター: フローモニターのユーザーインターフェイスとレイアウトを強化して、ヘッダーを永続化し、水平スクロールをなくしました。

■解決された問題
●API フレームワーク
- Webadminの複数の認証後SQLi脆弱性を解決しました (CVE-2022-1807)。
- i18n構成と実際の構成名のマッピングの問題。
- 事前認証RCE(CVE-2022-1040)を修正しました。

●CM
- シリアル番号の可視性について修正をしました。
- バックアップ名に [] が含まれている場合、バックアップは生成されません。
- ユーザーポータルのホストインジェクションについて修正をしました。

●CSC
- 1つのファイアウォールルールに多数のユーザーが含まれていると、システムの起動に失敗します。
- 定義名に特殊文字が含まれている場合、分割ネットワークに到達できませんでした。

●DDNS
- DDNSは一部の新しいgTLDには適用されません。
- DynDNS IPアドレスの生成中に不明なエラーが発生しました。

●IPS
- IPSサービスがダウンすることについて修正しました。
- IPSがコア ダンプで再起動していました。
- ATPパターンの更新によるSnortメモリの増加。
- 移行後にIPSポリシー画面に誤った署名日が表示される。
- IPSシグネチャをロードするためのアイコンの配置が正しくありません。

●IPS-DAQ
- DAQが原因でIPSサービスが開始されませんでした。
- Snortソフトロックアップとデバイスの再起動。

●IPS-DAQ-NSE
- ファイアウォールを介してWebサーバーにアクセスできません。SSL/TLSインスペクションエラーが表示されました:「TLS 内部エラーが原因でドロップされました」。
- 一部のTLSフローは、特定のサービスプロバイダーによって遅延します。
- SSL/TLSインスペクションがオンの場合、VeeamエージェントはVeeamサーバーに接続できません。
- TLSエンジンエラーのため、接続が切断されました。
- SSL2.0クライアントのhelloで問題を引き起こすDPI。
- do-not-decryptモードでSSL/TLSインスペクションが有効になっていると、大きなファイルをアップロードできません。

●IPsec
- Strongswanの「ANY」オブジェクトは、どのIPアドレスにも相当しません。

- .scxファイルが無効なため、IPsecリモートアクセスを使用して接続できません。
- Sophos Central SD-WANオーケストレーションを介してプッシュされたVPNで一定のIPSecフラッピングが発生する。
- ルートの優先順位がVPNに設定され、リモートサブネットが「任意」に設定されている場合、システム生成トラフィックは影響を受けます。
- VPN接続を使用してエクスポートされた構成には、暗号化コンポーネントが表示されません。
- メモリは20～25日で90%に増加します。
- 対応するルートベースのVPNトンネルが接続されて確立されている場合でも、XFRMインターフェイスがオフとして表示されます。
- SSHサーバーへのクライアントレスブックマークは、サイト間IPSec接続を介して接続しません。
- フェールオーバーグループを非アクティブ化できません。
- PPPoEの再接続後、IPsecトンネルが再接続されません。
- Apple iOSIPSecVPNクライアントの構成の問題。
- サービスが再起動するまでIPSecトンネルが立ち上がらない。
- トラフィックが正しくないインターフェイスを通過していたため、トンネルが確立されませんでした。
- IPSecフェールオーバーが機能せず、フェールオーバーグループを非アクティブ化してから再アクティブ化し、トンネルを起動する必要がありました。
- adapt_children_job.cの実行でCharonがクラッシュします。
- 認証タイプがSophos Connectクライアントの証明書の場合、ユーザーポータルからVPN iOSプロファイルをダウンロードできません。
- Sophos Connectクライアントでアイドル設定がオンになっていると、子SAが切断されました。
- ルートベースのIPSecVPNでのxfrmパケット損失。
- 組織単位(OU)が存在する場合は変更できません。
- すべてのIPSecトンネルがダウンし、無効なゲートウェイの検出が停止し、30分後にゲートウェイが見つかりませんでした。
- 接続リストの2ページ目にあるIPSec接続を削除できません。
- 証明書で構成されたIPSec接続が接続されません。
- リモートアクセスIPSecVPNの構成時にエラーが表示されます。
- カーネルパニックの問題。
- ESPシーケンス番号が一致しません。
- VPNトンネルの構成を更新しているときに、Web管理コンソールにエラーが表示されます。
- AES256GMACを使用すると、IPsecプロファイルで無効な構成が表示される場合があります。
- リモートアクセスIPSecのWeb管理コンソールで説明が必要です。

●ロギングフレームワーク (Central reporting)
- 過去1時間のレポートがレポートジェネレーターに読み込まれませんでした。

●SD-WANルーティング
- SD-WANルーティングを使用するルートベースVPNのVPNゾーンのキャプチャをオフにできません。
- VPNゾーンでキャプチャをオフにすることは、SD-WANルーティングを使用するRBVPNには適していません。
- ping: sendto: ネットワークがポリシールートの一部である場合、操作は許可されません。
- SD-WANルートポリシーの更新が失敗します。
- SD-WAN FTPプロキシトラフィックが透過プロキシで機能しません。
- TFTPトラフィックはSD-WANルーティングに従いません。

●SNMP
- MIBファイルのエントリが重複しています。
- netsnmp_add_varbind_to_cacheでのSNMPDクラッシュ。

●SSL VPN
- SSL VPNサイト間サーバー接続ファイルがダウンロードされません。
- リモートユーザーと接続ユーザーのカウントが正しくありません。
- SSL VPNグローバル設定を更新した後、SSL VPNポリシーからSecurityHeartbeat_over_VPNが削除されます。
- CVE: 2022-0547 openvpn遅延認証の脆弱性。
- バックアップが復元された後、サイト間およびリモートアクセスSSL VPNが機能しません。
- ダッシュボードにリモートユーザーが表示されません。
- OpenVPN 2.3.6のCVE-2020-15078パッチ。

●UIフレームワーク
- Web管理コンソールにアクセスできない場合があります。

●Up2Dateクライアント
- ファームウェアのダウングレード後のSASIパターンの表面的な問題。

●VFP-ファイアウォール
- カーネルパニック: ffff88036e000000 でカーネルページング要求を処理できません。
- ポートがLAGに追加されていません。
- ファイアウォールアクセラレーションがオンになっていると、ICMPがタイムアウトします。

●WAF
- WAFルールに複数のドメインがリストされている場合、WAFはページを適切なドメインにリダイレクトしません。
- Subject Alternative Name (SAN)がドメインの一部ではないという警告。
- Apacheを2.4.53+にアップグレードしました。

●Web
- ユーザーID3ではない管理ユーザーのOTPをオンにすることはできません。
- 多要素認証によって保護されていない管理者アカウントの［ユーザー］ページのアラート メッセージに、説明が必要な数字が表示されます。
- SSL/TLSルールはWeb管理コンソールに表示されません。
- connect_to_serverでskein segfaultが発生しました。
- ユーザーが多数のグループのメンバーである場合、ユーザーはKerberosで認証されません。
- 空白のconfファイルが原因で、Snortがsegfaultでクラッシュします。
- SSL/TLSルールはWeb管理コンソールに表示されません。
- SSL/TLSインスペクションがSMTPで機能しませんでした。
- Awarrenhttpがダウンしました。
- Webクォータをリセットできません。
- ダイレクトプロキシを使用してcPanelサーバーにサインインできません。
- ［ユーザーの追加］をクリックすると、Sophos Centralがファイアウォールコンソールから管理者をサインアウトします。
- 認証 > ユーザーのアラートに表示される、MFAによって保護されていない管理者アカウントの数を更新しました。

●WebInSnort
- libnsg_tcphold_preprocでのIPSセグメンテーション違反。
- 8080上の内部サーバーへのHTTPおよびHTTPSトラフィックは、IPS tcpholdによってドロップされます。
- IPS障害により、ユーザーのピーク時にユーザーが切断されます。
- カスタムアプリケーション制御ポリシーが適用されたときにWebサイトがブロックされました。
- SSL VPNを介して、LANネットワークでホストされているMicrosoft TFS (Team Foundation Server)にアクセスできません。
- DPIエンジンでカスタムブロックページを使用してユーザー名を表示できません。
- DPIエンジンとアプリケーション制御でGoogle Webサイトが開かない。

●アプリケーションフィルタポリシー
- いずれかのルールが［特性］で［クラウド アプリケーション］を選択した場合、アプリケーションフィルタポリシーをインポートすると、ルールとそのアプリケーションのリストが変更されました。

●インターフェイス管理
- Networkdサービスが停止しているため、ネットワークが停止しています。
- 別のアプライアンスにバックアップを復元できませんでした。

●キャプティブポータル
- サインインメッセージとサインアウトオプションが、カスタムキャプティブポータルで表示されません。

●クライアントレスアクセス
- クライアントレスアクセスで Windowsキーを押した後、キーが認識されません。

●ゲートウェイ管理
- CLIコマンドのタイプミスをsession-persistenceに修正しました。

●コアユーティリティ
- OpenSSL(CVE-2022-1292)を介したWeb管理コンソールでの認証後のシェルインジェクションを解決しました。
- セキュリティ監査レポート(SAR)との不一致。
- OpenSSL DoS脆弱性(CVE-2022-0778)を修正しました。

●コンフィグ移行フレームワーク
- ディスク使用率が高い。

●サポートアクセス
- バックアップ/リストア中に重複したサポートアクセスIDが作成されました。

●スタティックルーティング
- API経由でスタティックルートを削除する場合の必須設定要件。

●セキュリティ
- 複数のXSS脆弱性(CVE-2021-25267)を解決しました。
- 会社名による複数のXSS脆弱性を解決しました(CVE-2021-25268)。

●セキュリティハートビート
- delay-missing-heartbeat-detectionのために、補助デバイスがプライマリHAデバイスと同期されていません。

●ネットワークユーティリティ
- Azureで実行されているファイアウォールの断続的なWAN接続の問題。
- [診断] > [ツール] > [ルート ルックアップ] を修正しました。

●バックアップリストア
- キーが重複しているため、バックアップを復元できませんでした。
- tbl構成の問題により、バックアップをインポートできません。
- 一意のインデックスが原因で、ファームウェアのアップグレードが失敗します。
- VLANインターフェイスを削除できません。

●ファームウェア管理
- ファイル名にスペースが含まれていると、ファームウェアの更新に失敗します。

●ファイアウォール
- 2ページ目で作成したゾーンを削除すると、ゾーンのタブが空になります。
- カーネルパニック - カーネルNULLポインター"ip_route_me_harder"を処理できません。
- デバイスのフリーズの問題 (0010:queued_spin_lock_slowpath+0x14b/0x170)。
- ファイアウォールのポリシーテストで正しい結果が表示されません。
- httperf接続レートテスト中にFP fw_fp_track_connおよびfw_fp_reclaim_connエラーが表示される -（フロー 2)。
- ファイアウォールIDはID列に表示されません。
- Web管理コンソールへのサインイン試行が拒否された場合のログには、宛先ポートがカスタムポートとして表示されます。
- バックアップを復元した後、ファイアウォールがフェイルセーフモードになりました。
- 複数のローカルACLルールが設定されていると、バックアップの復元とファームウェアの移行が失敗します。
- 自動再起動 0010:queued_spin_lock_slowpath+0x148/0x170.
- ファイアウォールルールグループが重複しています。
- ファイアウォールが夏時間を正しく反映していません。

●メール
- 返されるヒットが多すぎる場合のSASI検出の問題。
- スマートホスト認証に失敗しました。パスワードの解読の問題。
- エンティティ"MtaBlockedSenders"のインポートが失敗します。
- UTF-8文字に関するエラー。
- SPXで暗号化された電子メール本文の情報がありません。
- SPXが適用されると、電子メールの添付ファイルが取り除かれます。
- MTAは完全な証明書チェーンを提供しません。
- Web管理コンソールの言語が繁体字中国語または簡体字中国語に設定されている場合、通知テストメールの件名が正しくエンコードされません。
- 検疫ダイジェストは、構成された時刻より6分早く電子メールを送信します。
- ブラジルの文字によるメール配信の問題。
- 115wアプライアンスで構成されたPOP3スキャンルールを使用してOutlookクライアントにアクセスすると、証明書関連のエラーが発生します。
- 隔離された電子メールを削除できません。
- SPXで暗号化された電子メールの本文で韓国語が壊れています。
- 外部電子メール通知サーバーのパスワードに特殊文字を使用することはできません。
- APIを使用してSMTP TLS設定の証明書を更新できません。
- メールスキャナによる高いCPU使用率。
- 不在、配信不能レポート、バウンスメールに対してDKIM署名が行われない。
- メールログの別のフィルターに同じメールが表示されます。

- 外部メールサーバーの通知設定の誤解を招くメッセージ。
- 本文に「credit card」という用語が含まれるCCLの誤検出。
- DKIM検証は送信メールに適用され、メールは隔離されていました。
- メールクライアントで設定されたYahooメールアカウントがIMAPSスキャンで機能していませんでした。
- ポート8094ではHSTSは提供されません。
- メールが受信されず、次のエラーメッセージが表示されます: smtp_check_forward_reply: コマンドなしで応答が到着しました。
- apxxファイルでのAviraエンジンエラー。
- SMTPスキャンが有効になっている場合、受信メールは配信されません。
- 文字化けして受信したレポート。

●メール、FQDN
- 通知設定でlx63.hoststar.hostingをメールサーバーに追加できません。

●レポート
- 大量のデータが原因でレポートデータベースがデッドロックし、システムが不安定になる。
- テーブルエントリが重複しているため、アップグレード中に構成が移行されません。
- ログビューアが/var/eventlogs/から結果を返していませんでした。
- レポートの生成は2021年1月1日以降停止しました。
- XSSペイロードを持つユーザー名を持つユーザーが存在する場合、最終アクセス時刻は生成されません。

●ローカライズ
- ドイツのメニューが壊れています。

●ロギング
- ログビューアからIPSポリシーへのリダイレクトに関する問題。

●ロギングフレームワーク
- ライブ接続の単位が正しくありません。
- active.dbが破損したときに、ログビューアーが動作しなくなった。
- ライブ接続ページが読み込まれませんでした。
- Sentryがcrformatter_free_dataのコアダンプを報告しました。

●ワイヤレス
- 時間ベースのSSIDが設定されている場合、再起動後にデバイスが応答しなくなります。
- ワイヤレスAPは、別のゾーンでIPアドレスをリースできません。
- 内蔵ワイヤレスがLocalWiFiのブロードキャストを停止します。
- 別のゾーンのWi-Fi SSIDに接続されているホストのインバウンドトラフィックは、ファイアウォールルールIDOによってドロップされ、アウトバウンドトラフィックが遅くなる可能性があります。
- 高速移行が有効になっていると、レガシーAPローミング キーの復号化が失敗します。

●集中管理
- Garnerサービスはビジー状態のままでした。

●証明書
- CA証明書をアップロードできません。
- CAはpfxファイルでは使用できませんが、CAアップロードオペコードが呼び出されます。

●認証
- キャプティブポータルでのユーザー認証の問題。
- RADIUSサーバーの共有シークレットの最大長。
- パスワードを変更すると、ユーザーはSSL VPNプロファイルのグループ外に配置されます。
- 診断のユーザーグラフの平均ライブユーザーの値は、浮動小数点であってはなりません。
- [認証] > [ユーザー] に [ステータス] 列が表示されません。
- CAAクライアントは、「管理者が切断しました」というメッセージをユーザーに繰り返し送信します。
- 匿名サインインによるLDAP認証が機能していませんでした。
- デバイスは、アプライアンスの再起動後、ポート6677でADサーバーへの要求を開始していませんでした。
- 一度パスワードを受け取ったゲストユーザーは、後でSMS経由でパスワードを取得できませんでした。
- 有効期限が切れたゲストユーザーは、空白のパスワードが記載されたSMSを受け取りました。
- デバイスからリモートユーザーをエクスポートできません。
- csdサービスが停止状態です。
- OTP設定では、グループを組織単位(OU)として追加できません。
- Sophos Centralのグループに移動されたファイアウォールはグループに追加されますが、「エラーには注意が必要です」に変わります。

- ライブユーザーに表示される古いユーザー。