統合脅威管理（UTM）スループットパフォーマンスの比較

WatchGuard Firebox M270

Cisco Meraki MX84

Fortinet FortiGate 100E

SonicWall NSA 2650

Sophos XG 210

2018年８月2日

DR180622E

Miercom.com

www.miercom.com

目次

概要 3

はじめに 5

評価対象製品 5

評価方法 8

テストツール 8

テストベッド図 9

パフォーマンステスト 11

ストートレスの*UDP 1518*バイトおよび*UDP IMIX*のスループット 11

ステートフルスループット（HTTP/HTTPS） 12

Miercomについて 15

お客様による利用と評価 15

レポートの使用について 15

概要

統合脅威管理（UTM）アプライアンスは、ルーティング、ファイアウォール、不正侵入防御、アンチウィルス、仮想プライベートネットワーク（VPN）など、中堅・中小企業のネットワーク保護を提供する統合セキュリティ製品です。これらのデバイスには次世代ファイアウォールとセキュアWebゲートウェイの機能が備わっていますが、増え続ける大量のトラフィック処理の必要性により、パフォーマンスは低下しています。さまざまなUTM製品のパフォーマンスを評価することによって、処理のメリットとデメリットを客観的に示し、それを基に自社製品を最適化することができます

Miercomは、WatchGuard Technologies, Inc.の依頼により、同社のFirebox M270のパフォーマンスを同レベルのいくつかの最新UTM製品と比較する、公平なパフォーマンス比較を実施しました。比較対象にしたUTM製品は、Cisco Meraki MX84、Fortinet FortiGate 100E、SonicWall NSA 2650およびSophos XG 210です。すべての製品を、さまざまなプロトコルでトラフィック負荷が増大する状況で稼働させ、ネットワークパフォーマンスへの影響を評価しました。このレポートのための競合他社の機器選定には、ラックマウント型アプライアンスで、標準価格（MSRP）がFirebox M270と同等レベルのものを選択しています。実際には、それぞれの評価について、WatchGuard Firebox M370と同じ価格帯の競合製品のモデルを含める必要がありました。

ファイアウォール、付加的なセキュリティ機能、フルUTMモードのそれぞれのシナリオを使用して製品比較を実施しました。ファイアウォールパフォーマンスとしては、トランスポートとアプリケーションのネットワークレイヤのトラフィックを測定しました。その後、個別にセキュリティ機能を有効にし、HTTPおよびHTTPSでの負荷におけるパフォーマンスへの影響を評価しました。最後に、HTTPおよびHTTPSですべてのセキュリティ機能（ファイアウォール、不正侵入防御、アンチウィルスおよびアプリケーション制御）を有効にしました。

M270のパフォーマンスのテスト結果の注目すべき点

- 現実的なIMIX UDPでのパフォーマンスの最高は1.5 Gbps、1518バイトフレームでの最高は4.7 Gbps
- UTM HTTPのスループットの最高値は1.2 Gbpsで、他のベンダーを48%以上凌駕
- 暗号化UTMスループットでは661 Mbpsと非常に高く、最も近い競合他社製品を11%上回る

当社のテスト結果によると、WatchGuard Firebox M270のパフォーマンスは非常に優れており、さまざまなファイアウォール機能を有効にしたステートレスおよびステートフルのトラフィックスループットシナリオにおいて、競合他社よりも高いパフォーマンスを実証しています。セキュリティ機能を有効にしたときのパフォーマンスの高さにより、*Miercom* の *Performance Verified* 認定を授与します。

Robert Smithers

CEO

Miercom

はじめに

統合脅威管理（UTM）デバイスは、発展中のネットワークエッジセキュリティプラットフォームであり、1台のアプライアンスの中に複数のセキュリティ機能が統合されています。このレポートのためにテストされたすべてのデバイスは、次のセキュリティ機能に対応し、これらの機能が統合されています。

セキュリティ機能	略語	説明
ファイアウォール	FW	トラフィックフローを制御・フィルタリングし、比較的低レベルの防護壁を提供することにより、信頼されている内部ネットワークを、セキュアでない外部ネットワーク（インターネットなど）から保護します。
不正侵入防御	IPS	ネットワーク全体を監視し、既知の脅威のシグネチャ、統計的異常、またはステートフルプロトコル分析に基づいて悪質な動作がないかどうか調べます。悪意のあるパケットや不審なパケットが検出された場合、それらが識別され、ログに記録され、レポートされた上で、IPSの設定によっては、内部ネットワークへのアクセスを自動的にブロックします。
アプリケーション制御	AppCtrl	どのアプリケーションのトラフィックがUTMを通過可能であるかを（通常は双方向）制限または制御することにより、セキュリティとリソース（ネットワーク帯域幅、サーバーなど）に関するポリシーを適用します。セキュリティ面でのアプリケーション制御の目的は、感染、攻撃、および悪意あるコンテンツを抑制することです。
Hypertext Transfer Protocolプロキシ/アンチウィルス	HTTP Proxy/AV	セキュリティアプライアンスは、HTTPトラフィックのためのプロキシです。クライアントはここでget要求を発行し、取り出されたファイルはセキュリティアプライアンスのメモリーのバッファに入れられます。ファイルはその後アンチウィルスエンジンによりウィルスがないかをスキャンされ、悪意あるコンテンツが含まれるパケットが削除されます。プロキシベースのウィルスおよびコンテンツのスキャンは、クライアント/サーバー間のトラフィックのストリームベースのインスペクションよりも安全性が高く、正確な方法です。プロキシ/AVのスキャンは、データ転送のハンドシェーク中に実行されます。
Hypertext Transfer Protocol Secure	HTTPS	セキュリティデバイスは、セキュアソケットレイヤ（SSL）の暗号化通信の接続要求に応答した後、HTTP/AVの処理と同様に、悪意あるコンテンツを含むパケットをアクティブにスキャンしてブロックします。HTTPSの暗号化/復号化プロセスはセキュリティデバイスに相当な負荷をかけ、それはデバイスの全体的なスループットに直接影響を与えます。
統合脅威管理（UTM）	UTM	あらゆるセキュリティ機能が含まれ、複数の機能が単体のセキュリティデバイスによって実行されます。通常これらの機能に含まれるのは、ファイアウォール、IPS、AV、VPN（仮想プライベートネットワークの制御）、コンテンツフィルタリング、および情報漏えい防止です。

セキュリティ機能は重要なものですが、ネットワークパフォーマンスにとっては負荷となります。このレポートでは、それぞれのUTMデバイスについて、そのセキュリティ機能がスループットに与える影響を検証していきます。セキュリティ機能がパフォーマンスに及ぼす影響が分かれば、IT 部門が、数ある類似したネットワークセキュリティ製品の中からそれぞれの企業に最も適したものを選ぶのにも役立ちます。

評価対象製品

製品	ファームウェアのバージョン
WatchGuard Firebox M270	ビルド:12.2.B563533（ベータ版）
Fortinet FortiGate 100E	5.6.4 B1575
Meraki MX84	13.28
SonicWall NSA 2650	6.5.1.1-42n
Sophos XG 210	SFOS 17.0.0 GA MR-8

WatchGuard Firebox M270

*Firebox M270*は、WatchGuardのFireboxシリーズの最新モデルです。これは、8つの1-GEポートを備え、中堅・中小企業にエンタープライズグレードのセキュリティを提供します。ファイアウォールスループットは最高5 Gbpsです。

このモデルでは、Intel Quick Assist Technology（Intel QAT）を備えた最新世代のIntel Atomプロセッサを使用し、ハイパフォーマンスのハードウェアベースセキュリティ高速化を実現します。HTTPSコンテンツの検査や高速なVPNトンネルでのスループットなど、最適なネットワークトラフィックに関するパフォーマンスを提供します。

サポートされているセキュリティ機能には、ファイアウォール、SSLおよびIPSecによる仮想プライベートネットワーキング、IPS、さまざまなプロトコル（HTTP、HTTPS、SMTP、DNSなど）のためのアプリケーションプロキシ、およびアンチウィルスが含まれます。ポリシーベースでのルーティングと、シンプルなレポートを提供します。

SonicWall Network Security Appliance（NSA）2650

*SonicWall NSA 2600*は、小規模企業、ブランチオフィス、キャンパスのセキュリティを守るためのシンプルで効果的な次世代ファイアウォールです。8つの1-GEポートがあり、最高1.9 Gbpsのファイアウォールスループットを提供します。

サポートされているセキュリティ機能には、ディープパケットインスペクション、ステートフルパケットインスペクションでのファイアウォール機能、アプリケーションインテリジェンスと制御、IPS、アンチウィルス、アンチスパイウェア、コンテンツとURLフィルタリング、およびSSLインスペクションが含まれます。

Fortinet FortiGate 100E

*FortiGate 100E*は、セキュリティおよびポリシーの一元管理のためのエンタープライズグレードのファイアウォールソリューションです。20個のネットワークポートを装備しています（WANポート2個、DMZポート1個、管理ポート1個、高可用性ポート2個、スイッチポート14個）。

仕様に記されているこの製品の最高スループットは、ファイアウォールでは7.4 Gbps、IPSでは500 Mbps、UTMでは360 Mbpsとなっています。サポートされているセキュリティ機能には、ファイアウォールポリシー、SSLおよびIPSecによる仮想プライベートネットワーキング、IPS、アプリケーション制御、および次世代ファイアウォールが含まれます。

Meraki MX84

*Meraki MX84*は、中規模のブランチオフィスネットワーク用のUTMソリューションです。クラウドで管理されるこの製品には、SD-WANのさまざまな機能および500Mbpsのステートフルファイアウォールパフォーマンス、そして320MbpsのUTMスループットを提供します。

サポートされているセキュリティ機能には、ファイアウォールポリシー、SSLおよびIPSecによる仮想プライベートネットワーキング、IPS、アプリケーション制御、および次世代ファイアウォールが含まれます。

Sophos XG 210

*Sophos XG 210*ファイアウォールは、強力なネットワーク保護を実現するためにユーザーおよびアプリケーションに基づいてポリシーを作成するための一元管理システムを提供します。6個のポートがあり、最大で14 Gbpsのファイアウォールスループットと1.7 Gbpsの次世代ファイアウォールパフォーマンスが提供されます。

サポートされるセキュリティ機能には、ファイアウォール、仮想プライベートネットワーキング、IPS、アプリケーション制御、Webフィルタリングおよびアンチウィルスが含まれます。

評価方法

Miercomは、実際の脅威環境をシミュレートするように設計されたハンズオンテストを使用して、製品の機能と効果に関する堅実で現実的な評価を行いました。テストは、それぞれのテスト対象デバイス（DUT）の長所と短所を明らかにします。

UDP、HTTP、およびHTTPSのトラフィックフロー処理に関する製品仕様を検証することを目的とした方法が採用されました。現実的なUDP、HTTP、およびHTTPSのトラフィックフローを生成してテストネットワーク内でフローさせることにより、一般的なクライアント/サーバー要求やファイル転送が再現されました。

セキュリティ機能がパフォーマンスに及ぼす影響を判別するため、各評価デバイスにおいて、個々の機能を有効にした状態でのスループットが分析されました。デバイスによっては、ファイアウォールをオフにすることができないこともあるため、この基本となるセキュリティレイヤが最初にテストされました。この基本レベルのプロセスは、各UTM製品で達成可能な最高のスループットを表します。付加的なセキュリティサービスを有効にして、そのパフォーマンスをファイアウォールスループットと比較することにより、保護機能の影響を判断しました。

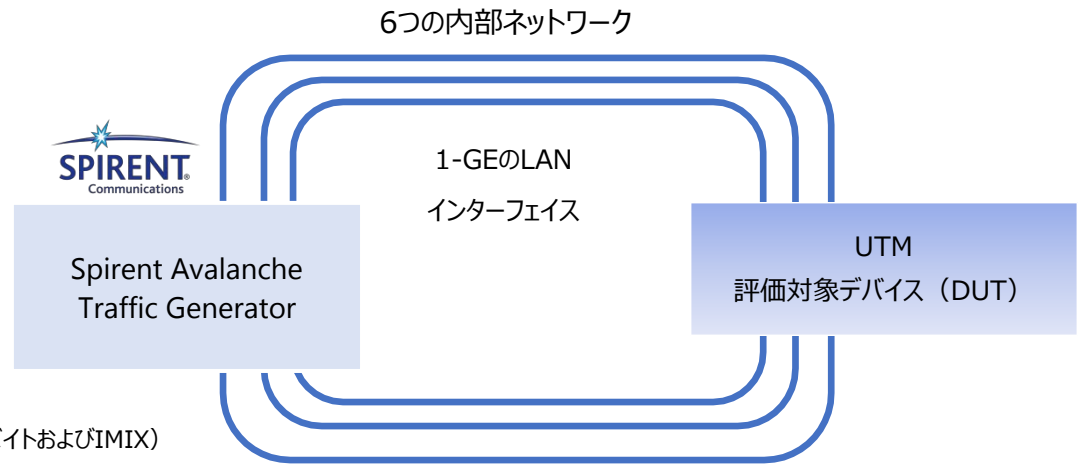
スループットは、業務環境にネットワークセキュリティアプライアンスを導入する際に参考になる測定値の1つにすぎません。スループットと同様にセキュリティも重要となります。しかし、ネットワークパフォーマンスの影響は、IT部門が、数々のネットワークセキュリティアプライアンスの中から最適な製品を選択するための参考になります。

テストツール

出典:Miercom

テスト中にリアルタイムのトラフィックの生成、トラフィック監視、およびデータキャプチャを行うために、上記のテストツールのいくつかが使用されています。テストの際に、トラフィック負荷の生成や、スループットデータの収集に、Spirent C100-S3（v4.85）が使用されました。

テストベッド図



- UDP（1518バイトおよびIMIX）
- 100のシミュレーションユーザー
  各ユーザーが100のHTTP/HTTPS GET要求（同じ1 MBの.dat（バイナリ）ファイルを取得するもの）を発行

出典:Miercom

UDPパフォーマンステストにはSpirent Test Centerを使用し、ステートフルトラフィックにはSpirent Avalancheを使用しました。 Meraki MX84のテストでは、ネットワークの信頼側と被信頼側との間でスイッチを使用しました。その動作にクラウドアクセスが必要であるためです。

3つの入力LANポートにつながる3つの1-GEリンクを使用してSpirent Test CenterまたはAvalancheから各DUTに外部クライアントトラフィックが送信され、3つの出力LANポートにつながる3つの1-GEリンクを通してサーバー応答が受信されました。全部で6つのインターフェイスが使用されたことになります。 ステートレスUDPトラフィックとステートフルのHTTP/Sトラフィックの両方のクライアント/サーバー接続を使用することにより、実世界の高ストレスなネットワークアクティビティを表すトラフィックが再現されました。

最初のファイアウォールテストには、ステートレスのUDPトラフィックとステートフルのHTTPおよびHTTPSトラフィックが使用されました。

ステートレストラフィックに関しては、6つのすべての1-GbEインターフェイス（合計で6 GbpsをDUTとの間でやり取りする）で250の双方向の別個のUDPパケットフローが送信されました。これは、2回の別個のテストで次のような2つの負荷として送信されました。

1. すべてのパケットが大きな1518バイトであるUDP
2. 66バイト（60.7パーセント）、594バイト（23.7パーセント）、および1518バイト（15.7パーセント）の各サイズの合計10,000個のパケットからなるIMIXのUDP

1つのパケットが失われるまでの各DUPのスループットの最大速度（メガバイト/秒（Mbps）単位）が測定されました。
この結果を11ページに掲載しています。

ステートフルトラフィックに関しては、クライアント側の100人のユーザーにより、100個のシミュレーションサーバーから1 MBのバイナリの.datファイルをダウンロードするHTTP GET要求が送信されました。クライアント側のユーザーごとに100個のGET要求が送信されました。この手順が、以下のそれぞれに対して実行されました。

1. HTTP
2. ECDHE-RSA-AES128-GCM-SHA256を使用するHTTPS
3. AES256-SHA256を使用するHTTPS（SonicWall（上記の暗号化スイートをサポートしていない）の場合のみ）

いずれかのファイル転送トランザクションが失敗に終わるまでの、スループットの最高速度（Mbps単位）が測定されました。DUTごとに、個々の付加的なセキュリティサービスを有効にした状態と、フルUTMモードで、このテストが繰り返されました。パフォーマンスをファイアウォールスループットと比較することにより、各DUTでのセキュリティサービスの影響を判断しました。

復号化機能を有効にした状態で、HTTPSを使用したステートフルスループットのテストを実施しました。しかし、Sophos XG 210では、必ず1つ以上のセキュリティ機能を有効にする必要がありました。Sophosの場合、復号化を行う構成では、AVも有効にする必要がありました。したがって、SophosのHTTPS FWのみのパフォーマンスは測定されていません。さらに、SophosでIPSのみを有効にした状態でのHTTPSのパフォーマンスは測定できませんでした。これには自動的にAVの有効化が必要になるためです。Cisco Merakiは、HTTPS復号化/プロキシをサポートしていないため、テストされませんでした。

公正な比較のため、この結果の詳細を13-14ページに掲載しています。

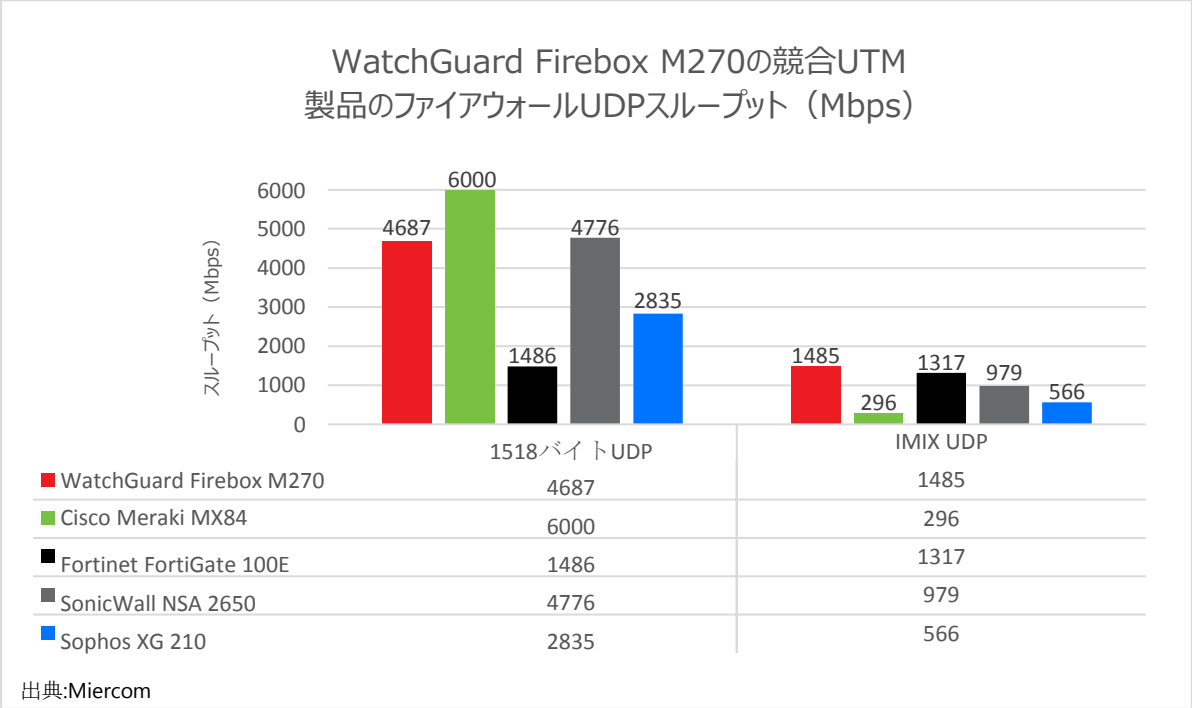
パフォーマンステスト

ステートレス UDP 1518バイトおよびUDP IMIXのスループット

このテストでは、テスト対象のセキュリティアプライアンスのトラフィックの最高速度がMbps単位で測定されました。ファイアウォールセキュリティサービスはセキュリティアプライアンスの最も基本的なサービスであるため、ファイアウォールセキュリティサービスのみが有効にされました。

最初のテストでは、6つのすべてのインターフェイスでステートレスの双方向のUDP 1518バイトパケット（最高6 Gbpsのトラフィック）が送信されました。2番目のステートレストラフィックテストでは、双方向のUDP IMIXトラフィックが使用されました。このトラフィックに含まれるパケットのサイズは同一ではありません。それぞれのサイズのパケットの数の割合は、60.7パーセントがスモールパケット（66バイト）、23.7パーセントがミッドサイズパケット（594バイト）、15.7パーセントがラージパケット（1518バイト）です。

図1:ステートレスのUDPトラフィックでの統合脅威管理（UTM）スループット



出典:Miercom

各製品のファイアウォールパケットルーティングのさまざまな機能を調べるために、ステートレスのUDPトラフィックが生成されました。DUTは6個の1GbEポートを使用しました。そのうち3つはクライアントからサーバーへの入力ポートで、残りの3つはサーバーからクライアントへの出力ポートです。最大回線速度パフォーマンスは6Gbpsでした。1518バイトパケットでは、WatchGuard Firebox M270は、期待される最大スループット4.96Gbpsの94.5パーセントを達成しました。このUTMのパフォーマンスは、Fortinetを68.3パーセント、Sophosを39.5パーセント上回っています。Cisco Merakiは1518バイトのトラフィックで回線速度レベルのパフォーマンスを達成しましたが、WatchGuardは現実的なIMIXトラフィックで最高のスループット1.5 Gbpsを達成しました。

ステートフルスループット（HTTP/HTTPS）

ほとんどのインターネット・トラフィックは、レイヤ4のプロトコル（TCP）でクライアント/サーバー接続を確立するために、ステートフルレイヤ7アプリケーションプロトコルHTTPを使用します。ネットワークでは、HTTPを使用して公衆インターネットからファイルをアップロードおよびダウンロードできます。それには、高レベルの処理と悪意のあるコンテンツの検査が必要になります。

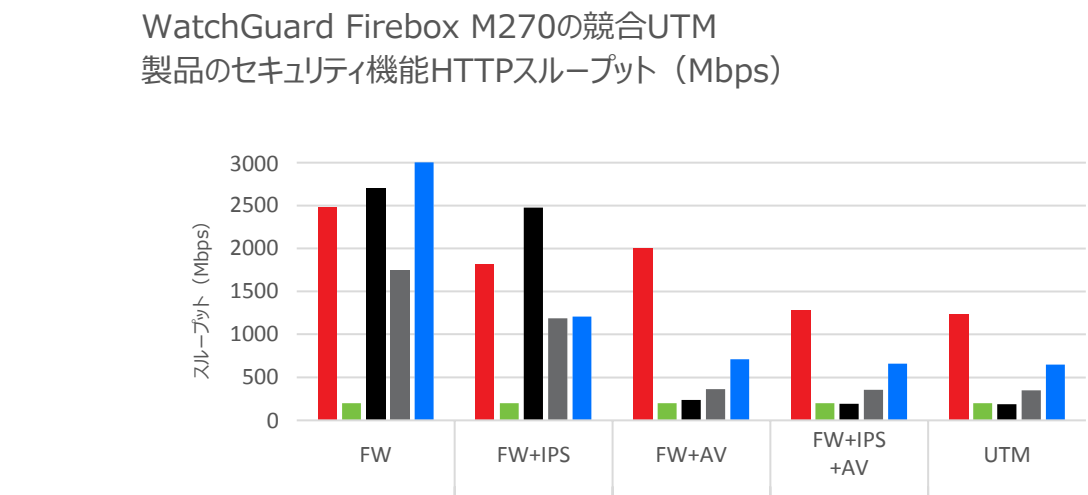
最も基本的な検査は、ファイアウォールと、各ベンダーで利用可能な付加的なセキュリティサービスを使用して実行されます。最もよく使用されているサービスには、復号化、IPS、AV、およびアプリケーション制御があります。下記のテスト結果は、類似したそれぞれのセキュリティアプライアンスに関する結果です。ファイアウォールと復号化を有効にして行った最初のテスト結果と、以下の構成を使用して付加的なセキュリティ機能を適用したときの結果を表しています。

1. **FW:** HTTPトラフィックストリームに対してファイアウォールのみを有効化。
2. **FW +IPS:** ファイアウォールに加えてIPSを有効化。
3. **FW +AV:** ファイアウォールに加えてWeb/HTTPプロキシとAVを有効化。この構成シナリオのパフォーマンステストに先立って、EICARと呼ばれる特殊なテスト用の疑似ウィルスを送信ファイルに含めることによって、製品のアンチウィルス処理が適切に構成され、ファイルがスキャンされてウィルス検出が通知されるようになっていることを確認。
4. **FW + AV + IPS:** ファイアウォールに加えてAVとIPSを有効化。
5. **フルUTM:** ファイアウォールに加えて、アプライアンスのAV、IPS、およびアプリケーション制御をすべて同時に有効化。

Spirent Avalancheで3組のインターフェイス上にHTTPテストトラフィックを生成して負荷を増大させていきました。インターフェイスごとに100台のシミュレーションクライアントが100台のシミュレーションサーバーに100回のGET要求を発行し、1MBのバイナリファイルをダウンロードして取得します。クライアントとサーバー間は、異なるLANにより分離されています。

同じように、ステートフルなHTTPSトラフィックの負荷も、この構成とテストセットアップを使用してDUTに送信されました。HTTPSによるアプリケーションレイヤのトラフィックのセキュリティ確保のため、ECDHE-RSA-AES128-GCM-SHA256暗号化標準規格が使用されました。ただし、SonicWallはこの暗号化スイートをサポートしていないので例外となります。SonicWallの場合のみ、AES256-SHA256を使用しました。1 MBのバイナリファイルが要求された時点で、各パケットが復号化されて再暗号化された後、転送されました。この処理によって、セキュリティアプライアンスとスループットに負荷がかかることが予想されました。暗号化トラフィックはセキュリティ上の脅威に対処する上で重要ですが、多くの攻撃者はまさにこの防衛手段を利用して、マルウェアが目的の場所に達するまでマルウェアだと悟られないようにしています。各DUTは、スループットを大きく低下させることなく暗号化メッセージを検査できなければなりません。

図2:ステートフルなHTTPトラフィックでの統合脅威管理（UTM）スループット

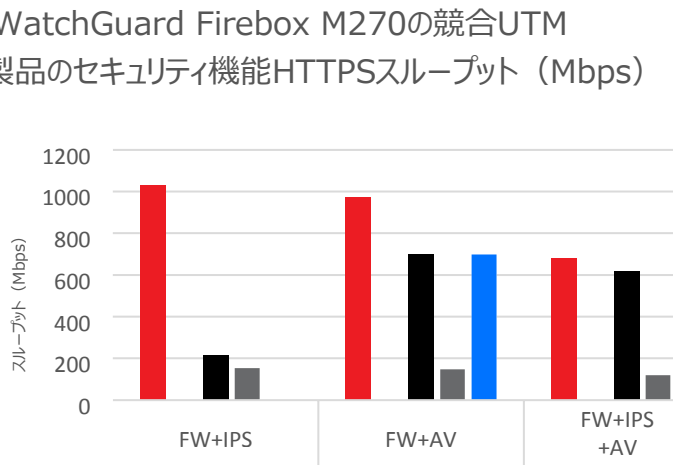


	FW	FW+IPS	FW+AV	FW+IPS +AV	UTM
WatchGuard Firebox M270	2485	1821	2003	1285	1237
Cisco Meraki MX84	200	200	200	200	200
Fortinet FortiGate 100E	2706	2475	238	192	190
SonicWall NSA 2650	1748	1186	365	356	350
Sophos XG 210	3000	1205	712	658	646

出典:Miercom

ステートフル*HTTP*トラフィックが各*DUT*の*6*つの*1GbE* ポートを使用して生成されました。*3*つのポートはクライアント側として動作し、*1MB*のデータファイルを要求しました。残りの*3*つのポートはサーバー側として動作し、応答としてそのファイルにレスポンスしました。出力ポートからのスループットが測定されました（最大回線速度パフォーマンスは*3Gbps*）。*WatchGuard Firebox M270*は、*FW+AV*、*FW+IPS+AV*、および*UTM*のセキュリティ機能を有効にした状態で、他のどれよりも高いパフォーマンスを示しました。この製品の最高のパフォーマンスは、ファイアウォール機能について観測され、あと少しで*2.5 Gbps*に達する数値でした。ファイアウォール機能については、他のベンダーの製品でもベストパフォーマンスが観測されることが予想されていました。*Sophos*は、*FW*のみの構成で回線速度パフォーマンスを達成しました。*WatchGuard*は、*FW+AV*において*2*番目に高いパフォーマンスを示し、この製品の最高のスループットからわずかに*19*パーセント下がっただけでした。対照的に、競合製品のパフォーマンスは、*92*パーセントも低下していました。*UTM*脅威保護を有効にした状態で*WatchGuard*は、*1.2 Gbps*を超えるスループットを達成し、これは競合製品よりも*47.8*パーセント高い数値でした。

図3:ステートフルなHTTPSトラフィックでの統合脅威管理（UTM）スループット



	FW+IPS	FW+AV	FW+IPS +AV	UTM
Watchguard Firebox M270	1030	972	680	661
Cisco Meraki MX84	N/A	N/A	N/A	N/A
Fortinet FortiGate 100E	213	698	616	589
SonicWall NSA 2650	153	147	120	118
Sophos XG 210	N/A	698	616	589

出典:Miercom

ステートフルな暗号化HTTPSトラフィックが、各DUTの6つの1 GbE ポートを使用して生成されました。HTTPパフォーマンステストと同様に、1 MBのファイルがサーバーからクライアントにダウンロードされた後で、3つの出力ポートからのスループットが測定されました。最大回線速度は3 Gbpsでした。Cisco Meraki MX84ではHTTPSがサポートされておらず、その意味でこの欄にはN/Aと記されています。上の図にも反映されているとおり、Sophos XG 210では、AV機能を有効にしないで暗号化トラフィックをサポートすることはできません。WatchGuard Firebox M270は、ファイアウォール構成とともにどの機能を有効にした場合にも、他のベンダーの製品より高いパフォーマンスを示しています。 WatchGuardはUTMパフォーマンスが661Mbpsで最高でした。 これは、その最大のライバル製品のUTMパフォーマンスを11パーセント上回っており、さらにSonicWall NSA 2650のUTMパフォーマンスを82パーセントも上回っています。

Miercomについて

Miercomは、これまでに数多くのネットワーク製品の分析結果を、主要な業界定期刊行物やその他の出版物の中で公開してきました。業界をリードする独立した製品テストセンターとしてのMiercomの評判は、誰もが認めるものとなっています。Miercomが提供するプライベートテストサービスには、競合製品の分析や個々の製品の評価も含まれています。Miercomは総合的な認定とテストのプログラムも提供しており、その中には、Certified Interoperable、Certified Reliable、Certified Secure、Certified Greenが含まれます。製品の使い勝手とパフォーマンスについての業界で最も徹底的かつ信頼性の高い評価が行われるPerformance Verifiedプログラムでの製品評価も受け付けています。

お客様による利用と評価

お客様には、独自に製品試験を実施するようおすすめします。テストは平均的な環境に基づいたものであり、あらゆるデプロイメントシナリオを反映したものではないためです。当社では、オンサイトでの評価の実施を希望するお客様を対象に、コンサルティングサービスや技術支援を提供しています。

テスト対象となったベンダー製品のいくつかで、より良いパフォーマンススループットを観測したことがありましたが、そのような場合は環境が異なっており、ファームウェアバージョン、テストツール、トラフィック構成などが異なっていました。

レポートの使用について

このレポートに含まれているデータを正確なものとするためにあらゆる努力が払われましたが、誤りや見落としが決してないとは限りません。このレポートに示されている情報が、各種のテストツールに依存している場合もあり、それらのツールの正確さについては当社の制御の及ばない分野です。さらに、本書にはベンダーからの情報に基づく部分もあり、それらの情報はMiercomでもある程度検証したとはいえ、100パーセント正確であることを検証することは当社には不可能です。

本書はMiercomにより「現存するままの状態で」提供され、明示または黙示を問わず、いかなる保証も代理責任も約束も適用されません。またこのレポートに含まれる情報の正確さ、完全性、有用性、適切性について、直接であれ間接であれ、その一切の法的責任を負いません。

本書で使用されているすべての商標は、それぞれの所有者が所有するものです。お客様は、当社のものではない活動、製品、サービスとの関連において、あるいは混乱や誤解を招く方法や欺瞞的な方法で、あるいは当社や当社の提供する情報やプロジェクトや開発物の評判を損ねる方法により、各商標をまるごとあるいはお客様自身の所有する商標の一部として使用しないことに同意するものとします。