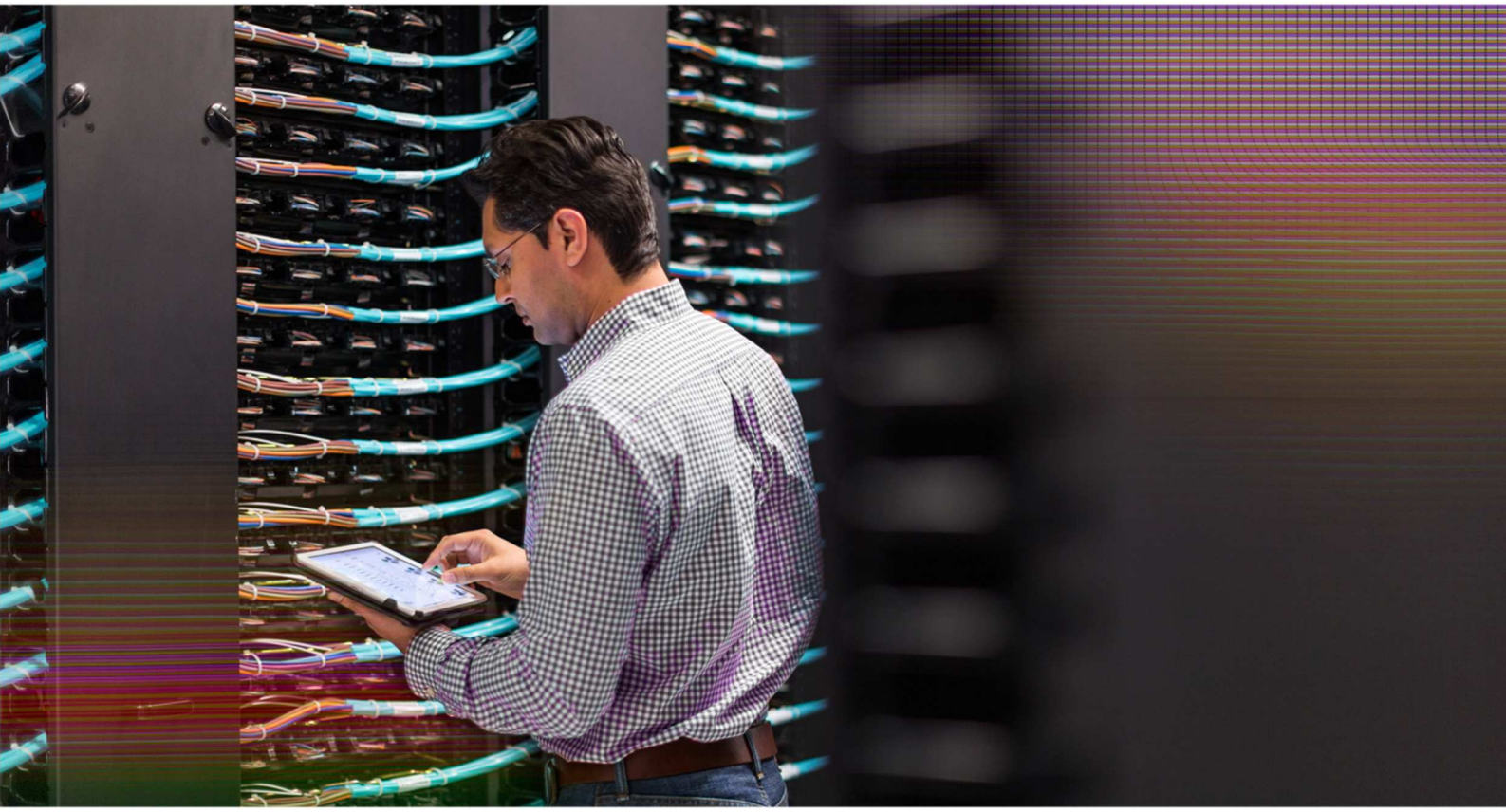
ホワイトペーパー



Citrix NetScaler：
次世代データセンターおよびクラウドベースセキュリティの礎

データセンターの堅牢なセキュリティがかつてないほど必要とされる今日では、さまざまな法的義務、標的型攻撃の増加、蝕まれ続ける境界中心型セキュリティモデルといった従来からの課題や懸念に加えて、自然な「関門」がほとんどない、極めて動的なエンタープライズクラウドアーキテクチャーやフラットネットワークへの対処の必要性が生じています。絶えず存在する予算のプレッシャーもあることから、データセンターの既存のインフラストラクチャーを利用して、セキュリティ強化の基盤を築かなければなりません。

エンタープライズクラウドネットワーク構築のための最高の ADC（アプリケーションデリバリーコントローラー）、Citrix® NetScaler®は、まさにこの目的にうってつけのソリューションです。すでに数千の企業データセンターで戦略的コンポーネントとして活用されている NetScaler には、データセンターに必須のセキュリティ機能が豊富に搭載されています。高額なスタンドアロンのセキュリティソリューションを多数買い揃える必要性もありません。NetScaler には重要性が極めて高いアプリケーションセキュリティ、ネットワーク/インフラストラクチャーセキュリティ、アイデンティティ/アクセス管理機能があるだけでなく、近隣のセキュリティ領域をもカバーする、パートナー製品の豊かなエコシステムが確立されています。

NetScaler のデータセンターセキュリティ機能

アプリケーションセキュリティ
- NetScaler アプリケーションファイアウォール
- データ漏洩防止
- レイヤ 7 攻撃からの保護

ネットワーク/インフラストラクチャーセキュリティ
- 妥協のない SSL
- DNS セキュリティ
- レイヤ 4 攻撃からの保護

アイデンティティ/アクセス管理
セキュリティファブリック/パートナーエコシステム

そのため、強力でありながらコスト効率の点でも優れた、次世代データセンターおよびクラウドベースセキュリティの基盤を構築できます。

NetScaler によるアプリケーションセキュリティ

セキュリティ担当者は、アプリケーション層のセキュリティに多大な時間、労力、資金を惜しみなく投入しています。結局は、アプリケーション層の脆弱性のあるサービス、欠陥のあるビジネスロジック、価値の高いデータを攻撃した方が実りが多いのは明らかだからです。そのため、NetScaler にはフル機能版のアプリケーションファイアウォール、データ漏洩防止、DoS（サービス妨害）のようなレイヤ 7 攻撃に対する防護策といった、アプリケーション層の保護機能が豊富に搭載されています。

NetScaler アプリケーションファイアウォール

アプリケーション層の脆弱性を狙った攻撃は、インターネット攻撃の 7 割以上を占めます。にもかかわらず、従来のネットワークファイアウォールには、これらの攻撃からの防護に必要な可視性と制御性がありません。NetScaler アプリケーションファイアウォールの存在意義はそこにあります。NetScaler アプリケーションファイアウォールは、Web アプリケーションや Web サービスアプリケーションに対する既知および未知の攻撃を未然に阻止する能力を持つ、ICSA の認定を受けた総合的な Web アプリケーション用セキュリティソリューションです。ハイブリッドセキュリティモデルの採用と、SSL 暗号化通信を含むすべての双方向トラフィックの解析により、アプリケーションに一切手を加えずに、セキュリティを脅かすさまざまな脅威に対処することができます。

ハイブリッドセキュリティモデル：ポジティブセキュリティモデルとネガティブセキュリティモデルの両方を組み合わせることにより、あらゆる方式の攻撃からの最も完璧な防護を実現できます。新しい未知の手口に対抗する手段として、ポジティブモデルのポリシーエンジンはユーザー/アプリケーション間の許容される通信についての知識を持ち、その範疇に入らないトラフィックをすべて遮断します。ネガティブモデルのエンジンはそれを補う手段として、攻撃のシグニチャに基づいて、既知の脅威からアプリケーションを守ります。

XML 保護：XML アプリケーションに対する一般的な脅威（クロスサイトスクリプティング、コマンドインジェクションなど）の阻止に加えて、NetScaler アプリケーションファイアウォールには XML に特化した豊富な保護機能があります。たとえば、スキーマ検証による SOAP メッセージと XML ペイロードの徹底チェック、悪意のある実行ファイルを含んだ XML アタッチメントの遮断、XPath インジェクションを利用した不正アクセスの防止、DoS 攻撃（過剰な再帰処理など）の阻止などを行うことができます。

動的要素の高度な保護：デフォルトの保護プロファイルを強化した高度なプロファイルを使用することにより、ユーザー固有のコンテンツを扱うアプリケーションのセキュリティを保つことができます。セッションに対応した複数の保護機能によって、cookie、フォームフィールド、セッション固有の URL といったアプリケーションの動的要素の保護を行えるため、クライアント/サーバー間の信頼関係を突く攻撃（クロスサイトリクエストフォージェリなど）を阻止することができます。アプリケーションの動的性はポジティブセキュリティエンジンで処理され、ポリシーの中で各動的要素の明示的な定義を行わずにセキュリティを保護することができます。検討する必要があるのは例外のみであるため、設定が簡単になり、変更管理もシンプルになります。

セキュリティポリシーのカスタマイズ：高度な学習エンジンにより、企業 Web アプリケーションの望ましい振る舞いを自動的に特定し、人間が判読できる形式で推奨ポリシーを生成できます。管理者はこのセキュリティポリシーを各アプリケーション固有の要件に合わせてカスタマイズし、誤検知を防止することができます。

法令順守：NetScaler アプリケーションファイアウォールは、データセキュリティに関する規制の順守にも役立ちます。たとえば、PCI DSS（クレジットカード業界データセキュリティ標準）では、クレジットカード情報を扱う一般向けのアクセス可能なアプリケーションを、Web アプリケーションファイアウォールで保護することが推奨されています。詳細レポートを生成し、ファイアウォールポリシーで定義されている、クレジットカード業界の規制に関係する保護をすべて文書化することができます。

妥協のない性能：業界最高レベルの性能を持つ Web アプリケーションセキュリティソリューションとして、最大 20Gbps の総合的保護処理スループットが実現されているため、アプリケーション応答時間が犠牲になることがありません。高度なアクセラレーション技術（コンテンツキャッシングなど）やサーバーオフロード機能（TCP 接続管理、SSL 暗号化/暗号化解除、データ圧縮などのオフローディング）により、アプリケーション性能も改善することができます。

完全統合アーキテクチャー：NetScaler アプリケーションファイアウォールは導入が簡単なだけでなく、NetScaler プラットフォームとの緊密な統合が実現されています。オブジェクトレベルとポリシーレベルの共有による管理の簡素化に加えて、システムレベルの処理共有によってパケット処理の重複を回避することができるため、高性能を保つことができます。

NSS Labs によるテスト：NetScaler アプリケーションファイアウォールは NSS Labs の推奨リストに登録されています。NSS Labs のレポートによると、競合製品の中で TCO が最も低く、総合防御率は 99.8%でした。詳細については、Citrix NetScaler アプリケーションファイアウォールが NSS Labs によるウェブアプリケーションファイアウォールテストで「推奨」の評価を獲得を参照してください。

データ漏洩防止

アプリケーションサーバーからの応答に含まれる重要データの漏洩は、アプリケーションに対する攻撃、アプリケーションの設計上の欠陥、または正規ユーザーの不注意から起こります。とるべき対策として、また多層防御セキュリティ戦略の要として、このような漏洩に対する積極的な防護策が必要となります。NetScaler には、この要件を満たすために、使いやすく、直感的に扱うことができるデータ漏洩保護機能があります。

NetScaler アプリケーションファイアウォールにはセーフオブジェクトデータチェック機能があり、社会保障番号、注文コード、国や地域が分かる電話番号といった重要ビジネス情報についての、カスタマイズ性のある保護を実現できます。管理者が指定した正規表現やカスタムプラグインによって、保護する必要のある情報の形式を指定し、その情報の漏洩を防止するためのルールを定めることができます。ユーザーからの要求の中に、セーフオブジェクト定義と一致するものが見つかると、次のような対策を発動することができます。

- 応答の遮断
- 保護すべき情報の隠蔽
- 保護すべき情報を取り除いたうえで応答をユーザーに送信

これらの防護策をセーフオブジェクトルールごとに個別に指定できます。

NetScaler には、クレジットカード番号のうっかり漏洩を防ぐクレジットカードチェック機能もあります。ヘッダ情報とペイロードデータの両方を調査することによって検知漏れを徹底的に防ぐと同時に、アルゴリズムによる文字列照合によって誤検知のない高精度な検出を行うことができます。クレジットカード番号が見つかり、管理者が当該アプリケーションへのクレジットカード番号送信を許可していない場合は、応答全体を遮断したり、（xxxx-xxxx-xxxx-5678 のように）番号の最後の 4 桁以外を隠蔽したりすることができます。

図 1：NetScaler は機密性のある顧客情報の漏洩を防ぎます。

これらも、うっかりミスや攻撃の監視・検出だけでなく、その影響を大きく抑えることのできる強力な機能の 1 つです。

レイヤ 7 攻撃からのその他の保護

NetScaler には、アプリケーション層攻撃からの保護機能が他にもあります。

HTTP プロトコル検証：不正な要求や HTTP プロトコルの不正な挙動を利用した攻撃を防ぐには、RFC 順守と HTTP の利用についてのベストプラクティスを守らせることが大変効果的です。NetScaler では、標準搭載されたコンテンツフィルタ機能、カスタム応答機能、双方向 HTTP 書き換え機能を利用することにより、セキュリティポリシーの中にさらなるカスタムチェックを追加することもできます。たとえば、特定の地域から接続しているときしか Web サイトの特定の部分にアクセスできないようにしたり、HTTP に基づく脅威（Nimda や Code Red など）からの保護を行ったり、サーバーからの応答の中から、攻撃の糸口になりえる情報を取り除いたりすることができます。

図 2：Citrix NetScaler は Web アプリケーションのセキュリティを守ります。

HTTP DoS 攻撃からの保護：NetScaler では、HTTP GET フラッド攻撃に対する革新的な手法が採用されています。攻撃状態が検出されると（キューの中の要求数が設定可能なしきい値を超えると）、一定割合のクライアント（この割合は調整できます）に負荷の低い演算問題を送ります。この演算問題は、正当なクライアントだけが適切な応答を容易に返すことができ、不正な DoS ドローンはそうすることができないように構築されています。この仕組みによって、不正な要求と正当なアプリケーションユーザーからの要求を区別することができます。さらに、アダプティブタイムアウトのようなその他の手法も利用すると、SlowRead 攻撃や SlowPost 攻撃のような他のタイプの DoS 型脅威からの防護も実現できます。

速度制限など：DoS 攻撃対策の 1 つとして、一定の上限を超えるトラフィックのスロットリングやリダイレクトを行うことにより、ネットワークやサーバーの過負荷を防ぐ手法があります。この目的のために、AppExpert 速度制御機能により、特定のリソース（仮想サーバー、ドメイン、URL）への、またはこれらのリソースからの接続、要求、データ通信速度に基づいて NetScaler ポリシーを発動させることができます。これと密接に関連する次の機能もあります。

- サージ保護（サーバーへのトラフィック殺到の影響緩和）
- 優先キューイング（高需要期間は重要なリソースをそれ以外のリソースより優先的に処理）

NetScaler によるネットワーク/インフラストラクチャーセキュリティ

NetScaler にはネットワークやインフラストラクチャーのセキュリティ機能もあります。その中で特に注目すべきなのは、SSL 暗号化の総合的サポート、DNS セキュリティ、およびレイヤ 4 攻撃からの保護です。

妥協のない SSL

暗号化トラフィックにアプリケーション配信ポリシーを完全適用するにしても、バックエンドサーバーインフラストラクチャーのオフローディングを行うにしても、ADC には SSL トラフィックの処理能力が必要です。しかし、2 つの要因によって、SSL 処理要件がインフラストラクチャーリソースの限界以上に高まっているため、もはやこの分野の基本機能を備えているだけでは十分ではありません。

第一の要因は、SSL Everywhere（常時 SSL）の普及です。SSL Everywhere とは、一般に顧客の不安を和らげ、Firesheep のようなハッキングツールに対抗することを目的として、ログインページのようなアプリケーションの秘匿性のある部分だけでなく、アプリケーション表面積全体に対して暗号化を適用する手法です。これによって SSL フットプリントが一気に増大します。

第二の要因は、1024 ビット鍵から 2048 ビット（またはそれ以上の長さの）鍵への移行です。この移行は NIST（米国国立標準技術研究所）からの勧告に従う意味もありますが、2013 年 12 月 31 日をもって、2048 ビットより脆弱な鍵を使用する Web サイトのサポートが主要ブラウザベンダー各社によって打ち切られたことも理由の 1 つです。その結果として暗号強度は飛躍的に高まりましたが、それと引き換えに必要な処理能力が 5 倍以上になりました。

NetScaler アプライアンスは、この両方のトレンドに対処することができます。2048 ビット鍵と 4096 ビット鍵の両方に対応した専用 SSL アクセラレーションハードウェアの搭載により、セキュリティ強化と高品位なユーザーエクスペリエンスを両立させることができます。

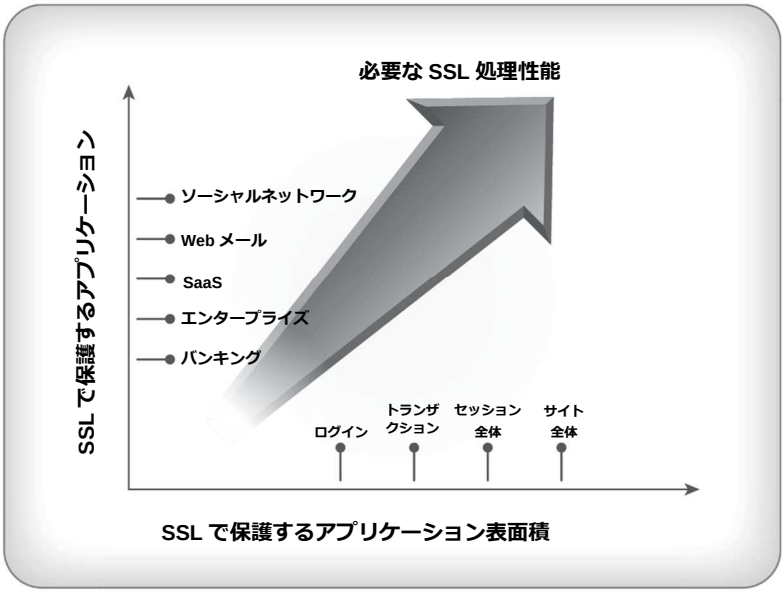


図 3：SSL Everywhere の実現には高いセキュリティ要件と性能要件が必要です。

もう 1 つの関連機能に、ポリシーに基づく暗号化があります。この機能を利用すると、本来は暗号化を利用できるように設計されていないレガシーWeb アプリケーションのうち、秘匿が必要になった部分を自動的に暗号化することができます。

高レベルな暗号保証が必要な場合は、FIPS 140-2 レベル 2 に準拠したモデルを実現することもできます。

SSL トラフィックアクセラレーション

知的資産、金融情報、顧客や社員の個人情報といった機密性のある企業情報の転送のために、ビジネスアプリケーションで SSL がますます使われるようになったため、SSL 暗号鍵の管理が多くの組織で見過ごされている重要なセキュリティ問題になっています。

この鍵管理には、鍵を直接的な攻撃からどのように保護するかだけでなく、鍵のバックアップとシステム障害/災害時の復旧といった運用上の問題、そして管理者による鍵の利用の制御と監視に関するコンプライアンスの問題なども含まれます。

SSL トラフィックが増大すると、接続の両側のシステムでのトラフィック暗号化/暗号化解除が必要なだけでなく、ハンドシェーク構築と信用証明情報の認証にかなりの演算リソースを割かなければならず、そのためにブラウザクライアント、Web サーバー、ネットワークの速度が低下することがあります。

基幹業務アプリケーション用により多くの機密情報が SSL 転送されるようになり、SSL トラフィックが増大したときに、ハードウェアとネットワーク帯域に対する多額の投資を行わずに、暗号鍵とアプリケーション性能を保護するには、どうすればよいのでしょうか。

Citrix NetScaler と Thales nShield を連携させると、暗号鍵のセキュリティ強化と SSL 処理のオフローディングおよびアクセラレーションを実現できます。Thales nShield は、数多くの SSL 鍵を FIPS 140-2 レベル 3 の認定を受けた環境で管理するソリューションです。この Citrix と Thales の複合ソリューションを利用すると、SSL トラフィックの最適化と重要な暗号鍵の安全な管理が可能になり、IT インフラストラクチャーの中で重要情報が晒される機会を最小限に抑えることができます。

この統合の詳細については「安全な SSL：高速な SSL」を参照してください。

DNS セキュリティ

DNS は今日のデータセンターに欠かせないインフラストラクチャーサービスです。堅牢で安全な DNS 環境がなければ、重要なサービスやアプリケーションの可用性とアクセス性が脅かされてしまいます。

NetScaler には、組織内の DNS サーバーの高スケーラブルな負荷分散を行うモード（DNS プロキシモード）に加えて、ADNS（権威 DNS）サーバーとして動作し、正引き/逆引き要求を直接処理するモードがあります。

どちらの導入方式でも、次の特長を備えた堅牢で安全な環境を構築できます。

堅牢な設計 – NetScaler の DNS サービスは最初から堅牢性を考慮して設計されています。オープンソースの BIND に基づいていないため、次々と見つかる BIND の脆弱性の影響を受けません。

RFC の順守/適用 – NetScaler には、DNS プロトコルの完全な検証と適用を行い、不正な形式の DNS 要求を利用した攻撃や DNS の悪用を自動的に阻止する機能があります。

ネイティブ DNS 速度制限 – DNS フラッド攻撃を防止するため、ポリシーを設定することによって、設定したパラメータに基づいて速度を制限したり、照会を破棄したりすることができます。この制御は照会のタイプ別やドメイン名別に実装することができるため、複数のドメインが存在する場合に、ドメインごとに別々のポリシーを適用できます。

DNSSEC によるキャッシュポイズニングからの保護 – 深刻な脅威の 1 つに、応答をハイジャックすることによってハッカーが DNS サーバーに偽造レコードを送りつけ、DNS キャッシュに不正な情報を忍び込ませる手口があります。このような攻撃を受けると、偽造レコードに基づいて、ハッカーが制御権を持つサイトにユーザーが誘導され、悪意のあるコンテンツが渡されたり、アカウントやパスワード情報の抜き取りが試みられてしまう可能性があります。NetScaler では、次の 2 つの強力な保護機能によって、これらの脅威からの保護を行うことができます。

- DNSSEC 機能の標準サポート：ADNS 構成とプロキシ DNS 構成のどちらでも、この機能を実装できます。NetScaler では応答に署名を付けることができるため、照会送信元のクライアントは応答が正当なものであり、その内容が改竄されていないことを確認できます。この標準に基づく手法によって、DNS キャッシュへの偽造レコードの侵入を防止することができます。
- DNS トランザクション ID とソースポート情報のランダム化：これらの対策によって、ハッカーが要求の中に必要な情報を挿入し、DNS レコードを偽造することが困難になります。

レイヤ 4 攻撃からの保護

NetScaler にはネットワーク層の DoS 攻撃に対する防護機能があり、クライアントとの正当な接続が確立され、正当な要求が渡されるまでは、バックエンドリソースの割り当てを行わないようにすることができます。

たとえば、TCP ベースの SYN フラッド攻撃に対する防護策は、クライアントと NetScaler アプライアンスとの 3 ウェイハンドシェークが完全に完了するまでは、リソースの割り当てを行わないことが基本となります。それに加えて、性能最適化/セキュリティ強化版の SYN cookie も利用することができます。

さらに、ハードウェアプラットフォーム/オペレーティングシステムアーキテクチャーには毎秒数百万の SYN パケットを処理する能力があるため、NetScaler そのものもこれらの攻撃に耐えることができます。

ネットワーク層のその他のセキュリティ保護機能には、（a）必要なアプリケーショントラフィックのみを許可し、それ以外のものはすべて阻止することのできるレイヤ 3/レイヤ 4 レベルの ACL（アクセス制御リスト）、（b）前述の速度制限、サージ保護、優先キューイング機能、および（c）次の能力を持つように拡張された、標準に準拠した高性能 TCP/IP スタックがあります。

- バックエンドリソースを危険に晒す可能性のある不正な形式のトラフィックの自動的な破棄
- ハッカーによる攻撃の糸口となる接続/ホスト情報（サーバーアドレスやポート番号など）の隠蔽
- ICPM フラッド攻撃、パイプライン攻撃、Teardrop 攻撃、Land 攻撃、Fraggle 攻撃、スモール/ゼロウィンドウ攻撃、ゾンビ接続攻撃といった、さまざまな DoS 型脅威の自動的な阻止

アプリケーションデリバリー用の AAA 機能

データセンターのセキュリティを高めるには、ネットワーク層、インフラストラクチャー層、アプリケーション層に堅牢性を持たせることが大切ですが、それだけでは十分ではありません。ユーザー層についての対策も必要です。NetScaler には次のような総合的な AAA（認証・アクセス権付与・監査）機能があります。

- **認証** – ユーザーの身元を確認する機能
- **アクセス権付与** – それぞれのユーザーがどのリソースにアクセスできるかを確認し、それ以外のリソースへのアクセスは行えないようにする機能
- **監査** –（トラブルシューティング、レポーティング、コンプライアンス順守の目的のために）各ユーザーの活動についての詳細な記録を残す機能

NetScaler の AAA ソリューションのメリットは、パスワード変更への対応や、認証方式（ローカル認証、RADIUS、LDAP、TACACS、証明書、NTLM/Kerberos、SAML/SAML2 など）の幅広いサポートといった多機能性だけではありません。むしろ、これらのサービスの中央化と整理統合を行えることのほうが重要です。NetScaler では、これらの制御の実装、適用、管理をアプリケーションごとに個別に行う代わりに、これらを一元化することができます。この手法には次のメリットがあります。

- **サーバー性能向上** – バックエンドリソースを AAA 処理の負担から解放することができるため、サーバー負荷軽減とアプリケーション性能向上を実現できます。
- **レガシーアプリケーションへのセキュリティの組み込み** – 本来は AAA 機能がないレガシーアプリケーションにセキュリティ機能を追加できます。アプリケーションの修正を行わずに、より強力な認証の採用や、よりきめ細かなロギングを行えるなど、選択肢が増すため、モダンアプリケーションにもメリットがあります。
- **統一的なユーザーエクスペリエンス** – 認証方式、パラメータ（タイムアウトなど）、ポリシー（エラーの扱いなど）を、複数のアプリケーションにわたって共通化することができるため、統一的なユーザーエクスペリエンスを実現できます。
- **SSO（シングルサインオン）** – 1 回ログインを行うだけで、特定のドメイン内の全リソースに対する透過的なログインを行うことができます。
- **セキュリティ強化** – 多要素認証や第二認証、安全なログアウト（認証 cookies による自動タイムアウト）、別々のユーザーやリソースに対するポリシーの共通化など、さまざまな手法によってセキュリティを強化できます。
- **シンプルなセキュリティ設計** –（数十、数百の場所からではなく）1 カ所から AAA サービスの実装と管理を行うことができるため、効率的な管理が可能となり、ミスによって組織の防衛網に抜け穴ができる可能性を減らすことができます。

NetScaler のパートナー製品によるセキュリティファブリックの構築

パートナー製品の豊かなエコシステムを活用すると、データセンターセキュリティソリューションとしての NetScaler の価値をさらに高めることができます。主な活用事例には次のようなものがあります。

- **レポーティングと分析** – 標準に基づくテクノロジー、NetScaler AppFlow®を利用すると、IPFIX（NetFlow 用の IETF 標準）で収集された TCP レベルの情報を拡張し、その中にフローごとのアプリケーション層データレコードを組み込むことができます。AppFlow は、専用のタップ、ソフトウェアエージェント、追加デバイスを使用する必要のない完全な非侵入型ソリューションであり、既存の NetScaler インフラストラクチャーを利用して、誰が、いつ、どのリソースを、どの程度利用したかを調査することができます。このデータを Citrix Ready®パートナーである Splunk 社の Splunk for NetScaler with AppFlow ソリューションに取り込むと、SSL VPN イベント、アプリケーションファイアウォールイベント、ポリシー違反、攻撃を受けたリソースのような、セキュリティに関する情報の分析とレポーティングを行うことができます。
- **SIEM（セキュリティ情報イベント管理）** – NetScaler AppFirewall™には、CEF（Common Event Format）形式および syslog 形式によるサードパーティ製ソリューションへのデータ出力機能も搭載されています。これにより、たとえば NetScaler のイベント情報やログ情報を SIEM プラットフォーム（HP ArcSight や RSA enVision など）で処理し、その情報をセキュリティやコンプライアンスの運用管理に役立てることができます。

- **脆弱性管理** – Citrix Ready パートナーである Cenzic 社の HailStorm および ClickToSecure を利用すると、Web サイトの動的なブラックボックステストを実施して、脆弱性の情報を生成することができます。この事例では、Cenzic 社のソリューションによるスキャン結果を NetScaler アプリケーションファイアウォールに簡単に取り込み、発見されたアプリケーションやサービスの脆弱性を突く脅威からの保護ルールを定めることができます。

その他の代表的パートナーとそのテクノロジーには、RSA（アダプティブ認証）、Qualys（脆弱性管理）, Sourcefire（IPS およびリアルタイムネットワーク検知）、TrendMicro（AV および Web セキュリティ）、Venafi（鍵/証明書管理）などがあります。これらの、およびその他の豊富なパートナー製品群を利用することにより、NetScaler によって築かれた基盤をもとにした、完全なデータセンターセキュリティファブリックを構築できます。

まとめ

NetScaler は、単なるデータセンターの保護に留まらない真の価値をもたらします。アプリケーションの可用性向上、最適化、セキュリティ保護に加えて、完全な可視性とレポーティング機能によって、コンプライアンスが守られているかどうか、サービスレベルが保たれているかどうかを検証できます。

常に限られている予算、そしてデータセンターのセキュリティを強化する必要性の高まりにより、より少ない予算でより多くの成果を上げなければならない状況が生まれています。エンタープライズクラウドネットワーク構築のための最高のアプリケーションデリバリーコントローラー、Citrix NetScaler は、この状況に完全にマッチします。アプリケーション層、ネットワーク層、ユーザー層の総合的セキュリティ機能、そして相互運用性を備えたパートナー製品の豊かなエコシステムにより、今日の企業組織の既存のインフラストラクチャーを利用して、次世代データセンターのための堅牢でコスト効率の高いセキュリティ基盤を築くことができます。

Citrix について

Citrix（NASDAQ:CTXS）は、企業と人々の新しい働き方を実現するソフトウェア定義型のワークプレース、仮想化統合、モビリティ管理、ネットワーキング、SaaS ソリューションのリーディングカンパニーです。シトリックスのソリューションは、あらゆるデバイス、あらゆるネットワーク、あらゆるクラウドからのアプリケーション、デスクトップ、データ、コミュニケーションの迅速な利用を可能にする安全なモバイルワークプレースを実現し、ビジネスにモビリティをもたらします。シトリックスの 2014 年度の年間売上高は 31.4 億ドルで、そのソリューションは世界中の 33 万以上の企業や組織において、1 億人以上の人々に利用されています。シトリックスの詳細については www.citrix.co.jp をご覧ください。