ネットワーク IPS の比較分析

セキュリティ

2013 - Jason Pappalexis、Jason Pappalexis

テストした製品

Check Point 13500、Dell SonicWALL SuperMassive E10800、Fortinet FortiGate-3600C、HP TippingPoint S7500NX、
IBM GX7800、Juniper SRX5800、McAfee NS-9100、McAfee NS-9200、Sourcefire 7120、Stonesoft 3206

概要

侵入防止システム（IPS）の実装は、ソリューション全体のセキュリティの有効性に影響する複数の要因を含む、複雑なプロセスになる可能性があります。ソリューションの耐用年数にわたって考慮されるべきこれらの要因には、以下のようなものがあります。

1. 攻撃ブロック率
2. 回避対策率（一般的な回避テクニックへの対策）
3. デバイスの安定性と信頼性
4. 全体的な管理可能性（「*管理比較分析（Management Comparative Analysis）CAR*」を参照）

そこで、市場における各デバイスの相対的なセキュリティの有効性を判断し、正確な製品比較を行うため、NSS Labs は価値を基準とした比較を可能にする独自の測定基準を考案しました。

セキュリティの有効性 = 攻撃ブロック率[1] x 回避対策率 x 安定性と信頼性

図 1 – セキュリティの有効性を求める式

NSS は、攻撃ブロック率だけでなく、全体的なセキュリティの有効性に焦点を合わせることで、どの防御をバイパスできるのかという点と、デバイスの信頼性について、簡単に検討することができます。

製品	攻撃ブロック率	回避対策率	安定性と信頼性	セキュリティの有効性
Check Point 13500	94%	100%	100%	94.4%
Dell SonicWALL SuperMassive E10 800	95%	100%	100%	94.8%
Fortinet FortiGate-3600C	94%	100%	100%	93.8%
HP TippingPoint S7500NX	91%	100%	100%	91.1%
IBM GX7800	96%	100%	100%	95.7%
Juniper SRX5800	89%	100%	100%	89.2%
McAfee NS-9100	95%	100%	100%	95.1%
McAfee NS-9200	95%	100%	100%	95.1%
Sourcefire 7120	98%	100%	100%	97.9%
Stonesoft 3206	95%	100%	100%	94.7%

図 2 – セキュリティの有効性

企業ユーザーは、効果的な管理を企業セキュリティ展開の重要な構成要素であると考えているので、これも総所有コストと全体的な製品選択に反映されるべきです。しかし、これは、このレポートの範囲外です。詳細については、「*総所有コスト CAR*」と「*管理 CAR*」を参照してください。*バリュー*に対してマッピングされた*セキュリティの有効性*の全体像については、「*セキュリティ バリュー マップ（SVM）CAR*」を参照してください。

[1] 攻撃ブロック率は、テスト中にブロックされた攻撃の数として定義されます。

大多数の企業が自社の IPS の調整を行っていることを NSS の調査は示しています。そのため、NSS が行う IPS 製品のテストでは、調整済みのポリシー使ってデバイスを展開します。セキュリティの有効性とパフォーマンスの最適な組み合わせを実現することは、ライブ ネットワーク環境にデバイスを展開する標準的な顧客の目標です。これを実現するため、展開ポリシーに対してあらゆる努力が行われます。これにより、読者が想定する使用法に応じて、IPS のセキュリティの有効性とパフォーマンスの主な能力に関して最も有益な情報を提供します。

回避テクニックとは、セキュリティ製品による検出とブロックを回避するために攻撃を偽装および変更する手段です。回避への対策は、IPS の重要な構成要素です。回避を 1 つでも検出できないと、攻撃者はあらゆる攻撃手段を利用して IPS を迂回し、IPS をほぼ無価値にします。このテストで使用するテクニックには最近のものもありますが、その多くは何年も前から広く知られているものであり、IPS 製品カテゴリでは最低限の要件であると見なされます。テストのこのカテゴリは、製品ガイダンスに関して最終的な評価を加える際に重要です。

このグラフは、調整したポリシーを使用したときの保護とパフォーマンスの関係を示しています。上にいくほどセキュリティの有効性が高く、右に行くほどスループットが高いことを示します。

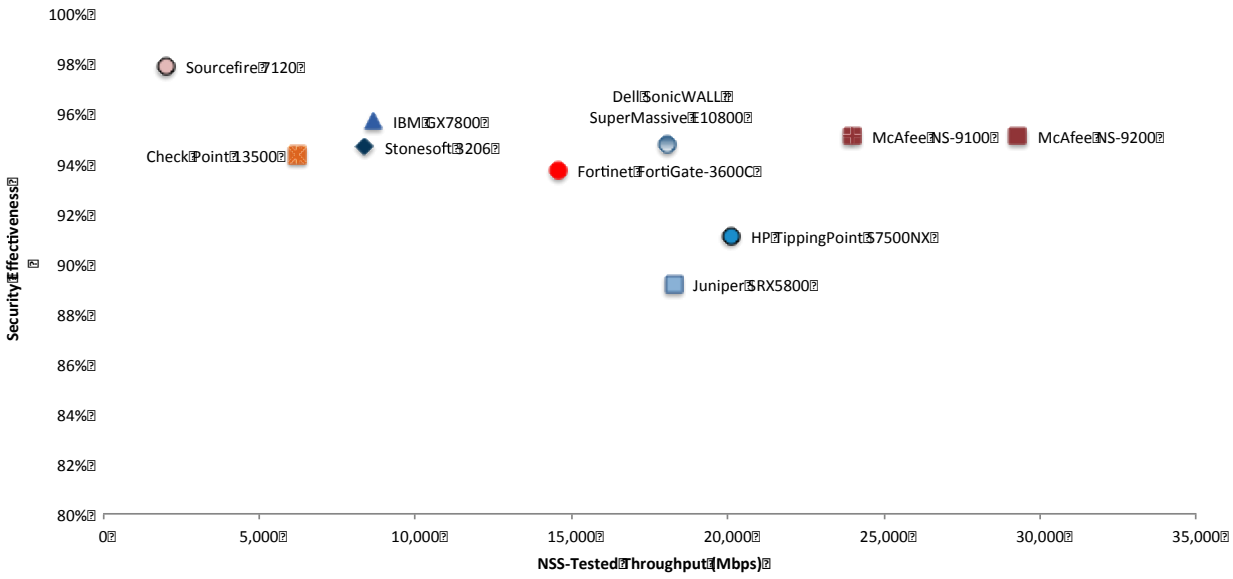

図 3 – セキュリティの有効性とパフォーマンス

製品を選択するときは、グラフの上部にある製品（セキュリティの有効性が 100% に近い製品）に優先順位を置くべきです。スループットは 2 番目の検討事項であり、各企業の展開要件に合わせて適したものを選択します。

目次

図の目次

分析

脅威を巡る状況は常に進化しています。攻撃者は戦略を磨き上げ、攻撃の量とインテリジェンスの両方を高めます。現在、企業は、標的型攻撃（TPA: targeted persistent attack）から身を守る必要があります。以前は、サーバーが主なターゲットでしたが、デスクトップ クライアント アプリケーションへの攻撃が主流となっており、これが組織に対する明確な脅威となっています。

調整

セキュリティ製品は複雑であることが多く、ベンダーは、ユーザー インターフェイスとセキュリティ ポリシーの選択を簡素化することで、拡大するユーザー基盤が求める使いやすさのニーズに対応しようとしています。多くの組織は、既定の設定をベンダーが一番に推奨する設定だと理解して受け入れ、展開します。この点では、IPS は例外です。NSS の調査は、すべてではないにせよ、大多数の企業が自社の IPS の調整を行っていることを示しています。一般的に、ベンダーの既定の設定を受け入れると、固有のシグネチャの多くが展開から省かれるため、組織がリスクに晒される可能性が高まります。

スキルを備えた経験豊富な熟練者の不足により、ソリューションを正しくインストール、保守、および調整するために必要な時間やリソースを考慮することが重要になります。インストール、保守、調整を正しく行わないと、製品のセキュリティ能力を完全には活かせなくなる可能性があります。したがって、すべての IPS 製品は、誤検出を取り除き、保護対象のシステムに最も適切なカバーを提供するため、テストの前に調整されます。一般的に、調整はベンダーの経験豊かなシステム エンジニアによって行われますが、これが不可能な場合は、NSS のエンジニアが必要な調整を行います。NSS のエンジニアは、テスト中のデバイス（DUT: device under test）の具体的な特性またはその構成がテストの通常の操作を妨げる場合、またはテストから得られた結果が DUT の実際の能力を表していないとエンジニアが考えた場合は、DUT の構成を変更する場合があります。セキュリティの有効性とパフォーマンスの最適な組み合わせを実現することは、ライブ ネットワーク環境に DUT を展開する標準的な顧客の目標です。これを実現するため、あらゆる努力が行われます。

IPS の調整は、複雑化する可能性のある作業であり、環境ごとに個別に実施すべきです。どのシグネチャまたはルールを IPS で有効化するかの判断には、ネットワーク アーキテクチャ、ターゲット アセット、パッチ レベル、許可されるプロトコルなど、さまざまな要因が影響を与えます。

攻撃ブロック率

NSS のセキュリティの有効性テストでは、NSS のエンジニアの深い専門知識を活用し、必要に応じて複数の市販ツール、オープン ソース ツール、独自ツールを用いて、現代のサーバー犯罪者が使用するのと同じ種類の攻撃を生成します。実際の攻撃の数は 1800 を超えます。これは、業界史上で最も包括的なテストです。最も注目すべき点は、これらのテストにおける実際の攻撃とペイロードのすべては、以下の要件を満たすことが検証されているということです。

- リバース シェルが返される
- バインド シェルがターゲットで開き、攻撃者が任意のコマンドを実行できる
- 悪意のあるペイロードがインストールされる

- システムが応答不能になる

年別の攻撃ブロック率

一般に考えられていることとは異なり、最大のリスクが常に最新の "パッチ チューズディ" の脆弱性開示をきっかけに発生するわけではありません。NSS の脅威に関する調査では、古い攻撃が今でも数多く出回っていることが分かっており、したがって、これらへの対策も意味を持ちます。

脆弱性が開示されたとき、カバーを追加するためのアプローチはベンダーによって異なります。完全に理解されていない脆弱性に対して迅速なカバーを提供しようと試みることで、不正確かつ非効率で、誤検出につながりやすい、特定の攻撃に対応する複数のシグネチャが導入される可能性があります。脆弱性を完全に調査できるリソースを持つベンダーは、その脆弱性に付け入ろうとするすべての攻撃に対するカバーとして、特定の脆弱性に対するシグネチャを作り出せる可能性があります。このアプローチにより、誤検出の少ない、より効果的なカバーが提供されます。

製品にパフォーマンスの制限がある場合、ベンダーはこうした制限を緩和するために古いシグネチャを使用中止する場合があり、このため、古い脆弱性のカバーに一貫性が失われます。これにより、製品の間で保護のレベルに差が生じます。次の表は、CVE 数による追跡に従い、開示日別にカバーを分類したものです。表は、保護の合計数で並べ替えられています。ヒート マップの緑のセクションは、その年（列）のカバー率が高かったベンダーを示します。

製品	<=2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	合計
Check Point 13500	100.0%	96.9%	98.9%	99.2%	96.9%	97.3%	93.4%	75.2%	90.2%	68.0%	94.4%
Dell SonicWALL Super Massive E10800	100.0%	100.0%	100.0%	99.6%	97.8%	98.4%	93.1%	71.8%	90.2%	64.0%	94.8%
Fortinet FortiGate-3600C	100.0%	97.9%	98.9%	97.7%	97.5%	96.8%	94.0%	70.9%	87.8%	60.0%	93.8%
HP TippingPoint S7500NX	93.3%	95.8%	97.9%	96.2%	93.4%	93.5%	88.2%	70.9%	87.8%	60.0%	91.1%
IBM GX7800	100.0%	97.4%	100.0%	98.9%	97.8%	97.8%	94.6%	82.1%	90.7%	92.0%	95.7%
Juniper SRX5800	100.0%	90.6%	93.2%	91.6%	92.8%	94.6%	89.1%	70.9%	82.9%	68.0%	89.2%
McAfee NS-9100	100.0%	99.5%	99.5%	99.6%	97.8%	97.8%	93.4%	75.2%	91.7%	68.0%	95.1%
McAfee NS-9200	100.0%	99.5%	99.5%	99.6%	97.8%	97.8%	93.4%	75.2%	91.7%	68.0%	95.1%
Sourcefire 7120	100.0%	99.5%	100.0%	99.2%	99.4%	99.5%	98.2%	88.9%	93.2%	100.0%	97.9%
Stonesoft 3206	80.0%	94.3%	96.3%	96.2%	93.8%	94.6%	97.9%	80.3%	97.1%	96.0%	94.7%

図 4 - 年別の攻撃ブロック率 – 既定のポリシー

攻撃ベクトル別の攻撃ブロック率

サーバーに対する攻撃は、ターゲット（デスクトップ クライアント）によってローカルで開始されることも、攻撃者によってリモートで開始されることもあります。2007 年以降、NSS の調査担当者は、クライアント サイドの攻撃が大幅に増加していることを報告しています。これは、感染した Web サイトを訪問した善意のユーザーによって簡単に開始できるからです。ウィルス対策製品が対処すべき問題だと考えられていたこの種の攻撃について、以前は IPS 製品は焦点を合わせていませんでした。

現在では、これは容認されるアプローチとは考えられていません。そのため、IPS 産業は、クライアント サイドの攻撃に対して広範なカバーを提供する困難さを乗り越え、より包括的なクライアント サイドのカバーを提供しようと試みています。

NSS は以下の定義を使用します。

攻撃者による開始: 脅威/攻撃は、脆弱なアプリケーションやオペレーティング システムに対して、攻撃者によってリモートで遂行されます。こうした攻撃は、以前から主にサーバーがターゲットとなります（このため、サーバー サイドの攻撃と呼ばれることもあります）。

ターゲットによる開始: 脅威/攻撃は、脆弱なターゲットによって開始されます（このため、クライアント サイドの攻撃と呼ばれることもあります）。攻撃者は、ターゲットのユーザーまたはアプリケーションがいつ脅威を遂行するのかについて、ほとんど、またはまったくコントロールすることができません。こうした攻撃のターゲットとなるのは、以前から主にデスクトップ クライアントアプリケーションです。ターゲットの例としては、Explorer、Adobe、Firefox、QuickTime、Office アプリケーションを挙げることができます。

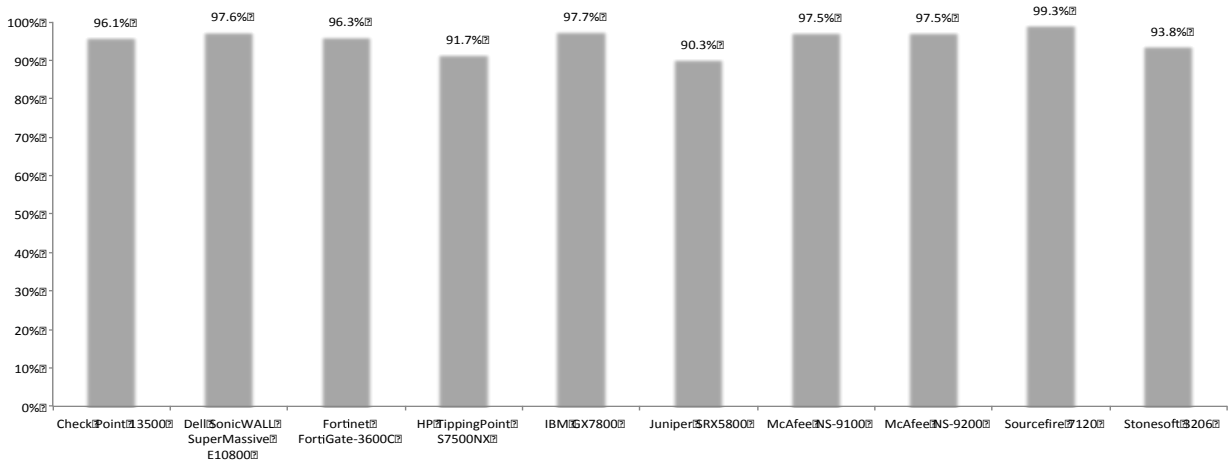

図 5 – 攻撃者が開始した攻撃のブロック率

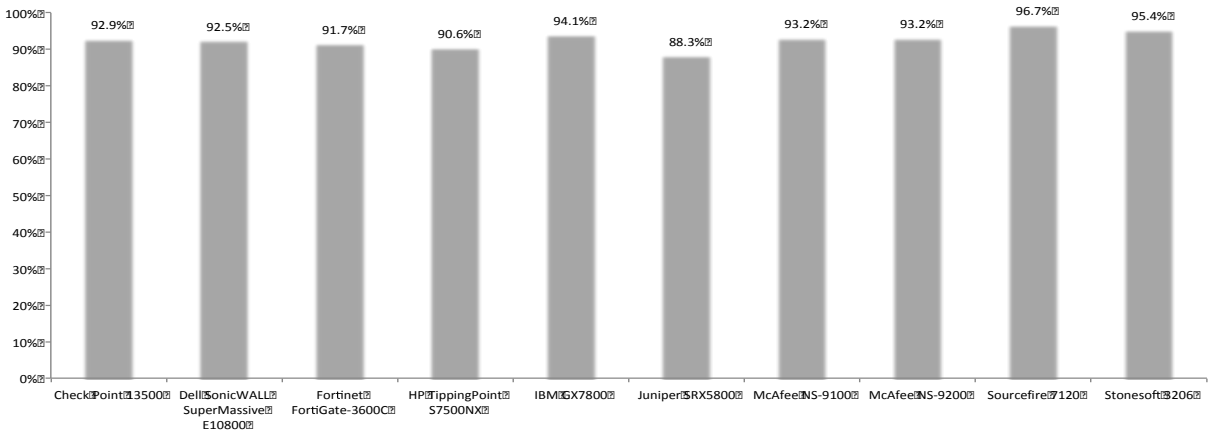

図 6 – ターゲットが開始した攻撃のブロック率

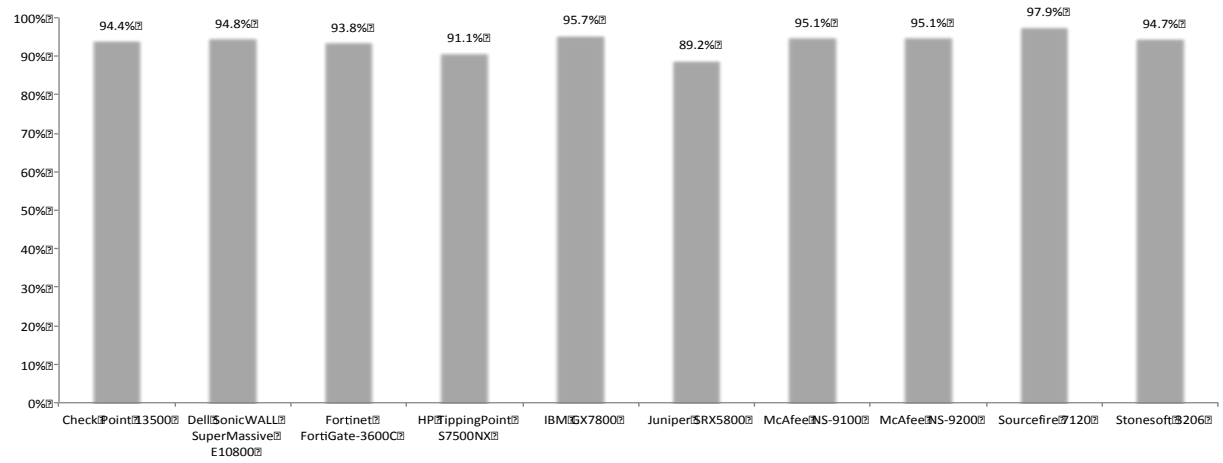

図 7 - 全体的な攻撃ブロック率

NSS の調査により、ほとんどの企業がデスクトップ クライアント アプリケーションの異種ミックスをサポートしなければならないことが分かっています。さらに、企業の IT 部門は、社員のデスクトップで実行されているクライアント アプリケーションを明確に識別できないことがよくあります。

この調査は、調整のベスト プラクティスを新たに明確に定義するとともに、DMZ やデータ センターの IPS で保護されたサーバーを調整することが今でも必要であることを示しています。また、デスクトップ クライアント アプリケーションの保護に関する IPS の使用については、特定のデスクトップ クライアント アプリケーションに基づいて IPS を調整することは現実的でないため、シグネチャの（ほぼ）すべてを有効にするのが最善である場合が多いことに企業が気付き始めていることを、調査は示しています。

デスクトップ クライアント アプリケーションをターゲットとする犯罪行為は急速に進化しているので、2013 年と 2014 年には、企業はクライアント サイドの保護により多くのリソースを割く必要に迫られます。

影響タイプ別の攻撃ブロック率

最も深刻な攻撃は、リモート システムのセキュリティを突破し、攻撃者がシステム レベルの任意のコマンドを実行できるようにするものです。このクラスのほとんどの攻撃は ″兵器化″ されており、攻撃者に対して、ターゲットのクライアントまたはサーバーで完全にインタラクティブなリモート シェルを提供します。

これよりも若干深刻度の低い攻撃は、個別のサービスのセキュリティを突破しますが、システム レベルの任意のコマンドを実行することはできないものです。このカテゴリの一般的な攻撃には、SQL インジェクションなど、サービス固有の攻撃が含まれます。これにより、攻撃者は、データベース サービス内で任意の SQL コマンドを実行できます。これらの攻撃はほぼ特定のサービスに隔離されるので、オペレーティング システムやすべてのサービスへの完全なシステム レベルのアクセスに直ちにつながることはありません。しかし、局部的な追加のシステム攻撃を使用して、サービス レベルからシステム レベルへと攻撃をエスカレートすることが可能です。

最後は、システムまたはサービス レベルの障害を発生させる攻撃（多くの場合、ターゲットによって開始される攻撃）で、ターゲットとなったサービスやアプリケーションを強制終了させ、サービスの再開やシステムの再起動に管理アクションが必要となります。これらの攻撃では、攻撃者は任意のコマンドを実行することはできません。しかし、攻撃者は保護されたシステムやサービスを強制終了させることができるので、ビジネスに対して大きな影響が出る可能性があります。

製品	システムのエクスポージャー	サービスのエクスポージャー	システムまたはサービスの障害
Check Point 13500	93.7%	98.3%	97.9%
Dell SonicWALL SuperMassive E10800	93.9%	100.0%	100.0%
Fortinet FortiGate-3600C	93.1%	98.3%	97.2%
HP TippingPoint S7500NX	91.2%	96.7%	84.8%
IBM GX7800	95.3%	99.2%	97.2%
Juniper SRX5800	88.8%	88.3%	94.5%
McAfee NS-9100	94.4%	100.0%	98.6%
McAfee NS-9200	94.4%	100.0%	98.6%
Sourcefire 7120	97.6%	100.0%	99.3%
Stonesoft 3206	95.6%	93.3%	85.5%

図 8 – 影響タイプ別の攻撃ブロック率

詳細は、それぞれの*製品分析レポート*（PAR）を参照してください。

ターゲット ベンダー別の攻撃ブロック率

NSS 攻撃ライブラリは、さまざまなソフトウェア ベンダーの広範囲にわたるプロトコルとアプリケーションを網羅します。このグラフは、今回のテストにおいて NSS 攻撃ライブラリに含まれるベンダー特定の攻撃の数に基づいてベンダーをランク付けし、その上位 5 社（全体では 70 社以上）に対するカバー率を示したものです。

説明	Microsoft	Oracle	Apple	IBM	Adobe
Check Point 13500	99.5%	98.7%	100.0%	100.0%	100.0%
Dell SonicWALL SuperMassive E10800	100.0%	100.0%	100.0%	100.0%	100.0%
Fortinet FortiGate-3600C	99.1%	97.3%	95.7%	100.0%	93.3%
HP TippingPoint S7500NX	95.7%	97.3%	97.1%	93.3%	97.8%
IBM GX7800	99.5%	100.0%	98.6%	97.8%	100.0%
Juniper SRX5800	95.4%	77.3%	95.7%	97.8%	93.3%
McAfee NS-9100	99.1%	100.0%	100.0%	100.0%	97.8%
McAfee NS-9200	99.1%	100.0%	100.0%	100.0%	97.8%
Sourcefire 7120	100.0%	100.0%	97.1%	100.0%	100.0%
Stonesoft 3206	96.8%	96.0%	98.6%	93.3%	100.0%

図 9 – ターゲット ベンダー別の攻撃ブロック率

詳細は、それぞれの*製品分析レポート*（PAR）を参照してください。

回避

回避テクニックとは、セキュリティ製品による検出とブロックを回避するために、配信の時点で攻撃を偽装および変更する手段です。セキュリティ デバイスが特定の種類の回避を正しく処理できない場合、攻撃者は、デバイスが保護を提供しているはずの攻撃クラス全体を使用できる可能性があります。これにより、デバイスはほぼ無価値になります。このテストで使用するテクニックの多くは何年も前から広く知られているものであり、IPS 製品カテゴリでは最低限の要件であると見なされます。

回避を完全に考慮していない攻撃保護結果を提供することは、誤解を招くおそれがあります。IP フラグメンテーション、RPC フラグメンテーション、URL 難読化、TCP 分割ハンドシェイク、FTP 回避など、見逃された回避クラスが多いほど、デバイスの有効性は低下します。例えば、各カテゴリで 1 つのテクニックを見逃した場合、1 つの回避カテゴリ（FTP 回避など）のすべてのテクニックを見逃した場合に比べ、攻撃対象がより広範になるので、後者の方がより有効です。

さらに、ネットワーク スタックの低層で行われる回避（IP フラグメンテーションまたは TCP セグメンテーション）は、上層で行われる回避（HTTP または FTP 難読化）に比べてセキュリティの有効性に大きな影響を与えます。これは、低層レベルの回避はより多数の攻撃に影響を与える可能性があるからです。したがって、TCP セグメンテーションを見逃すことは、FTP 難読化を見逃すことよりも、はるかに深刻な問題です。

難読化や回避テクニックを使用する攻撃を検出できなかった場合、製品の有効性は著しく低下し、NSS の製品ガイダンスはこれを反映して調整されます。

攻撃と同様に、回避も、ターゲットによってローカルで開始された攻撃（クライアント サイド）、またはサーバーに対して攻撃者によってリモートで開始された攻撃（サーバー サイド）を特に難読化するために利用されます。サーバー サイドの攻撃とクライアント サイドの攻撃の**両方**で、同じように有効な回避もあります。詳細は、「*攻撃ベクトル別の攻撃ブロック率*」を参照してください。

次のグラフは、攻撃者またはターゲットが開始した攻撃と回避、およびその合計を示しています。

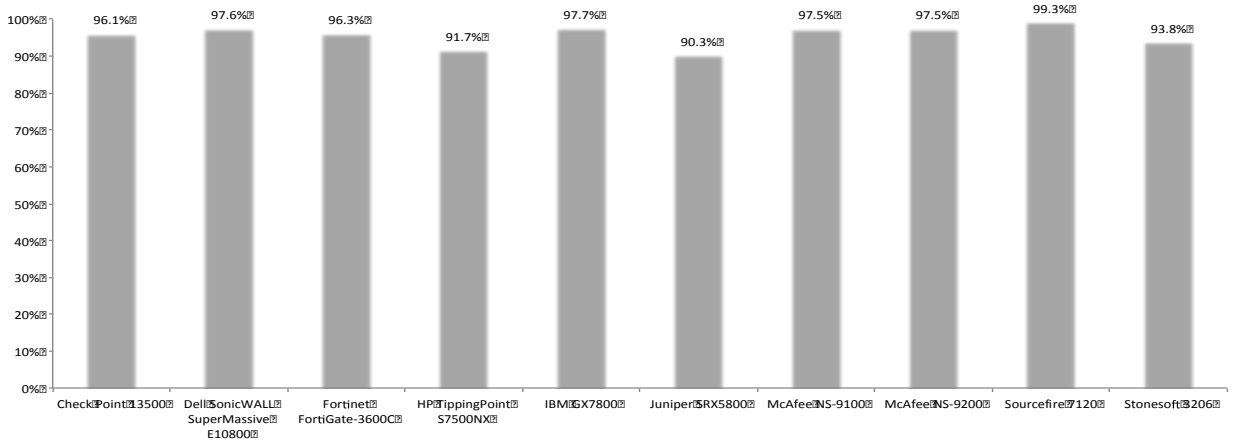

図 10 – 攻撃と回避（サーバー サイド）

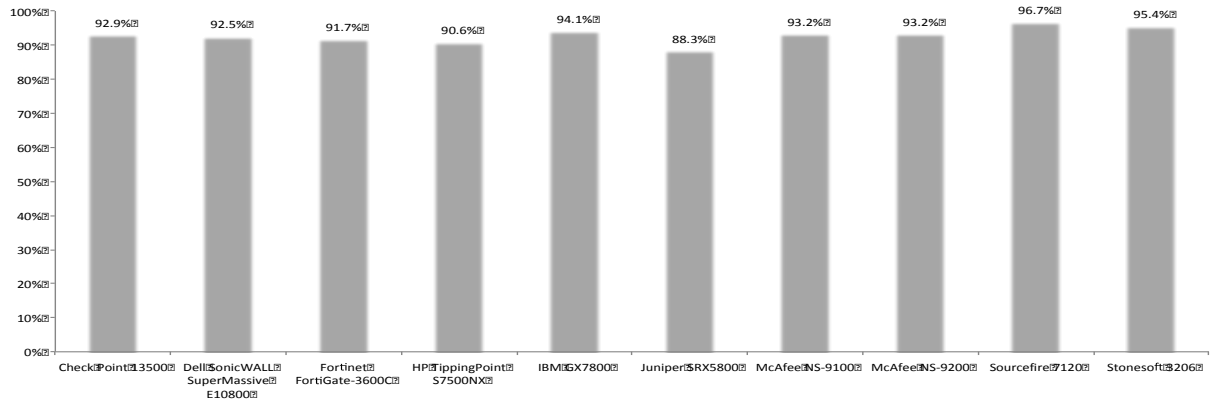

図 11 - 攻撃と回避（クライアント サイド）

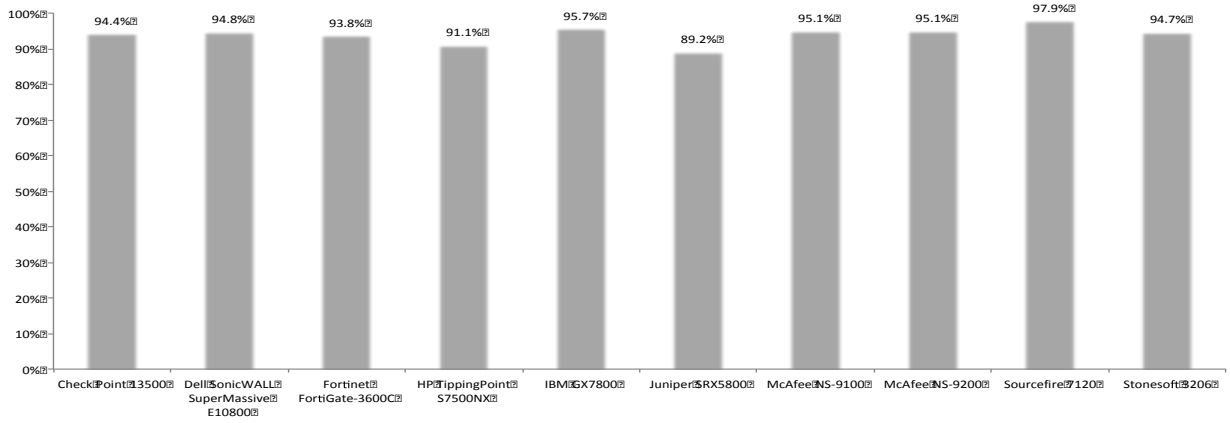

図 12 - 攻撃と回避（合計）

Fortinet FortiGate-3600C については、競合製品に比べてクライアント サイドの攻撃をブロックする率が低く、「*セキュリティの有効性*」に関して "平均を下回る" 結果となりました（「*セキュリティ バリュー マップ CAR*」を参照してください）。しかし、このデバイスの全体的なパフォーマンスは平均を上回っています。したがって、クライアントサイドの攻撃が関係しない環境（純粋なサーバー環境など）では、この問題を検討事項から外す必要があります。

次の図は、テストした製品に関する回避の対策について詳細を示したものです。

製品	IP パケット フラグメンテーション	TCP ストリーム フラグメンテーション	RPC フラグメンテーション	SMB および NetBIOS 回避	URL 難読化	HTML 難読化
Check Point 13500	合格	合格	合格	合格	合格	合格
Dell SonicWALL SuperMassive E10800	合格	合格	合格	合格	合格	合格
Fortinet FortiGate-3600C	合格	合格	合格	合格	合格	合格
HP TippingPoint S7500NX	合格	合格	合格	合格	合格	合格
IBM GX7800	合格	合格	合格	合格	合格	合格
Juniper SRX5800	合格	合格	合格	合格	合格	合格

McAfee NS-9100	合格	合格	合格	合格	合格	合格
McAfee NS-9200	合格	合格	合格	合格	合格	合格
Sourcefire 7120	合格	合格	合格	合格	合格	合格
Stonesoft 3206	合格	合格	合格	合格	合格	合格

図 13 – 回避の対策 (I)

製品	ペイロードのエンコード	FTP 回避	IP フラグ + TCP セグ	IP フラグ + MSRPC フラグ	IP フラグ + SMB 回避	TCP セグ + SMB / NetBIOS 回避	TCP 分割ハンドシェイク
Check Point 13500	合格	合格	合格	合格	合格	合格	合格
Dell SonicWALL SuperMassive E10800	合格	合格	合格	合格	合格	合格	合格
Fortinet FortiGate-3600C	合格	合格	合格	合格	合格	合格	合格
HP TippingPoint S7500NX	合格	合格	合格	合格	合格	合格	合格
IBM GX7800	合格	合格	合格	合格	合格	合格	合格
Juniper SRX5800	合格	合格	合格	合格	合格	合格	合格
McAfee NS-9100	合格	合格	合格	合格	合格	合格	合格
McAfee NS-9200	合格	合格	合格	合格	合格	合格	合格
Sourcefire 7120	合格	合格	合格	合格	合格	合格	合格
Stonesoft 3206	合格	合格	合格	合格	合格	合格	合格

図 14 – 回避の対策 (II)

製品	全体的な回避の結果
Check Point 13500	合格
Dell SonicWALL SuperMassive E10800	合格
Fortinet FortiGate-3600C	合格
HP TippingPoint S7500NX	合格
IBM GX7800	合格
Juniper SRX5800	合格
McAfee NS-9100	合格
McAfee NS-9200	合格
Sourcefire 7120	合格
Stonesoft 3206	合格

図 15 – 全体的な回避の結果

すべてのデバイスは、テストした回避技法のすべてに対して有効性を証明しました。

安定性と信頼性

インライン デバイスでは、障害の発生がネットワークの故障につながりうるので、長期的な信頼性が特に重要です。これらのテストでは、DUT の安定性に加え、通常負荷の状態、および悪意のあるトラフィックを通過させる際にセキュリティの有効性を維持する DUT の能力を検証します。敵対的な攻撃の際に適切なトラフィックを維持できない（強制終了してしまう）製品は合格しません。

これらのテストの間、DUT は業務に支障のない安定したスループットを維持し、攻撃ごとにアラートを発生させながら、以前ブロックしたトラフィックの 100% をブロックする必要があります。何らかの理由で DUT がオープンにならなかったことやトラフィックの量が原因で、禁止されたトラフィックの通過を許した場合、テスト結果は不合格になります。

製品	広範な攻撃下でのブロック	広範な攻撃下での適切なトラフィックの通過	負荷を受けた際の状態エンジンの動作	攻撃検出/ブロック – 通常負荷	状態保存 – 通常負荷	適切なトラフィックの通過 – 通常負荷
Check Point 13500	合格	合格	合格	合格	合格	合格
Dell SonicWALL SuperMassive E10800	合格	合格	合格	合格	合格	合格
Fortinet FortiGate-3600C	合格	合格	合格	合格	合格	合格
HP TippingPoint S7500NX	合格	合格	合格	合格	合格	合格
IBM GX7800	合格	合格	合格	合格	合格	合格
Juniper SRX5800	合格	合格	合格	合格	合格	合格
McAfee NS-9100	合格	合格	合格	合格	合格	合格
McAfee NS-9200	合格	合格	合格	合格	合格	合格
Sourcefire 7120	合格	合格	合格	合格	合格	合格
Stonesoft 3206	合格	合格	合格	合格	合格	合格

図 16 – 安定性と信頼性 (I)

製品	状態保存 – 最大数超過	トラフィック ドロップ – 最大数超過	プロトコル ファジングとミューテーション	電源障害	データの持続性	安定性と信頼性のスコア
Check Point 13500	合格	合格	合格	合格	あり	合格
Dell SonicWALL SuperMassive E10800	合格	合格	合格	合格	あり	合格
Fortinet FortiGate-3600C	合格	合格	合格	合格	あり	合格
HP TippingPoint S7500NX	合格	合格	合格	合格	あり	合格
IBM GX7800	合格	合格	合格	合格	あり	合格
Juniper SRX5800	合格	合格	合格	合格	あり	合格
McAfee NS-9100	合格	合格	合格	合格	あり	合格
McAfee NS-9200	合格	合格	合格	合格	あり	合格
Sourcefire 7120	合格	合格	合格	合格	あり	合格

Stonesoft 3206	合格	合格	合格	合格	あり	合格

図 17 – 安定性と信頼性 (II)

セキュリティの有効性

デバイスのセキュリティの有効性は、回避テストおよび安定性と信頼性のテストの結果を攻撃ブロック率に換算して判断します。図 18 には、各デバイスのセキュリティの有効性が示されています。

製品	攻撃ブロック率	回避対策率	安定性と信頼性	セキュリティの有効性
Check Point 13500	94%	100%	100%	94.4%
Dell SonicWALL SuperMassive E10 800	95%	100%	100%	94.8%
Fortinet FortiGate-3600C	94%	100%	100%	93.8%
HP TippingPoint S7500NX	91%	100%	100%	91.1%
IBM GX7800	96%	100%	100%	95.7%
Juniper SRX5800	89%	100%	100%	89.2%
McAfee NS-9100	95%	100%	100%	95.1%
McAfee NS-9200	95%	100%	100%	95.1%
Sourcefire 7120	98%	100%	100%	97.9%
Stonesoft 3206	95%	100%	100%	94.7%

図 18 – セキュリティの有効性

セキュリティの有効性の管理

セキュリティ デバイスの展開は複雑です。一元的管理コンソール オプション、ログ集計、イベント相関/管理システムなどの基本的なシステムが、購入の意思決定をさらに複雑なものにします。企業のセキュリティ担当者が、安全で効果的な方法で、企業全体で複数のファイアウォールを展開して管理できることが重要です。デバイスを効果的に管理できない場合、デバイスのセキュリティの有効性は低下します。

このテストの一環として、NSS は、各ベンダーが提供するエンタープライズ管理システムの主要な機能と能力について、以下のような主要エリアにおいて詳細な技術評価を行いました。

- **一般的な管理と構成** – デバイスをインストールおよび構成し、大規模な企業ネットワークで複数のデバイスを展開するのがどれくらい簡単か?
- **ポリシー処理** – 複雑なセキュリティ ポリシーを作成、編集して、企業全体に展開するのがどれくらい簡単か?
- **アラート処理** – アラートの生成がどれくらい正確で適時性があるか? および、セキュリティの問題を修正するために必要な重要な情報を見つけるために、ドリルダウンするのがどれくらい簡単か?
- **レポート** – レポート機能はどれくらい効果的か? および、カスタマイズがどれくらい容易か?

これらのテスト結果は、詳細なコスト モデルと共に、「*管理 CAR* 」および「*総保有コスト (TCO) CAR*」でレポートされます。

テスト手法

テスト手法のバージョン: ネットワーク侵入防止システム (IPS) v7.2

テスト手法のコピーは NSS Labs の Web サイト (www.nsslabs.com) から入手できます。

連絡先情報

NSS Labs, Inc.
206 Wild Basin Rd
Building A, Suite 200
Austin, TX 78746
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com