# SWARM レポート

SonicWall アプリケーション リスク管理レポート

**レポート先:**
SonicWall

**レポート元ファイアウォール:**
18**********

**ファイアウォール モデル:**
SONICWALL TZ400W Japan

**SonicOS バージョン:**
6.2.7.1-23n.jpn

**収集日:**
Aug 10 2017 08:28:58 +0900

# 目次

# 執行状況の説明

SonicWall ネットワーク セキュリティ装置は、従来のステートフル検知ファイアウォールではまったく不可能であった複雑な攻撃を検知および遮断できます。弊社の次世代ファイアウォールは、特許取得済みの再構築不要精密パケット検査 (RFDPI) ファイアウォール エンジンを、自動化された動的セキュリティ機能に対して包括的かつ多様に統合しています。これらの機能には、高度な対回避型侵入防御、クラウド更新型ゲートウェイ アンチマルウェア、SSL の復号および検査 (DPI-SSL)、アプリケーション制御、コンテンツ フィルタなどが含まれます。これらすべてが、ライセンス購読、配備、管理、メンテナンスの容易な、高パフォーマンスの単独の装置によって提供されています。

それに加え、SonicWall は、単独の物理装置でのパワフルなセキュリティと管理ツール一式を、分かりやすいライセンス体系でバンドル提供しています。

監査用のローカル ログは、SonicWall 装置に保存されています。このレポートは、ネットワークの高レベルな要約を以下の通り提供します。

- ✔ 検知および遮断された脆弱性の特定
- ✔ 脆弱性の説明
- ✔ 使用されているアプリケーションの説明
- ✔ 地域別、URL 種別別、トラフィック種別別のトラフィック分布統計の提供
- ✔ 高帯域幅アプリケーションの上位ハイライト
- ✔ リスクの定義
- ✔ アプリケーションの一覧
- ✔ 高リスク アプリケーションおよびプロトコルの一覧

# SWARM の概要

SonicWall アプリケーション リスク管理 (SWARM) レポートは、SonicWall 次世代ファイアウォール装置によって検知および遮断された異なる脅威が起こった時点でのスナップショットです。また、ネットワーク上の様々なトラフィックを洞察するために、このレポートは上位アプリケーション トラフィック、上位ユーザ、上位 URL 種別およびセッション数を含むアプリケーションとユーザ基準のデータを提供します。

## 脅威指標

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| 低 | 中 | 高 | 深刻 |
| ネットワークに起こる識別可能な活動も悪意のあるコード活動もありません。 | 違法となり得るアプリケーションまたは脅威がネットワーク上に確認されました。 | ネットワーク上のいくつかのアプリケーションが、性能に影響を及ぼしているか、ポリシーを回避するサービスを提供している | いくつかのアプリケーションが、ネットワークの性能に影響を及ぼしており、悪意のある活動することで知られるアプリケーショ |

この格付けは、ネットワーク上に確認されたすべてのアプリケーションのリスク レベルの平均点であり、ネットワークにもたらす脅威の指標となります。

## 脅威 防御

| | |
|---|---|
| 10 | ボットネット イベン |
| 1 | ウイルス イベント |
| 0 | スパイウェア イベ |
| 6 | IPS イベント |

## エンドポイント

| | |
|---|---|
| 3 | 上位イベント 101 IPs |

## 上位トラフィック (国別)

1. United States
2. Japan
3. China

組織名
SonicWall

SonicWall 装置
SONICWALL TZ400W Japan

SonicOS バージョン
6.2.7.1-23n.jpn

購読サービス
App Control, GAV, IPS, SPY, CFS, GeoIP, Botnet

収集期間
1 Days

# アプリケーション インテリジェンス、制御および可視化

SonicWall ファイアウォールは、ネットワークの制御を IT 管理者の支配下に置くことができます。いくつかのアプリケーションは、重要な業務で使用され、より多くの帯域幅を使用しますが、その他のアプリケーションは、非生産的であり、ネットワーク上で遮断するポリシーや帯域幅を制限する必要がある場合があります。SonicWall の次世代ファイアウォールは、堅牢なアプリケーション識別方式、きめ細かいポリシー制御オプション、および、詳細な可視化ツールによって、それらの作業を簡単に行えます。

## アプリケーション インテリジェンス

SonicWall ファイアウォールは、すべてのネットワーク トラフィックを検査することで、ポートやプロトコルに関係なくアプリケーションを識別します。

- SSL で暗号化されたトラフィックを含むすべてのトラフィックのディープ パケット インスペクション
- 統合されたデータ漏洩防止
- アプリケーションおよび URL フィルタ

## アプリケーション制御

遮断および帯域幅管理のポリシーを管理者の手元で管理できます。事前定義されたアプリケーション種別が、アプリケーション管理とユーザ管理と伴って利用可能です。

- 多数のアプリケーション シグネチャを含む動的更新データベース
- 56 の種別に分類された百万を超える URL と IP アドレスを含む動的更新クラウド データベース
- 遮断、帯域幅管理、DPI バイパスなどの事前定義された動作

## アプリケーション可視化

フロー監視は、アプリケーション トラフィック、送受信帯域幅、ウェブ トラフィック、および標準的なユーザの行動を視覚的に提供します。これは、急速に変化する条件下での生産的ネットワークを維持するために必要な重要な情報を管理者に提供します。

- ネットワーク脅威の恐れや閲覧した URL など、あらゆる情報のリアルタイム データ
- カスタマイズ可能なレポート アクセスのためのフィルタ表示
- 円グラフ表示などのウィジェット作成

# 上位アプリケーション (リスク レベル別)

アプリケーションに影響を及ぼす脆弱性は、プライベート ネットワークに潜入するためにしばしばハッカーによって悪用されます。そのような攻撃からの防御をするために、SonicWall ファイアウォールはネットワークを通るトラフィックを検知、ログ記録、およびランク付けします。

| アプリケーション | リスク ⇅ | トラフィック | セッション |
|---|---|---|---|
| Executable | 3 High | 163.04 KB | 4 |
| General HTTPS MGMT | 2 Elevated | 11.23 MB | 671 |
| Non-SSL traffic over SSL port | 2 Elevated | 4.16 MB | 18 |
| General HTTPS | 2 Elevated | 3.99 MB | 88 |
| HTTP User-Agent | 2 Elevated | 2.19 MB | 68 |
| Twitter | 2 Elevated | 1.58 MB | 18 |
| Document | 2 Elevated | 271.05 KB | 1 |
| General UDP | 2 Elevated | 163.58 KB | 519 |
| General HTTP | 2 Elevated | 95.64 KB | 111 |
| General DNS | 2 Elevated | 41.04 KB | 95 |
| Microsoft Internet Explorer | 2 Elevated | 39.95 KB | 24 |
| Service Version 2 Multicast Listener Re | 2 Elevated | 16.40 KB | 221 |
| Dropbox | 2 Elevated | 10.57 KB | 1 |
| General NETBIOS | 2 Elevated | 3.21 KB | 13 |
| General SNMP | 2 Elevated | 318.00 Bytes | 1 |
| Google | 1 Low | 56.98 MB | 103 |
| YouTube | 1 Low | 27.60 MB | 59 |
| Image | 1 Low | 1.92 MB | 60 |
| Facebook | 1 Low | 685.87 KB | 41 |
| AddThis.com | 1 Low | 134.36 KB | 5 |

⇅ = sorted by

# 上位アプリケーション（種別別）

「上位アプリケーション（種別別）」セクションは、上位のアプリケーション、種別、リスク レベル、トラフィック量、およびセッション数の情報を提供します。この情報は、ネットワーク上で使用されているそれらのアプリケーションのリスク スコアと共に、アプリケーション帯域幅の使用量を知覚的に提供します。

| アプリケーション | 種別 ⇅ | リスク | トラフィック | セッション |
|---|---|---|---|---|
| Dropbox | BACKUP-APPS | 2 Elevated | 10.57 KB | 1 |
| AddThis.com | BROWSING-PRIVACY | 1 Low | 134.36 KB | 5 |
| AppNexus | BROWSING-PRIVACY | 1 Low | 10.55 KB | 1 |
| Executable | FILETYPE-DETECTION | 3 High | 163.04 KB | 4 |
| Document | FILETYPE-DETECTION | 2 Elevated | 271.05 KB | 1 |
| Image | FILETYPE-DETECTION | 1 Low | 1.92 MB | 60 |
| General HTTPS MGMT | General | 2 Elevated | 11.23 MB | 671 |
| General HTTPS | General | 2 Elevated | 3.99 MB | 88 |
| General UDP | General | 2 Elevated | 163.58 KB | 519 |
| General HTTP | General | 2 Elevated | 95.64 KB | 111 |
| General DNS | General | 2 Elevated | 41.04 KB | 95 |
| Service Version 2 Multicast Listener Re | General | 2 Elevated | 16.40 KB | 221 |
| General NETBIOS | General | 2 Elevated | 3.21 KB | 13 |
| General SNMP | General | 2 Elevated | 318.00 Bytes | 1 |
| OCSP | INFRASTRUCTURE | 1 Low | 90.26 KB | 29 |
| Google | MISC-APPS | 1 Low | 56.98 MB | 103 |
| YouTube | MULTIMEDIA | 1 Low | 27.60 MB | 59 |
| SSL | PROTOCOLS | 1 Low | 3.29 MB | 77 |
| DNS Protocol | PROTOCOLS | 1 Low | 293.91 KB | 1,501 |
| SNMP | PROTOCOLS | 1 Low | 5.59 KB | 18 |

⇅ = sorted by

# 上位アプリケーション（種別別） （続き）

「上位アプリケーション（種別別）」セクションは、上位のアプリケーション、種別、リスク レベル、トラフィック量、およびセッション数の情報を提供します。この情報は、ネットワーク上で使用されているそれらのアプリケーションのリスク スコアと共に、アプリケーション帯域幅の使用量を知覚的に提供します。

| アプリケーション | 種別 ⇅ | リスク | トラフィック | セッション |
|---|---|---|---|---|
| Non-SSL traffic over SSL port | PROXY-ACCESS | 2 Elevated | 4.16 MB | 18 |
| Twitter | SOCIAL-NETWORKING | 2 Elevated | 1.58 MB | 18 |
| Facebook | SOCIAL-NETWORKING | 1 Low | 685.87 KB | 41 |
| LinkedIn | SOCIAL-NETWORKING | 1 Low | 27.76 KB | 4 |
| HTTP User-Agent | WEB-BROWSER | 2 Elevated | 2.19 MB | 68 |
| Microsoft Internet Explorer | WEB-BROWSER | 2 Elevated | 39.95 KB | 24 |

⇅ = sorted by

# 上位アプリケーション（帯域幅別）

過度の需要、特に大きいダウンロードやビデオ ストリーミングは、ネットワーク インフラストラクチャ上に容認できない負担をかけます。

これらのアプリケーションは、ネットワーク帯域幅を一番多く消費する代表です。

| アプリケーション | リスク | トラフィック ⇅ | セッション |
|---|---|---|---|
| Google | 1 Low | 56.98 MB | 103 |
| YouTube | 1 Low | 27.60 MB | 59 |
| General HTTPS MGMT | 2 Elevated | 11.23 MB | 671 |
| Non-SSL traffic over SSL port | 2 Elevated | 4.16 MB | 18 |
| General HTTPS | 2 Elevated | 3.99 MB | 88 |
| SSL | 1 Low | 3.29 MB | 77 |
| HTTP User-Agent | 2 Elevated | 2.19 MB | 68 |
| Image | 1 Low | 1.92 MB | 60 |
| Twitter | 2 Elevated | 1.58 MB | 18 |
| Facebook | 1 Low | 685.87 KB | 41 |
| DNS Protocol | 1 Low | 293.91 KB | 1,501 |
| Document | 2 Elevated | 271.05 KB | 1 |
| General UDP | 2 Elevated | 163.58 KB | 519 |
| Executable | 3 High | 163.04 KB | 4 |
| AddThis.com | 1 Low | 134.36 KB | 5 |

## 次のステップ

非生産的かつネットワーク帯域幅の多くを使用するアプリケーションを発見した場合は、SonicWall ファイアウォールのアプリケーション制御を使用して、それらのアプリケーションに対する帯域幅制限またはアクセス遮断を行うポリシーを作成することができます。

⇅ = sorted by

# 上位アプリケーション（帯域幅別）（続き）

過度の需要、特に大きいダウンロードやビデオ ストリーミングは、ネットワーク インフラストラクチャ上に容認できない負担をかけます。

これらのアプリケーションは、ネットワーク帯域幅を一番多く消費する代表です。

| アプリケーション | リスク | トラフィック ⇅ | セッション |
|---|---|---|---|
| OCSP | 1 Low | 90.26 KB | 29 |
| General DNS | 2 Elevated | 41.04 KB | 95 |
| Microsoft Internet Explorer | 2 Elevated | 39.95 KB | 24 |
| LinkedIn | 1 Low | 27.76 KB | 4 |

## 次のステップ

非生産的かつネットワーク帯域幅の多くを使用するアプリケーションを発見した場合は、SonicWall ファイアウォールのアプリケーション制御を使用して、それらのアプリケーションに対する帯域幅制限またはアクセス遮断を行うポリシーを作成することができます。

⇅ = sorted by

# 上位悪用回数

「上位悪用回数」セクションは、SonicWall 次世代ファイアウォールによって遮断された上位の悪用を提供します。レポートには、イベント種別、名前、およびシグネチャ毎に遮断された企ての合計数が含まれます。ファイアウォールによって遮断されたその他の悪用の可能性については、SonicWall SonicAlerts ページをご参照ください。

| イベント種別 | 名前 | 遮断 |
|---|---|---|
| GAV | Eicar-Test-Signature | 1 |
| IDP | MHTML Protocol Handler XSS 2 | 5 |
| IDP | Echo Reply | 1 |

## 次のステップ

上位悪用回数の情報を使用することによって、ネットワーク上のシステムがこれらの種別のマルウェア攻撃または脆弱性に対して対策がされているかどうかを判断することができます。未対策のほとんどは、パッチが当てられていないソフトウェア、またはエンドポイントで使用される脆弱性のあるバージョンのソフトウェアが原因です。

= sorted by

# 上位 URL 種別

「上位 URL 種別」セクションは、SonicWall コンテンツ フィルタ サービスの種別を元にした、HTTP/HTTPS URL トラフィック帯域幅の割合詳細を提供します。

| URL 種別 | トラフィック (%) ⇅ | セッション/回数 |
|---|---|---|
| Business and Economy | 37 | 17 |
| Information Technology/Computer | 24 | 11 |
| Search Engines and Portals | 15 | 7 |
| Social Networking | 7 | 3 |
| Web Communications | 7 | 3 |
| Not Rated | 4 | 2 |
| Gambling | 2 | 1 |
| Sports/Recreation | 2 | 1 |
| Pornography | 2 | 1 |

⇅ = sorted by

# 上位アプリケーション種別（帯域幅別）

「上位アプリケーション種別（帯域幅別）」セクションは、SonicWall アプリケーション制御種別を元にした、上位アプリケーション トラフィック帯域幅の割合詳細を提供します。

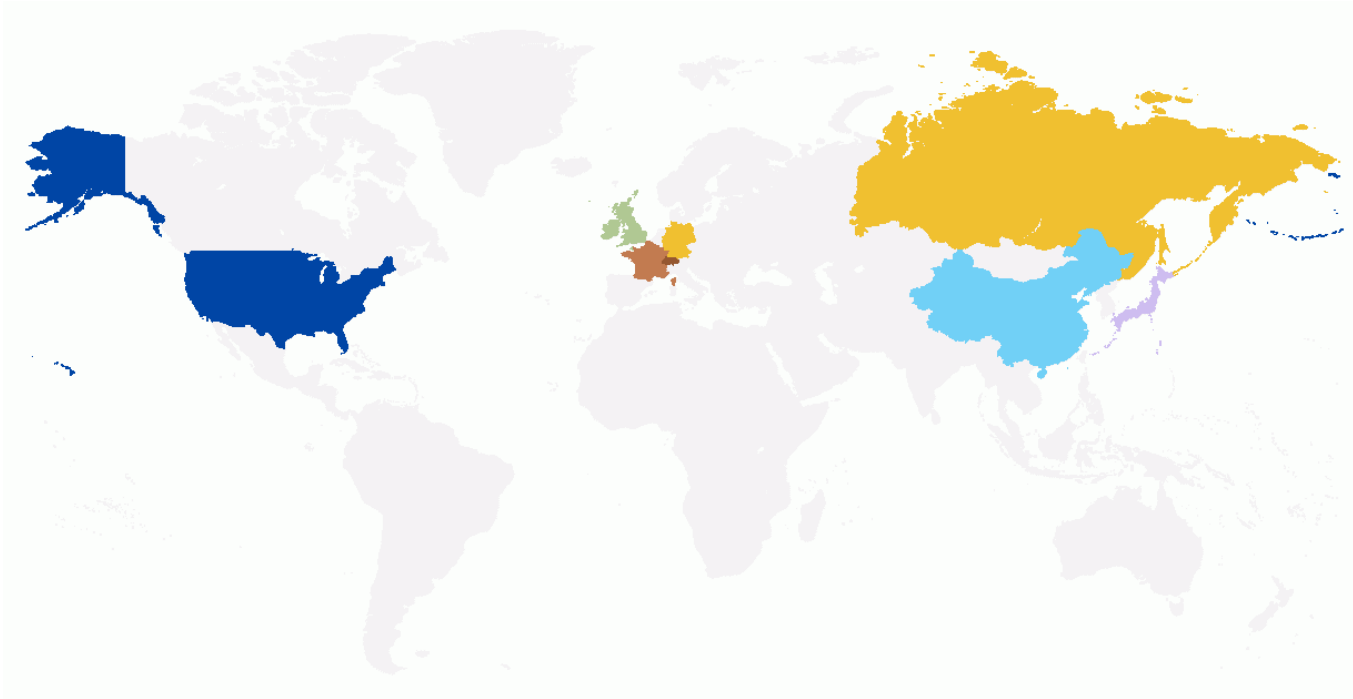
| アプリケーション種別 | トラフィック (%) ⇅ | セッション/回数 |
|---|---|---|
| Browser | 77 | 288 |
| None | 14 | 1724 |
| Application | 6 | 119 |
| Network Infrastructure | 3 | 1621 |

⇅ = sorted by

# 上位国 (トラフィック別)

「上位国 (トラフィック別)」セクションは、ファイアウォール背後のデバイスまたは特定の国に送信されるトラフィックの概要を提供します。このデータは、トラフィックが特定の場所に送信されているのか、また、それらの企てに対して地域 IP またはボットネット ポリシーを作成するべきなのかを判断するために使用されます。

監査期間中において検知された送信元による上位 10 ヶ国が以下に示されます。



| 国 | トラフィック | セッション ⇅ | 遮断 |
|---|---|---|---|
| United States | 96.36 MB | 662 | 0 |
| Japan | 2.86 MB | 80 | 0 |
| China | 1.57 MB | 21 | 0 |
| Germany | 115.46 KB | 20 | 0 |
| Ireland | 576.72 KB | 12 | 0 |

⇅ = sorted by

# 上位セッション使用 (IP 別)

「上位セッション使用 (IP 別)」セクションは、ファイアウォール背後のデバイスの上位 IP アドレスと合計セッション数の一覧を提供します。この情報は、ファイアウォールを通り出るトラフィックの最大消費者の洞察を提供します。

| IP | アドレス | セッション ⇅ |
|---|---|---|
| Total | 229.86 MB | 7,050 |
| 192.168.168.62 | 110.79 MB | 2,975 |
| 192.168.1.1 | 396.56 KB | 1,774 |
| 192.168.168.168 | 11.23 MB | 671 |
| 239.255.255.250 | 140.72 KB | 449 |
| 8.8.8.8 | 34.70 KB | 191 |
| 192.168.1.220 | 56.91 KB | 144 |
| 192.168.1.253 | 4.00 MB | 86 |
| 203.169.10.70 | 2.84 MB | 66 |
| 192.168.1.100 | 509.08 KB | 61 |
| 172.217.26.46 | 4.25 MB | 47 |
| 65.55.158.119 | 6.62 KB | 30 |
| 65.55.158.118 | 14.63 KB | 30 |
| 209.87.209.93 | 3.75 MB | 23 |
| 13.107.5.80 | 3.92 KB | 20 |
| 10.31.1.21 | 6.05 KB | 20 |
| 213.211.198.62 | 115.46 KB | 20 |
| 121.18.231.85 | 2.00 KB | 20 |
| 192.28.144.84 | 21.29 KB | 16 |
| 172.217.26.33 | 1.02 MB | 15 |

⇅ = sorted by

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

# 上位セッション使用 (IP 別) （続き）

「上位セッション使用 (IP 別)」セクションは、ファイアウォール背後のデバイスの上位 IP アドレスと合計セッション数の一覧を提供します。この情報は、ファイアウォールを通り出るトラフィックの最大消費者の洞察を提供します。

| IP | アドレス | セッション ⇅ |
|---|---|---|
| 209.85.228.213 | 11.43 MB | 14 |
| 74.125.171.234 | 14.16 MB | 13 |
| 117.18.237.70 | 1.51 MB | 13 |
| 192.168.1.255 | 3.21 KB | 13 |

⇅ = sorted by

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

# 上位トラフィック使用 (IP 別)

「上位トラフィック使用 (IP 別)」セクションは、ファイアウォール背後のデバイスからの上位 IP アドレスと合計トラフィック数の一覧を提供します。この情報は、ファイアウォールを通るトラフィックの量別の最大消費者の洞察を提供します。

| IP | トラフィック ⇅ | セッション |
|---|---|---|
| Total | 229.86 MB | 7,050 |
| 192.168.168.62 | 110.79 MB | 2,975 |
| 74.125.171.234 | 14.16 MB | 13 |
| 209.85.228.24 | 12.15 MB | 4 |
| 74.125.106.199 | 11.93 MB | 2 |
| 209.85.228.213 | 11.43 MB | 14 |
| 173.194.4.15 | 11.37 MB | 8 |
| 74.125.102.182 | 11.23 MB | 4 |
| 192.168.168.168 | 11.23 MB | 671 |
| 74.125.106.203 | 8.15 MB | 2 |
| 172.217.26.46 | 4.25 MB | 47 |
| 192.168.1.253 | 4.00 MB | 86 |
| 209.87.209.93 | 3.75 MB | 23 |
| 203.169.10.70 | 2.84 MB | 66 |
| 216.58.196.227 | 2.08 MB | 4 |
| 117.18.237.70 | 1.51 MB | 13 |
| 74.125.106.170 | 1.46 MB | 4 |
| 204.212.170.37 | 1.04 MB | 2 |
| 172.217.26.33 | 1.02 MB | 15 |
| 74.125.12.198 | 846.72 KB | 5 |

⇅ = sorted by

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

# 上位トラフィック使用（IP 別） （続き）

「上位トラフィック使用 (IP 別)」セクションは、ファイアウォール背後のデバイスからの上位 IP アドレスと合計トラフィック数の一覧を提供します。この情報は、ファイアウォールを通るトラフィックの量別の最大消費者の洞察を提供します。

| IP | トラフィック ⇅ | セッション |
|---|---|---|
| 31.13.82.36 | 501.41 KB | 5 |
| 172.217.26.34 | 431.33 KB | 12 |
| 192.168.1.1 | 396.56 KB | 1,774 |
| 172.217.25.206 | 316.51 KB | 10 |

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

⇅ = sorted by

# 上位ユーザ セッション

「上位ユーザ セッション」セクションは、合計セッション数と名前別の上位ユーザの一覧を提供します。この情報は、SonicWall ファイアウォール背後のトラフィックの最大消費者の洞察を提供します。

| ユーザ | トラフィック | セッション ⇅ |
|---|---|---|
| Total | 114.95 MB | 3,752 |
| admin | 110.79 MB | 2,975 |
| UNKNOWN | 4.16 MB | 777 |

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

⇅ = sorted by

# 上位ユーザ トラフィック

「上位ユーザ トラフィック」セクションは、合計トラフィックと名前別の上位ユーザの一覧を提供します。この情報は、この情報は、SonicWall ファイアウォール背後のトラフィックの最大消費者の洞察を提供します。

| ユーザ | トラフィック ⇅ | セッション |
|---|---|---|
| Total | 114.95 MB | 3,752 |
| admin | 110.79 MB | 2,975 |
| UNKNOWN | 4.16 MB | 777 |

⇅ = sorted by

## 次のステップ

SonicWall ファイアウォールは、AD グループを活用してユーザ基準のアプリケーション制御と URL フィルタのポリシー作成を可能にする、LDAP/アクティブ ディレクトリ (AD) を伴うシングル サインオン (SSO) インテグレーションをサポートします。レポート ツールはファイアウォール上で利用可能です。GMS/Analyzer でユーザをアプリケーションと URL 基準のレポートに連結することができます。

# レポートの設定

レポートの完全な一式を提供するために、SonicWall 次世代ファイアウォールの管理 GUI で次のオプションを有効にしてください。オプションが設定されていない場合、最終的な SWARM レポートには全データの内の部分集合のみが含まれます。

| ページ | 状況 | |
|---|---|---|
| Aggregate Reporting | ✓ | Enabled. Reporting for aggregate data logs enabled. |
| App Reporting | ✓ | Enabled. Reporting for aggregate application data logs enabled. |
| URL Reporting | ✓ | Enabled. Reporting for aggregate URL data logs enabled. |
| URL Category Reporting | ✓ | Enabled. Reporting for URL category data logs enabled. |
| GAV Reporting | ✓ | Enabled. Either GAV is licensed or GAV status is enabled. |
| Spyware Reporting | ✓ | Enabled. Either Spyware is licensed or Spyware status is enabled. |
| IPS Reporting | ✓ | Enabled. Either IPS is licensed or IPS status is enabled. |
| Geo IP Reporting | ✓ | Enabled. Reporting for aggregate geo IP data logs enabled. |
| App IP Reporting | ✓ | Enabled. Reporting for aggregate app IP data logs enabled. |
| User IP Reporting | ✓ | Enabled. Reporting for aggregate user IP data logs enabled. |

# 付記 1: リスクの定義

1

## 低

識別可能な事件性のあるネットワークの活動、および、リスクの格付けが中程度または深刻である悪質なコードの活動が存在しない場合は、この条件が適用されます。この条件下では、通常の格付けの脅威を阻止するために設計された規定のセキュリティ状態のみが保証されています。

2

## 中

このアプリケーションは、ネットワークに対して正当な目的を持っていない場合があります、また、このアプリケーションは、内部ネットワークに対する不要なトラフィックの源泉である可能性があります。Meebo などの一部のメッセンジャー サービスが、この種別に分類されます。

3

## 高

このアプリケーションは、リソースを大量に消費するか、あるいは、通常のネットワーク ルールを回避するサービスを提供する場合があります。このアプリケーションの実行を許可すると、ユーザが知らないうちに悪意のあるファイルをダウンロードする可能性があります。Ultrasurf などの一部のプロキシ サービスがこの種別に分類されます。また、BitComet などの一部のピアツーピア アプリケーションもこれに該当します。

4

## 深刻

このアプリケーションは、リソースを大量に消費し、大量のネットワーク帯域幅を使用します。また、このアプリケーションは、悪意のある行為を促進ものとしてよく知られており、エンドポイントを感染するためにしばしば利用されます。eMule などの一部のピアツーピア サービスが、この種別に分類されます。

# 付記 2: 脆弱性の説明

### Echo Reply

Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite. ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes.
ICMP traffic may be used to map a network, or help fingerprint an OS. The information used from these methods may be used for

### Eicar-Test-Signature

Trojan

### MHTML Protocol Handler XSS 2

The MHTML protocol handler in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly handle a MIME format in a request for content blocks in a document, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a

# 付記 3: アプリケーションの説明

## AddThis.com

AddThis.com is a web user tracking company.  They partner with websites to include invisible code in the partner website which reports user browsing data to addthis.com backend for the purpose of commercializing user data.

## AppNexus

This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what you do and what you click on, as you go from site to site, surfing the Web. Over time, sites like this can help make an online profile of you usually including the sites you visit, your searches, purchases, and other behavior. Your profile can then be exchanged and sold between various companies like this as well as being sold to other advertisers and marketers.

## DNS Protocol

The Domain Name System (DNS) is a naming system for computers and services connected to the Internet, where DNS translates the hostnames into IP addresses.

## Document

The PDF file format, or Portable Document Format, was created by Adobe Systems to help users in facilitating the exchange of document files.

## Dropbox

Dropbox is storage service that allows users to store and synchronize file content between computers, over the Internet. Dropbox has is compatible with Windows, Mac OS X and Linux platform clients. No-cost user accounts offer 2 GB of storage space, while paid accounts offer significantly higher storage space.

## Executable

Executable and Linking Format files (.exe) are a common standard file format for executable files and libraries.

## Facebook

facebook is an enormously popular social networking site that lets users build a profile page and then seek out and connect with other friends on the service. Users can also join networks for various interests or geographic locations, upload digital media content, and even play games online through the site. facebook is subject to blocking and censure in some countries, and the site appears to continually be re-vamping their privacy policy in an effort to balance user security and business needs.

# 付記 3: アプリケーションの説明

## Google

Google Inc. is most universally known for its leading Internet search capabilities. Google also provides a myriad of additional free services to users, including email, messaging, mapping services, and office productivity tools and applications.

## HTTP User-Agent

HTTP User-Agent is a collection of signatures that identify network traffic based on HTTP User-Agent header, or elements within the header.

## ICMP

The Internet Control Message Protocol (ICMP) is  used by networked computers' operating systems to send error messages.

## Image

BMP (.bmp), also known as BitMap, is a file format for storing digital image data.

## LinkedIn

LinkedIn is a business-oriented social networking for professional contact networking purposes.

## Microsoft Internet Explorer

Microsoft Internet Explorer is the popular web browser from Microsoft.

## Non-SSL traffic over SSL port

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. SSL ports usually exclusively used by SSL/TLS traffic.

# 付記 3: アプリケーションの説明

## OCSP

The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends

## SNMP

Simple Network Management Protocol (SNMP) is an IETF standard for interoperability between Network Management Device communication of data exchange.

## SSL

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are cryptographic protocols that provide secure communications on the Internet.

## Twitter

Twitter is a no-cost-to-user, micro-blogging messaging service, known for allowing user posts of up to 140 characters. Users can send and receive "tweets" through the Twitter website, Short Message Service (SMS), or third-party applications.

## YouTube

YouTube is a popular video sharing website which lets users upload, view, and share video clips. The company uses Adobe Flash Video technology to display a wide variety of user-generated video content, including movie clips.

# 付記 4: アプリケーション

次のアプリケーションがネットワーク上に検知されました。赤色のアプリケーションは、深刻なリスク レベルです。

## アプリケーション (伝送されたデータ)

1. Google (56.98 MB)
2. YouTube (27.60 MB)
3. General HTTPS MGMT (11.23 MB)
4. Non-SSL traffic over SSL port (4.16 MB)
5. General HTTPS (3.99 MB)
6. SSL (3.29 MB)
7. HTTP User-Agent (2.19 MB)
8. Image (1.92 MB)
9. Twitter (1.58 MB)
10. Facebook (685.87 KB)
11. DNS Protocol (293.91 KB)
12. Document (271.05 KB)
13. General UDP (163.58 KB)
14. Executable (163.04 KB)
15. AddThis.com (134.36 KB)
16. General HTTP (95.64 KB)
17. OCSP (90.26 KB)
18. General DNS (41.04 KB)
19. Microsoft Internet Explorer (39.95 KB)
20. LinkedIn (27.76 KB)
21. Service Version 2 Multicast Listener Re (16.40 KB)
22. Dropbox (10.57 KB)
23. AppNexus (10.55 KB)
24. SNMP (5.59 KB)
25. General NETBIOS (3.21 KB)
26. ICMP (960.00 Bytes)
27. General SNMP (318.00 Bytes)