次世代SWG
評価ガイド

Netskopeの次世代セキュアWebゲートウェイ（NG SWG）は、精度の高いポリシー管理、Webフィルタリング、脅威防御、そしてマネージド／アンマネージドアプリやクラウドサービス、Webトラフィックのデータ保護をはじめとするクラウドとWebセキュリティの主要なユースケースに対応するために設計されています。

本書では、6つの一般的なユースケースと各ユースケースに対応するための機能要件、導入・展開時の構成、Netskopeや他社製品の性能をテストする方法を記載しています。

netskope

01 クラウドアプリとWebサイトの使用状況の監視とリスク評価

02 シャドーITなどを含むアンマネージドアプリの精度の高い制御

03 Webフィルタリング機能とクラウドアプリの使用において、どのような操作が許容できるかをユーザーにコーチング

04 マルウェア対策と多層型の高度な脅威検出

05 クラウドやWebサイト全体にわたる高度なデータ保護

06 インターネットへ直接アクセス可能なリモートワーク環境を提供

netskope

01

クラウドアプリとWebサイトの使用状況の監視とリスク評価

調査によると、一般的な企業においてWebトラフィックの約85%は、平均して1,295におよぶアプリとクラウドへの通信によるものです。次世代セキュアWebゲートウェイ（NG SWG）では、Webサイトやクラウドアプリにアクセスする際のアクティビティを基にしたユーザーの行動を監視し、可視化する必要があります。さらに、95%を超えるクラウドアプリがIT部門が管理出来ていないいわゆるシャドーITであるため、IT部門が使用したことのない、もしくは聞いたことがない数多くのクラウドアプリのリスク評価も必要です。

Netskopeは、TLSで暗号化されたトラフィックを復号して検査し、可視化と監視を実施します。ユーザアクティビティを分析し、数千ものマネージドアプリとアンマネージド(管理外)アプリに対するユーザーの行動とWebトラフィックを確認します。Netskope Cloud Confidence Index™（CCI）は、CSAの属性に基づく7つのプロファイル（セキュリティ、リスク、プライバシー、コンプライアンス、脆弱性、財務、法務／監査）により、33,000を超えるクラウドアプリのリスクを評価します。また、リモートワーク時にはインターネット直接アクセス（direct-to-internet）、IPsecとGREトンネルに対応し、モバイルユーザー向けの軽量なステアリング（Netskope Security Cloudとの間に暗号化されたトンネルを張り、そこにクラウドやWeb向けの通信を流す）機能を持ったクライアントを提供しています。

01

機能要件

- Webサイトを分類するとともに、リスク評価によって数万ものクラウドアプリを分析することで、ユーザーのアクティビティと行動を分析します
- クラウドアプリのトラフィックをデコードし、ユーザー、アプリ、インスタンス、データ、アクティビティを分析することで、ユーザー行動の詳細とコンテキストを把握します
- クラウドアプリ間のデータ移動と、この移動に対するアラートを管理します

展開要件

- オフィスとリモートユーザーに対して次世代SWGを展開します。VPNは使用せず、Webトラフィックのバックホールもなくす必要があります。ユーザー、デバイス、またはオフィスからの通信がオンプレミスのデータセンターを一度通ることなく、インターネットへ直接アクセスできる環境を実現します。
- TLSで暗号化されたWebトラフィックを検査するための高い性能と拡張性を提供します

アドバイス：

NG SWGの性能を確認したい場合は、マネージドクラウドアプリから機密データをダウンロードし、同じデータをIT部門のアンマネージドクラウドアプリにアップロードしてください。可視性と監視の精度の高さを検証してください。

テスト方法

- Webセキュリティ製品をインラインで適用するため、オフィスにIPsecトンネルやGREトンネルを使用して展開します。またはリモートユーザーにNetskopeのクライアントを導入します
- 個人の財務および医療のカテゴリなど、暗号化通信を検査してはいけないサイトに対しては例外にします
- Web上でのアクティビティをログするために24～48時間のテスト期間を設けます
- 24～48 時間以内にアクセスしたすべてのアプリおよびクラウドのリスク評価を表示 します
- アプリの個人インスタンスと業務インスタンスの操作という観点からでユーザーを選択し、分析してください
- 特定のユーザーを選択し、サマリページとイベントページ上にそのユーザーに関するすべてのWebアクティビティと動作を表示します
- データ流出を引き起こしたユーザーを調査します
- ユーザー、アプリケーション、インスタンス、データ、アクティビティの可視性と監視を検証します

02

シャドーITなどを含むアンマネージドアプリの精度の高い制御

IT部門で今まで管理されていなかった数千ものクラウドアプリを、ただブロックすることでビジネスの速度を低下させることなく、代わりに精度の高い制御を適用し、リスクのあるアクティビティに照準を当てることでクラウドを安全に有効にすることができます。今必要な次世代セキュアWebゲートウェイ（NG SWG）は、不正を阻止し、正当な操作を安全に実現するために不可欠な精度の高い制御を提供する必要があります。

他社のセキュリティ製品とは異なり、 Netskope の NG SWG は企業やユーザーの回線をとおるクラウドアプリへの通信を含め、数千ものクラウドアプリをリアルタイムで詳細に可視化し、制御できるように最初から設計されています。これにより、リスクの高いクラウドアプリの使用をブロックすることもできますが、注目すべきなのは、企業が使用するアプリの多くを安全に有効活用できることです。

02

機能要件

- あらゆるクラウドトラフィック（数千ものクラウド）を制御し、ログイン、ログアウト、アップロード、ダウンロード、共有、投稿、表示、編集など、多数のアクティビティをリアルタイムでデコードします
- クラウドアプリの、企業が管理するインスタンスと個人インスタンスを区別し、それぞれ違うポリシーを適用します
- ポリシーの一部として、アプリのカテゴリ選択に対応します
- 階層化ポリシーの一部として、「許可」アクションを提供します

アドバイス：
インスタンス認識機能をテストしたい場合は、アプリのインスタンスに対して一貫したURLを持つクラウドアプリを使用します。たとえば、Google Drive、OneDrive for Businessをはじめとする多くのアプリでは、drive.google.comなどの共通のURLが常に使用されるため、どのインスタンス（業務、パートナーまたは個人用）が使用されているかの判断が困難になります。

テスト方法

- Slack、Dropbox、Evernoteなど、業務で使用する可能性がありながら、IT部門で管理されていないクラウドアプリを5〜6個選択します
- IT部門で管理され、個人インスタンスが使用されている可能性のあるクラウドアプリケーションを少なくとも 2つ選択します。たとえば、IT部門が管理するGoogle DriveとSlack 、個人用（管理対象外）のGoogle Drive、OneDrive for Businessなどを選択します
- クラウドセキュリティ製品で、前述で選択したアプリにおいて IT部門が管理しているインスタンスかどうかを識別します
- リアルタイムで可視化および制御をするために構成されたクラウドセキュリティ製品によって、識別された各クラウドアプリに機密データをアップロードし、製品によってそのアクティビティが認識されていることを確認します
- クラウドセキュリティ製品のポリシーを構成し、前述で選択したアプリのいずれかにアップロードされる 個人情報などのPIIデータをブロックしつつも、IT部門で管理されているアプリに対してのみPIIがアップロードできるようにします
- PIIを管理されていないアプリにアップロードし、ブロックされることを確認します
- PIIをIT部門で管理されているアプリインスタンスにアップロードし、アップロードが可能であることを確認します

03

Webフィルタリング機能とクラウドアプリの使用において、どのような操作が許容できるかをユーザーにコーチング

Webフィルタリング機能とクラウドアプリの使用において、どのような操作が許容できるかをユーザーにコーチング。

Webフィルタリングは、新しいWebサイト、Webページ、またはWebコンテンツのURLカテゴリ、カスタムカテゴリ、および動的なWebページを評価するセキュリティソリューションとしてよく知られています。Webトラフィックの85%がクラウドとの通信であるため、次世代セキュアWebゲートウェイ（NG SWG）は、使用されている数千ものクラウドアプリに対してポリシーを適用できる必要があります。

NG SWGは、クラウドアプリおよびWebサイトへのアクセスに対して包括的なWebフィルタリングとユーザーへのコーチング（指導）を実施します。

03

機能要件

- Webトラフィックのカテゴリとカスタムカテゴリによる URLフィルタリングを提供します
- アプリの可視性と監視およびアプリのリスク分析評価を実施します
- 組織で許容される使用方法とリスクの低い、使用が推奨されるアプリに関するユーザー向けのコーチングを実施するためのアラート機能を提供します
- クラウドとWebのポリシーを1つにまとめた、統合ポリシーを提供します

展開要件

- TLSで暗号化されたWebトラフィックを高速で検査するための性能と拡張性を提供します
- 透過型プロキシ経由でWebトラフィック、アプリ、クラウドをインラインで可視化し ます

04

マルウェア対策と多層型の高度な脅威検出

クラウドアプリやSNSを悪用したWebの脅威が増大するにつれ、直接的な標的型攻撃が増加しています。クラウドストレージは従来の、TLSで暗号化されたトラフィックを検査しない防御をバイパスすることが多い場所です。

Officeファイル内のスクリプトやマクロの数は増加傾向にあり、Web脅威のキルチェーンが開始される可能性があります。そのため、ヒューリスティック分析を使用しての実行前スクリプトとマクロの検査は、機械学習の異常検出とともに、多層防御において重要な要素となります。

NG SWGは、Webサイトやクラウドアプリにアクセスする際に、多層型の高度な脅威 保護機能を提供します。

04

展開要件

- マネージドデバイスを使用して、アプリやクラウドサービスをバイパスさせることなく、オフィスやリモートユーザーのすべてのWebトラフィック、アプリ、クラウドに対してリアルタイムの脅威保護機能を提供します
- 検証の一環として、サードパーティの脅威インテリジェンスフィードに加えて、カスタマイズされた侵害指標 IoC（Indicator of Compromise）のハッシュ値とURLを活用します

展開要件

- クラウドベースかつインラインでのWebセキュリティプロキシをオフィスとリモートユーザー向けに展開し、Office 365やその他のマネージドアプリを含むすべてのトラフィックをそちらに誘導します
- TLSで暗号化されたWebトラフィックを検証するための性能と拡張性を提供します

アドバイス：

Webサイトとアプリを使用して、製品のカスタムされたコーチングページ機能をテストします。

テスト方法

- クラウドベースのWebセキュリティ脅威保護機能を有効にして設定します
- 既知のマルウェアに感染したWebサイトにアクセスして、ソリューションがマルウェアをブロックすることを確認します
- 共有フォルダに保存したマルウェアテストファイルをローカルのBoxまたはOneDrive同期クライアントに同期し、ソリューションがそのファイルの同期をブロックしていることを確認します
- HTMLファイルをWeTransferなどのアンマネージドアプリに投稿します。この特定のアプリのアップロード、共有、ダウンロードをブロックするようにWebセキュリティソリューションを設定し、再テストを実施してHTMLファイルがブロックされることを確認します。これは一部のメールセキュリティソリューションを回避する既知のフィッシング詐欺手法です
- ソリューションに含まれたクエリツール内で特定のファイル名またはハッシュ値を検索すると 、Webトラフィック、アプリ、およびクラウドサービスの過去90日間のアクティビティを提供できます。
- ソリューションに対する新しい脅威インテリジェンスとしてカスタマイズされたIoCの ハッシュ値または悪意のあるURLを入力します

05

クラウドやWebサイト全体にわたる高度なデータ保護

アプリとデータがクラウドに移動している昨今、セキュリティ対策もクラウドで提供する必要があります。データおよびデータプライバシーの保護がクラウド導入における主な懸念事項となっている理由に、データの投稿、共有、ダウンロードが容易なことが挙げられます。次世代セキュアWebゲートウェイ（NG SWG）には、精度の高いポリシー管理にコンテンツとコンテキストの両方を適用するクラウド向けの高度なデータ漏洩損失防止（DLP）機能が必要です。

05

機能要件

- すぐに使用できる、数多くのコンプライアンスおよび規制のためのテンプレートを用意しています
- クラウドやWebとの間で送受信されるファイル、Webサイトやsnsへの投稿、Slackなどのクラウドアプリへの投稿を精査します
- あるアプリからダウンロードされ、別のアプリにアップロードされたデータを追跡し ます
- ユーザー、デバイス、場所、アプリ、アプリインスタンス、アクティビティ、コンテ ンツなどのコンテキストを取り入れて、精度を向上させます
- 類似性の照合を可能にするフィンガープリントに対応します

アドバイス：

Slackデスクトップなどのネイティブアプリや、Box DriveやOneDriveなどの同期クライアントを使用して、データ漏洩のテストを試みます。このトラフィックも検査されることを確認します。

展開要件

- TLSで暗号化されたWebトラフィックを検証するための性能と拡張性を提供します
- 透過型プロキシ経由でクラウドおよびWebトラフィックをインラインで可視化します

テスト方法

- PCI、HIPAA、GDPR、日本の住所、氏名、マイナンバーなどに関連するコンプライアンス違反を引き起こす機密データのサンプルを使用します
- DLPポリシーを構成して、コンプライアンスに違反するデータがクラウドアプリやWebサイトのカテゴリにアップロードされたときにアラートを送信します
- さまざまなクラウドアプリやSNSからWeb上のフォーラムまでといった幅広いWebサイトに対してデータをアップロードします
- Slackの投稿に機密データをコピーして貼り付けます
- アラートが発生することを確認し、インシデント管理プロセスを見ていきます

06

インターネットへ直接アクセス可能なリモートワーク環境を提供

デジタルトランスフォーメーションが推進される中、企業ネットワークはリモートオフィスが高価な専用回線を経由してデータをバックホールするハブ＆スポークアーキテクチャから、インターネットへの直接アクセスへと変化しています。次世代セキュアWebゲートウェイ（NG SWG）には、ユーザーがどこにいてもクラウドとWebに高速かつ安全にアクセスできるインフラストラクチャと機能が必要です。

06

機能要件

- 高いパフォーマンスとセキュリティのために最適化された、グローバルに展開された分散ネットワークインフラストラクチャを提供します
- インターネットへの直接アクセスのためにリモートオフィスに、そのインフラストラクチャに対してIPsecまたはGREトンネルを提供します
- オフィス外のマネージドデバイスには軽量なステアリング機能のあるクライアント（約10MB）を提供します
- 場所、カテゴリ、またはドメインに基づいてトラフィックをバイパスします
- セキュリティポスチャーに基づいてデバイスを分類し、それをアクセスポリシーに反映します

展開要件

- マネージドデバイスからのすべてのクラウドおよびWebへのトラフィックを、クラウド型で提供されるセキュリティサービスに誘導するクライアントを展開します

ユースケース	製品 A 点数 (0-5): 必要な製品:	製品 B 点数 (0-5): 必要な製品:
クラウドアプリとWebサイトの使用状況の監視とリスク評価	点数: 製品:	点数: 製品:
シャドーITなどを含むアンマネージドアプリの精度の高い制御	点数: 製品:	点数: 製品:
Webフィルタリング機能とクラウドアプリの使用において、どのような操作が許容できるかをユーザーにコーチング	点数: 製品:	点数: 製品:
マルウェア対策と多層型の高度な脅威検出	点数: 製品:	点数: 製品:
クラウドやWebサイト全体にわたる高度なデータ保護	点数: 製品:	点数: 製品:
インターネットへ直接アクセス可能なリモートワーク環境を提供	点数: 製品:	点数: 製品:
完全に要件を満たせたユースケース数		

About Netskope

従来のセキュリティ対策ではもはや対応しきれなくなってきています。業務に支障をきたすことなく、あらゆる場所でデータとユーザーを保護できる新しい対策が必要です。Netskopeのセキュリティクラウドは、クラウド、Webサイト、プライベートアプリにアクセスする際に、場所やデバイスを問わずに、他にはない可視性やリアルタイムのデータ保護、脅威防御を提供します。クラウドを理解し、世界最大かつ最速レベルのセキュリティネットワークからデータを中心にして考えるセキュリティを提供できるのはNetskopeだけです。業務の効率をあげ、安全なデジタルトランスフォーメーションを推進するために不可欠な保護とスピードをバランスよく保つアプローチで、世界のトップ企業や組織を支えています。Netskopeのセキュリティソリューションで新しい対策を構築しませんか？

netskope.com