■新機能
SSL VPNおよびWAFポート：SSL VPNトラフィックは、WAFと同じポートおよびプロトコル（例：TCPポート443）を共有している場合、WAFルール用に構成されたホスト型IPアドレスを通過しません。詳細については、VPN設定を参照してください。
同時IPsecトンネル：すべてのハードウェアアプライアンスで同時IPsec VPNトンネルが50%以上増加しました。詳細については、アドバイザリを参照してください。

IPsecプロビジョニングファイル：IPsecリモートアクセスVPNのプロビジョニングファイルサポートを提供しました。ユーザーは、SophosConnectクライアントのバージョン2.1をインストールする必要があります。

SD-WAN：AzureセキュアSD-WANとXGファイアウォールの統合
認証：AzureADとXGファイアウォールの統合
合理化されたフォームと複数のSAN：CSRと証明書を作成するためのフォームを更新して、DNS名とIPアドレスを使用してサブジェクト代替名をより柔軟に追加できるようにし、不要な入力を削除しました。
セキュリティの強化：CSRおよびローカルで署名された証明書の秘密鍵資料のダウンロードを防止することにより、セキュリティの懸念に対処しました。
アップロード、ダウンロード、インポート：CSRの取得を可能にする新しいダイアログボックス、および署名証明書（CA）とリーフ証明書の証明書のアップロードを提供しました。ボックスを使用すると、DER、PKCS、およびPEMファイル転送に加えて、PEM形式の証明書をコピーして貼り付けることができます。
ローカル署名された証明書：自己署名証明書は、ローカル署名された証明書に名前が変更されました。
ダウンロード形式：CSRと証明書は、それぞれ.csrファイルと.crtファイルとしてダウンロードできます。
tar.gzファイルとしてダウンロードできなくなりました。
CAを使用した証明書：CAを使用して証明書をインポートするときに同じ名前を使用して、証明書のCAをCAリストに追加するオプションを提供しました。
ワークフロー：証明書管理をより直感的にするためのワークフローとリストの改善。
ハートビートの欠落に関する通知：シャットダウン、再起動、スリープ、休止状態、ネットワーク切り替えなどの意図的なアクションの後に、エンドポイントがハートビートの欠落状態になることに関する通知を遅延または抑制するために、CLIにシステムコマンドを提供しました。詳細については、CLIヘルプを参照してください。
ソフォスセントラルを介したアップグレード：XGシリーズファイアウォール18.0MR3以降のソフォスセントラルからのファームウェアアップグレードをスケジュールできます。
DPIモード：DPIモードでのTLSトラフィックのネットワークパフォーマンスの向上が、VCRのすべてのフォームファクタで利用できるようになりました。
解決されたFragAttackの脆弱性：XGシリーズデスクトップシリーズアプライアンスのすべての内部およびアドオンWi-FiモジュールのWi-Fi仕様で最近発見されたこれらの脆弱性を解決しました。他のすべての更新は、このアドバイザリで概説されているように続きます。
VPNトンネルロギング：VPNトンネルフラップイベントとIPsecIKEv2キー再生成のロギングが改善されました。

■解決された問題
●SNMP
- 2つのSNMPコミュニティが同じ送信元IPアドレスで構成されている場合の移行の問題。
- SNMPに誤ったライセンスの詳細が表示されます。
- SNMPDのメモリ使用量は、失敗するまで増加します。

●Sophos Connect client
- macOSおよびWindowsのユーザーポータルからSophosConnectClientをダウンロードできません。
- 事前共有キーの長さが128文字以上の場合、接続に失敗します。

●VPN
IPsecリモートアクセスおよびL2TPの事前共有キーは、暗号化された値を示します。

●認証
- SATCユーザーは散発的に認証されていません。
- [監視と分析]> [現在のアクティビティ]でリモートユーザーの詳細が欠落しています。

●ブリッジ
- ブリッジインターフェイスのVLANは、デバイスアクセスのZoneIDに従いません。

●診断
- システムグラフ：日本語では、1か月のメモリ使用量が見出しに1週間表示されます。

●メール
- DKIM検証をオンにできません。
- デフォルト設定でも、ユーザーポータルの隔離ページにDKIM確認メールを表示できません。

- レガシーモード：スパムチェック例外を削除できません。
- SSL / TLSが選択されている場合でも、通知設定で証明書の選択は必須ではありません。
- 例外を保存して再度開く場合は、電子メール例外の送信元/ホストフィールドを空にします。
- Exim4.94でDKIM署名が壊れています。

●ファイアウォール
- Awarrenhttpプロキシは、ポート443でのインバウンド接続をブロックします。
- ファイアウォールルールのポリシーテストで正しい結果が表示されません。
- DNATトラフィックをFQDN（動的IPアドレス）で負荷分散すると、ファイアウォールが再起動します。
- 同じ発信元から同じ宛先に同時に複数のパケットが送信されると、最初のパケットはドロップされます。
- FastPathがオンになっている場合、ブリッジ上のVLANはトラフィックを許可しません。
- CLIは、カスタムSNATルールに存在しないPortB4を表示します。
- ネットワークホストがホストグループに追加された場合、IPv6ホストグループはIPv6アドレスの一致を示しません。
- 未使用ステータスのファイアウォールルールフィルターが機能しません。
- ユーザーがサインアウトすると、イベントはネットワークベースのルールを使用した接続のconntrackのファイアウォールルールフィールドをクリアし、パケットがドロップします。

●IPS、DAQ、NSE
- SSL / TLSルールが適用される場合、証明書要求メッセージはクライアントに渡されません。

●IPSエンジン
- バージョン17.5から18.0に移行した後、WAFのIPSログには、パブリックIPアドレスではなく送信元IPアドレスとしてLANインターフェイスのIPアドレスが表示されます。

●IPSec
- IPsecトンネルのアップまたはダウン：接続が終了すると、いくつかの電子メール通知が送信されます。

●ネットワークユーティリティ
- pingがIPv6に設定されている場合、Web管理コンソールでIPv4に切り替わりますが、IPv6インターフェイスが表示されます。

●ポリシールーティング
- Nameにアポストロフィ（'）が付いている場合、ポリシールートを作成できません。
- RTPストリームはVPNではなくWANに転送されます。
- 着信VPNトラフィックはSD-WANポリシールートに従いません。

●レポーティング
- ファームウェアのアップグレード後に統計を報告するユーザーはいません。
- ブロックされたWebレポートは、2020年10月には表示されません。
- 時間フィルターは、ログビューアーに空白または不正確な出力を表示します。
- カスタムロゴは、2ページ目以降のエグゼクティブレポートに広がります。

●SSLVPN
- SSL VPNは切断されますが、ステータスは接続済みであることを示しています。
- 許可されたLANネットワークの更新後にユーザーが再接続しても、ユーザー構成ファイルは更新されません。
- リモートアクセスSSLVPNの場合、push_replyパケットには、更新された許可されたLANネットワークは含まれません。

●UIフレームワーク
- メモリの問題が原因で、Web管理コンソールとユーザーポータルページが読み込まれない場合があります。
- ラップバッファをオンにしてパケットキャプチャページを更新するときのページロードの問題。
- ユーザーは、AppleiOS用のIPsecVPNクライアントの構成で[インストール]をクリックすると、ユーザーポータルからサインアウトします。
- サードパーティのスキャンで誤検知が報告されました。

●WAF
- syslog.logのWAFルールIDの解決が正しくありません。
- ポートをWAFとして使用する場合、SSLVPNは機能しません。
- WAFサブスクリプションが存在する場合でもWAFライセンスの警告。

●日時とタイムゾーン
- バックアップ構成の復元後に/ etc / timezoneが更新されないため、レポートのタイムゾーンが正しくありません。

●インターフェース管理
- DMZおよびLANインターフェースにエイリアスを追加できません。タイムアウトエラーを表示します。

●QOS
- Noneという名前のトラフィックシェーピングポリシーがある場合、ユーザーを追加または編集できません。